



广东省数字证书认证中心

GDCA 信鉴易® 代码签名证书使用指南

2015/11/23

目录

一、使用说明.....	2
二、生成证书请求.....	2
1. 安装 OpenSSL 工具.....	2
2. 生成服务器证书私钥.....	2
3. 生成服务器证书请求 (CSR) 文件.....	3
4. 提交证书请求.....	5
三、代码签名证书转换成 PFX 格式.....	5
1. 获取服务器证书的根证书和 CA 证书.....	5
1.1 从邮件中获取	5
1.2 从 GDCA 官网上下载:	5
1.3 转换证书编码	6
2. 合成 PFX 证书.....	9
2.1 合并证书链	9
2.2 合成 PFX 证书	10
四、备份.....	11
六、证书遗失处理.....	11



一、文档说明

1. GDCA 信鉴易® 代码签名证书使用指南主要描述如何通过 openssl 产生密钥对及如何将代码签名证书合成 PFX 格式。
2. 本文档适用于恒信企业 (EV) 代码签名证书和速信个人代码签名证书。




二、生成证书请求

1. 安装 OpenSSL 工具

使用 Openssl 工具创建证书请求。通过下面地址下载安装版 OpenSSL:

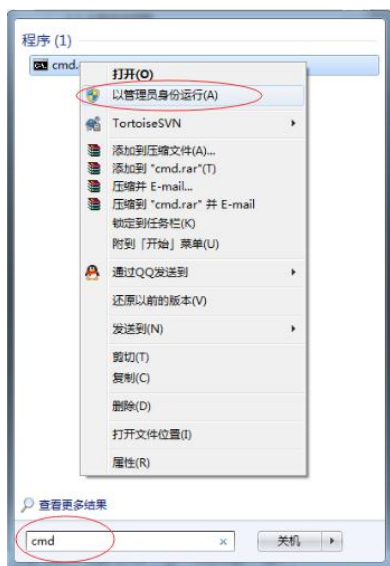
<http://slproweb.com/products/Win32OpenSSL.html>

此处以 win7 64 位系统为例。双击将 OpenSSL 安装到 C:\OpenSSL-Win64, 安装完后将 bin 目录下的 openssl.cfg 重命名为 openssl.cnf

 nuron.dll	2015/7/9 19:21	应用程序扩展	
 openssl.cfg	2015/7/9 4:57	CFG 文件	
 openssl	2015/7/9 19:21	应用程序	4

