



数安时代科技股份有限公司

GDCA 信鉴易® SSL 服务器证书部署指南

For Apache 2.4 windows 版本

修订日期：2017/03/08

目录

一、部署前特别说明.....	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.....	3
3. 生成服务器证书请求（CSR）文件.....	3
4. 提交证书请求.....	5
三、服务器证书的导入.....	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
1.3 转换证书编码.....	错误！未定义书签。
2. 导入根证书和 CA 证书到服务器证书.....	7
四、安装服务器证书.....	8
五、备份和恢复.....	9
1. 备份服务器证书.....	9
2. 恢复服务器证书.....	10
六、证书遗失处理.....	10



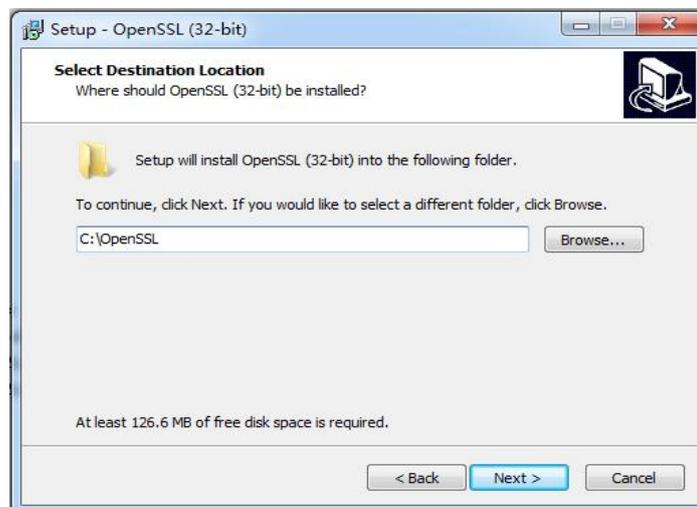
一、部署前特别说明

1. GDCA 信鉴易® SSL 服务器证书部署指南(以下简称“本部署指南”)主要描述如何通过 openssl 产生密钥对和如何将 SSL 服务器证书部署到 Apache 服务器
2. 本部署指南适用于 windows 系统下 Apache 2.4 版本;
3. Apache 服务器部署恒信企业 EV SSL 和睿信 SSL 证书的操作步骤一致, 区别在于: 前者在 IE7 以上浏览器访问时, 浏览器会显示安全锁标志, 地址栏会变成绿色; 而后者在浏览器访问时, 浏览器显示安全锁标志, 但地址栏不会变成绿色。
4. 本部署指南使用 testweb.95105813.cn 作为样例进行安装配置, 实际部署过程请用户根据正式的域名进行配置。
5. 您可以使用其它方式并不要求按照本部署指南在 windows 下使用 OpenSSL 工具方式生成证书请求文件。
6. 如用户已经生成证书请求文件, 请从第四三点服务器证书的导入开始阅读。

二、生成证书请求

1. 安装 OpenSSL 工具

您需要使用 Openssl 工具来创建证书请求。下载 OpenSSL 安装版 <http://slproweb.com/products/Win32OpenSSL.html> 安装 OpenSSL 到 C:\OpenSSL



安装完后将 C:\OpenSSL\bin 目录下的 openssl.cfg 重命名为 openssl.cnf



2. 生成服务器证书私钥

命令行进入 C:\OpenSSL\bin，生成证书私钥。产生的私钥文件可以是 server.key 这样简单的命名或者使用我们推荐的使用主机域名方式进行命名。

```
cd c:\OpenSSL\bin
```

