



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 linux 版本

2015/11/23

## 目录

一、部署前特别说明.....	2
二、安装 apache 2.4.....	2
1. openssl 环境.....	2
2. 安装依赖环境.....	2
3. 编译安装 apache.....	3
三、生成证书请求.....	3
1. 安装 OpenSSL 工具.....	3
2. 生成服务器证书私钥.....	4
3. 生成服务器证书请求（CSR）文件.....	5
4. 提交证书请求.....	7
四、服务器证书的导入.....	7
1. 获取服务器证书的根证书和 CA 证书.....	7
1.1 从邮件中获取.....	7
1.2 从 GDCA 官网上下载：.....	9
1.3 转换证书编码.....	10
2. 导入根证书和 CA 证书到服务器证书.....	14
五、安装服务器证书.....	15
六、备份和恢复.....	16
1. 备份服务器证书.....	16
2. 恢复服务器证书.....	16
七、证书遗失处理.....	16



## 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 linux 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. 本部署指南提供参考的 apache 2.4 服务器部署方式。如果您的服务器已部署好 apache 服务您可以继续使用原来的服务在其基础上完成服务器证书的安装配置, 并不要求重新进行安装;
7. 您可以按照自己的方式部署 apache2.4 并不要求必须按照本部署指南的方式安装。
8. 如用户已经生成证书请求文件, 请从第四点服务器证书的导入开始阅读。

## 二、安装 apache 2.4

### 1.openssl 环境

使用操作系统自带的 openssl 版本

### 2.安装依赖环境

下载 apr-1.5.2

wget <http://mirrors.cnnic.cn/apache//apr/apr-1.5.2.tar.gz>

安装 apr-1.5.2



```
tar zxvf apr-1.5.2.tar.gz
cd apr-1.5.2
./configure --prefix=/usr/local/apr
make &&make install
```

下载 apr-util-1.5.4

```
wget http://mirrors.hust.edu.cn/apache//apr/apr-util-1.5.4.tar.gz
安装 apr-util-1.5.4
tar zxvf apr-util-1.5.4.tar.gz
cd apr-util-1.5.4
./configure --prefix=/usr/local/apr-util --with-apr=/usr/local/apr
```

### 3. 编译安装 apache

下载 apache

```
wget http://mirrors.cnnic.cn/apache//httpd/httpd-2.4.17.tar.gz
```

安装 apache

```
tar zxvf httpd-2.4.17.tar.gz
```

```
cd httpd-2.4.17
```

```
./configure --prefix=/usr/local/apache24 --with-apr=/usr/local/apr
```

```
--with-apr-util=/usr/local/apr-util --enable-so --enable-ssl --enable-modules=most
```

```
# enable-ssl 添加 ssl 模块
```

```
make && make install
```

