3．配置环境变量

打开安装后路径（本例为 D:\var\OpenSSL-Win32\bin），安装后文件信息如图 18-7 所示。

图 18-7　安装后文件信息

其中最常用的有 openssl.exe（命令行工具）、libeay32.dll（算法库实现）、ssleay32.dll（SSL/TLS 协议实现）、openss.cfg（参数配置文件）。本例主要使用 openssl.exe 完成 CA 功能演示。

在安装目录下，打开命令行窗口（所有程序→附件→命令提示符），执行命令“openssl.exe version”可查询版本信息，显示如图 18-8 所示信息，表示 OpenSSL 版本为 1.0.1g。（下文中“执行命令”均指在命令行窗口中输入该命令。）

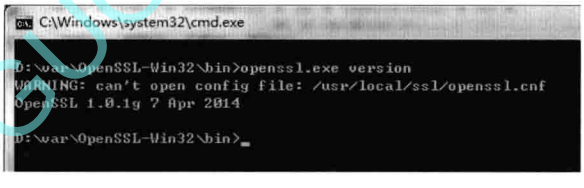

图 18-8　显示 OpenSSL 版本

在显示版本时，出现“WARNING: can't open config file: /usr/local/ssl/openssl.cnf”消息，这是因为缺省的配置文件/usr/local/ssl/openssl.cnf 不存在。可以通过环境变量进行更改。

设置环境变量 OPENSSL_CONF，使其指向新的配置文件，执行命令：

```
set OPENSSL_CONF=D:\var\OpenSSL-Win32\bin\openssl.cfg
```

然后再执行命令“openssl.exe version”，显示如图 18-9 所示信息，此时没有了警告信息。

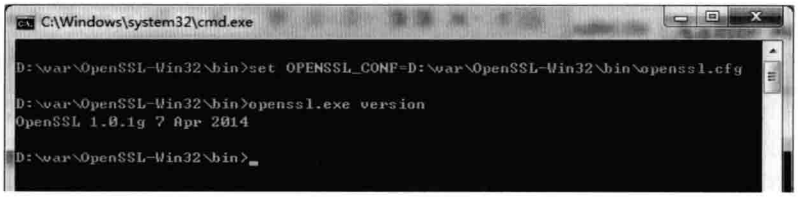

图 18-9　设置环境变量 OPENSSL_CONF 后查看版本

QUQU.nonlaMS

18.1.3 申请证书

1. 创建相关文件

在 D:\var\OpenSSL-Win32\bin 下创建文件夹 demoCA，并在 demoCA 下创建子文件夹：certs、crl、newcerts、private。

创建几个文本文件：

① index.txt。

② serial。在 serial 文件中写入初始证书序列号，可以设置为 AEF0（十六进制表示的初始证书序列号）。

③ crlnumber。在 crlnumber 中写入 CRL 序列号，可以设置为 01（十六进制表示）。

创建完成后结果如下所示：

```
-- demoCA/
    |-- certs/
    |-- crl/
    |-- newcerts/
    |-- private/
    |-- index.txt
    |-- serial
    |-- crlnumber
```

2. 创建 CA 证书

先用缺省配置文件产生 CA 证书和用户证书，此处 CA 证书为自签名证书。

创建的根 CA 证书的名字为 OpenSSL CA，执行命令：

```
openssl.exe req -x509 -newkey rsa:2048 -days 3660 -out .\demoCA\cacert.pem -outform PEM -keyout .\demoCA\private\cakey.pem -subj "/C=CN/CN=OpenSSL CA"
```

在执行过程中需要输入私钥保护口令两次，显示信息如图 18-10 所示。openssl.exe req 支持的参数可以通过执行命令“openssl.exe req help”查看。

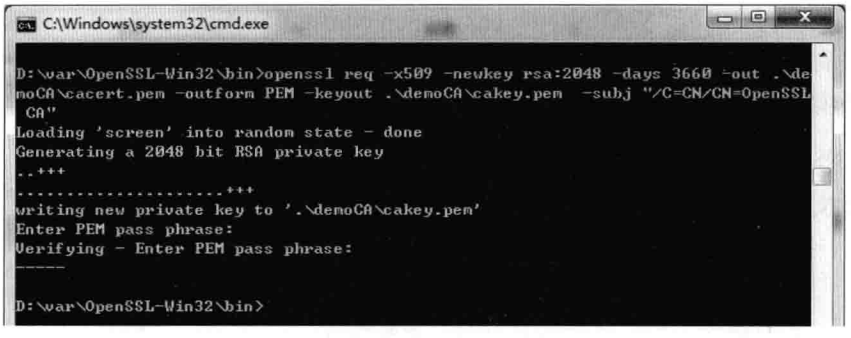

图 18-10　产生根证书的过程

上面命令的含义为：产生密钥长度为 2048 位的 RSA 密钥，证书的有效期为 3660 天，这是一个自签名证书，产生的证书输出为 demoCA 目录下的 cacert.pem，证书格式为 PEM，

