

**CA-Admin**

**V6.3**

**用户手册**

**北京信安世纪科技股份有限公司**

版权声明

本文档受版权保护，未经北京信安世纪科技股份有限公司许可，任何人不得以任何理由和形式使用、复制、传播和编辑本文档，除非是在版权法的许可范围内。

本手册所涉及的案例均是当前情况，北京信安世纪科技股份有限公司有权利随时更改，恕不提前通知。对于本手册内容，包括但不限于隐含的商业性能和特定用途适应性说明，北京信安世纪科技股份有限公司不承担任何责任。

北京信安世纪科技股份有限公司对于因本手册的提供造成的产品性能、使用和操作错误而导致的相关事故或因之引起的损害不承担任何责任。

警告：未经北京信安世纪科技股份有限公司许可，任何人不得对NetCert产品做任何改动，否则将无权继续使用该设备。

商标声明

本手册中所涉及的产品名称仅作识别之用。手册中涉及的其他公司的注册商标或版权属各商标注册人所有，恕不逐一列明。

关于信安世纪

北京信安世纪科技股份有限公司是中国领先的应用安全产品和解决方案供应商，主要为金融、能源、电信等行业和政府机构提供应用安全的产品、解决方案和服务，致力于实现互联网络和企业内部网络的通讯安全、交易安全和网络资源安全保护。

联系信安世纪

**官方网站**: http://www.infosec.com.cn/

**电子信箱**: [support@infosec.com.cn](mailto:support@infosec.com.cn)

**地址**: 北京市西城区宣武门外大街甲一号环球财讯中心C座4层403

**邮编**: 100052

**电话**: 86-10-68025518

86-10-68025528

86-10-68025519（传真）

电话联系时间：周一至周五早9点至晚6点

目录

[版权声明 II](#_Toc18075259)

[商标声明 II](#_Toc18075260)

[关于信安世纪 II](#_Toc18075261)

[联系信安世纪 II](#_Toc18075262)

[目录 IV](#_Toc18075263)

[第1章 引言 1](#_Toc18075264)

[1.1 编写目的 1](#_Toc18075265)

[1.2 适用对象 1](#_Toc18075266)

[1.3 参考资料 1](#_Toc18075267)

[第2章 产品简介 2](#_Toc18075268)

[2.1 概述 2](#_Toc18075269)

[2.2 功能特点 2](#_Toc18075270)

[第3章 CA-Admin介绍 2](#_Toc18075271)

[3.1 环境要求 2](#_Toc18075272)

[3.2 安可环境 3](#_Toc18075273)

[3.3 目录结构 3](#_Toc18075274)

[第4章 CA-Admin的使用 4](#_Toc18075275)

[4.1 概述 4](#_Toc18075276)

[4.2 CA-Admin的配置 4](#_Toc18075277)

[4.2.1 前提 4](#_Toc18075278)

[4.2.2 软件配置 5](#_Toc18075279)

[4.2.2.1 配置CA-Server服务器信息 6](#_Toc18075280)

[4.2.2.2 SM2算法驱动名称配置 6](#_Toc18075281)

[4.3 下载管理员证书 7](#_Toc18075282)

[4.4 管理员登录 9](#_Toc18075283)

[4.5 超级管理员功能 11](#_Toc18075284)

[4.5.1 新建业务管理员 12](#_Toc18075285)

[4.5.2 查看BA信息 13](#_Toc18075286)

[4.5.3 修改BA信息 14](#_Toc18075287)

[4.5.4 作废BA证书 14](#_Toc18075288)

[4.5.5 重获BA证书 15](#_Toc18075289)

[4.6 业务管理员功能 15](#_Toc18075290)

[4.6.1 新建BO管理员 16](#_Toc18075291)

[4.6.2 查看BO信息 17](#_Toc18075292)

[4.6.3 修改BO信息 18](#_Toc18075293)

[4.6.4 作废BO证书 18](#_Toc18075294)

[4.6.5 重获BO证书 19](#_Toc18075295)

[4.6.6 BO授权 19](#_Toc18075296)

[4.6.6.1 用户操作权限 20](#_Toc18075297)

[4.6.6.2 模板操作权限 20](#_Toc18075298)

[4.6.6.3 提交操作授权 21](#_Toc18075299)

[4.6.6.4 修改操作授权 21](#_Toc18075300)

[4.7 业务操作员功能 21](#_Toc18075301)

[4.7.1 用户管理 21](#_Toc18075302)

[4.7.1.1 注册用户 22](#_Toc18075303)

[4.7.1.2 下载证书 23](#_Toc18075304)

[4.7.1.3 查询用户/证书 25](#_Toc18075305)

[4.7.2 证书管理 26](#_Toc18075306)

[4.7.2.1 证书更新 26](#_Toc18075307)

[4.7.2.2 获取两码 27](#_Toc18075308)

[4.7.2.3 冻结证书 27](#_Toc18075309)

[4.7.2.4 解冻证书 28](#_Toc18075310)

[4.7.2.5 作废证书 28](#_Toc18075311)

[4.7.3 RA管理 28](#_Toc18075312)

[4.7.3.1 查看RA管理员信息 29](#_Toc18075313)

[4.7.3.2 创建RA 30](#_Toc18075314)

[4.7.3.3 修改RA信息 31](#_Toc18075315)

[4.7.3.4 作废RA证书 31](#_Toc18075316)

[4.7.3.5 重获RA证书 31](#_Toc18075317)

[4.7.3.6 RA授权 32](#_Toc18075318)

[4.7.4 模板管理 34](#_Toc18075319)

[4.7.4.1 查看模板列表 34](#_Toc18075320)

[4.7.4.2 查看模板详细信息 35](#_Toc18075321)

[4.7.4.3 添加模板 37](#_Toc18075322)

[4.7.4.4 添加签名模板 38](#_Toc18075323)

[4.7.4.5 添加加密模板 46](#_Toc18075324)

[4.7.4.6 修改模板 46](#_Toc18075325)

[4.7.4.7 克隆模板 48](#_Toc18075326)

[4.7.4.8 删除模板 49](#_Toc18075327)

[4.7.4.9 作废模板 50](#_Toc18075328)

[4.7.4.10 特殊说明 50](#_Toc18075329)

[4.8 审计管理员功能 50](#_Toc18075330)

[4.8.1 新建审计员 51](#_Toc18075331)

[4.8.2 查看审计员信息 52](#_Toc18075332)

[4.8.3 修改审计员信息 52](#_Toc18075333)

[4.8.4 作废审计员证书 53](#_Toc18075334)

[4.8.5 重获审计员证书 53](#_Toc18075335)

[4.9 审计员功能 54](#_Toc18075336)

[4.9.1 待审计日志 54](#_Toc18075337)

[4.9.1.1 查询待审计日志 54](#_Toc18075338)

[4.9.1.2 查看待审计日志详情/日志审计 55](#_Toc18075339)

[4.9.2 已审计日志 58](#_Toc18075340)

[4.9.2.1 查询已审计日志 58](#_Toc18075341)

[4.9.2.2 查看审计日志详情/日志审计 59](#_Toc18075342)

[4.9.2.3 查看日志审计详情 62](#_Toc18075343)

[4.9.3 日志归档 63](#_Toc18075344)

[4.9.3.1 设置归档任务 64](#_Toc18075345)

[4.9.3.2 归档任务查看 65](#_Toc18075346)

[4.9.4 归档日志 65](#_Toc18075347)

[4.10 CA-Admin异常排查 67](#_Toc18075348)

[附录B：ＣＡ管理体系图 68](#_Toc18075349)

# 引言

## 编写目的

本手册详细介绍了CA-Admin产品的安装、配置与使用，指导用户正确使用该产品。

## 适用对象

本手册适用对象为售前、产品实施及技术支持人员、网络管理员、以及测试人员等，假定具备以下概念知识：

* PKI知识和标准
* 数据库
* 应用服务器
* LDAP

## 参考资料

X509因特网公钥技术设施证书和证书作废列表：rfc5280

<http://www.ietf.org/rfc/rfc5280.txt>

X509因特网公钥基础设施在线证书状态协议：rfc2560

<http://www.ietf.org/rfc/rfc2560.txt>

# 产品简介

## 概述

CA-Admin是CA-Server的管理终端程序，通过CA-Admin，可以用来下载管理员证书，使用管理员证书登录CA-Server，进行各种策略控制和管理功能。

## 功能特点

CA的业务操作员，可以通过CA-Admin进行用户管理、以及证书申请、冻结、解冻、作废等操作。

CA-Admin的主要功能：在没有RA系统的情况下，对NetCert产品的其他系统，比如KMC Server、OCSP Server进行初始化时，需要各种管理员证书及系统证书，均可通过CA-Admin进行申请与下载。

不建议使用CA-Admin管理用户：由于CA-Admin无法审核用户的身份，故不建议使用该方法进行最终用户证书的下载。

# CA-Admin介绍

## 环境要求

* 软件环境：
* java8；
* 适配过的国密USBKey：
* 海泰ISSKFAPI31001（驱动文件ISSKFAPI31001.dll）

## 安可环境

* 产品没有提供linux的java运行环境。要求系统有能够正常使用的jre8运行环境。如果系统中的java必须以绝对路径调用，请修改start.sh，在java命令前加上绝对路径。
* 对start.sh给予执行权限，需要在图形界面环境下执行此启动脚本。
* 查看java运行环境的版本：java -version
* 需使用支持安可运行环境的USBkey国密驱动库

## 目录结构

1. 将CA-Admin压缩包拷贝至某一路径下，并解压至某一目录中。
2. 解压完成，进入程序目录查看目录结构，如下表所示：

|  |  |
| --- | --- |
| 文件及目录 | 说明 |
| jre/ | 64位Java运行环境（jre8 for windows） |
| lib/ | 运行需要的支持包 |
| res/ | 资源文件 |
| log/ | 运行过程中日志记录 |
| doc/ | 使用手册 |
| start.bat | Windows环境下的启动脚本 |
| start.sh | Linux环境下程序的启动脚本 |

（以上程序携带文件，不得自行修改和删除）

（3）程序运行过程中，产生的文件：

|  |  |
| --- | --- |
| 文件及目录 | 说明 |
| log/error.log | 程序运行过程中的错误日志 |
| caadmin.cfg | 程序运行过程中需要的配置文件 |
| key.cfg | 程序运行过程中需要的驱动配置文件 |

（以上程序产生的文件，不得自行修改和删除）

Windows版本的安装包里自带jre 文件，start.bat脚本指定了jre/bin/java 工具用来启动程序。

Linux版本中没有jre文件，start.sh脚本使用系统配置的jre启动程序，在执行脚本之前，请检查系统是否安装jre并配置环境变量。（jre的最低版本为64位操作系统的jre1.8）

