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 Nginx

2015/11/23

目录

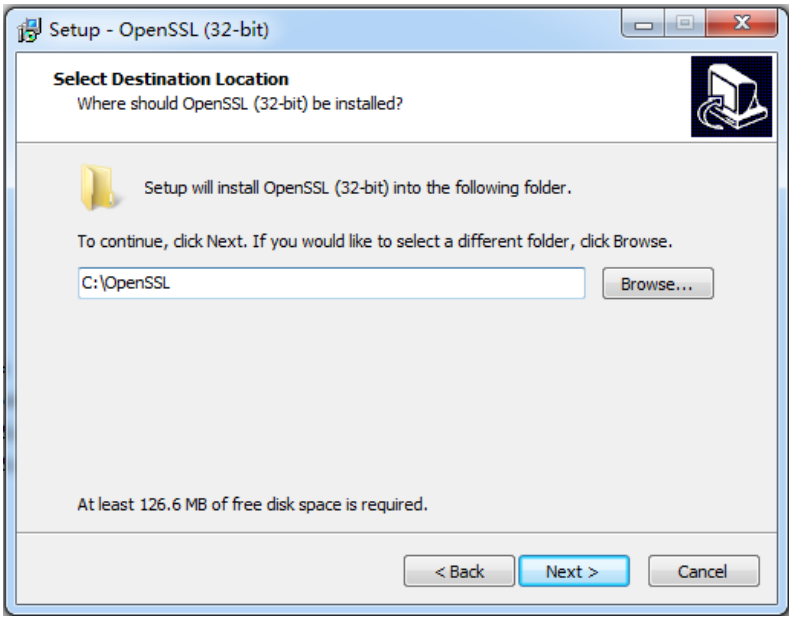
一、部署前特别说明

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 Nginx 服务器
2. 本部署指南适用于 Nginx 服务器环境;
3. Nginx 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;

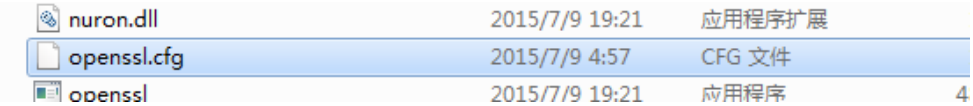
二、生成证书请求

1. 安装 OpenSSL 工具

您需要使用 Openssl 工具来创建证书请求。下载 OpenSSL：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

