TOPCA V4.0　RA 管理员操作手册

V2.0

目录

1. 前言

RA 管理员手册用来帮助 RA 管理员管理最终用户证书服务。作为 RA 管理员，您的职责就是配置 RA 帐户选项、检查证书请求，并对证书进行管理以及指导用户如何申请、安装证书等。您还要负责对每一申请人的身份进行确认，并决定是批准还是拒绝每一证书请求。

1.1. 关于本手册

本手册的目的是：

- 指导您配置自己的 RA 帐户和证书。
- 指导您批准或拒绝证书请求并帮助用户获得和使用证书。
- 描述一些重要的要求，以便对提交证书请求的个人和组织的身份进行确认。

本手册提供了管理员进行日常操作和向客户提供服务时所需的文档。

2. RA 管理员证书服务中心

访问站点： http://ip /TopCA/raManager 进入 RA 管理员证书服务中心，进入时需输入帐户信息，。

RA 管理员证书服务中心功能包含：申请帐户、申请管理员、申请时获取管理员证书、更新时获取管理员证书、更新管理员证书、查询管理员证书、安装 CA 证书链、下载吊销列表、下载 CA 通信证书，证书替换等功能，如**图 2- 1**。

图 2- 1　RA 管理员证书服务中心首页

2.1. RA 管理员证书服务中心功能结构

RA 管理员证书服务中心包含以下几个功能：

- 申请帐户
- 申请管理员
- 申请时获取管理员证书
- 更新管理员证书
- 更新时获取管理员证书
- 查询管理员证书
- 安装 CA 证书链
- 下载吊销列表（CRL）
- 下载 CA 通信证书
- 证书替换

2.2. 申请帐户

在 RA 管理员证书服务中心页面点击“申请帐户”，进入 RA 帐户申请页，如图 2- 2。输入必填信息（带*号为必填项），提交帐户申请后，系统会向帐户信息中填写的邮箱发送待批准邮件。

图 2- 2　申请帐户

2.3. 申请管理员

管理员证书可用于管理您的 RA 帐户，该单位和部门名称必须与 RA 帐户的单位和部门名称一致。RA 帐户初始管理员数量为 1，当 RA 帐户已存在初始管理员时，增加管理员只能申请额外管理员。其中，额外管理员的数量是无限制的，且可根据需要对额外管理员进行角色分配，完成管理员职责。

在 RA 管理员证书服务中心页面点击“申请管理员”，进入管理员证书申请页，如图 2-3。输管理员信息和口令，点击“确定”进行申请额外 RA 管理员。申请成功，CA 系统自动向管理员信息中邮箱发送申请邮件。

图 2- 3 申请管理员

2.4. 申请时获取管理员证书

RA 帐户或额外管理员证书申请被批准后，系统自动给申请时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 RA 管理员证书服务中心页面点击“申请时获取管理员证书”，进入操作页面，如图 2-4。，复制邮件中 PIN 码后，在“身份识别码（PIN）”中，粘贴 PIN 码，输入用户口令，选择正确的加密服务提供者。

说明：RA 帐户或额外管理员证书申请被批准后，您填写的邮箱会收到有 PIN 码的邮件。

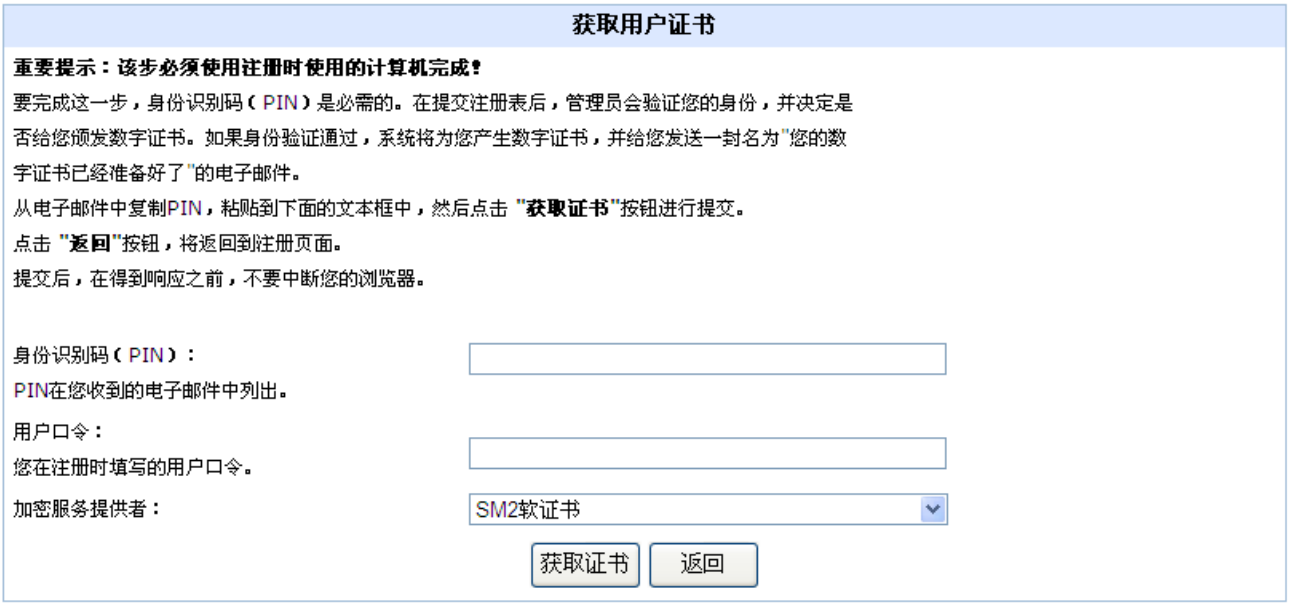

图 2- 4 申请时获取管理员证书

点击“获取证书”后， 进入下一步操作。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，如图 2- 5。

图 2- 5 获取证书成功

2.5. 更新管理员证书

本系统将默认列出所有有效期限在 30 天内的所有证书，您可以在本页面进行即将到期证书的更新，点击“更新管理员证书”进入操作页面，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，如图 2- 6。

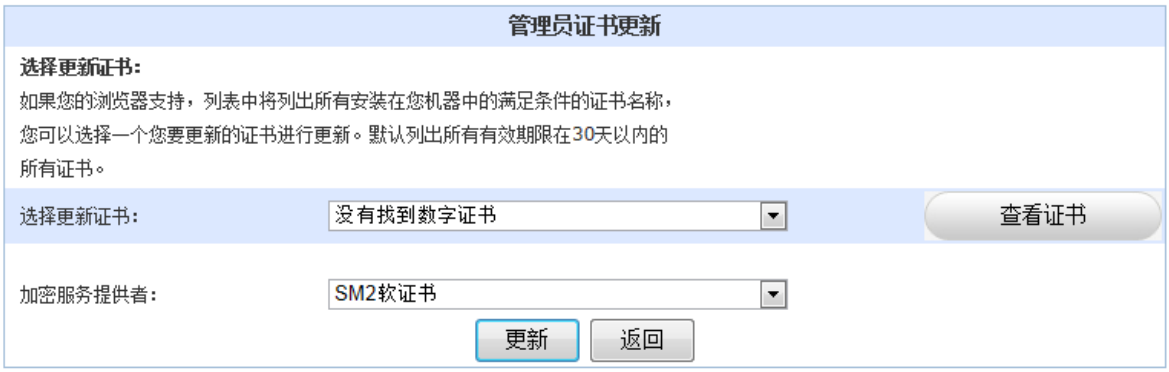

图 2- 6 更新管理员证书

2.6. 更新时获取管理员证书

管理员证书更新成功后，继续进行证书的获取。请点击“更新时获取管理员证书”进入操作页面。注册时您填写的邮箱已经收到有 PIN 码的邮件，复制此 PIN 码后，返回“注册中心管理员证书服务中心”页面，点击“更新时获取管理员证书”，在“身份识别码（PIN）”中，粘贴邮箱中的 PIN 码，输入用户口令，点击“获取证书”， 如图 2- 7。

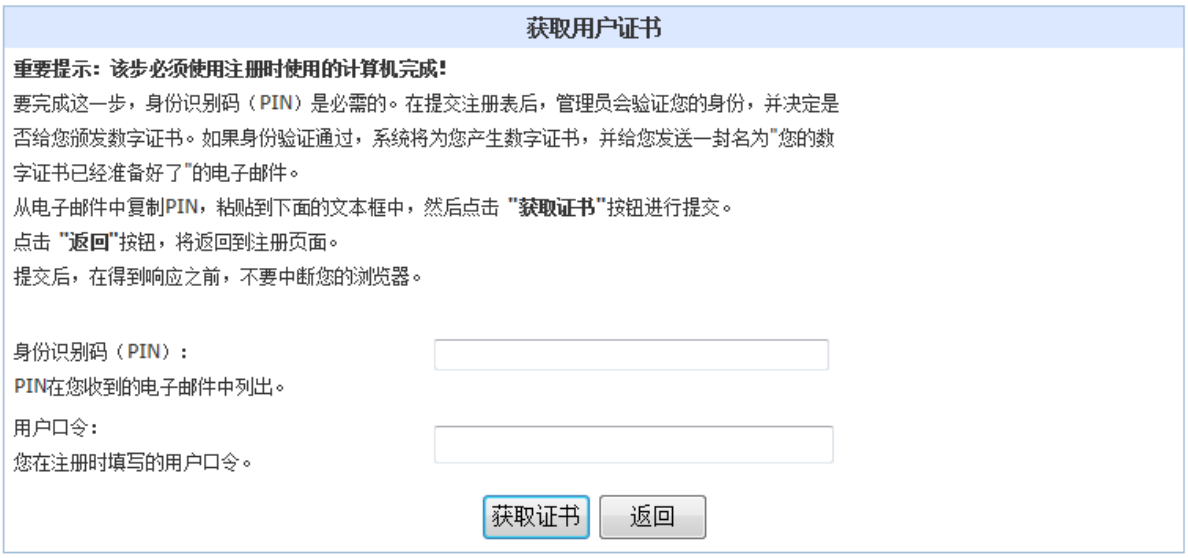

图 2- 7　更新时获取管理员证书

点击“获取证书”后， 进入下一步操作。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，如图 2- 5。

2.7. 查询管理员证书

本系统提供查询管理员证书功能，请点击“查询管理员证书”进行所有证书、有效证书、过期证书、已吊销证书的查询，如图 2-8。

图 2-8 查询管理员证书

进入“查询管理员证书”页面后，输入用户名或者电子邮件，选择对应的证书状态，点击“查询”即可查询到您需要的证书信息，支持用户名或电子邮件两者的组合进行查询过滤，并支持模糊查询，如图 2-9。

图 2-9 查询管理员证书结果

2.8. 安装 CA 证书链

本节为安装 CA 证书链的功能，如需要安装请点击“安装 CA 证书链”，进入操作页面，如 **Error! Reference source not found.**。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- 10 安装 CA 证书链

2.9. 下载吊销列表

本系统提供“下载吊销列表”功能，请点击“下载吊销列表”获取证书吊销列表。您可以选择直接查看，或保存到本地。打开吊销列表，可查看吊销列表的常规信息，如颁发者、生效时间、签名算法等项，如图 2- 11 ；可查看吊销列表中已吊销的证书信息，如证书序列号、吊销时间等项，如图 2- 12。