Apache 将被安装到/usr/local/apache

## 三、生成证书请求

### 1. 安装 OpenSSL 工具

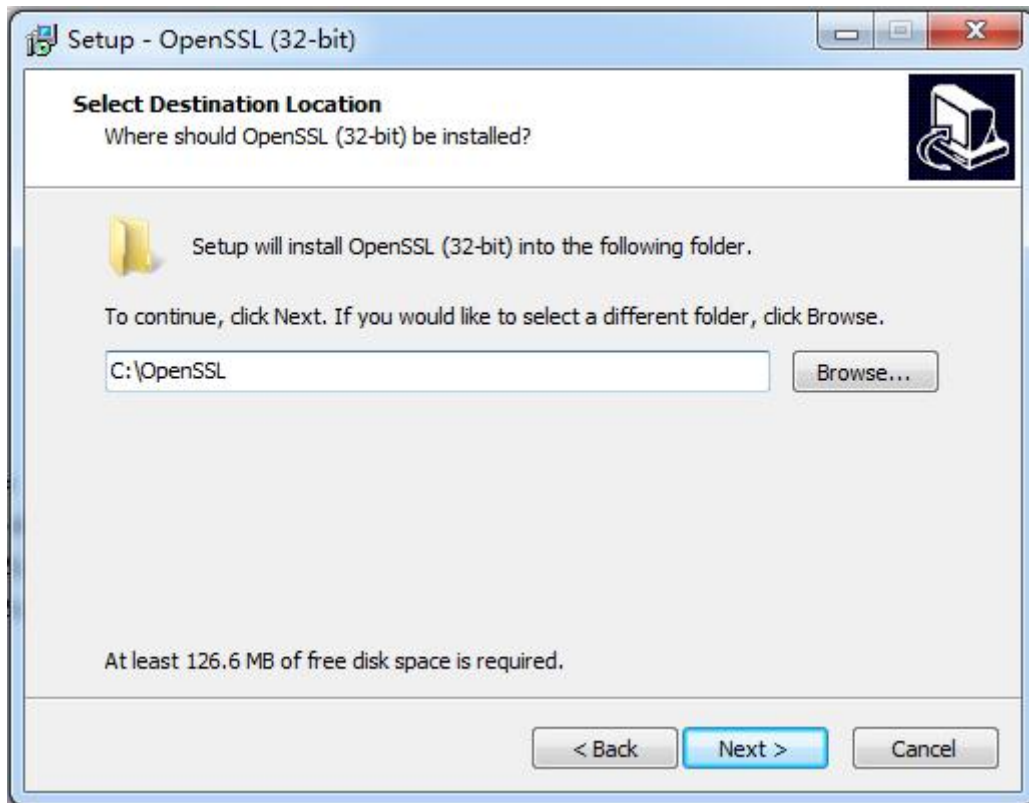
您需要使用 openssl 工具来创建证书请求。下载 OpenSSL：

地址：广州市东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：[www.gdca.com.cn](http://www.gdca.com.cn)

电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813



<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

## 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:\> 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

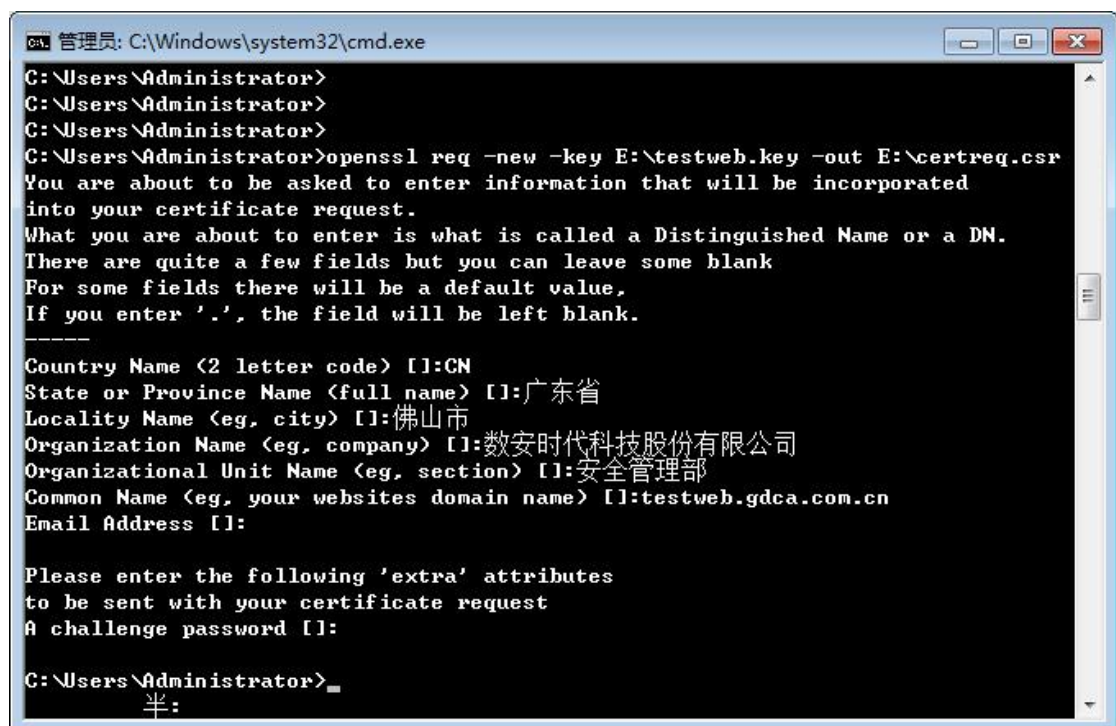
7. Email Address:

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。

例：



```
ca. 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。

## 四、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

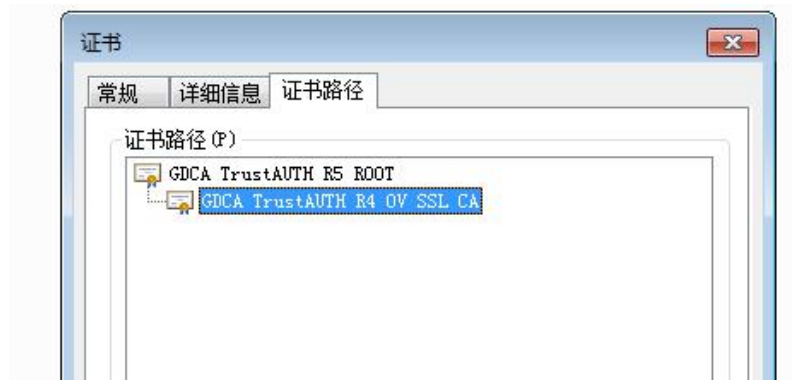
在您完成申请 GDCA 服务器证书的流程后, GDCA 将会在返回给您的邮件中附上服务器证书以及根证书 GDCA\_TrustAUTH\_R5\_ROOT.cer 和相应的 CA 证书。如果您申请的是睿信(OV) SSL 证书 (Organization Validation SSL Certificate), CA 证书就是文件就是 GDCA\_TrustAUTH\_R4\_OV\_SSL\_CA.cer; 如果您申请的是恒信企业 EV SSL 证书 (Extended Validation SSL Certificate), CA 证书就是文件就是 GDCA\_TrustAUTH\_R4\_EV\_SSL\_CA.cer, 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)



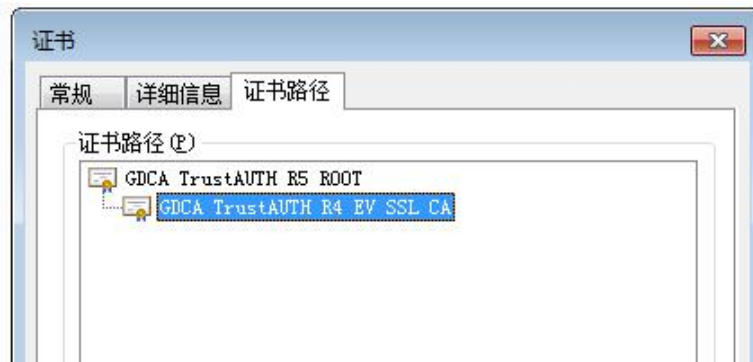




GDCA\_TrustAUTH\_R4\_OV\_SSL\_CA.cer:

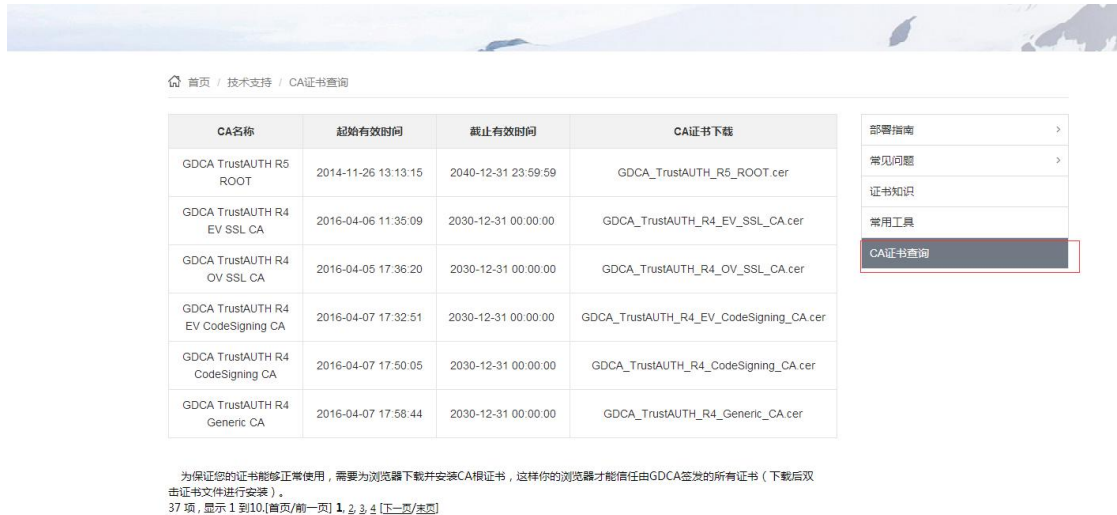


GDCA\_TrustAUTH\_R4\_EV\_SSL\_CA.cer:



## 1.2 从 GDCA 官网上下载:

[https://www.trustauth.cn/support/ca\\_cq/](https://www.trustauth.cn/support/ca_cq/)



CA名称	起始有效时间	截止有效时间	CA证书下载
GDCA TrustAUTH R5 ROOT	2014-11-26 13:13:15	2040-12-31 23:59:59	GDCA_TrustAUTH_R5_ROOT.cer
GDCA TrustAUTH R4 EV SSL CA	2016-04-06 11:35:09	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_EV_SSL_CA.cer
GDCA TrustAUTH R4 OV SSL CA	2016-04-05 17:36:20	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_OV_SSL_CA.cer
GDCA TrustAUTH R4 EV CodeSigning CA	2016-04-07 17:32:51	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_EV_CodeSigning_CA.cer
GDCA TrustAUTH R4 CodeSigning CA	2016-04-07 17:50:05	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_CodeSigning_CA.cer
GDCA TrustAUTH R4 Generic CA	2016-04-07 17:58:44	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_Generic_CA.cer

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）。

37 项，显示 1 到 10 { 首页/前一页 } 1, 2, 3, 4 [ 下一页/末页 ]

