



广东省数字证书认证中心

GDCA 信鉴易® SSL 服务器证书部署指南

For Apache 2.4 windows 版本

2015/11/23

# 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.....	6
1.2 从 GDCA 官网上下载: .....	6
1.3 转换证书编码.....	8
2. 导入根证书和 CA 证书到服务器证书.....	11
四、安装服务器证书.....	12
五、备份和恢复.....	14
1. 备份服务器证书.....	15
2. 恢复服务器证书.....	15
六、证书遗失处理.....	15



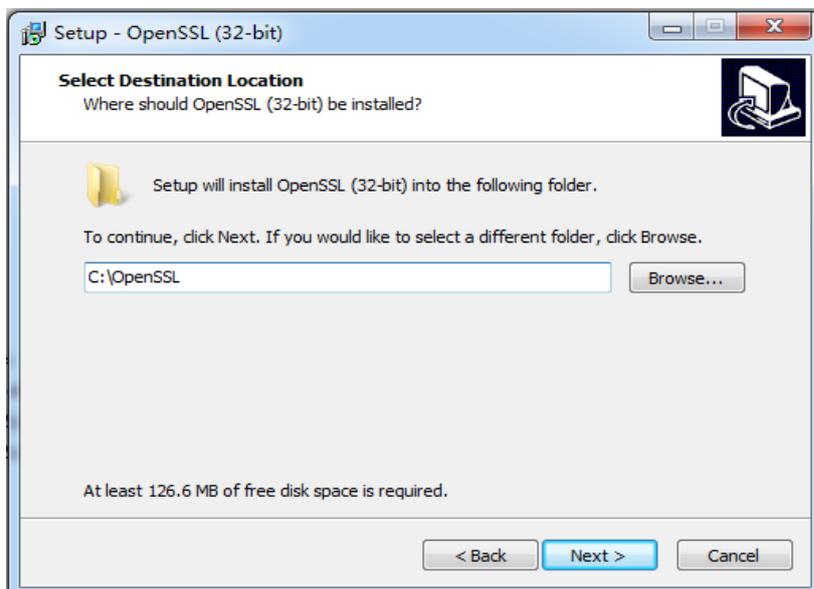
## 一、部署前特别说明

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。

## 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

 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

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

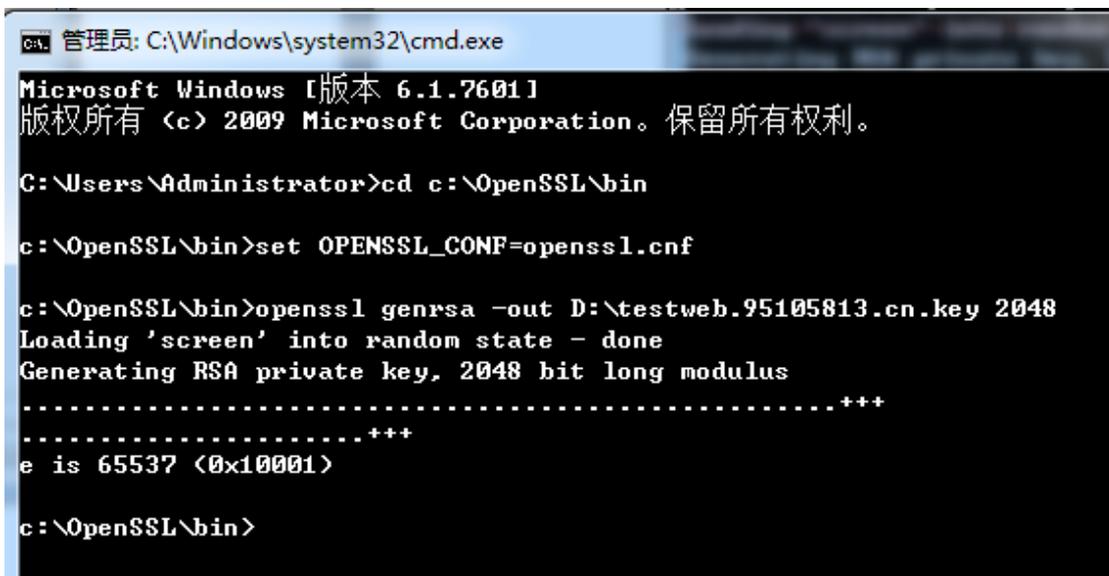
```
set OPENSSL_CONF=openssl.cnf
```

参考：

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

例：

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



```
管理员: 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, 如广东数字证书认证中心有限公司或 Guangdong Certification 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:\OpenSSL\bin>openssl req -new -key D:\testweb.95105813.cn.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) []:佛山市
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) []:安全管理部
Common Name (e.g. server FQDN or YOUR name) []:testweb.gdca.com.cn
Email Address []:

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

c:\OpenSSL\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，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

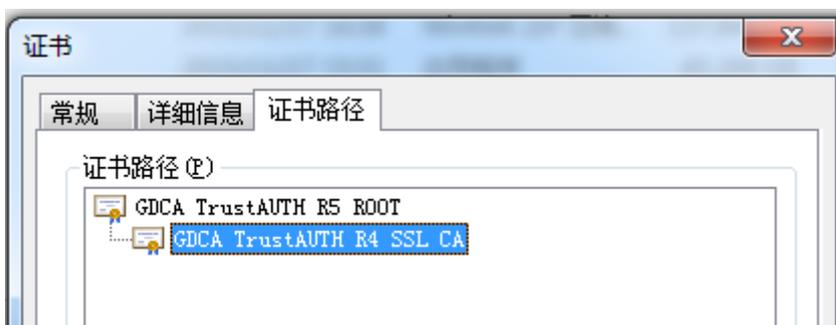
服务器证书需要安装根证书和 CA 证书，以确保证书在浏览器中的兼容性。有两种方式获取。