2. 生成服务器证书私钥

使用管理员权限打开命令行窗口，进入 bin 目录。

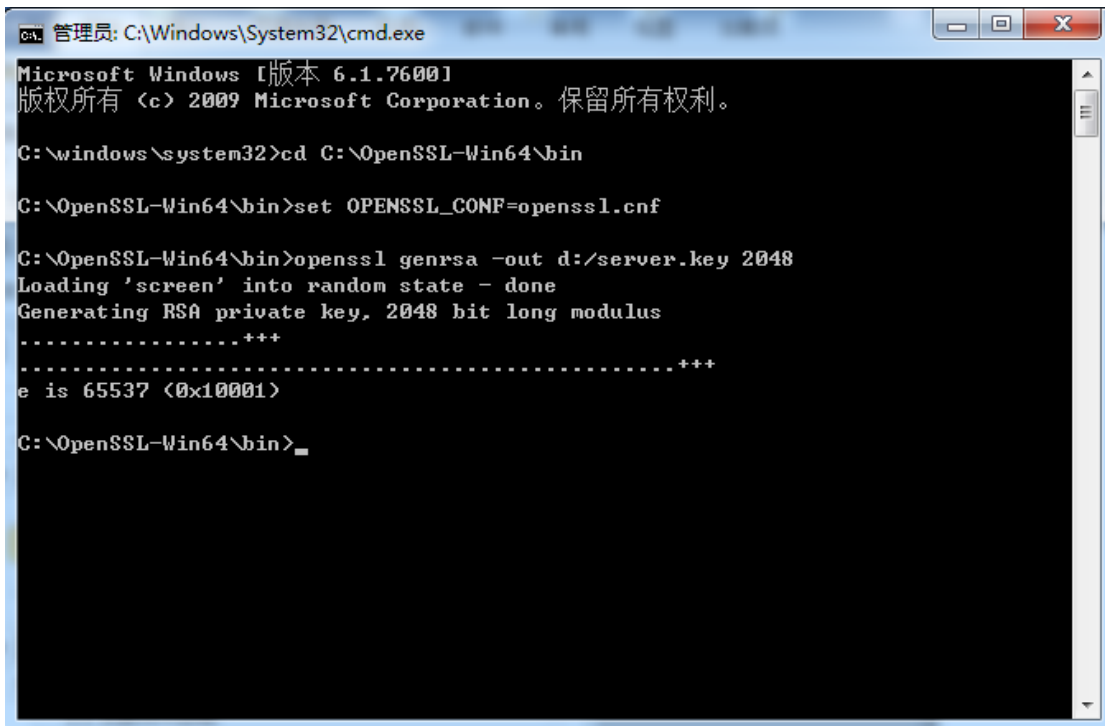


设置环境变量:

```
set OPENSSL_CONF=openssl.cnf
```

生成私钥:

```
openssl genrsa -out d:/server.key 2048
```



```
ca. 管理员: C:\Windows\System32\cmd.exe
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\windows\system32>cd C:\OpenSSL-Win64\bin

C:\OpenSSL-Win64\bin>set OPENSSL_CONF=openssl.cnf

C:\OpenSSL-Win64\bin>openssl genrsa -out d:/server.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)

C:\OpenSSL-Win64\bin>
```

3. 生成服务器证书请求 (CSR) 文件

生成证书请求:

```
openssl req -new -key d:\server.key -out d:\certreq.csr
```

如出现以下报错请先设置环境变量

```
set OPENSSL_CONF=openssl.cnf
```



```
c:\OpenSSL\bin>openssl req -new -key D:\testweb.95105813.cn.key -out D:\certreq.csr
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Unable to load config info from /usr/local/ssl/openssl.cnf

c:\OpenSSL\bin>
```

执行成功后提示要输入您的相关信息。填写说明:

1. Country Name:

填您所在国家的 ISO 标准代号, 如中国为 CN



2. State or Province Name:

填您单位所在地省/自治区/直辖市，如广东省或 Guangdong

3. Locality Name:

填您单位所在地的市/县/区，如广州市或 Guangzhou

4. Organization Name:

企业填写单位/机构/企业合法的名称，如广东数字证书认证中心有限公司或 Guangdong Certification Authority Co.,Ltd.

个人可直接按回车键跳过。

5. Organizational Unit Name:

企业用户可填部门名称，如技术支持部或 Technical support

个人用户可直接按回车键跳过。

6. Common Name:

企业填写单位/机构/企业合法的名称，如广东数字证书认证中心有限公司或 Guangdong Certification Authority Co.,Ltd.

个人填写身份证上姓名。

7. Email Address:

填写您的邮件地址。

8. 'extra' attributes

按回车跳过直至命令执行完毕。

```
C:\OpenSSL-Win64\bin>openssl req -new -key d:\server.key -out d:\certreq.csr
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:广东省
Locality Name (eg, city) []:广州市
Organization Name (eg, company) [Internet Widgits Pty Ltd]:广东数字证书认证中心
有限公司
Organizational Unit Name (eg, section) []:技术中心
Common Name (e.g. server FQDN or YOUR name) []:广东数字证书认证中心有限公司
Email Address []:mail@gdca.com.cn

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

C:\OpenSSL-Win64\bin>
```



除第 1、6、7、8 项外，2-5 的信息填写请统一使用中文或者英文填写。并确保您填写的所有内容和您提交到 GDCA 的内容一致。

4. 提交证书请求

请您保存好私钥文件 server.key，并将证书请求文件 certreq.csr 提交给 GDCA。

三、代码签名证书转换成 PFX 格式

1. 获取服务器证书的根证书和 CA 证书

服务器证书需要安装根证书和 CA 证书, 以确保证书在浏览器中的兼容性。有两种方式获取。

1.1 从邮件中获取

GDCA 完成证书签发后，会通过邮件方式，将代码签名证书、CA 证书及根证书返回给您，通过邮件获取根证书和 CA 证书：

➤ 根证书：

GDCA_TrustAUTH_R5_ROOT.cer

➤ 恒信企业 (EV) 代码签名证书 CA 证书：

GDCA_TrustAUTH_R4_Extended_Validation_CodeSigning_CA.cer

➤ 速信个人代码签名证书 CA 证书：

GDCA_TrustAUTH_R4_CodeSigning_CA.cer

1.2 从 GDCA 官网上下载：

根证书和 CA 证书也可以通过 GDCA 官网下载获得：

➤ 根证书：

http://www.gdca.com.cn/cert/GDCA_TrustAUTH_R5_ROOT.der

➤ 恒信企业 (EV) 代码签名证书 CA 证书：



http://www.gdca.com.cn/cert/GDCA_TrustAUTH_R4_Extended_Validation_CodeSigning_CA.der