先设置环境变量

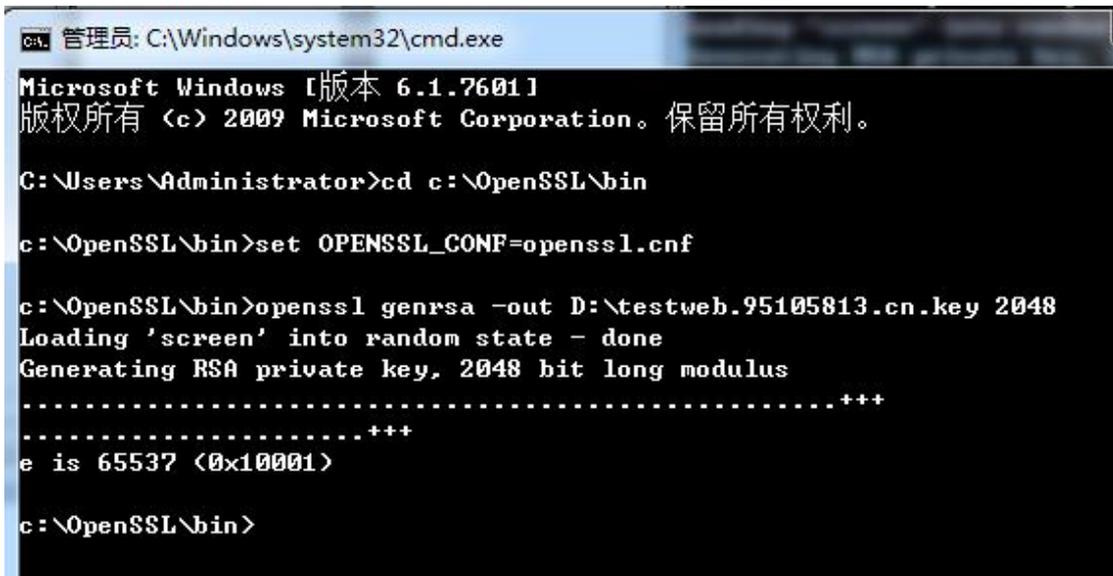
```
set OPENSSL_CONF=openssl.cnf
```

参考：

```
openssl genrsa -out server.key 2048
```

例：

```
openssl genrsa -out D:\testweb.95105813.cn.key 2048
```



```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>cd c:\OpenSSL\bin

c:\OpenSSL\bin>set OPENSSL_CONF=openssl.cnf

c:\OpenSSL\bin>openssl genrsa -out D:\testweb.95105813.cn.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)

c:\OpenSSL\bin>
```

3. 生成服务器证书请求（CSR）文件

参考：

```
openssl req -new -key server.key -out certreq.csr
```

例：

```
openssl req -new -key D:\testweb.95105813.cn.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，美国为 US

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，如佛山市或 Foshan

4.Organization Name:

填您单位/机构/企业合法的名称，如数安时代科技股份有限公司或 Global Digital Cybersecurity Authority Co., Ltd.

5.Organizational Unit Name:

填部门名称，如技术支持部或 Technical support

6.Common Name:

填域名，如： testweb.95105813.cn。在多个域名时，填主域名

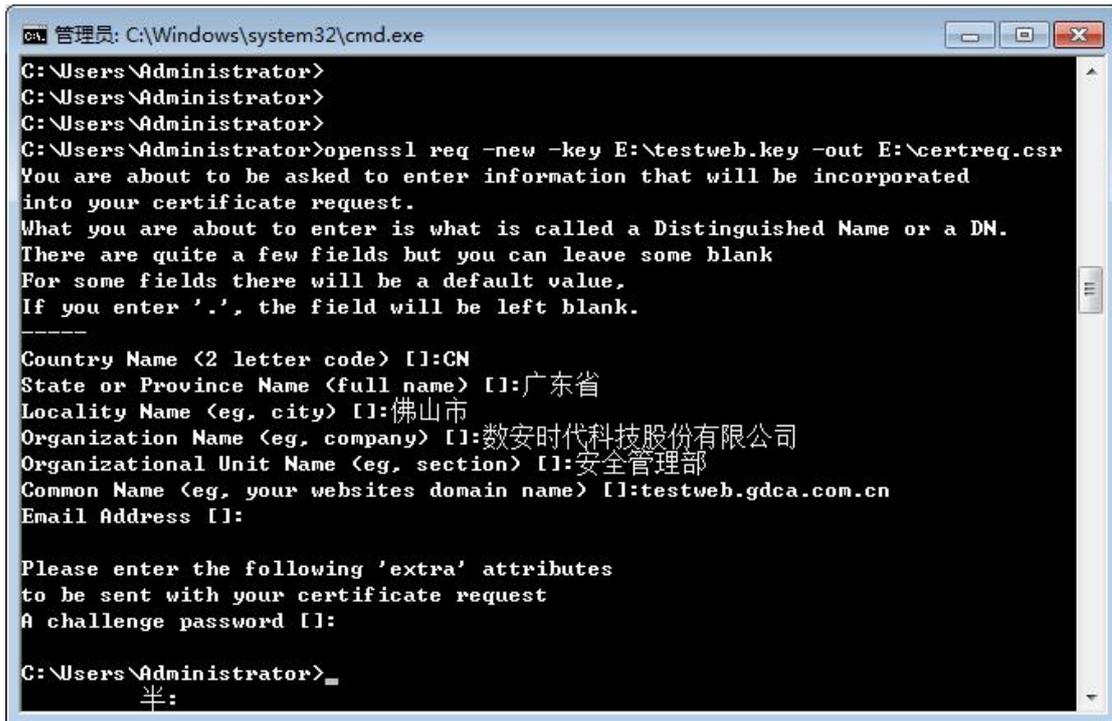
7.Email Address:

填您的邮件地址，不必输入，按回车跳过

8.'extra'attributes

从信息开始的都不需要填写，按回车跳过直至命令执行完毕。





