TOPCA V4.0 用户操作手册

V1.9

目 录

1. 前言

用户操作手册用来帮助用户申请并管理证书服务。作为用户证书管理员，您的职责就是配置申请用户证书，并对证书生命周期的管理。

1.1. 关于本手册

本手册的目的是：

- 指导您申请用户证书。
- 指导您获得和使用证书。
- 叙述一些重要的要求，以便对提交证书请求的个人和组织的身份进行确认。

本手册提供了用户进行日常操作时所需的文档。

2. 用户证书服务中心

在开始使用用户证书服务之前，需要向上级 RA 系统申请用户证书服务。

2.1. 用户证书服务中心

用户证书服务中心即为最终用户提供申请数字证书的站点，在使用该服务之前，需登录该系统。访问“http://ip/TopCA/userEnroll ”，进入登录页面，如图 2-1，在输入框中输入帐户 O 或 OU 关键字，进行实时查找帐户，在结果列表中选择帐户进行登录。登录成功，进入用户证书服务中心，如图 2-2。

图 2-1 登录页面

图 2-2 用户证书服务中心首页（双证书）

2.2. 用户证书服务中心功能结构

若帐户的证书类型为单证书，则用户证书服务中心将显示以下几个功能：

- 申请用户证书
- 获取用户证书
- 查询用户证书
- 更新用户证书
- 吊销用户证书
- 安装 CA 证书链
- 下载证书吊销列表（CRL）
- 证书替换
- 证书预览

若帐户的证书类型为双证书，则用户证书服务中心显示以下几个功能：

- 申请用户证书
- 获取用户证书
- 查询用户证书
- 更新用户证书
- 吊销用户证书
- 恢复加密证书
- 安装 CA 证书链
- 下载证书吊销列表（CRL）
- 证书替换
- 证书预览

2.3. 申请用户证书

在用户证书服务中心页面点击“申请用户证书”，进入申请用户证书页面，如图 2-3。输入必填项信息（带*号为必填项），点击确定后提交。

图 2- 3 用户证书的申请

提交成功后，您将看到如图 2- 4 所示提示信息，此时管理员将向您所填写的邮箱中发送证书注册确认邮件。

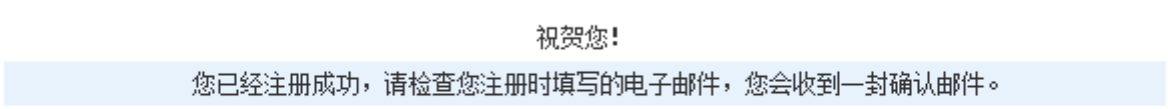

图 2- 4 注册成功提醒

2.4. 获取用户证书

用户证书申请被 RA 管理员批准后，系统自动给申请人填写的邮箱发送包含 PIN 码的邮件，您可以通过该 PIN 码进行证书的获取。

在用户证书服务中心页面点击“获取用户证书”，进入操作页面，如图 2- 5。请将邮件中的 PIN 码复制到如图 2- 5 中身份识别码的文本框中，并输入注册时填写的用户口令，点击“获取证书”即可获取证书。

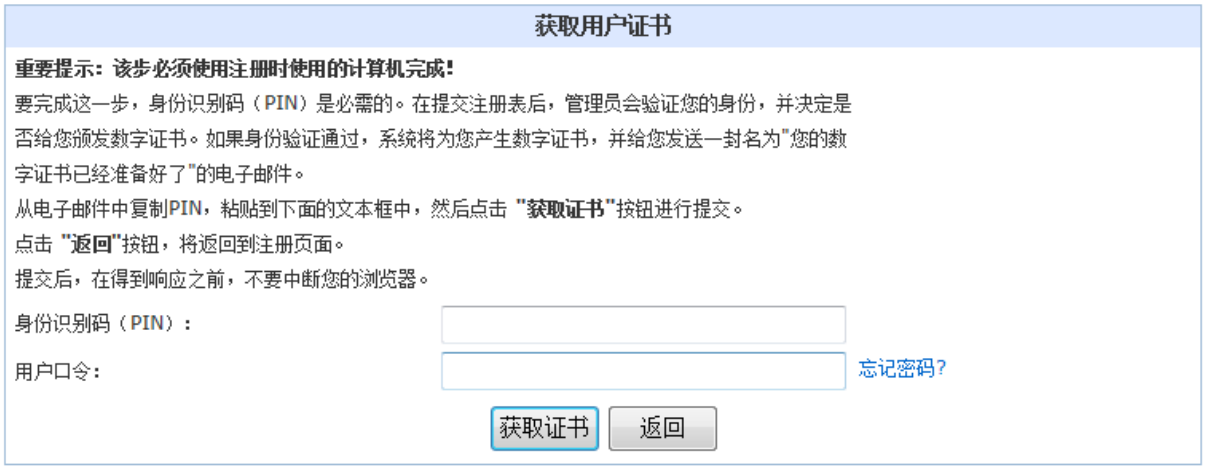

图 2- 5 获取用户证书

获取成功，显示如 **Error! Reference source not found.**所示，该页面中将包含您所获得的证书信息（若是双证书，页面将显示加密证书的序列号）。如此步骤获取证书失败，请继续点击“获取证书”进行证书获取，或者点击“返回”重新进行证书获取操作。

