1.产生rsa 2048私钥

```
openssl genrsa -out rsa_2048_private.pem 2048
openssl genrsa -aes256 -passout pass:rockchip 2048
```

2.解出公钥

```
openssl rsa -in rsa_2048_private.pem -out rsa_2048_public.pem -pubout
```

3.pem转换der

```
openssl rsa -in rsa_2048_private.pem -outform DER -out rsa_2048_private.der
```

4.输出私钥的内容

```
openssl rsa -in rsa_2048_private.pem -text -noout
```

5.输出公钥的内容

```
openssl rsa -in rsa_2048_public.pem -pubin -text -noout
```

6.产生mykey.bin的sha256摘要,保存到mykey_sha256.bin中

```
openssl dgst -sha256 -binary -out mykey_sha256.bin mykey.bin
```

7.用私钥对mykey_sha256.bin进行rsa签名

```
openssl rsautl -sign -in mykey_sha256.bin -inkey rsa_2048_private.pem -out mykey_sha256_signed.bin
```

8.用公钥对mykey_sha256_signed.bin进行签名验证

```
openssl rsautl -verify -in mykey_sha256_signed.bin -inkey rsa_2048_public.pem -pubin
 -hexdump
```

9.用私钥对mykey_sha256.bin进行rsa签名,填充模式pss,salt值-1

```
openssl pkeyutl -sign
  -in mykey_sha256.bin -inkey rsa_2048_private.pem
  -out mykey_sha256_pss_signed.bin
  -pkeyopt digest:sha256
  -pkeyopt rsa_padding_mode:pss
  -pkeyopt rsa_pss_saltlen:-1
```