```
管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>openssl req -new -key E:\testweb.key -out E:\certreq.csr
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> []:CN
State or Province Name <full name> []:广东省
Locality Name <eg, city> []:佛山市
Organization Name <eg, company> []:数安时代科技股份有限公司
Organizational Unit Name <eg, section> []:安全管理部
Common Name <eg, your websites domain name> []:testweb.gdca.com.cn
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
C:\Users\Administrator>_
半:
```

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，以保证 SSL 证书的签发。

4. 提交证书请求

请您保存证书私钥文件 testweb.95105813.cn.key，最好复制一份以上副本到不同的物理环境上（如不同的主机），防止丢失。并将证书请求文件 certreq.csr 提交给 GDCA。

三、服务器证书的导入

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

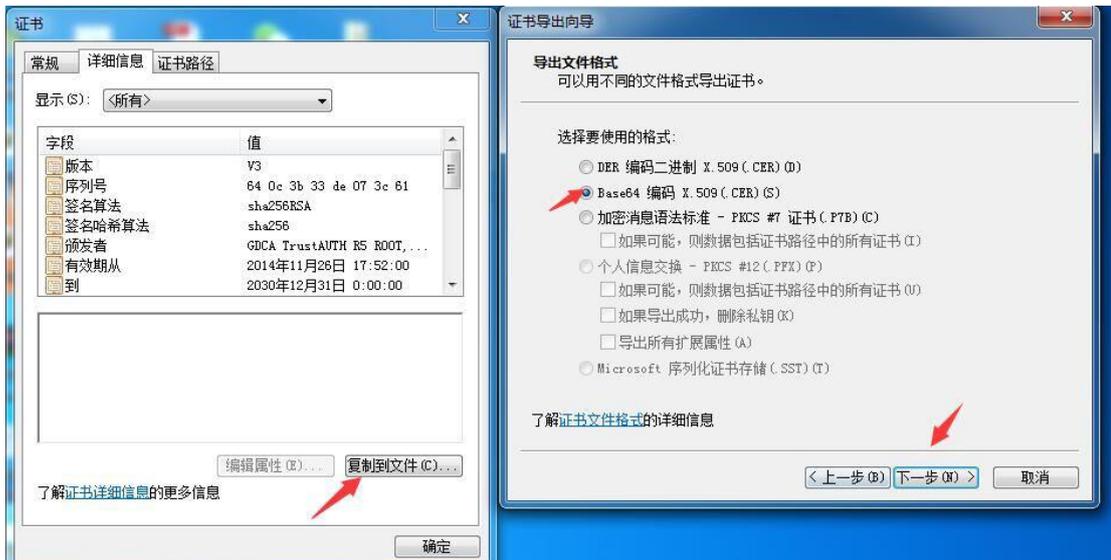
在您完成申请 GDCA 服务器证书的流程后，GDCA 将会在返回给您的邮件中附上根证书 GDCA_TrustAUTH_R5_ROOT.cer 和相应的 CA 证书，请留意查看申请证书时填写的邮箱。如



果您申请的是睿信(OV) SSL 证书 (Organization Validation SSL Certificate), CA 证书文件就是 **GDCA_TrustAUTH_R4_OV_SSL_CA.cer**; 如果您申请的是恒信企业 EV SSL 证书 (Extended Validation SSL Certificate), CA 证书就是文件就是 **GDCA_TrustAUTH_R4_EV_SSL_CA.cer**, 请确认所收到的证书文件是您需要的 CA 证书。(注意: 所发至邮箱的文件是压缩文件, 里面有 3 张证书, 请确认所收到的证书文件是您需要的 CA 证书文件)



从 GDCA 官网获取根证书和 CA 证书后需要转换成 Base64 编码格式, 如下图所示:



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-----
MIIFiDCCA3CgAwIBAgIIfQmX/vBH6nowDQYJKoZIhvcNAQELBQAwYjELMAkGA1UE
BhMCQ04xMjAwBgNVBAoMKUdVQU5HIERPTkcgQ0VSVElGSUNBVEUgQVVUSE9SSVRZ
IENPLixMVEQuMR8wHQYDVQDDDBZHRENBIFRydXN0QVVUSCBSNSBST09UMB4XDTE0
MTEyNjA1MTMxNVoXDQWMTIzMTE1NTk1OVowYjELMAkGA1UEBhMCQ04xMjAwBgNV
BAoMKUdVQU5HIERPTkcgQ0VSVElGSUNBVEUgQVVUSE9SSVRZ IENPLixMVEQuMR8w
