# 1 签名机制

为了防止数据被篡改，合作方和支付宝的请求和应答都会使用签名机制。

一是：合作方发起请求时，对输入参数（请求参数）进行签名；

二是：支付宝处理请求，同步返回请求的应答数据或异步通知时，也会对输出参数进行签名。

下面分别说明：合作方如何对请求参数签名，合作方如何对返回的数据进行验证签名。

## 1.1 合作方如何对请求参数签名

### 1.1.1 需要参与签名的参数

- 在接口请求参数列表中，除去 sign、sign_type 两个参数外，其他需要使用到的参数皆是要签名的参数。

### 1.1.2 生成待签名字符串

对于如下的参数数组：

```
string[] parameters={
    "service=alipay.witkey.task.pay.by.platform",
    "partner=2088101115793868",
    "_input_charset=UTF-8",
    "notify_url=http://www.xx.com/notify_url",
    "outer_task_id=youxi201111400018",
    "alipay_user_id=2088101115793868",
    "transfer_detail=20111212001~*@^100.50~*@^2088102116203728~*@^ 天 之蓝*@|$20111212002~*@^200.60~*@^2088102116208991~*@^红彤彤"
};
```

对数组里的每一个值从 a 到 z 的顺序排序，若遇到相同首字母，则看第二个字母，以此类推。

排序完成之后，再把所有数组值以“&”字符连接起来，如：

```
_input_charset=UTF-8&alipay_user_id=2088101115793868&notify_url=http://www.xx.com/notify_url&outer_task_id=youxi201111400018&partner=2088101115793868&service=alipay.witkey.task.pay.by.platform&transfer_detail=20111212001~*@^100.50~*@^2088102116203728~*@^天之蓝
```

```
*@|$20111212002~*@^200.60~*@^2088102116208991~*@^红彤彤
```

这串字符串便是待签名字符串。

⚠ 注意：

- 没有值的参数无需传递，也无需包含到待签名数据中；
- 签名时将字符转化成字节流时指定的字符集与_input_charset 保持一致；
- 如果传递了_input_charset 参数，这个参数也应该包含在待签名数据中；
- 根据 HTTP 协议要求，传递参数的值中如果存在特殊字符（如：&、@等），那么该值需要做 URL Encoding，这样请求接收方才能接收到正确的参数值。这种情况下，待签名数据应该是原生值而不是 encoding 之后的值。例如：调用某接口需要对请求参数 email 进行数字签名，那么待签名数据应该是 email=test@msn.com，而不是 email=test%40msn.com。

### 1.1.3 DSA 签名

在 DSA 的签名时，需要私钥和公钥一起参与签名。私钥与公钥皆是客户通过 OPENSSL 来生成得出的。客户把生成出的公钥与支付宝技术人员配置好的支付宝公钥做交换。因此，在签名时，客户要用到的是客户的私钥及支付宝的公钥。

- **请求时签名**

  当拿到请求时的待签名字符串后，把待签名字符串与客户的私钥一同放入 DSA 的签名函数中进行签名运算，从而得到签名结果字符串。

- **通知返回时验证签名**

  当获得到通知返回时的待签名字符串后，把待签名字符串、支付宝提供的公钥、支付宝通知返回参数中的参数 sign 的值三者一同放入 DSA 的签名函数中进行非对称的签名运算，来判断签名是否验证通过。

## 1.2 合作方如何对返回的数据进行验证签名

赏金类网站接入的接口调用返回有三种方式：

- 系统同步返回。
- 异步通知返回。
- 页面跳转返回。

### 1.2.1 系统同步返回验签

合作网站调用系统接口后，支付宝会立即将返回数据以 XML 格式 Response 给调用接口的合作网站。sign 和 sign_type 将包含在 xml 中

示例：

```
<?xml version="1.0" encoding="UTF-8" ?>
- <alipay>
    <is_success>T</is_success>
  - <request>
      <param name="sign">MCwCFBmrioGkN3kV5gT2zT89x75tlg8nAhRa+dq+c165zqe0jz2jnj9VUoWFEA==</param>
      <param name="outer_task_id">youxi-2011-12-17-test1</param>
      <param name="cancel_transfer_detail">20111214007~*@^20111214008</param>
      <param name="_input_charset">UTF-8</param>
      <param name="sign_type">DSA</param>
      <param name="service">alipay.witkey.task.cancel.confirm.by.platform</param>
      <param name="partner">2088101115793868</param>
    </request>
  - <response>
    - <task_info>
        <outer_task_id>youxi-2011-12-17-test1</outer_task_id>
      </task_info>
    </response>
    <sign>MCwCFD2bZw9fUhdLXZr45osWp4OP32RXAhRUmJTt8oIeugHRmx8bmIzxmNLm+g==</sign>
    <sign_type>DSA</sign_type>
  </alipay>
```