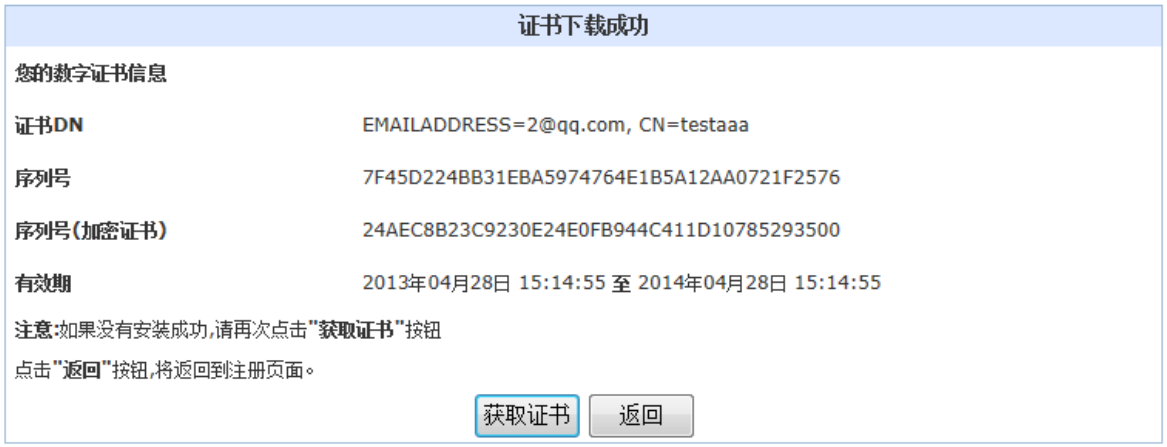

图 2- 6 获取成功

2.5. 查询用户证书

在用户证书服务中心页面点击“查询用户证书”，进入证书查询页面，如图 2- 7。输入电子邮件或用户名，并选择需要的筛选条件，点击查询即可查询打到符合条件的用户证书。查询用户证书支持两种方式：根据电子邮件查询和根据用户名称查询。

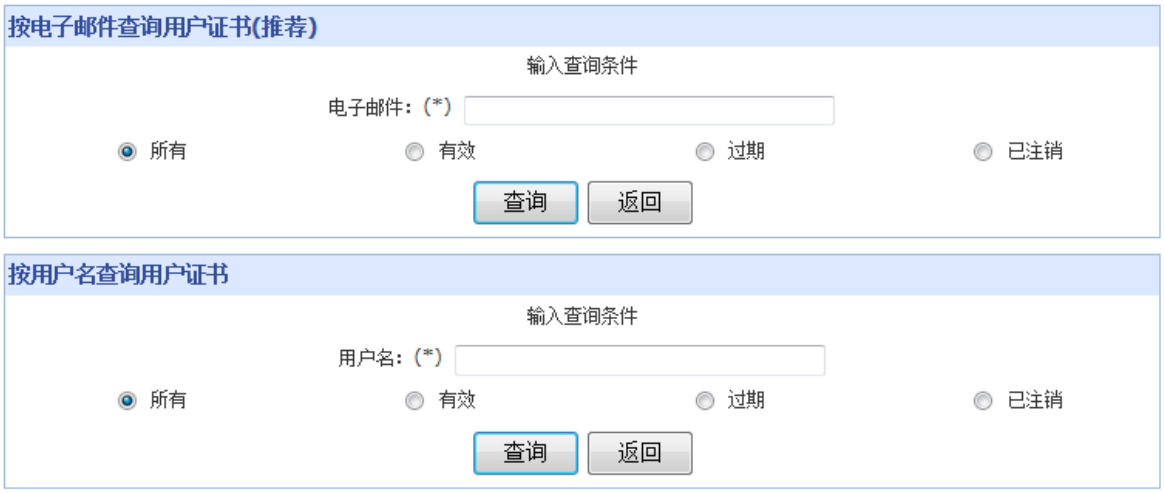

图 2- 7 查询用户证书页面

查询到符合条件的数字证书后显示（根据电子邮件查询），如图 2- 8Error! Reference source not found.

图 2- 8 根据电子邮件查询的结果

2.6. 更新用户证书

在用户证书服务中心页面点击“更新用户证书”，进入更新用户证书页面，如图 2- 9，页面自动检测出本地在 30 天以内即将到期的证书，若系统不存在 30 天以内的证书，则选择更新证书列表显示没有找到数字证书。通过下拉菜单中选择您所要更新的证书，然后点击“更新”按钮即可提交更新证书申请。

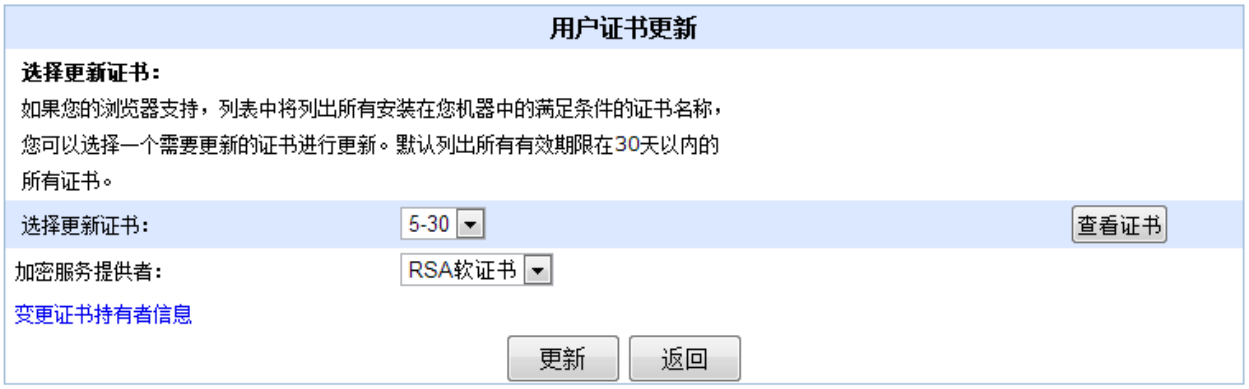

图 2- 9 用户证书更新

更新证书请求提交后，提交的申请被 RA 管理员批准后，系统会自动将获取证书的 PIN 码发到您注册时填写的邮箱中。更新证书获取流程，参见本文档 2.4 获取用户证书。

