图 18-15　产生 CRL 文件

执行命令“openssl.exe crl -in .\demoCA\crl\democrl.crl -text -noout”，显示 CRL 内容，如图 18-16 所示。

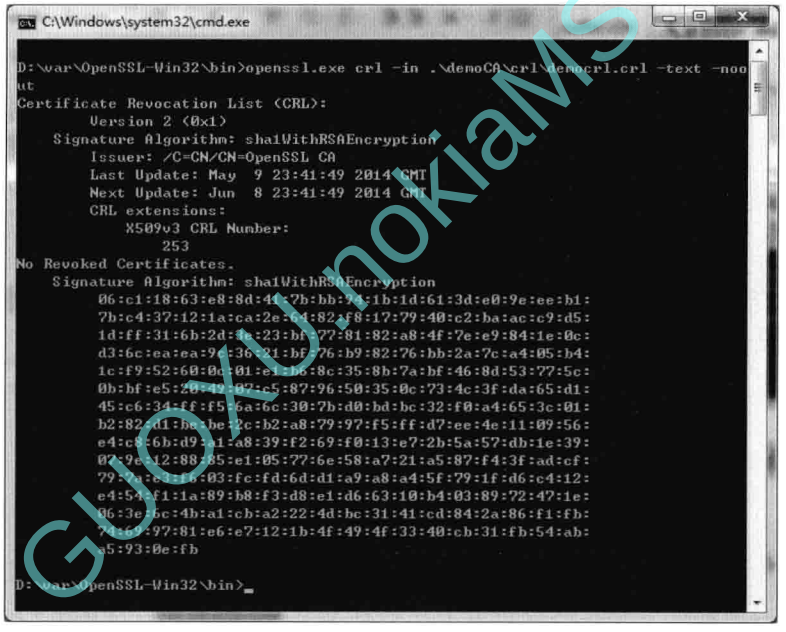

图 18-16　无吊销证书的 CRL 内容

2．作废证书

执行命令“openssl.exe ca -revoke user3cert.pem”，作废证书 user-3，如图 18-17 所示。

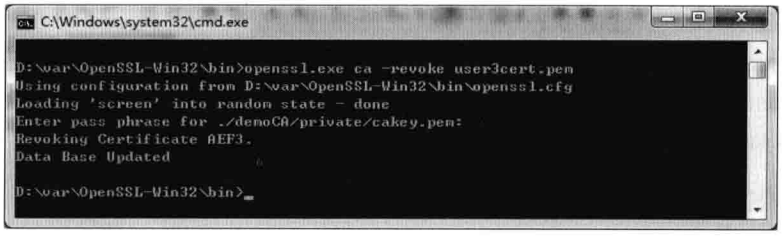

图 18-17　吊销 user-3 用户证书

3．生成新 CRL

执行命令“openssl.exe ca -gencrl -out .\demoCA\crl\democrl.crl”，生成新 CRL，如图 18-18

所示。

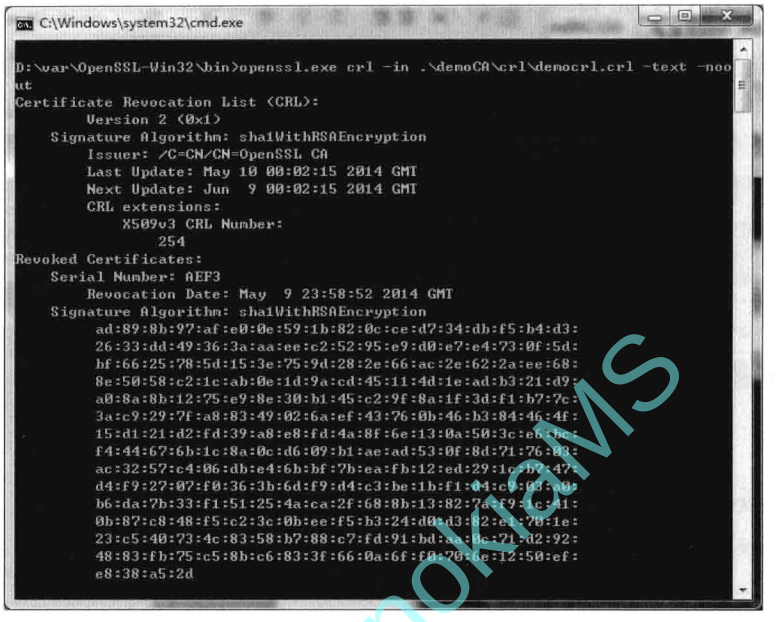

图 18-18　包含 user-3 用户证书的 CRL 内容

可以看到 user-3 用户对应证书的序列号 AEF3 已经在 CRL 里了。在 Windows 环境下双击产生的 CRL 文件 democrl.crl，显示如图 18-19 所示信息。

