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 2.2 windows 版本

2015/11/23

目录

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

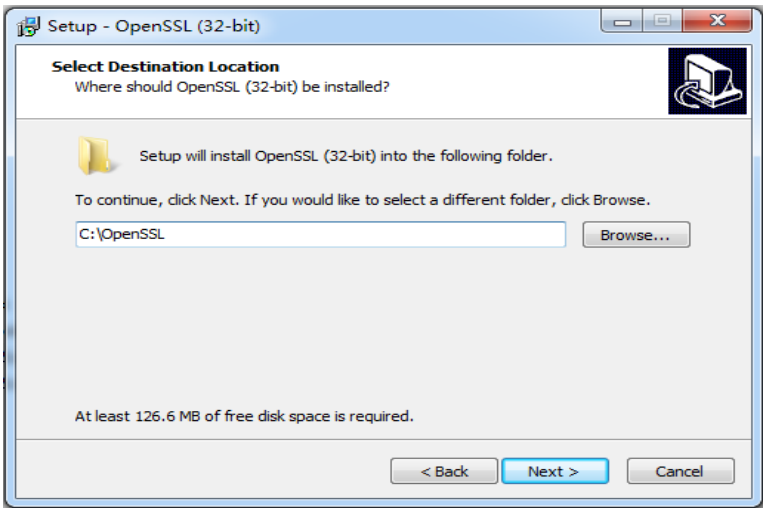
一、部署前特别说明

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 2.2 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

