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 Apache2.2 Linux 版

修订日期：2017/03/08

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 Apache 服务器

2. 本部署指南适用于 linux 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. 本部署指南提供参考的 apache 2.2 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 apache2.2 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转码与 CA 证书链生成开始阅读。

二、 安装 Apache 2.2

1. OpenSSL 环境

使用操作系统自带的 openssl 版本（已经编译 openssl 的 Apache 请跳过以下安装 apache 步骤）
OpenSSL 1.0.1~1.0.1f 存在不安全漏洞，请升级到最新版本。

2. 编译安装 apache

下载 apache

wget http://mirrors.cnnic.cn/apache//httpd/httpd-2.2.31.tar.gz

tar zxvf httpd-2.2.31.tar.gz

cd httpd-2.2.31

./configure --prefix=/usr/local/apache --enable-so --enable-ssl --enable-mods-shared=all

enable-ssl 添加 ssl 模块

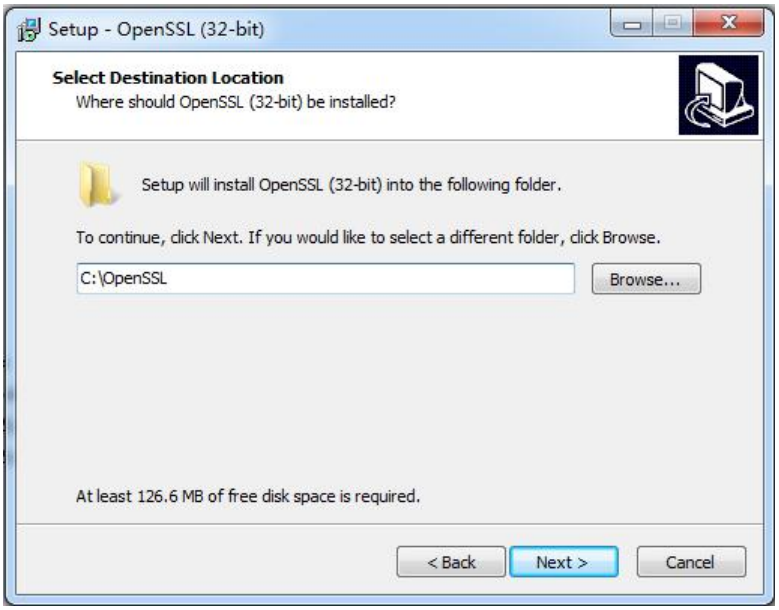
make && make install

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：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。如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，如数安时代科技股份有限公司或 Global Digital Cybersecurity Authority Co., Ltd.