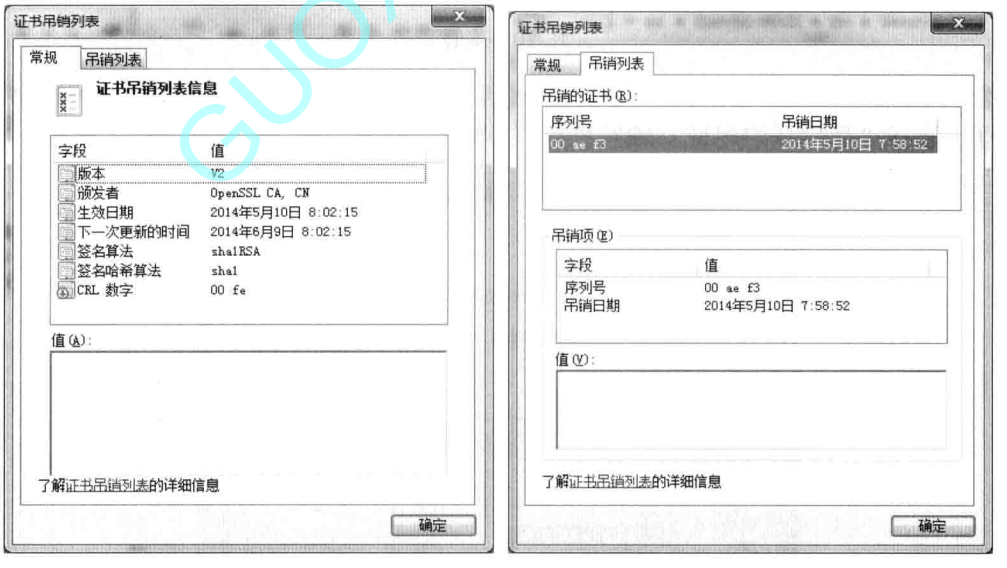

图 18-19　Windows 下 CRL 文件显示内容

可以看到 CRL 签发者为 OpenSSL CA，即前面签发的 CA 证书。作废证书序列号为 00 ae f3（证书序列号前面增加了 00），实际序列号就是 user-3 证书的 AEF3。