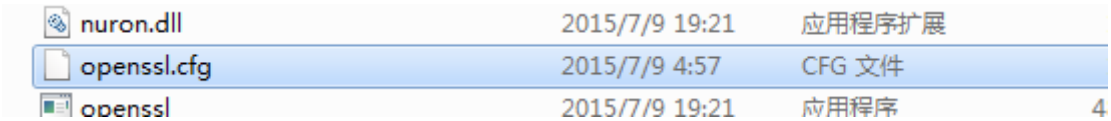
1. 安装 OpenSSL 工具

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



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

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

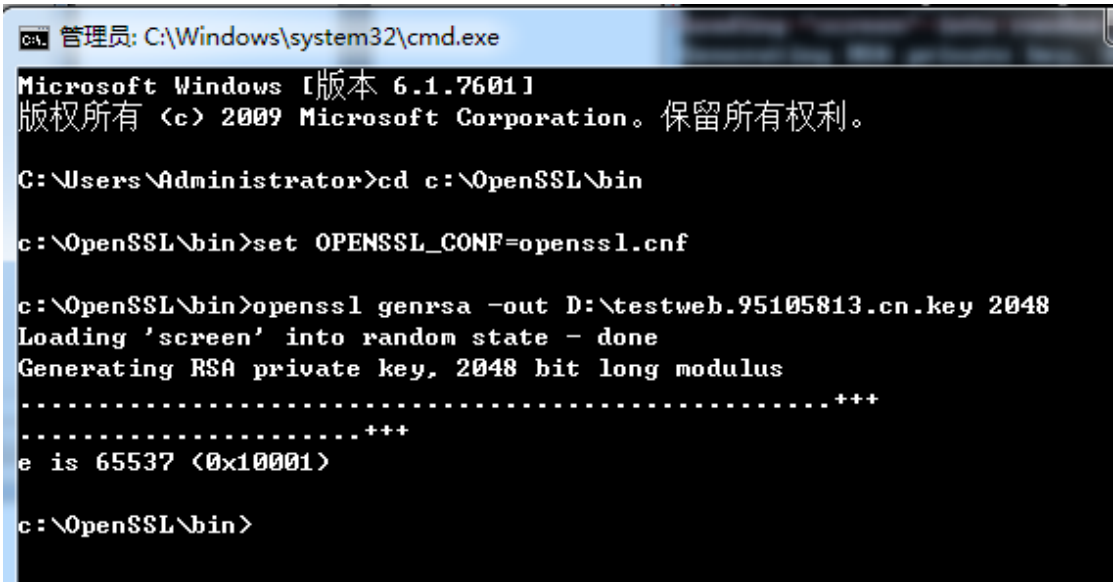
set OPENSSL_CONF=openssl.cnf

参考：

openssl genrsa -out server.key 2048

例：

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



3. 生成服务器证书请求（CSR）文件

参考：

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

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

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

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

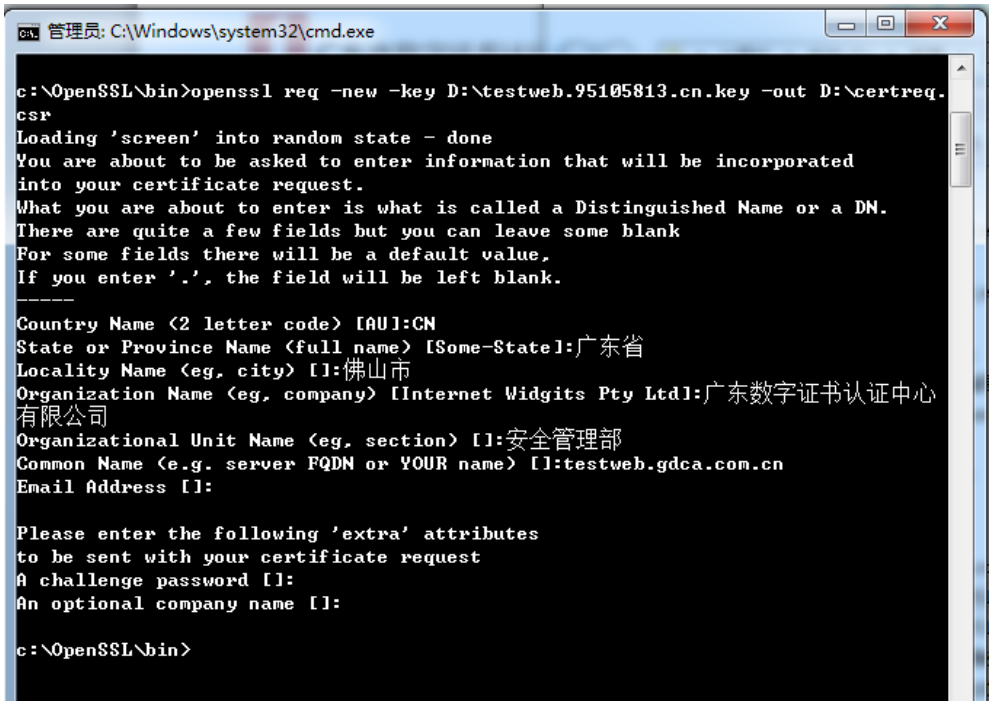
7.Email Address：

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。

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



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、服务器证书转码与 CA 证书链生成

1. 获取服务器证书的根证书和 CA 证书

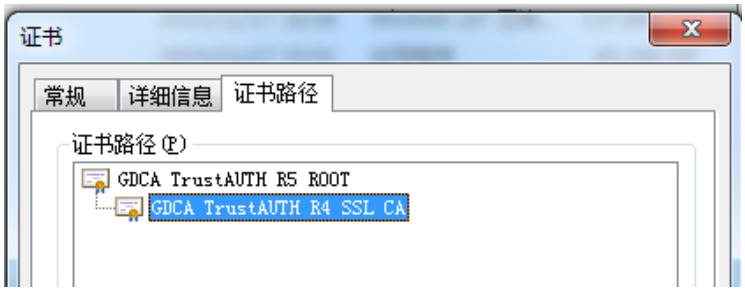
服务器证书需要安装根证书和 CA 证书,以确保证书在浏览器中的兼容性。有两种方式获取。