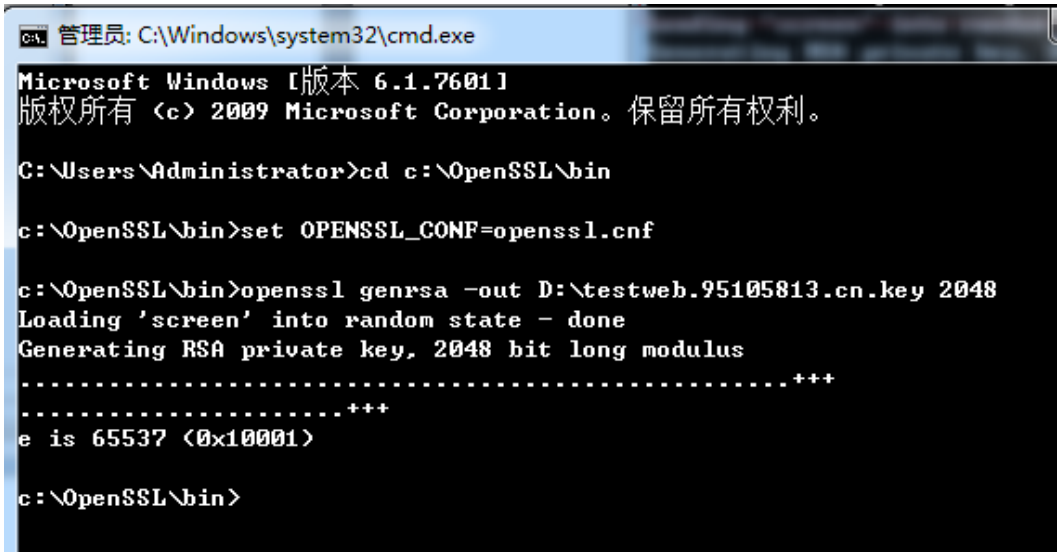
set OPENSSL_CONF=openssl.cnf

参考：

openssl genrsa -out server.key 2048

例：

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



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

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：

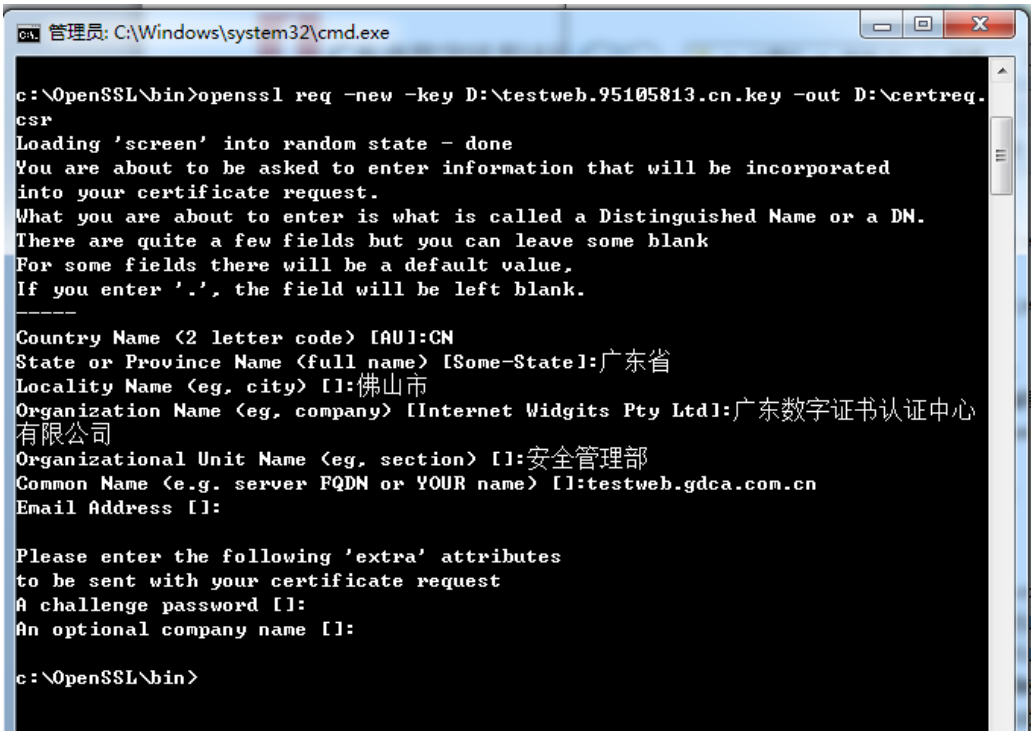
域名，如：testweb.95105813.cn。在多个域名时，填主域名

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。



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

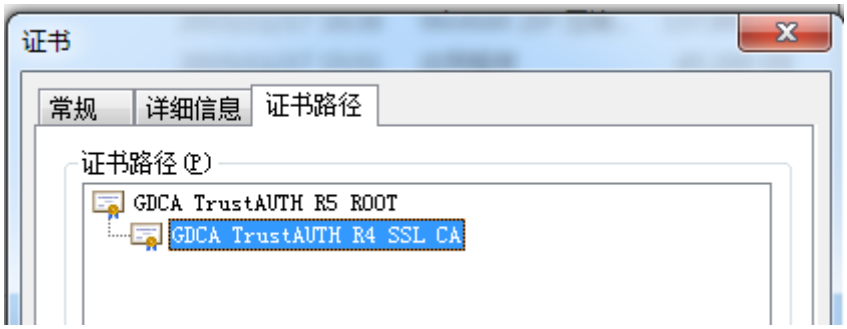
服务器证书需要安装根证书和 CA 证书,以确保证书在浏览器中的兼容性。有两种方式获取。