# CA-Admin的使用

## 概述

本章将介绍如何通过CA-Admin来实现CA-Server的策略管理与配置。请严格按照步骤使用该软件。

## CA-Admin的配置

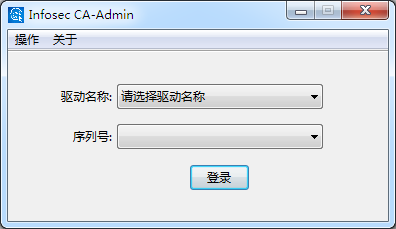
### 前提

在使用该软件之前，请确定存在一个已完成初始化并处于激活状态的CA-Server服务。

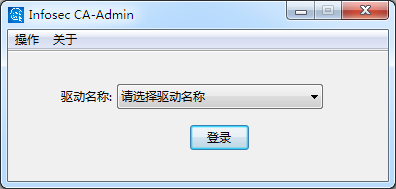
### 软件配置

Windows系统双击start.bat文件即可启动程序。（Linux系统双击start.sh启动程序）

默认以SM2算法设定显示登录页面，启动之后的程序登录页面如下图所示：



通过在CA-Admin端修改CA-Server的配置信息为RSA之后，启动之后的程序登录页面如下图所示：



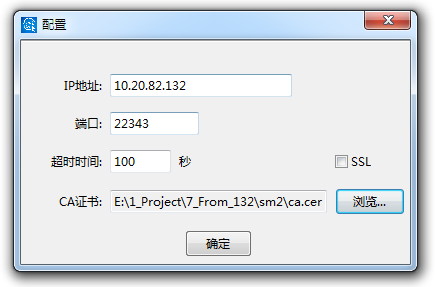
软件使用需要：

配置CA-Server服务器信息；

如果是SM2算法还需要配置USBKey驱动名称；

#### 配置CA-Server服务器信息

在登录界面，选择【操作】/【配置】，弹出配置对话框，如下图所示：



**IP地址：**CA-Server管理服务所绑定的IP地址，默认为服务器地址；

**端口**：CA-Server管理服务所绑定的端口，默认为22343；

**超时时间：**客户端与CA-Server之间的通信超时时间；

**通讯方式：**应与CA-Server管理服务中配置的通讯方式一致，比如CA管理服务中配置的是内部协议，那么此处必须选择内部协议。如果CA-Server管理服务配置为SSL通信，此处应该勾选SSL项。

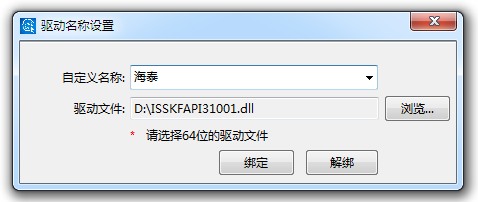
**CA证书：**与之通讯的CA根证书；无论是否选择SSL通讯，都需要配置此项

#### SM2算法驱动名称配置

为了方便对不同厂商的USBKey以及同一厂商不同操作系统的驱动文件进行区分，增加了驱动名称设置功能，提供驱动文件的自定义名称设置，可以在登录页面和下载证书页面显示自定义的的名称。

**如果CA-Server是SM2的算法，此时需要配置驱动名称。RSA则不需要。**

在登录界面，选择【操作】/【驱动名称设置】，弹出设置对话框，如下图所示：

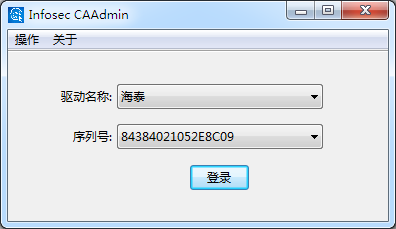


**自定义名称：**使用者自行定义的名称；

**驱动文件：**USBKey的驱动文件，用来操作USBKey;

提醒：选择文件时，严格按照提示根据【操作系统】选择驱动文件。

配置完成之后的登录页面显示如下图：（如果没有显示序列号，请通过下拉框选定驱动名称）

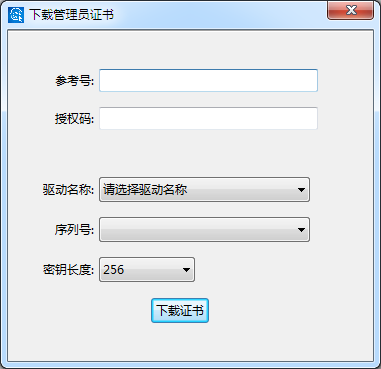


## 下载管理员证书

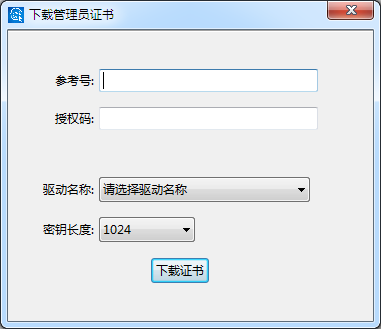
配置完毕后，便可连接CA-Server进行管理员证书下载操作了，CA-Server初始化完成之后，分别提供了超级管理员和审计管理员的两码，用来下载管理员的证书，超级管理员和审计管理员的证书均通过CA-Admin下载。

在CA-Admin登录界面，选项菜单【操作】/【下载管理员证书】，系统弹出下载管理员证书窗口，正确填写参考号和授权码，选择密钥长度，进行管理员证书下载。（支持下载SA/AA/BA/BO/AO管理员证书）

SM2算法的下载管理员证书页面显示如下图：



RSA算法下载管理员证书页面显示如下图：



**参考号和授权码：**

SA和AA的两码来自于CA-Server初始化时生成；

其他管理员两码在创建管理员时产生。

**驱动名称：**

SM2算法的驱动名称显示为之前配置时绑定的驱动名称；

RSA算法的驱动名称显示为系统中的所有CSP驱动名称。

**序列号：**

SM2算法读取插入的USBKey的序列号，

RSA算法在点击【下载证书】之后选择下载到哪个USBKey中，如果只有一个USBKey，则不用选择，直接下载到USBKey中。

**密钥长度：**SM2只支持256的密钥，RSA支持1024和2048两种长度。

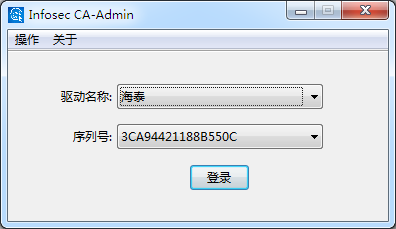
**下载证书**：下载证书并保存到USBKey中。

## 管理员登录

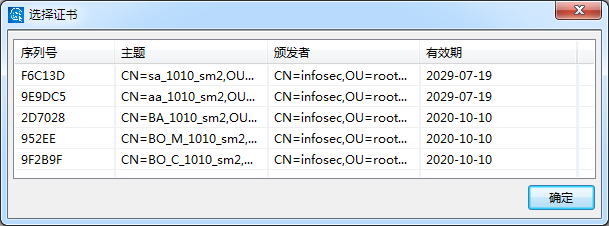
在完成CA-Admin的配置之后，可以使用管理员证书登录。

在客户端插入存有管理员证书的USBKey，执行启动脚本启动。

**SM2算法的登录**页面如下图：（如果没有显示序列号，请通过下拉框选定驱动名称）



选择合适的驱动名称，选择保存登录证书的USBKey的序列号，点击【登录】，点击之后的显示页面如下图：（如果USBKey中只有一张证书，就直接使用唯一的证书登录，不再显示【选择证书】视图）



**RSA算法的登录**页面如下图：

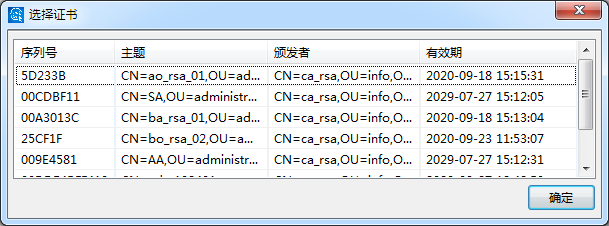


选择合适的驱动名称，点击【登录】，

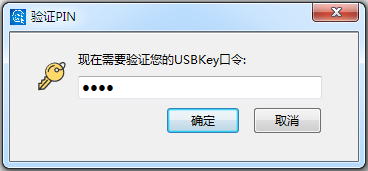
如果终端有多个USBKey，需要选择存有管理员证书的USBKey，

如果只有一张USBKey，则默认选择USBKey，

通过筛选（管理员证书与配置的CA根证书颁发者一致），列出符合条件的证书。如下图：



选择证书之后，点击【确定】按钮，使用选中的证书登录。在选中证书登录的时候，USBKey需要验证身份，请输入正确的PIN码。输入PIN码视图如下：（RSA可能略有不同）

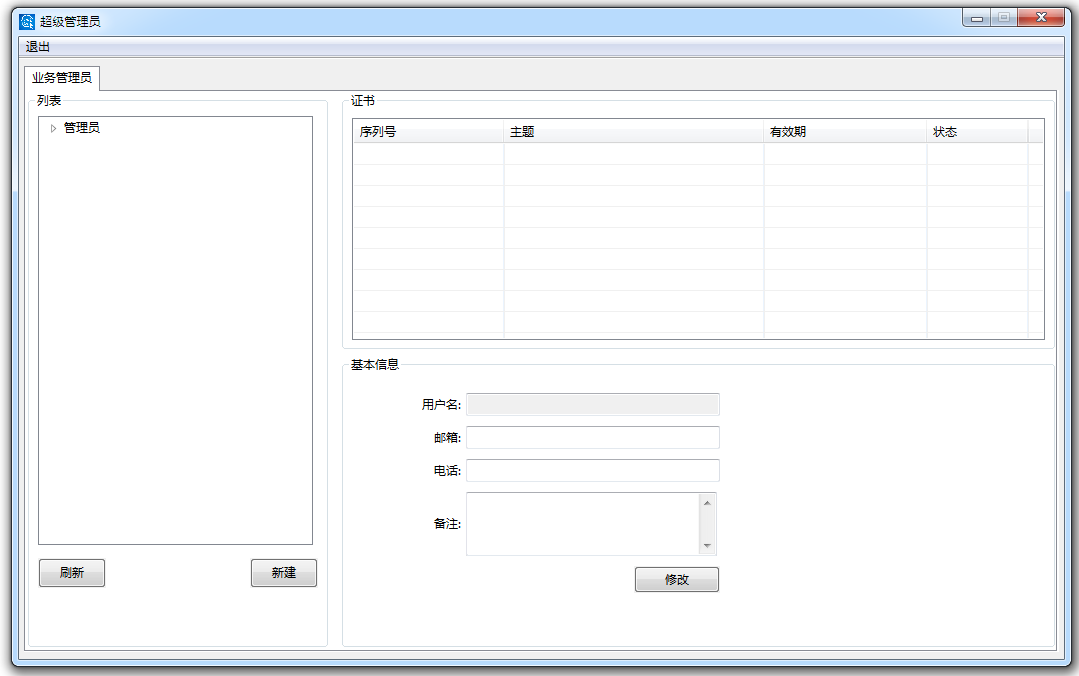


输入PIN码之后，点击【确定】按钮。如果CA-Server验证证书通过，便可登录成功，进入相应管理员的操作界面，不同的管理员角色拥有不同的操作权限，因此CA-Admin展现视图内容也不一样，下面将逐一介绍各个管理员的操作权限，管理员视图在RSA算法和国密算法情况下，几乎一致，如无特殊之处，不再区别展示。

提醒：如果通讯方式采用“SSL通讯”，则管理员进行CA-Admin登录的前提是“在配置CA-Server服务器信息时，勾选【SSL】项”，否则登录失败。

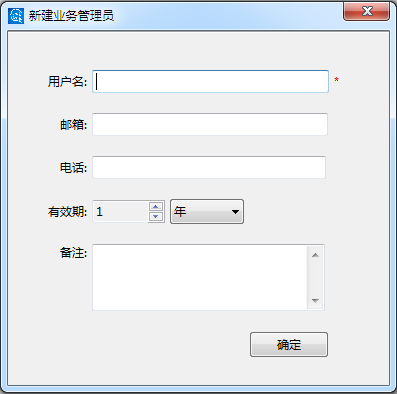
## 超级管理员功能

超级管理员（以下简称为‘SA’）：主要的功能是管理业务管理员（以下简称为‘BA’），包括新建管理员、查看管理员信息、修改管理员信息、作废管理员证书、重获管理员证书。

