<https://docs.open.alipay.com/291/105971>

**第一步：生成 RSA 密钥**

更新时间：2019-10-09

**工具下载**

支付宝为技术开发人员提供一键生成工具，便于开发者生成一对 RSA 密钥、公钥证书申请CSR文件（在线申请应用公钥证书需要）。

应用公钥（public key）需提供给支付宝账号管理者上传到支付宝开放平台；应用私钥（private key）由开发者自己保存，需填写到代码中供签名时使用。加密的过程为系统使用公钥（public key）进行加密，并将密文发送到解密者，解密者用私钥（private key）解密将密文解码为明文。

开发者要保证接口中使用的私钥与此处的公钥匹配，否则无法调用接口。开发者可通过下方链接下载对应的密钥生成工具：

[WINDOWS](https://ideservice.alipay.com/ide/getPluginUrl.htm?clientType=assistant&platform=win&channelType=WEB)**（windows版本工具请不要安装在含有空格的目录路径下）**

[MAC\_OSX](https://ideservice.alipay.com/ide/getPluginUrl.htm?clientType=assistant&platform=mac&channelType=WEB)

WINDOWS老版本下载地址：[WINDOWS](http://p.tb.cn/rmsportal_6680_secret_key_tools_RSA_win.zip)

MAC OS老版本下载地址：[MAC\_OSX](http://p.tb.cn/rmsportal_6680_secret_key_tools_RSA_macosx.zip)

**注意：**

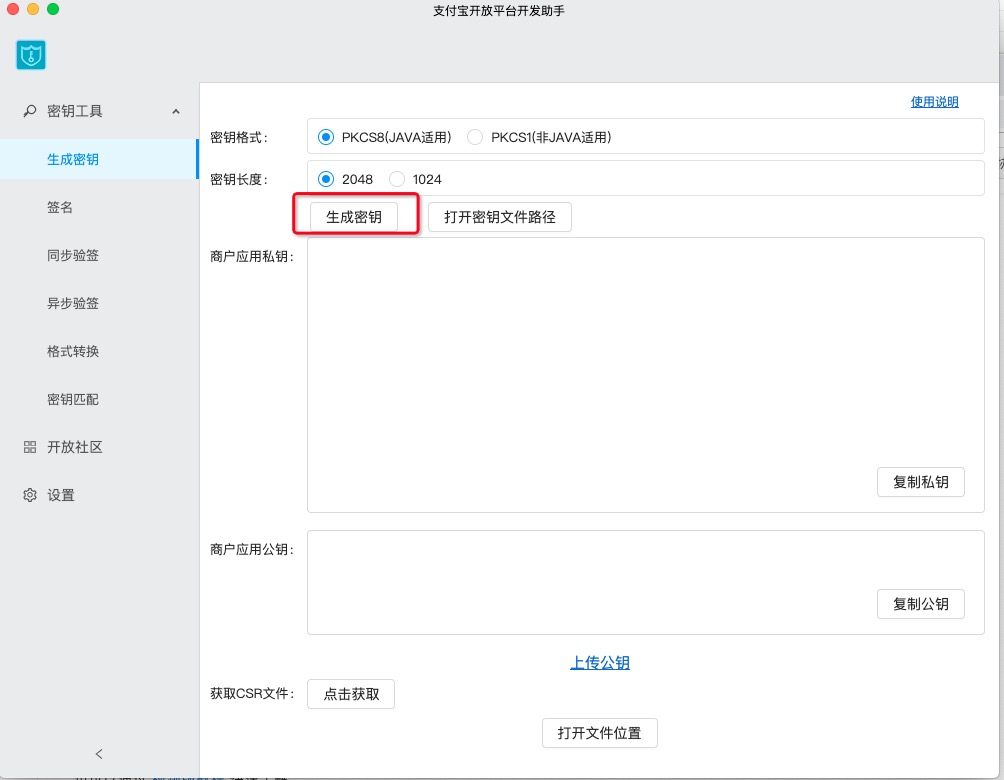
密钥和应用（APPID）一一对应，即开发者需要为名下的每个应用分别设置密钥，且不同应用的密钥不能混用。