HQYDVQDDDBZHRENBIFRydXN0QVVUSCBSNSBST09UMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCGKCAgEA2aMW8Mh0dHeb7zMNOWZ+Vfy1YI92hhJCFVZmPoiC7XJj
Dp6L3TQsAlFRwxn9WVSEyffrs0yw6ehGXTjGoqcuEve6ghWinI9tsJlKcVlriXBj
TnnEt1u9o12x8kEck62pOqPseQrsXzrj/e+APK00mxqriCZ7VqKCh/rNYmDf1+u
KU49tm7srsHwJ5uu4/Ts765/94Y9cnrrpftZTqfrlywiOXnhLQiPzLyRuEH3FMEj
qcOtmkVES7LXLM3GKeJQEK5cy4KOFxg2fzfmiJgwTTQJ9Cy5WmYqsBebnh52nUpm
MUHFp/vFBu8btn4aRjb3ZGM74zkYI+dndRTVdVeSN72+ahsmUPI2JgaQxXABZG12
ZuGR224HwGGALrIuL4xwp9E7PLOR5G62xDtw8mySlwnNR30YwPO7ng/Wi64HtloP
zgsMR6f1Pri9fcebNaBhlzpbDRfMK5Z3KpIhHtmVdiBnaM8Nvd/WHwlqmuLmC3Gk
L30SgLDtMEZeS1SZD2fJpcjyIMGC7J0R38IC+xo70e0gmu91zJIQDSri3nDxGGec
jGHeuLzRL5z7D9Ar7Rt2ueQ5Vfj4oR24qoAATILnsn8JuLwwoC8N9VKejveSswoA
HQBU1wbgsQfZxw9cZX08bVlX5021jelAU58VS6Bx9hoh49pwBiFYFieFd3mqgnkC
AwEAAaNCMEAwHQYDVR0OBBYEFOLJQJ9NzuiaoxzPDj91xSmIahlRMA8GA1UdEwEB
/wQFMAMBAf8wDgYDVR0PAQH/BAQDAggGMA0GCSqGSIb3DQEBCwUAA4ICAQDRSVfg
p8xoWLoBdysZzY2wYUWsEeljUGn4H3++Fo/9nesLqjJHdtJnJO29fDmlyrHBYZm
DRd9FBUB1Ov9H5r2XpdptxolpAqzkT9fnqyL7FeoPueBihhXOYV0GkLH6VsTX4/5
ComSdI31R9Kr09b7eGZONn356ZlpBN79SWP8bfsUcZnNL0dKt7n/HipzcEYwv1ry
L3ml4Y0M2fmyYzeMN2WfCgpcWwlyualjPLhd+PwyvzeG5LuOmCd+uh8W4XAR8gPf
JWlYjYYYMoSf/wA6E7qaTfRPuBRwlrHKK5DOKcFw9C+df/KQhtZa37dG/OaG+svg
IHZ6uqbL9XzeYqWxi+7egmaKTjowHz+Ay60nugxe19CvVsp3cbK1daFQQUBDF8Io
2c9SilvIY9RCPqAzekYu9wogRlR+ak8x8YF+QnQ4ZXMn7sZ8uI7XpTrXmKGCjBBV
09tL7ECQ8s1uV9JiDnxXk7Gnbc2dg7sq5+W2O3FYrf3RRbxake5TFW/TRQ11brqQ
XR4EzzffhQhmsYzmIGrv/EhOdJhCrylvLmrH+33RZjEizIYAfmaDDEL0vTSSwXrq
T8p+ck0LcIymSLumoRT2+1hEmRSugguTaaApJUqlyyvdimYHFngVV3Eb7PVHhPoe
MTd61X8kreS8/f3MboPoDKi3QWwH3b08hpcv0g==
-----END CERTIFICATE-----
```

