

天威诚信车联网PKI系统 用户手册

■ 版权声明

本文件中出现的全部内容，除另有特别注明，版权均属北京天诚安信科技股份有限公司（以下简称天诚安信）所有，未经天诚安信书面许可，任何人不得以任何形式擅自拷贝、传播、复制、泄露本文件的全部或部分内容。

■ 保密事宜

本文档包含北京天诚安信科技股份有限公司的专有商业信息和保密信息。

接受方同意维护本文档所提供信息的保密性，承诺不对其进行复制，或向评估小组以外、非直接相关的人员公开此信息。对于以下三种信息，接受方不向天诚安信公司承担保密责任：

- 1) 接受方在接收该文档前，已经掌握的信息。
- 2) 可以通过与接受方无关的其它渠道公开获得的信息。
- 3) 可以从第三方，以无附加保密要求方式获得的信息。

目录

1. 前言.....	4
1.1. 关于本手册.....	4
1.2. 天诚安信技术支持.....	4
2. 用户证书服务中心.....	5
2.1. 用户证书服务中心.....	5
2.2. 用户证书服务中心功能结构.....	5
2.3. 申请用户证书.....	6
2.4. 获取用户证书.....	7
2.5. 查询用户证书.....	8
2.6. 更新用户证书.....	10
2.7. 吊销用户证书.....	11
2.8. 恢复加密证书.....	12
2.9. 安装 CA 证书链.....	13
2.10. 下载证书吊销列表（CRL）.....	13
2.11. 证书替换.....	15
2.12. 证书预览.....	18
3. 服务器证书服务中心.....	20
3.1. 服务器证书服务中心.....	20
3.2. 服务器证书服务中心功能结构.....	20
3.3. 申请服务器证书.....	21
3.4. 查询服务器证书.....	22
3.5. 吊销服务器证书.....	23
3.6. 下载 CA 证书链.....	24
3.7. 下载证书吊销列表.....	25
4. 常见问题（FAQ）.....	28

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。

1.2. 天诚安信技术支持

如果您对您的责任有疑问，可参阅本手册中的目录或索引找到您要查找的信息。对本手册中未能完全体现的信息，可访问我公司网站 <http://www.topca.cn/>。

如果您在处理中心库或网站上找不到您需要的信息，可按照如下方式请求天诚安信支持：

Email: support@topca.cn

24 小时客服热线：400-876-1177

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:port/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。

输入注册信息

用户基本信息：
填写所有字段，带有“*”号的信息将包括在您的数字证书中，并向公众公开。

姓名：（*）	
电子邮件：（*）	
单位：（*）	
部门：（*）	

用户口令：
这个唯一的验证口令保护您的证书，避免没有被授权的操作，它不能与其他人共享。
不要丢失！在证书下载和注销时需要它。

用户口令：（*）		（用户口令至少为8位）
再次输入口令：（*）		
加密服务提供者：	RSA软证书	

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。

祝贺您！

您已经注册成功，请检查您注册时填写的电子邮件，您会收到一封确认邮件。

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。

获取用户证书

重要提示：该步必须使用注册时使用的计算机完成！

要完成这一步，身份识别码（PIN）是必需的。在提交注册表后，管理员会验证您的身份，并决定是否给您颁发数字证书。如果身份验证通过，系统将为您产生数字证书，并给您发送一封名为“您的数字证书已经准备好了”的电子邮件。

从电子邮件中复制PIN，粘贴到下面的文本框中，然后点击“**获取证书**”按钮进行提交。

点击“**返回**”按钮，将返回到注册页面。

提交后，在得到响应之前，不要中断您的浏览器。

身份识别码（PIN）：

用户口令： [忘记密码？](#)

图 2-5 获取用户证书

获取成功，显示如图 2-6 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。

证书下载成功

您的数字证书信息

证书DN	EMAILADDRESS=2@qq.com, CN=testaaa
序列号	7F45D224BB31EBA5974764E1B5A12AA0721F2576
序列号(加密证书)	24AEC8B23C9230E24E0FB944C411D10785293500
有效期	2013年04月28日 15:14:55 至 2014年04月28日 15:14:55

注意:如果没有安装成功,请再次点击“**获取证书**”按钮

点击“**返回**”按钮,将返回到注册页面。

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。

按电子邮件查询用户证书(推荐)

