

# 使用shell脚本生成自签名证书

## [下载自签名证书脚本](#)

shell脚本的使用说明如下：

- 脚本中使用openssl命令生成证书，执行前需要保证openssl命令可用。
- 脚本在centos 7和ubuntu 16.04中已经验证通过；在windows中的git bash里无法正确执行，不要在windows上的git bash里面执行脚本。
- 脚本命令格式如下：

```
./gen-cert.sh -a 算法 -d 域名 -n 证书文件名
```

脚本中的参数说明：

- -a 生成的证书中使用的算法，有rsa和ecc两种选项，rsa会生成2048位的key，ecc生成prime256v1的key；
- -d 证书中的域名，可以支持写多个域名，多个域名使用逗号分隔。第一个域名会作为CN（common name），这个参数里面所有的域名会写入证书的SAN（通过这可以一个证书支持多个不同域名）。
- -n 生成的服务器证书文件名。脚本生成的证书文件都放在certs目录下，如果目录下已经存在同名的证书文件则会跳过。第二次执行脚本时，如果-n参数指定为与第一次不同的名称，则会使用第一次生成的CA证书签发新的服务器证书。
- -h 查看脚本帮助。

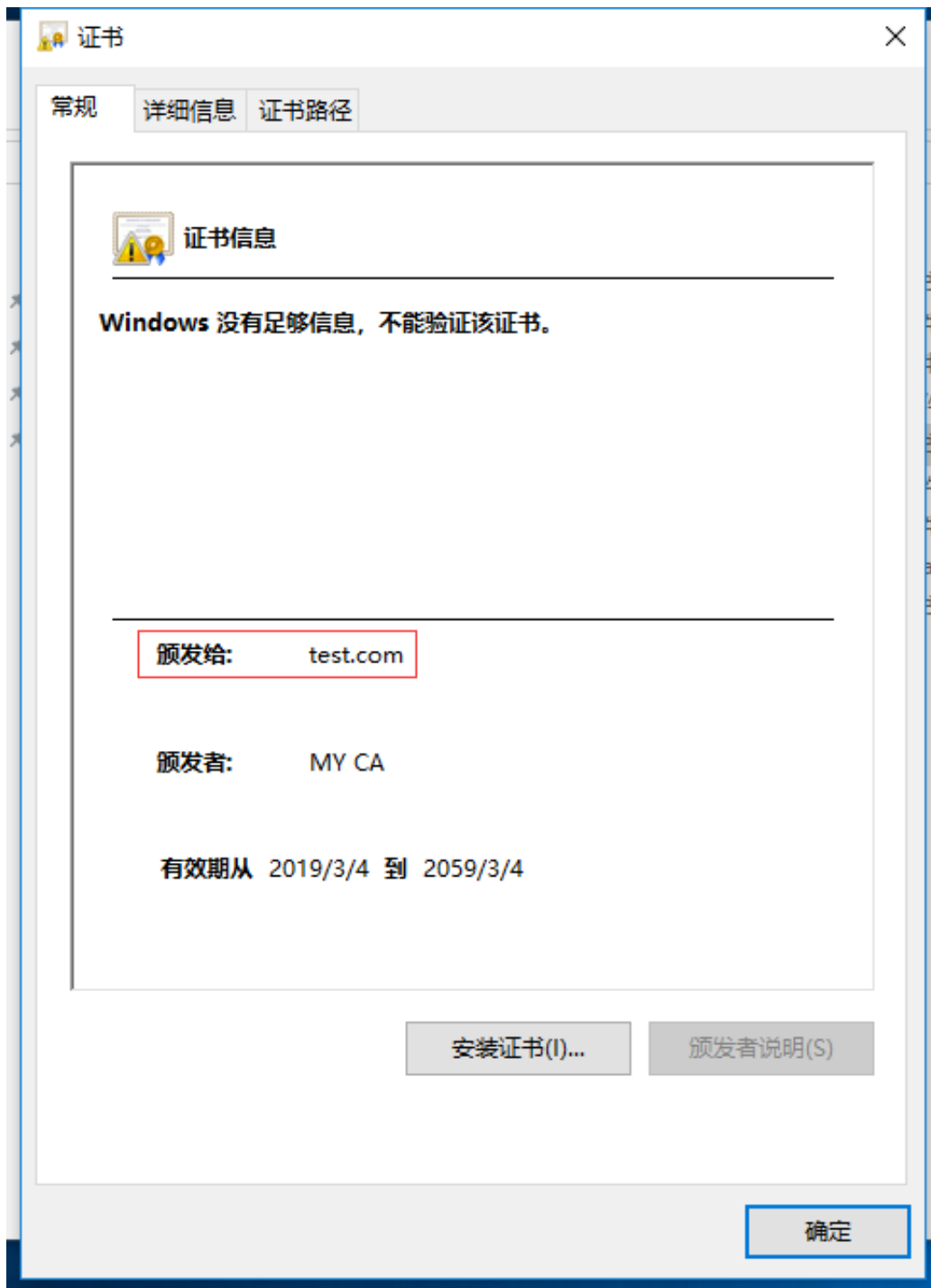
## 脚本执行示例

执行命令下面命令生成证书，生成pkcs12格式证书过程中会提示输入证书密码，请保持两次输入一致。虽然输入密码时可以直接回车设为空，由于某些使用证书的场景必须要密码，所以最好设置一个密码。生成的文件中ca.crt与ca.key为CA证书的公钥与私钥；test.crt与test.key为服务器证书的公钥与私钥；test.p12为pkcs12格式的文件，包含了公私钥。