- 基本节点说明：

  is_success 表示接口调用是否异常。T 正常，F 失败

  request 表示请求的参数。

  response 表示返回参数的内容。

  task_info 表示某个具体对象值。

  sign：返回参数签名后的值。

  sign_type：返回参数签名方式，DSA。

- 在 XML 返回参数列表中，一个节点作为一个参数，节点名代表参数名，节点值代表参数值。需要签名的参数是节点<response>的子节点<task_info>下的所有子节点。如果参数值中出现 HTML 转义字符，那么需要将这些转义字符调整成正常的字符，如：“<”代表的就是“<”。

- 验签过程：

  a) 将节点<task_info>下的所有节点，按节点名升序排序，并以”&“拼装成参数字符串，形如：“节点 1”=“节点 1 的值”&“节点 2”=“节点 2 的值”&“节点 3”=“节点 3 的值”……

  b) 使用“拼装后的参数字符串”、“sign 的值”、“支付宝公钥”进行验证签名。

### 1.2.2 异步通知返回验签

合作网站在请求参数存在 notify_url 的接口调用成功后，支付宝会将结果数据异步 post 给合作网站。包含四个属性数据 xml、notify_id 、sign 和 sign_type，sign 的值是对 notify_id 和 xml 字符串进行的 DSA 签名

验证签名的过程为：

a) 将通知中的 POST 数据，除 sign、sign_type 之外的所有属性都解析出来。
b) 按属性名以升序排序，并以”&“拼装成参数字符串，形如：“属性 1”=“属性 1 的值”&“属性 2”=“属性 2 的值”&“属性 3”=“属性 3 的值”……

   举例：

   notify_id=ccb58f2f9752549d18517aa5cf87ef2d05 &xml=<?xml ……>

c) 使用“拼装后的参数字符串”、“sign 的值”、“支付宝公钥”进行验证签名，签名数据的编码格式是 utf-8。
d) 如果验证签名返回的是 true，则表明该通知是有支付宝发送的。

### 1.2.3 页面跳转返回验签-POST 方式

合作网站在请求参数存在 return_url 的页面接口调用成功后，支付宝会将结果数据 post 给合作网站。

post 数据中包含一个属性“resultMsg”。xml 格式的结果数据、sign 和 sign_type 均包含在“resultMsg”中。

验证签名的过程为：

a) 获得属性“resultMsg”中数据，并且使用 URLDecoder 对数据内容进行“utf-8”的解码。
b) “resultMsg”中数据中的数据形如：
   xml=<?xml ……>&sign= MCwCFDFbpt……ihe+BaRipBPFlTJeDw==&sign_type=DSA
   xml 对应字符串的字符串即为结果数据。
c) 使用“xml 对应字符串”、“sign 的值”、“支付宝公钥”进行验证签名，签名数据的编码格式是 utf-8
d) 如果验证签名返回的是 true，则表明该通知是有支付宝发送的。

### 1.2.4 页面跳转返回验签-GET 方式

需要验签的数据：请求参数列表中，所有支付宝返回参数，除去参数 sign、sign_type 和参数值为空的参数。（注意 return_url 中合作网站传的参数不会签名。）

a) 将 url 中的参数，除 sign、sign_type 之外的所有属性都解析出来。
b) 按属性名以升序排序，并以”&“拼装成参数字符串，形如：“属性 1”=“属性 1 的值”&“属性 2”=“属性 2 的值”&“属性 3”=“属性 3 的值”……
c) 使用“拼装后的参数字符串”、“sign 的值”、“支付宝公钥”进行验证签名，签名数据的编码格式是 utf-8。