输入查询条件

电子邮件: (*)

☒ 所有 ☐ 有效 ☐ 过期 ☐ 已注销

按用户名查询用户证书

输入查询条件

用户名: (*)

☒ 所有 ☐ 有效 ☐ 过期 ☐ 已注销

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- 8。

查询数字证书结果	
本次查询找到了以下符合条件的数字证书。 通过点击名称，您可以查看该数字证书的详细信息， 或者进行诸如下载或吊销数字证书之类的操作。	
共有[9]条	
用户名: test419(REVOKE)	
邮箱: 2@qq.com	
证书序列号: 1F64D887DA20179AFD2C623B832975D17D13673B	
有效期从2013/04/19(GMT)到 2014/04/19 (GMT)	
用户名: hello4-26(VALID)	
邮箱: 2@qq.com	
证书序列号: 1CA19B4647D4775B2CD18A268387CDD6522C7112	
有效期从2013/04/26(GMT)到 2014/04/26 (GMT)	
用户名: hello4-26-1(VALID)	
邮箱: 2@qq.com	
证书序列号: 1F11C2AAA9BEF3A5C36EE258E8137225006FDC5A	
有效期从2013/04/26(GMT)到 2014/04/26 (GMT)	
用户名: hello4-26-1(VALID)	
邮箱: 2@qq.com	
证书序列号: 53B4D45C9E29A25C6DB1AEDE79F518CEDE450784	
有效期从2013/04/26(GMT)到 2014/04/26 (GMT)	
用户名: a-4-26(VALID)	
邮箱: 2@qq.com	

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。

用户证书更新

选择更新证书：
如果您的浏览器支持，列表中将列出所有安装在您机器中的满足条件的证书名称，您可以选择一个需要更新的证书进行更新。默认列出所有有效期限在30天以内的所有证书。

选择更新证书：

5-30

查看证书

加密服务提供者：

RSA软证书

[变更证书持有者信息](#)

更新

返回

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。

用户证书更新

选择更新证书:
如果您的浏览器支持，列表中列出所有安装在您机器中的满足条件的证书名称，您可以选择一个需要更新的证书进行更新。默认列出所有有效期限在30天以内的所有证书。

选择更新证书: 5-30

[查看证书](#)

加密服务提供者: RSA软证书

[变更证书持有者信息](#)

提示：以下内容若有更改，系统将为您签发一张新证书，您原来的证书（更新前的证书）将失效，请慎重操作。

单位名称: topca

部门名称: ra

姓名: 5-30 [确认](#)

电子邮件: 2@qq.com [修改](#)

国家: [修改](#)

更新
返回

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。

查询用户证书

输入查询条件

电子邮件:

用户名:

查询
返回

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，如图 2-12。

数字证书信息	
姓名:	t
电子邮件:	2@qq.com
状态:	VALID
有效期:	有效期从2013/04/26(GMT)到 2014/04/26 (GMT)
	OU=用户证书注册中心
	O=topca
主题:	EMAILADDRESS=2@qq.com
	CN=t
序列号:	5EC51FA098915D90DF4CCAEC60B8B289014D8122

吊销查到的数字证书	
用户口令:	
吊销原因:	密钥遭受损害 ▾
吊销 返回	

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。

密钥恢复

选证书: 1111[有效期内]

授权码:

签发者: user

主 题: 1111

序列号: 4f0d613cb889d71c5400...

开 始: 2013年4月7日 10:43:56

结 束: 2014年4月7日 10:43:56

状 态: [有效期内]