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

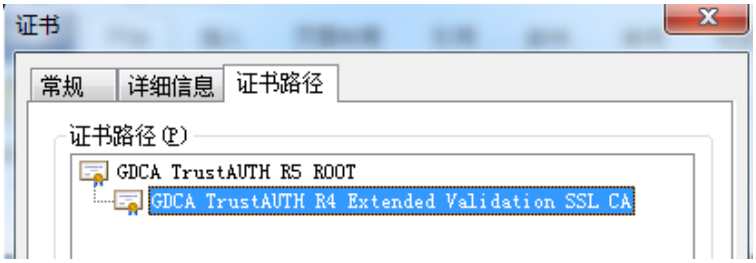
1.1 从邮件中获取

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

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

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）。

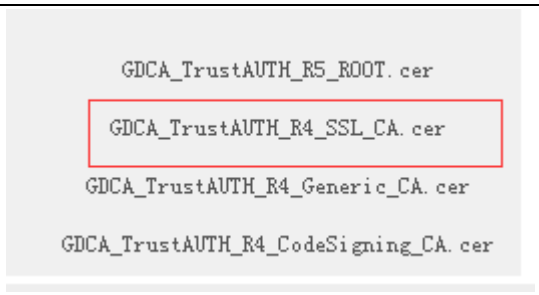
12 项 ， 显示 1 到10.[首页/前一页] 1, 2 [下一页/末页]

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 Certificate），下载 GDCA_TrustAuTH_R4_SSL_CA.cer

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

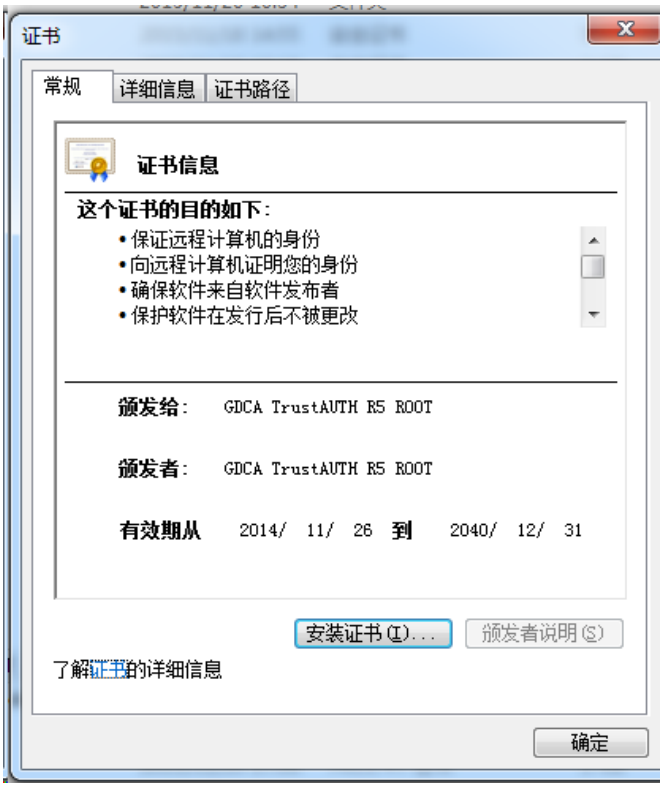


如果您申请的证书是恒信企业 EV SSL 证书（Extended Validation SSL Certificate），则下载 GDCA_TrustAUTH_R4_Extended_Validation_SSL_CA.cer