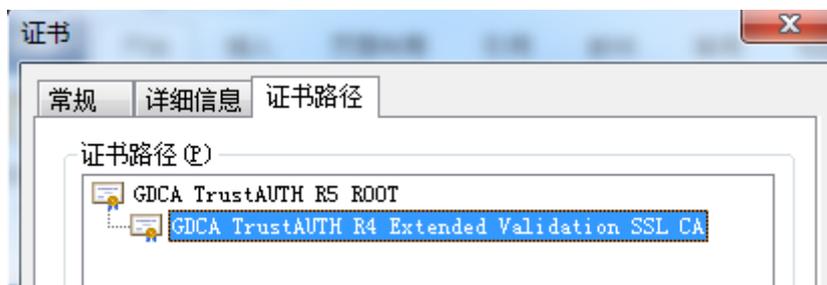
## 1.1 从邮件中获取

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服务器证书以及根证书 GDCA\_TrustAUTH\_R5\_ROOT.cer 和相应的 CA 证书。如果您申请的是睿信(OV) SSL 证书 (Organization Validation SSL Certificate)，CA 证书就是文件就是 GDCA\_TrustAUTH\_R4\_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\_Extended\_Validation\_SSL\_CA.cer, 请确认所收到的证书文件是您需要的 CA 证书。

GDCA\_TrustAUTH\_R4\_SSL\_CA.cer:



GDCA\_TrustAUTH\_R4\_Extended\_Validation\_SSL\_CA.cer:



## 1.2 从 GDCA 官网上下载:

<http://www.gdca.com.cn/channel/001002002>





获取根证书: GDCA\_TrustAUTH\_R5\_ROOT.cer:

#### 下载根证书

为保证您的证书能够正常使用，需要为浏览器下载并安装CA根证书，这样您的浏览器才能信任由GDCA签发的所有证书（下载后双击证书文件进行安装）。

12 项, 显示 1 到10. [首页/前一页] 1 2 [下一页/末页]

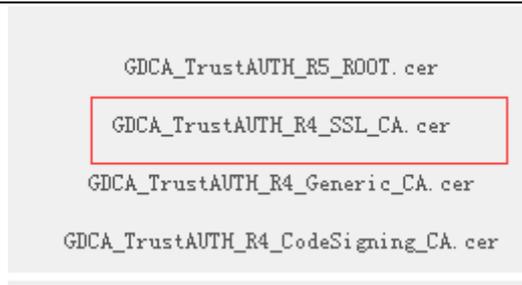
CA名称	起始有效时间	截止有效时间	CA证书下载
ROOTCA_sm2	2012-07-14 11:11:59	2042-07-07 11:11:59	社会公众应用根证书 (SM2) .cer
GDCA TrustAUTH E1 CA	2014-06-26 15:02:11	2034-06-21 15:02:11	广东数字证书认证中心有限公司_sm2.cer
ROOTCA_rsa	2005-08-28 16:16:16	2025-08-23 16:16:16	社会公众应用根证书 (RSA) .cer
GDCA TrustAUTH R2 CA	2013-12-16 14:29:40	2018-12-15 14:29:40	广东数字证书认证中心有限公司_rsa.cer
GDCA Root CA	2004-01-11 17:34:22	2024-12-11 00:00:00	GDCA_Root_CA.cer
GDCA Guangdong Certificate Authority	2004-01-12 10:13:07	2024-01-12 10:13:07	GDCA_Guangdong_Certificate_Authority.cer
GDCA TrustAUTH R5 ROOT	2014-11-26 13:13:15	2040-12-31 23:59:59	GDCA_TrustAUTH_R5_ROOT.cer
GDCA TrustAUTH R4 SSL CA	2014-11-26 17:52:00	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_SSL_CA.cer