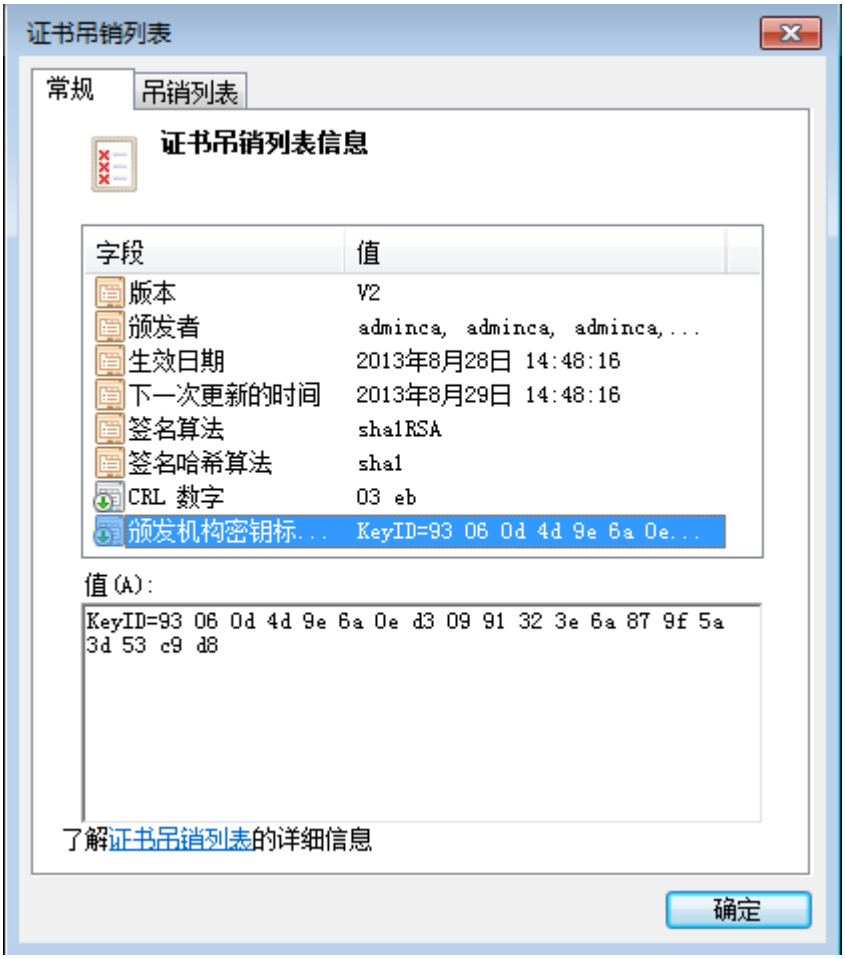

图 2- 11 证书吊销列表

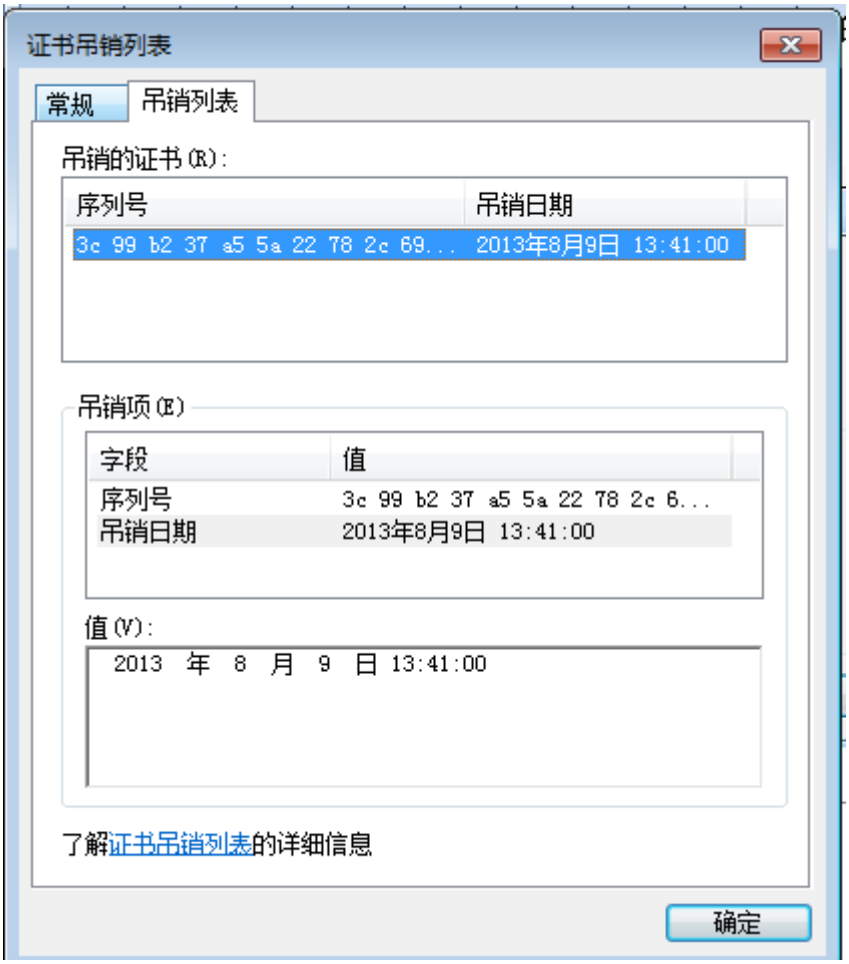

图 2- 12 证书吊销列表 1

2.10. 下载 CA 通信证书

本系统提供“下载 CA 通信证书”功能，请点击“下载 CA 通信证书”获取，如图 2- 13，点击保存，将该证书保存到指定位置，下载成功后，在指定位置生成一个.Cer 文件。

图 2- 13 下载 CA 通信证书

2.11. 证书替换

证书替换即当 RA 管理员的证书丢失或损坏后，RA 管理员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，如

图 2- 14。证书替换需要以下几个步骤，完成证书替换操作。

图 2- 14 证书替换申请

1、输入姓名和电子邮件，点击“提交”，系统通过邮件的方式将确认替换申请信息发送至 RA 管理员邮箱，并提示 RA 管理员查收邮件，如**图 2- 15**，提交申请后，您还可以返回到首页进行其他操作。

图 2- 15 证书替换邮件提示

2、RA 管理员打开邮件，点击邮件里的链接地址（若邮件中的链接地址不正确，请到管理员控制中心帐户管理—查询编辑帐户页，配置帐户证书服务地址），进入替换确认页，如图 2- 16。

图 2- 16 确认替换申请

3、点击“吊销证书”，进入吊销证书页，如图 2- 17。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- 18。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- 17　吊销原证书

图 2- 18　申请替换

4、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。

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。

注：加密服务提供者需与原证书一致。

3. 使用 RA 控制中心

在开始使用 RA 服务之前，需要向上级 CA 系统申请 RA 服务。作为 RA 服务注册过程的一部分，您将得到一张 RA 管理员证书，它将确保您与 RA 控制中心的通信安全可靠。在下载安装了 RA 管理员证书之后，您则可以准备访问控制中心进行管理工作。

3.1. 使用 RA 控制中心

与 RA 连接的接口是基于 Web2.0 标准开发的 RA 控制中心。在管理您组织的 RA 服务时，该接口是执行所有任务的接口。只有 RA 管理员才有权通过使用 CA 系统提供的 RA 管理员证书，访问特定的控制中心页面。RA 控制中心通过 RA 管理员证书来验证 RA 管理员的身份。

管理员登录管理中心后将显示图 3-1 所示界面，左侧是当前管理员所能操作的链接，包括证书管理、处理请求、通行码管理、系统设置、管理员管理，点击不同的链接，右侧主窗体中将打开相应的操作界面。页面右上方显示的是当前登录管理员所属的帐户信息以及管理员名称。

图 3-1 RA 控制中心

3.1.1. RA 控制中心功能

要访问控制中心，您需要使用浏览器访问指定的 URL。此 URL 在安装时已指定，例如：http://ica3-ra.itrus.com.cn 。控制中心会通过您所提供的管理员证书来校验您的身份，证书验证通过后即可进入控制中心。

管理员角色权限包括证书管理和安全管理两个类型角色。其中具有证书管理权限的管理员可对证书、请求、通行码、系统设置等项进行管理，具有安全管理权限的管理员可对管理员进行管理。

缺省情况下，帐户的第一个管理员拥有全部权限。当添加一个管理员时，缺省的额外新管理员都需要初始管理员来赋予权限，该操作是在“管理员角色设置”中完成的。

成功登录控制中心后，会在页面右上方显示当前管理员所管理的 RA 帐户信息。如图 3-1 所示，控制中心包括以下几个组成部分：

- 证书管理
- 处理请求
- 通行码管理
- 系统设置
- 管理员管理

注：具有证书管理权限的管理员，登录成功后，显示证书管理、请求处理、通行码管理、系统设置四项。

具有安全管理权限的管理员，登录成功后，显示管理员管理一项。

具有证书管理和安全管理权限的管理员，登录成功后，显示全部项。

以下分别介绍各项：

- 证书管理

管理员使用本项进行每天的证书管理工作，如证书的查看、吊销、挂起、恢复以及注册用户证书和证书发行量查询等等。

- 处理请求

管理员使用本项对新请求、更新请求、替换请求进行处理，查看等操作。

- 通行码管理

管理员使用通行码管理模块可以对通行码进行管理操作，如管理通行码策略，创建通行码向导，查看通行码和批量制证等工作。

- 系统设置

管理员使用该项可以对帐户进行重新初始化，修改数据字典的操作。

- 管理员管理

安全管理权限的管理员使用本项进行管理员角色设置和管理员操作审计等操作。

3.1.2. RA 管理员的职责

作为一个 RA 管理员，您要负责对申请证书的每一个人、组织的身份进行确认。一般来说，每个组织都会预先保存着有关其雇员的信息，这些信息大多数情况下可以用来鉴别申请人员的身份，从而决定批准或拒绝证书请求。

3.2. 证书管理

您一旦定制了证书注册页面，我们将认为您已经准备好为您的用户提供证书管理服务。本章将对 RA 管理员管理证书所必须执行的日常工作和按需执行的工作进行详细的介绍。

证书管理部分提供以下功能，我们将在本章中分节对这些功能进行详细介绍。

- 查看证书
- 吊销证书
- 挂起证书
- 恢复证书
- 注册用户证书
- 证书发行量查询

3.2.1. 查看证书

在“证书管理”模块，点击“查看证书”链接，将在右侧主窗体中打开查找特定证书的页面，如图 3-2，通过输入查询条件查找证书。当控制中心检索出符合搜索标准的证书目录时，您可以查看注册信息和证书的细节，不正确时可以吊销证书。

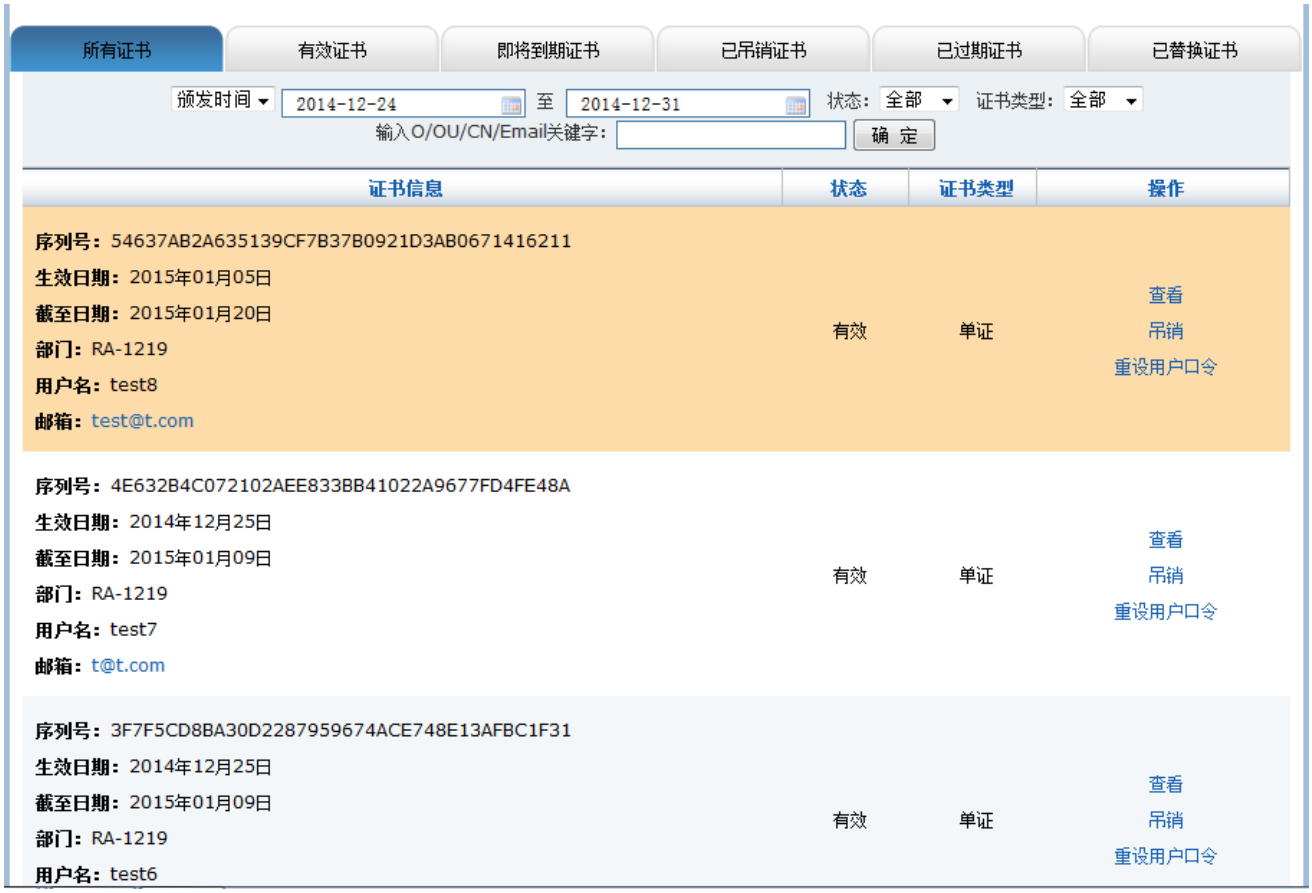

图 3-2　查询证书

您可以通过设置不同的筛选条件，进行过滤证书。通过证书有效期，时间范围、证书类型等组合条件可查询统计该帐户下证书签发情况。此外还可以指定您想查看的证书种类，这些种类包括：

- 所有证书 即所有状态下证书
- 有效证书　即状态为有效的
- 即将到期证书 即满足证书模版设置允许更新的时间，默认为 30 天
- 已吊销证书　即状态为吊销证书
- 已过期证书　即已过期的证书
- 已替换证书　即已完成替换的证书

1)　查看所有证书

通过证书颁发时间范围、证书主题项、证书状态等项进行筛选当前 RA 管理员帐户已签发的证书，支持模糊查询，查询结果以列表分页显示，如图 3-2，可对已筛选出的证书进行操作，如查看证书详细，吊销证书操作。

✓ 查看证书详细

点击“查看”，进入查看证书详情页面，如图 3- 3，可查看证书用户信息、证书信息、base64 编码、管理信息。

图 3- 3 查看证书详情

✓ 吊销证书

点击“吊销”链接，弹出吊销证书操作框，如图 3- 4，选择吊销原因，点击“吊销”，完成证书的吊销。

图 3-4　吊销证书

✓　重设用户口令

点击“重设用户口令”链接，进入重设用户证书口令页面，如图

图 3-5　重设用户口令

2)　查看有效证书

通过证书颁发时间范围或下载时间范围、证书类型等项进行筛选当前 RA 管理员帐户已签发的有效证书，支持模糊查询，查询结果以列表分页显示，如图 3-　6，可对已筛选出的证书进行操作，如查看证书详细，吊销证书操作（同查看所有证书）。