1.1 从邮件中获取

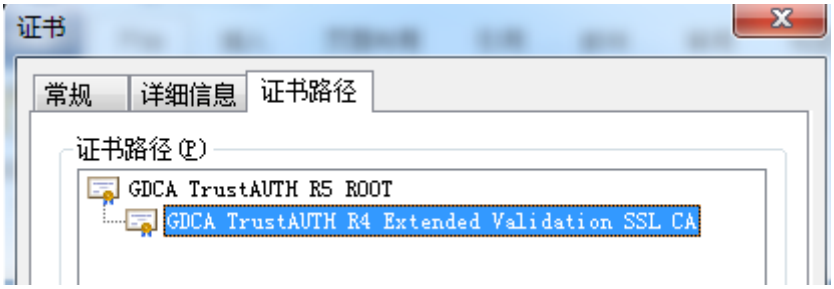
在您完成申请 GDCA 服务器证书的流程后，GDCA 将会在返回给您的邮件中附

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

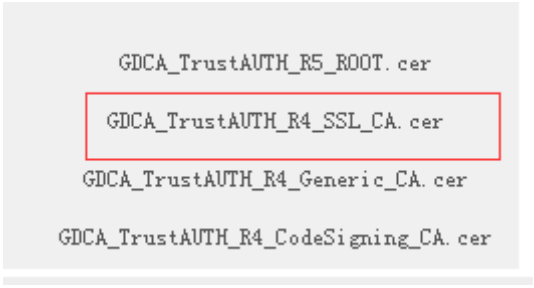
为保证您的证书能够正常使用，需要为浏览器下载并安装CA根证书，这样你的浏览器才能信任由GDCA签发的所有证书（下载后双击证书文件进行安装）。

12 项，显示 1 到10.[首页/前一页] 1, 2 [下一页/末页]

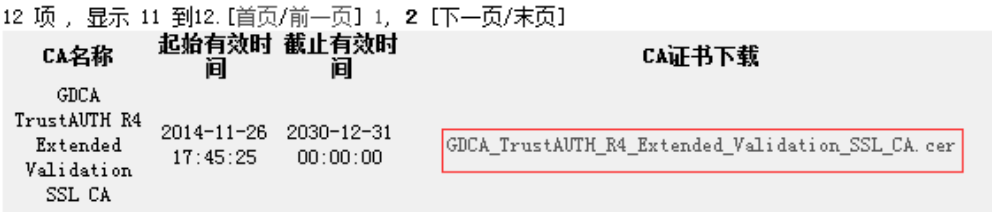
CA名称	起始有效时间	截止有效时间	CA证书下载
ROOTCA_sm2	2012-07-14 11:11:59	2042-07-07 11:11:59	社会公众应用根证书（SM2）.cer
GDCA TrustAUTH E1 CA	2014-06-26 15:02:11	2034-06-21 15:02:11	广东数字证书认证中心有限公司_sm2.cer
ROOTCA_rsa	2005-08-28 16:16:16	2025-08-23 16:16:16	社会公众应用根证书（RSA）.cer
GDCA TrustAUTH R2 CA	2013-12-16 14:29:40	2018-12-15 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



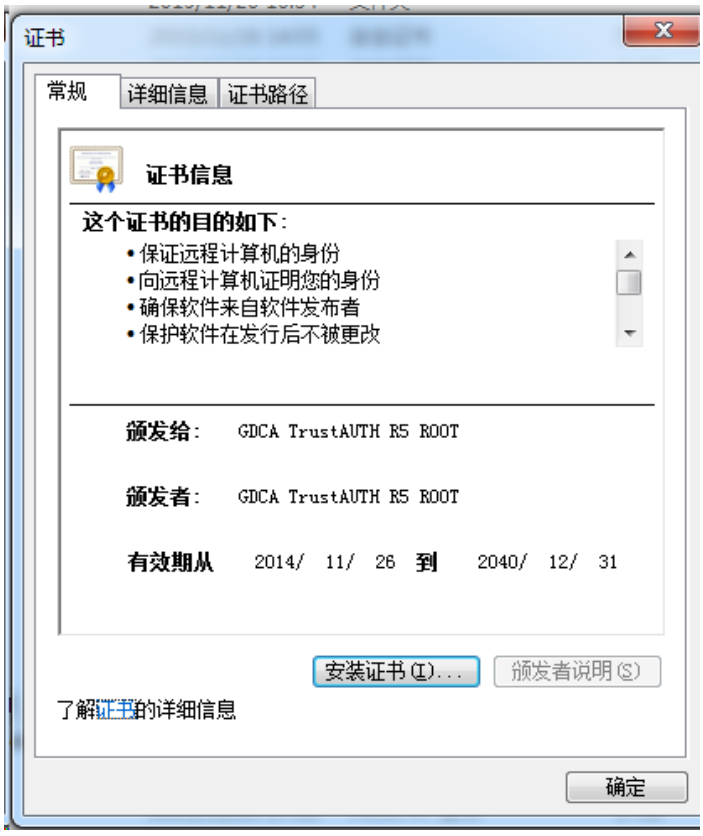
如果您申请的证书是恒信企业 EV SSL 证书（Extended Validation SSL Certificate），则下载 GDCA_TrustAUTH_R4_Extended_Validation_SSL_CA.cer