**使用步骤**

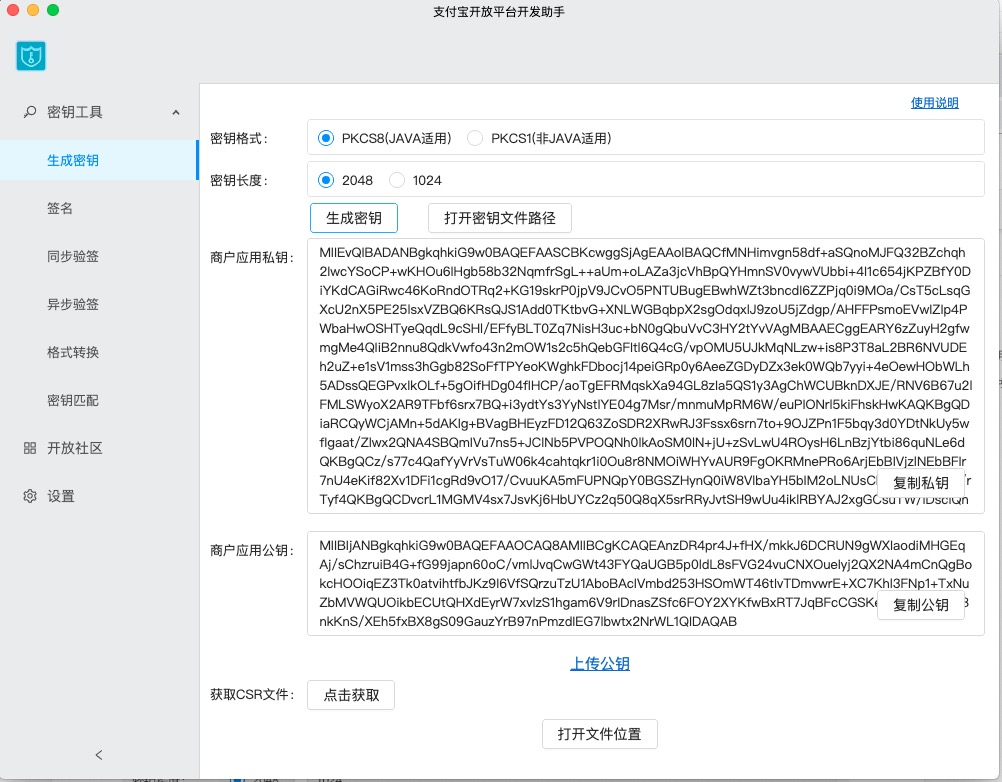
支付宝开放平台支持开发者使用**普通公钥**、**公钥证书**两种签名方式；下面分别向您介绍两种方式的工具操作步骤，包括如何使用密钥生成工具，生成应用公钥（public key）、应用私钥（private key）和公钥证书申请 CSR 文件；您也可以通过 [视频版教程](https://docs.open.alipay.com/291/106103#k0dDI) 快速了解。

**普通公钥方式**

1.下载相应环境工具并安装后即可使用，本步骤指引以 MAC\_OSX 界面为例，如下图所示：



2.开发者根据开发语言选择密钥格式和密钥长度，新建应用请务必使用 2048 位（目前已使用 1024 位密钥长度的应用仍然可以正常调用接口，详情请见[开放平台接口签名方式升级公告](https://open.alipay.com/platform/announcement.htm?id=18)）。点击 **生成密钥** 后，工具会自动生成商户应用公钥（public key）和应用私钥（private key），如下图所示：



3.开发者点击工具界面下方的 **打开文件位置**，即可找到生成的公私钥文件，如下图所示：



4.生成密钥后，开发者就可以在应用的开发配置页面进行配置。点击 **设置应用公钥** 后，复制上一步生成的公钥，点击 **保存**，即可完成公钥的设置，如下图所示。





**注意**：

生成的私钥需妥善保管，避免遗失，不要泄露。应用私钥需填写到代码中供签名时使用。应用公钥需提供给支付宝账号管理者上传到支付宝开放平台。

除了使用支付宝提供的一键生成密钥工具外，也可以使用 OpenSSL 工具命令生成密钥。点击了解相关[教程](https://docs.open.alipay.com/291/106130)。