点击“变更证书持有者信息”链接，显示修改证书持有者信息项，单位名称、部门名称不允许修改，如图 2- 10。若需要变更单位名称和部门名称信息重新申请新证书。点击“修改”，进入信息编辑状态，点击“确认”完成信息修改。

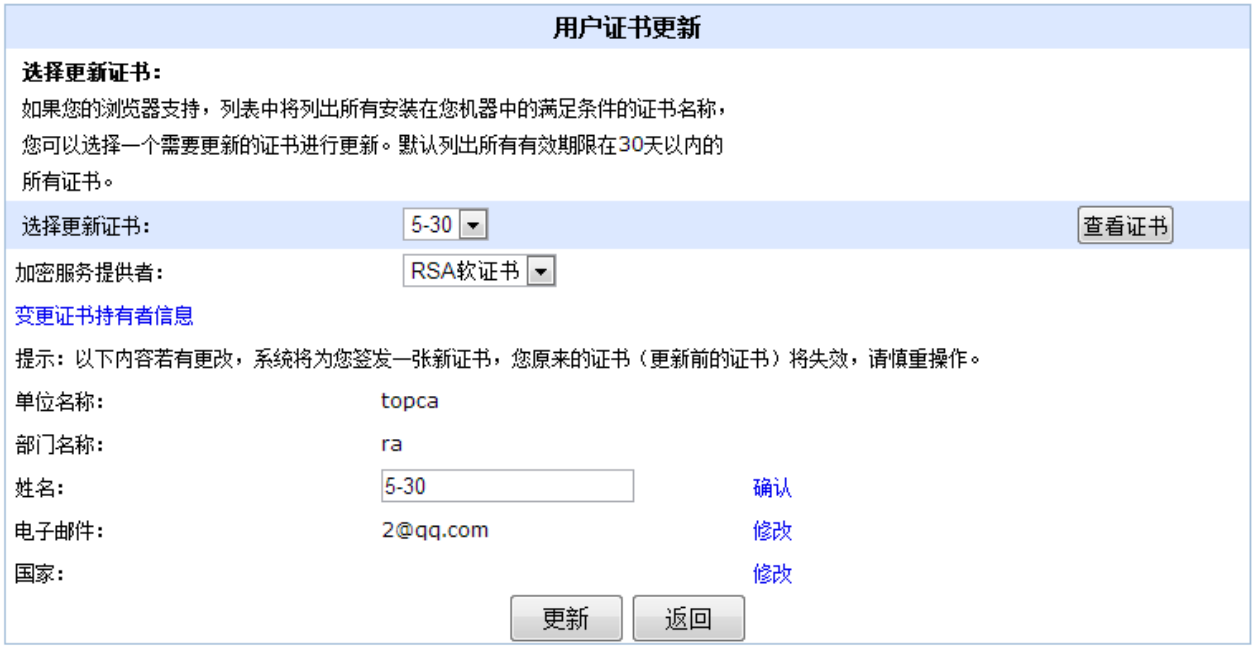

图 2- 10 变更证书持有者信息

2.7. 吊销用户证书

在用户证书服务中心页面点击“吊销用户证书”，进入用户证书查询页面，如图 2- 11。证书查询操作参考本文档 2.5 查询用户证书。

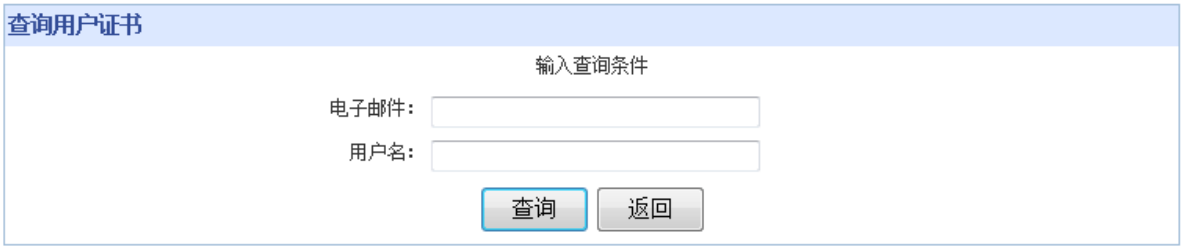

图 2- 11 吊销查询页

点击需要吊销的用户证书，进入吊销证书页面，如 **Error! Reference source not found.**。

图 2- 12 吊销页面

确定需要吊销的证书后，输入用户口令，并选择吊销证书的原因，然后点击“吊销”按钮。吊销成功后将提示您证书吊销成功；若吊销失败，则会返回失败原因。

2.8. 恢复加密证书

该功能仅为您的用户证书为“双证书”时方有效，并且仅能恢复加密证书。

恢复加密证书的前提是，此时您已获得恢复证书的授权码。

授权码是 KMC 系统管理员经过创建密钥恢复申请-管理员批准后产生的一个授权恢复操作码，使用后立即作废。

打开恢复加密证书页，如图 2- 13，选择恢复的（加密）证书时使用的签名证书，输入授权码，点击确定即可完成加密证书的恢复。

图 2- 13 恢复加密证书

2.9. 安装 CA 证书链

在用户证书服务中心点击“安装 CA 证书链”将打开如图 2- 14 的页面，点击确定即可完成证书链安装。安装成功，则在查看证书路径时，证书的上级及根证书存在该路径上。