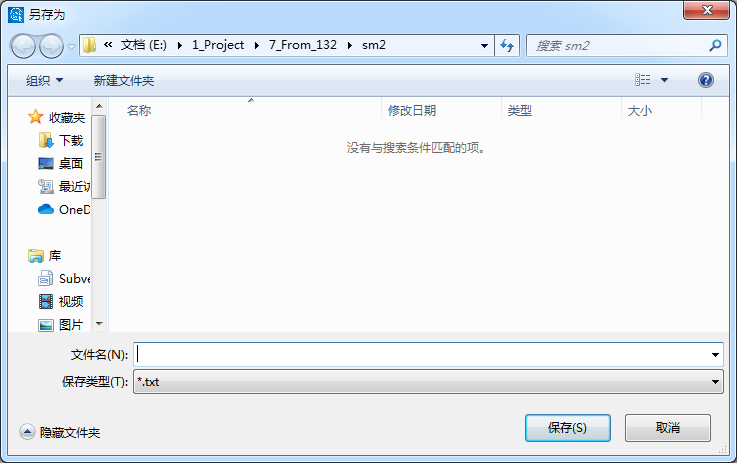


### 新建业务管理员

点击【新建】按钮，弹出新建对话框，其中用户名、有效期长度和有效期单位为必填项，其他为选填项，填写完毕点击【确定】按钮进行创建。



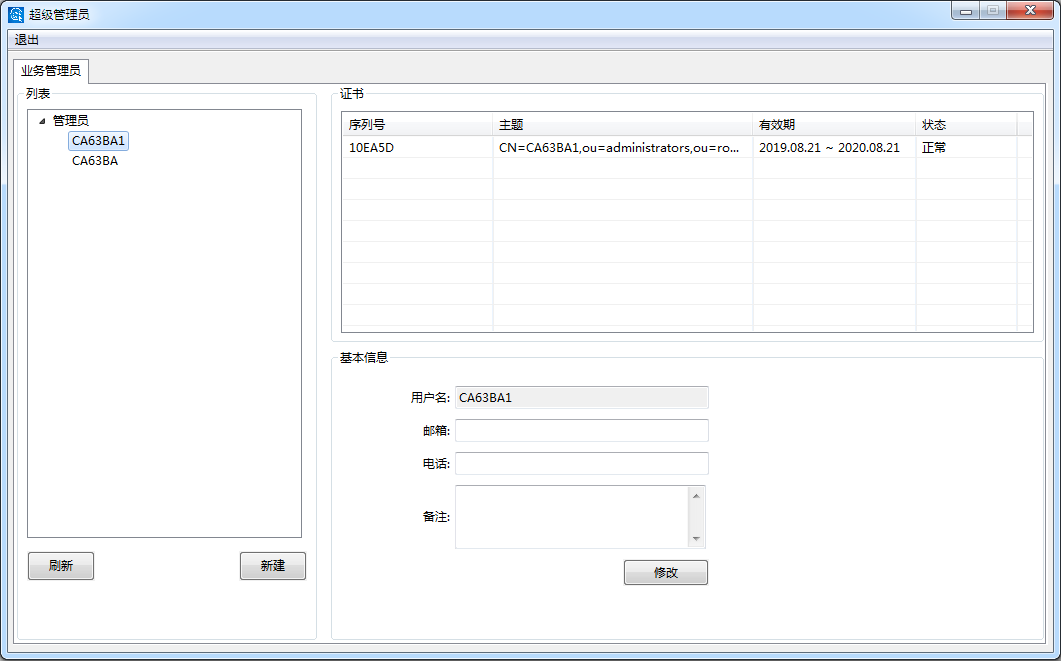
创建成功会弹出【另存为】对话框，如下图：



选择路径后保存【两码文件】完成新建管理员操作。

完成新建管理员操作之后，在【登录页面】的菜单栏选择【操作】/【下载管理员证书】利用管理员的两码下载管理员证书到USBKey中，之后就可以使用该管理员证书登录CA-Admin。

### 查看BA信息

点击【刷新】按钮，左侧列表区显示所有的BA管理员名单，选中某一个BA管理员，可以在【证书】和【基本信息】部分显示该管理员的证书信息和用户信息。

**证书部分：**序列号、主题、有效期、状态

**基本信息部分：**用户名、邮箱、电话及备注。

### 修改BA信息

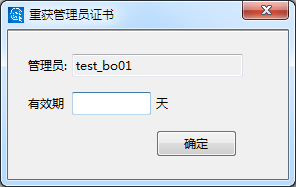
在BA列表中，选中某个管理员，在【基本信息】部分可以直接修改管理员信息，只支持修改邮箱、电话、备注信息，点击【修改】按钮即可完成修改。

### 作废BA证书

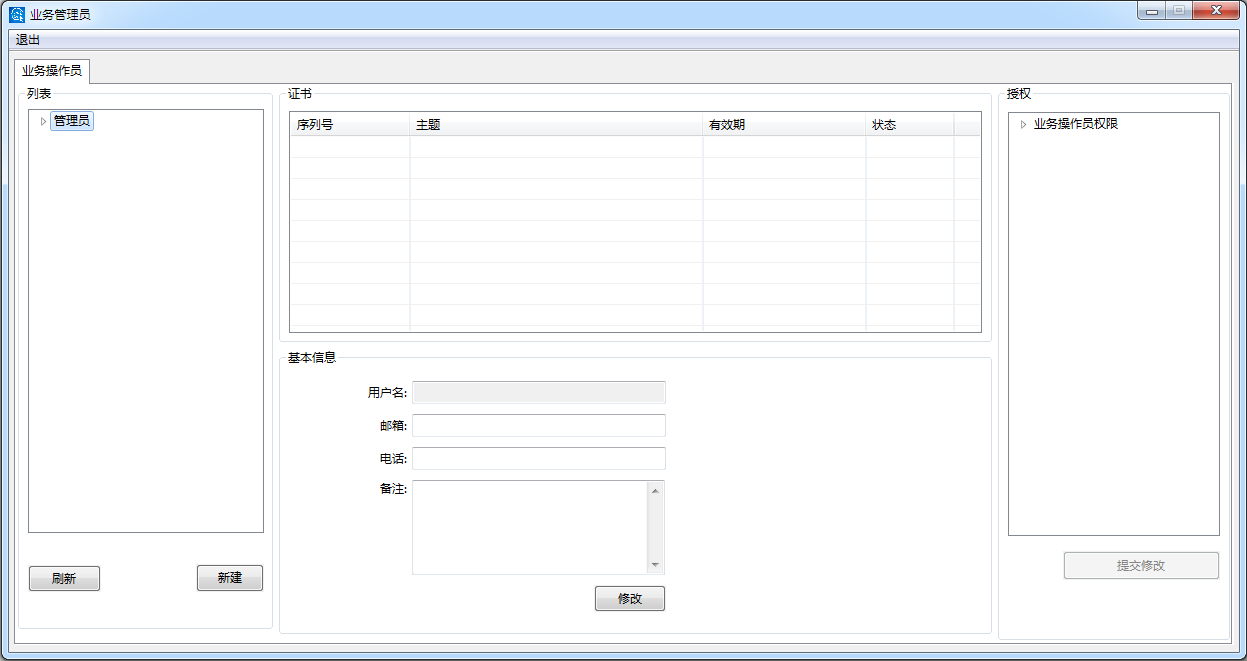
在BA视图的【证书】部分，选中待作废的证书记录，右击鼠标选择【作废管理员证书】按钮，弹出【确定对话框】，再次确认即可作废证书。证书一旦作废成功，则该BA将无法登录CA-Admin。

### 重获BA证书

对于已作废的证书，可以进行【重获管理员证书】操作，在【证书】区选中状态为作废的证书，右击鼠标选择菜单中的【重获管理员证书】，弹出对话框，填写新证书的有效期，点击申请按钮，弹出【另存为】对话框，选择保存路径后保存【两码文件】，两码保存成功之后，可以通过【登录页面】菜单栏的【操作】/【下载管理员证书】按钮重新下载证书。

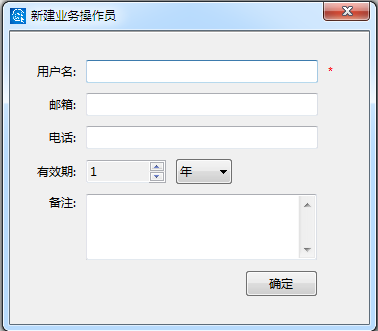


## 业务管理员功能

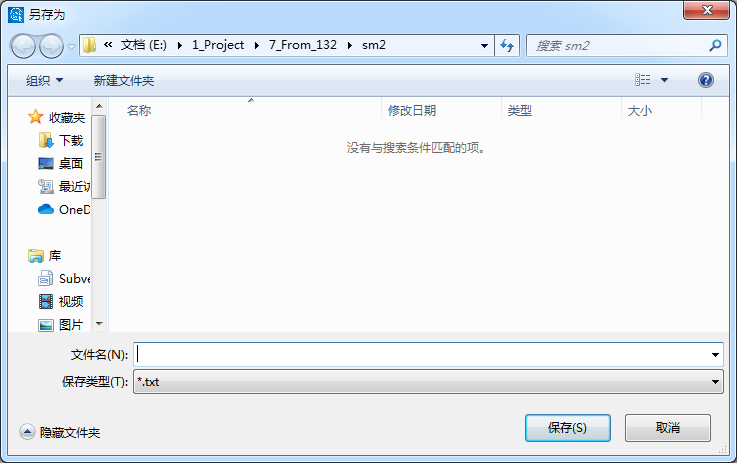
BA主要功能：管理业务操作员（以下简称为‘BO’）。包括：新建管理员、查看管理员信息、修改管理员信息、作废管理员证书、重获管理员证书、业务管理员授权。

### 新建BO管理员

点击【新建】按钮，弹出新建对话框，其中用户名、有效期长度和有效期单位为必填项，其他为选填项，填写完毕点击【确定】按钮进行创建。



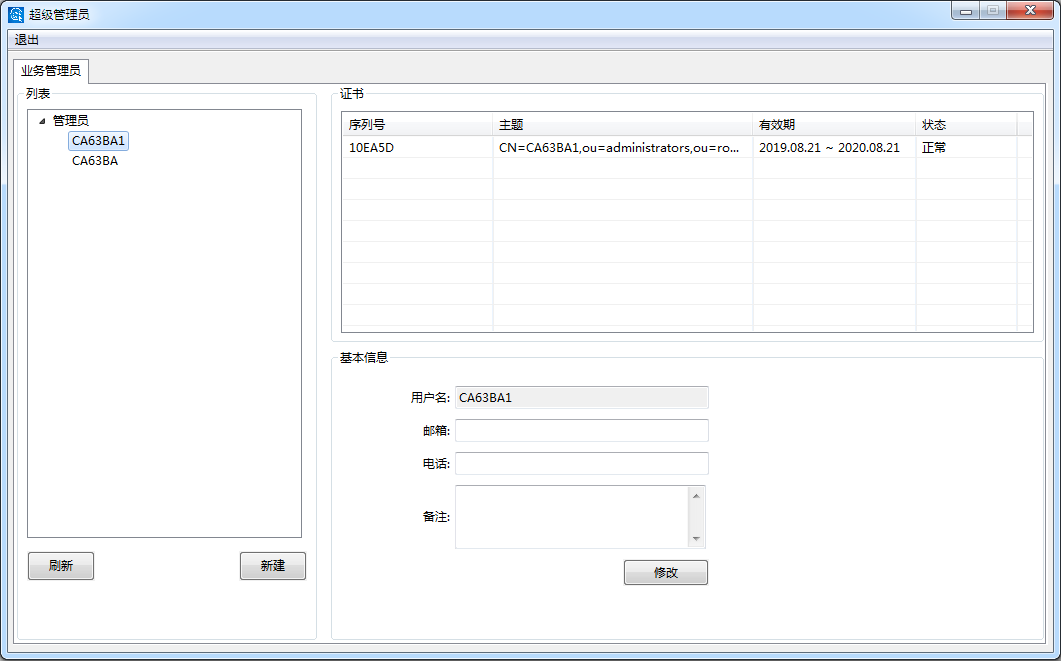
系统会弹出【另存为】对话框，如下图：



选择路径后保存【两码文件】完成新建管理员操作。

完成新建管理员操作之后，在【登录页面】菜单栏选择【操作】/【下载管理员证书】利用该两码下载新的管理员证书到USBKey中，下载完成之后就可以使用该管理员的证书登录CA-Admin。