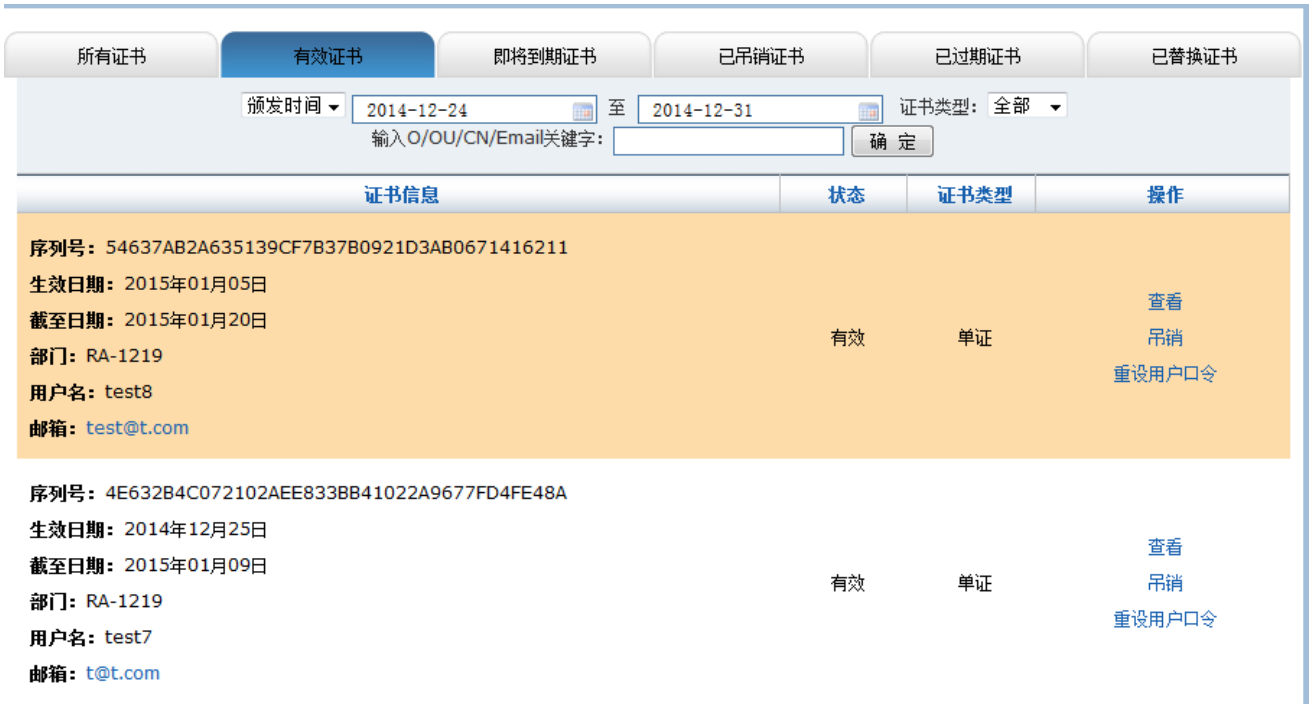

图 3- 6　查看有效证书

3)　查看即将到期证书

通过证书到期时间、证书主题项、证书类型等项进行筛选当前 RA 管理员帐户已签发的即将到期证书，支持模糊查询，查询结果以列表分页显示，如图 3-　7，可对已筛选出的证书进行操作，如查看证书详细（同查看所有证书），更新证书操作。

注：此处默认罗列了到期时间为 30 天以内的证书，可根据需要，进入控制台站点下加载证书模板进行自定义配置。

图 3-7 查看即将到期证书

✓ 更新证书

点击“更新”，弹出更新证书操作框，输入证书有效期，点击“更新”完成更新操作，如图 3-8。

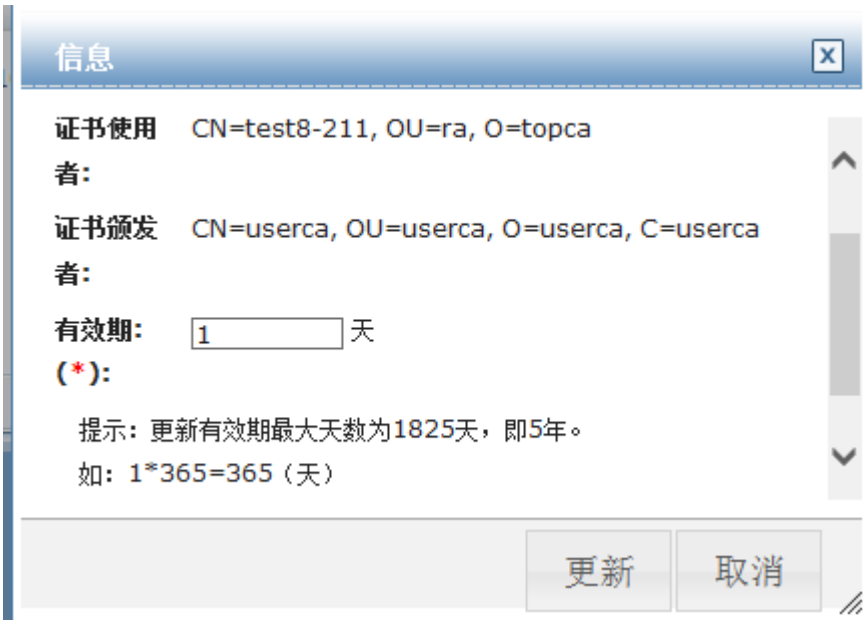

图 3-8 更新即将过期证书

4) 查看已吊销证书

通过吊销时间范围、证书主题项、证书类型进行筛选当前 RA 管理员帐户已签发的已吊销的证书，支持模糊查询，查询结果以列表分页显示，如图 3- 9，可对已筛选出的证书进行操作，如查看证书详细操作（同查看所有证书）。

图 3- 9 查看已吊销证书

5) 查看已过期证书

通过过期时间或有效期范围、证书主题项、证书类型进行筛选当前 RA 管理员帐户已签发的已过期的证书，支持模糊查询，查询结果以列表分页显示，如图 3- 10，可对已筛选出的证书进行操作，如查看证书详细操作（同查看所有证书）。

图 3- 10 查看已过期证书

6) 查看已替换证书

通过过期时间或有效期范围、证书主题项、证书类型进行筛选当前 RA 管理员帐户已签发的已替换的证书，支持模糊查询，查询结果以列表分页显示，如图 3- 11。列表中

将显示替换前和替换后的证书，可对已筛选出的证书进行操作，如查看证书详细、吊销（该项同查看所有证书）操作。

图 3- 11 查看已替换证书

✓ 查看已替换证书详情

点击 “查看”，进入查看已替换证书详细页面，如图 3- 12，该页面显示替换前与替换后证书的详细信息。

图 3- 12 替换证书详情

3.2.2. 吊销证书

在某些情况下，会不允许某人再继续使用证书。作为一个 RA 管理员，您的职责之一就是在这种情况下，决定何时吊销一个证书。如果出现以下任何一种情况，您必须吊销证书：

- 发生丢失、偷窃、修改、非法泄露，或用户私钥的其它泄密现象
- 用户或授权代理人有充分的理由请求吊销证书。
- 对安全站点服务器证书，用户组织名和 / 或区域名已更改。
- 组织名和 / 或区域名注册更改了。

除上述情况外，一般不应吊销证书。

吊销证书是一种不能取消的永久性行为。只有拥有证书管理权限的 RA 管理员，才有权进行吊销证书操作。

注意：可在吊销证书操作完成前的任何时间退出吊销过程。

在“证书管理”页面，点击“吊销证书”链接，在右侧主界面中将可以按照您的需求查找特定的证书，并吊销它。您可以指定用户的姓名或电子邮件地址、证书的序号，或通过指定当时证书签发时的日期范围的方式来查找证书，查询结果如图 3-13。

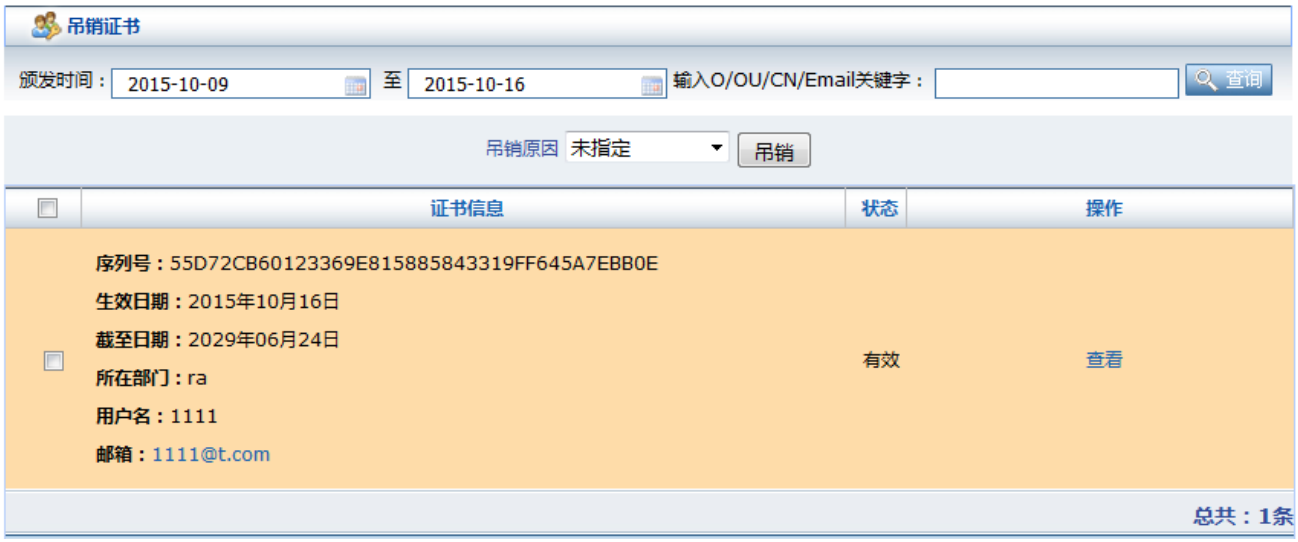

图 3-13　吊销证书页面

在该页面中，只有拥有证书管理权限的 RA 管理员，方能进行这两种操作：

- 点击“查看详情”链接，将打开显示用户的所有注册信息和证书信息的页面。可在此页面中确认这是否是您想吊销的证书。
- 如图 3-14，在该页面下方选择一种吊销理由，然后对证书进行吊销操作。

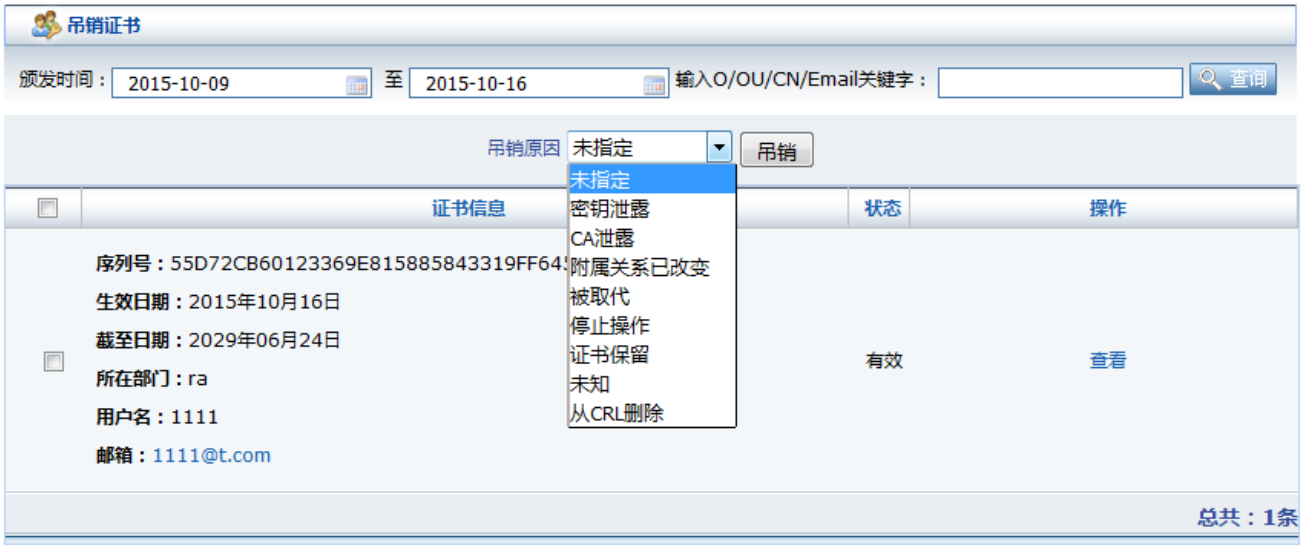

图 3-14　吊销原因

3.2.3. 挂起证书

在某些情况下，某人由于某种原因想使证书暂时不可用，但非永久不可用。作为一个 RA 管理员，您可以进行挂起证书操作。

挂起证书是一种可以取消的暂时行为。只有拥有证书管理权限的 RA 管理员，才有挂起证书的权限。

注意：可在挂起证书操作完成前的任何时间退出挂起过程

在“证书管理”页面，点击“挂起证书”链接，在右侧主界面中将可以按照您的需求查找特定的证书，通过指定用户的姓名或电子邮件地址、证书的序号，或指定当时证书签发时的日期范围来查找证书。查询结果将在右侧主界面中罗列出来，如图 3-15。

