1.第三方接⼝交互数据加密

说明

本功能旨在第三方系统对接码上生活时保证数据安全 、调用方身份确认。

字段说明

appId 以通知本系统调用方身份 本文示例： poppy\_life timeStamp 秒级时间戳校验， 防止拦截签名后重复使用 本文示例： 1551925807

sign 签名 本文示例： AC23CFAC9E0357205E76943095CFD984

appSecret 密钥串 本文示例： A787sHGJShghsT898HJy

功能点描述

创建身份信息

第三方通过填写appId 注册至本系统， 用于申请密钥串appSecret 。 加密方式目前仅支持 ND5

注： 身份信息⼀旦生成无法修改， 请妥善保管好密钥串。

请求参数签名

调用方在请求头中携带属性如下：

appId

timeStamp

sign

以充值积分调用过程举例：



1. 不同请求参数处理

 Get请求

将参数列表按传递先后顺序排列成⼀个 string。 用 & 分隔每个参数 。当前 Payload 如 下所示。

merchantId=1157967831234&merchantName=多多评商户

&rechargeType=2&point=30&remark=充值积分

 非Get请求

将请求头属性 Content-Type 设置为 context/json， 参数以 body 方式传入 。当前 Payload 如下所示。

{

"merchantId":1157967831234,

"merchantName":"多多评商户",

"rechargeType":2,

"point":30,

"remark":"充值积分"

}

2. 组装Payload

1. timeStamp

2. appId

3. 参数PayLoad

4. secretKey

Get请求组装后结果如下：



1551925807poppy\_lifemerchantId=1157967831234&merchantName=多多评商户 &rechargeType=2&point=30&remark=充值积分A787sHGJShghsT898HJy

计算签名

使用创建身份信息时的加密方式对 Payload 进行加密

MD5

使用MD5工具类进行32位大写加密， 以下例子为

spring-core:5.3.9

中的工具类加密。



DigestUtils.md5DigestAsHex(payload.getBytes()).toUpperCase(Locale.ROOT);

请求接⼝： POST[*http://prepare.mssh.landdt.cn:18100/point/recharge*](http://prepare.mssh.landdt.cn:18100/point/recharge)

请求参数：



{

"merchantId":1157967831234,

"merchantName":"多多评商户",

"rechargeType":2,

"point":30,

"remark":"充值积分"

}

请求头：



{

"appId":"poppy\_life"

"timeStamp":1551925807

"sign":"AC23CFAC9E0357205E76943095CFD984"

}