把 CRL 文件 democrl.crl 复制出来就可以使用了。

18.1.5 导入 CA 证书到 IE 可信任证书库

为确保浏览器信任 OpenSSL CA 签发的证书，需要将 OpenSSL CA 证书导入浏览器中的可信任根证书库中。

双击 CA 证书文件 cacert.pem，将出现证书信息界面。单击“安装证书”按钮，将出现证书导入向导界面，单击“下一步”按钮，如图 18-20 所示。

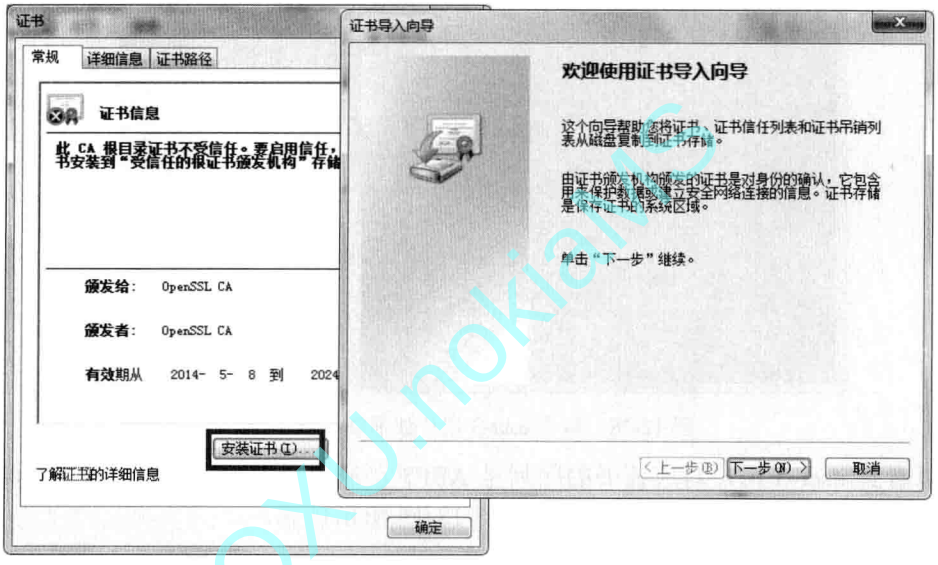

图 18-20 安装证书

选中“将所有的证书放入下列存储”，然后单击“浏览”按钮，将弹出“选择证书存储”对话框，选择“受信任的根证书颁发机构”，单击“确定”按钮，如图 18-21 所示。

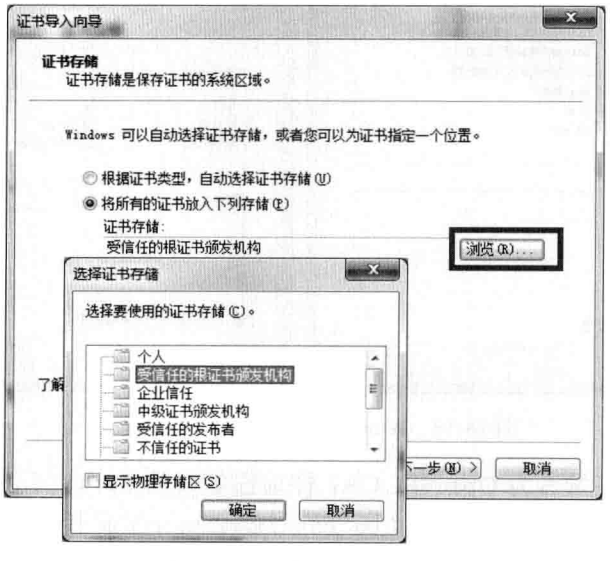

图 18-21 证书导入选择界面

单击“完成”按钮后，将弹出“安全性警告”对话框，系统提示“Windows 不能确认证书是否来自 OpenSSL CA”等警告信息，单击“是”按钮，弹出“导入成功”对话框，如图 18-22 所示。