图 3-15 挂起证书页面

查找得到的“挂起证书”页面提供以下两种操作，只有拥有证书管理权限的 RA 管理员，方能进行这两种操作：

- 点击“查看详情”链接，右侧主界面中将打开显示用户的所有注册信息和证书信息的页面。可在此页面中确认这是否是您想挂起的证书，然后进行挂起操作。
- 点击“挂起证书”链接，将直接挂起该证书。

3.2.4. 解挂证书

在某些情况下，证书由挂起状态变更为有效状态。作为一个 RA 管理员，您可以对证书进行恢复挂起操作，同 3.2.5 节中“挂起证书”是相反的操作。

解挂证书是一种可以取消的暂时行为。只有拥有证书管理权限的 RA 管理员，才有权解挂证书。

注意：可在解挂证书操作完成前的任何时间退出解挂过程。

在“证书管理”模块，点击“解挂证书”链接，在右侧主界面中将可以按照您的需求，通过指定用户的姓名或电子邮件地址、证书的序号或指定当时证书签发时的日期范围来查找已挂起的证书。如图 3- 16。

图 3- 16　恢复证书页面

查找后的证书页面中，拥有证书管理权限的 RA 管理员可以进行如下两种操作：

- 点击“查看详情”链接，右侧主界面中将打开显示用户的所有注册信息和证书信息的页面。可在此页面中确认这是否是您想恢复的证书。
- 点击“恢复证书”链接，取消证书的挂起状态，恢复证书为有效状态。

注意：恢复证书只能查询到证书状态为 SUSPEND 的证书。

3.2.5. 签发证书

本节将介绍作为管理员的您，直接为最终用户申请证书的操作。在用户证书申请成功后，您即可将其按照通常的证书来进行处理。此处进行的证书注册过程与用户通过用户证书服务中心申请证书的过程是完全相同的，如图 3-17，该页面的用户信息项根据系统设置->注册项配置中显示一致（除 CSR 外）。输入用户证书所需信息，其中带*号必填项。

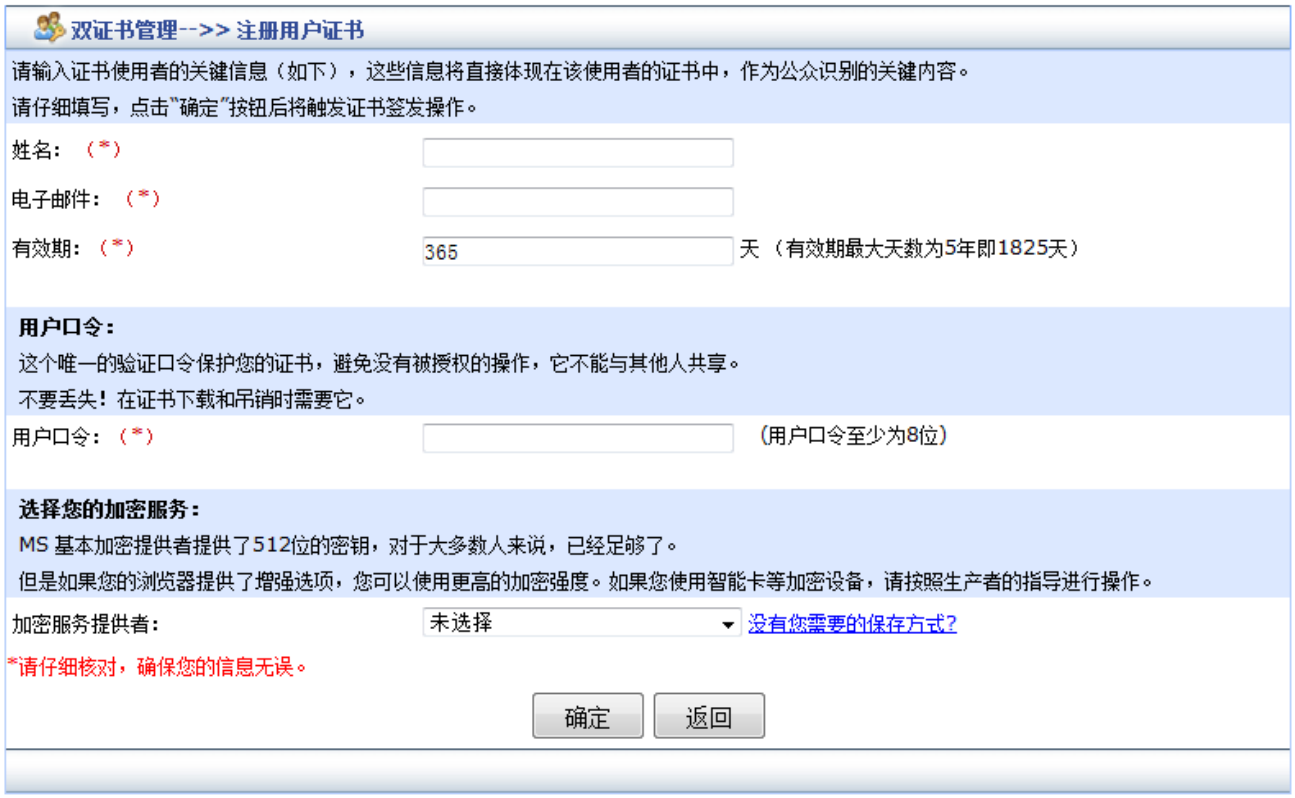

图 3-17　用户信息编辑

签发成功，系统自动将签发的证书安装到指定的证书容器中，如图 3-　18。您可点击“查看证书”，查看该证书的详细信息；点击“返回”，返回到申请证书页面。

图 3- 18 证书签发成功

注：若您帐户配置的是可签发单证书，则签发的证书为单证书。

若您帐户配置的是签发双证书，则签发的证书为双证书。

3.2.6. 证书发行量查询

点击“证书发行量查询”链接，将在右侧主界面显示当前帐户证书发行量的统计情况，如图 3- 19，统计当前管理员所属帐户的订购使用情况及证书发行情况。

其中帐户订购使用情况，统计帐户订购数量、帐户使用情况、帐户剩余数量。帐户订购数量=帐户使用情况+帐户剩余数量。

其中帐户证书发行量查询，统计帐户下证书发行总量、有效证书数量、吊销证书数量、过期证书数量、挂起证书数量。证书发行总量=有效证书数量+吊销证书数量+过期证书数量+挂起证书数量

证书管理-->> 证书发行量查询

一、订购使用量统计

统计证书订购使用情况，详细如下表：（已使用证书记录所有已发行的证书，因此已使用证书数量即为当前帐户下已发行证书总量）

已购买证书数量	已使用证书数量	剩余证书数量
2500张	1张	2499张

二、证书发行量统计

统计当前帐户下各个状态（有效、吊销、过期、挂起）的证书数量及总发行证书数量，详细如下表：

已发行证书数量	有效证书数量	吊销证书数量	过期证书数量	挂起证书数量
1张	0张	0张	0张	1张

图 3- 19 证书发行量查询

3.3. 处理请求

本章介绍拥有管理权限的管理员使用请求的处理，查看，处理申请、替换、更新请求等操作。请您根据您组织的证书批准规则来决定是批准还是拒绝每一个请求。这种方法能确保您在批准并将证书发放给申请用户时，履行自己作为 RA 管理员的职责。

处理请求部分提供以下功能：

- 处理新请求
- 查看新请求
- 处理更新请求
- 查看更新请求

3.3.1. 处理新请求

在“处理请求”菜单下，点击“处理请求”链接，将在右侧主界面罗列出所有未被处理的证书请求（如图 3- 20）。请求类型包括证书申请和证书替换请求。您需要根据您组织的证书批准规则来决定是批准还是拒绝每一个请求。

在进行请求的批准操作时，系统提供单管理员处理或双管理员处理（该项在帐户管理-查询编辑帐户下进行设置）。

✓ 单管理员

当设置为单管理员时，只需当前登录的管理员进行批准操作即可完成请求的处理，如图 3- 20。

图 3- 20 处理请求（单管理员）

✓ 双管理员

当设置为双管理员时，当前登录的管理员进行鉴别操作后，需等待该帐户下另外一个管理员进行验证后才能完成请求的处理，如图 3- 21。

图 3- 21 处理请求（双管理员）

注意：只有拥有证书管理权限的 RA 管理员才能得到进入处理请求页面。

通过“处理请求”界面中的“操作”表格栏，您能完成以下操作：

- 查看注册信息详情。

单击“查看详情”，如图 3- 22，以查看证书申请组织的所有注册信息（参见图 3.2.3，3.2.4）。此信息用来检验用户请求的正确性，并检查当前请求是否与您组织内的证书签发规则一致。

——从本页，您可以更改证书的有效期（默认为一年）。

——您一旦证实了证书申请组织的身份，并证实其它所有打算包含在证书中的信息都是准确的，您就可以批准该请求了。

当帐户设置为单管理员批准时，只需当前登录的管理员进行批准操作即可完成请求，如图 3- 22。当帐户设置为双管理员批准时，当前登录的管理员验证或鉴别操作后，还需等待另外一位管理员进行鉴别或验证操作，才能完成批准操作，如图 3- 23。当您批准了证书请求，CA 系统就将为该帐户签发证书。

注意：如果注册信息中有输入错误或其它细小错误，请拒绝请求，并请申请人提交重新提交新请求，以此确保证书信息的准确性。

图 3- 22　查看详细信息（单管理员）

图 3- 23 查看详细信息（双管理员）

- 批准最终用户的证书请求。

单击“批准”按钮即完成证书请求的批准操作。本操作会将管理员的批准操作请求发送给 CA 系统，证书在 CA 系统产生、签发、并(在公开证书情况下)发布到证书库。然后 CA 系统将自动向申请人邮箱发送一份电子邮件，通知申请人随时可以获得证书。该邮件中包含一个 PIN 码以及 CA 系统“证书下载”页面的 URL。申请人通过 Web 下载证书后，即成功成为一个证书用户。

- 拒绝最终用户的证书请求。

如果您不能对证书请求的正确性/有效性，建议您拒绝该请求。单击“拒绝”按钮，完成拒绝请求操作。RA 管理员将自动向申请人发送一份电子邮件予以说明。

3.3.2. 查看新请求

在“处理请求”页面，点击“查看新请求”链接，您能查看已经处理过的特定证书请求的详细信息（如图 3-24）：

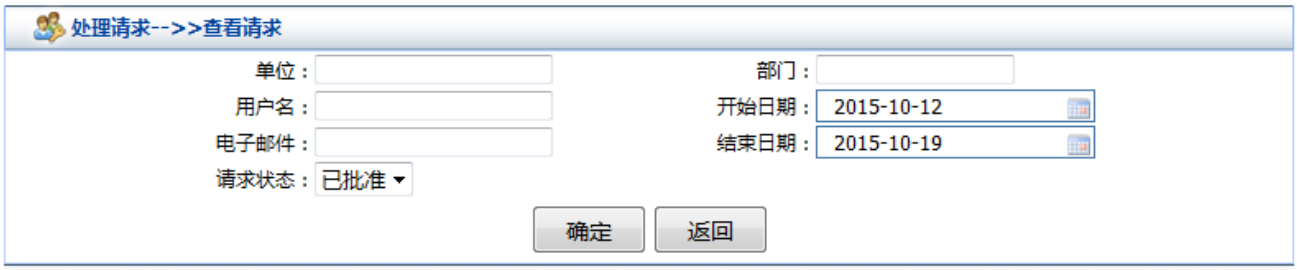

图 3-24　查看请求页面

管理员可根据申请人的姓名或电子邮件地址以及提交请求的时间段来进行精确搜索。

此外，还可根据请求状态进行搜索：

- 待批准：已提交请求，但还没有得到批准或拒绝信息。
- 已拒绝：已提交请求，且已被 RA 管理员拒绝。

对于已拒绝的请求，控制中心将列出所有请求的列表（如图 3-25），这些请求是在您规定的期间内满足搜索标准的。选择操作表格栏中的链接，与 3.3.1 节中描述的“处理请求”页面中的操作相同。已批准的请求，允许在拒绝。

图 3-25　请求列表

- 查看详情：查看请求的详细信息，如图 3- 26。

图 3- 26　已处理请求的详细信息

- 拒绝：已批准的请求，管理员可再次拒绝操作。
- 重发批准邮件：请求被批准后，系统自动给申请人邮箱发送批准邮件，若用户未收到，管理员可通过该功能再次发送批准邮件。点击重发批准邮件时弹出确认邮箱地址信息框，如图图 3- 27 在邮箱地址输入框可编辑修改邮箱地址，点击发送，此时将批准邮件发送到此页面填写的邮箱地址。

图 3- 27 重发批准邮件

- 重设用户口令：当用户口令忘记后，不能对证书进行操作，此时管理员可通过该功能对用户证书口令进行重新设置，设置成功，系统自动将重新设置的口令发送到申请人的邮箱。

3.3.3. 处理更新请求

在“处理请求”页面，点击“处理更新请求”链接，将打开列出所有未处理的证书请求页面。请您根据您组织的证书批准规则来决定是批准还是拒绝每一个请求。这种方法能确保您在批准并将证书发放给申请人时，履行自己作为 RA 管理员的职责。