1.3 转换证书编码

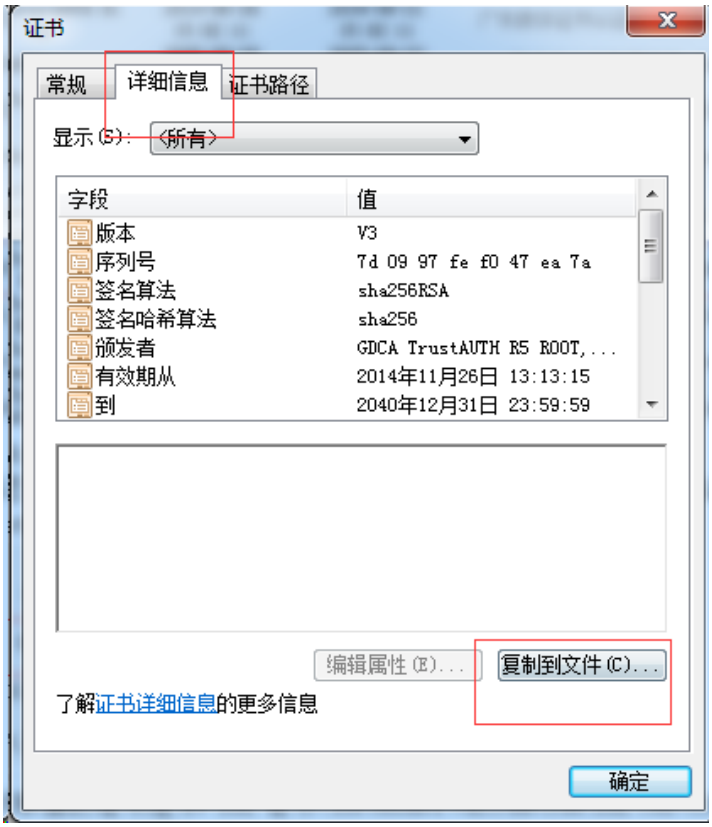
从官网上下载的证书需要先转换为 Base64 编码格式。以根证书为例：

打开证书：



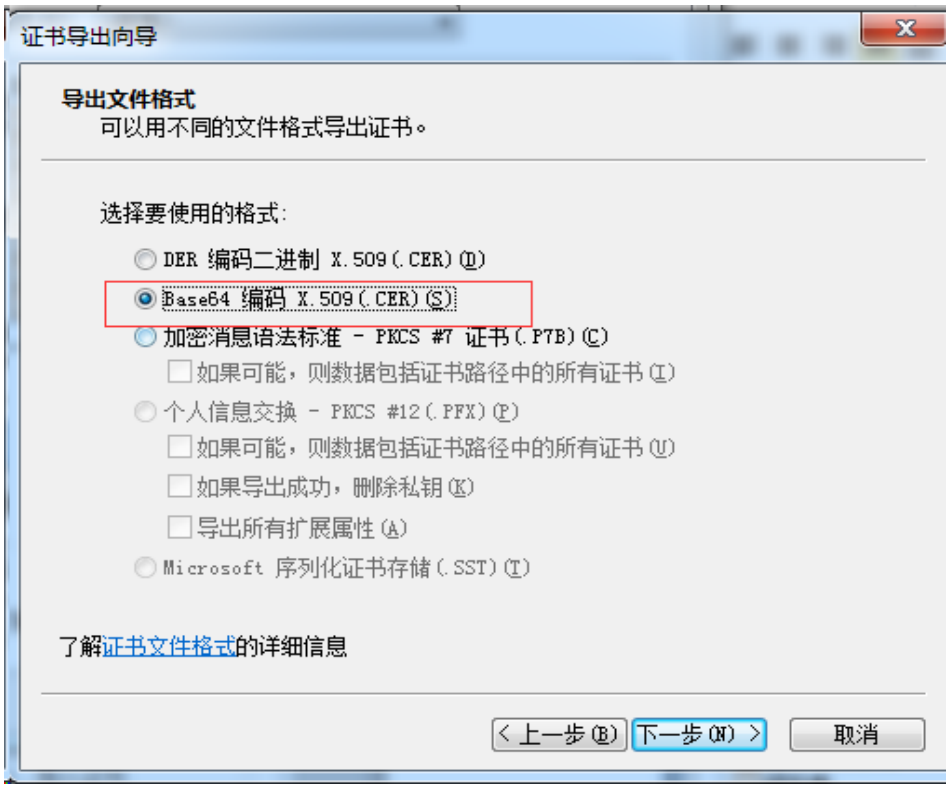
详细信息-复制到文件

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

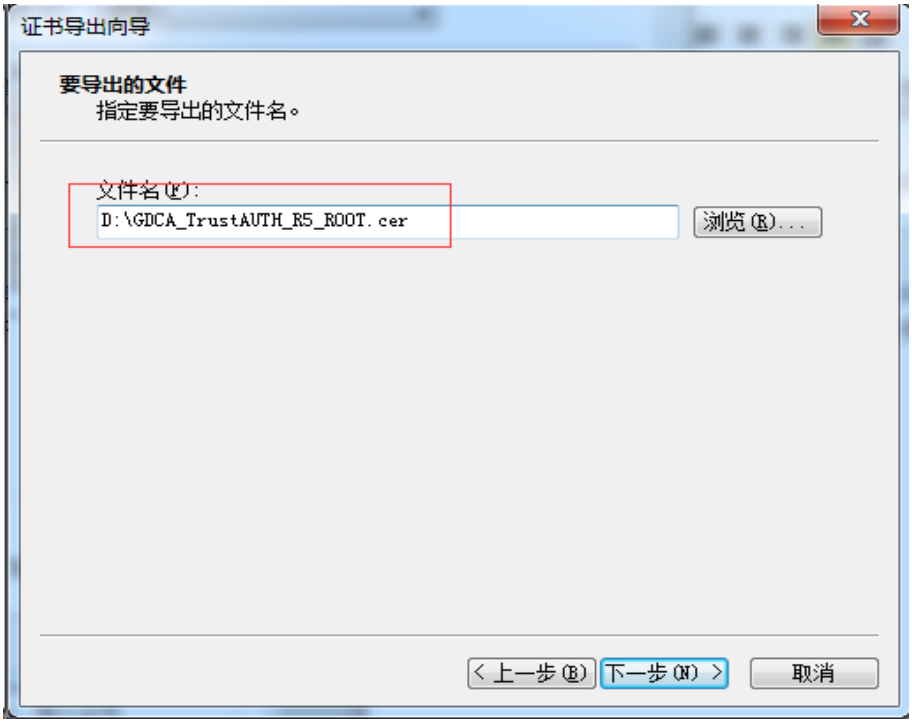