获取根证书: GDCA\_TrustAUTH\_R5\_ROOT.cer:

CA名称	起始有效时间	截止有效时间	CA证书下载
GDCA TrustAUTH R5 ROOT	2014-11-26 13:13:15	2040-12-31 23:59:59	GDCA_TrustAUTH_R5_ROOT.cer
GDCA TrustAUTH R4 EV SSL CA	2016-04-06 11:35:09	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_EV_SSL_CA.cer
GDCA TrustAUTH R4 OV SSL CA	2016-04-05 17:36:20	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_OV_SSL_CA.cer
GDCA TrustAUTH R4 EV CodeSigning CA	2016-04-07 17:32:51	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_EV_CodeSigning_CA.cer
GDCA TrustAUTH R4 CodeSigning CA	2016-04-07 17:50:05	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_CodeSigning_CA.cer
GDCA TrustAUTH R4 Generic CA	2016-04-07 17:58:44	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_Generic_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 Certificate), 下载 GDCA\_TrustAuth\_R4\_OV\_SSL\_CA.cer



CA名称	起始有效时间	截止有效时间	CA证书下载
GDCA TrustAUTH R5 ROOT	2014-11-26 13:13:15	2040-12-31 23:59:59	GDCA_TrustAUTH_R5_ROOT.cer
GDCA TrustAUTH R4 EV SSL CA	2016-04-06 11:35:09	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_EV_SSL_CA.cer
GDCA TrustAUTH R4 OV SSL CA	2016-04-05 17:36:20	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_OV_SSL_CA.cer
GDCA TrustAUTH R4 EV CodeSigning CA	2016-04-07 17:32:51	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_EV_CodeSigning_CA.cer
GDCA TrustAUTH R4 CodeSigning CA	2016-04-07 17:50:05	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_CodeSigning_CA.cer
GDCA TrustAUTH R4 Generic CA	2016-04-07 17:58:44	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_Generic_CA.cer

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，这样你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）。