在进行更新请求的批准操作时，系统提供单管理员处理或双管理员处理（该项在帐户管理-查询编辑帐户下进行设置）。

✓ 单管理员

当设置为单管理员时，只需当前登录的管理员进行批准操作即可完成请求的处理，如图 3- 28。

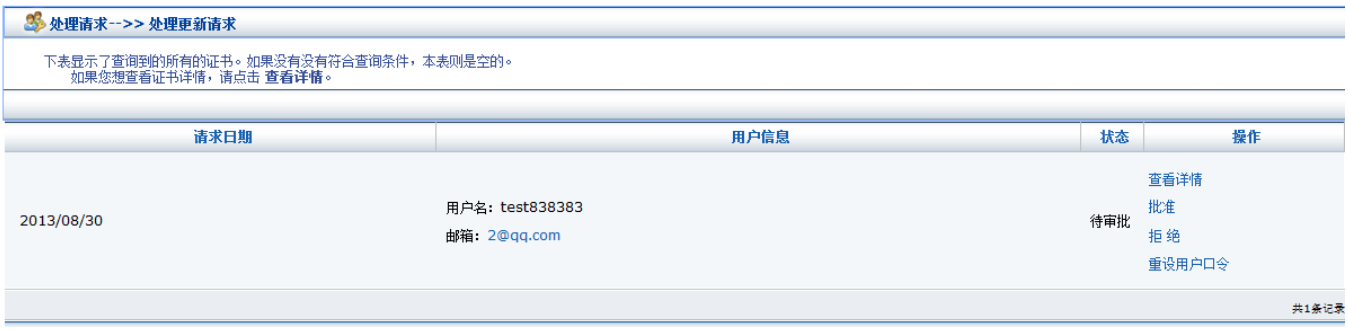

图 3- 28 处理更新请求（单管理员）

✓ 双管理员

当设置为双管理员时，当前登录的管理员进行鉴别操作后，需等待该帐户下另外一个管理员进行验证后才能完成请求的处理，如图 3- 29。

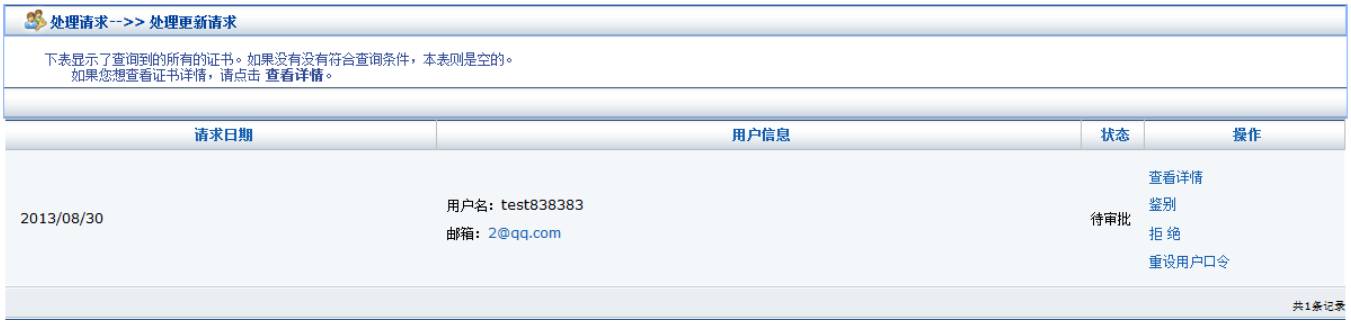

图 3- 29 处理更新请求（双管理员）

注意：只有拥有证书管理权限的 RA 管理员才能得到进入处理更新请求页面。

通过“处理更新请求”页面中的“操作”表格栏，您能完成以下操作：

- 查看注册信息细节。单击“查看详情”，以查看证书申请人的所有注册信息（如图 3-30）。此信息用来检验用户请求的正确性，并检查当前请求是否与您组织内的证书签发规则一致。

  ——从本页，您可以更改证书的有效期（默认为一年）。

  ——您一旦证实了证书申请人的身份（即他或她是一个“相关的个人” ），并证实其它所有打算包含在证书中的信息都是准确的，您就可以批准该请求了。

当帐户设置为单管理员批准时，只需当前登录的管理员进行批准操作即可完成请求，如图 3- 30。当帐户设置为双管理员批准时，当前登录的管理员验证或鉴别操作后，还需等待另外一位管理员进行鉴别或验证操作，才能完成批准操作，如图 3- 31。当您批准了证书请求，CA 系统就将为该帐户签发证书。

注意：如果注册信息中有输入错误或其它细小错误，请拒绝请求，并请申请人提交重新提交新请求，以此确保证书信息的准确性。

图 3- 30 查看详细信息（单管理员）

图 3- 31 查看详细信息（双管理员）

- 批准最终用户的证书请求。

  单击“批准”按钮，即完成证书请求的批准操作。本操作会将管理员的批准操作请求发送给 CA 系统，证书在 CA 系统产生、签发、并(在公开证书情况下)发布到证书库。随后 CA 系统将自动向申请人邮箱发送一份电子邮件，通知申请人随时可以获得证书。该邮件中包含一个 PIN 码以及 CA 系统“证书下载”页面的 URL。申请人通过 Web 下载证书，即成功成为一个证书用户。

- 拒绝最终用户的证书请求。

  如果您不能确认证书请求的正确性/有效性，建议您拒绝该请求。点击“拒绝”按钮，完成拒绝请求操作。RA 管理员将自动向申请人发送一份电子邮件予以说明。

3.3.4. 查看更新请求

在“处理请求”模块，点击“查看更新请求”链接，您能查看需要处理的特定证书更新请求的详细信息（如图 3- 32）：

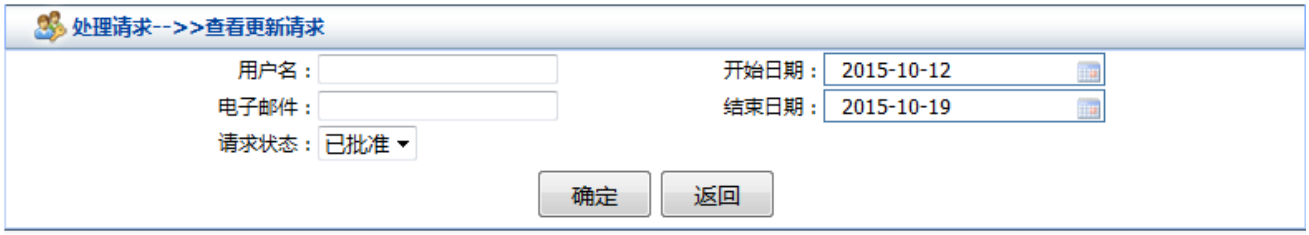

图 3- 32 查看更新请求页面

管理员可根据申请人的姓名或电子邮件地址以及提交请求的时间段来进行搜索。

此外，还可根据请求状态进行搜索：

- 待批准：已提交请求，但还没有得到批准或拒绝。
- 已拒绝：已提交请求，且已被 RA 管理员拒绝。

对于已拒绝的请求，控制中心将列出所有请求的列表（如图 3-33），这些请求是在您规定的期间内满足搜索标准的。选择操作表格栏中的操作，与 3.1.1 节中描述的“处理新请求”页面中的操作相同。

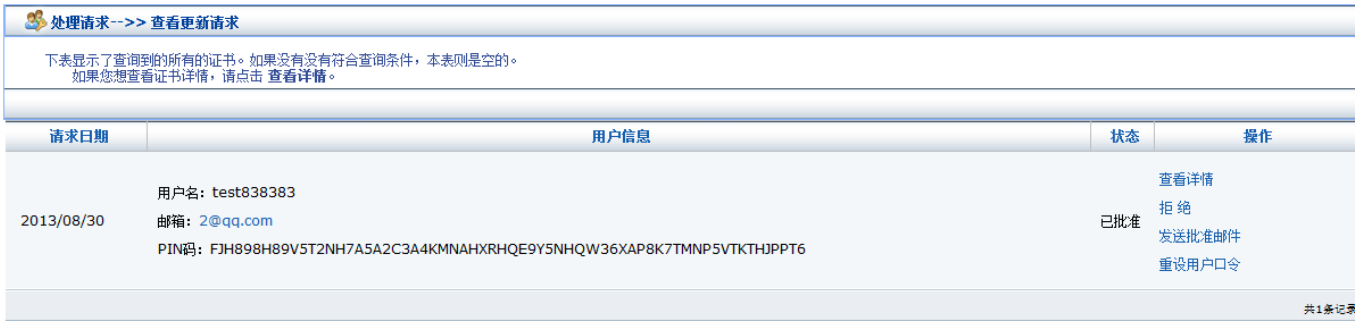

图 3-33　查看新请求列表

- 查看详情：查看请求的详细信息，如图 3- 30。
- 拒绝：已批准的请求，管理员可再次拒绝操作。
- 重发批准邮件：请求被批准后，系统自动给申请人邮箱发送批准邮件，若用户未收到，管理员可通过该功能再次发送批准邮件。
- 重设用户口令：当用户口令忘记后，不能对证书进行操作，此时管理员可通过该功能对用户证书口令进行重新设置，设置成功，系统自动将重新设置的口令发送到申请人的邮箱。

3.4. 通行码管理

通行码，是用于自动颁发数字证书的一串字符。拥有证书管理权限的 RA 管理员，您还需要对于通行码进行维护。通行码的管理包括创建通行码、将指定通行码给最终用户使用。

通行码管理部分提供以下功能：

- 管理通行码策略
- 创建通行码向导
- 查看通行码
- 批量制证

3.4.1. 管理通行码策略

我们创建通行码策略来定制通行码所需相关项目，如 O、OU 等。通行码策略类型根据通行码的不同用途，可分为通行码策略和授权码策略。

通行码策略即绑定用户信息项的策略，用户使用该略下的通行码申请证书时，证书的用户信息即为通行码绑定的用户信息。

授权码策略即不绑定任何用户信息项的策略，用户使用该略下的授权码申请证书时，用户还需填写用户信息。

点击“管理通行码策略”链接后，右侧主界面将打开通行码策略管理页面，如图 3-34，单击表格右上角“新建通行码策略”链接，进入通行码策略选择页面，如图图 3- 35，在该页面输入策略名称，选择通行码策略类型点击“确定”。如选择的是通行码策略，即可进入定制化通行码策略界面，如图 3-36；如选择的是授权码策略，则提示创建策略成功。

图 3-34　管理通行码策略界面

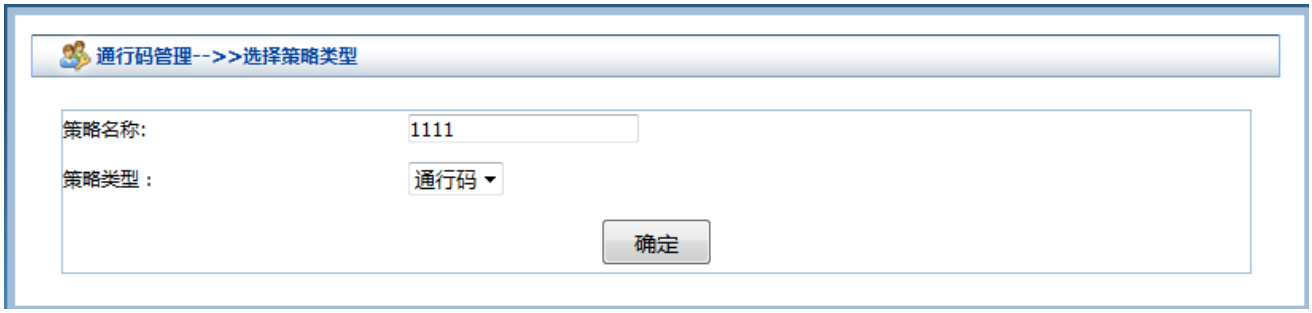

图 3- 35 选择通行码策略页面

图 3-36 新建通行码策略

3.4.2. 创建通行码

在使用系统前，您需要事先创建好一批通行码，以备用户使用。通行码向导就是来辅助您完成这一操作的。

单击后“创建通行码向导”链接，右侧主界面打开如图 3-37 所示页面，您可以选择指定的通行码策略，选择创建通行码的方式，如手动创建或文件导入创建。

- 创建通行码

如选择通行码手动创建，进入到手动创建通行码页面，该页面将显示策略中绑定的用户信息项，如图图 3- 38，输入用户名和邮箱信息后即可完成通行码创建，后续可使用该通行码下载证书。