在证书导出向导里，将证书编码改成 Base64 编码

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



导出到指定目录里



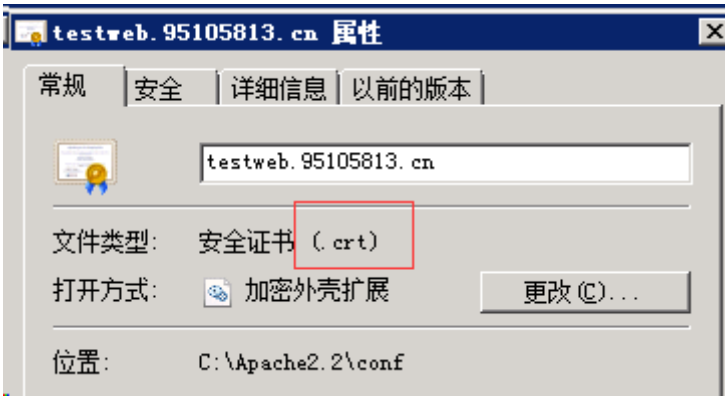
转换成 Base64 编码格式后，用编辑器打开，可以看到文件内容是以-----BEGIN CERTIFICATE-----开头，-----END CERTIFICATE-----结尾。以同样方式将 CA 证书也转换成 Base64 编码格式。

