清源支付 SDK 异步通知说明文档

一、概述

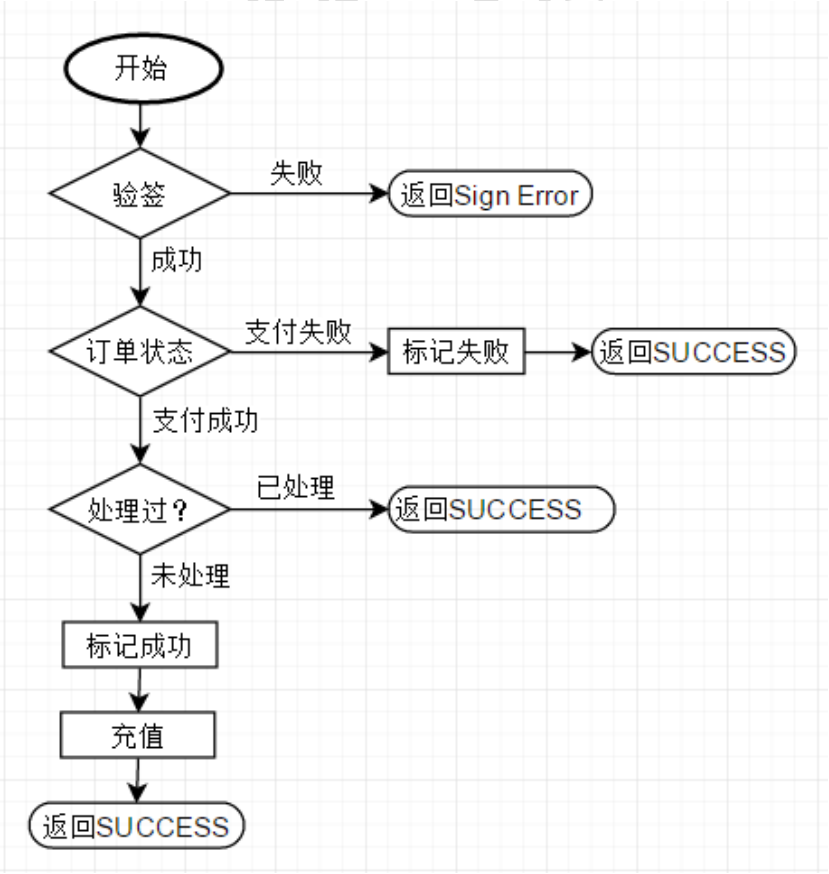
用户支付完成后，平台会将支付结果异步通知到开发商提供的回调地址上。开发商有两种方式设置回调地址：

1. 调用 startPay 方法时设置 notifyUrl 字段，优先使用。
2. 在平台创建 App 时，设置一个全局的通知地址。（目前这一步由我们手工完成，请在对接时将通知地址告诉我方）

如果回调地址返回"SUCCESS"（不包含双引号）这 7 个字符，视为通知成功。其它任何情况都视为通知失败，并将再次通知。同一订单再次通知的间隔时间按照 1s, 2s, 4s, 8s 的规律依次递增，最多通知 20 次。

注意：

1. 支付失败也会发送通知，所以开发人员务必检查状态值。status=5 才是支付成功。
2. 平台有可能会重复发送通知。如果用户的充值已经到帐，也请返回 SUCCESS，否则程序会判为通知失败，继续发送通知。



通知处理流程参考

二、字段说明

通知采用 HTTP POST 请求，字段说明如下：

字段名称	参数名称	描述
商户订单号	orderid	商户系统生成的订单号
交易流水号	transid	支付平台的交易流水号
支付渠道	channel	1=微信，2=支付宝，3=AppStore 内购
应用 ID	appid	平台分配的应用编号
商品名称	ordername	订单显示的商品名称
订单价格	price	支付金额，单位为元
用户 ID	userid	商户系统中的用户编号
用户名	username	商户系统中的用户名
商户私有信息	attach	创建订单时填写的私有信息
订单状态	status	3=系统异常，4=交易失败，5=交易成功
沙盒环境	sandbox	0=正式环境，1=沙盒环境
订单创建时间	createat	调用订单创建接口的时间
订单开始时间	startat	用户开始支付的时间
订单支付时间	payat	支付时间
参数签名	sign	为保证数据安全，请验证参数签名