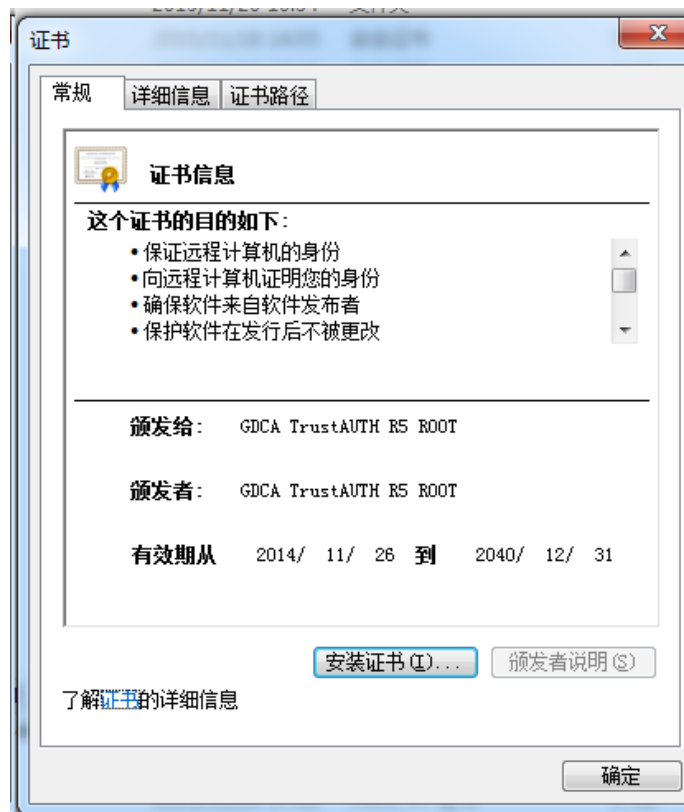
➤ 速信个人代码签名证书 CA 证书:

http://www.gdca.com.cn/cert/GDCA_TrustAUTH_R4_CodeSigning_CA.der

1.3 转换证书编码

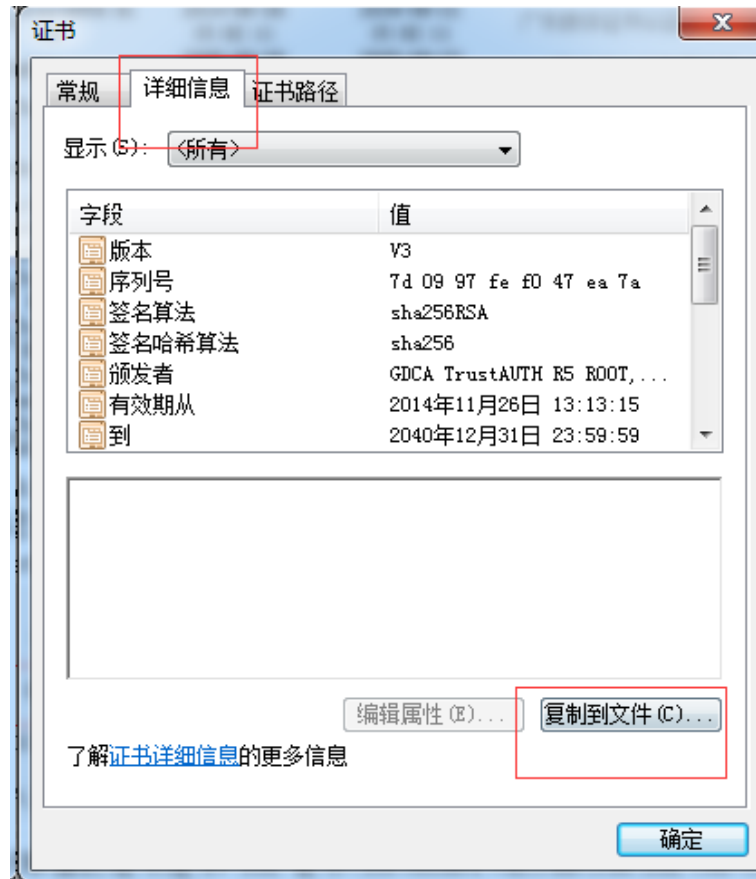
从官网上下载的证书需要先转换为 Base64 编码格式。以根证书为例:

打开证书:



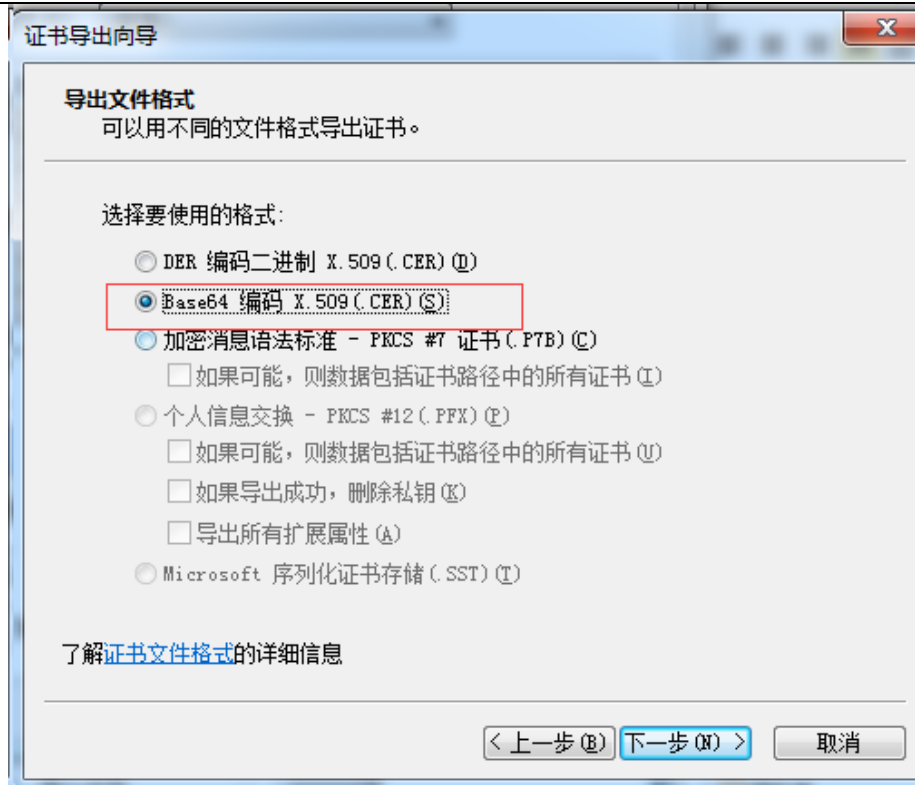
详细信息-复制到文件



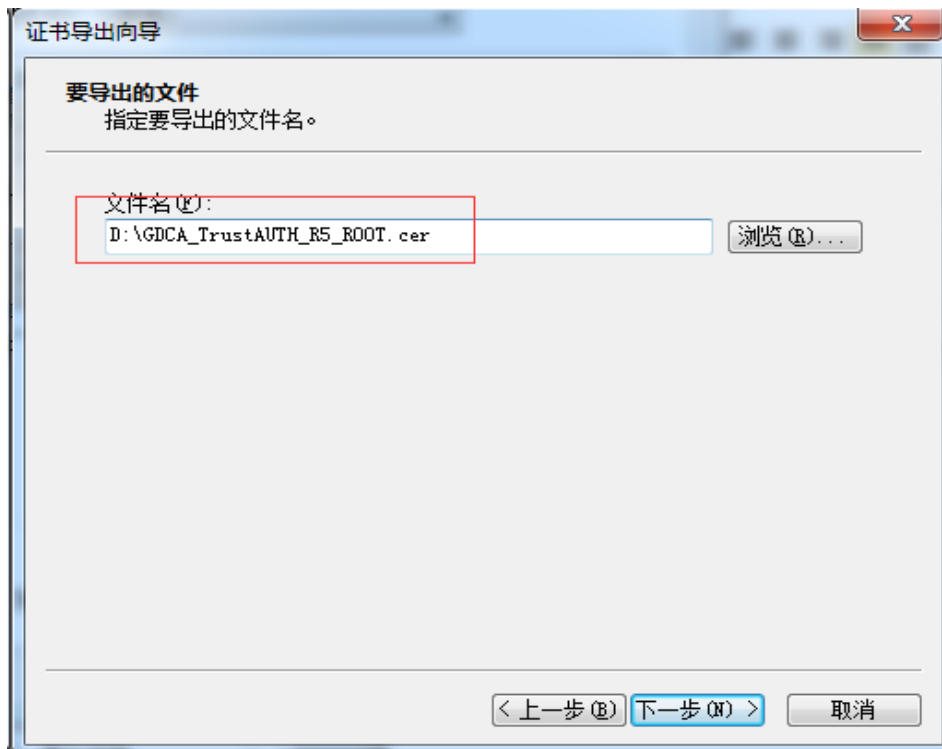


在证书导出向导里，将证书编码改成 Base64 编码格式





导出到指定目录里



转换成 Base64 编码格式后，用编辑器打开，可以看到文件内容是以
-----BEGIN CERTIFICATE-----开头，-----END CERTIFICATE-----结尾。以同样
方式将 CA 证书也转换成 Base64 编码格式。



```
-----BEGIN CERTIFICATE-----
MIIFiDCCA3CgAwIBAgIIIfQmX/vBH6nowDQYJKoZIhvcNAQELBQAwYjELMAkGA1UE
BhMCQ04xMjAwBgNVBAoMKUdVQU5HIERPTkcgQ0VSVElGSUNBVEUgQVVVUSE9SSVRZ
IENPLixMVEQuMR8wHQYDVQDDDBZHRENBIFRydXN0QVVUSCBSNSBST09UMB4XDTE0
MTEyNjA1MTMxNvOxDTQwMTIzMTk1OVowYjELMAkGA1UEBhMCQ04xMjAwBgNV
BAoMKUdVQU5HIERPTkcgQ0VSVElGSUNBVEUgQVVVUSE9SSVRZ IENPLixMVEQuMR8w
HQYDVQDDDBZHRENBIFRydXN0QVVUSCBSNSBST09UMIICiJANBgkqhkiG9w0BAQEF
AAOCAg8AMIICGKCAgEA2aMW8Mh0dHeb7zMNOWZ+Vfy1YI92hhJcFvZmPoiC7XJj
Dp6L3TQsAlFRwxn9WVSEyfFrs0yw6ehGXTjGoqcuEVe6ghWinI9tsJlKcVlriXBj
TnnEtlu9o12x8kECK62pOqPseQrsXzrj/e+APK00mxqriCZ7VqKChh/rNYmDf1+u
KU49tm7srsHwJ5uu4/Ts765/94Y9cnrrpftZTqfrlYwiOXnhLQiPzLyRuEH3FMEj
qc0tmkVes7LXLM3GKeJQEK5cy4KOFxg2fZfmiJqwTTQJ9Cy5WmYqsBebnh52nUpm
MUHFp/vFbu8btn4aRjb3ZGM74zkYI+dnRTVdVeSN72+ahsmUPI2JgaQxXABZG12
ZuGR224HwGGALrLuL4xwp9E7PLOR5G62xDtw8mySlwnNR30YwPO7ng/Wi64HtloP