GDCA TrustAUTH R4 Generic CA	2014-11-26 17:53:00	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_Generic_CA.cer
GDCA TrustAUTH R4 CodeSigning CA	2014-11-26 17:54:35	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_CodeSigning_CA.cer

#### 获取 CA 证书:

如果您申请的证书是睿信(OV) SSL 证书 (Organization Validation SSL),

下载 GDCA\_TrustAuTH\_R4\_SSL\_CA.cer





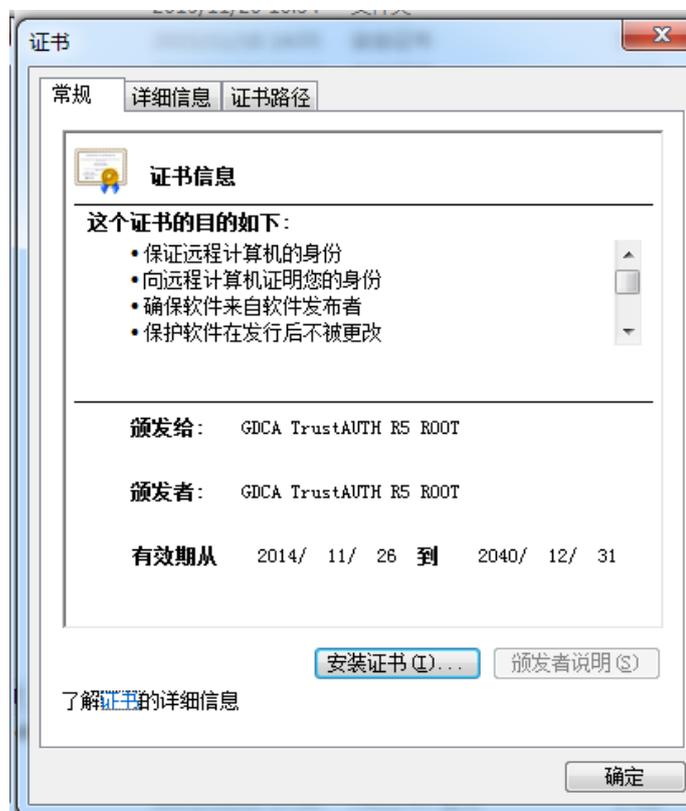
如果您申请的证书是恒信企业 EV SSL 证书 (Extended Validation SSL Certificates), 则下载 GDCA\_TrustAUTH\_R4\_Extended\_Validation\_SSL\_CA.cer

12 项, 显示 11 到 12. [首页/前一页] 1, 2 [下一页/末页]

CA名称	起始有效时间	截止有效时间	CA证书下载
GDCA TrustAUTH R4 Extended Validation SSL CA	2014-11-26 17:45:25	2030-12-31 00:00:00	<b>GDCA_TrustAUTH_R4_Extended_Validation_SSL_CA.cer</b>

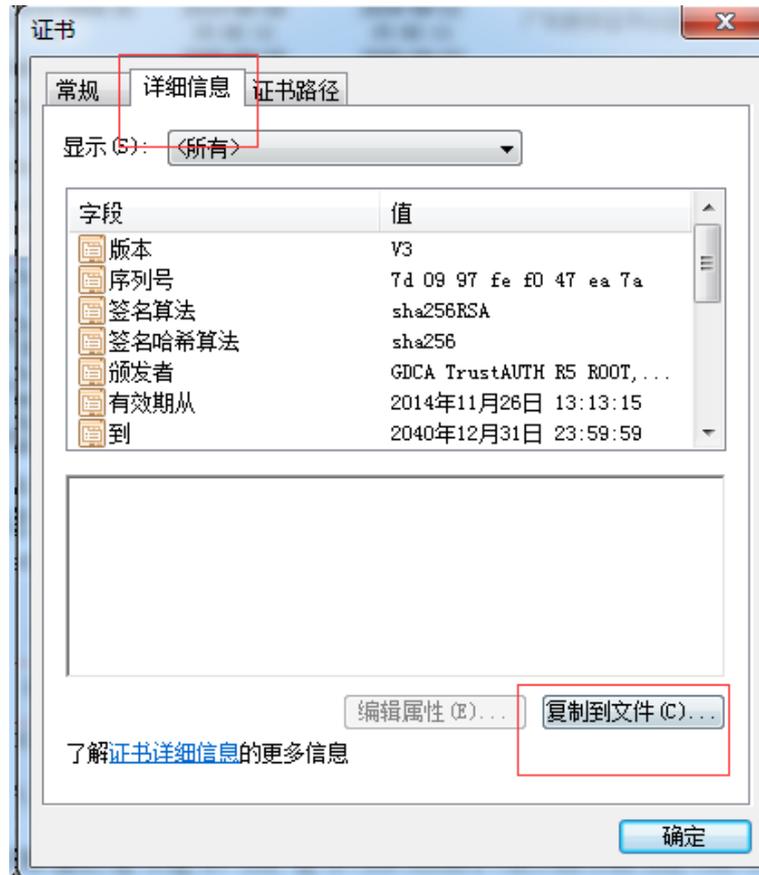
### 1.3 转换证书编码

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：



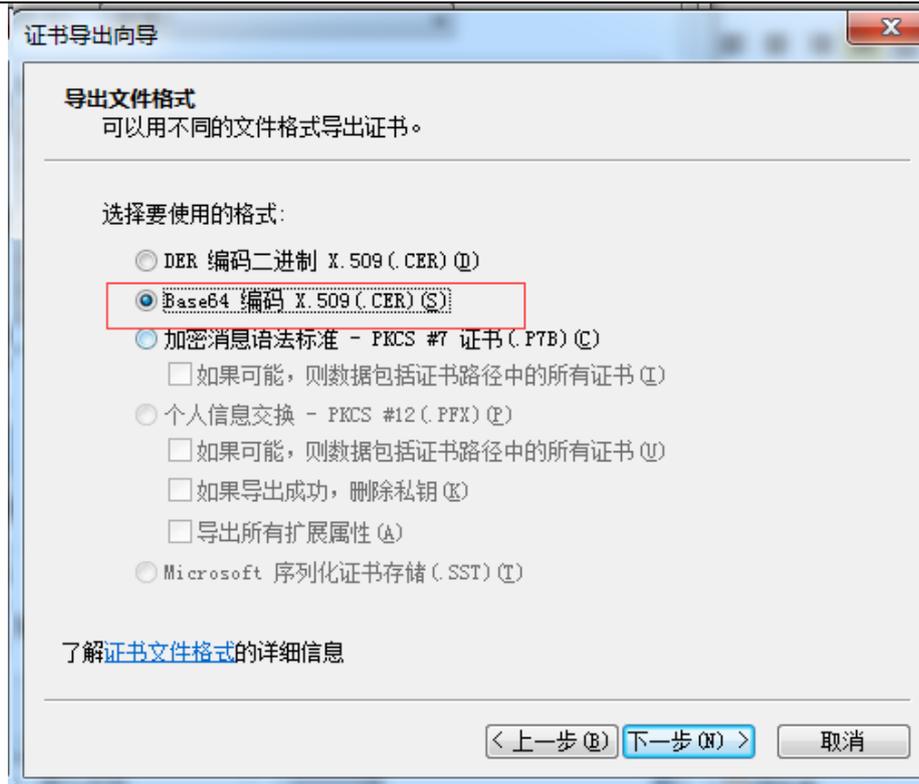
详细信息-复制到文件



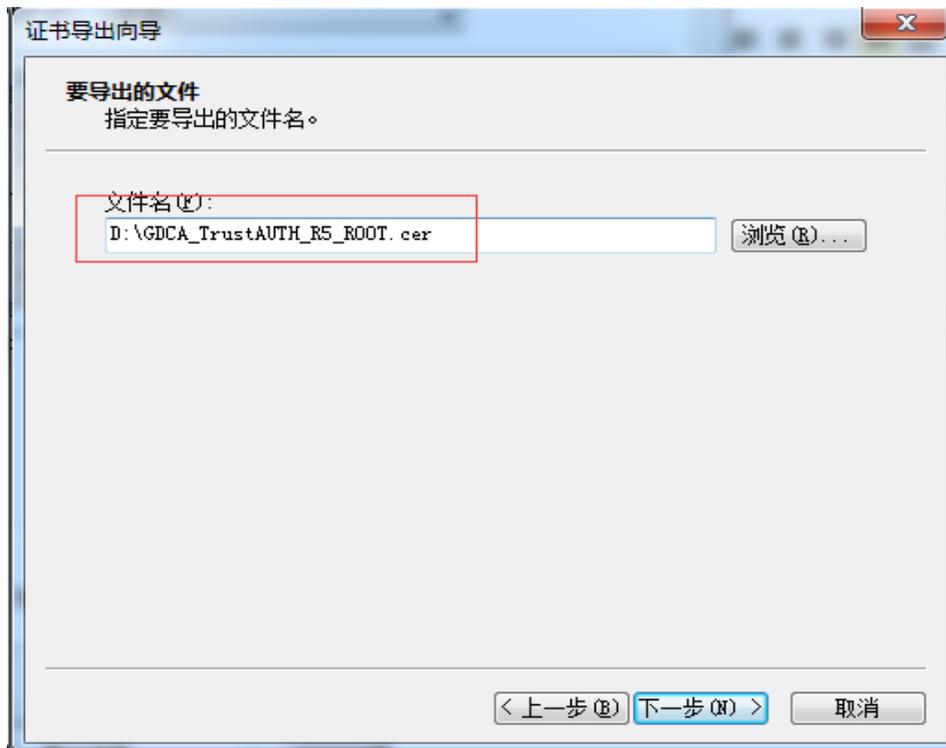


在证书导出向导里，将证书编码改成 Base64 编码格式





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-----
MIIFiDCCA3CgAwIBAgIIfQmX/vBH6nowDQYJKoZIhvcNAQELBQAwYjELMAkGA1UE
BhMCQ04xMjAwBgNVBAoMKUdVQU5HIERPTkcgQ0VSVElGSUNBVEUgQVVUSE9SSVRZ
IENPLixMVEQuMR8wHQYDVQDDDBZHRENBIFRydXN0QVVUSCBSNSBST09UMB4XDTE0
MTEyNjA1MTMxNVoXDTQwMTIzMTk1NTk1OVowYjELMAkGA1UEBhMCQ04xMjAwBgNV
BAoMKUdVQU5HIERPTkcgQ0VSVElGSUNBVEUgQVVUSE9SSVRZIENPLixMVEQuMR8w
HQYDVQDDDBZHRENBIFRydXN0QVVUSCBSNSBST09UMIICiANBgkqhkiG9w0BAQEF
AAOCAg8AMIICGKCAgEA2aMW8Mh0dHeb7zMN0wZ+Vfy1YI92hhJcFVZmPoiC7XJj
Dp6L3TQsAlFRwxn9WVSEyfFrs0yw6ehGXTjGoqcuEVe6ghWinI9tsJLKcVlriXBj