2. 导入根证书和 CA 证书到服务器证书

按照 1.3 步骤将 GDCA 返回给您的服务器证书如 testweb.95105813.cn 也转换为 Base64 编码。然后将用文本编辑器打开您的服务器证书、CA 证书和根证书，将 CA 证书和根证书都加入到您的服务器证书文件里，将文件保存为 testweb.95105813.cn.crt。

文件里证书的保存顺序是 服务器证书-CA 证书-根证书：

例： testweb.95105813.cn.crt



```
testweb.95105813.cn.crt  GDCA_TrustAUTH_R4_Extended_Validation_SSL_CA.cer  GDCA_TrustAUTH_R5_P...
28  NTqMy5jboIudGVzdHd1YjYjIuOTUxMDU4MTMuY24wDQYJKoZIhvcNAQELBQADggEB
29  AHoyjJiXnz2687cmFRgdBZfC+SjLnu6d1BWeSc9qojEWWFz4xO6S3EAgSXbsNe6mx
30  kKtghECL1WK0x3b25xbQ8YsXaUw8owYB9FLHN/pP15Y9EddpupNnSbesKGCvUDV
31  eePK4ht5IpBNqQRoMh6HyVcIO/kiwmg3YSsMk4tWKjspbUU34ASTAjyXLIbu/V8G
32  7LJoFEJzOrK5yh4K3S2Ccys0h2kK6FvxD8iN7J+HXKjJlWQJ975ox3jhlI+nuUy/F
33  x87U9gTSuer1I45c2yFGOF0whI6LsNnN293... 服务器证书
34  Ovjky+kubBgU0LctMI70+ATI=
35  -----END CERTIFICATE-----
36
37  -----BEGIN CERTIFICATE-----
38  MIIF3TCCA8WgAwIBAgIINy+Ch1zmLbEwDQYJKoZIhvcNAQELBQAwYjELMAkGA1UE
39  BhMCQ04xMjAwBgNVBAAcMkUdVQU5HIERPTkcgQ0VSVE1GSUNBVEUgQVU5E9SSVRZ
40  IENPLi4xMVEQuMR8wHQYDVQDDZHRENBIFRydXNOQVU5C0VSU0VSU0VSU0VSU0VSU0
41  MTEyNjA5NDUyNVc0XDTMwMTIzMDUyMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEw
42  BAOMKUDVQU5HIERPTkcgQ0VSVE1GSUNBVEUgQVU5E9SSVRZ IENPLi4xMVEQuMTUw
43  MwYDVQDDCkxHRENBIFRydXNOQVU5C0VSU0VSU0VSU0VSU0VSU0VSU0VSU0VSU0VSU0
44  TCBDQCCASiEwDQYJKoZIhvcNAQELBQADggEAPDCCAQcCggEBAAMcA1HwmgR2biK15
45  a46bkeXyOruAocQZx779CY9Yq7kUdW4nPdiTKK1k/xkIJJUwA6xzJomrCuMzr1Z0
46  J17LviwOIN6rDBSSOKjR6V0P82kkVHLIgd7n6mpJU22Evyj06Pj/NC5maYchb0sOh
47  TA05Yt58q9a3qMpDq9fS/AzYKAVXWBMXh4x1B0XmGUpjYv3NXAtEznScauk9mg1
48  NzMMYu09iDqG7clqsoFdsauRKnAk1ExvgkdoSjg9w2Q2wem0cbbGgF8uQGAy/+
49  o/wop1GvmcL+P7b7bgYUaxI9HlMrFhBSscNK+cEFBkkW7K/0PpXBd41RHHWLLkE
50  Z9ieC4ECawEAAaOCAx3wggF7MIGFBggrBgqEFAOMKUDVQU5HIERPTkcgQ0VSVE1GSUNB