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

```
-----BEGIN CERTIFICATE-----
MIIFiDCCA3CgAwIBAgIIfQmX/vBH6nowDQYJKoZIhvcNAQELBQAwYjELMAkGA1UE
BhMCQ04xMjAwBgNVBAoMKUdVQU5HIERPTkcgQ0VSVElGSUNBVEUgQVVUSE9SSVRZ
IENPLixMVEQuMR8wHQYDVQQDDBZHRENBIFRydXN0QVVUSCBSNSBST09UMB4XDTE0
MTEyNjA1MTMxNVoXDTQwMTIzMTE1NTk1OVowYjELMAkGA1UEBhMCQ04xMjAwBgNV
BAoMKUdVQU5HIERPTkcgQ0VSVElGSUNBVEUgQVVUSE9SSVRZIENPLixMVEQuMR8w
HQYDVQQDDBZHRENBIFRydXN0QVVUSCBSNSBST09UMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEA2aMW8Mh0dHeb7zMNOwZ+Vfy1YI92hhJCfVZmPoiC7XJj
Dp6L3TQsAlFRwxn9WVSEyfFrs0yw6ehGXTjGoqcuEVe6ghWinI9tsJlKCvLriXBj
TnnEt1u9ol2x8kECK62pOqPseQrsXzrj/e+APK00mxqriCZ7VqKChh/rNYmDf1+u
KU49tm7srsHwJ5uu4/Ts765/94Y9cnrrpftZTqfrlYwiOXnhLQiPzLyRuEH3FMEj
qcOtmkVEs7LXLM3GKeJQEK5cy4KOFxg2fZfmiJqwTTQJ9Cy5WmYqsBebnh52nUpm
MUHfP/vFBu8btn4aRjb3ZGM74zkYI+dndRTVdVeSN72+ahsmUPI2JgaQxXABZG12
ZuGR224HwGGALrIuL4xwp9E7PLOR5G62xDtw8mySlwnNR30YwPO7ng/Wi64HtloP
zgsMR6flPri9fcebNaBhlzpBdRfMK5Z3KpIhHtmVdiBnaM8Nvd/WHwlqmuLMc3Gk
L30SgLdTMEZeS1SZD2fJpcjyIMGC7J0R38IC+xo70e0gmu9lZJIQDSri3nDxGGeC
jGHeuLzRL5z7D9Ar7Rt2ueQ5Vfj4oR24qoAATILnsn8JuLwwoC8N9VKejveSswoA
HQBUlwbgsQfZxw9cZX08bVlX5O2ljelAU58VS6Bx9hoh49pwBiFYFIeFd3mqgnkC
AwEAAaNCMEAwHQYDVR0OBBYEFOLJQJ9NzuiaoXzPDj9lxSmIahlRMA8GA1UdEwEB
/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgGGMA0GCSqGSIb3DQEBCwUAA4ICAQDRSVfg
p8xoWLoBDysZzY2wYUWsEe1jUGn4H3++Fo/9nesLqjJHdtJnJO29fDMylyrHBYZm
DRd9FBUb1Ov9H5r2XpdptxolpAqzkT9fNqyL7FeoPueBihhXOYV0GkLH6VsTX4/5
COmSdI31R9KrO9b7eGZONn356ZLpBN79SWP8bfsUcZNnL0dKt7n/HipzcEYwv1ry
L3ml4Y0M2fmyYzeMN2WFcGpcWwlyua1jPLHd+PwyvzeG5LuOmCd+uh8W4XAR8gPf
JWIyJyYYMoSf/wA6E7qaTfRPuBRwIrHKK5DOKcFw9C+df/KQHtZa37dG/OaG+svg
IHZ6uqbL9XzeYqWxi+7egmaKTjowHz+Ay60nugxe19CxVsp3cbK1daFQqUBDF8Io
2c9Si1vIY9RCPqAzekYu9wogRlR+ak8x8YF+QnQ4ZXMn7sZ8uI7XpTrXmKGcjBBV
09tL7ECQ8s1uV9JiDnxXk7Gnbc2dg7sq5+W2O3FYrf3RRbxake5TFW/TRQl1brqQ
XR4EzzffHqhmsYzmIGrv/EhOdJhCrylvLmrH+33RZjEizIYAfmaDDEL0vTSSwxrq
T8p+ck0LcIymSLumoRT2+1hEmRSuqguTaaApJUqlyyvdimYHFngVV3Eb7PVHhPOe
MTd61X8kreS8/f3MboPoDKi3QWwH3b08hpcv0g==
-----END CERTIFICATE-----
```