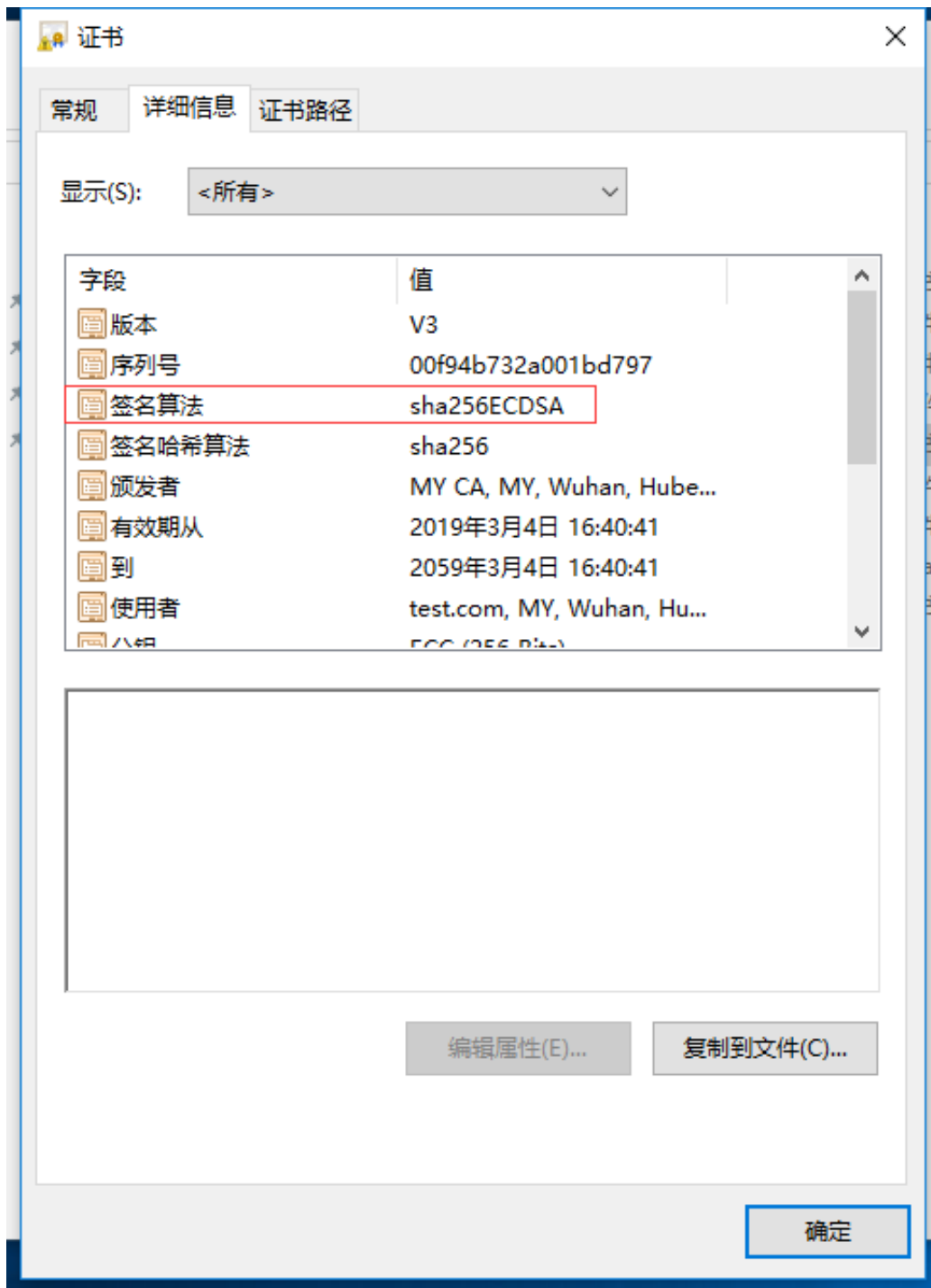
```
./gen-cert.sh -a ecc -d test.com,a.com,*.a.com -n test
```

```
[root@080tssp test]# ./gen-cert.sh -a ecc -d test.com,a.com,*.a.com -n test
san:DNS:test.com,DNS:a.com,DNS:*.a.com
algorithm:ecc
----- gen ca key-----
----- gen server key-----
Signature ok
subject=/C=CN/ST=Hubei/L=Wuhan/O=MY/CN=test.com
Getting CA Private Key
Enter Export Password:
Verifying - Enter Export Password:
[root@080tssp test]# ll ./certs/
total 36
-rw-r--r-- 1 root root 709 Mar  4 16:40 ca.crt
-rw-r--r-- 1 root root 302 Mar  4 16:40 ca.key
-rw-r--r-- 1 root root  17 Mar  4 16:40 ca.srl
-rw-r--r-- 1 root root 198 Mar  4 16:40 san.cnf
-rw-r--r-- 1 root root 733 Mar  4 16:40 test.crt
-rw-r--r-- 1 root root 436 Mar  4 16:40 test.csr
-rw-r--r-- 1 root root 1442 Mar  4 16:40 test-fullchain.crt
-rw-r--r-- 1 root root 302 Mar  4 16:40 test.key
-rw-r--r-- 1 root root 1542 Mar  4 16:40 test.p12
```

生成的服务器证书中“颁发给”为test.com，即-d参数中指定的第一个域名。



签名算法采用的ECC算法。



使用者可选名称包含了-d参数中指定的所有域名。