TnnEtlu9o12x8kEck62pOqPseQrsXzrj/e+APK00mxqriCZ7VqKCh/rNYmDf1+u
KU49tm7srsHwJ5uu4/Ts765/94Y9cnnrpfTzTqfrlYwiOXnhLQiPzLyRuEH3FMEj
qc0tmkVes7LXLM3GKeJQEK5cy4KOFxg2fZfmiJqwTTQJ9Cy5WmYqsBebnh52nUpm
MUHFp/vFBU8btn4aRjb3ZGM74zkYI+dndRTVdVeSN72+ahsmUPI2JgaQxXABZG12
ZuGR224HwGGALrIuL4xwp9E7PLOR5G62xDtw8mySlwnNR30YwPO7ng/Wi64HtloP
zgsMR6f1Pri9fcebNaBhlzpbDRfMK5Z3KpIhHtmVdiBnaM8Nvd/WHwlqmuLMc3Gk
L30SgLDtMEZEslSZD2fJpcjyIMGC7J0R38IC+xo70e0gmu9lZJIQDsri3nDxGGeC
jGHeuLzRL5z7D9Ar7Rt2ueQ5Vfj4oR24qoAATILnsn8JuLwwoC8N9VKejveSswoA
HQBULwbgSqfZxw9cZX08bV1X5021jelAU58VS6Bx9hoh49pwBiFYFIEFd3mqgnkC
AwEAAaNCMEAwHQYDVROBBYEFOLJQJ9NzuiaoXzPDj9lxSmIahlRMA8GA1UdEwEB
/wQFMAMBAf8wDgYDVR0PAQH/BAQDAggGMA0GCSqGSIb3DQEBwUAA4ICAQDRSVfg
p8xoWLoBDysZzY2wYUWsEeljUGn4H3++Fo/9nesLqjJHdtJnJO29fDMylrHBYZm
DR9FBUb1Ov9H5r2XpdptxolpAqzkT9fnqyL7FeoPueBihhXOYV0GkLH6VsTX4/5
COMsdI31R9Kr09b7eGZONn356ZLpBN79SWP8bfsUcZnNl0dKt7n/HipzcEYwv1ry
L3ml4Y0M2fmyYzeMN2WFcGpcWwlyualjPLhd+PwyvzeG5LuOmCd+uh8W4XAR8gPf
JWIyJyYMoSf/wA6E7qaTfRPuBRwIrhKK5DOKcFw9C+df/KQhtZa37dG/OaG+svg
IHZ6uqbL9XzeYqWxi+7egmaKTjowHz+Ay60nugxel9CxVsp3cbK1daFQqUBDF8Io
2c9S1lvIY9RCPqAzekYu9wogRlR+ak8x8YF+QnQ4ZXMn7sZ8uI7XpTrXmKGcjBBV
09tL7ECQ8sluV9JiDnxXk7Gnbc2dg7sq5+W2O3FYrf3RRbxake5TFW/TRQ11brqQ
XR4EzZffHqhmsYzmIGrv/EhOdJhCrylvLmrH+33RZjEizIYAfmaDDEL0vTSSwxrQ
T8p+ck0LcIymSLumoRT2+1hEmRSugguTaaApJUqlyyvdimYHFngVvV3Eb7PVHhPoe
MTd6lX8kreS8/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_R
28 NTgxMy5jboIUdGVzdHdlYjIuOTUxMDU4MTMuY24wDQYJKoZIhvcNAQELBQADggEB
