



数安时代科技股份有限公司

GDCA 信鉴易® SSL 服务器证书请求生成指南

2015/11/23

目录

一、部署前特别说明.....	1
二、生成证书请求.....	1
1. 安装 OpenSSL 工具.....	1
2. 生成服务器证书私钥.....	2
3. 生成服务器证书请求 (CSR) 文件.....	3
4. 提交证书请求.....	5
三、服务器证书转码与 CA 证书链生成.....	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.....	5
1.2 从 GDCA 官网上下载:	7
1.3 转换证书编码.....	错误! 未定义书签。
2. crt 格式的服务器证书和 CA 证书链.....	错误! 未定义书签。
四、证书遗失处理.....	8

一、部署前特别说明

1. 本文档主要描述如何通过 openssl 产生密钥对;
2. 本指南在 windows 下适用 OpenSSL 工具方式生成证书请求文件;
3. 您可以使用其它方式并不要求按照本指南在 windows 下使用 OpenSSL 工具方式生成证书请求文件;

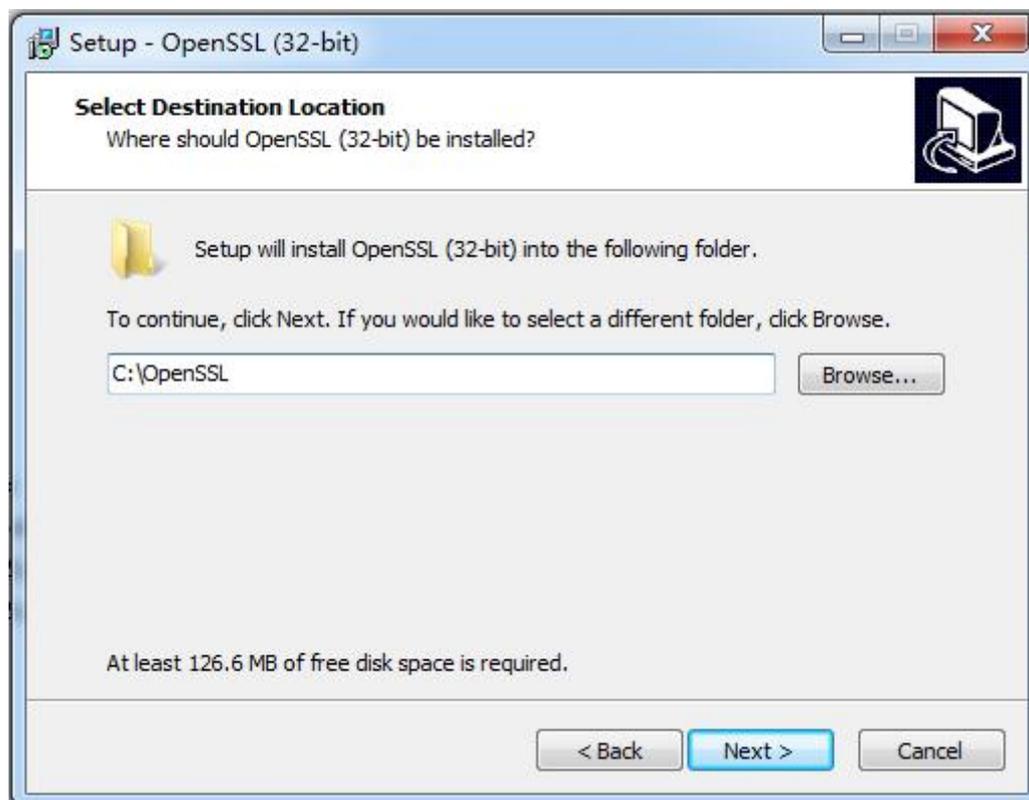
二、生成证书请求

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

 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。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
```



```
ca: 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:

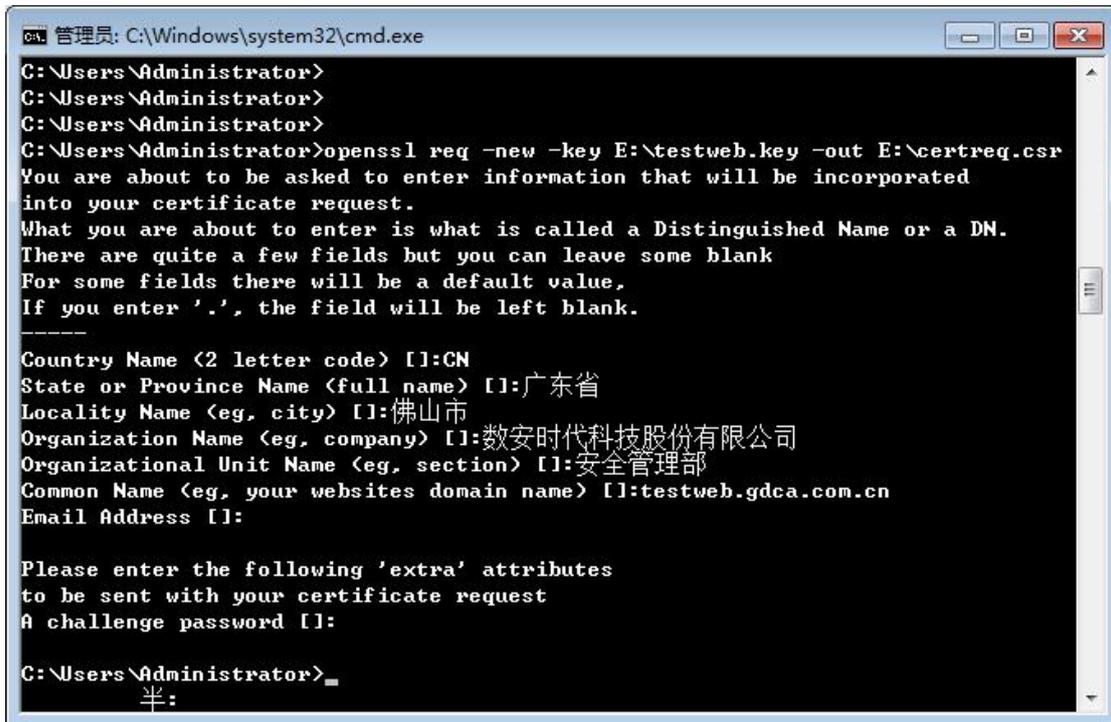
填域名，如：testweb.95105813.cn。在多个域名时，填主域名

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。



```
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。

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。

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.gdca.com.cn/customer_service/knowledge_universe/ca_cq/



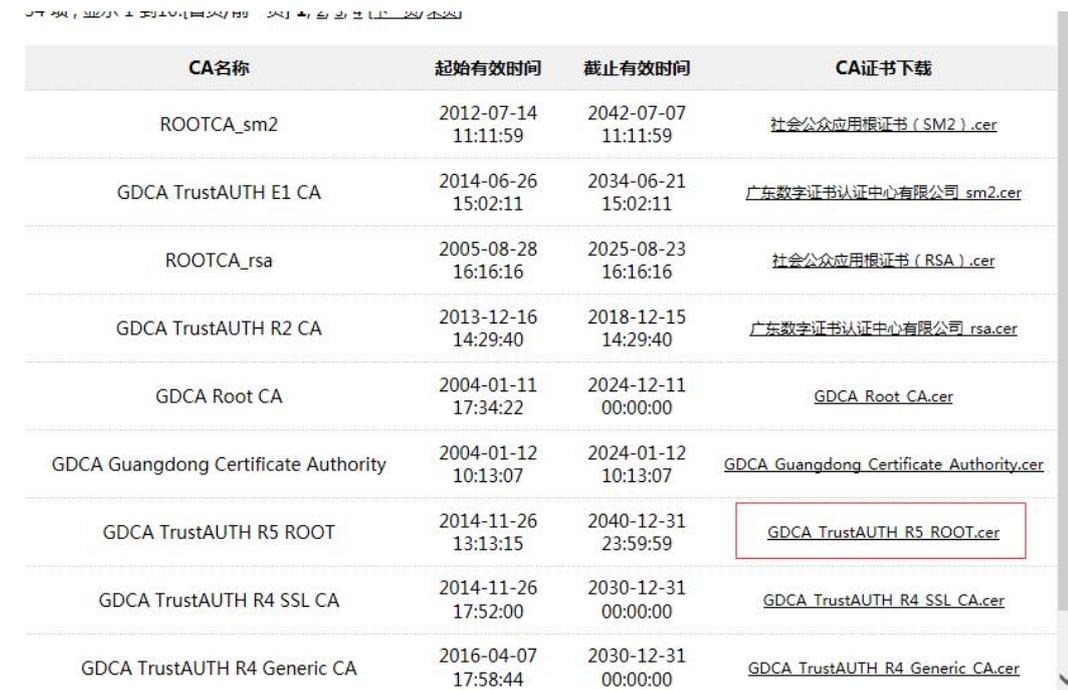
CA证书查询

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）。

34 项，显示 31 到34. [首页/前一页] 1, 2, 3, 4 [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 E4 Primer CA	2016-03-31 17:55:52	2030-12-31 00:00:00	GDCA_TrustAUTH_E4_Primer_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 SSL CA	2016-04-06 11:35:09	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_EV_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

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
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	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



34 项, 显示 31 到 34. [首页/前一页] 1, 2, 3, 4 [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 E4 Primer CA	2016-03-31 17:55:52	2030-12-31 00:00:00	GDCA_TrustAUTH_E4_Primer_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 SSL CA	2016-04-06 11:35:09	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_EV_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

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

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)。

34 项, 显示 31 到 34. [首页/前一页] 1, 2, 3, 4 [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 E4 Primer CA	2016-03-31 17:55:52	2030-12-31 00:00:00	GDCA_TrustAUTH_E4_Primer_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 SSL CA	2016-04-06 11:35:09	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_EV_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

四、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。