### 查看BO信息

点击【刷新】按钮，左侧列表区显示所有的BO管理员列表，选中某个BO管理员，可以在【证书】和【基本信息】部分显示该管理员的证书信息和用户信息。

**证书部分：**序列号、主题、有效期、状态，

**基本信息部分：**用户名、邮箱、电话及备注。

### 修改BO信息

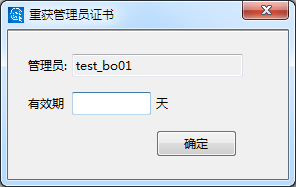
在BO列表中，选中待修改的管理员，在【基本信息】部分直接修改管理员信息，只支持修改邮箱、电话、备注。点击【修改】按钮即可完成修改。

### 作废BO证书

在BO页面的【证书】区，选中待作废的证书，右击鼠标选择【作废管理员证书】按钮，弹出确定对话框，再次确认即可作废证书。证书一旦作废成功，则该BO将无法登录CA-Admin。

### 重获BO证书

对于已作废证书，可以进行【重获管理员证书】操作，在【证书】部分，选中对应的证书，右击选择菜单中的【重获管理员证书】按钮，弹出对话框，填写新证书的有效期，点击确定按钮，弹出【另存为】对话框，选择路径后保存文件，保存成功之后，可以通过【登录页面】的菜单栏的【操作】/【下载管理员证书】按钮下载证书。



（备注：对于证书状态为正常的操作员，无法执行该操作）

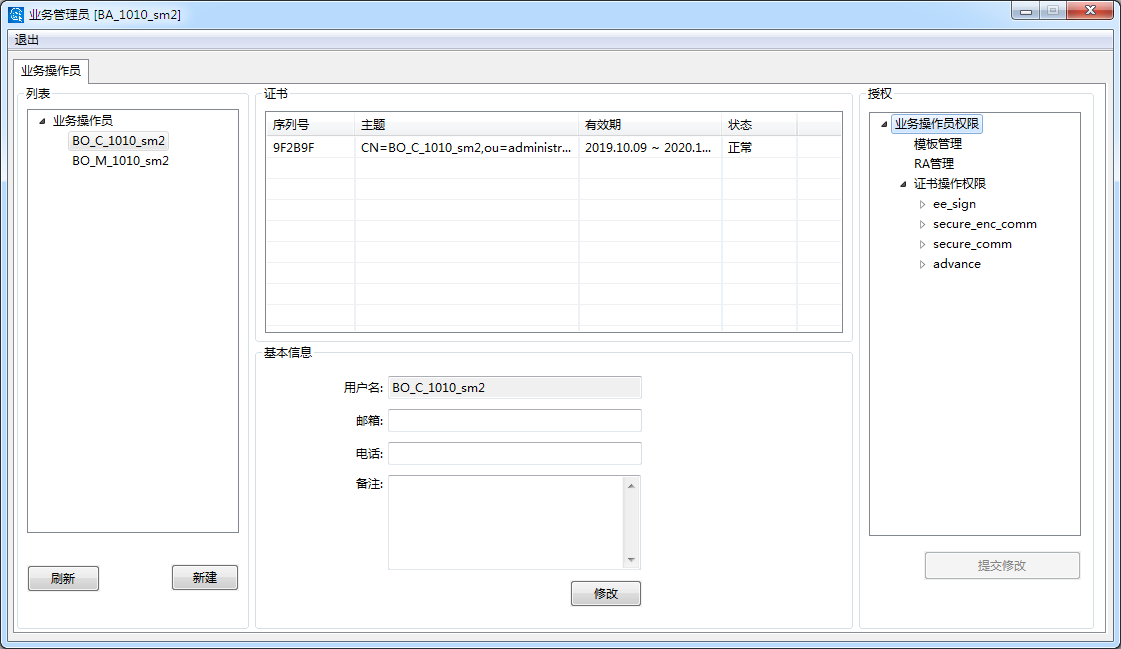
### BO授权

对于已经下载证书的BO管理员，可以进行授权操作，选中要授权的BO，可以在【授权】部分，根据自己的需要给BO管理员添加合适的操作权限。

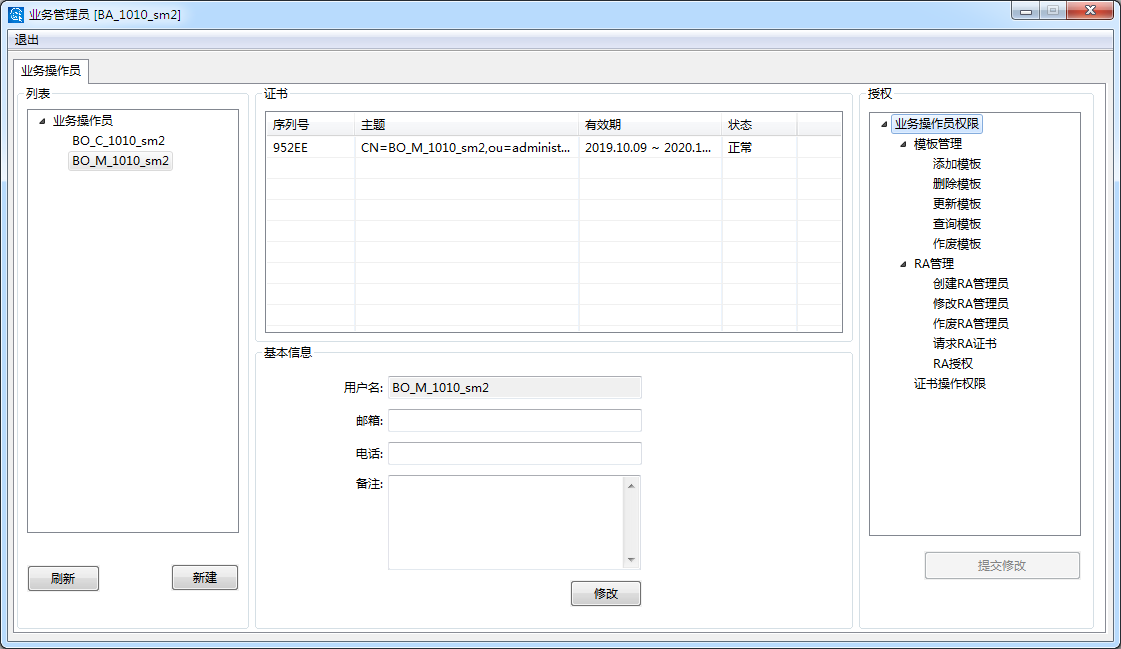
BO管理员的权限包括证书管理、模板管理、RA管理。其中模板管理和RA管理可以授权给同一个BO管理员，证书管理只能授权给没有管理权限的BO管理员。

注意：模板管理是对模板进行增删改查的操作，证书管理是对该BO管理员授权对某个模板下证书的操作权限，包括申请该模板的证书、下载该模板的证书等。

具有证书操作权限的BO管理员示意图如下：



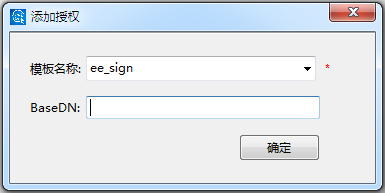
具有模板和RA管理权限的BO管理员视图如下：



提醒：BO管理员需要授权才能登录CA-Admin

#### 证书操作授权

在【授权】区，添加模板操作权限，添加功能如下图：



选择要授权的模板、并正确填写baseDN（baseDN填写\*代表baseDN可以是任何结构，及用户证书主题可以任意填写，均可正常签发），点击【确定】按钮进行保存即可。

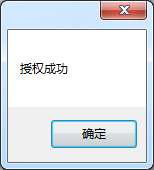
添加模板权限时，默认添加的模板权限有：申请证书、重取两码、更新证书、密钥恢复、冻结证书、解冻证书、作废证书。

#### 模板和RA授权

在【授权】区，选中想授权的权限，右击选择添加权限即可。

#### 提交操作授权

授权信息添加完成之后，通过【提交修改】按钮提交新的授权情况。提交成功，会有授权成功提示。



#### 修改授权

修改授权与添加授权类似，依次修改证书操作权限、模板管理权限和RA管理权限。之后通过【提交修改】按钮提交即可。

## 业务操作员功能

BO管理员在登录之前需要先通过BA 对BO管理员做授权操作。

BO管理员分为权限管理员和证书管理员，权限管理员功能包括RA管理和模板管理，证书管理员功能包括申请证书、下载证书、作废证书等。

BO的功能主要有：证书管理、模板管理、RA管理。

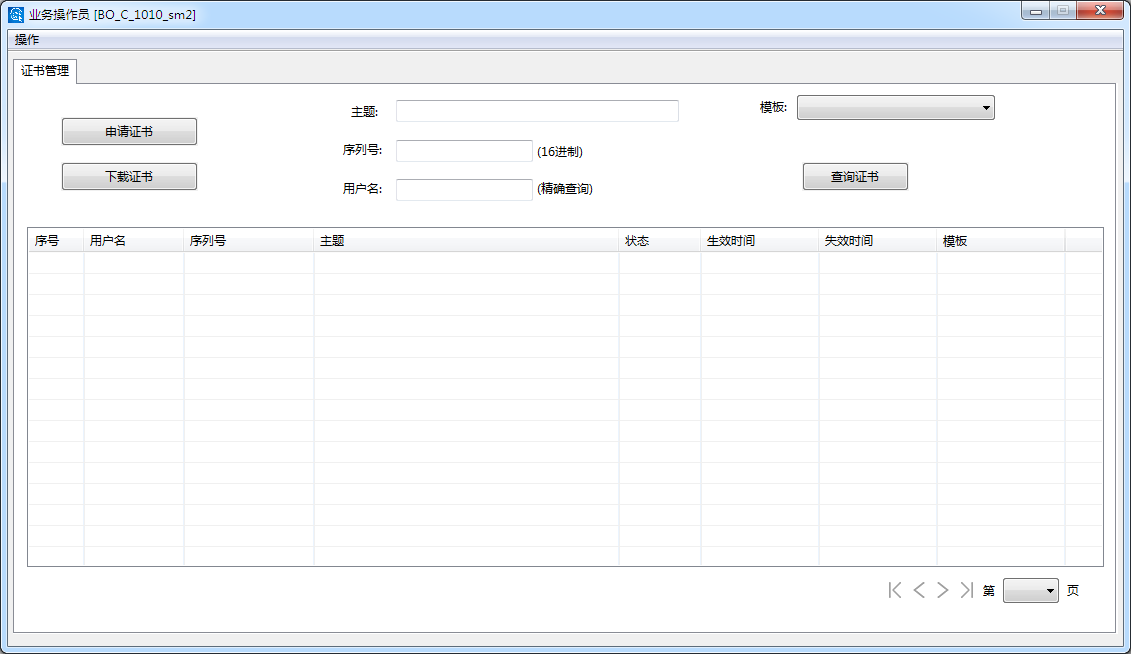
BO 还具有产生CA的证书请求的功能和查询该BO权限的功能。

产生CA证书请求用于产生该CA公钥的一个证书请求，使用该证书请求向其他CA申请证书，该CA便可作为签发证书根CA的子CA。

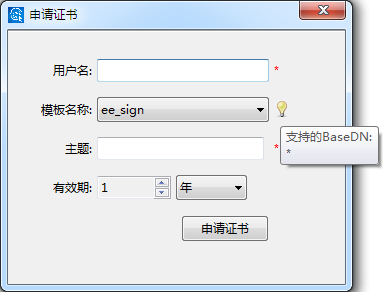
查询BO管理员权限，有助于了解该BO是否有管理RA或者管理模板的权限，或者是否有某些模板的操作权限。