确定

返回

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。

安装CA证书链

点击“确定”按钮可以安装CA证书链

确定

返回

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。

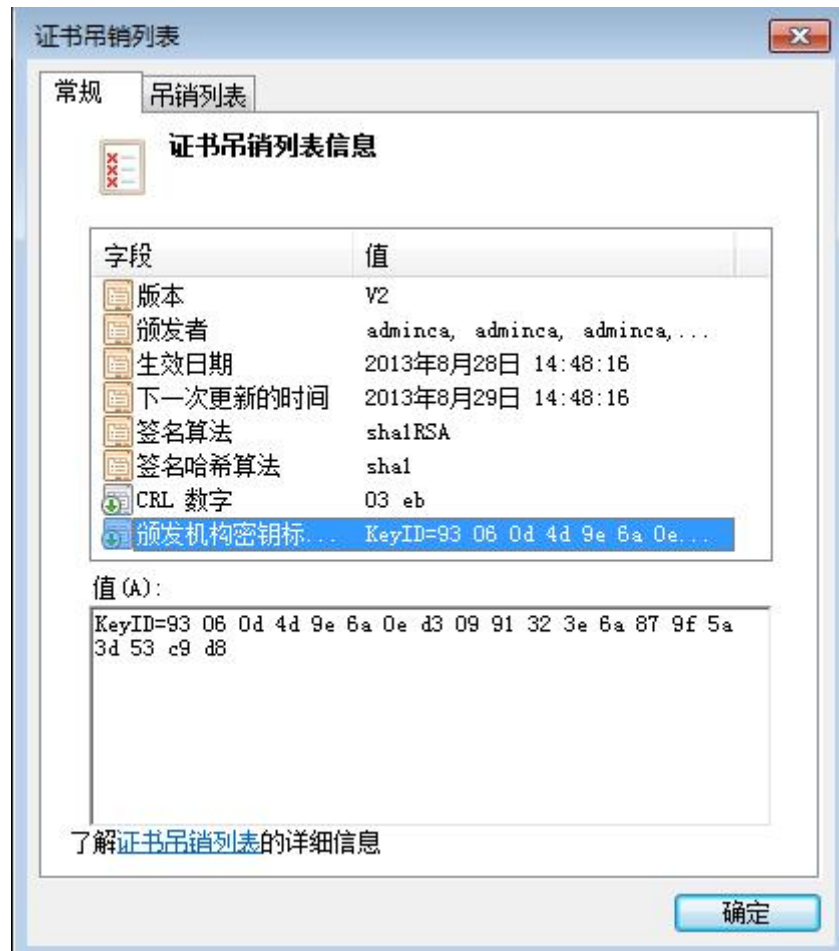


图 2-15 证书吊销列表



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。

证书替换步骤：
填写替换申请 > 确认替换申请 > 管理员审批 > 获取证书

证书替换申请

请填写以下基本信息，用以核对您的证书状态。若证书尚未失效，系统将向您注册时提供的邮箱发送证书邮件，请注意查收。

姓名：(*)

电子邮件：(*)

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。

证书替换步骤:
[填写替换申请](#) > [确认替换申请](#) > [管理员审批](#) > [获取证书](#)

提示
证书替换的确认链接已发送至您的邮箱，请注意查收。

[返回首页](#)

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。

证书替换步骤:
[填写替换申请](#) > [确认替换申请](#) > [管理员审批](#) > [获取证书](#)

确认替换申请
您的身份已得到验证，可以进行证书替换操作。替换之前，请先吊销需要替换的证书
您名下有以下证书尚在有效期，可以进行替换。
通过点击名称，您可以查看该数字证书的详细信息
找到需要替换的证书后，点击右侧的吊销证书，对原证书进行吊销操作，而后进行证书的替换操作。

共有[1]条

用户名: aaaaaaaaaa(VALID)	吊销证书
邮箱: 2@qq.com	
证书序列号: 1A273E492A02225953B329BA25081124688635FC	
有效期从 2013/05/20(GMT)到 2013/07/08 (GMT)	

[返回](#)

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。

证书替换步骤：
[填写替换申请](#) > [确认替换申请](#) > [管理员审批](#) > [获取证书](#)

数字证书信息

姓名: aaaaaaaaaaaaaa
 电子邮件: 2@qq.com
 状态: VALID
 有效期: 有效期从2013/05/20(GMT)到 2013/07/08 (GMT)
 主题: EMAILADDRESS=2@qq.com
 CN=aaaaaaaaaaaaaa
 序列号: 1A273E492A02225953B329BA25081124688635FC

吊销查到的数字证书

用户口令:
 吊销原因:

图 2-20 吊销原证书

证书替换步骤：
[填写替换申请](#) > [确认替换申请](#) > [管理员审批](#) > [获取证书](#)

证书吊销成功

证书吊销已经操作成功！
 点击“申请替换”完成请求提交。

加密服务提供者:

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。

证书: [刷新证书列表](#)