5.Organizational Unit Name：Country Name ISO

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：

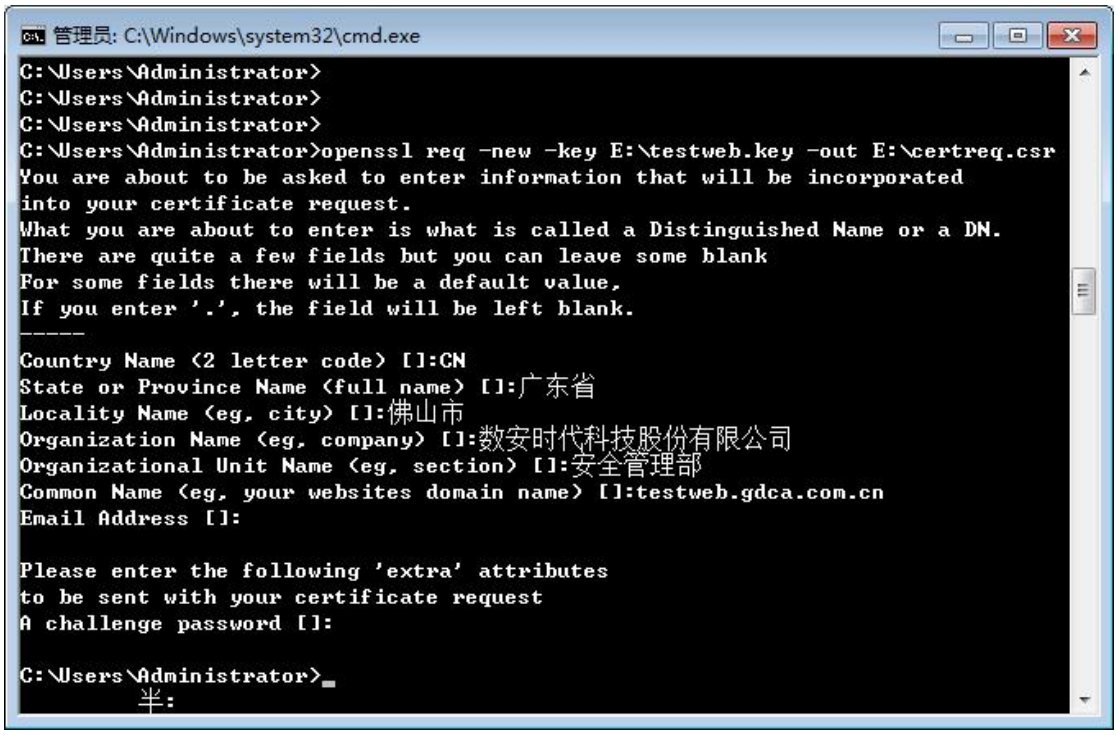
填您的邮件地址，不必输入，按回车跳过

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。

输入信息说明表如下：

字段	说明	示例
Country Name	ISO 国家代码（两位字符）	CN
State or Province Name	所在省份	Guangdong
Locality Name	所在城市	Guangzhou
Organization Name	公司名称	Digital Cybersecurity Authority Co., Ltd.
Common Name	申请证书的域名	www.trustauth.cn
Email Address	不需要输入	
A challenge password	不需要输入	
Anoptionalcompany name	不需要输入	



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。

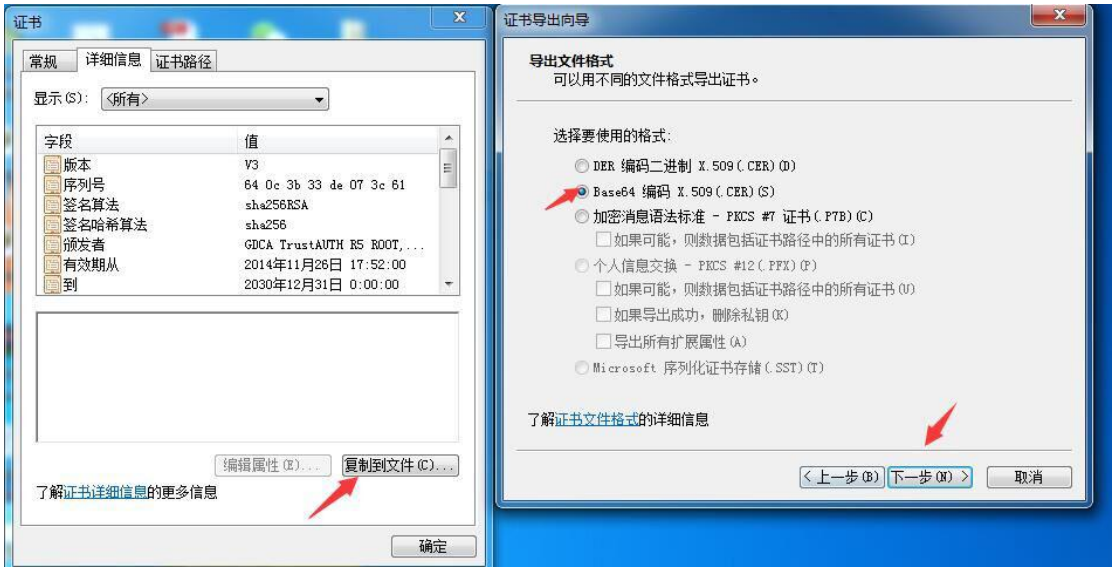
四、 获取服务器证书

1. 获取服务器证书的根证书和 CA 证书

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

```
-----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
ZuGR224HwGGALrIuL4xwp9E7PLOR5G62xDtw8myS1wnNR30YwPO7ng/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，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：

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,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 Apache2.2/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,

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。

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 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。

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。