



http

[illegible]

□□□□□□□□□□RSA□□RSA□□□□

- `XXXX(APP_PRIVATE_KEY)`
- `XXXX(APP_PUBLIC_KEY)`

RSA



--	--	--	--	--	--	--	--

1. openssl

```
CMD> openssl
```

2. RSA

```
OpenSSL> genrsa -out rsa_private_key.pem 2048
```

- [rsa_private_key.pem 2048 
-  openssl  PKCS#1-PEM

3. RSA

```
OpenSSL> rsa -in rsa_private_key.pem -pubout -out rsa_public_key.pem
```

- [illegible]

4. java PKCS8

```
OpenSSL> pkcs8 -topk8 -inform PEM -in rsa_private_key.pem -out rsa_private_key.pkcs8 -nocrypt
```

- [rsa_private_key.pem rsa_private_key.pkcs8 PKCS8]

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

- 公钥(WHALE_PUBLIC_KEY)

XXXXXXXXXXXX

1. 请求

请求头	请求体
请求方法	HTTPS 请求
请求URL	POST (application/json)
请求数据格式	JSON
请求编码	UTF-8
请求签名	SHA256WithRSA
请求内容	XXXXXXXXXXXX

2. 响应

XXXXXXXXXXXXXXXXXXXX

序号	字段名	数据类型	示例值	说明	备注
1	action	String	MakeCode	操作类型	枚举值
2	app_id	String	2014072300007148	应用ID	XXXXXXXXXXXXID
3	biz_content	String	BASE64	业务内容BASE64	XXXXXXXXXXXXBA
4	timestamp	String	1483372334	Unix时间戳	时间戳
5	version	String	20171212	版本号	XXXXXXXXXXXXXXXXXXXX
6	sign	String	7E65B60DCFA42B04	签名	XXXXXXXX

响应头

- 业务内容XXXXXXXXXXXXBASE64XXXXXXXXXXXX

JSON

```
{
  "traceNo": "99000009100010101732123",
```

```
"originalTraceNo": "99000009100010101732124"
}
```

- BASE64

```
ewogICAgICAgICAidHJhY2VObyl6ICI5OTAwMDAwOTEwMDAxMDEwMTczMjEyMyIsCiAgICAgICAgICJvcmlnaW5hbFRyYWNITm8iOiAiOTkwMDAwMDkxMDAwMTAxMDE3MzlxMjQiCiAgICAgfQ==
```

- biz_content
- app_idsign

JSON

```
{
  "action" : "efuli.cashvoucher.send",
  "app_id" : "2014072300007148",
  "biz_content" :
  "ewogICAgICAgICAidHJhY2VObyl6ICI5OTAwMDAwOTEwMDAxMDEwMTczMjEyMyIsCiAgICAgICAgICJvcmlnaW5hbFRyYWNITm8iOiAiOTkwMDAwMDkxMDAwMTAxMDE3MzlxMjQiCiAgICAgfQ==",
  "timestamp" : "1483372334",
  "version" : "20171212",
  "sign" : "7E65B60DCFA42B04"
}
```

3.

a.

signASCIIASCII

- biz_contentBase64

b.

“=”&

C.

SHA256WithRSAAPP_PRIVATE_KEYBase64

```
{
  "action" : "efuli.cashvoucher.send",
  "app_id" : "102410000",
  "biz_content" :
"ewogICAgICAgICAidHJhY2VObyl6ICI5OTAwMDAwOTEwMDAxMDEwMTczMjEyMyIsCiAgICAgICAgICJvcmlnaW5hbFRyYWNITm8iOiAiOTkwMDAwMDkxMDAwMTAxMDE3MzIxMjQiCiAgICAgfQ==",
  "timestamp" : "1483372334",
  "version" : "20171212",
  "sign" : "7E65B60DCFA42B04"
}
```