2. crt 格式的服务器证书和 CA 证书链

按照 1.3 步骤将 GDCA 返回给您的服务器证书如 testweb.95105813.cn.cer 也转换为Base64编码格式，并保存为crt格式文件，如testweb.95105813.cn.crt。



新建一个文本文档，将 CA 证书和根证书加入到文件里，将文件保存为 gdca-cert-chain.crt。文件里证书的保存顺序是 CA 证书-根证书：

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

testweb.95105813.cn.crt | gdca-cert-chain.crt

```
BhMCQ04xMjAwBgNVBAoMKUdVQU5HIERPTkcgQOVSVE1GSUNBVEUgQVVUSE9SSVRZ
IENPLixMVEQuMR8wHQYDVQQDDBZHRENBIFRydXNOQVVUSCBSNSBST09UMB4XDTEO
MTEyNjA5NDUyNVoXDTMwMTIzMDE2MDAwMFoweDELMAkGA1UEBhMCQO4xMjAwBgNV
BAoMKUdVQU5HIERPTkcgQOVSVE1GSUNBVEUgQVVUSE9SSVRZIENPLixMVEQuMTUw
MwYDVQQDDCxHRENBIFRydXNOQVVUSCBSNCBFeHRlbmRlZCBWYWxpZGF0aW9uIFNT
TCBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMcA1Hwmgr2biKZO
a46bkeXyOruAorQZx779CY9Yq7kUDwW4nPdiTXK1k/xkIJJuwA6xzJOmrCuMzr15
J17LviwOIW6rDBSSOKjR6VoPS2kkVHLigD7n6mpJU22Evjo6gP/NC5maYchbOsoH
TAO5Yt58qA9qsMpDq9fS/AzYKAVWXBmWXh4x1BOXmGUpjYv3NXAtEznScauk9mgi
NzMMyuO9iDq8G7c1q5oFd5auRKnbAk1BxvgkdoSjg8w2Q2wemOcbbGgfU8QGAy/+
o/wopiGvmcL+p7b7bgYUaxI9H1mrfhB55cNK+cEFB8kkW7K/OPpXBd4lRHHWTLkE
Z9ieC4ECAwEAAaOCAX8wggF7MIGFBggrBgEFBQcBAQR5MHcwQgYIKwYBBQUHMAKG
NmhOdHA6Ly93d3cuZ2RjYS5jb2OuY24vY2VydC9HRENBX1RydXNOQVVUSF9SNV9S
TO9ULmRlcjAxBggrBgEFBQcwAYYlaHR0cDovL3d3dy5nZGNhLmNvbS5jbi9UcnVz
dEFVVEgvb2NzcDAdBgNVHQ4EFgQUHmrq3vUvv6jTbMfGP9tsZGDc4OEwDwYDVR0T
AQH/BAUwAwEB/zAfBgNVHSMEGDAWgBTiyUCfTc7omqF8zw4/ZcUpiGoKUTBCBgNV
HSAEOTA/MD0GCiqBHIbvLwEBBgEwLzAtBggrBgEFBQcCARYhaHR0cDovL3d3dy5n
ZGNhLmNvbS5jbi9jcHMvZXYtY3BzMEYGA1UdHwQ/MD0wO6A5oDeGNWh0dHA6Ly93
d3cuZ2RjYS5jb2OuY24vY4vY3JsL0dEQOFfVHJ1c3RBVVRIX1I1X1JPT1QuY3JsMA4G
A1UdDwEB/wQEAwIBhjANBgkqhkiG9w0BAQsFAAOCAgEAJ+QTFR1oac6PljrKm58L
gIdCKwkybREfAj+QTnDTONNMiapn6mZeuSLHhbZB1oyetddz1OMM8iJyU+ktJIHY
mlM3opIt3IuTWBbJobyDZYD+doed6H7gLcpOM1lbDVraXPVCNRTVM7OTfved9oB3
E8BisBTAKV/MPo1tFWBDWK2NV8jHItE65OzOMXI+sF9EKOoQwzBBhx3vG1WpeMdY
Hpu7z7xdZdYbOMT8Iub+iPh4vVMshXLKohejXByEpWEyVr+L8dEOmdaZzSku/VQm
ZQyDfNrHfUm2hH/XhC6IlNMA8/oeW99J/yfc/TNiCpImqHkOXBNeZeqK2HPBKj39
oMGOq5/kMT43jvTpjvjIX3tNnD+nrLcS48IogZ/X2qyGGh7FHkntLC2DBj/ipmHh
4CJt/dxAXODH/Z/rwhGVciR3zAXaLbZ1tIS+AhUVmcwIrzJC1kI6gU2dcUCkjo5M
1VfTjjyrWxpK7aE1kJpdmL7fcBmUWsJKnzV6H5YETONK2YXSxDjDqrUn1S67qbIB
XAYQnEc/MYoispbeYRKsVciKV1D1Dehl/gGQQ8OnCwsxj7gUTewVWgON3h/HP/+z
W8fh7J1c5YfbjS5zWLOGEEAomWoscOBa1KHxVR+1yVfn/yxGYpKd4tA+7vRc3GWd
blVRfCZEmVBCWTdOBC5ZGxM=
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIFiDCCA3CgAwIBAgIIfQmX/vBH6nowDQYJKoZIhvcNAQELBQAwYjELMAkGA1UE
BhMCQO4xMjAwBgNVBAoMKUdVQU5HIERPTkcgQOVSVE1GSUNBVEUgQVVUSE9SSVRZ
IENPLixMVEQuMR8wHQYDVQQDDBZHRENBIFRydXNOQVVUSCBSNSBST09UMB4XDTEO
MTEyNjA1MTMxNVoXDTQwMTIzMTE1NTk1OVowYjELMAkGA1UEBhMCQO4xMjAwBgNV
BAoMKUdVQU5HIERPTkcgQOVSVE1GSUNBVEUgQVVUSE9SSVRZIENPLixMVEQuMR8w
HQYDVQQDDBZHRENBIFRydXNOQVVUSCBSNSBST09UMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEA2aMW8MhOdHeb7zMNOwZ+Vfy1YI92hhJCfVZmPoiC7XJj
```