### 证书管理

具有证书管理权限的BO管理员只能操作证书，BO对证书的操作有：申请证书、下载证书、查询证书、证书更新、获取两码、冻结证书、解冻证书、作废证书。BO视图如下：



#### 申请证书



用户名和主题为必填。

**用户名：**没有唯一限制，请尽量填写其他内容便于区分同名用户；

**模板名称：**模板列表为该BO管理员被BA授权的模板；

**BaseDN：**在BA对BO授权时添加的模板的BaseDN,主题名称应按这个格式添加，如有疑问，请参考4.6.6.2。

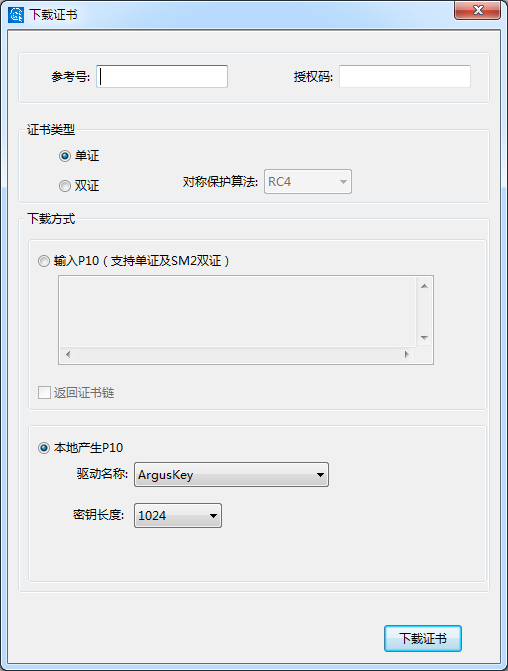
**证书主题：**填写完整的用户证书主题；

**有效期长度**：填写证书有效期天数、选择单位。

填写完成后点击【注册用户】按钮。用户注册成功会生成两码，弹出文件保存对话框，保存【两码文件】，以便下载证书。

#### 下载证书

申请证书成功之后，可以使用保存的两码下载用户证书，点击【下载证书】按钮，下载证书视图如下图所示：



依次输入参考号和授权码，选择证书类型，选择下载方式，然后点击【下载证书】按钮，下载证书。

**参考号和授权码：**在用户注册时得到的两码；

**证书类型：**单证为签名证书，双证为签名证书和加密证书，根据申请证书时选择的模板确定。（下载证书时选择的证书类型需要和申请证书时选择的模板类型一致）

**下载方式：**

输入P10：将客户端产生的证书请求的Base64内容复制到文本框中。如果勾选了【返回证书链】，返回的证书信息为带证书链的格式即p7b。

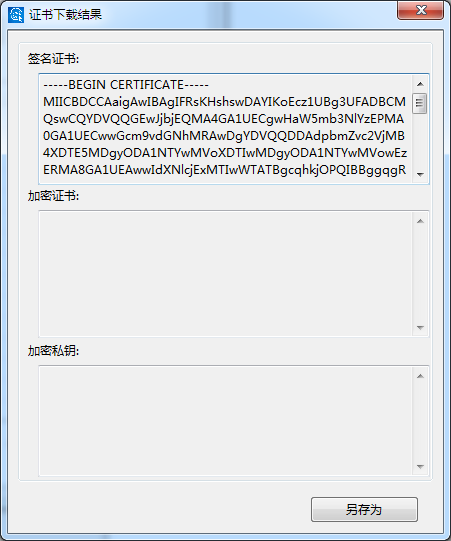
本地产生P10：选择USBKey产生P10。

填写完所有信息后点击【下载证书】按钮，进行证书下载。

**返回结果：**

* 输入P10下载证书

下载证书的结果以视图方式显示，如下图：



输入P10下载证书支持SM2单证、SM2双证、RSA单证。

单证下载只有签名证书信息；

国密SM2的双证下载，返回信息有签名证书、加密证书和加密私钥；

返回的证书格式默认为CERT，如需要证书链格式，请在下载页面勾选【返回证书链】。

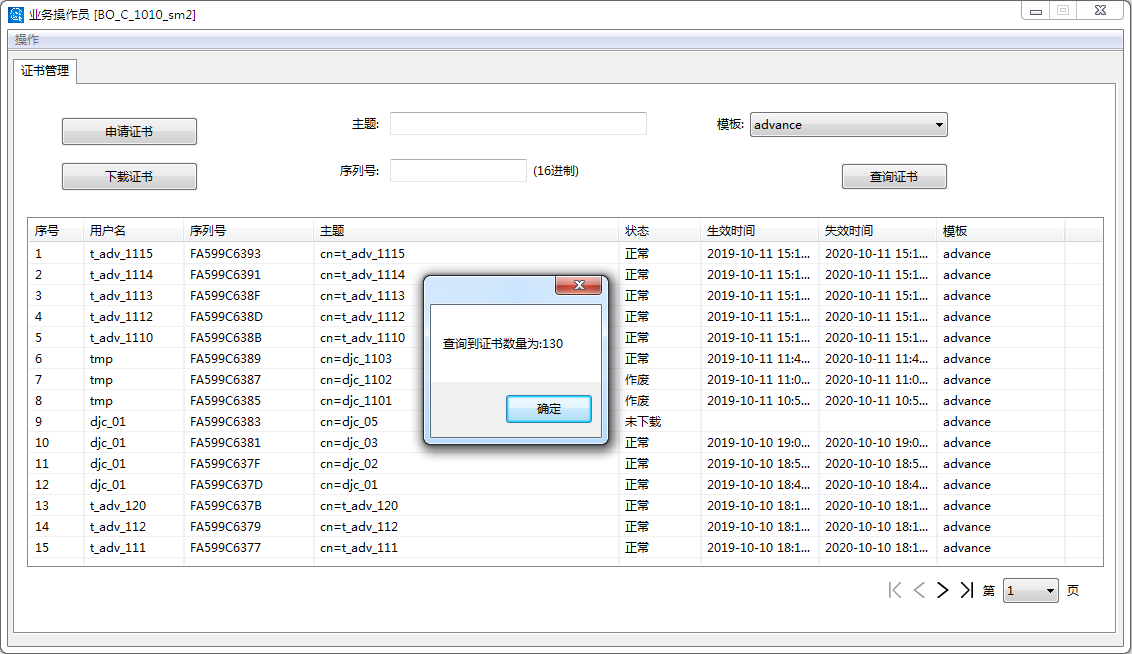
通过【另存为】按钮可以将信息保存到文件中，之后通过截取文件内容保存为.cer证书文件。也可以直接复制证书信息保存为.cer证书文件。

* 本地产生P10下载证书

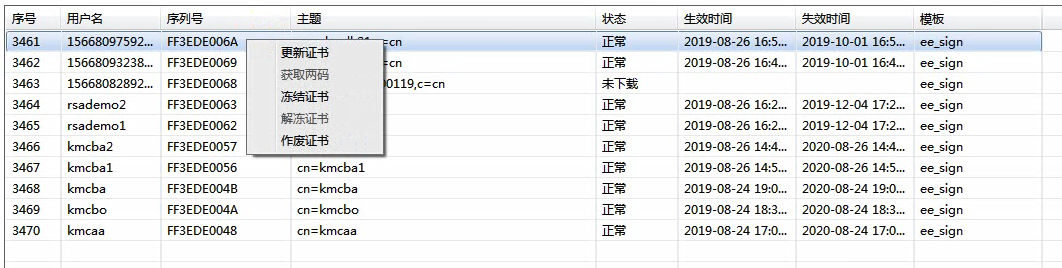
选择合适的驱动名称、密钥长度、序列号（SM2点击【下载证书】按钮之前选择，RSA点击【下载证书】之后选择），点击【下载证书】按钮即可下载证书，证书会下载到指定的USBKey中，下载完成之后，可以通过相应的USBKey管理工具查看证书下载情况。

#### 查询证书

在【证书管理】视图中，可以通过主题，序列号，模板进行证书查询，输入至少一个查询条件，查询结果如下图所示：



查询结果包括：用户名、序列号、主题、状态、生效时间、失效时间、模板。



选中某个证书记录，右击可以对该证书做证书管理，包括：更新证书、获取两码、冻结证书、解冻证书、作废证书。

#### 证书更新

在证书列表中右键单击一条证书状态为【已下载】的条目，在弹出菜单中选择【证书更新】。出现如下对话框：



只需输入新证书的有效期天数和选择日期单位，点击【更新证书】按钮即可。如果选择的是双证证书的话，则签名/加密两张证书将被一起更新，且有效期天数相同，更新成功会提示【保存两码】，之后通过两码下载新的证书。

#### 获取两码

对于待下载的证书，如果忘记两码或两码过期，可重取两码。

在证书列表中选择状态为【待下载】的证书，在右键菜单中选择【重取两码】。成功后，系统将提示保存新的两码。

#### 冻结证书

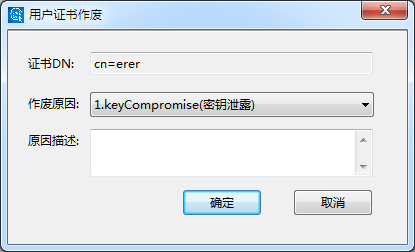
在证书列表中选择状态为【正常】的证书，在右键菜单中选择【冻结证书】。

#### 解冻证书

在证书列表中选择状态为【冻结】的证书，在右键菜单中选择【解冻证书】。

#### 作废证书

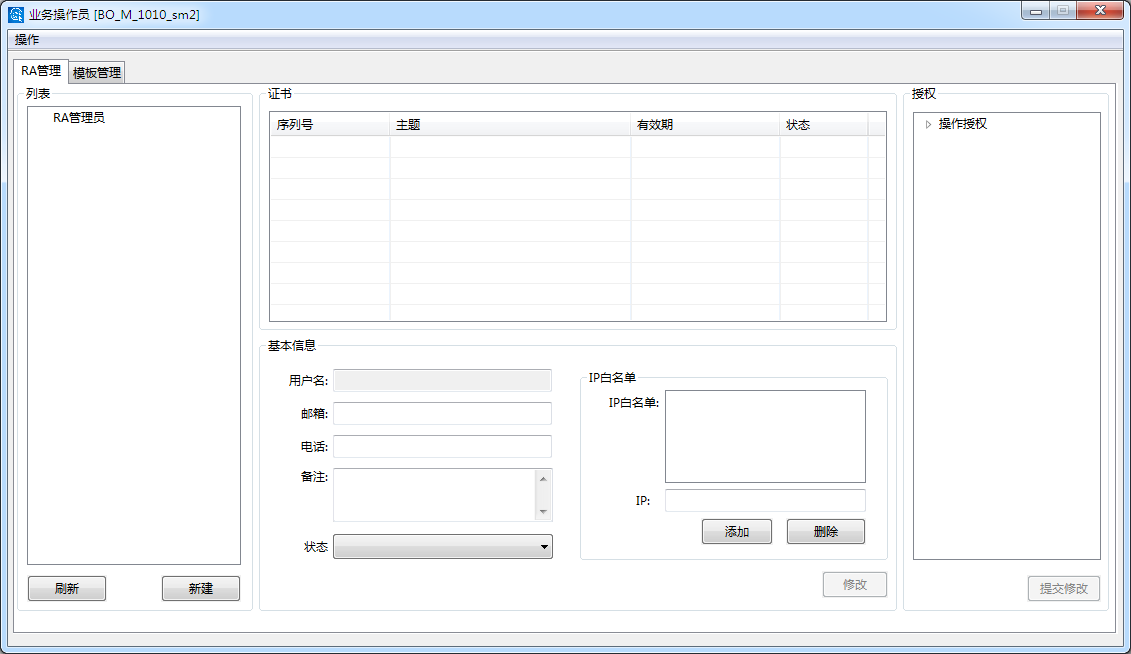
在证书列表中右键单击一个非作废的证书，在弹出菜单中选择【证书作废】，弹出作废证书对话框。如下图所示：