常规	详细信息																
<table border="1"><thead><tr><th>域</th><th>值</th></tr></thead><tbody><tr><td>版本</td><td>V3</td></tr><tr><td>序列号</td><td>6a28249fa6fff7922e89fe...</td></tr><tr><td>颁发者</td><td>CN=adminca, OU=adminca...</td></tr><tr><td>有效期从</td><td>2013年7月3日 10:35:34</td></tr><tr><td>到</td><td>2013年7月21日 11:26:25</td></tr><tr><td>使用者</td><td>CN=test7-2, OU=ra, O=t...</td></tr><tr><td>密钥用法</td><td>keyEncipherment</td></tr></tbody></table>		域	值	版本	V3	序列号	6a28249fa6fff7922e89fe...	颁发者	CN=adminca, OU=adminca...	有效期从	2013年7月3日 10:35:34	到	2013年7月21日 11:26:25	使用者	CN=test7-2, OU=ra, O=t...	密钥用法	keyEncipherment
域	值																
版本	V3																
序列号	6a28249fa6fff7922e89fe...																
颁发者	CN=adminca, OU=adminca...																
有效期从	2013年7月3日 10:35:34																
到	2013年7月21日 11:26:25																
使用者	CN=test7-2, OU=ra, O=t...																
密钥用法	keyEncipherment																
CN=adminca OU=adminca O=adminca C=CN																	

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 3-3，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 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。

输入证书请求

证书请求（CSR）：（*）
CSR无论必须与否，都必须填写。 确认删除带有“开始证书”和“结束证书”（BEGIN CERTIFICATE和END CERTIFICATE）的行。

MIIBwjCCASsCAQAwTEWMBQGA1UEAwNdGVzdC1zZXJ2ZXIwODERMA8GA1UECwwIdG9wY2EuY24xETAPBgNVBAoMCHRvcGNhLmNuMREwDwYDVQQHDAh0b3BjYS5jbJERMA8GA1UECAwIdG9wY2EuY24xCzAJBgNVBAYTAkNOMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCA/bQ9VzG1LGqYJX2SfbMN/Lsh0Q09kV4GEZkwZdqWe
/SQlnQj4EXc3ERgv8vAsqbuZrGNVQgPGiFz6o2oDDz7QDFav/Cp04+0/whBo8BtTlf1k4HmZFrH
/UrOVIJkI2vH0WzXiiTXHMRpxL+hT+Rk2vzr5yWmlJqh
/uuWRIIFXwIDAQABOBEwDwYJKoZIhvcNAQkOMQIwADANBgkqhkiG9w0BAQUFAA0BgQBicKCA1+KP5u4m5Hd1+7J9RPhJ
/eITWnVRVzzKPiwZgTNaUmu5JEPsZs62lJSOCUFys+Lze8EDhphi/3nthKvddZ/Ak38SA1UFOQUuVr
/44qrrls3aSOMi7xhLTEH+qNdn5k/QmnhMXWuqa5WP6CeIZbq4kNiAXQ7mrWmjTRoiZg==

提交

返回

图 3-3 输入服务器证书 CSR

输入注册信息

证书请求信息：

以下项由证书请求中解析出来，请确认是否与产生证书请求时输入的信息一致。

单位名称：(*) topca.cn

部门名称：(*) topca.cn

域名：(*) test-server08

直辖市/省：(*) topca.cn

地址：(*) topca.cn

国家：(*) CN

电子邮件：(*)

用户口令：

这个唯一的验证口令保护您的证书，避免没有被授权的操作，它不能与他人共享
不要丢失！在证书下载和注销时需要它

用户口令：(*) (用户口令至少为8位)

再次输入口令：(*)

天威诚信数字证书使用协议

请仔细阅读下面的使用协议，只有同意遵守本协议才能提交证书申请请求。

北京天威诚信电子商务服务有限公司（以下简称“天威诚信”）根据《中华人民共和国电子签名法》和《天威诚信认证业务规则》的规定提供相应服务，证书持有人应当同意本协议的全部条款并按照页面上的提示完成全部的注册程序。证书持有人在进行注册程序过程中点击“接受”按钮即表示完全接受本协议项下的全部条款。

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。

按电子邮件查询用户证书(推荐)

输入查询条件

电子邮件: (*)