点击确定进入到创建通行码页面，如图

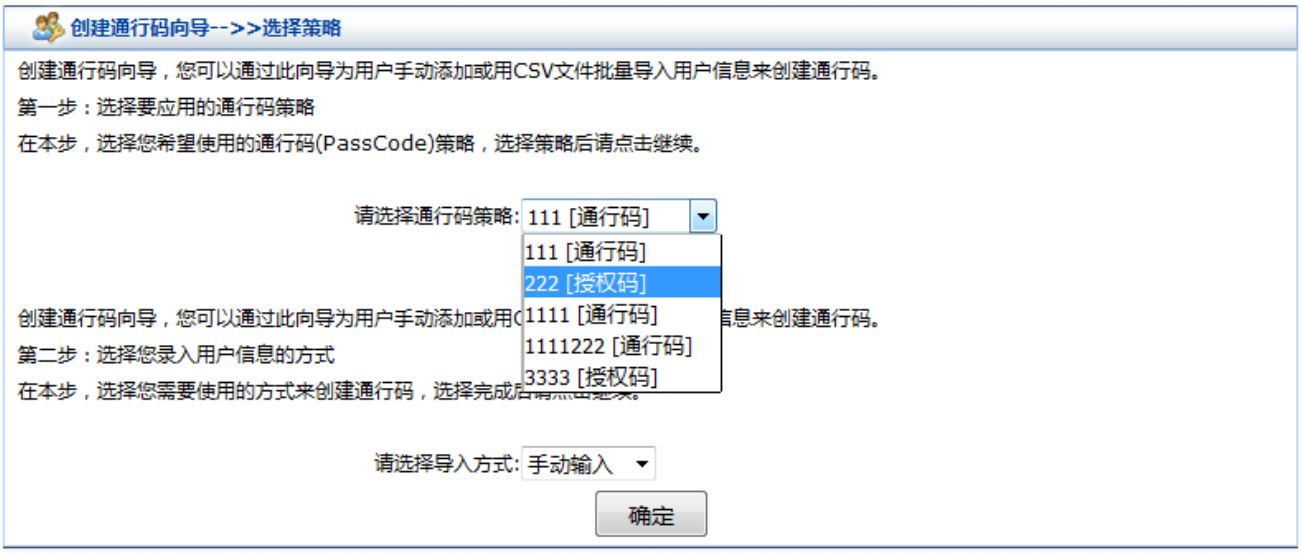

图 3-37　创建通行码-选择策略

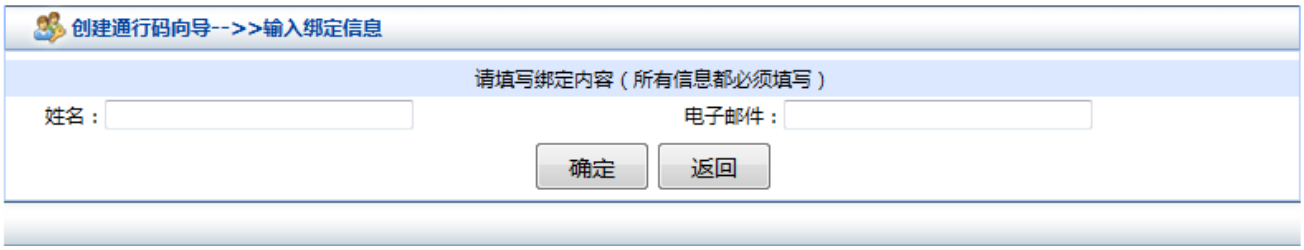

图 3- 38 创建通行码-手动创建通行码

如选择通行码文件导入方式创建，则进入如图 3-39，点击下载模版链接，下载该文件的模版。您将用户信息按照模板中填好后，点击“浏览”上传填好用户数据的模板，上传成功，页面将显示上传文件中的用户信息，如图图 3-42，确认信息无误后，点击“确定”完成通行码创建。

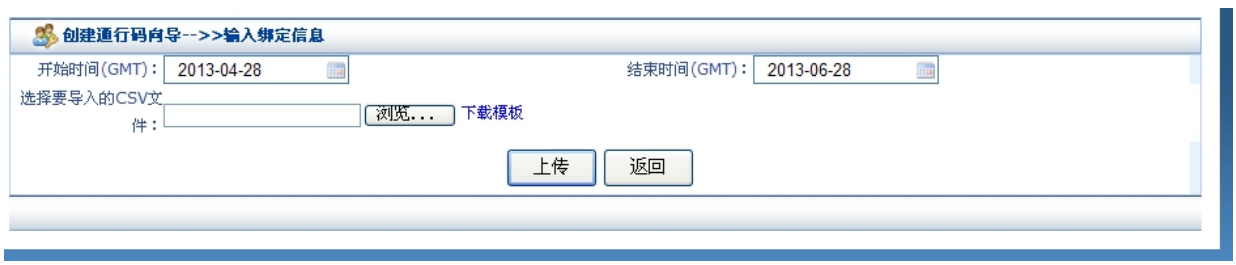

图 3-39　创建通行码-文件导入创建

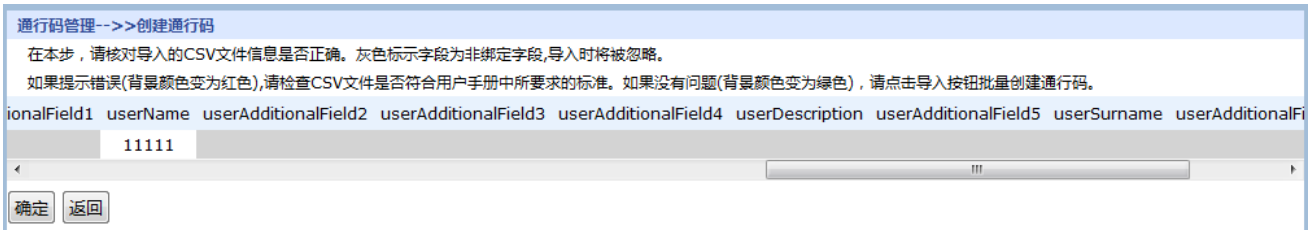

图 3- 40 创建通行码-文件导入确认

- 创建授权码

  在创建通行码时选择授权码，将进入授权码创建页面，如图图 3-　41，在该页面输入授权码的数量和授权码的有效期即可完成授权码的创建。

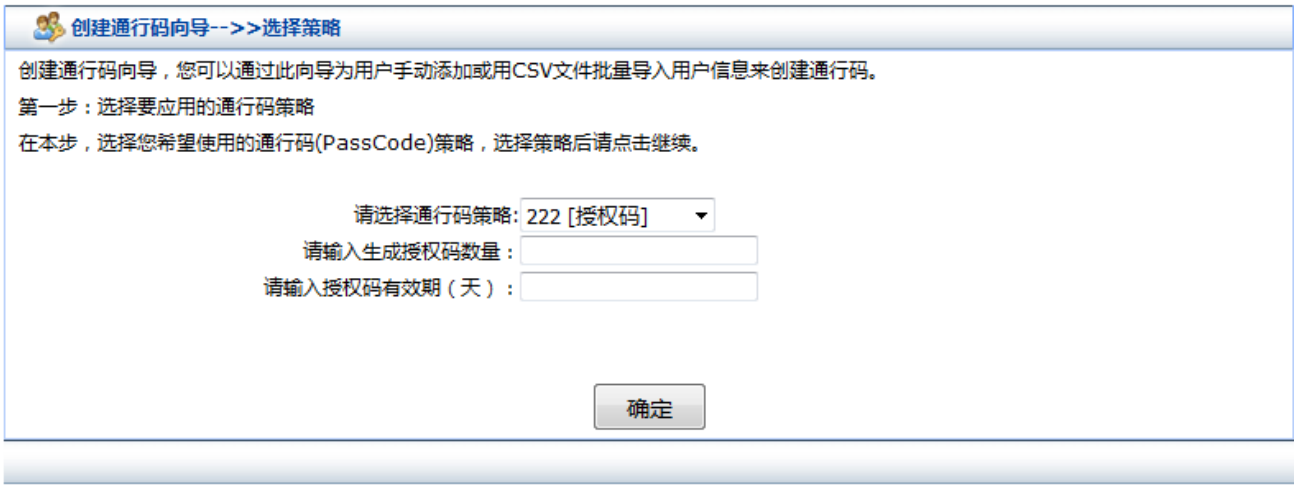

图 3- 41 创建授权码

3.4.3. 查看通行码

如果帐户设置成使用通行码方式，则该项和下边的“创建通行码”是管理员需要做的操作。

通行码是用来给最终用户申请证书使用的，如果 RA 帐户打开了通行码的功能，则用户在申请证书时需要提交通行码。管理员需要事先在控制中心创建并上传通行码，同时在用户申

请证书前发给用户本人。利用通行码实现用户证书的自动发放可以很大的减少 RA 管理员的负担。

创建通行码后，点击“查看通行码”链接可以打开如图 3-42 所示页面，您可以根据创建通行码的时间段和通行码的使用状态来查找。

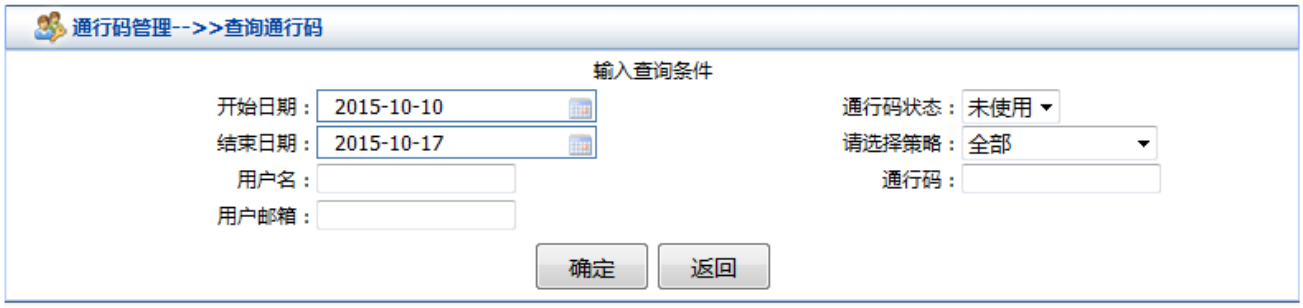

图 3-42　查看通行码的查询页面

查询出符合条件的通行码列表后，根据通行码的状态，您可以进行的操作有“查看详情” 、“删除”和“发送”（授权码无此功能），如图 3-43。每次查询通行码，当通行码的有效期小于等于 5 天时，通行码列表操作栏将显示重发通行码链接。

重发通行码即重新产生一个通行码，有效期默认 15 天，由系统给出，且起始日期为重发通行码执行的日期，此时原有的通行码将被替换。重发通行码完成后，通行码列表通行码列将显示重发后新产生的通行码。

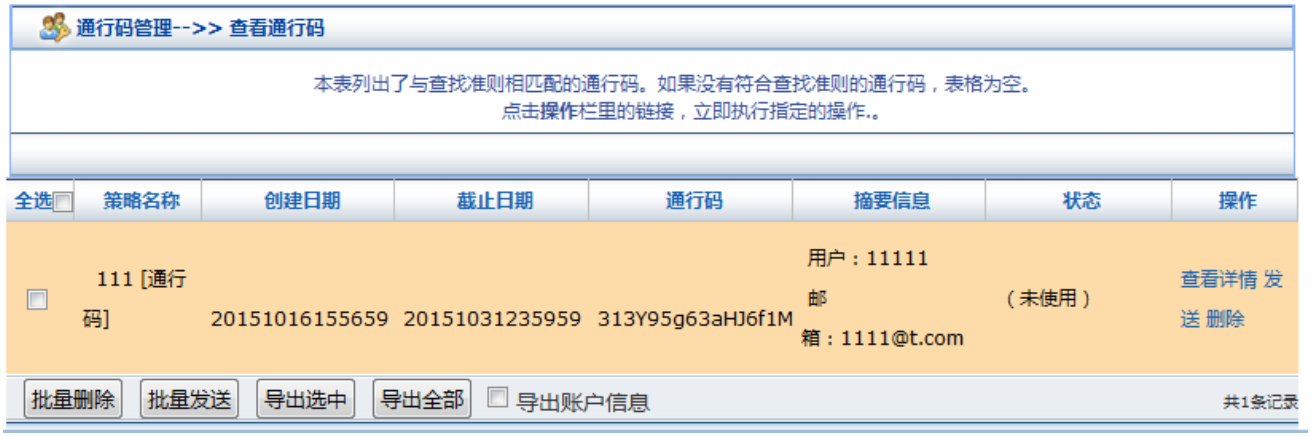

图 3-43　查看通行码

通过“查看通行码”页面中的“操作”表格栏，您能完成以下操作：

- “查看详情”链接打开如图 3-44 所示页面，在该页面可点击“发送通行码”执行通行码发送操作。

图 3-44　通行码详情

在这里，您能查到该通行码的创建时间，截至日期（必须在该日期前使用）及通行码的内容。

- 点击“删除”链接可以直接将该通行码删除；
- 点击“发送”或“重发”链接，将通行码发送到通行码中填写的邮箱地址。

3.4.4. 批量制证

在“通行码管理”页面，点击“批量制证”链接，您能够为满足查询条件的操作员进行批量制证，如图 3-45。

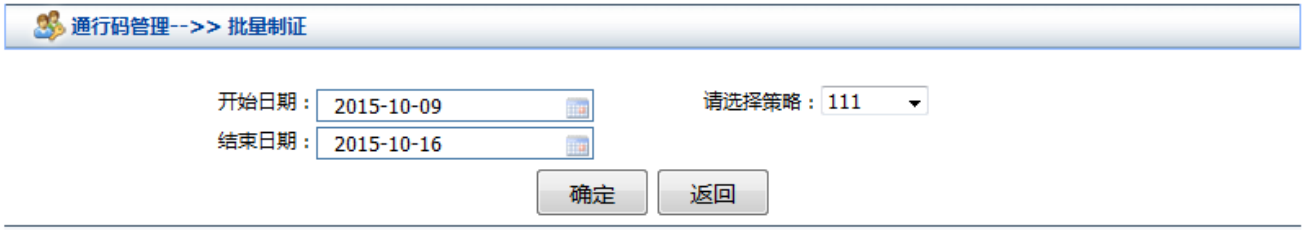

图 3-45　批量制证查询条件页

指定查询条件后，单击“确定”按钮返回查询结果，如图 3-46。

图 3-46 批量制证

RA 管理员通过选择每条记录前面的复选框标记来选择需要制证的操作员，也可通过“全选”和“取消全选”按钮进行选择或取消选择所有复选框。单击“确定”按钮系统开始从上至下生成证书，每个证书生成完，会提示拔出 Key 和插入 Key 等信息，同时该条记录对应的复选框灰显。