三、签名验证方法

1. 取出 sign 字段，将剩下的参数按照字典序进行排序。
2. 将排序后的参数（不包含 sign）与其对应值，组合成“参数=参数值”的格式，并且把这些参数用&字符连接起来，此时生成的字符串为待签名字符串。
3. 将签名参数（sign）使用 base64 解码为字节码串。
4. 使用 RSA 的验签方法，通过签名字符串、签名参数（经过 base64 解码）及平台公钥验证签名。

四、平台公钥

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDvpBDYeWK1VGZCwETz5MHSzmZa
g8zgDDH89JqgJ1EUDThBrHYlbksR3ACORfvDh6J+jSKWoXIQJcS12ElyqzwUaTpT
thnUh0jU8mJgOzJuTwtk2xZKNEk71M098h4tmriJCPMWEHMn+0U/qCoHSdzbftNw
XTpjRrf6L4PyFAeePQIDAQAB
-----END PUBLIC KEY-----

五、参考代码(PHP)

```
<?php
$public = "请替换成平台公钥";
$data = $_POST;
// 取出并解码 sign
$sign = base64_decode($data['sign']);
unset($data['sign']);
ksort($data);
// 拼接待签名字符串
$str = '';
foreach ($data as $k => $v) {
	$str .= '&'.$k.'='.$v;
}
$str = ltrim($str, '&');
// 调用验签方法
$key = openssl_pkey_get_public($public);
$result = (bool)openssl_verify($str, $sign, $key, OPENSSL_ALGO_SHA1);
openssl_free_key($key);
if ($result) {
	// 验签成功
} else {
	// 验签失败
}
?>
```

商户服务器端查询接口

- URL: http://pay.aldsd.net/order/query
- 方法: POST

请求参数:

字段名称	参数名	必填	类型	描述
应用 ID	appid	是	String(32)	平台分配的应用编号
商户订单号	orderid	是	String(64)	商户系统生成的订单号
签名算法类型	signtype	是	String(32)	目前只支持 RSA
签名	sign	是	String	签名
SDK 版本	versdk	是	String	SDK 版本，请传 0.1

返回参数

字段名称	参数名称	描述
错误代码	code	0=成功，其它=失败。参考错误代码
错误描述	msg	错误描述
商户订单号	orderid	商户系统生成的订单号
交易流水号	transid	支付平台的交易流水号
支付渠道	channel	1=微信，2=支付宝
应用 ID	appid	平台分配的应用编号
商品名称	ordername	订单显示的商品名称
订单价格	price	支付金额
用户 ID	userid	商户系统中的用户编号
用户名	username	商户系统中的用户名
商户私有信息	attach	创建订单时填写的私有信息
订单状态	status	1=待支付，2=正在处理，3=系统异常，4=交易失败，5=交易成功
沙盒环境	sandbox	0=正式环境，1=沙盒环境
订单创建时间	createat	调用订单创建接口的时间
订单开始时间	startat	用户开始支付的时间
订单支付时间	payat	支付时间
订单统治时间	notifyat	上次通知商户系统的时间
通知状态	notifystatus	0=未通知，1=通知失败，2=通知成功

签名方法

1. 将待签名参数按照字典顺序（字母升序）排列。
2. 将排序后的参数与其对应值，组合成“参数=参数值”的格式，并且把这些参数用&字符连接起来，此时生成的字符串为待签名字符串。
3. 使用各自语言对应的 SHA1WithRSA 签名函数利用商户私钥对待签名字符串

进行签名，并进行 Base64 编码。

参考代码(PHP)

```
<?php
$private = "请替换成平台给您分配的私钥";
// 待签名参数
$data = [.....];
// 排序
ksort($data);
// 拼接待签名字符串
$str = '';
foreach ($data as $k => $v) {
	$str .= '&'.$k.'='.$v;
}
$str = ltrim($str, '&');
// 调用签名方法
$key = openssl_pkey_get_private($private);
openssl_sign($str, $sign, $key, OPENSSL_ALGO_SHA1);
openssl_free_key($key);
// $sign_b64 即为编码后的签名
$sign_b64 = base64_encode($sign);
?>
```