APP_PRIVATE_KEY

```
-----BEGIN RSA PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCdR0+PdnzkvvaNbSEp5Q8RpaelnrHu4msHAPiw1/
DJXFPucoEPqPmDAq4loaW02/mbvHQGr8d/g/g+cbCqUVctl8ygigTvlOAsOWJWrd76gk9IK+SsQBx3BN1pMbPADAljtF
S3ojw10MjCg/wlgmwWaqdCRB1QGwjzw3HnripbHr59BKMv/VYPvgDjx+ohQrfLd9fysbjRcsQKqCs72jxD8U9KHO87u
pvpZtjT2QYdVrntsWL1UUxfyElKmZy2Lf3UZvqKC4sahgH6pQhCMIhwBWm06FyktRji1ewNfF6zlpkCla/HvJzfqXaqhou
XJm2qgRjj/crftJONdd/9iuNIAgMBAAECggEAS4GbwY0p4ouHRFha7okIVfmIZautUrkilscxnXzeHV2U8cnjCiKePvY/ZOd
t7UkaKVks/rTO+vn5aMkd/nZ0evAAjiYUvoxjnymPU3u/q9Z5IWGgM83HnKAaR9FTsWRV8ab2cP3LYM6uQywoCFHM
4GotiFO5GucMo1T2Tzq/HOUAjmZQASQ0ywaANZvNoZDw6ScMPUGnYnHWbs34l7F2abyKyDiNo7sPtMtRpFYi+go+
S7dygMX0G1IFoClr4X2HNu/4e3XIFvjzoUhCF/byDcM992LvcWVgM3Ke/F1oBm+bCFit67hN6mxoi2SEARdQGnBysv
Vo1FLPHKZ60FVQKBgQDidFk8hq8YKEvcjqPSJsd8Oo30zeyWf0R/QNLQOAlqYKCJAcAiHDcYMx5clQQxjFTYXriY+B1J3
he6w3+5NStZqL1o1lcy5w7dhcVFXt1yn2KwUiO6YSJ25KeJHvXtDH66WGIQJMmbg90J2u4HRJxYNODmeVdS1seK5q
aL0uxs6wKBgQCxzHbdbkoiJgFd/c7BdTKnZh2h6x7SsX44lcbTqKsx7zA61ogoegHaKB4yq3xaR8Gm9uazo5SCtbjS0b
O5iQLrv8oLUDaNm5Ckm2ENk/M+TB0Hq24eFytiwUAS6FmdCncjq4xb2x8mqOQQiGvlyD91Na4HRBwxP16Wqwhz3
Nac7wKBgAY1IIDRXJm3+SSKELnhZOzGGkBdKSCTSSiGeYFWF9Ebpys6jg8hYO1b8XguadgF9gmcx0kCfKMa4OGxHJ
5yc8bYlqD6R5fQuBqg4WDehqHO9wDlr8wbf7ts158t5yZh0IO/uqigqZqHCheMFjzCx9qvUH9hUmCmHQCVBHoPBYa
TAoGBAJcixAPURaYjglQAdOIUE3vivNuvvqLBCBb090tifCvVM71AMBuegsaMBadyyCECECY6iL85FPvLN1HVuh3DzrzR
ahEV3VmgXGLgRa7CDintj1u+qLthXjr0xN+NrOdmRwIGSCio6iD1vfAj1vwbrX2X5Nf+WKywPlp7BpNerPv3AoGALv4i
JpOJVAW3Pmuvmc1a3cAsAvv0DGjiGOXn+lyBdX9tjKppVPEwElibNAltvvgWX++5ctYD2SXNQLV56rkZCmauXP2gT
PG3tCutH4jNiNIBUCfDXIt9DDyQAe0KfRFemzla5rTWA7wRNsVTCm3n4ZqPIKfMC4HmOGU2hgN3LY=
-----END RSA PRIVATE KEY-----
```

String List

```
action=efuli.cashvoucher.send&app_id=2014072300007148&biz_content=ewogICAglCAglCAidHJhY2VObyl6ICI5
OTAwMDAwOTEwMDAxMDEwMTczMjEyMyIsCiAgICAglCAglCJvcmlnaW5hbFRyYWNIbm8
iOiAiOTkwMDAwMDkxMDAwMTAxMDE3MzIxMjQiCiAgICAglCAglCAgQ==&timestamp=1483372334&version=20171212
```

□□□□

```
gUTdEB0IAS/ECKP98weSHf6k31Fmd4hcw0zPG8ewbMTfDFSubKlel/1C16upb2AHzN873HMwUlkcTg7ZuN92KDIkfsbl
Nd2lwVY2tWMvKt5O8gqC2a8XbS25ZObUILK5zMU7mQ/DLbyY+EAhkYdGnwsKloJkydi2zmLv99xT5G01yXBLSNiTr
PBTsc2OhBkA44kknok0x+hS4HfcgQwGPMG4y+V5aT1bhPDypwdbfAg+EN/5XoSECslcsvBirdk+BGPjBluwHHF+Hi
r/3E3i20lmtlowBc6jwh5qFOVqGN/w2UEPfg6xJxHyW04FBipt6mw7huD4PA4pA4qZRnsg==
```

□□**Demo Java**□

[□□□ signdemo.zip](#)

Revision #5

Created 21 July 2021 13:18:37 by zhangkexin

Updated 2 April 2022 16:28:06 by xieyuanhao