选择作废原因，如有必要可在【原因描述】文本框中输入简单的描述信息。点击【确定】按钮，将作废该证书。如果作废的是双证模板的证书，则两张证书将被一起作废。

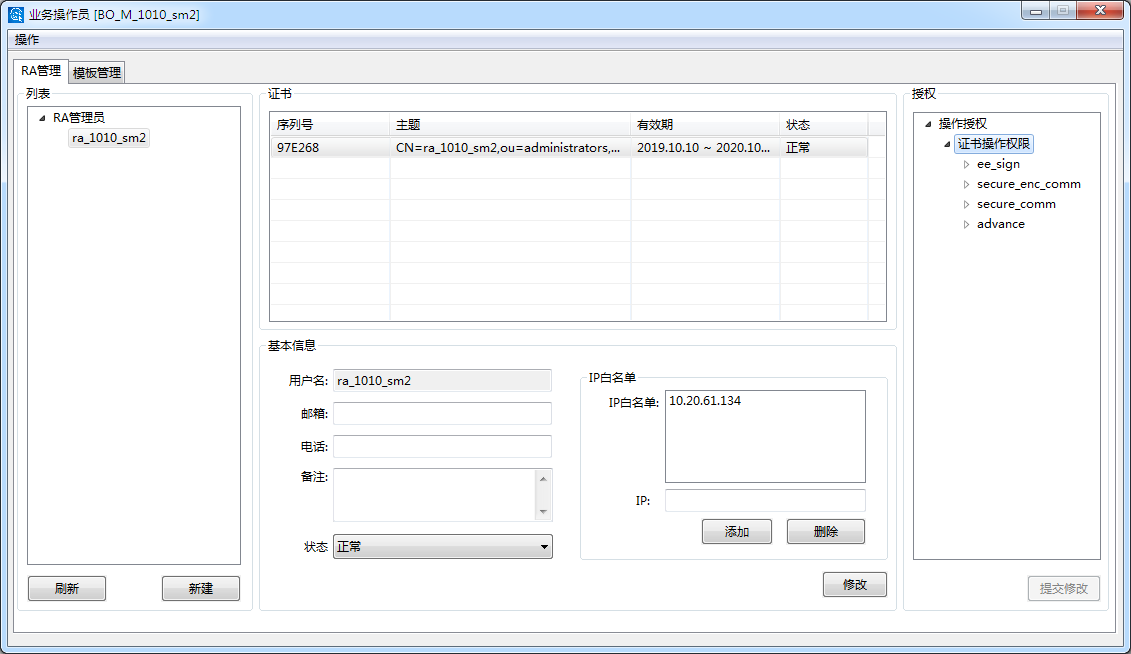
### RA管理

以具有RA管理权限的BO管理员证书登录到系统，显示视图如下：页面分为四个部分：【列表】、【证书】、【基本信息】、【授权】。其中：列表部分显示所有的RA管理员，证书部分显示选中的管理员的证书信息，基本信息显示选中的管理员的用户信息，授权部分显示选中的管理员的权限信息。（下图使用的登录管理员同时具有 RA和模板管理权限，所以同时显示RA管理和模板管理两项内容）如下图：



#### 查看RA管理员信息

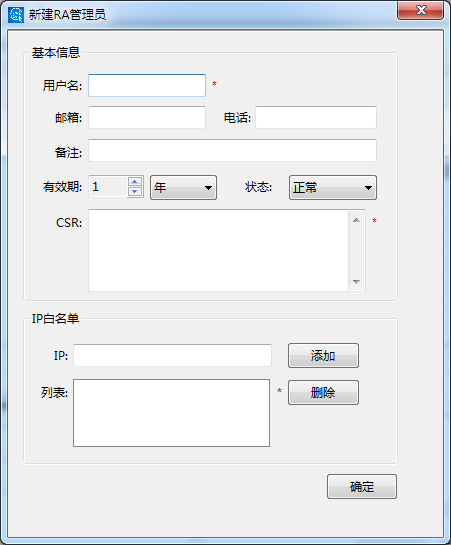
列表部分显示所有的RA管理员，如图：



当选中某一个管理员的同时，证书部分、基本信息和授权部分显示该管理员的对应信息。

#### 创建RA

点击【新建】，弹出创建对话框，填写RA信息。



**用户名：**必填，

联系人姓名：可选，

联系人电话：可选，

联系人邮箱：可选，

备注：可选，

**CSR：**证书请求（p10），必填，

**证书有效期：**必填，

**IP白名单：**必填，

状态：默认为‘正常’，可选项为正常、停用。

其中 “IP白名单”项为该RA使用者本机的ip地址，设置了白名单之后，使用在设置的IP主机上使用RA证书连接CA-Server。

#### 修改RA信息

在【基本信息】部分，可以对RA管理员进行信息修改。可修改的信息包括：邮箱、电话、备注、状态、白名单。白名单为标准的IP地址格式。

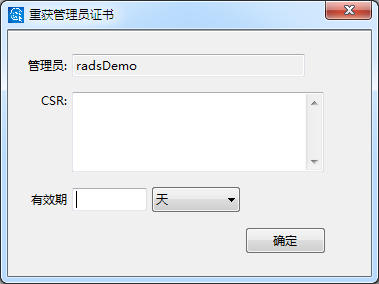
其中【状态】项为正常的时候，该RA可以正常使用，如若改为停用，则该RA不可使用。

#### 作废RA证书

选中【证书】部分显示的证书，右击选择菜单中的【作废管理员证书】，对证书状态正常的证书进行作废。

#### 重获RA证书

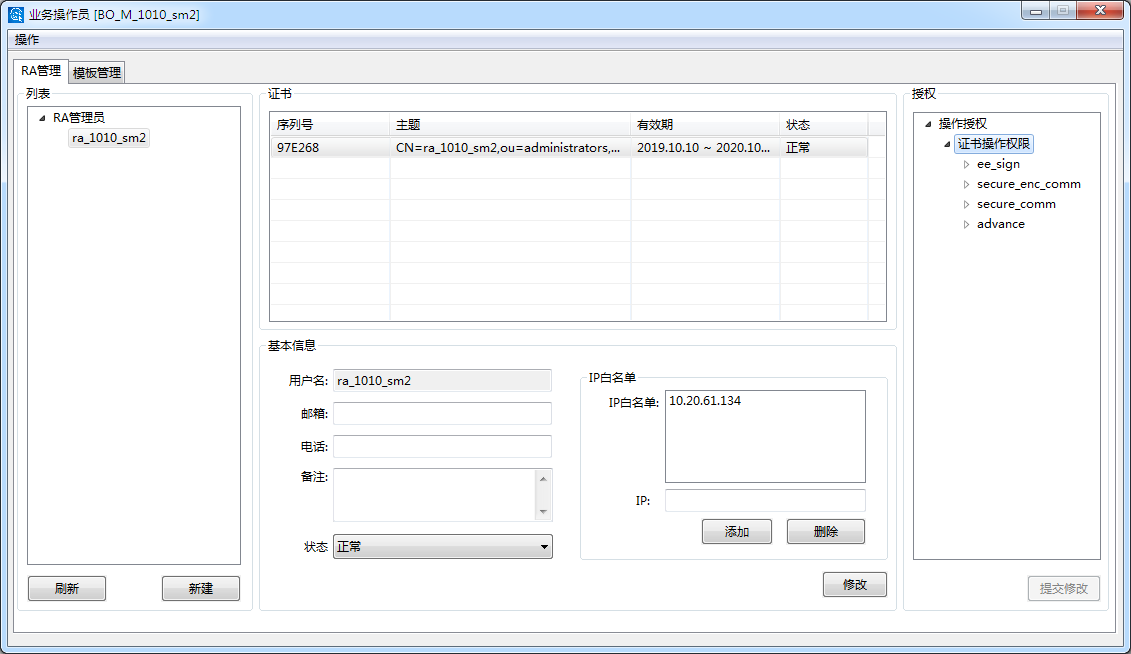
选中【证书】部分【已作废】证书，右击选择菜单中的【重获管理员证书】，弹出对话框，填写证书请求、证书有效期和选择有效期单位。重获管理员视图如下图：



点击【确定】获取证书，成功之后，会提示保存【证书】到某个目录下。

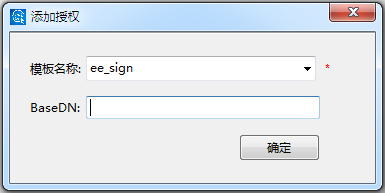
#### RA授权

对于RA管理员（证书状态为正常），可以进行授权操作，选中要授权的RA，可以在【授权】部分，根据自己的需要给RA管理员添加合适的操作权限。示意图如下：



* 模板操作权限

在【授权】区，添加模板操作权限，添加功能如下图：

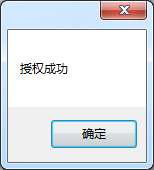


选择要授权的模板、并正确填写baseDN（baseDN填写\*代表baseDN可以是任何结构，及用户证书主题可以任意填写，均可正常签发），点击【确定】按钮进行保存即可。

添加模板权限时，默认添加的模板权限有：申请证书、重取两码、更新证书、密钥恢复、冻结证书、解冻证书、作废证书。

* 提交修改

授权信息添加完成之后，通过【提交修改】按钮提交新的授权情况。提交成功，会有授权成功提示。



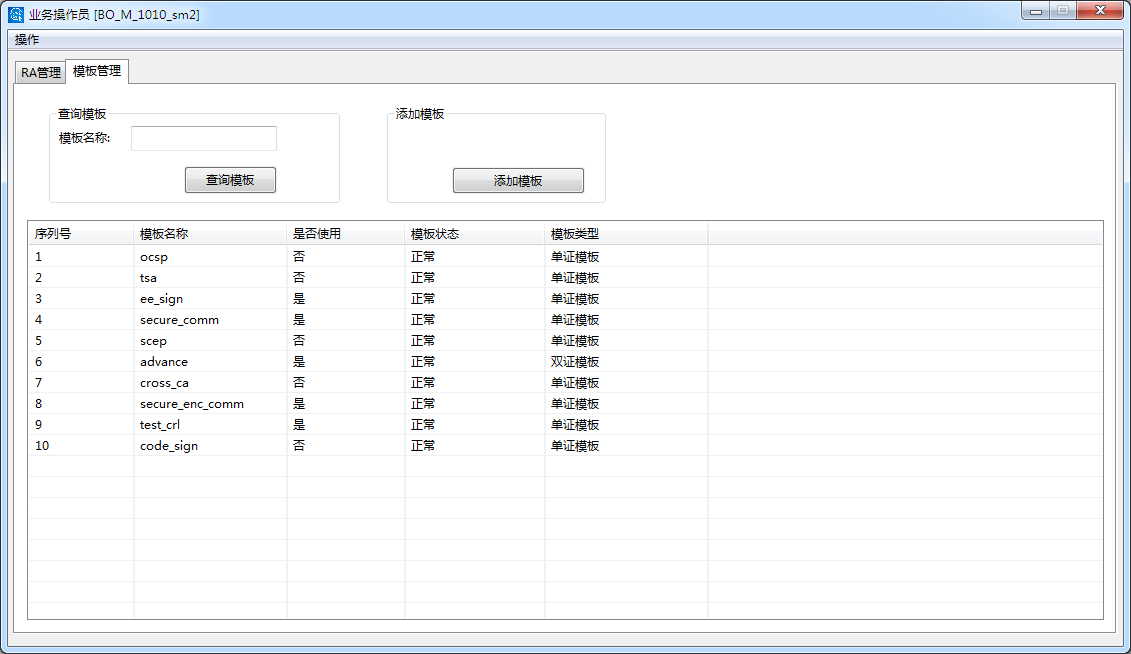
* 修改授权

修改操作授权与添加功能类似，依次修改用户操作权限和模板操作权限。

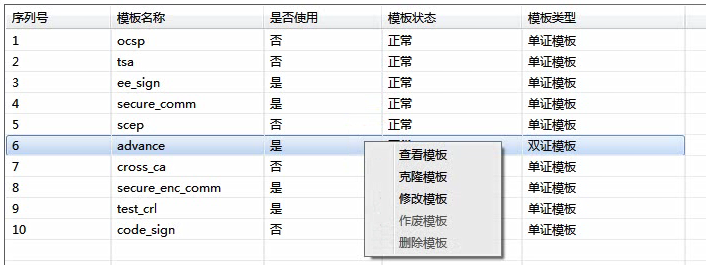
之后通过【提交修改】按钮提交即可。

### 模板管理

模板管理包括：添加模板、查看模板、克隆模板、修改模板、作废模板等。使用具有模板管理权限的BO管理员证书登录，视图如下（此时使用的管理员具有RA管理和模板管理权限，所以能同时看到两项内容）：



