签名与验签

开放平台下载的sdk已封装签名验签方法，开发者只需要调用sdk配置业务入参即可，用sdk封装的方法发送请求到开放平台时，sdk会自动签名。如开发者不用sdk，可根据签名规则自己拼写签名方法。以下是结合开放平台业务对自主签名进行简单说明：

请求参数签名

筛选

获取所有请求参数，不包括字节类型参数，如文件、字节流，剔除sign字段。

排序

将筛选的参数按照第一个字符的键值ASCII码递增排序（字母升序排序），如果遇到相同字符则按照第二个字符的键值ASCII码递增排序，以此类推。

拼接

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。SDK中已封装签名方法，开发者可直接调用，详见SDK说明。如自己开发，则需将待签名字符串和私钥放入SHA1 RSA算法中得出签名（sign）的值。

调用签名函数

现将拼接后的参数，按照编码类型处理为byte数组，使用各自语言对应的RSA签名函数利用商户私钥对待签名字符串进行签名，并将签名后结果进行Base64编码。

返回参数验证签名

开发者只对工行API平台返回的json中response_biz_content的值做验签。response_biz_content的Json值内容，如为json则需要包含首尾的“{”和“}”两个尖括号，如为字符串则需包括前后引号，如为数组，则需包含首位的“[”和“]”，作为验签整体。

签名验签示例

应用私钥示例（非生产密钥）

```
MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBALAWAcPiTMRU906PTdy0ozspX7XptZnkEw2C8R64RDB9BiRFXAj0cU4aTA1MyfmGIlceeVdgJf7OnmvpHnYxjQ7sGxMItPtodrGwA2y8j0AEbHc5pNWU8Hn0zoY9smHS5e+KjSbWv+VNbdnrRFTpDeiJ3+s2E/cKI2CDRbo7cAarAgMBAAECgYABiA933q4APyTvf/uTYdbRmuiEMoYr0nn/8hWayMt/CHdXNWs5gLbDkSL8MqDHFM2TqGYxxlpOPwnNsndbW874QIEKmtH/SSHuVUJSPyDW4B6MazA+/e6Hy0TZg2VAYwkB1IwGJox+OyfWzmbqpQGgs3FvuH9q25cDxkWntWbDcQJBAP2RDXlqx7UKsLfM17uu+ol9UvpdGoNEed+5cpScjFcsB0XzdVdCpp7JLlxR+UZNwr9Wf1V6FbD2kDflqZRBuV8CQQCxxpq7CJUaLHfm2kjmVtaQwDDw1ZKRb/Dm+5MZ67bQbvbXFHCRKkGI4qqNRlKwGhqIAUN8Ynp+9WhrEe0lnxo1AkEA0flSDR9tbPADUtDgPN0zPrN3CTgcAmOsAKXSylmwpWciRrzKiI366DZ0m6KOJ7ew8z0viJrmZ3pmBsO537llRQJAZLrRxZRRV6lGrwmUMN+XaCFeGbgJ+lphN5/oc9F5npShTLEKL1awF23HkZD9HUdNLS76HCp4miNXbQOVSbHi2QJAUw7KSaWENXbCl5c7M43ESo9paHHXHT+/5bmzebq2eoBofn+IFsyJB8Lz5L7WciDK7WvrGC2JEbqwpFhWwCOl/w==
```

开放平台公钥示例（非生产密钥）

```
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCwFgHD4kzEVPdOj03ctKM7KV+16bWZ5BMNgvEeuEQwfQYkRVwI9HFOGkwNTMn5hiJXHnlXYCX+zp5r6R52MY0O7BsTCLT7aHaxsANsvI9ABGx3OaTVlPB59M6GPbJh0uXvio0m1r/lTW3Z60RU6Q3oid/rNhP3CiNgg0W6O3AGqwIDAQAB
```

请求签名示例

```
REQUEST URL:  https://gw.open.icbc.com.cn/api/preciousmetal/V1/purchase
REQUEST METHOD: POST
CONTENT:
app_id=2014072300007148
trade_id=123456
charset=GBK
sign_type=RSA
timestamp=2014-07-24 03:07:50
biz_content={"id":"student_id","name":"student_name"}
```

待签名数据：

```
/api/preciousmetal/V1/purchase?app_id=2014072300007148&biz_content={"id":"student_id","name":"student_name"}&charset=GBK&sign_type=RSA&timestamp=2014-07-24 03:07:50&trade_id=123456
```

使用示例私钥签名结果：

```
A7ibf97cez7UudFZCSePEn8kgr0DSDlvu+CqCAm0JJ65xsQtU7vFuGAwPoUfPYVWG2q+9DXbL4el8pAq6TPicg8Nn/zCCGGF4PRSmi4ZLzU+7fhrsMMo5hMhhQhLhYplbvHLwsRy/XqF8o49g2+es9ZX4mzpVR/gwMcINi8rXlE=
```

返回参数签名验证示例

```
{
  "response_biz_content":{
    "return_code":0,
    "return_msg":"success",
    "class_id":"your class id",
    "class_name:"your class name"
  },
  "sign":"Vf2F1pZns+bIfUeTu91wcV7EDnKA94AE1cJB1OLpOgfQDqqmYOfxgT/zGkeXkczaaWLdwbVFQ8EnCoA5yU+UjqGexfZCVrr+ObAzK0N/dmhx541iazOha7AFoJQSo2lybAfU7QPge7WZPWK2mleTVDeA5l6G3kEFbUQ5BBS5uUM="
}
```

待签名数据：

```
{
    "return_code":0,
    "return_msg":"success",
    "class_id":"your class id",
    "class_name:"your class name"
  }
```

即：

```
{\n    "return_code":0,\n    "return_msg":"success",\n    "class_id":"your class id",\n    "class_name:"your class name"\n  }
```

公钥说明

开发者上传至工行API开放平台的公钥必须为PKCS8格式的RSA 2048密钥，该密钥还必须经过Base64转换。工行提供的API公钥也遵从同样标准。