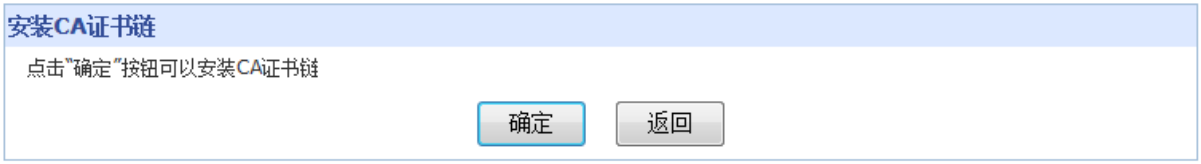

图 2- 14 安装证书链

2.10. 下载证书吊销列表（CRL）

点击“下载证书吊销列表”，页面将弹出打开或保存的提示框，您可以直接打开或将该吊销列表文件保存指定目录下，保存成功的文件是扩展名为.crl 的文件。打开证书吊销列表（CRL），您可以查看该 CRL 列表的常规信息和吊销列表信息，如图 2- 15，图 2- 16。

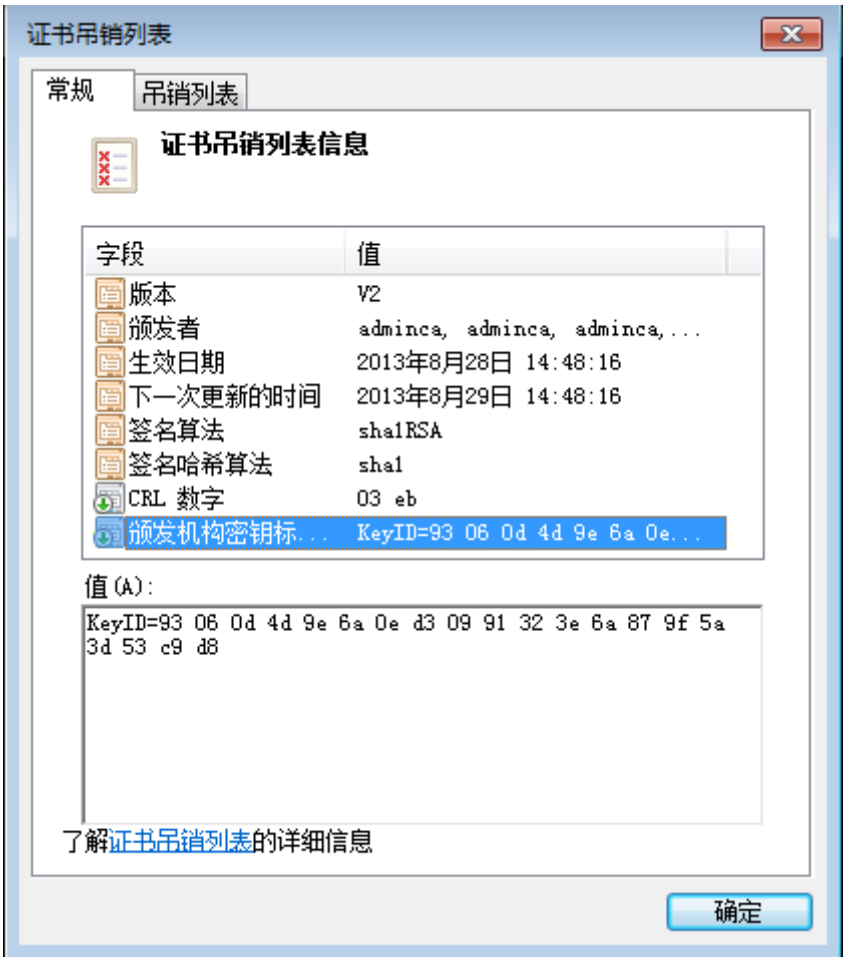
证书吊销列表
常规
吊销列表
证书吊销列表信息
字段
值
版本
V2
颁发者
adminca, adminca, adminca, ...
生效日期
2013年8月28日 14:48:16
下一次更新的时间
2013年8月29日 14:48:16
签名算法
sha1RSA
签名哈希算法
sha1
CRL 数字
03 eb
颁发机构密钥标...
KeyID=93 06 0d 4d 9e 6a 0e...
值(A):
KeyID=93 06 0d 4d 9e 6a 0e d3 09 91 32 3e 6a 87 9f 5a
3d 53 c9 d8
了解证书吊销列表的详细信息
确定

图 2- 15 证书吊销列表

图 2- 16　证书吊销列表 1

2.11. 证书替换

证书替换即当用户的证书丢失或损坏后，用户“重新获取与原证书信息相同的剩余有效期证书”的操作。点击证书替换，进入证书替换申请页面，如

图 2- 17。证书替换需要以下几个步骤，完成证书替换操作。

图 2- 17　证书替换申请

1、填写替换申请

输入姓名（企业证书为公司名称）和电子邮件，提交成功后，系统将通过邮件的方式将确认替换申请信息的邮件发送至用户邮箱，如图 2- 18。

图 2- 18 证书替换邮件提示

2、确认替换申请

用户点击确认替换申请信息的邮件中的链接地址，进入“确认替换申请”页面，如图 2- 19。若邮件中的链接地址不正确，请登录 RA 管理员控制中心系统设置—帐户配置，配置帐户的证书服务地址。

图 2- 19 确认替换申请

3、吊销被替换的证书

在所需要替换的证书信息页面右上方点击“吊销证书”，进入吊销证书页，如**图 2- 20**。输入用户证书口令，选择吊销原因， 吊销需要替换的证书原证书，吊销成功，进入申请证书替换页，如**图 2- 21**。若您取消该次替换操作，点击“返回”进行取消该次操作。