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 ssl_module modules/mod_ssl.so

#Include conf/extra/httpd-ssl.conf

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 Apache2.2\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：如

```
#   General setup for the virtual host
DocumentRoot "C:/Apache2.2/htdocs"
ServerName testweb.95105813.cn:443
ServerAdmin admin@gdca.com.cn
ErrorLog "C:/Apache2.2/logs/error.log"
TransferLog "C:/Apache2.2/logs/access.log"
```

找到 SSLCertificateFile 和 SSLCertificateKeyFile 这两个配置项，将

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

testweb.95105813.cn.crt 和 tetweb.95105813.cn.key 放到相关目录下，根据实际情况修改对应的证书名称：

```
#   in mind that if you have both an RSA and a DSA certificate you
#   can configure both in parallel (to also allow the use of DSA
#   ciphers, etc.)
SSLCertificateFile "C:/Apache2.2/conf/testweb.95105813.cn.crt"
#SSLCertificateFile "C:/Apache2.2/conf/server-dsa.crt"

#   Server Private Key:
#   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.)
SSLCertificateKeyFile "C:/Apache2.2/conf/testweb.95105813.cn.key"
#SSLCertificateKeyFile "C:/Apache2.2/conf/server-dsa.key"

#   Server Certificate Chain:
```

找到 SSLCertificateChainFile 项，将证书链 gdca-cert-chain.crt，放到相关目录下，根据实际情况修改对应的证书名称：

```
#   when the CA certificates are directly appended to the server
#   certificate for convinience.
SSLCertificateChainFile "C:/Apache2.2/conf/gdca-cert-chain.crt"
#SSLCertificateChainFile "C:/Apache2.2/conf/server-ca.crt"
```

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，请务必要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，以及服务器证书链文件 gdca-cert-chain.crt 即可完成服务器证书的备份操作。

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

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。

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