

## Chapter 6

# 证书生成及应用实验——利用证书进行安全邮件通信

### 6.1 工具

OpenSSL

### 6.2 提供的信息

我们事先利用 OpenSSL 生成了 Buu 的 CA 私钥和证书，私钥在实际使用中需要严格保密 (最高机密)。Buu 的 CA 证书 buucacert.cer，已发布在 QQ 群文件夹“证书发布目录”。Buu 的私钥文件 buucakey.pem，我们通过微信群发给大家，我们暂且认为这是个“安全信道”。指导老师的证书 lxf.cer，也已发布在 QQ 群文件夹“证书发布目录”。

### 6.3 任务

首先你“扮演”CA 的工作人员，为客户 (现在就是你自己) 生成一个私钥和证书，然后你要通过安全的方式将私钥交给客户，将客户的证书发布在 QQ 群文件夹“证书发布目录”中，证书文件用客户名字命名 (汉语)。

特别要注意的是，你给客户需要生成公私钥信息的 PKCS#12 文件，在实验中使用。

利用支持公钥签名和加密的 email 客户端 (例如：Thunderbird)，给指导老师发一个**加密的签名**邮件。指导老师邮箱：xxtxiaofeng@buu.edu.cn。

注：生成证书时，序列号可以随机生成，也可以指定，根据前几届有些同学式样情况，发现有些同学使用的是同一个序列号，那么老师在导入证书时，会出现冲突，为了避免这样的情况发生，要求生成证书时，制定序列号，序列号是自己的学号，在指定序列号时，通常要求使用的是十六进制的数，所以需要将你的十进制学号转为十六进制数。比如某同学的学号为：2022240381012，转为十六进制后为：1D6D6EB6854

### 6.3.1 邮件格式要求

说明：下文中的 \*\*\* 表示发件人的姓名，??? 表示日期。

邮件主题：\*\*\* 加密签名练习邮件

邮件正文如下：

这是我的第一封加密的签名邮件。

\*\*\*

???

## 6.4 评价

此练习评价不使用编程类练习评价标准，只是看最终结果，是否能正确地收到你的加密、签名邮件，以及文件格式是否按照要求的格式。