注：在替换证书之前，系统需将需要替换的证书进行吊销操作，吊销后该证书不可用，请在吊销之前确认是否进行替换。

图 2- 20 吊销原证书

图 2- 21 申请替换

4、获取证书

选择加密服务提供者，点击申请替换，完成证书替换申请操作，加密服务提供者需与原证书一致。

A．AA 模式或自动验证

若在配置文件中已配置了开启 AA 模式或在证书配置中已配置验证方式为自动验证，申请替换成功，则直接下载安装已替换成功的证书。申请替换失败，则提示失败信息。

B．审批模式

申请替换成功， 提示替换请求已发送成功。此时，需要等待管理员批准该请求。管理员批准该请求后，系统将会把包含证书 PIN 码的邮件发送到您填写的邮箱。您通过该 PIN 码在获取用户证书页获取已成功替换的证书。获取成功，则完成证书替换操作。

2.12. 证书预览

证书预览即展示证书常规信息和详细信息。点击“证书预览”，进入证书预览页，如图 2- 22，默认显示证书的常规信息。证书下拉列表罗列了系统已经签发的所有证书，通过“刷新证书列表”可手动更新该证书列表。

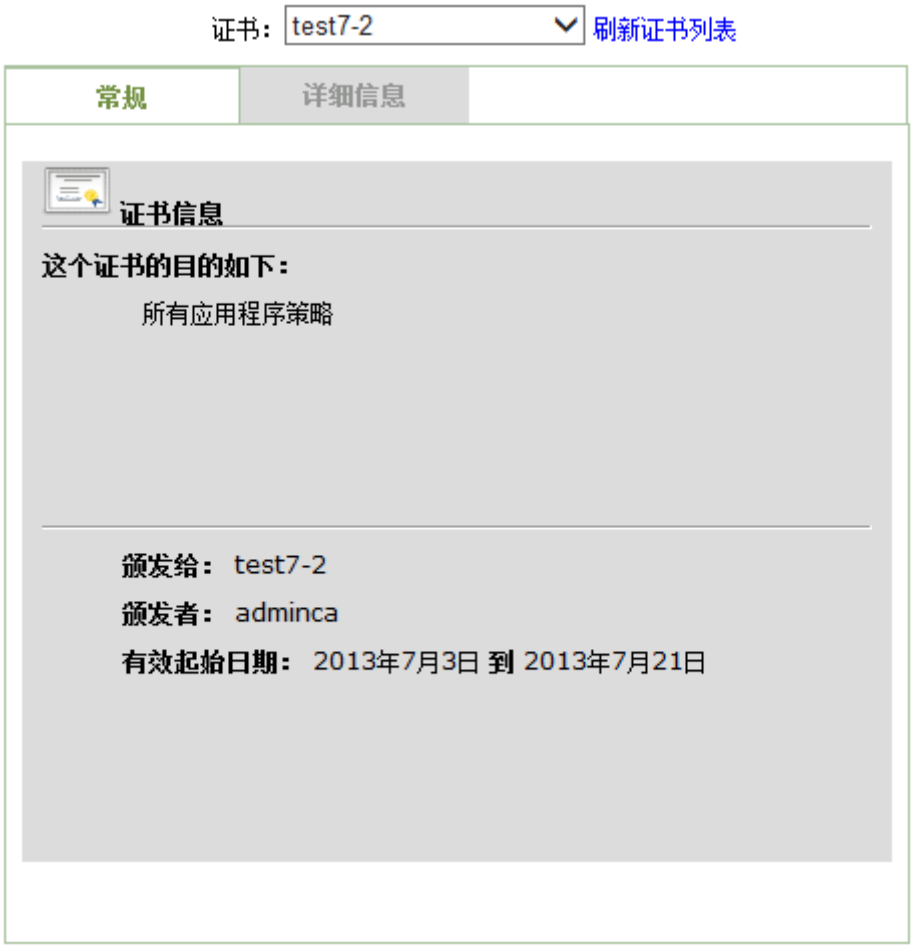

图 2- 22 证书预览

点击“详细信息”可查看证书各个属性及属性的详细信息，如图 2- 23。点击域和值中任意一行，显示该项的完整信息。

图 2- 23 证书详细信息预览

3. 服务器证书服务中心

在开始使用服务器证书服务之前，需要向上级 RA 系统申请服务器证书服务。

注：服务器证书只支持用户申请-管理员审批方式，不支持 AA 模式、passcode 模式、管理员集中制证、管理员批量制证等方式。

3.1. 服务器证书服务中心

服务器证书服务中心即为服务器提供申请数字证书的站点，在使用该服务之前，需登录该系统。访问“http://ip:port/TopCA/serverEnroll ”，进入登录页面，如图 3- 1，在输入框中输入帐户 O 或 OU 关键字，进行实时查找帐户，在结果列表中选择帐户进行登录。登录成功，进入服务器证书服务中心，如图 3- 2。

图 3- 1 登录页面

图 3- 2 服务器证书服务中心首页

3.2. 服务器证书服务中心功能结构

服务器证书服务中心将显示以下几个功能：

- 申请服务器证书
- 查询服务器证书
- 吊销服务器证书
- 下载 CA 证书链

- 下载证书吊销列表（CRL）

3.3. 申请服务器证书

在服务器证书服务中心页面点击“申请服务器证书”，进入申请服务器第一步，如图 2-3，输入在服务器上产生的 CSR，点击确定后提交。提交成功，此时页面上将显示申请服务器证书页面，如图图 3- 4，在该页面上将显示从上一步提交的 CSR 解析出的服务器证书申请信息，如单位、部门、国家等项，如 CSR 中包含邮件地址项，此时电子邮件输入框将显示解析出的值。如发现电子邮件地址不正确，可进行修改。