如果记录过多（超过一页），则可通过“下一页”和“上一页”按钮进行翻页浏览。

3.5. 系统设置

管理员可以通过系统设置中提供的功能对帐户进行重新初始化操作。

3.5.1. 证书配置

该项功能提供您对用户证书进行配置，如图 3-47。您可以设置是否允许相同的用户名，是否启用 PASSCODE 申请证书，是否启用私钥保护等的配置。

是否开启注册项联动，即 raManager 站点的签发证书页面的用户信息项是否随注册项的配置进行显示，默认已开启。如勾选“否”，则该页面将显示固定的项。

证书申请审批方式包含普通模式、passcode 模式、AA 模式三种，可根据需要配置。

- 普通模式即用户申请管理员审批；
- passcode 模式即管理员提前将用户信息收集到创建 passcode 码，管理员将 passcode 码下发到用户，用户使用该码进行下载证书。
- AA 模式即不需要任何审批的方式，用户申请即下发证书。

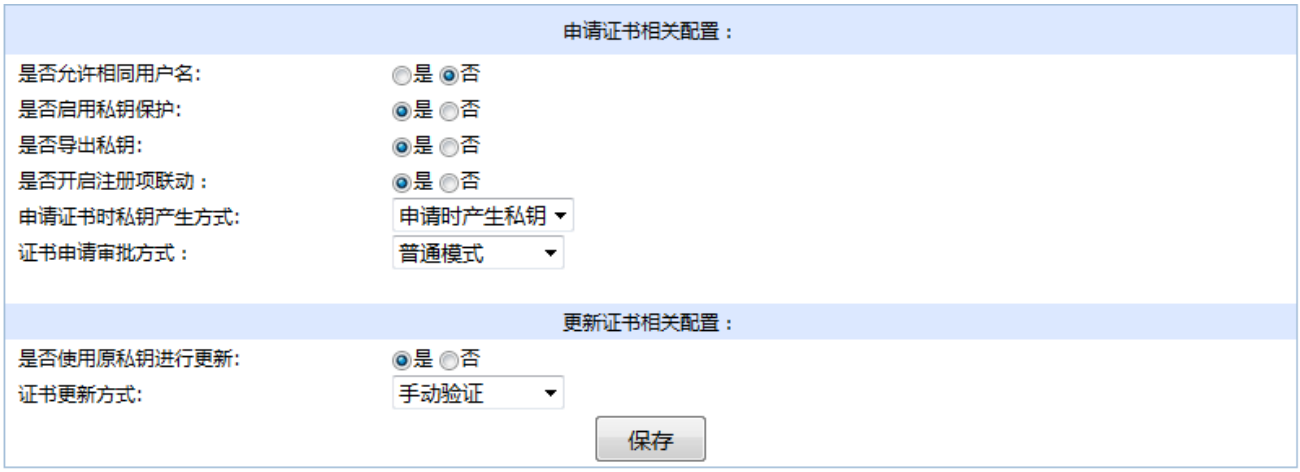

图 3-47 证书配置

3.5.2. 帐户配置

您通过本项可查看该帐户连接 CA 状态（连接成功时显示成功标识，连接失败显示失败标识），配置用户证书服务中心的的证书服务地址、该帐户的别名、帐户通知模版配置等信息。

证书服务地址即用户申请证书时，管理员发送给用户通知邮件中，引导用户获取证书时的地址。

帐户别名可根据自己需要设置不同的名称，通过该名称可快捷访问该帐户服务地址，访问方式如：http://ip:port/TopCA/帐户别名 。

通知方式模版配置即根据不同的帐户配置用户申请、更新证书等操作时，管理员向用户发送通知详细内容，包括邮件和短信两种通知方式。若需要配置启动邮件和短信通知，请登录 CA 控制台完成启用和配置。

当您配置的 RA 为托管 RA 时，帐户设置显示如图 3-48，其中 CA 连接状态、同步帐户信息是该模式下 RA 特有的。点击同步帐户信息，从 CA 端同步 RA 帐户信息，同步成功，提示同步成功；同步失败，提示失败原因。

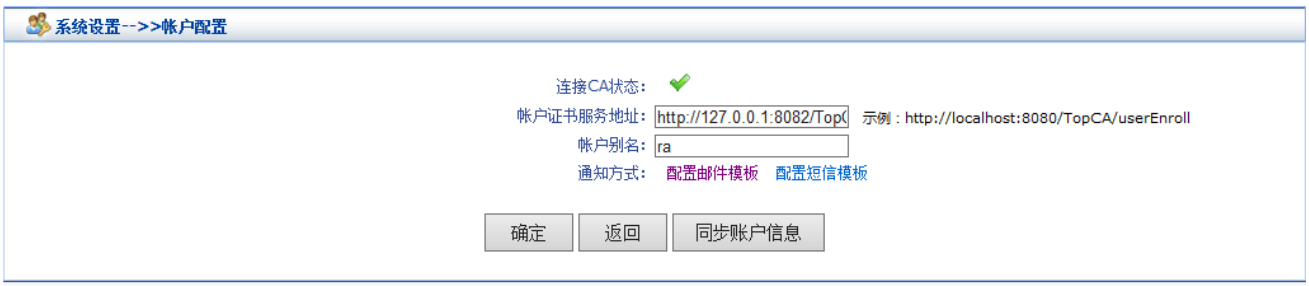

图 3-48 帐户配置（托管 RA）

当您配置的 RA 为自建 RA 时，帐户设置显示如图 3- 49。

图 3- 49 帐户配置（自建 RA）

点击配置邮件模版，进入如图 3-50 ，邮件模版包括申请证书，签发证书，更新证书等操作邮件发送通知内容。如果需要修改邮件的内容，您可以对该内容编辑修改，需保持其中的变量不变，如$(USER_NAME)等；同时，修改过的邮件内容还可以恢复到默认内容。

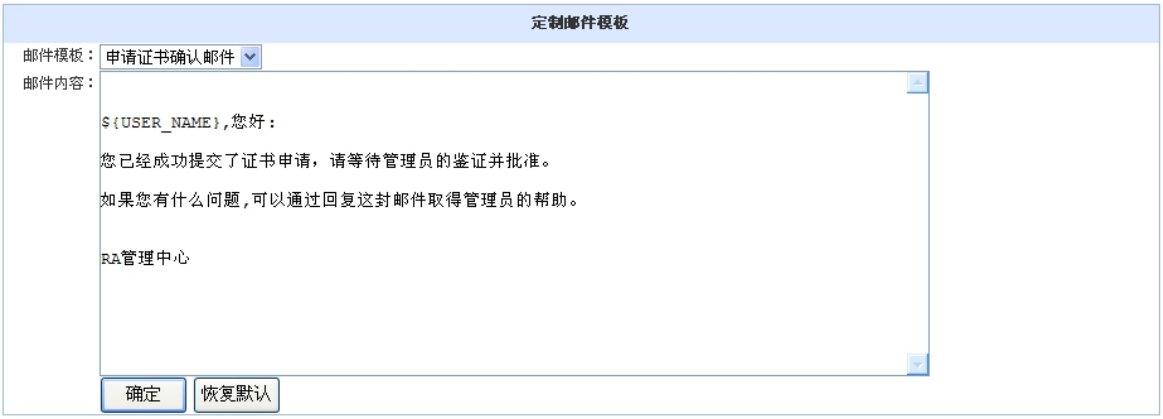

图 3-50 定制邮件模版

点击配置短信模版，进入如图 3-51，短信模版包括申请证书，批准证书，拒绝证书、吊销等操作短信发送通知内容。如果需要修改短信的内容，您可以对该内容编辑修改，需保持其中的变量不变，如$(USER_NAME)，${ CERT_PIN}等；同时，修改过的邮件内容还可以恢复到默认内容。

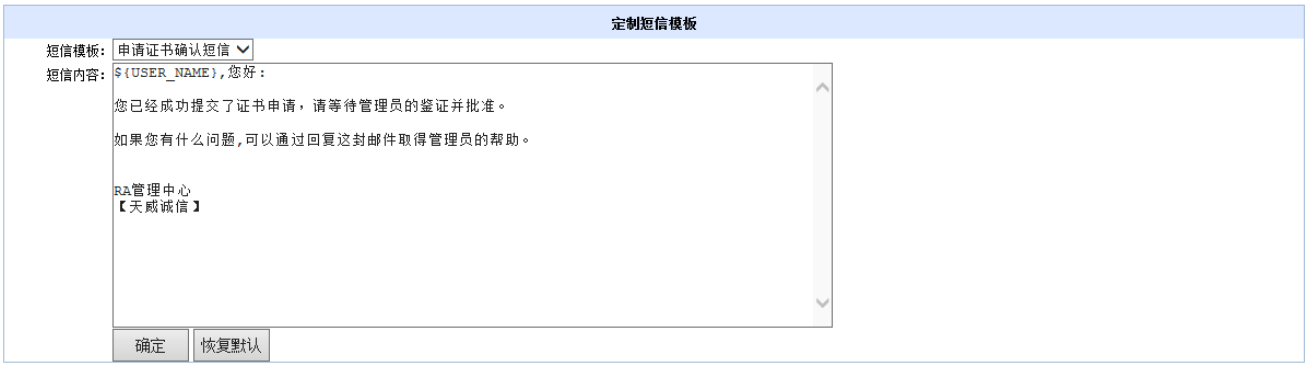

图 3-51　定制短信模版

3.5.3. 注册项配置

该项用于配置用户申请证书时所需要填写的信息项，如图 3-52。

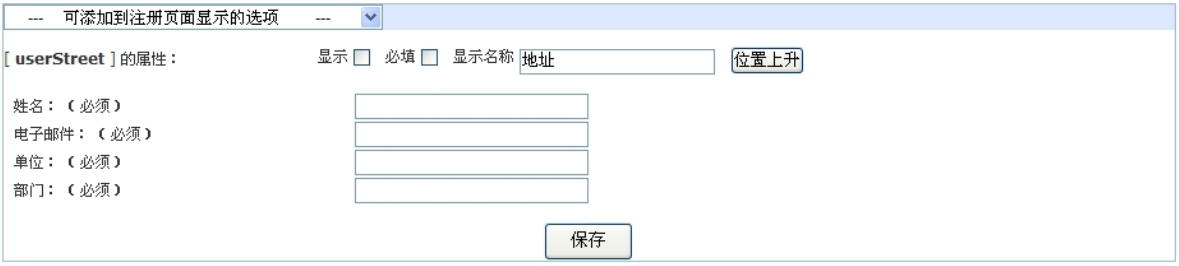

图 3-52　注册项配置

您可以在列表中选择注册项，然后设置是否在用户申请证书时要填写该信息，是否该项信息为必填项，该项信息显示名称，设置该项信息的位置等信息。

3.5.4. 通知服务配置

该项用于配置本地 RA 帐户的通知服务，包括邮件和短信通知服务，如图 3- 53。填写邮件配置或短信配置信息后点击“保存配置”即可配置完成。此时在已开启的通知提醒区域显示已配置服务，如图 3- 54，若您不再使用通知服务，勾选需要关闭的通知服务，点击“关闭”即可。

图 3- 53 通知服务配置

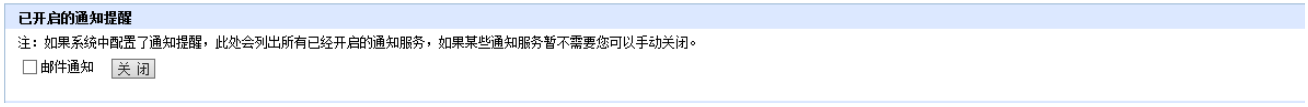

图 3- 54 已配置的通知服务

3.6. 管理员管理

3.6.1. 管理员角色设置

安全管理员可以通过“管理员管理”页面，点击“管理员角色设置”链接打开为本帐户额外管理员配置权限的向导，该向导分两步进行。如图 3-55。输入关键字，过滤管理员，选择需设置的管理员，点击继续进入角色定义页。如图 3-56。