**公钥证书方式**

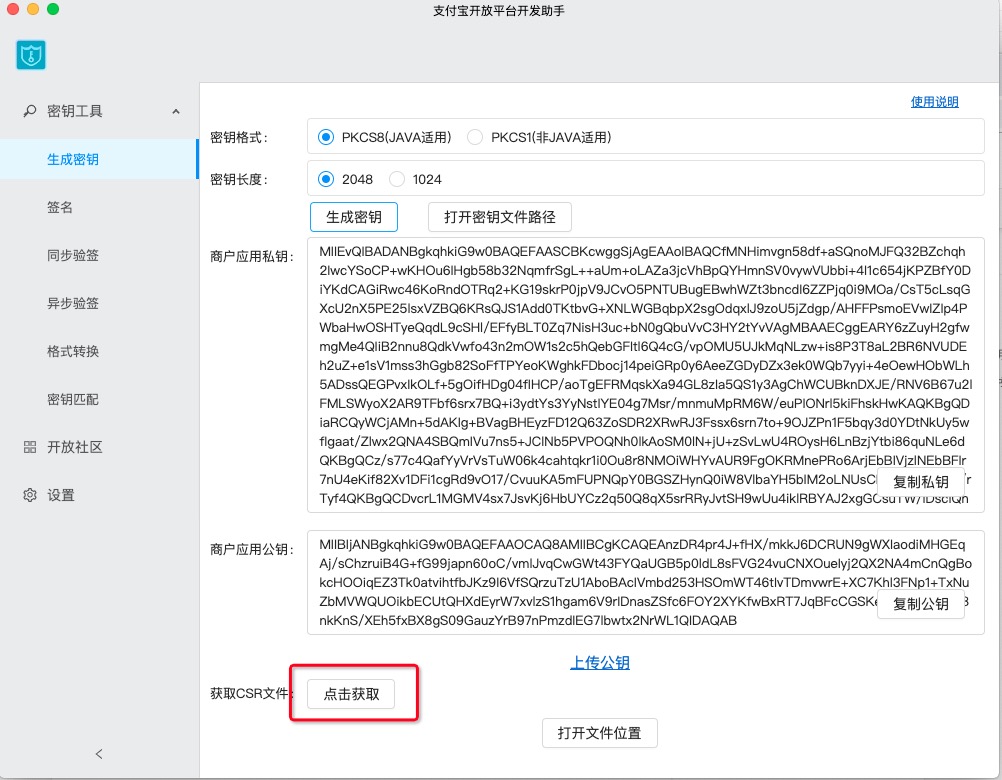
**注意：**

1. **对于之前没有上传过任何公钥，首次接入即使用“公钥证书”的应用，不允许再切换到“公钥”模式。**
2. **对于从“公钥”变更到“公钥证书”模式的，在变更一周内允许开发者撤销证书回退到“公钥”模式；变更一周后不允许再回退到原模式。开发者调用支付宝网关的代码也需要升级，否则变更一周后原来的“公钥”模式接入会被支付宝网关拦截而无法成功调用，具体升级参考文档。**
3. **个人开发者因为不涉及到资金类接口，建议使用“公钥”方式进行加签。**

若开发者使用公钥证书签名方式，开放平台支持通过上传 CSR 文件的方式给开发者在线签发应用公钥证书，新的开放平台 RSA 验签和签名工具支持生成 CSR 文件（个人用户由于不涉及到资金接口，建议使用普通公钥方式接入，降低接入成本），具体操作步骤如下：

同“普通公钥方式”一样，下载相应环境工具并安装后即可使用，本步骤指引以 MAC\_OSX 界面为例：

1.点击工具界面下方的 **点击获取**，生成应用公钥证书 CSR 申请文件。



2.点击进入 **获取csr** 页面后，根据如下提示完善填写信息，点击 **生成CSR文件**。请注意“组织/公司”名称**一定要和开发者中心门户账号信息的公司名称保持一致，否则会导致后续步骤中上传csr证书文件校验失败**。

**Tips：**沙箱环境下“组织/公司”名称应填写为“**沙箱环境**”。



3.在生成 CSR 文件后，点击 **打开密钥文件路径**，在对应的文件夹里可以看到三个文件：应用公钥 key 串、应用私钥key 串，以及 csr格式的应用公钥证书文件。如下图所示：