GUOXU.nokiaMS

产生的私钥为 demoCA 目录下的 cakey.pem，证书的通用名为 OpenSSL CA。

打开刚产生的证书，在 Windows 下显示如图 18-11 所示信息。

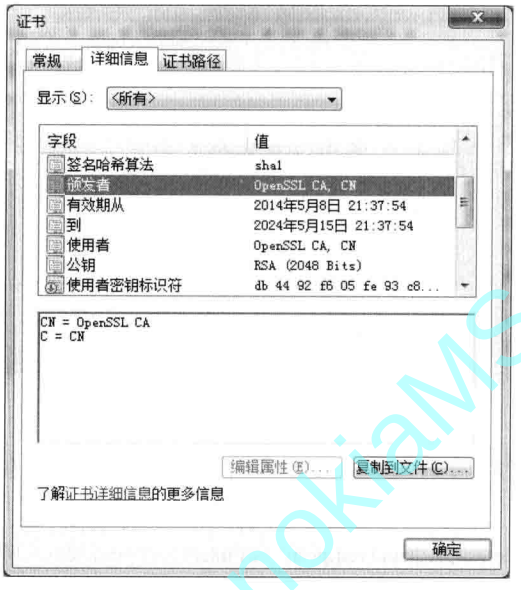

图 18-11　产生的 CA 证书信息

根证书产生后，把 cakey.pem 复制到.\demoCA\private\目录下，然后修改 openssl.cfg 文件，找到[CA_default]标志，具体信息如下：

```
[ CA_default ]
dir             = ./demoCA              # Where everything is kept
certs           = $dir/certs            # Where the issued certs are kept
crl_dir         = $dir/crl              # Where the issued crl are kept
database        = $dir/index.txt        # database index file.
#unique_subject = no                    # Set to 'no' to allow creation of
                                        # several ctificates with same subject.
new_certs_dir   = $dir/newcerts         # default place for new certs.
certificate     = $dir/cacert.pem       # The CA certificate
serial          = $dir/serial           # The current serial number
crlnumber       = $dir/crlnumber        # the current crl number
                                        # must be commented out to leave a V1 CRL
crl             = $dir/crl.pem          # The current CRL
private_key     = $dir/private/cakey.pem# The private key
RANDFILE        = $dir/private/.rand    # private random number file
```

找到[CA_default]下的“policy = policy_match”并将其修改为“policy = policy_anything”。其他值采用缺省值。

3．创建用户证书

在创建完 CA 证书并修改配置文件后，就可以创建用户证书了。先创建用户证书请求

GUOXU.nokiaMS

文件，用户名字为 user-1，执行命令：

```
openssl.exe req -newkey rsa:1024 -days 3640 -keyout .\demoCA\private\user1key.pem -keyform PEM
-out .\demoCA\user1req.pem -outform PEM -nodes -subj "/C=CN/CN=user-1"
```

显示信息如图 18-12 所示。

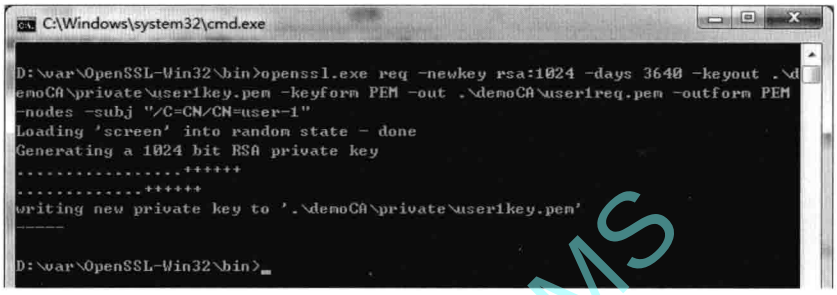

图 18-12　产生用户证书请求命令

接着，使用产生的用户请求文件，向刚才产生的 OpenSSL CA 证书申请生成用户证书。执行命令：

```
openssl.exe ca -in .\demoCA\user1req.pem -out user1cert.pem -days 3640
```