37 项, 显示 1 到10.[[首页/前一页](#)] [1](#), [2](#), [3](#), [4](#) [[下一页/末页](#)]

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

CA名称	起始有效时间	截止有效时间	CA证书下载
GDCA TrustAUTH R5 ROOT	2014-11-26 13:13:15	2040-12-31 23:59:59	GDCA_TrustAUTH_R5_ROOT.cer
GDCA TrustAUTH R4 EV SSL CA	2016-04-06 11:35:09	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_EV_SSL_CA.cer
GDCA TrustAUTH R4 OV SSL CA	2016-04-05 17:36:20	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_OV_SSL_CA.cer
GDCA TrustAUTH R4 EV CodeSigning CA	2016-04-07 17:32:51	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_EV_CodeSigning_CA.cer
GDCA TrustAUTH R4 CodeSigning CA	2016-04-07 17:50:05	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_CodeSigning_CA.cer
GDCA TrustAUTH R4 Generic CA	2016-04-07 17:58:44	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_Generic_CA.cer

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，这样你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）。

37 项, 显示 1 到10.[[首页/前一页](#)] [1](#), [2](#), [3](#), [4](#) [[下一页/末页](#)]

### 1.3 转换证书编码

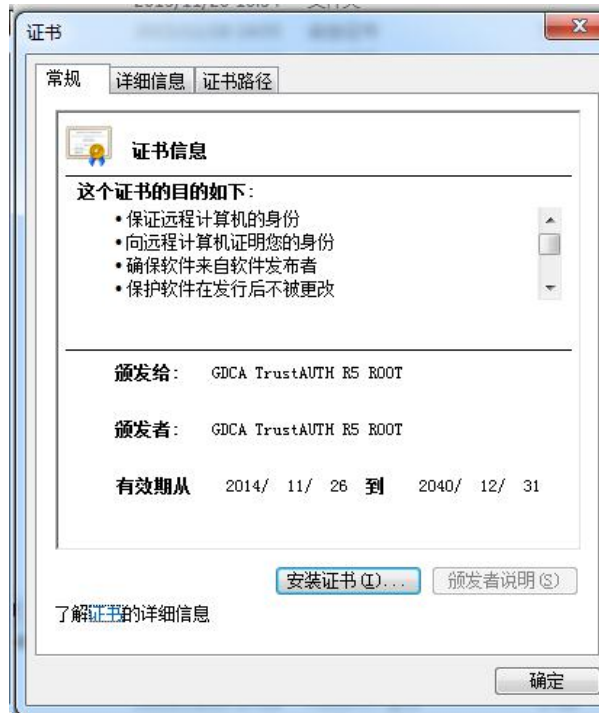
从官网上下载的证书需要先转换为 Base64 编码。以根证书为例：

打开证书：

地址：广州市东风中路 448 号成悦大厦第 23 楼 邮编：510030 网址：[www.gdca.com.cn](http://www.gdca.com.cn)

电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813



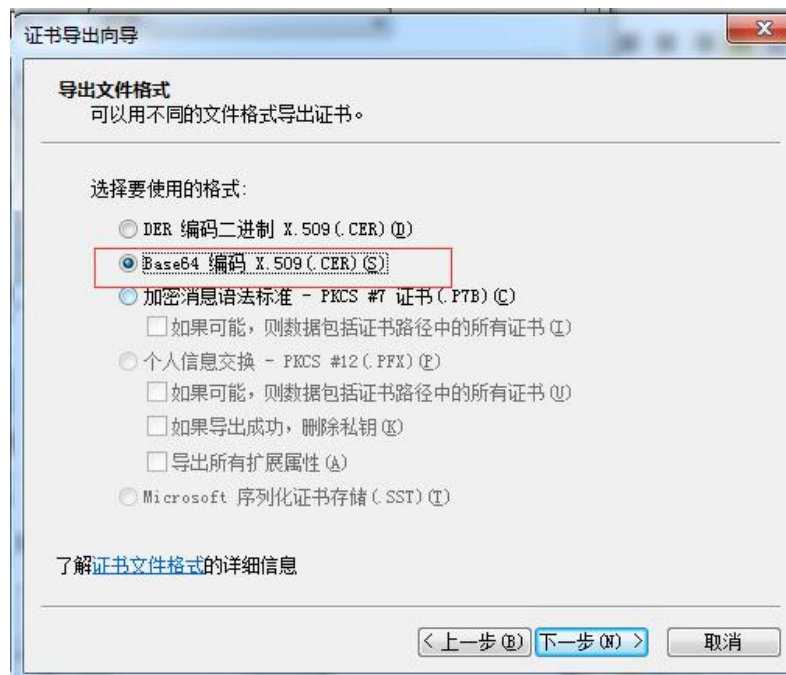


详细信息-复制到文件



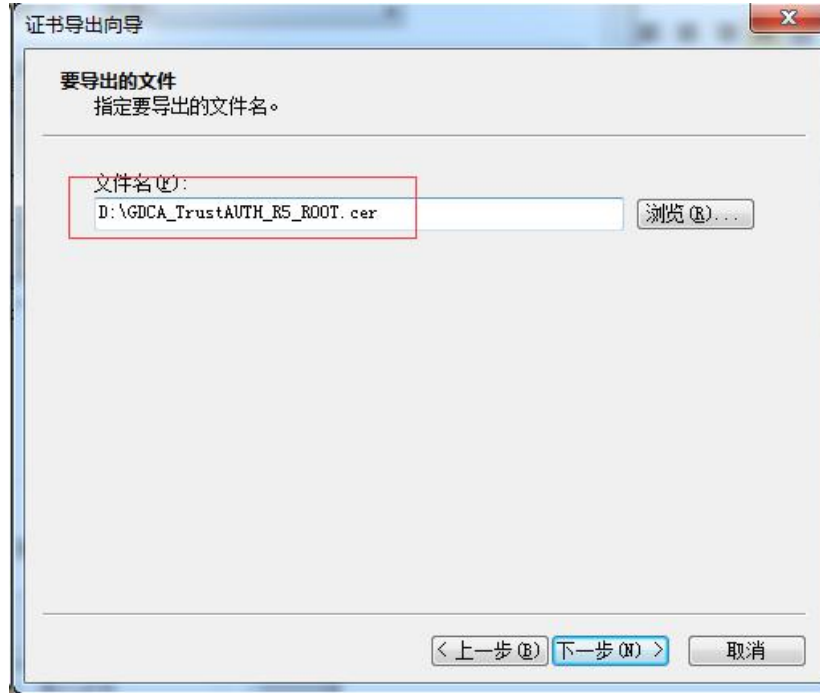
在证书导出向导里，将证书编码改成 Base64 编码格式





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-----
MIIFiDCCA3CgAwIBAgITfQmX/vBH6nowDQYJKoZIhvcNAQELBQAwYjELMAkGA1UE
BhMCQ04xMjAwBgNVBAAoMKUdVQU5HIERPTkcgQ0VSVElGSUNBVEUgQVVVUSE9SSVRZ
IENPLixMVEQuMR8wHQYDQDDBZHRENBIFRydXN0QVVUSCBSNSBST09UMB4XDTE0
MTEyNjA1MTMxNV0XDTQwMTIzMTk1NTk1OVowYjELMAkGA1UEBhMCQ04xMjAwBgNV