29 AHoyjJizxZ687omFRgdBZfC+SjLnu6d1BWe5c9qojEWFVz4x0653EagSXbsNe6mx
30 kKIghEC1WK0x3b25bxbQ8YsXAUw8owYB9FLHN/pP15Y9EddpupNn5bcsKgCGVtDV
31 eePK4ht5IpbNqQRoMh6HyVoIO/kiwmg3YSaMk4tWKjapbUU34ASTAjyXLIBu/V8G
32 7LJoFEJzOrKSyh4X3SZCcys0h2kX6FvxD8iN7J+HXKjjLWQJ975ox3jhLi+nUy/F
33 x87U9gTSueriI45c2yPGOFowhI61sNn293...
34 OvjkY+kubBgU01tMI70+ATI=
35 -----END CERTIFICATE-----
36
37 -----BEGIN CERTIFICATE-----
38 MIIFF3TCCASWgAwIBAgIINY+ChlzmLbEwDQYJKoZIhvcNAQELBQAwYjELMAkGA1UE
39 BhMCQ04xMjAwBgNVBAoAMKUDVQU5HIERPTkcgQ0VSVE1GSUNBVEUgQVVVUSE9SSVRZ
40 IENPLixMVEQumR8wHQYDVQQDBBZHRENBIFRydXNOQVVUSCBSNSBST09UMB4XDTE0
41 MTEyNjA5NDUyNVoXDTMwMTIzMDUyMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEw
42 BAoMKUDVQU5HIERPTkcgQ0VSVE1GSUNBVEUgQVVVUSE9SSVRZ IENPLixMVEQumR8w
43 MwYDVQQDDCkxHRENBIFRydXNOQVVUSCBSNSCBFeHRlbmRlZCBWYXpZGF0aW9uIFNT
44 TCBDQTCASiDQYJKoZIhvcNAQELBQADggEAPADCCAQoCggEBAMcA1HwmgR2biKZ0
45 a46keXyOruAorQZx779CY9Yq7kUDwW4nPdiTKKlk/xkIJJwA6xzJomrCuMzr15
46 J17LviwOIQW6DBSSOKjR6VoPS2kkVHLiGd7n6mpJU22Evjo6gP/NC5maYchb0soH
47 TA05Yt58qA9qsMpDq9fS/AzYKAVWXBmWXh4x1BOXmGUpjYv3NXAtEznScauk9mgi
48 NzMMyu09iDq8G7c1q5oFd5auRKnBAk1BxvgkdoSjg8w2Q2wem0cbbGgfU8QGAY/+
49 o/wopiGvmcL+p7b7bgYUaxI9H1mrFhB5ScNK+cEFB8kkW7K/0PpXBd41RHHWTLkE
50 Z9ieC4ECAwEAaOCAX8wggF7MIGFBggrBgEFBQcBAQDCEU...
51 Nmh0dHA6Ly93d3cuZ2R2RjYS5jb20uY24vY2Y2VydC9HRENBx1RydXNOQVVVSE9SNV9S
52 T09ULmRlCjAxBggrBgEFBQcwAYY1aHR0cDovL3d3dy5nZGNhLmLmVnbS5jb20uY24v
53 dEFVVEgub2NzcDAdBgNVHQ4EFgQUHmrq3vUvv6jTbMfGP9tsZGDC40EwDwYDVR0T