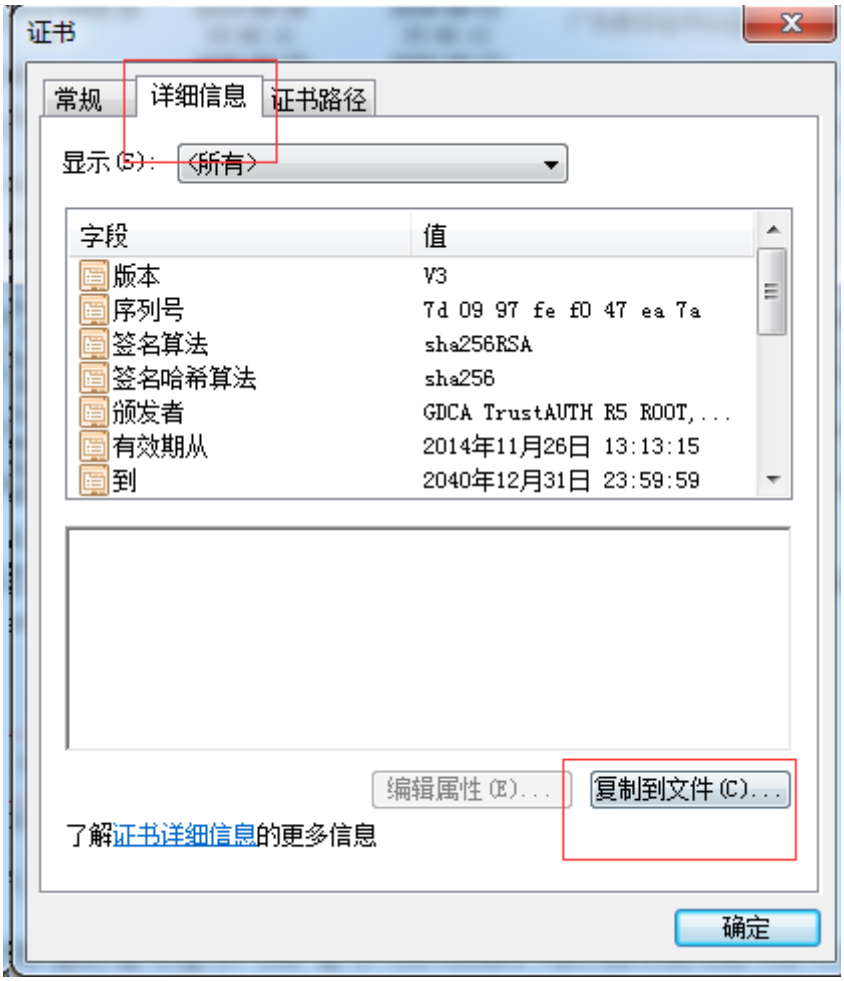
1.3 转换证书编码

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：

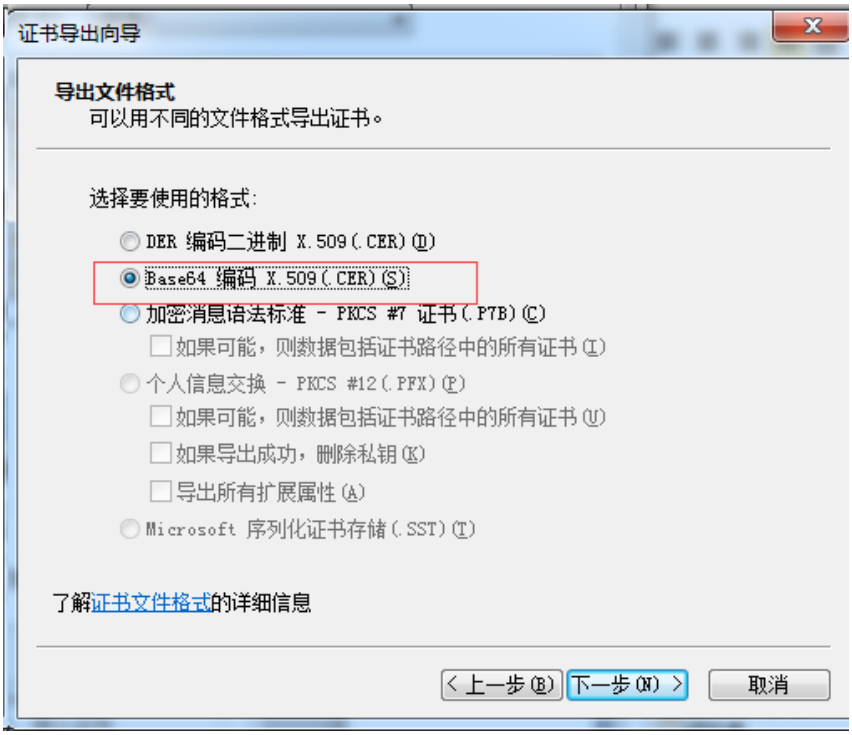
打开证书：



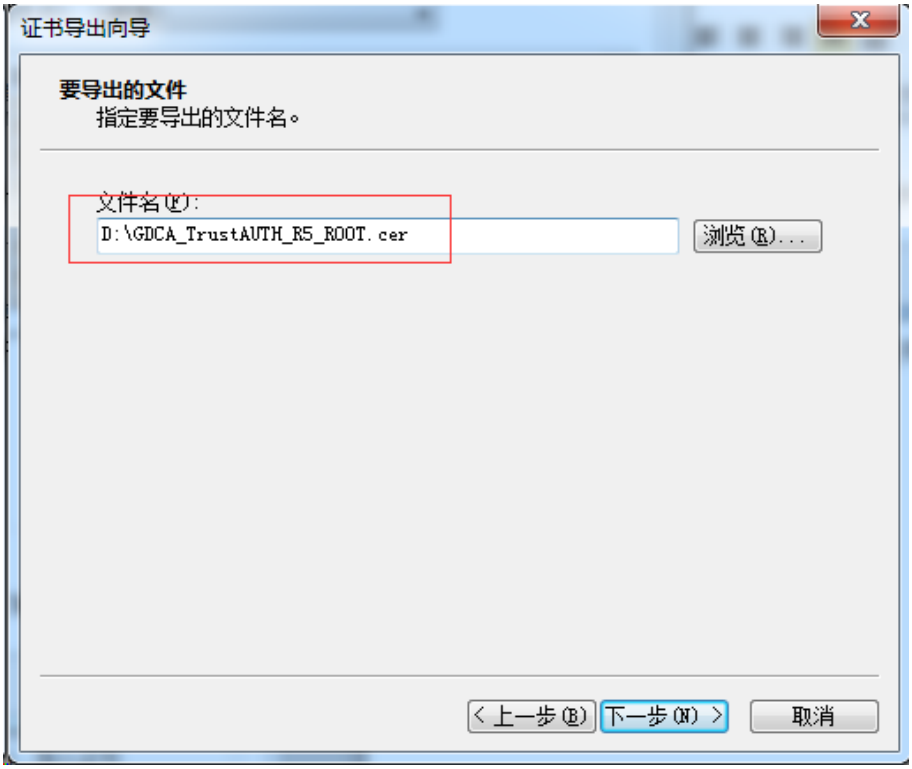
详细信息-复制到文件