BAoMKUdVQU5HIERPTkcgQ0VSVElGSUNBVEUgQVVVUSE9SSVRZIENPLixMVEQuMR8w
HQYDQDDBZHRENBIFRydXN0QVVUSCBSNSBST09UMIICiANBgkqhkiG9w0BAQEF
AAOCAg8AMIICgKCAgEA2aMw8Mh0dHeb7zMN0wZ+Vfy1YI92hhJCFvZmPoiC7XJj
Dp6L3TQsAlFRwxn9WVSEyFrs0yw6ehGXTjGoqcuEVe6ghWinI9tsJLKVCvLriXBj
TnnEtlu9o12x8kEck62pOqPseQrsXzrj/e+APK00mxqriCZ7VqKChh/rNYmDf1+u
KU49tm7srsHwJ5uu4/Ts765/94Y9cncrrpftZTqfrylYwiOXnhLQiPzLyRuEH3FMEj
qcOtmkVes7LXLM3GKeJQEK5cy4KOFxg2fzfmiJqwTTQJ9Cy5WmYqsBebnh52nUpm
MUHfP/vFBu8btn4aRjb3ZGM74zkYI+dndRTVdVeSN72+ahsmUPI2JgaQxXABZG12
ZuGR224HwGGALrIuL4xwp9E7PLOR5G62xDtw8mySlwnNR30YwPO7ng/Wi64HtloP
zgsMR6f1Pri9fcebNaBhlzpbDrfMK5Z3KpIhHtmVdiBnaM8Nvd/WHwlqmuLmc3Gk
L30SgLDtMEZeS1SZD2fJpcjYIMGC7J0R38IC+xo70e0gmu9lZJIQDSri3nDxGGcJ
gHeuLzRL5z7D9Ar7Rt2ueQ5Vfj4oR24qoAATILnsn8JuLwwoC8N9VKejveswoA
HQBULwbgS9fZxw9cZX08bVlX5021je1AU58VS6Bx9hoh49pwBiFYFIEFd3mqgnkC
AwEAAANcMEAwHQYDVR0OBBYEFOLJQJ9NzuiacXzPDj91xSmIahlRMA8GA1UdEwEB
/wQFMAMBAf8wDgYDVR0PAQH/BAQDAggGMA0GCSqGSIb3DQEBCwUAA4ICAQRDRSVfz
p8xoWLoBDysZzY2wYUWsEeljUGn4H3++Fo/9nesLqjJHdtJnJO29fDMylyrHBYZm
DRd9FBub1Ov9H5r2XpdptxolpAqzkT9fNqyL7FeoPueBihhXOYV0GkLH6VstX4/5
C0mSdI31R9Kr09b7eGZONn356ZLpBN79SWP8bfsUcZnNl0dKt7n/HipzceYwv1ry
L3ml4Y0M2fmyYzeMN2WfCgpcWwlyua1jPLHd+PwyvzeG5LuOmCd+uh8W4XAR8gPf
JWIYjYyYMoSf/wA6E7qaTfRPuBRWIrHKK5DOKcFw9C+df/KQhtZa37dG/OaG+svg
IHZ6uqbL9XzeYqWxi+7egmaKTjowHz+Ay60nugxel9CvSp3cbK1daFQqUBDF8Io
2c9S1lvIY9RCPqAzekYu9wogRlR+ak8x8YF+QnQ4ZXmN7sZ8uI7XpTrXmKgcjBBV
09tL7ECQ8sluV9JiDnxXk7Gnbc2dg7sq5+W2O3FYrf3RRbxake5TFW/TRQ11brqQ
XR4EzzffHqhmsYzmIGrv/EhOdJhCrylvLmrH+33RZjEizIYAfmaDDEL0vTSSwxrq
T8p+ck0LcIymSLumoRT2+lhEmRSugguTaaApJUqlyyvdimYHFngVV3Eb7PVHhPoe
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