54 AQH/BAUwAwEB/zAfBgNVHSMGDAWgBTiYUCfTc7omqF8zw4/ZcUpiGoZUTBIBgNV
55 HSAEQTA/MD0GCiqBHIbvLwEBBgEwLzAtBggrBgEFBQcCARYnaHR0cDovL3d3dy5n
56 ZGNhLmLmVnbS5jb20uY24vY2Y2VydC9HRENBx1RydXNOQVVVSE9SNV9S
57 d3cuZ2R2RjYS5jb20uY24vY2Y2VydC9HRENBx1RydXNOQVVVSE9SNV9S
58 A1UdDwEB/wQEAwIBhjANBgkqhkiG9w0BAQsFAAOCAgEAJ+QTFR1oac6P1jrKm58L
59 gIDckwkyREfAj+QTnDTONNMiapn6mZeuSLHhbZB1oyetddd1OMM8iJyU+ktJIHY
60 mlM3opIt3IuTWBbJobyDZYD+doed6H7gLcpOM1lbDVraXPVCNRTVM70Ifved9oB3
61 E8BisBTAkv/MPo1tFWBDWK2NV8jHItE650zOMXI+sF9EK0oQwzBBhx3vG1WpeMdy
62 Hpu7z7xdZdYb0MT8Iub+iPh4vVMshXLKohejXByEpWEyVr+L8dEomdaZzSku/VQm
63 ZQyDfNzrHfUm2hH/XhC61lNMA8/oeW99J/yfc/TNiCpImqHk0XBNeZeqK2HPBKj39
64 oMGOq5/kMT43jvTpjvjIX3tNnd+nrxLcS48IogZ/X2qyGGh7FHkntLC2DBj/ipmHh
65 4CJt/dxAX0DH/Z/rwhGVciR3zAXaLbZ1tIS+AhUVmcwIrxJc1ki6gU2dcUckj05M
66 1VFTjyRwXpK7aE1kJpdmL7fcBmUWsJKnzV6H5YETONK2YXSxDjDqrUn1S67qbIB
67 XAYQnEc/MYoispbeyRkSvciKV1D1Dehl/gGQQ80nCwsxj7gUTewVWgON3h/HP/+z
68 W8fh7J1c5YfbjS5zWLOGEEAomWosc0Ba1KHxVR+1yVfn/yxGYpKd4tA+7vRc3GWd
69 blVRfCZEmVBCWTd0BC5ZGxM=
70 -----END CERTIFICATE-----
71
72 -----BEGIN CERTIFICATE-----
73 MIIFFiDCCA3CgAwIBAgIIfQmX/vBH6nowDQYJKoZIhvcNAQELBQAwYjELMAkGA1UE
74 BhMCQ04xMjAwBgNVBAoAMKUDVQU5HIERPTkcgQ0VSVE1GSUNBVEUgQVVVUSE9SSVRZ
75 IENPLixMVEQumR8wHQYDVQQDBBZHRENBIFRydXNOQVVUSCBSNSBST09UMB4XDTE0
76 MTEyNjA5NDUyNVoXDTMwMTIzMDUyMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEw
77 BAoMKUDVQU5HIERPTkcgQ0VSVE1GSUNBVEUgQVVVUSE9SSVRZ IENPLixMVEQumR8w
```