zgsMR6f1Pri9fcebNaBhlzpbDRfMK5Z3KpIhHtmVdiBnaM8Nvd/WHwlqmuLMc3Gk
L30SgLDtMEZeS1SZD2fJpcjyIMGC7J0R38IC+xo70e0gmu9lZJIQDSri3nDxGGeC
jGHeuLzRL5z7D9Ar7Rt2ueQ5Vfj4oR24qoAATILnsn8JuLwwoC8N9VKejveSswoA
HQBulwbgSqfZxw9cZx08bV1X5021jelAU58VS6Bx9hoh49pwBiFYFIEFd3mqgnkC
AwEAAaNCMEAwHQYDVROBBYEFOLJQJ9NzuiiaoXzPdJ9lxSmIahlRMA8GA1UdEwEB
/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgGGMMA0GCSqGSIb3DQEBCwUAA4ICAQDRSVfg
p8xoWLoBDysZzY2wYUWsEeljUGn4H3++Fo/9nesLqjJHdtJnJO29fDMylrHBYZm
DRd9FBUB10v9H5r2XpdptxolpAqzkT9fNqyL7FeoPueBihhXOYV0GkLH6VsTX4/5
C0mSdI31R9Kr09b7eGZONn356ZLpBN79SWP8bfsUcZnNl0dKt7n/HipzceYwv1ry
L3ml4Y0M2fmyZeMN2WFcGpcWwlyualjPLHd+PwyvzeG5LuOmCd+uh8W4XAR8gPf
JWIYjYyMoSf/wA6E7qaTfRPuBRwlrHKK5DOKcFw9C+df/KQhtZa37dG/OaG+svg
IHZ6uqbL9XzeYqWxi+7egmaKTjowHz+Ay60nugxe19CxVsp3cbKldaFQQUBDF8Io
2c9S1lvIY9RCPqAzekYu9wogR1R+ak8x8YF+QnQ4ZXmN7sZ8uI7XpTrXmKGcjBBV
09tL7ECQ8sluV9JiDnxXk7Gnbc2dg7sq5+W2O3FYrf3RRbxake5TFW/TRQ11brqQ
XR4EzZffHqhmsYzmIGrv/EhOdJhCrylvLmrH+33RZjEizIYAfmaDDEL0vTSSwxrQ
T8p+ck0LcIymSLumoRT2+1hEmRSuqguTaaApJUqlyyvdimYHFngVv3Eb7PVHhPOe
MTd61X8kreS8/f3MboPoDKi3QWwh3b08hpcv0g==
-----END CERTIFICATE-----
```