未勾选服务器证书申请协议时，不显示提交按钮，勾选服务器证书协议后，将显示提交按钮。输入所需信息，完成提交。提交成功后，提示请您查收申请确认邮件。

图 3- 3 输入服务器证书 CSR

图 3- 4 申请服务器证书页面

3.4. 查询服务器证书

在服务器证书服务中心页面点击“查询服务器证书”，进入证书查询页面，如图 3-5。输入电子邮件或服务器证书用户名，并选择需要的筛选条件，点击查询即可查询打到符合条件的服务器证书。查询服务器证书支持两种方式：根据电子邮件查询和根据服务器证书名称查询。

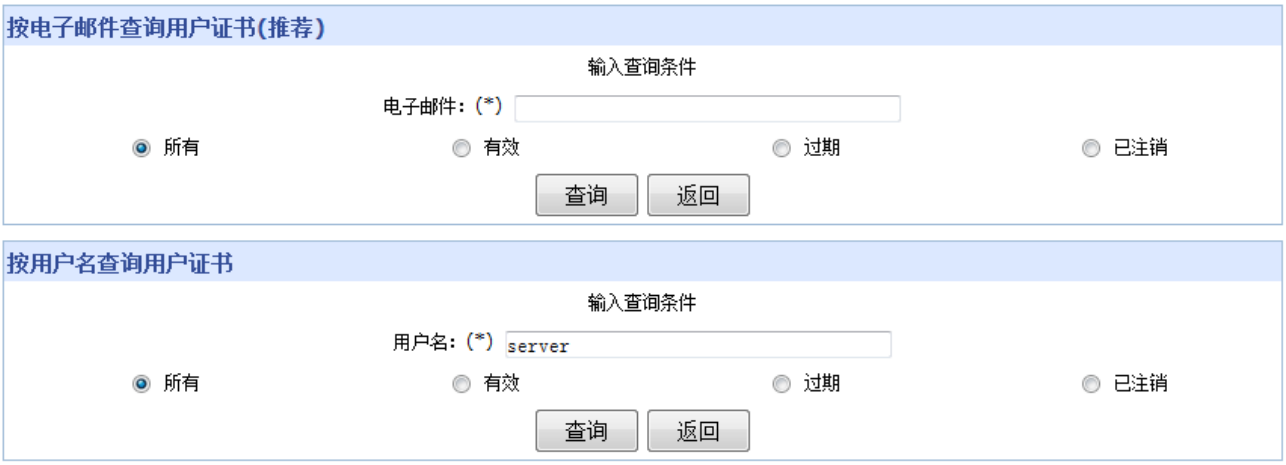

图 3- 5 查询服务器证书页面

查询到符合条件的数字证书后显示（根据服务器证书名称查询），如图 3- 6。

图 3- 6 根据服务器名称查询的结果

3.5. 吊销服务器证书

在服务器证书服务中心页面点击“吊销服务器证书”，进入服务器证书查询页面，如图 3- 7，输入服务器证书的电子邮件地址或服务器证书名称进行查询，查询结果如图图 3- 8。

点击需要吊销的证书名称，进入吊销证书页面。确定需要吊销的证书后，输入用户口令，并选择吊销证书的原因，然后点击“吊销”按钮。吊销成功后将提示您证书吊销成功；若吊销失败，则会返回失败原因。

图 3- 7　吊销查询页

图 3- 8　吊销页面

3.6. 下载 CA 证书链

在服务器证书服务中心点击“下载 CA 证书链”将打开如图 3- 9 的页面，此时页面提示保存名称为 certChain.p7b 的文件，直接选择保存的路径即可。打开该文件可看到服务器证书的上级证书链（包含多张证书），如图图 3- 10。