```
28 NTgxMy5jboIUDGVzdHd1YjIuOTUxMDU0MTMuY24wDQYJKoZIhvcNAQELBQADggEB
29 AHoyjJizxZ687omFRgdBZfC+SjLnu6d1BWe5c9qojEWFVz4xO653EagSXbsNe6mx
30 kKIghEC1WK0x3b25bxbQ8YsXAuW8owYB9FLHN/pPl5Y9EddpupNn5bcsKgCGVtDV
31 eePK4ht5IpBNqQRoMh6HyVoIO/kiwmg3YSsMk4tWKjSpbUU34ASTAjXLiBu/V8G
32 7LJoFEJzOrK5yh4X3S2CcyS0h2kX6FvxD8iN7J+HXKjjlWQJ975cox3jhLi+nUy/F
33 x87U9gTSueriI45c2yPGOF0whI61sNNn293...
34 OvjkY+kubBgU01tMI70+ATI=
35 -----END CERTIFICATE-----
36
37 -----BEGIN CERTIFICATE-----
38 MIIF3TCCAs8wAwIBAgIINy+ChlzmLbEwDQYJKoZIhvcNAQELBQAwYjELMAkGA1UE
39 BhMCQ04xMjAwBgNVBAAoMKUdVQU5HIERPTkcgQ0VSVE1GSUNBEUgQVVU5E9SSVRZ
40 IENPLixMVEQuMR8wHQYDVQDDDBZHRENBIFRydXNOQVU5C3NSBSTO9UMB4XDTE0
41 MTEyNjA5NDUyNVoXDTMwMTIzMDU0MTU0MTU0MTU0MTU0MTU0MTU0MTU0MTU0MTU0
42 BAoMKUdVQU5HIERPTkcgQ0VSVE1GSUNBEUgQVVU5E9SSVRZ IENPLixMVEQuMTUw
43 MwYDVQDDDCxHRENBIFRydXNOQVU5C3NSC3BFeHRlbnRlZCBWYWxpZGF0aW9uIFNT
44 TCBDQ0VU5E9SSVRZ IENPLixMVEQuMTUwMTU0MTU0MTU0MTU0MTU0MTU0MTU0MTU0
45 a46bkeXyOruAorQ2x779CY9Yq7kUDw4nPdITXK1k/xkIJJuWA6xzJ0mrCuMzr15
46 J17LvwIOW6rDBSSOKjR6VoPS2kkVHLigD7n6mpJU22EvjoeGgP/NC5maYchbOsoH
47 TA05Yt58qA9qsMpDq9fS/AzYKAVWXEmWXh4x1BOXmGUpjYv3NXAtEznScauk9mgi
48 NzMMYu09iDq8G7c1q5oFd5auRKnBAk1BxvqkdoSjg8w2Q2wem0cbbGgfU8QGAy/+
49 o/wopiGvmcL+p7b7bgYUaxI9H1mrFhB5ScNK+cEFB8kkW7K/0PpXBd41RHHWTLkE
50 Z9ieC4ECAwEAaOCAX8wggF7MIGFBggrBgEFQ0cBAQ0EMU...
51 Nmhd0HA6Ly93d3cuZ2RjY5S5jb20uY24vY2VycC9HRENBX1RydXNOQVU5F9SNV9S
52 T09ULmRlcljAxBggrBgEFBQcwAYY1aHR0cDovL3d3dy5nZGNhLmNvbS5jbi9UcnVz
53 dEFVVEgvd2NzdDAdBgNVHQ4EFgQUHmrq3vUvv6jTbMfGP9tsZGdc40EwDwYDVR0T
54 AQH/BAUwAwEB/zAFBgNVHSMEGDAWgBTiYUCFtc7omqF8zw4/ZcUpiGoZUTBIBgNV
55 HSAEQTA/MD0GciqBHIbvLwEBBgEwLzAtBggrBgEFBQcCARYaHR0cDovL3d3dy5n
56 ZGNhLmNvbS5jbi9jcmVzYXZlY3BzMEYGA1UdHwQ/MD0wO6A5oDeGNW0dHA6Ly93
57 d3cuZ2RjY5S5jb20uY24vY3JsL0deQ0FfVHJ1c3RBVVVX11I1X1JPT1QuY3J3MA4G
58 A1UdWEB/wQEAwIBhJANBgkqhkiG9w0BAQsFAAOCAgEAJ+QTFR1oac6P1jrKms8L
59 gIdCkkybREfAj+QTnDTONMiapn6mZeuSLHhbZBl0yetddz10MM8iJyU+ktJIHY
60 mlM3opIt3IuTWBbJobyDZYD+doed6H7gLcp0M1lbDVraXPVCNRTVM70Tfved9oB3
61 E8BisBTAKV/MPo1tFWBDWK2NV8jHItE650zOMXI+sF9EK0oQwzBBhx3vG1WpeMdY
62 Hpu7z7xdZdYb0MT8Iub+iPh4vVMshXLKohejXByEpWEyVr+L8de0mdaZzSku/VQm