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

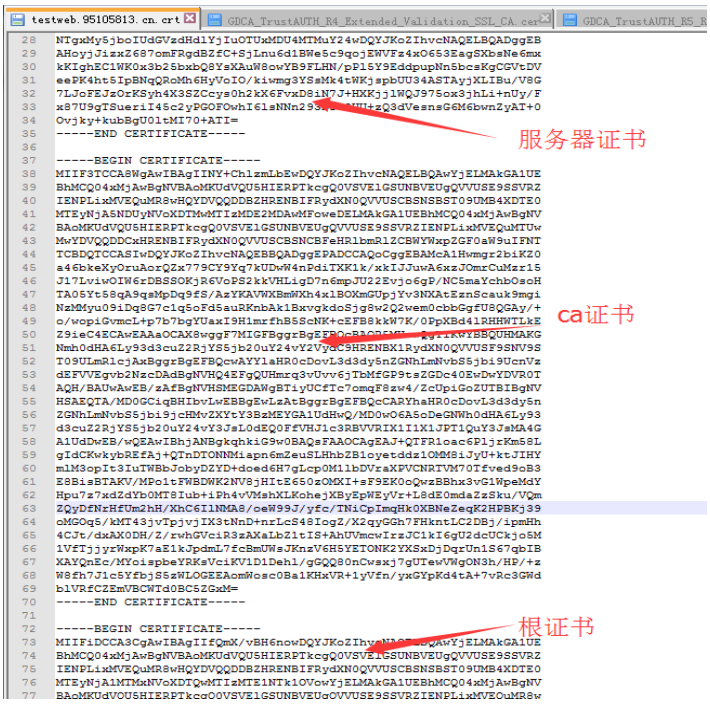


转换成 Base64 编码格式后，用编辑器打开，可以看到文件内容是以-----BEGIN CERTIFICATE-----开头，-----END CERTIFICATE-----结尾。以同样方式将 CA 证书也转换成 Base64 编码格式。