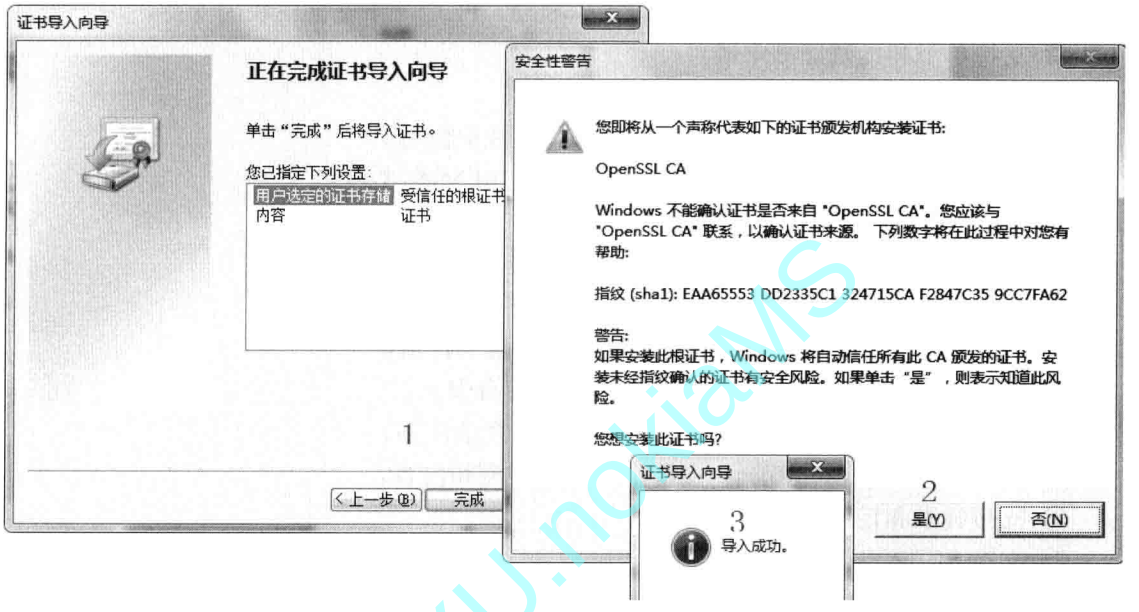

图 18-22　导入证书确认界面

18.2　EJBCA 示例

18.2.1　简介

EJBCA（Enterprise Java Bean Certificate Authority）是一个全功能的 CA 系统软件，它基于 J2EE 技术，并提供了一个强大的、高性能的、基于组件的 CA。EJBCA 兼具灵活性和平台独立性，能够独立使用，也能和任何 J2EE 应用程序集成。EJBCA 有如下特点：

① 支持多个 CA 或多级 CA，可在一个 EJBCA 实例中建立多个 PKI 基础设施。

② 根 CA 和子 CA 数量不受限制。支持从其他 CA 申请交叉证书，从桥 CA 申请桥证书，给其他 CA 颁发交叉证书。

③ 从公开运营 CA 获取自己的 CA 证书。

④ 遵循 X509 和 PKIX 相关标准。

⑤ 支持 RSA 密钥长度到 8192 位。

⑥ 支持 DSA 密钥长度到 1024 位。

⑦ 支持 ECDSA 密钥算法。

⑧ 支持多种哈希算法签名，包括 SHA1、SHA2。

⑨ 兼容 NSA SUITE B 算法和证书。

⑩ 支持 X.509 证书和卡验证证书（Card Verifiable certificates）。

⑪ 支持硬件安全模块，内建对 Thales/nCipher、SafeNet Luna、SafeNet ProtectServer、Utimaco CryptoServer、AEP Keyper、ARX CoSign、PKCS#11 安全模块的支持。

⑫ 支持单个和批量证书申请。

⑬ 颁发满足大多数服务器的 SSL/TLS 证书。

⑭ 支持通过插件方式扩展管理员注册和用户注册流程。

⑮ 服务器和客户端证书支持 PKCS12、JKS、PEM 格式。

⑯ 支持 Firefox、IE 等浏览器。

⑰ 通过 API 方式支持其他应用进行证书注册。

⑱ 注册 VPN 用户证书时，可产生 OpenVPN 证书安装包。

⑲ 移动注册支持，如以 SCEP 方式支持 iOS 证书注册。

⑳ 支持 CRL 生成，及符合 RFC5280 的 CRL 分发点。

㉑ 支持 Windows、Linux、Mac OS X 智能卡登录证书。

㉒ 通过证书模板（profiles）支持不同证书类型和内容。

㉓ 支持标准和定制扩展项。

㉔ 支持 SCEP 协议。

㉕ 支持 RFC3739（Qualified Certificate Statement），能够发布 EU/ETSI 限定证书。

㉖ 支持 OCSP，包括 AIA 扩展项。

㉗ 支持 RFC4387 通过 HTTP 获取 CA 证书和 CRL。

㉘ 支持德国通用 PKI SigG CertHash OCSP 扩展。

㉙ 支持 CMP（RFC4210 和 RFC4211）。

㉚ 支持异步 XKMS。

㉛ 支持密钥恢复。

EJBCA 系统支持的部署结构如图 18-23 所示。

在防火墙 1 后面是 RA 服务器和 OCSP 服务（和 LDAP 查询服务器）集群，在 RA 和 CA 之间是防火墙 2，CA 服务器受防火墙 2 保护。为了数据安全性，对 CA 数据库进行备份，建立备份数据库服务器。在后续测试中，为了方便，把相关组件安装在一台应用服务器中。

18.2.2 安装配置

安装配置 EJBCA 相对复杂些，需要分多个步骤依次进行：

① 下载安装 JDK。

② 下载安装 JDK 策略文件。

③ 下载安装 Apache Ant。

④ 下载 EJBCA 文件。