4.生成公钥证书 CSR 申请文件，开发者就可以在应用的开发配置页面/接口加签方式进行配置（如下图 1）。点击 **设置** 后，选择**公钥证书**（如下图2）> **上传CSR文件在线生成证书**>**上传CSR文件在线生成**，选择上一步骤生成的 .csr文件上传，即可完成公钥证书的设置，如下图所示。





**注意：**

生成的私钥需妥善保管，避免遗失，不要泄露。应用私钥需填写到代码中供签名时使用，并且必须保证应用私钥和上传到开放平台申请应用公钥证书的 CSR 文件是匹配的。

**第二步：上传应用公钥并获取支付宝公钥**

更新时间：2019-08-14

以下步骤向您分别介绍了支付宝账号管理者如何上传上一步生成的应用公钥（public key）并获取相应的支付宝公钥（alipay public key），您可以通过[视频版教程](https://docs.open.alipay.com/291/106103#70e23f5c)快速了解；以及如何在线申请应用公钥证书、上传开发者自己申请的应用公钥证书，并获取相应的支付宝公钥证书。

1. 点击签名验签工具右下角的“上传公钥”会打开支付宝[开放平台网页](https://openhome.alipay.com/platform/appManage.htm)，输入账号登录。（建议使用 IE 或 Chrome 浏览器。)
2. 在“我的应用”中，选择要配置密钥的应用，点击“查看”。记录对应的 **APPID**（下图红框处），在代码中使用。  
     
   若首次登录管理中心，请根据引导填写所需信息完成开发者入驻：  
   第一步：点击认证，完成实名认证。  
     
   第二步：点击编辑，完善信息。  
     
   根据引导流程，完成手机绑定。  
     
   第三步：签署协议，完成入驻。  
   
3. 在 “应用信息” - “开发设置” - “接口加签方式”中设置应用公钥信息。支付宝开放平台支持开发者设置应用公钥、公钥证书两种方式，下面步骤4、5分别介绍两种方式的设置方式。  
   **注意**：  
   1）接口中的 sign\_type 参数应与上传密钥的加签方式一致。例如接口参数中 sign\_type=RSA2,请求时就会使用此处设置的 RSA2(SHA256)公钥验签。  
   2）新建应用仅支持 RSA2 加签方式，详情请见[开放平台接口签名方式升级公告]
4. 设置应用公钥  
   1）点击接口加签方式“设置”按钮，在打开的页面中“选择加签模式”选择**公钥**  
     
   

2）把签名验签工具里 “公钥” 的内容复制到此处，点击 “保存” 完成密钥设置。  


3）保存成功后，系统会提示应用公钥上传成功。

若未绑定手机，请根据引导，完成手机绑定。  
  
完成手机短信验证。  


1. 设置应用公钥证书  
   开发者选择设置公钥证书。设置完成后可以查看并下载应用公钥证书、支付宝公钥证书、支付宝根证书到本地，以便代码验签中使用。

1）点击接口加签方式“设置”按钮，在打开的页面中“选择加签模式”选择**公钥证书**  


2）在**公钥证书**加签模式下，开发者有两个选项，上传CSR文件（推荐方式，该方式生成的应用公钥证书由蚂蚁签发）或上传开发者自己申请的公钥证书文件（证书必须由权威CA签发，[当前支持的CA列表](https://docs.open.alipay.com/291/106098#9cjwY)，且仅支持X.509格式的证书，[证书说明](https://docs.open.alipay.com/291/106124)）。