将 GDCA 返回给您的代码签名证书也转换为 Base64 编码。

2. 合成 PFX 证书

2.1 合并证书链

新建一个 txt 文件，分别用文本编辑器打开根证书和 CA 证书，将文件内容是以-----BEGIN CERTIFICATE-----开头，-----END CERTIFICATE-----结尾都拷到 txt 文件里，将 txt 文件重命名为 ca.crt。



```

ca.crt
-----BEGIN CERTIFICATE-----
1  MIIFFSjCCAsGgAwIBAgIIb1Jz+4AagwDQYJKoZIhvcNAQELBQAwYjELMAkGA1UE
2  BHMCCQ04xMjAwBgNVBAcMKUdVQU5HIERPTkcgQ0VSVe1GSUNBVEUgQVUUSE9SSVRZ
3  IENPLkxvEQuMR8wHQYDVQDDb2HRENBIFRydXNOQVUUSCBNSBStO9UMB4XDTEO
4  MTEybnAsNDYwMjEwMDYwMTEzMDZMDRwMFowYXkzZjA3BGNVBAITAKN0MTIwMAYD
5  VQgQDC1HVUFORyBET0SHIENFULRJRklDQVRFEFVVEhFuk1UWSBDTY4tFFRELJzE9
6  MDgSA1UEAwORORDQSBUCnVzdeFVVEgUjQgRXhoOzW5kzWQgVmfFsaWRhG1v1b1BD
7  b2R1U21nbmluZyBDQCCASwDQYJKoZIhvcNAQELBQDggEPAADCAQgCcgEBAM2U
8  Masd1WuALHqFFocafNr2K5Pj5n6YVU3WyzQShkqpo+aKt6Muc0+U6LoYy1yGJNHG
9  jCnT4LoBwFj9oQtQs75n85K1/N1JPYvDEj4eMKgLL1D8urea+LhmKgJwZHSJ4r
10  6o+/keWkFvUNqqkeLJyghERDB2+XrnsQIZtyfAKL4R19LzomJ38WAVRF97pHFgO
11  3Fxa5WrTne6xewB1ZTc6q+SOJA0oUD2wvGRZBap/QGI+sQeUVpwXkKZcAyJ2mf
12  ZwgRdAyuqkmdXNdg7kzS851u70vq312tLTa509JppPC8tftIa+B4Ftes1QCXNI80z
13  S1dMaFkQXkR1VCAcM7kCAWAAaOCAX8wggF7MIgFBggrBgEFBQCBAQR5HwQgYI
14  KwYBBQUHMAKGNmhdHAE6Ly93d3cuZ2RjY5S5jb20uY24yY2VydC9HRENBX1RyZXNO
15  QVUUSCBNSBStO9ULMrlcjAxBggrBgEFBQcwAYY1aHR0cDovL3d3dy5nZGhhLnMv
16  BS5jbl19UcnVzdeFVVEgUjQgRXhoOzW5kzWQgVmfFsaWRhG1v1b1BD
17  OHQWbWYDMVROTAKH/BAUwAwEB/zAFBgNVHSMEDAwgBT1yUCFtc7cmqF8zw4/ZcUq
18  1GoZUTBIBGNVHSAEQTA/MDOGC1qBHIbvLwEBBwEwLzAtBggrBgEFBQcCARThaHR0
19  cDovL3d3dy5nZGhhLnMvS5jbl19jcmVzXyY3BzMEYGA1UdHicwMDw06A5oDeG
20  21NWh0HAE6Ly93d3cuZ2RjY5S5jb20uY24yY3UsLodEQ0FFVHJ1c3RBVWwvX1I1X1JF
21  TIQuY3JmM4GA1UgdwEB/wQEAwIBh3ANBgkqhkiG9w0BAQsFAAOCAQEAAhplQmCZCA证书
22  TBu5oQk0ERzZp399y95Mtk0479d0s7W4Jb0eHe15MprndJ0dlcL2Ka7dSHy7