openssl.exe ca 命令行参数可以通过执行命令“nssl.exe ca help”查看。

显示如图 18-13 所示的操作步骤。首先要求输入 CA 私钥的保护口令，这个值是在产

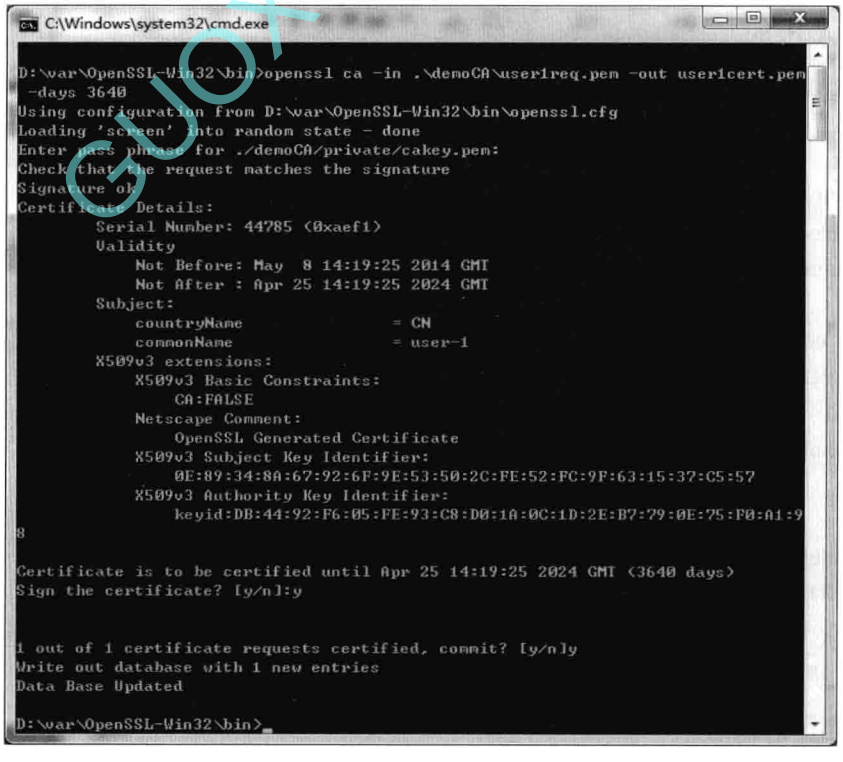

图 18-13　用户证书签发步骤

GUOXUNokiaMS

生 CA 证书时两次重复输入的保护口令，接着显示了证书信息，然后询问是否签发证书，输入 y 表示同意。然后显示是否提交证书请求，输入 y 表示提交。命令行显示将产生的证书提交到证书库成功。

产生的证书除了在当前目录存放一份名为 user1cert.pem 的证书文件外，还存放在.\demoCA\newcerts 目录下，以证书的序列号命名，如刚才产生的 user-1 证书的序列号为 AEF1，证书的文件名为 AEF1.pem。

打开产生的用户证书，可以看到图 18-14 所示信息。

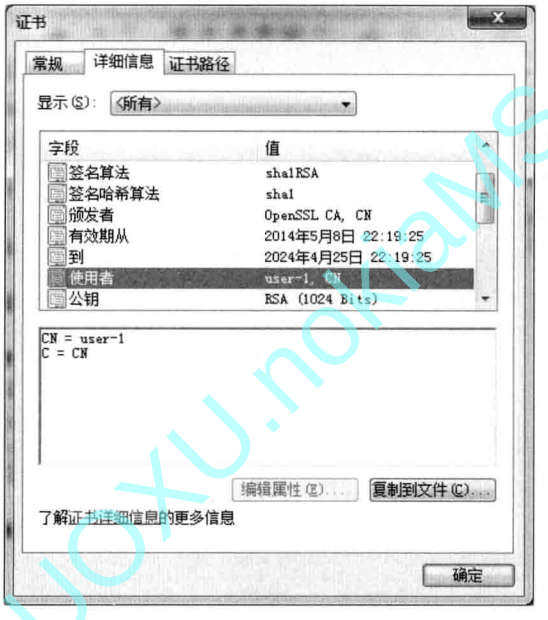

图 18-14　签发的 user-1 用户证书

重复同样的步骤，可以签发多张证书，此处签发 user-2、user-3 证书。

产生 user-2 证书，执行命令：

```
openssl.exe req -newkey rsa:1024 -days 360 -keyout .\demoCA\private\user2key.pem -keyform PEM -out .\demoCA\user2req.pem -outform PEM -nodes -subj "/C=CN/CN=user-2"
openssl.exe ca -in .\demoCA\user2req.pem -out user2cert.pem -days 360
```

产生 user-3 证书，执行命令：

```
openssl.exe req -newkey rsa:1024 -days 360 -keyout .\demoCA\private\user3key.pem -keyform PEM -out .\demoCA\user3req.pem -outform PEM -nodes -subj "/C=CN/CN=user-3"
openssl.exe ca -in .\demoCA\user3req.pem -out user3cert.pem -days 360
```

18.1.4　生成并下载 CRL

1．生成空 CRL

执行命令“openssl.exe ca -gencrl -out .\demoCA\crl\democrl.crl”，生成空 CRL，如图 18-15 所示，需要输入 CA 私钥的保护口令。

GUOXU.nokaMS