51  Nmh0dHA6Ly93d3cuZ2RjYSSjB20uY24vY2V5ZVY5ZDZHRENB1RydXNOQVU5F9SNV9S
52  T09ULmR1c3AxBggrBgqEFAOMKUDVQU5HIERPTkcgQ0VSVE1GSUNBVEUgQVU5E9SSVRZ
53  dEFVVEgub2NzDAdBdGVHQU5HIERPTkcgQ0VSVE1GSUNBVEUgQVU5E9SSVRZ IENPLi4x
54  AQH/BAUwAwEB/zAfBgNVHSMGDAWgBTiyUCFtc7cmqF8zw4/ZcUpiGoZUTBIgNV
55  HSAEQTA/MD0GC1gBH1bvLwEBBgEwLzAtBggrBgqEFAOMKUDVQU5HIERPTkcgQ0VSVE1GSUNB
56  ZGNhLmNvbS5jb20uY24vY3J5L0dEdEQ0FVHJ1c3RvVVRX11X1JPT1QuY3JwMA4G
57  A1UdDwEB/wQEAwIBhjANBgkqhkiG9w0BAQsFAAOCAgEAJ+QTFRloac6P1jKtKm58L
58  gIdCKwybREfAj+QTDNTOhM1apn6mZeuSLHbZB1oyetddz1OMM8iJyU+ktJIHY
59  mlM3opIt3IuTWBbJobyDZyD+doed6H7gLcpOM11bDVraXpVcNRTVM70Tfved90B3
60  E8Bi+sBTAkV/Mp01tFWBDK2Nk29jHtE650zOMK1+sF9EK0cQwzBbX3vG1WpeMdY
61  Hpu7z7xdZdYbOMT8Iub+1Ph4vUMahXLKohEjXBypWeyUr+L8dE0mdaZsZku/VQm
62  ZQyDfNzHfUm2hH/XhC611NMA8/oeW99J/yfc/TN1CpImqHk0XBNeZeqK2HPBKj39
63  oMG0q5/KMT43jvTpjvjIX3tNnD+nzLcS48IogZ/X2qyGgh7FHntLC2DBj/1pmHh
64  4CJt/dxAXODH/Z/rwhGVciR3zAXaLb21tLS+AhUvMwIrrzJC1kI6gU2deUCkjoSM
65  1VFTjyyWxpK7e1kUpdml7fcBmUWsjKnzV6H5YETONK2YKsXDJdgrUn1S67qbIB
66  XAYQnEc/MYoi.spbeYRksVciKV1D1Dehl/gGQ80nCWsxj7gUTewVWgON3h/HP/+z
67  W8fh7J1c5YfbjSszWLOGEEAomWos0Ba1KHxVR+1yVfn/yxGypKd4t+7vRc3GwD
68  blVRfCZEmVBCWtd0BC52GxM=
69  -----END CERTIFICATE-----
70
71  -----BEGIN CERTIFICATE-----
72  MIIF1DCCA3CgAwIBAgIIIfQmX/vBH6nowDQYJKoZIhvcNAQELBQAwYjELMAkGA1UE
73  BhMCQ04xMjAwBgNVBAAcMkUdVQU5HIERPTkcgQ0VSVE1GSUNBVEUgQVU5E9SSVRZ
74  BHMCCQ04xMjAwBgNVBAAcMkUdVQU5HIERPTkcgQ0VSVE1GSUNBVEUgQVU5E9SSVRZ
75  IENPLi4xMVEQuMR8wHQYDVQDDZHRENBIFRydXNOQVU5C0VSU0VSU0VSU0VSU0VSU0
76  MTEyNjA5NDUyNVc0XDTMwMTIzMDUyMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEw
77  BAOMKUDVQU5HIERPTkcgQ0VSVE1GSUNBVEUgQVU5E9SSVRZ IENPLi4xMVEQuMR8w...
```