服务器证书

ca证书

根证书

## 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，找到

```
#LoadModule ahssl_module modules/mod_ssl.so

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

删除行首的配置语句注释符号“#”。

如果在行 Include conf httpd-ssl.conf 前后有“Include conf httpd-ahssl.conf”这一项，将其注释掉



```
18 #
19 <IfModule ssl_module>
20 Include conf/extra/httpd-ssl.conf
21 #Include conf/extra/httpd-ahssl.conf
22 SSLRandomSeed startup builtin
23 SSLRandomSeed connect builtin
```

保存退出。

打开 apache 安装目录下 conf/extra 目录中的 httpd\_ssl.conf 文件编辑 Apache24\conf\extra\ 目录下的 httpd-ssl.conf 文件将 "ServerName [www.example.com:443](http://www.example.com:443)" 改成您的主机域名：如

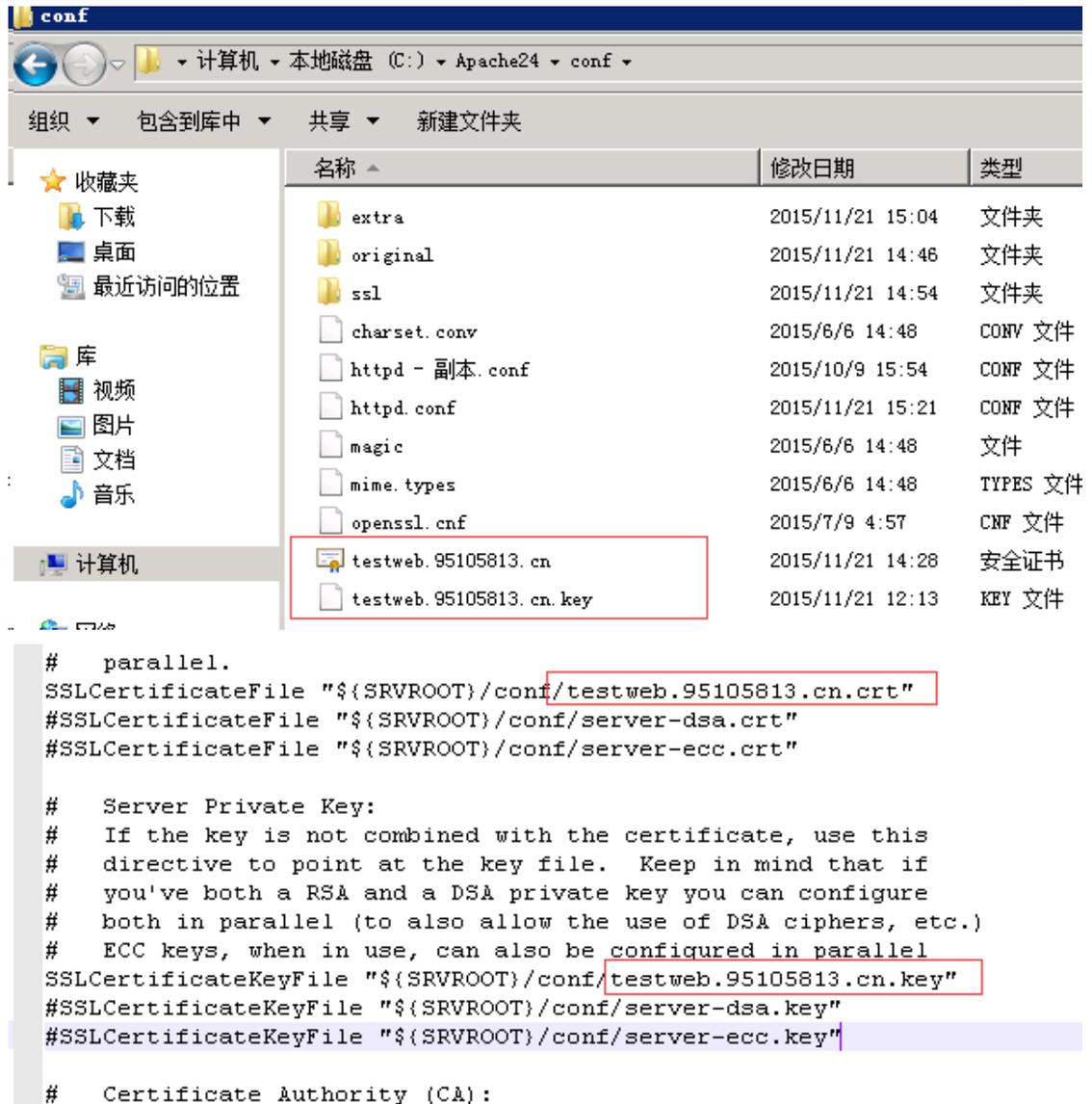
```
65 # General setup for the virtual host
66 DocumentRoot "${SRVROOT}/htdocs"
67 ServerName testweb.95105813.cn:443
68 ServerAdmin admin@example.com
69 ErrorLog "${SRVROOT}/logs/error.log"
70 TransferLog "${SRVROOT}/logs/access.log"
71
72 # SSL Engine Switch.
```

找到 SSLCertificateFile 和 SSLCertificateKeyFile 这两个配置项，将 testweb.95105813.cn.crt 和 testweb.95105813.cn.key 放到该目录下：

```
1 # require an ECC certificate which can also be configured
2 # parallel.
3 SSLCertificateFile "${SRVROOT}/conf/server.crt"
4 #SSLCertificateFile "${SRVROOT}/conf/server-dsa.crt"
5 #SSLCertificateFile "${SRVROOT}/conf/server-ecc.crt"
6
7 # Server Private Key:
8 # If the key is not combined with the certificate, use thi