d) 如果验证签名返回的是 true，则表明该通知是有支付宝发送的。

# 2 错误码

## 2.1 业务错误码

| 错误代码 | 说明 |
|---|---|
| ACCOUNT_AT_RISK | 账号有风险 |
| TASK_TYPE_NOT_EXIST | 任务类型不存在 |
| TASK_ALREADY_PAID | 任务已经支付 |
| ACCOUNT_BLOCK | 账户被冻结 |
| ACCOUNT_CANCELLED | 账户已注销 |
| ACCOUNT_STATUS_ILLEGAL | 账户状态异常 |
| FREEZE_AMOUNT_ILLEGAL | 冻结金额不正确 |
| OUTER_ACCOUNT_ID_IS_NOT_OWNER | 合作网站用户ID不是任务的发起者 |
| TASK_OWNER_IS_NOT_EXIST | 任务发布者不存在 |
| TASK_OWNER_ILLEGAL | 任务发布者不正确 |
| TASK_OUT_OF_DATE | 任务已过期 |
| TRANSFER_DETAIL_ILLEGAL | 打款请求明细格式有误 |
| OVER_MAX_BIDDERS | 中标者数量超限 |
| TOTAL_TRANSFER_AMOUNT_ILLEGAL | 中标总金额为0，不能确认赏金 |
| OVER_REMAINS_OF_TASK_AMOUNT | 确认中标金额大于剩余赏金金额 |
| TRANSFER_REPEAT_OR_BIDDER_ACCOUNT_ILLEGAL | 重复请求或者中标账户不合法 |
| BIDDERS_DATA_PROCESS_ERROR | 处理中标者数据失败 |
| QUERY_TASK_TYPE_CHARGE_ERROR | 查询分润类型失败 |
| QUERY_COMMISSION_RULE_ERROR | 查询分润规则模型失败 |

| | |
|---|---|
| WITKEY_TASK_EXIST_ERROR | 威客合作网站任务已存在 |
| WITKEY_RECHARGE_EXIST_ERROR | 威客合作网站任务赏金已支付 |
| RECHARGE_INFO_MODIFIED | 充值数据被修改 |
| PLATFORM_AUTHORITY_ILLEGAL | 操作权限限制 |
| WITKEY_RECHARGE_ID_EMPTY | 任务充值ID为空 |
| WITKEY_RECHARGE_EMPTY | 任务充值记录为空 |
| WITKEY_TASK_NOT_EXIST | 任务不存在 |
| WITKEY_TRANSFER_NOT_EXIST | 转账不存在 |
| WITKEY_TRANSFER_ALREADY_EXIST | 转账已经存在 |
| WITKEY_AMOUNT_NOT_MATCH | 金额不匹配 |
| WITKEY_TASK_LEFT_AMOUNT_NOT_ENOUGH | 剩余金额不足 |
| WITKEY_COUNT_NOT_MATCH | 笔数不匹配 |
| WITKEY_NOT_ALLOW | 中标者不允许撤销 |
| WITKEY_OUTER_TRANSFER_ALREADY_PAID | 合作网站转账流水已提交支付 |
| WITKEY_OUTER_TRANSFER_REPEAT | 合作网站转账流水号重复 |
| WITKEY_DATA_NOT_MATCH | 数据不匹配 |
| WITKEY_DATA_VALIDATE_FAILURE | 数据校验失败 |
| BIDDER_EQUALS_TASK_CREATOR_ERROR | 中标者不能和发布者相同 |
| PLATFORM_CREATE_PLATFORM_SHARE_GREATER_0 | 平台创建，剩余赏金平台划拨金额大于0 |
| PLATFORM_CREATE_ADDITIONAL_AMOUNT_GREATER_0 | 平台创建任务增值服务费大于0 |
| PLATFORM_CREATE_COMMISSION_RATE_GREATER_0 | 平台创建分润比例大于0 |
| ACCOUNT_QUERY_ERROR | 账号查询错误 |
| ACCOUNT_NOT_EXIST | 账号不存在 |
| AUTH_TOKEN_ERROR | 授权令牌不正确 |
| NOT_DONE_OF_TRANSFER_FOUND | 转账流水未处理完成 |

| | |
|---|---|
| REMAINS_OF_TASK_AMOUNT_FOUND | 悬赏任务还有剩余赏金 |

## 2.2 公共错误码

| 错误代码 | 说明 |
|---|---|
| ILLEGAL_ARGUMENT | 参数不正确 |
| ILLEGAL_SIGN | 数字验签失败 |
| SYSTEM_ERROR | 支付宝系统错误 |
| SESSION_TIMEOUT | 连接超时错误 |
| ILLEGAL_PARTNER | 表示请求中的partner 错误 |
| HAS_NO_PRIVILEGE | 无权访问该接口 |
| ILLEGAL_SERVICE | 请求的接口信息不存在 |