23  M5ZCGD4x0Sawz2Utz01bPasfOW0Ia8MwEJ2SB9yPoNgrJFFVcKq0x3teFgU3a0s
24  PenOrb+/p1TuB0rOgDPvEkMth4KG1L1KVVd+OfJ08vOspTzffaf5hkoYB1vqbUEN
25  0v/gKcN1sawAenLr7Tbz5V4MhYEEe/fKp0h72Xme6N1ZJT7y4hNVy3EfmGM0
26  SNAx2NtcmY1wksE04QMGrrvdPzPmv117XJeOYABqBLJy99yNS+sSAnkhl1jFIZfv
27  1y3AS8M0H052vMYeMstCmpsfEZX3pX+fjJ88zeLpmpU2y30FRroIkjruUMycRY
28  HdI7cVDldf5ZnrmSgFhEbjRrUn/+OCTPBXX54ujUJTBMMBrci92LpZDOV30QnAy
29  YScwUSHvvlE7W5Oy2hWUz3Y5WmEWHDavRqZrd1FpJV0aR9Z5NkInNjwvY1ZBEX
30  Ke100XnFOcVH6uNw2CmLnc0ECEQs57cvHcqFe7uCXj6VXte20dMcd0805DpPRLWB
31  Pe/jBFLFgk6x31uU0HkKT7cB0UAbVnYFA4bgh4ezxIS/VWVbNuxdVMgI43z2bwR
32  d2VNMZbYh60VBOA2I31nOR3hQbvyFLdQeUE=
33  -----END CERTIFICATE-----
34
35
36  -----BEGIN CERTIFICATE-----
37  MIIFFSjCCAsGgAwIBAgIIIfQmX/vBH6nowDQYJKoZIhvcNAQELBQAwYjELMAkGA1UE
38  BHMCCQ04xMjAwBgNVBAcMKUdVQU5HIERPTkcgQ0VSVe1GSUNBVEUgQVUUSE9SSVRZ
39  IENPLkxvEQuMR8wHQYDVQDDb2HRENBIFRydXNOQVUUSCBNSBStO9UMB4XDTEO
40  MTEybnAsNDYwMjEwMDYwMTEzMDZMDRwMFowYXkzZjA3BGNVBAITAKN0MTIwMAYD
41  VQgQDC1HVUFORyBET0SHIENFULRJRklDQVRFEFVVEhFuk1UWSBDTY4tFFRELJzE9
42  MDgSA1UEAwORORDQSBUCnVzdeFVVEgUjQgRXhoOzW5kzWQgVmfFsaWRhG1v1b1BD
43  b2R1U21nbmluZyBDQCCASwDQYJKoZIhvcNAQELBQDggEPAADCAQgCcgEBAM2U
44  Masd1WuALHqFFocafNr2K5Pj5n6YVU3WyzQShkqpo+aKt6Muc0+U6LoYy1yGJNHG
45  jCnT4LoBwFj9oQtQs75n85K1/N1JPYvDEj4eMKgLL1D8urea+LhmKgJwZHSJ4r
46  6o+/keWkFvUNqqkeLJyghERDB2+XrnsQIZtyfAKL4R19LzomJ38WAVRF97pHFgO
47  3Fxa5WrTne6xewB1ZTc6q+SOJA0oUD2wvGRZBap/QGI+sQeUVpwXkKZcAyJ2mf
48  ZwgRdAyuqkmdXNdg7kzS851u70vq312tLTa509JppPC8tftIa+B4Ftes1QCXNI80z
49  S1dMaFkQXkR1VCAcM7kCAWAAaOCAX8wggF7MIgFBggrBgEFBQCBAQR5HwQgYI
50  KwYBBQUHMAKGNmhdHAE6Ly93d3cuZ2RjY5S5jb20uY24yY2VydC9HRENBX1RyZXNO
51  QVUUSCBNSBStO9ULMrlcjAxBggrBgEFBQcwAYY1aHR0cDovL3d3dy5nZGhhLnMv