9 # directive to point at the key file. Keep in mind that i
10 # you've both a RSA and a DSA private key you can configur
11 # both in parallel (to also allow the use of DSA ciphers,
12 # ECC keys, when in use, can also be configured in paralle
13 SSLCertificateKeyFile "${SRVROOT}/conf/server.key"
14 #SSLCertificateKeyFile "${SRVROOT}/conf/server-dsa.key"
15 #SSLCertificateKeyFile "${SRVROOT}/conf/server-ecc.key"
```

例：





名称	修改日期	类型
extra	2015/11/21 15:04	文件夹
original	2015/11/21 14:46	文件夹
ssl	2015/11/21 14:54	文件夹
charset.conv	2015/6/6 14:48	CONF 文件
httpd - 副本.conf	2015/10/9 15:54	CONF 文件
httpd.conf	2015/11/21 15:21	CONF 文件
magic	2015/6/6 14:48	文件
mime.types	2015/6/6 14:48	TYPES 文件
openssl.cnf	2015/7/9 4:57	CNF 文件
testweb.95105813.cn	2015/11/21 14:28	安全证书
testweb.95105813.cn.key	2015/11/21 12:13	KEY 文件

```
# parallel.  
SSLCertificateFile "${SRVROOT}/conf/testweb.95105813.cn.crt"  
#SSLCertificateFile "${SRVROOT}/conf/server-dsa.crt"  
#SSLCertificateFile "${SRVROOT}/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 "${SRVROOT}/conf/testweb.95105813.cn.key"  
#SSLCertificateKeyFile "${SRVROOT}/conf/server-dsa.key"  
#SSLCertificateKeyFile "${SRVROOT}/conf/server-ecc.key"  
  
# Certificate Authority (CA):
```

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“四、安装服务器证书”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。

