RSA 操作命令 - rsautil

- **RSA 操作命令 - rsautil**

openssl rsautl [-in file] [-out file] [-inkey file] [-pubin] [-certin] [-sign] [-verify] [-encrypt] [-decrypt] [-pkcs] [-ssl] [-raw] [-hex-dump] [-asn1parse]

RSA 簽署文件範例

RSA 簽署文件範例

```
[tsnien@csu_linux study]$ openssl rsautl -sign -inkey rsaprivate.pem -in data.txt -out sign.txt
[tsnien@csu_linux study]$ ls -l sign.txt
Enter pass phrase for rsaprivate.pem:                    【輸入通行碼】
-rw-rw-r-- 1 tsnien tsnien 64  8月  5 14:06 sign.txt
[tsnien@csu_linux study]$ openssl rsautl -verify -pubin -inkey rsapublic.pem -in sign.txt -out plain.txt
[tsnien@csu_linux study]$ cat plain.txt
01234567890123456789012345678 9
```

RSA 驗證文件範例

```
D:\OpenSSL_study>openssl rsautl -verify -in sig_1 -inkey rsa1.pem
```