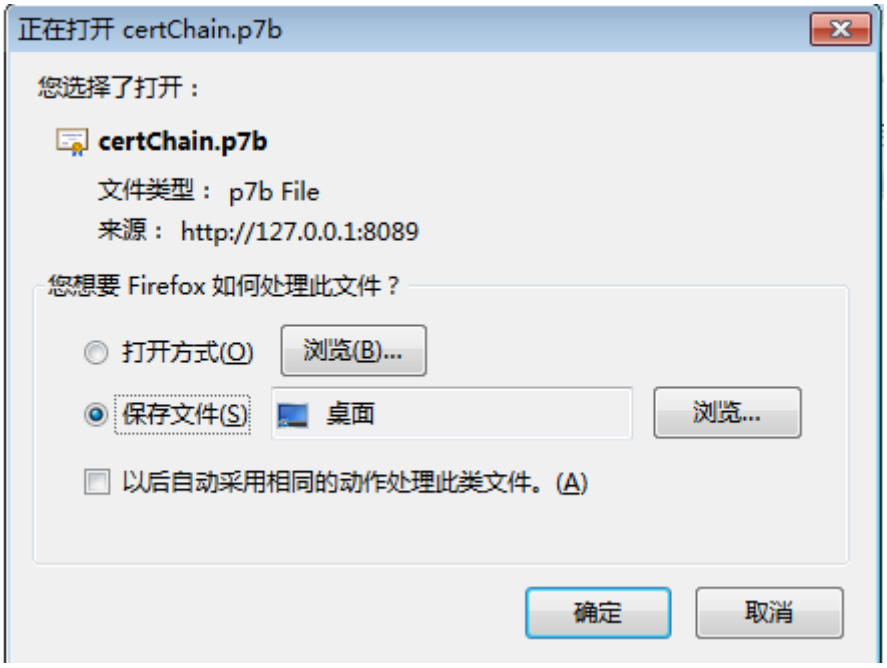

图 3- 9　下载服务器证书链

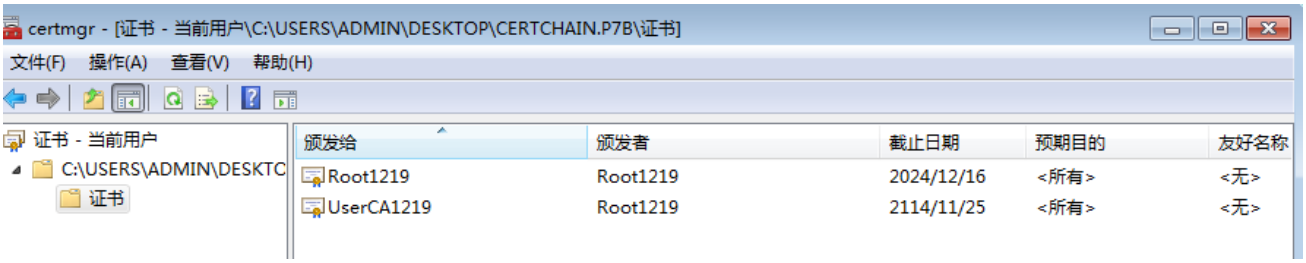

图 3- 10　打开服务器证书链

3.7. 下载证书吊销列表

点击“下载证书吊销列表”，页面将弹出打开或保存的提示框，您可以直接打开或将该吊销列表文件保存指定目录下，保存成功的文件是扩展名为.crl 的文件。打开证书吊销列表（CRL），您可以查看该 CRL 列表的常规信息和吊销列表信息，如图 3- 11，图 3- 12。

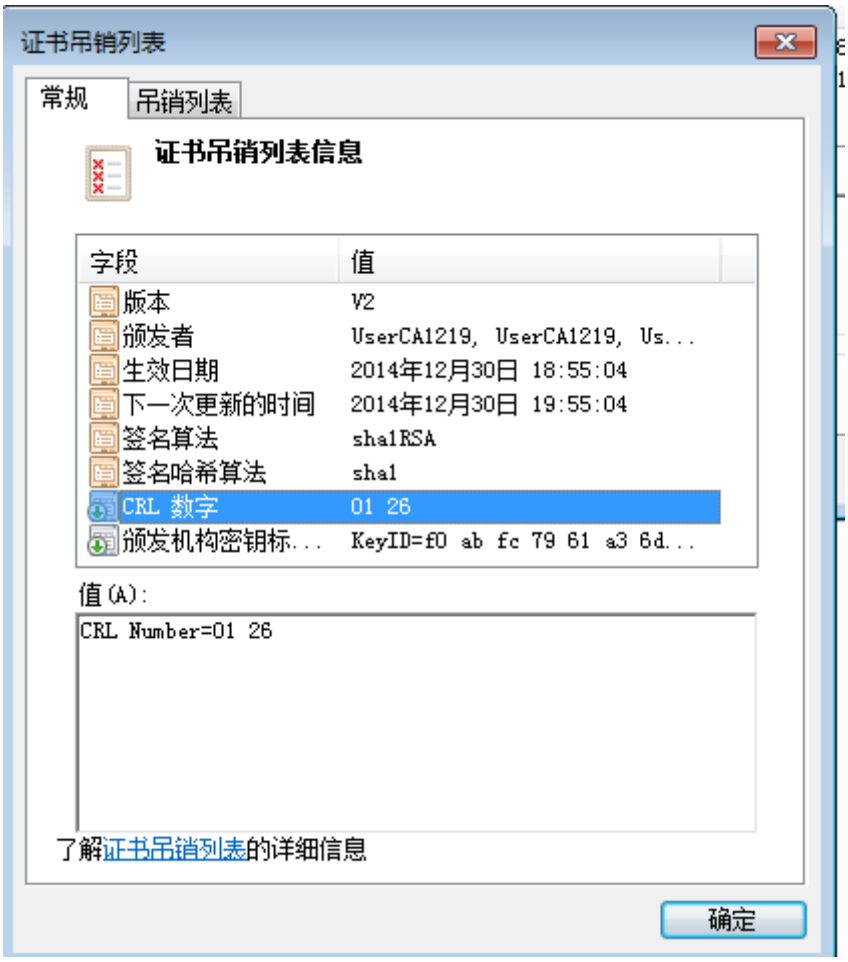
证书吊销列表
常规
吊销列表
证书吊销列表信息
字段
值
版本
V2
颁发者
UserCA1219, UserCA1219, Us...
生效日期
2014年12月30日 18:55:04
下一次更新的时间
2014年12月30日 19:55:04
签名算法
sha1RSA
签名哈希算法
sha1
CRL 数字
01 26
颁发机构密钥标...
KeyID=f0 ab fc 79 61 a3 6d...
值(A):
CRL Number=01 26
了解证书吊销列表的详细信息
确定