对于模板的操作主要有：查看模板、克隆模板、修改模板、作废模板、删除模板。

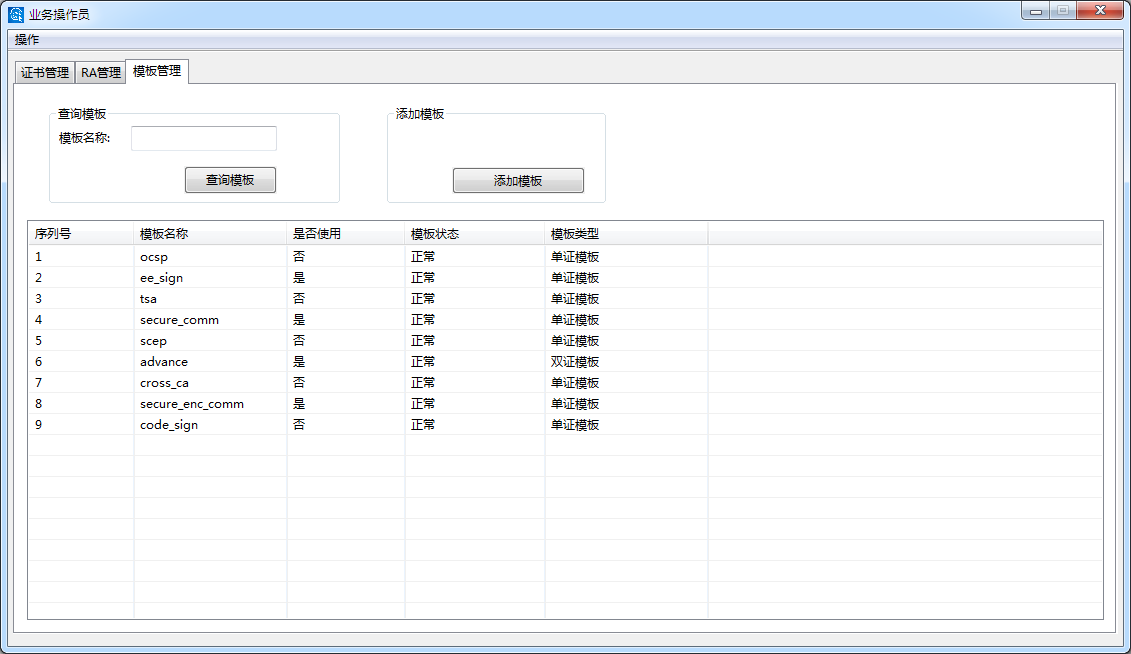


#### 查看模板列表

以BO的身份登录，点击【模板管理】进入模板列表界面，列表中显示了所有的模板信息.

列属性有：序列号、模板名称、是否被使用、模板的状态、模板类型。

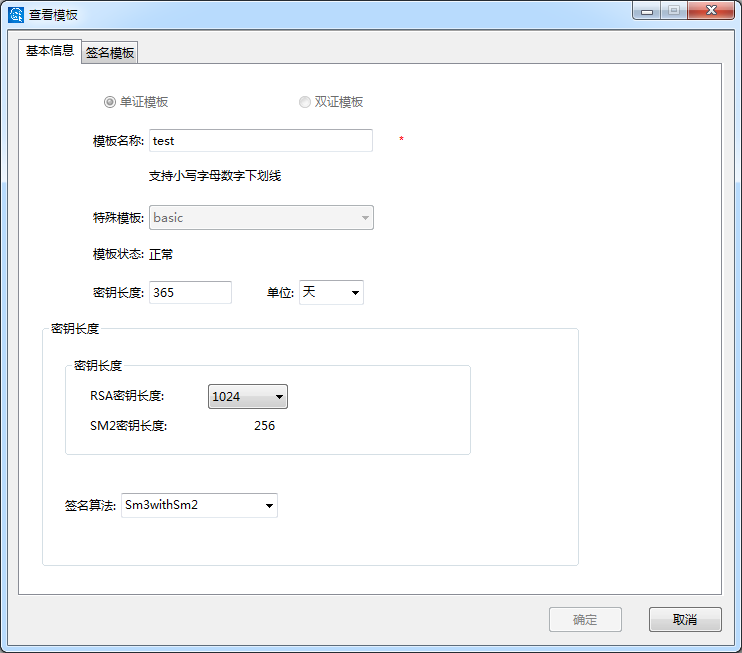
模板类型中显示为【签名模板】的是签名证书模板，【双证模板】的指签名和加密双证书模板。



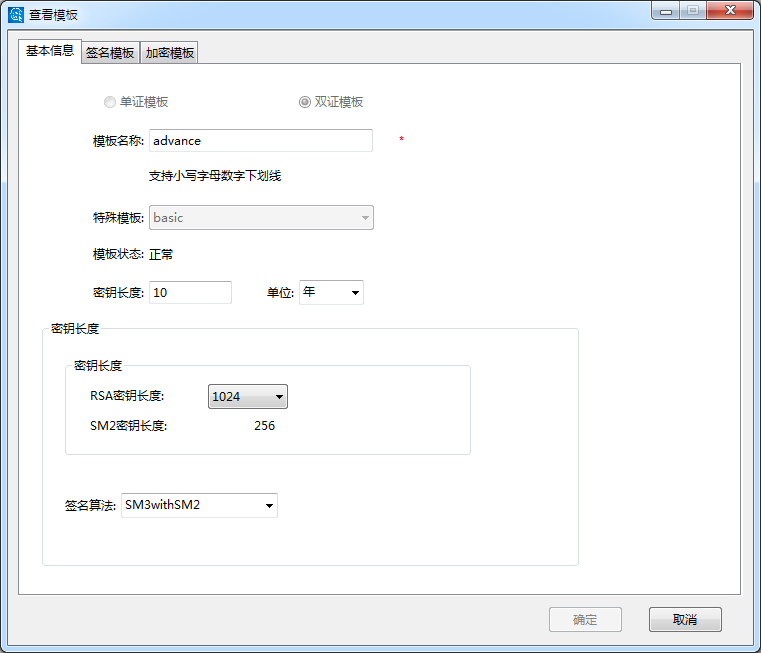
#### 查看模板详细信息

选中要查看的模板，右键选择【查看模板】可以查看该模板的详细信息。

查看单证模板，如图：

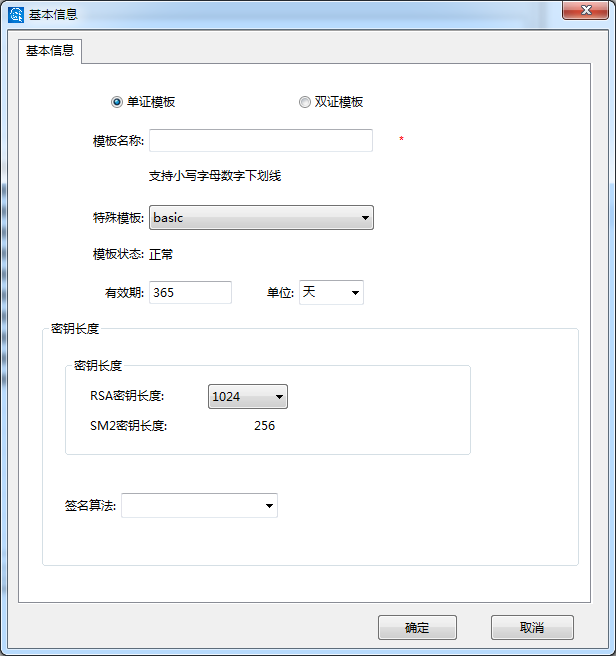


查看双证模板，如图：



#### 添加模板

右击选择【添加模板】，在弹出的添加模板对话框中，依次填写模板的属性，点击保存即可。



**模板类型：**单证模板表示签名证书模板，双证模板表示签名/加密双模板；

**模板名称:**不能重复，且系统不区分其大小写。也不能使用系统保留字作为模板名称；

**特殊模板：**设置为特殊值时，后续设置已经勾选了一些特殊的项；

**有效期：**按照需要设定，在使用该模板申请证书时，证书有效期应小于模板的有效期；

**签名算法：**与CA-Server保持一致；

**模板名称保留字：admin\_signing, ca\_id, ca, secure\_sign, secure\_enc，不能使用结尾为‘\_enc’作为模板名。**

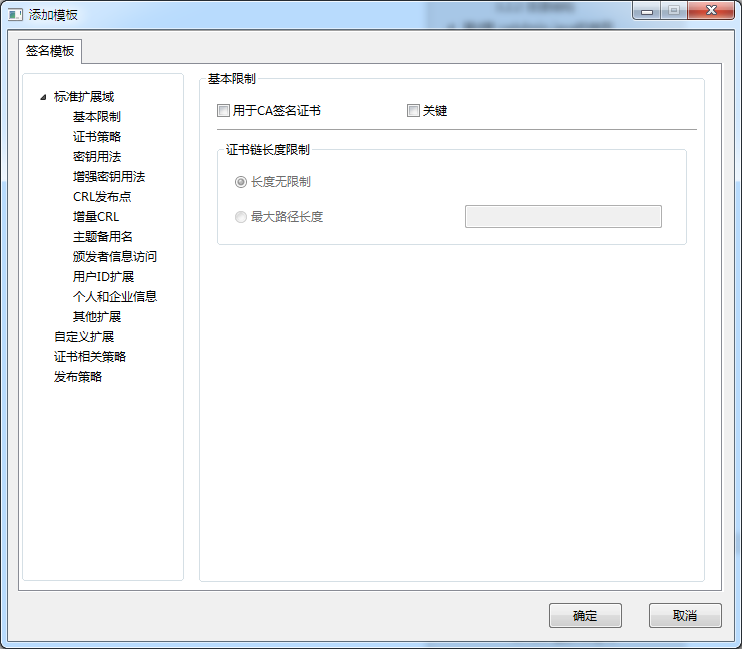
**选择添加单证模板（签名模板）还是双证模板。签名模板参考4.7.4.3.双证模板参考4.7.4.3 + 4.7.4.4.**

#### 添加签名模板

* 标准扩展域

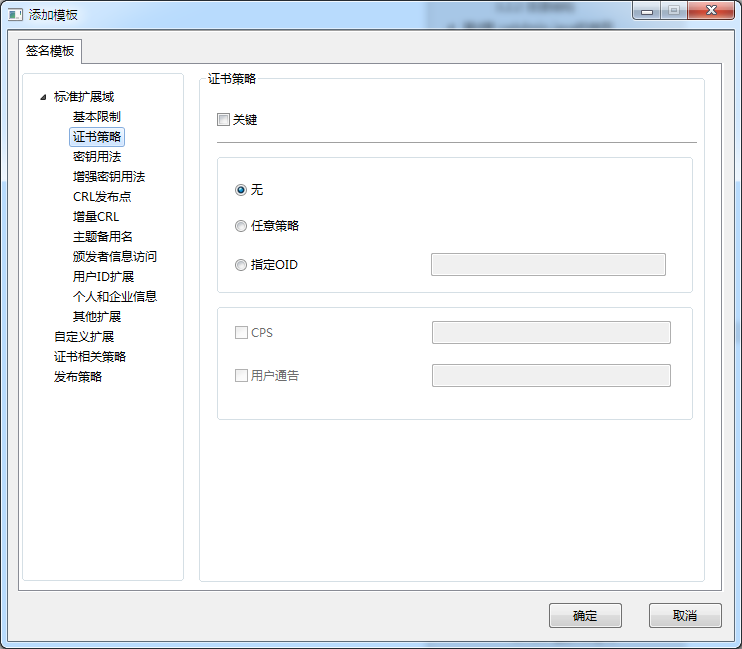
*以下列出的扩展项，未特殊说明的为RFC5280定义的扩展项，各内容的含义、应该设置什么样的内容，请查看RFC文档。*