上传CSR文件，该文件由第一步开发者工具生成  


上传开发者自己申请公钥证书文件  


3）提示上传成功，开发者可查看、下载已生成（或已上传）的应用公钥证书，以及下载对应的支付宝公钥证书、支付宝根证书。  


**注意：**  
公钥证书模式中，上传的文件，无论是csr文件或者开发者自己申请的公钥证书文件，必须和用户本地代码中加密的应用私钥是匹配的，否则会导致支付宝开放平台验签失败。

**第三步：使用应用私钥生成请求签名**

更新时间：2019-08-26

本步骤向您介绍了开发者分别在选择普通公钥、公钥证书两种签名方式下，如何对请求内容进行签名，并对支付宝返回的内容进行验签。

简而言之，签名的过程即生成签名方（通常为支付宝客户端）将传送的消息用私钥加密的过程；验签则是指验签方（通常为开放平台的服务端）使用公钥对消息进行验证的过程。

以 JAVA 语言为例，签名和验签的过程大致为：

1. 生成签名方（通常为商户）首先对参数放入一个字符串数组 signFields，把参数和值放入一个对象或 map 中，使用 JSONObject 把这个对象转化成 json 对象。然后构建签名原文，在构建签名原文时，我们需把参数按照字典（比如a,b,c）顺序排序，具体排序方法直接调用 JAVA 的 Arrays.sort 方法。 然后使用 RSA 的私钥对签名原文进行签名。
2. 验签方（通常为开放平台的服务端）：和生产签名方一样先生成签名原文，然后使用 RAS 的公钥生成签名方传入的签名，把签名原文对生成签名方传入的签名进行验证，验证结果为 true 则说明验证成功，否则未通过。

支付宝开放平台 SDK 封装了签名和验签过程，只需配置账号及密钥参数即可，强烈建议使用。

[SDK 下载地址](https://docs.open.alipay.com/54/103419)

**说明：** 文中代码部分以 JAVA 语言演示，其他语言请参考各自 SDK。

**普通公钥方式**

以下介绍了开发者如何把以下内容配置在代码中，对请求内容进行签名，并对支付宝返回的内容进行验签：

* APPID
* 应用私钥 （private key）
* 支付宝公钥（alipay public key）

**使用开放平台 SDK 接入**

开放平台 SDK 封装了签名实现，只需在创建 DefaultAlipayClient 对象时，设置请求网关 (gateway)，应用 id (app\_id)，应用私钥 (private\_key)，编码格式 (charset)，支付宝公钥 (alipay\_public\_key)，签名类型 (sign\_type)即可，报文请求时会自动进行签名。

AlipayClient alipayClient = new DefaultAlipayClient(gateway,app\_id,private\_key,"json",charset,alipay\_public\_key,sign\_type);

**未使用开放平台 SDK**

如果未使用开放平台SDK，需要自行实现签名过程，参考[此处流程](https://docs.open.alipay.com/291/106118)。

**公钥证书方式**

以下介绍了开发者如何把以下内容配置在代码中，对请求内容进行签名，并对支付宝返回的内容进行验签：

* APPID
* 应用私钥 （private key）
* 应用公钥证书（public key cert）
* 支付宝公钥（alipay public key）
* 支付宝公钥证书（alipay public key cert）
* 支付宝根证书（alipay root cert）

**使用开放平台 SDK 接入**

**如果你当前已经使用了服务端SDK，请注意：**

* **当前仅Java版SDK（**[**4.4.2.ALL及以上版本**](https://mvnrepository.com/artifact/com.alipay.sdk/alipay-sdk-java)**）支持证书签名方式，其他语言SDK还未支持。**
* **Java版SDK 4.4.2.ALL中并没有对**[**APP支付**](https://docs.open.alipay.com/54/106370/)**场景添加证书支持，若业务使用到该场景，请下载**[**4.4.5.ALL**](https://ideservice.alipay.com/ide/getPluginUrl.htm?clientType=sdk&platform=all&channelType=WEB)**及以上版本的SDK。**

开放平台 SDK 封装了签名实现，只需在创建 DefaultAlipayClient 对象时，设置请求网关 (gateway)，应用 id (app\_id)，应用私钥 (private\_key)，应用公钥证书路径（app\_cert\_path 文件绝对路径），支付宝公钥证书文件路径（alipay\_cert\_path 文件绝对路径），支付宝CA根证书文件路径（alipay\_root\_cert\_path 文件绝对路径），编码格式 （charset），签名类型 （sign\_type）即可，报文请求时会自动进行签名。

//构造client

CertAlipayRequest certAlipayRequest = new CertAlipayRequest();

certAlipayRequest.setServerUrl(gateway);

certAlipayRequest.setAppId(app\_id);

certAlipayRequest.setPrivateKey(privateKey);

certAlipayRequest.setFormat("json");

certAlipayRequest.setCharset(charset);

certAlipayRequest.setSignType(sign\_type);

certAlipayRequest.setCertPath(app\_cert\_path);

certAlipayRequest.setAlipayPublicCertPath(alipay\_cert\_path);

certAlipayRequest.setRootCertPath(alipay\_root\_cert\_path);