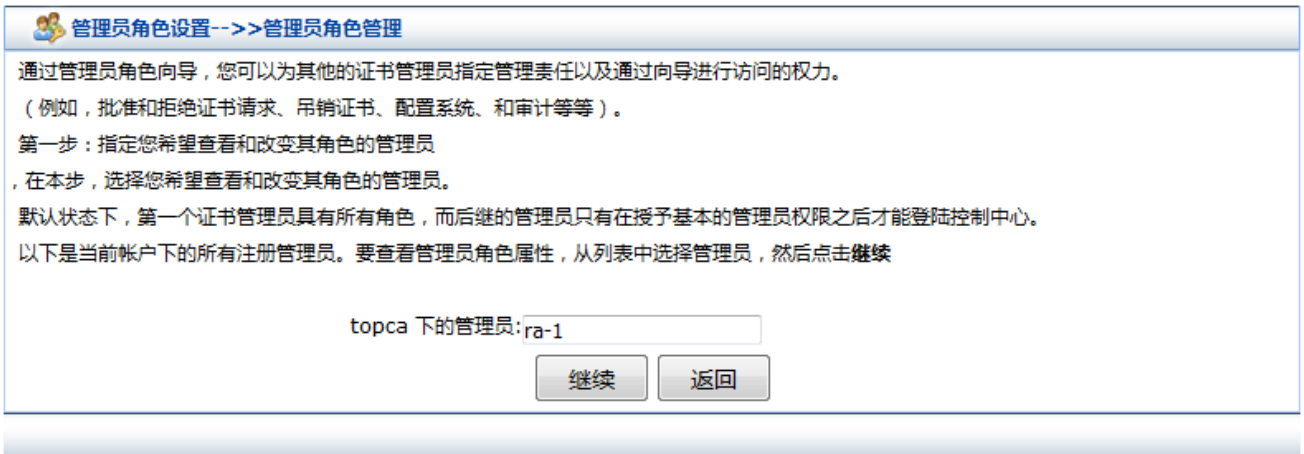

图 3-55　管理员角色名称

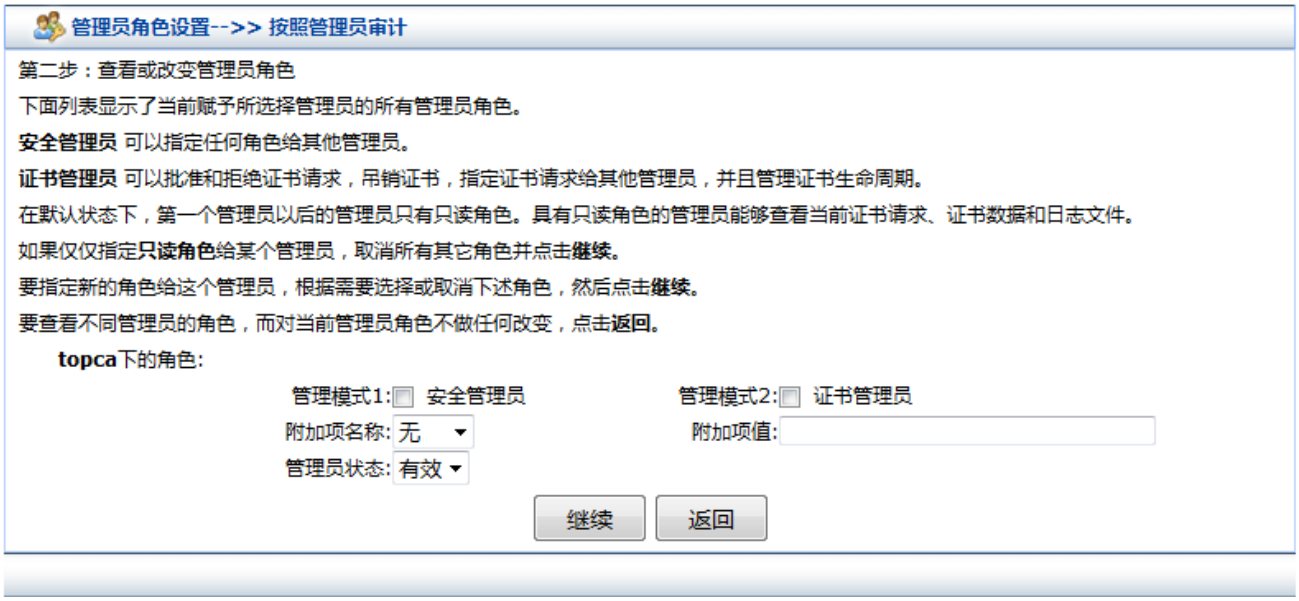

图 3-56　管理员角色定义

在上图页面中，您可以更改所选管理员的管理模式，可以复选，没有相应权限的管理员不能操作相应的功能模块。第 2 行的“附加项名称”和“附加项值”是用来指定管理员可管理证书范围的，如只能管理附加项中指定的省或某一城市的证书等。“管理员状态”可以将管理员置为挂起或有效状态。勾选相应的管理员权限后，点击继续按钮，如果操作成功系统会返回操作成功的页面。

3.6.2. 管理员操作审计

通过这个链接，您可以查询到所有管理员的操作记录，如批准和拒绝证书请求，挂起和恢复管理员证书等操作记录。点击导出全部，导出所有该管理员的操作记录；点击导出当前页，导出该管理员所在当前页的操作记录，如图 3-57。

图 3-57 管理员操作审计

3.6.3. 帐户审计

该向导分两步进行，查询帐号操作的日志； 按照帐户审计，可以查看在特定时间段对某帐户的所有操作（包括证书批准、挂起、恢复、吊销等等），如图 3-58。

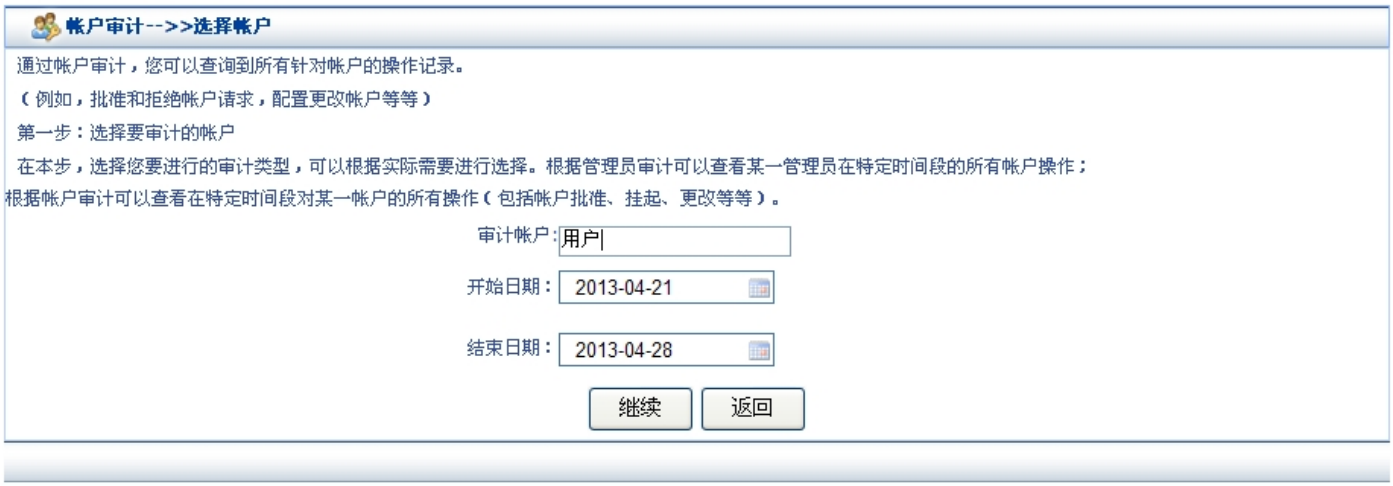

图 3-58 帐户审计

输入帐户的 O，OU 关键字，在列出的帐户下选择需要审计的帐户，点击继续，进入帐户审计页，如图 3-59。 点击导出全部，导出所有该帐户的操作记录；点击导出当前页，导出该帐户所在当前页的操作记录。

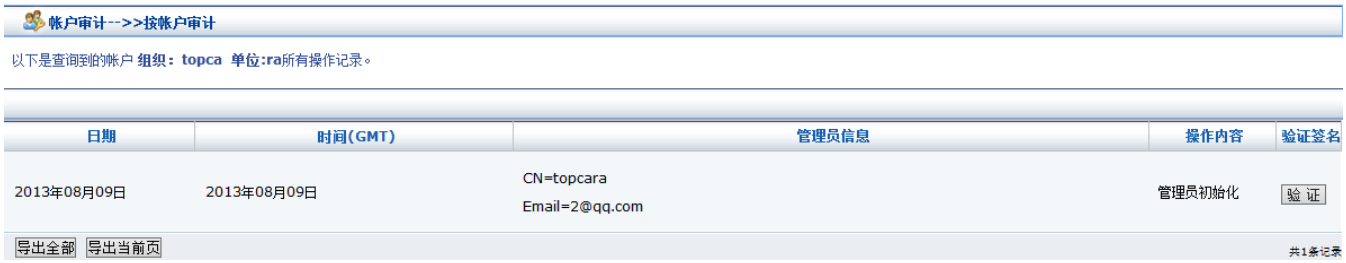

图 3-59 按帐户审计

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

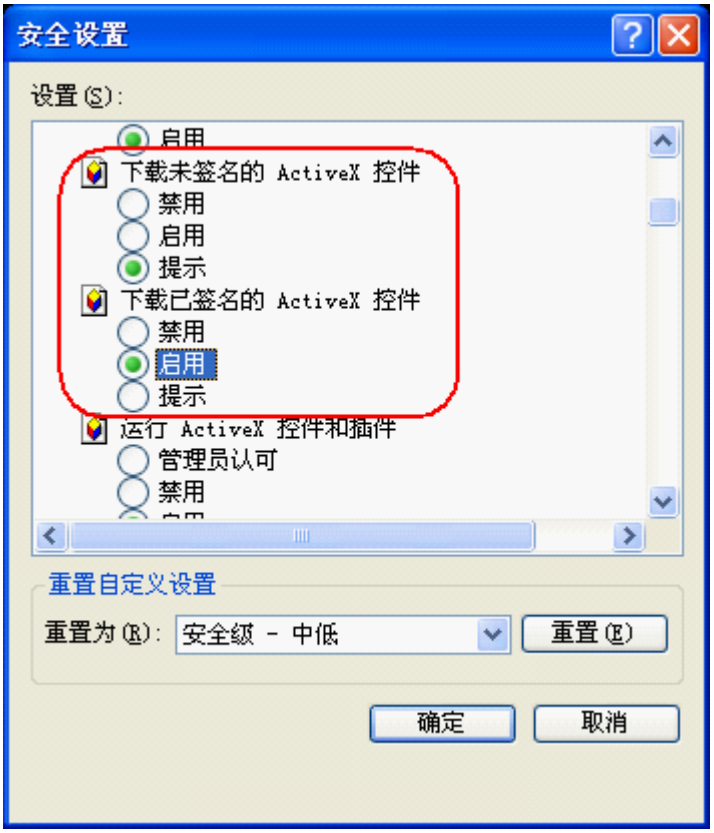

图 4-2 设置 ActiveX 控件选项组

4) 设置完成后，单击“确定”按钮即可。

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：进入 RA 管理员证书服务中心申请 RA 帐户或者管理员证书批准获得证书后，登录系统提示没有初始化和管理员权限错误，如图 4-3，图 4-4。

图 4-3 管理员登录提示未初始化

图 4-4 管理员登录提示权限错误

A：提示没有初始化是因为在总控制台（console 站点）尚未加载该帐户下的 CA 证书和证书模板。提示管理员权限错误是因为没有通过上级管理员设置管理员的权限角色，通知管理员完成这些操作即可。

Q：RA 管理员控制中心查看证书，证书信息显示不全，如图 4-5。

A：因为系统保存了已经申请且管理员未批准的证书，此时该证书没有证书序列号，有效期期限。

图 4-5　证书信息缺失

Q：签发证书，填写信息完成后，确认签发跳转到错误提示页面，报未知错误，如图 4- 6。

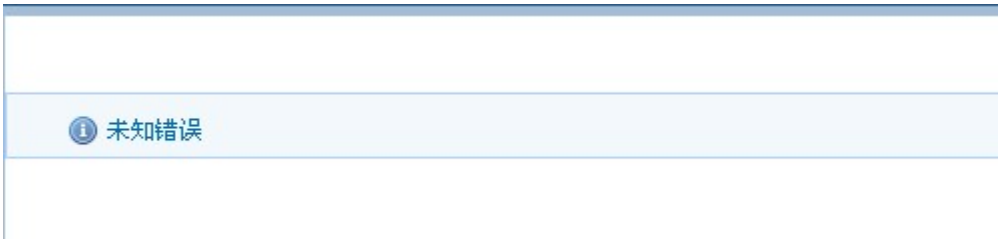

图 4- 6 未知错误

A：因为 topca 的配置文件中 crs 配置的信息错误，不加密的 CSR 配置如：

Crs.url=http://ip:port/TopCA/crs/crs；加密的 CSR 配置如

Crs.url=http://ip:port/TopCA/crs/evpCrs。

Q：“查询证书”—“有效证书”中为什么有相同的证书？

A：因为更新过证书后，原有证书与更新过的证书都未过期，故都会罗列出来。

Q：“证书管理”—“签发证书”页面显示双证书管理--注册用户证书，签发的都是双证书

吗？

A：如果未配置连接 KMC 系统，则当前帐户下签发的都是单证书。

Q：“证书管理”—“更新证书”页面显示证书的机制？

A：该页面中会将 30 天内即将到期的证书罗列出来，而不论更新过一次或多次，同一张证书只显示最新即将到期的一张。

Q：当帐户的 O，OU 设置为中文时，帐户登录页面输入关键字搜索不到相应的帐户。

A：web 容器未设置正确的编码，修改 tomcat\conf\目录下 Server.xml 文件 URIEncoding=”UTF-8”即可，如图 4-7。

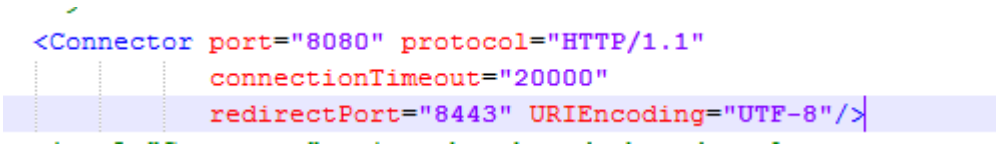

图 4-7　设置编码