63 ZQyDfNrHfUm2h/HXc6I1NMA8/oeW99J/yfc/TNiCImgHkOKBNeZeqK2HPBKj39
64 oMGOq5/kMT43jvTpjvjIX3tNnd+nzLcs48IogZ/X2qyGGh7FHkntLC2DBj/ipmHh
65 4CJc/dxAX0DH/Z/rwhGVciR3zAXaLbZ1tIS+AhUVmewIrcJC1kI6gU2dcUCkjo5M
66 1VfTjyyzWxpK7aE1kJpdmL7fcBmUWsJKnzV6H5YETONK2YXsDjDqrUn1S67qbIB
67 XAYQnEc/MyoispeYRksVciKV1D1Dehl/gGQQ80nCwsxj7gUTewVWgON3h/HP/+z
68 W8fh7J1c5YfbjSSzWLOGEEAcmWosc0Ba1KHxVR+1yVfn/yxGYpKd4tA+7vRc3Gwd
69 b1VRFcZEmVBCWtd0BC5ZGxM=
70 -----END CERTIFICATE-----
71
72 -----BEGIN CERTIFICATE-----
73 MIIFiDCCA3CgAwIBAgIIfQmX/vBH6nowDQYJKoZIhvcNAQELBQAwYjELMAkGA1UE
74 BhMCQ04xMjAwBgNVBAAoMKUdVQU5HIERPTkcgQ0VSVE1GSUNBEUgQVVU5E9SSVRZ
75 IENPLixMVEQuMR8wHQYDVQDDDBZHRENBIFRydXNOQVU5C3NSBSTO9UMB4XDTE0
76 MTEyNjA5NDUyNVoXDTMwMTIzMDU0MTU0MTU0MTU0MTU0MTU0MTU0MTU0MTU0MTU0
77 BAoMKUdVQU5HIERPTkcgQ0VSVE1GSUNBEUgQVVU5E9SSVRZ IENPLixMVEQuMR8w
```

## 五、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

#LoadModule socache_shmcb_module modules/mod_socache_shmcb.so

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

删除行首的配置语句注释符号“#”。

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

```
# General setup for the virtual host
DocumentRoot "/usr/local/apache24/htdocs"
ServerName testweb.95105813.cn:443
ServerAdmin you@example.com
ErrorLog "/usr/local/apache24/logs/error_log"
TransferLog "/usr/local/apache24/logs/access_log"
```

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 (/usr/local/apache24/conf)：

```
...
# ciphers, etc.)
# Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)
# require an ECC certificate which can also be configured in
# parallel.
SSLCertificateFile "/usr/local/apache24/conf/testweb.95105813.cn.crt"
#SSLCertificateFile "/usr/local/apache24/conf/server-dsa.crt"
#SSLCertificateFile "/usr/local/apache24/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/apache24/conf/testweb.95105813.cn.key"
#SSLCertificateKeyFile "/usr/local/apache24/conf/server-dsa.key"
#SSLCertificateKeyFile "/usr/local/apache24/conf/server-ecc.key"
```

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。

## 六、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“五、安装服务器证书”即可完成恢复操作。

## 七、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。