52  BS5jbl19UcnVzdeFVVEgUjQgRXhoOzW5kzWQgVmfFsaWRhG1v1b1BD
53  OHQWbWYDMVROTAKH/BAUwAwEB/zAFBgNVHSMEDAwgBT1yUCFtc7cmqF8zw4/ZcUq
54  1GoZUTBIBGNVHSAEQTA/MDOGC1qBHIbvLwEBBwEwLzAtBggrBgEFBQcCARThaHR0
55  cDovL3d3dy5nZGhhLnMvS5jbl19jcmVzXyY3BzMEYGA1UdHicwMDw06A5oDeG
56  21NWh0HAE6Ly93d3cuZ2RjY5S5jb20uY24yY3UsLodEQ0FFVHJ1c3RBVWwvX1I1X1JF
57  TIQuY3JmM4GA1UgdwEB/wQEAwIBh3ANBgkqhkiG9w0BAQsFAAOCAQEAAhplQmCZCA证书
58  TBu5oQk0ERzZp399y95Mtk0479d0s7W4Jb0eHe15MprndJ0dlcL2Ka7dSHy7
59  M5ZCGD4x0Sawz2Utz01bPasfOW0Ia8MwEJ2SB9yPoNgrJFFVcKq0x3teFgU3a0s
60  PenOrb+/p1TuB0rOgDPvEkMth4KG1L1KVVd+OfJ08vOspTzffaf5hkoYB1vqbUEN
61  0v/gKcN1sawAenLr7Tbz5V4MhYEEe/fKp0h72Xme6N1ZJT7y4hNVy3EfmGM0
62  SNAx2NtcmY1wksE04QMGrrvdPzPmv117XJeOYABqBLJy99yNS+sSAnkhl1jFIZfv
63  1y3AS8M0H052vMYeMstCmpsfEZX3pX+fjJ88zeLpmpU2y30FRroIkjruUMycRY
64  HdI7cVDldf5ZnrmSgFhEbjRrUn/+OCTPBXX54ujUJTBMMBrci92LpZDOV30QnAy
65  YScwUSHvvlE7W5Oy2hWUz3Y5WmEWHDavRqZrd1FpJV0aR9Z5NkInNjwvY1ZBEX
66  Ke100XnFOcVH6uNw2CmLnc0ECEQs57cvHcqFe7uCXj6VXte20dMcd0805DpPRLWB
67  Pe/jBFLFgk6x31uU0HkKT7cB0UAbVnYFA4bgh4ezxIS/VWVbNuxdVMgI43z2bwR
68  d2VNMZbYh60VBOA2I31nOR3hQbvyFLdQeUE=
69  -----END CERTIFICATE-----
70

```

2.2 合成 PFX 证书

通过 OpenSSL 命令，输入密码，合成 PFX 格式证书，注意两次输入密码要一致：

openssl pkcs12 -export -inkey d:\server.key -in 代码签名证书 -CAfile d:\ca.crt -chain -out 输出 pfx 证书 -name usercert

```

C:\OpenSSL-Win64\bin>openssl pkcs12 -export -inkey d:\server.key -in d:\usercert
.cer -CAfile d:\ca.crt -chain -out d:\usercert.pfx -name usercert
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:
C:\OpenSSL-Win64\bin>

```



四、备份

备份证书私钥文件 server.key 及代码签名证书。

六、证书遗失处理

若您的证书文件损坏或者丢失且没有证书的备份文件，请联系 GDCA（客服热线 95105813）办理遗失补办业务，重新签发证书。