四、安装服务器证书

打开 apache 安装目录下 conf 目录中的 httpd.conf 文件,如:

```
vi /usr/local/apache/conf/httpd.conf
```

找到以下两项去掉注释:

```
# LoadModule ssl_module modules/mod_ssl.so
```

```
#Include conf/extra/httpd-ssl.conf
```

保存退出。



a. 打开 Apache2.4/conf/extra/目录下的 httpd-ssl.conf 文件,将
"ServerName www.example.com:443"改成您的主机域名,

b.添加 SSL 协议支持语句, 关闭不安全的协议和加密套件

```
SSLProtocol all -SSLv2 -SSLv3
```

c.修改加密套件如下

```
SSLCipherSuite AESGCM:ALL:!DH:!EXPORT:!RC4:+HIGH:!MEDIUM:!LOW:!aNULL:!eNULL
```

d.找到如下三个选项 SSLCertificateFile、SSLCertificateKeyFile 和 SSLCertificateChainFile 这三个配置项, 将 testweb.95105813.cn.crt 和 tetweb.95105813.cn.key 及证书链 gdca-cert-chain.crt 文件上传到该目录 (这里是/usr/local/apache/conf) 下:

```
# require an ECC certificate which can also be configured in
# parallel.
SSLCertificateFile "/usr/local/apache/conf/testweb.95105813.cn.crt"
#SSLCertificateFile "/usr/local/apache/conf/server-dsa.crt"
#SSLCertificateFile "/usr/local/apache/conf/server-ecc.crt"

# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
# ECC keys, when in use, can also be configured in parallel
SSLCertificateKeyFile "/usr/local/apache/conf/testweb.95105813.cn.key"
#SSLCertificateKeyFile "/usr/local/apache/conf/server-dsa.key"
#SSLCertificateKeyFile "/usr/local/apache/conf/server-ecc.key"

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convenience.
SSLCertificateChainFile "/usr/local/apache/conf/gdca-cert-chain.crt"

# Certificate Authority (CA):
-- INSERT --
```

保存退出, 并重启 Apache, 通过 https 方式访问您的站点, 测试站点证书的安装配置。

五、备份和恢复

在您完成服务器证书的安装与配置后, 请务必备份好您的服务器证书, 避免证书遗失给您造成不便:

1. 备份服务器证书

备份服务器证书私钥文件 testweb.95105813.cn.key, 服务器证书文件



testweb.95105813.cn.crt，即可完成服务器证书的备份操作。

2. 恢复服务器证书

参照步骤第四步即可完成恢复操作。

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，重新签发服务器证书。