DefaultAlipayClient alipayClient = new DefaultAlipayClient(certAlipayRequest);

//发送API请求

AlipayRequest request = new AlipayTradeQueryRequest();

AlipayTradeQueryResponse response = alipayClient.certificateExecute(request);

**未使用开放平台 SDK**

如果未使用开放平台SDK，需要自行实现签名过程，参考[此处流程](https://docs.open.alipay.com/291/106118)。

**第四步：使用支付宝公钥验签**

# 

# 更新时间：2019-08-26

本步骤向您介绍了开发者分别在选择普通公钥、公钥证书两种方式下，如何对支付宝返回内容进行验签  
支付宝开放平台 SDK 封装了签名和验签过程，开发者只需配置账号及密钥参数，建议使用。

[SDK 下载地址](https://docs.open.alipay.com/54/103419)  
**说明：** 文中代码部分以 JAVA 语言演示，其他语言请参考各自 SDK。

# 普通公钥方式

## 使用开放平台SDK接入

同步返回和异步通知报文格式及验签方法有所区别。

### 同步返回验签

开放平台SDK封装了同步返回验签实现，只需在创建 DefaultAlipayClient 对象时，设置请求网关 (gateway)，应用 id (app\_id)，应用私钥 (private\_key)，编码格式 (charset)，支付宝公钥 (alipay\_public\_key)，签名类型 (sign\_type)即可，同步返回报文时会自动进行验签。

AlipayClient alipayClient = new DefaultAlipayClient(gateway,app\_id,private\_key,"json",charset,alipay\_public\_key,sign\_type);

### 异步通知验签

某些情况下（比如扫码支付成功时），支付宝会给商户发送异步通知。  
如果某商户设置的通知地址为“https://api.xx.com/receive\_notify.htm”，对应接收到通知的示例如下：

https://api.xx.com/receive\_notify.htm?total\_amount=2.00&buyer\_id=2088102116773037&body=大乐透2.1&trade\_no=2016071921001003030200089909&refund\_fee=0.00&notify\_time=2016-07-19 14:10:49&subject=大乐透2.1&sign\_type=RSA&charset=utf-8&notify\_type=trade\_status\_sync&out\_trade\_no=0719141034-6418&gmt\_close=2016-07-19 14:10:46&gmt\_payment=2016-07-19 14:10:47&trade\_status=TRADE\_SUCCESS&version=1.0&sign=kPbQIjX+xQc8F0/A6/AocELIjhhZnGbcBN6G4MM/HmfWL4ZiHM6fWl5NQhzXJusaklZ1LFuMo+lHQUELAYeugH8LYFvxnNajOvZhuxNFbN2LhF0l/KL8ANtj8oyPM4NN7Qft2kWJTDJUpQOzCzNnV9hDxh5AaT9FPqRS6ZKxnzM=&gmt\_create=2016-07-19 14:10:44&app\_id=2015102700040153&seller\_id=2088102119685838&notify\_id=4a91b7a78a503640467525113fb7d8bg8e

开放平台 SDK 提供了 AlipaySignature.rsaCheckV1 方法，可以使用该方法对通知报文验签。

/\*\*

@param params 参数列表(包括待验签参数和签名值sign) key-参数名称 value-参数值

@param publicKey 验签公钥

@param charset 验签字符集

\*\*/

boolean AlipaySignature.rsaCheckV1(Map<String, String> params, String publicKey, String charset)

**注意：** 生活号异步通知需要使用 AlipaySignature.rsaCheckV2 方法，会保留 sign\_type 参数参与验签。

## 未使用开放平台SDK

如果未使用开放平台 SDK，需要自行实现验签过程，参考[此处流程](https://docs.open.alipay.com/200/106120)。

# 公钥证书方式

## 使用开放平台SDK接入

如果你当前已经使用了服务端SDK，请注意：

* **当前仅Java版SDK（**[**4.4.2.ALL及以上版本**](https://mvnrepository.com/artifact/com.alipay.sdk/alipay-sdk-java)**）支持证书签名方式，其他语言SDK还未支持。**
* **Java版SDK 4.4.2.ALL中并没有对**[**APP支付**](https://docs.open.alipay.com/54/106370/)**场景添加证书支持，若业务使用到该场景，请下载**[**4.4.5.ALL**](https://ideservice.alipay.com/ide/getPluginUrl.htm?clientType=sdk&platform=all&channelType=WEB)**及以上版本的SDK。**