☒ 所有
 ☐ 有效
 ☐ 过期
 ☐ 已注销

查询

返回

按用户名查询用户证书

输入查询条件

用户名: (*) server

☒ 所有
 ☐ 有效
 ☐ 过期
 ☐ 已注销

查询

返回

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。

查询数字证书结果

本次查询找到了以下符合条件的数字证书。

通过点击名称，您可以查看该数字证书的详细信息，或者进行诸如下载或吊销数字证书之类的操作。

共有[1]条

用户名: server1(VAID)

邮箱: server1@t.com
 证书序列号: 2BCBEFFD3E3961F718E441115A6DE79F760AA620
 有效期从 2014/12/23(GMT)到 2015/12/23 (GMT)

返回

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 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。

查询用户证书

输入查询条件

电子邮件:

用户名:

图 3-7 吊销查询页

数字证书信息

姓名: t

电子邮件: 2@qq.com

状态: VALID

有效期: 有效期从2013/04/26(GMT)到 2014/04/26 (GMT)

OU=用户证书注册中心

O=topca

主题: EMAILADDRESS=2@qq.com

CN=t

序列号: 5EC51FA098915D90DF4CCAEC60B8B289014D8122

吊销查到的数字证书

用户口令:

吊销原因:

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。

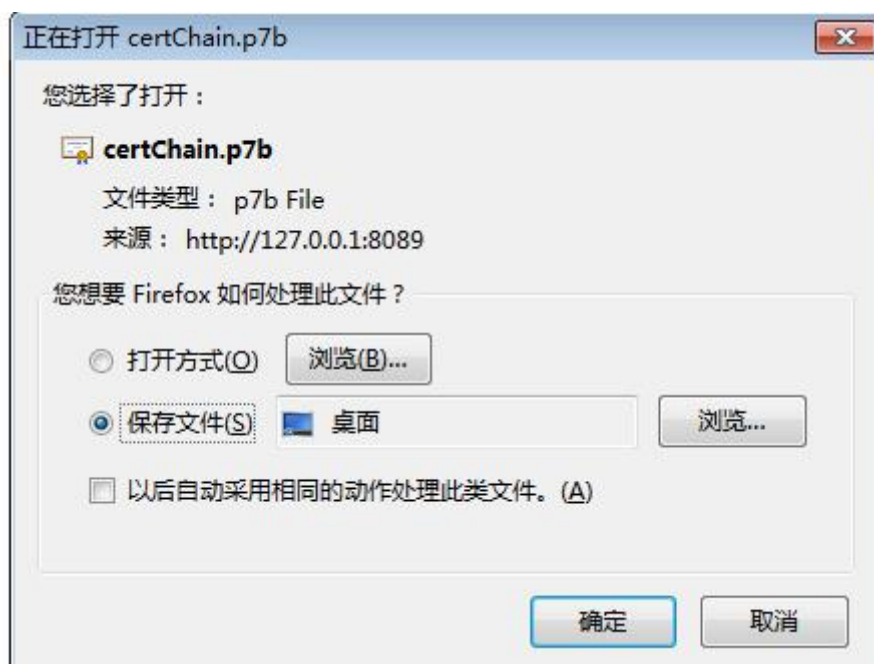


图 3-9 下载服务器证书链



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。



图 3- 11 证书吊销列表

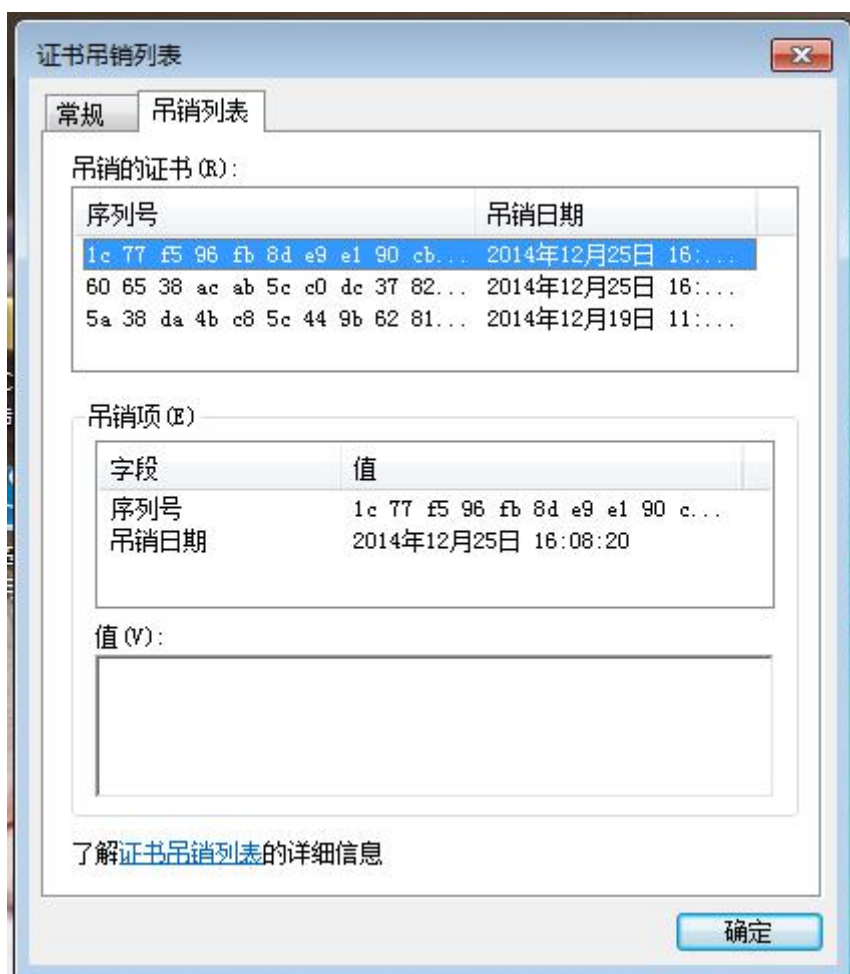


图 3-12 证书吊销列表 1

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

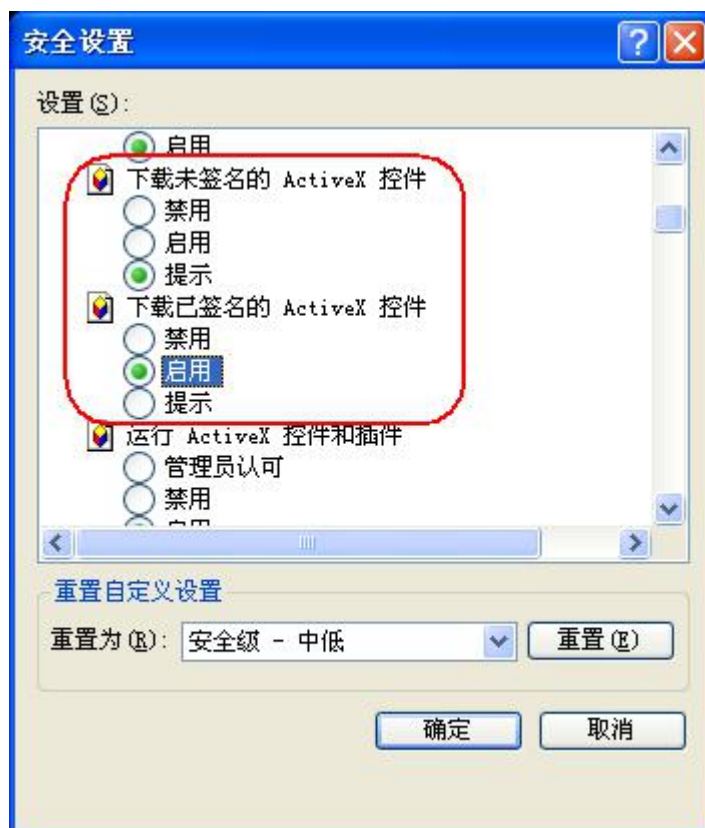


图 4-2 设置 ActiveX 控件选项组

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。

Q: 初始化完成后，登录用户证书服务中心申请用户证书出错。

A: 初始化过程配置信息错误，删除数据库重新初始化即可解决。

Q: 下载吊销列表，数据库出错。

A: 旧版数字认证系统数据库中 ica_global_crl_rec_V2 表中的 crl_buf 字段的类型不为“text”，将其改为 text 类型即可解决。

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

A: web 容器中未设置编码的原因导致，修改 tomcat\conf\目录下 Server.xml 文件中的 URLEncoder="UTF-8"即可，如图 4-3。

```
<Connector port="8080" protocol="HTTP/1.1"  
           connectionTimeout="20000"  
           redirectPort="8443" URLEncoder="UTF-8"/>
```

图 4-3 设置编码