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



四、安装服务器证书

1. 配置给 nginx 服务器本机使用

打开 nginx 安装目录下 conf 目录中的 nginx.conf 文件，找到被注释掉的 server 配置，进行修改：

```
# HTTPS server
#
#server {
#    listen       443 ssl;
#    server_name  localhost;

#    ssl_certificate      /usr/local/ngi
#    ssl_certificate_key  /usr/local/ngi
#    ssl_session_cache    shared:SSL:1m;
#    ssl_session_timeout  5m;

#    ssl_ciphers  HIGH:!aNULL:!MD5;
#    ssl_prefer_server_ciphers  on;

#    location / {
#        root   html;
#        index  index.html index.htm;
#    }
#}
```

```
server {
    listen       443 ssl;
    server_name  localhost;

    ssl_certificate /usr/local/nginx/conf/testweb.95105813.cn.crt;
    ssl_certificate_key  /usr/local/nginx/conf/testweb.95105813.cn.key;
    ssl_protocols  TLSv1 TLSv1.1 TLSv1.2;
    ssl_session_cache    shared:SSL:1m;
    ssl_session_timeout  5m;
    ssl_ciphers  HIGH:!aNULL:!MD5;
    ssl_prefer_server_ciphers  on;

    location / {
        root   html;
```

```
            index  index.html index.htm;
        }
    }
```

把服务器证书 testweb.95105813.cn.crt 和私钥 testweb.95105813.cn.key 上传到配置文件指向的目录/usr/local/nginx/conf/

保存退出，并重新加载 nginx 配置 nginx -s reload 后通过 https 方式访问您的站点，测试站点证书的安装配置。

2. 使用 nginx 作为反向代理

Nginx 常被用作反向代理服务器使用。以下是配置示例：

在 /usr/local/nginx 目录下创建 servers 和 ssls 目录

mkdir ssls

mkdir servers

把服务器证书 testweb.95105813.cn.crt 及其私钥 testweb.95105813.cn.key 上传到 ssls 目录下。在 servers 目录创建服务器 testweb.95105813.cn 的配置文件 testweb.95105813.cn.conf:

```
server{
        listen       443;
        server_name  testweb.95105813.cn;
        ssl                  on;
        ssl_certificate      /usr/local/nginx/ssls/testweb.95105813.cn.crt;
        ssl_certificate_key  /usr/local/nginx/ssls/testweb.95105813.cn.key;
        ssl_protocols  TLSv1 TLSv1.1 TLSv1.2;
      location /{
          proxy_pass https://192.168.100.13:8002; #后端的 web 服务器
          proxy_set_header Host $host;
          proxy_set_header X-Real-IP $remote_addr;
          proxy_set_header   X-Forwarded-For  $proxy_add_x_forwarded_for;
```

```
        fastcgi_param HTTPS $https if_not_empty;
        proxy_set_header X-Forwarded-Proto https;
        }
    error_page   500 502 503 504  /50x.html;
    error_page 400  https://$host$uri?$args;
    location = /50x.html {
       root   html;
       }
     }
```

打开 nginx 安装目录下 conf 目录中的 nginx.conf 文件，加入：

include /usr/local/nginx/servers/testweb.95105813.cn.conf

```
http {
    include       mime.types;
    default_type  application/octet-stream;

    #log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
    #                  '$status $body_bytes_sent "$http_referer" '
    #                  '"$http_user_agent" "$http_x_forwarded_for"';

    #access_log  logs/access.log  main;

    sendfile        on;
    #tcp_nopush     on;

    #keepalive_timeout  0;
    keepalive_timeout  65;
    include /usr/local/nginx/servers/testweb.95105813.cn.conf
    #gzip  on;

    server {
        listen       80;
```

保存退出，并重新加载 nginx 配置 nginx -s reload，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，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。