同步返回和异步通知报文格式及验签方法有所区别。

### 同步返回验签

开放平台SDK封装了同步返回验签实现，只需在创建 DefaultAlipayClient 对象时，设置请求网关 (gateway)，应用 id (app\_id)，应用私钥 (private\_key)，应用公钥证书路径（app\_cert\_path 文件绝对路径），支付宝公钥证书文件路径（alipay\_cert\_path 文件绝对路径），支付宝CA根证书文件路径（alipay\_root\_cert\_path 文件绝对路径），编码格式 (charset)，签名类型 (sign\_type)即可同步返回报文时会自动进行验签。

CertAlipayRequest certAlipayRequest = new CertAlipayRequest();

certAlipayRequest.setServerUrl(gateway);

certAlipayRequest.setAppId(app\_id);

certAlipayRequest.setPrivateKey(privateKey);

certAlipayRequest.setFormat("json");

certAlipayRequest.setCharset(charset);

certAlipayRequest.setSignType(sign\_type);

certAlipayRequest.setCertPath(app\_cert\_path);

certAlipayRequest.setAlipayPublicCertPath(alipay\_cert\_path);

certAlipayRequest.setRootCertPath(alipay\_root\_cert\_path);

DefaultAlipayClient alipayClient = new DefaultAlipayClient(certAlipayRequest);

### 异步通知验签

某些情况下（比如扫码支付成功时），支付宝会给商户发送异步通知。  
如果某商户设置的通知地址为“https://api.xx.com/receive\_notify.htm”，对应接收到通知的示例如下：

https://api.xx.com/receive\_notify.htm?total\_amount=2.00&buyer\_id=2088102116773037&body=大乐透2.1&trade\_no=2016071921001003030200089909&refund\_fee=0.00&notify\_time=2016-07-19 14:10:49&subject=大乐透2.1&sign\_type=RSA&charset=utf-8&notify\_type=trade\_status\_sync&out\_trade\_no=0719141034-6418&gmt\_close=2016-07-19 14:10:46&gmt\_payment=2016-07-19 14:10:47&trade\_status=TRADE\_SUCCESS&version=1.0&sign=kPbQIjX+xQc8F0/A6/AocELIjhhZnGbcBN6G4MM/HmfWL4ZiHM6fWl5NQhzXJusaklZ1LFuMo+lHQUELAYeugH8LYFvxnNajOvZhuxNFbN2LhF0l/KL8ANtj8oyPM4NN7Qft2kWJTDJUpQOzCzNnV9hDxh5AaT9FPqRS6ZKxnzM=&gmt\_create=2016-07-19 14:10:44&app\_id=2015102700040153&seller\_id=2088102119685838&notify\_id=4a91b7a78a503640467525113fb7d8bg8e

开放平台 SDK 提供了 AlipaySignature.rsaCertCheckV1 方法，可以使用该方法对通知报文验签。

/\*\*

@param params 参数列表(包括待验签参数和签名值sign) key-参数名称 value-参数值

@param alipayPublicCertPath 验签支付宝公钥证书路径

@param charset 验签字符集

\*\*/

boolean AlipaySignature.rsaCertCheckV1(Map<String, String> params, String alipayPublicCertPath, String charset)

**注意：**  
1）生活号异步通知需要使用 AlipaySignature.rsaCertCheckV2 方法，会保留 sign\_type 参数参与验签。  
2）针对之前已入驻开放平台，后续升级成证书模式的应用，开放平台生成的支付宝公钥证书文件中的密钥和原密钥是一致的，即开发者仍可使用原异步通知验签代码。

/\*\*

@param params 参数列表(包括待验签参数和签名值sign) key-参数名称 value-参数值

@param publicKey 验签公钥

@param charset 验签字符集

\*\*/

boolean AlipaySignature.rsaCheckV1(Map<String, String> params, String publicKey, String charset)

**注意：** 生活号异步通知需要使用 AlipaySignature.rsaCheckV2 方法，会保留 sign\_type 参数参与验签。

## 未使用开放平台SDK

如果未使用开放平台 SDK，需要自行实现验签过程，参考[此处流程](https://docs.open.alipay.com/200/106120)。