图 3- 11 证书吊销列表

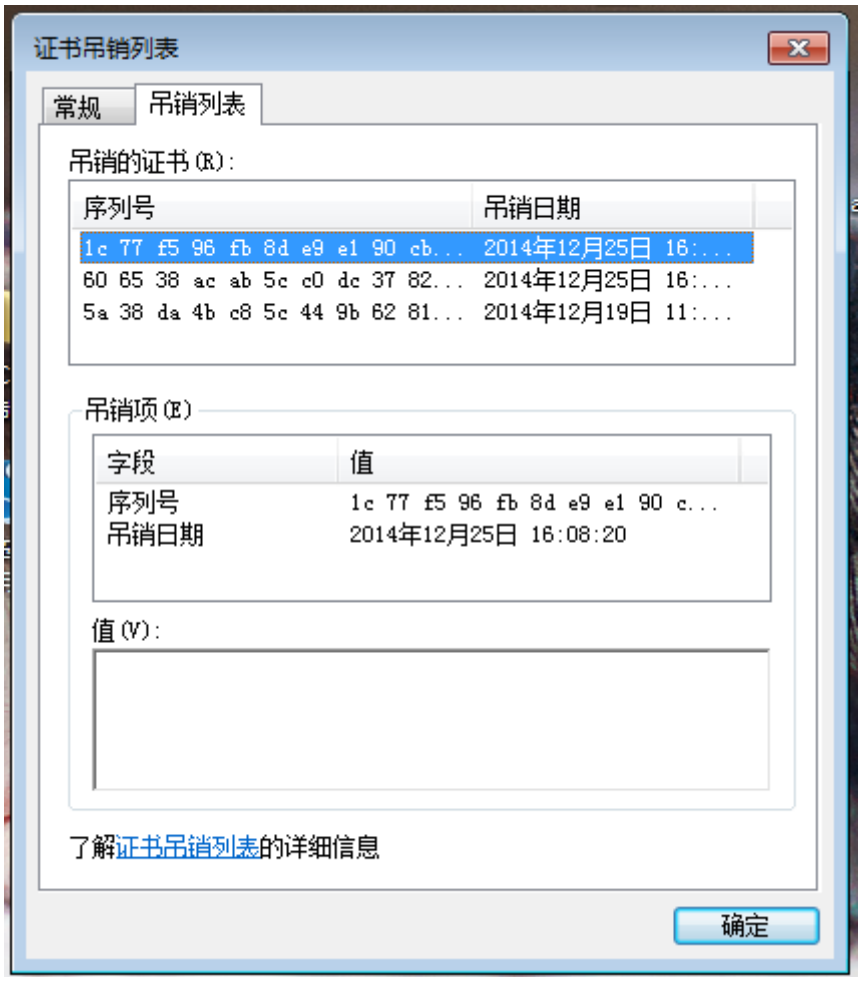

图 3- 12　证书吊销列表 1

4. 常见问题（FAQ）

Q：当安装证书时，无法安装成功，如何处理？

A：需要下载 2 个 ActiveX 控件，所以运行前需要对 IE 进行相应的设置

1) 选择“工具”|“Internet 选项”，打开“Internet 选项”对话框。

2) 单击“安全”选项卡，选择 Internet，然后单击“自定义级别”按钮，如图 4-1，设置如下：

图 4- 1 “Internet 选项”对话框

说明：如果是本地 Intranet，则选择“本地 Intranet”设置内容相同。

3) ActiveX 控件和插件 选项组 需要设置如下内容，如图 4- 2。

- 下载未签名的 ActiveX 控件 —— 提示
- 下载已签名的 ActiveX 控件 —— 启用

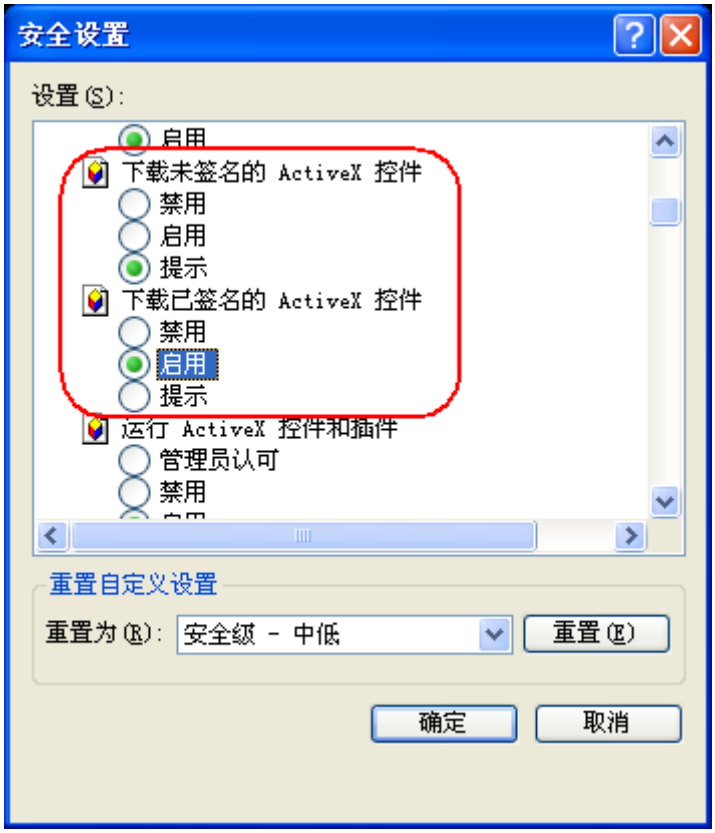

图 4- 2 设置 ActiveX 控件选项组

4) 设置完成后，单击“确定”按钮即可。

程序运行时，当提示下载未签名的 ActiveX 控件时，下载控件即可正常使用。

Q：用户证书服务中心获取用户证书、下载吊销列表、安装 CA 证书链，RA 管理员控制中心签发证书，跳转到错误提示页面，报未知错误。

A：出现该问题一般是因为 topca 的配置文件中 crs 配置的信息有误，请参考以下说明检查配置文件。

- 不加密的 CSR 配置为：Crs.url=http://ip:port/TopCA/crs/crs；
- 加密的 CSR 配置为：Crs.url=http://ip:port/TopCA/crs/evpCrs。

Q：在用户证书服务中心更新用户证书，在选择证书的下拉列表中显示多张同名证书。

A：该现象应该是在更新证书后，未删除证书存储介质中原有证书而引起的正常现象。在更新证书页面所有有效期限在 30 天以内的证书都被过滤显示，如想避免麻烦，可从存储介质中删除原来的证书。