**基本限制**

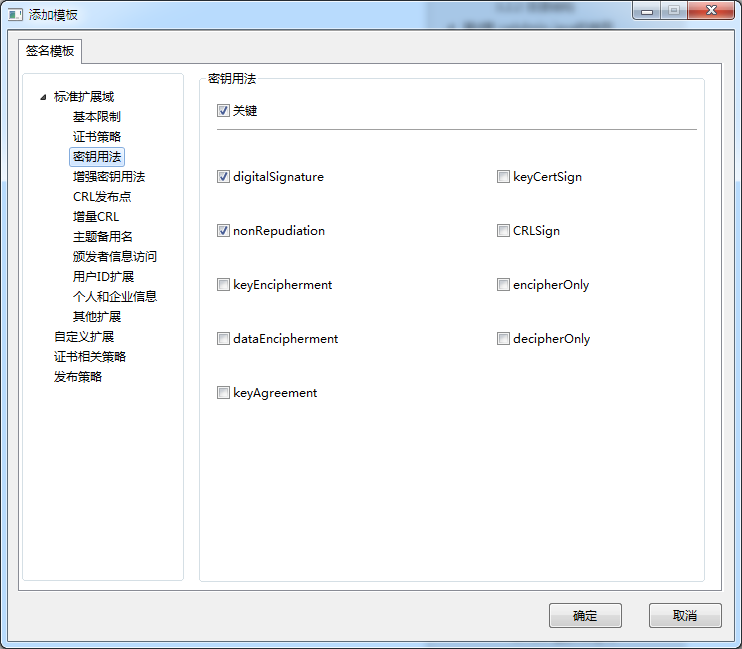


当勾选【用于CA签名证书】的复选框后，此模板将成为子CA模板。此类模板下载的证书都是证书链格式，在使用该模板注册用户之后，在下载页面使用两码下载证书时，请使用【输入p10】的方式下载，并手动勾选【返回证书链】的选项，**不要下载到USBKey里**。

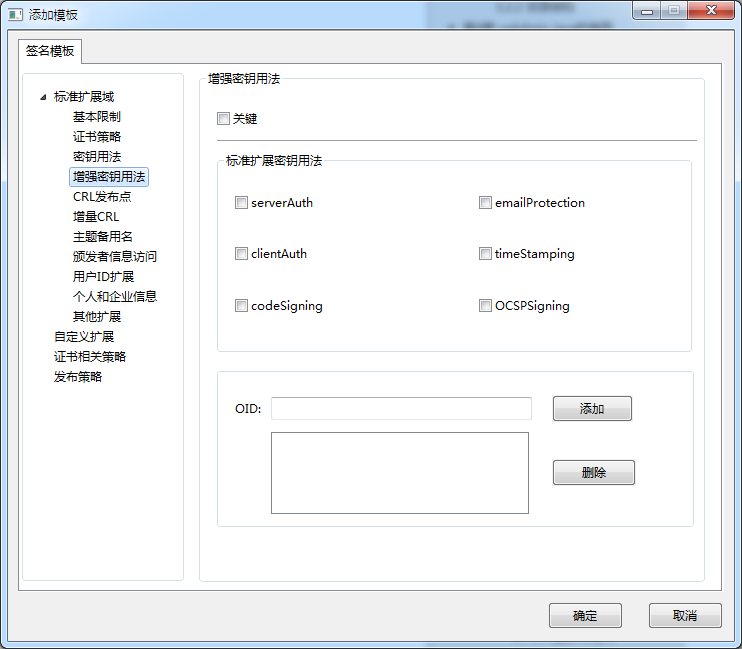
**证书策略**



**密钥用法**

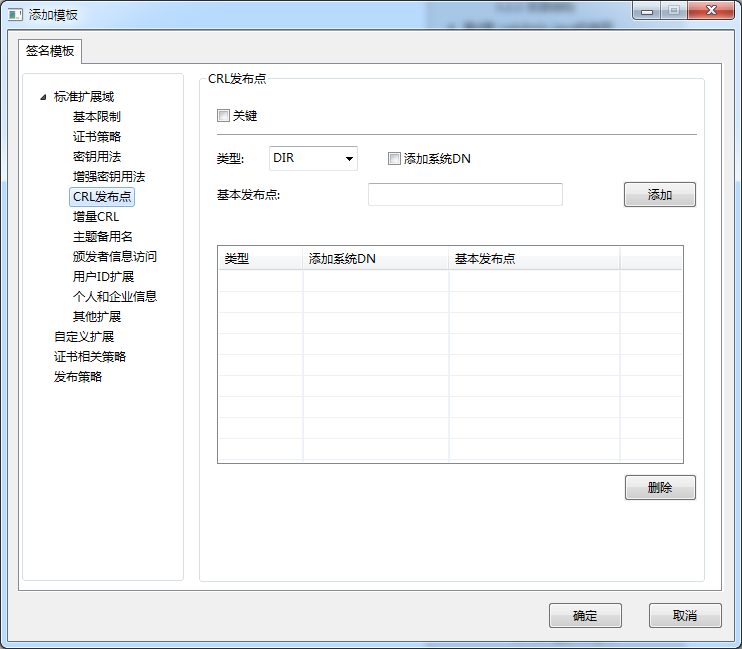


**增强密钥用法**



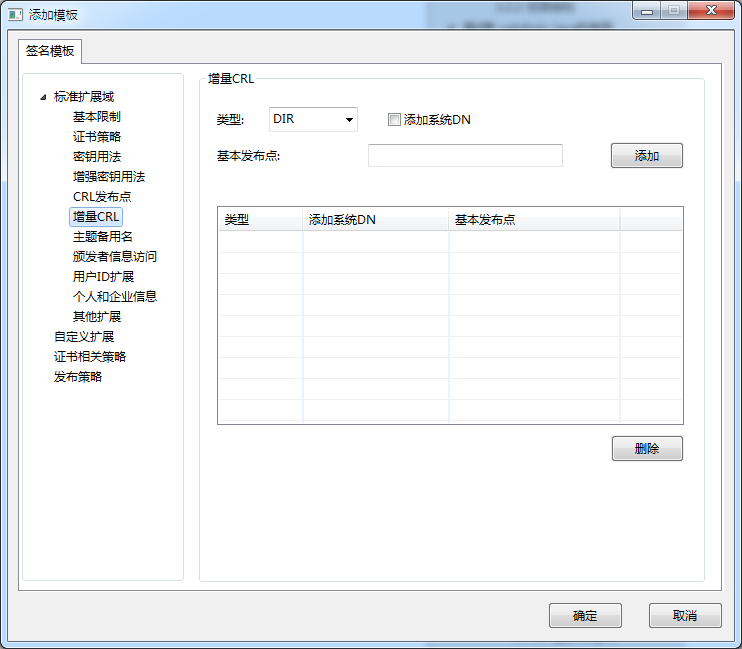
增强密钥用法可以是自定义的内容。此时在自定义部分输入。

**CRL发布点**

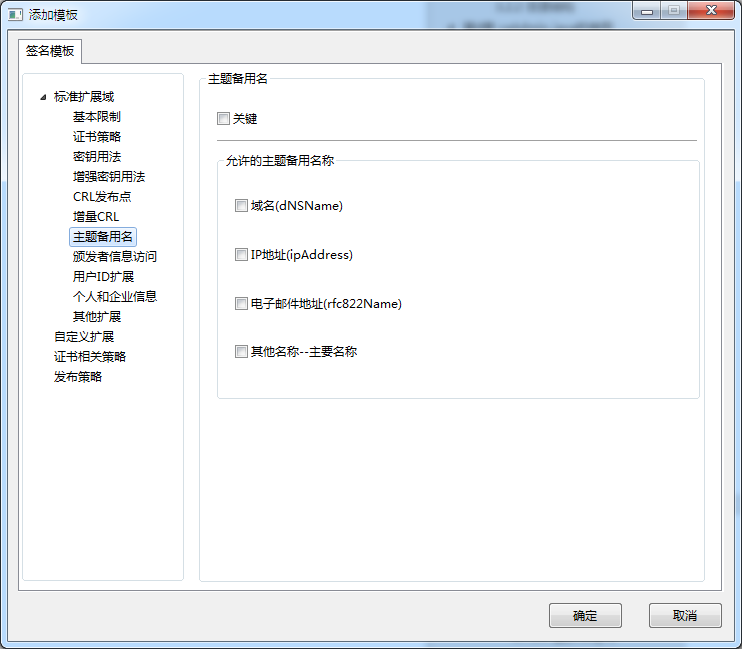


只是证书中出现的扩展内容。实际发布路径需要在web管理界面的“系统配置”菜单中设置。

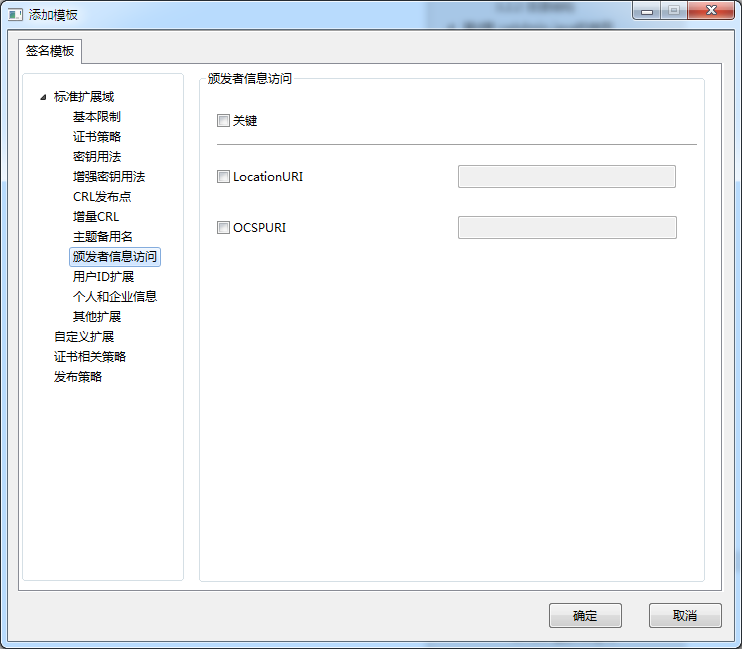
**增量CRL**



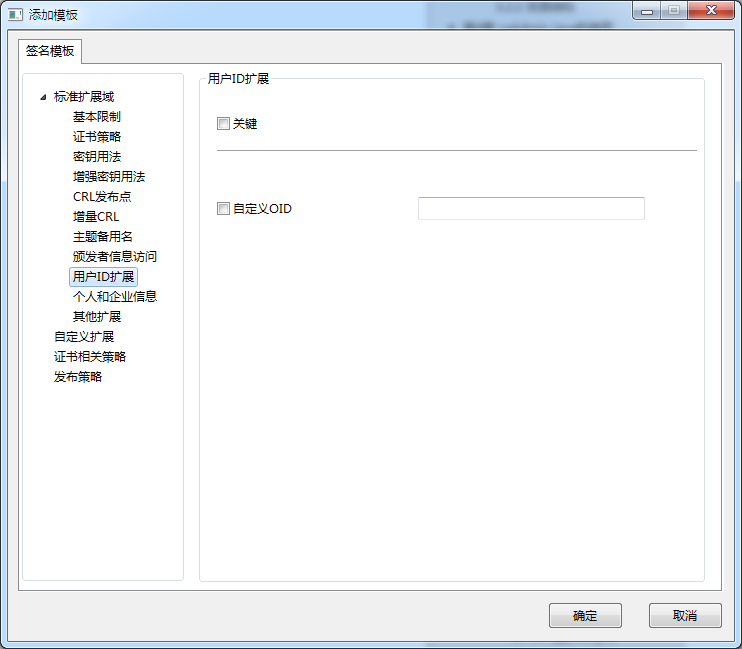
**主题备用名**



**颁发机构信息**

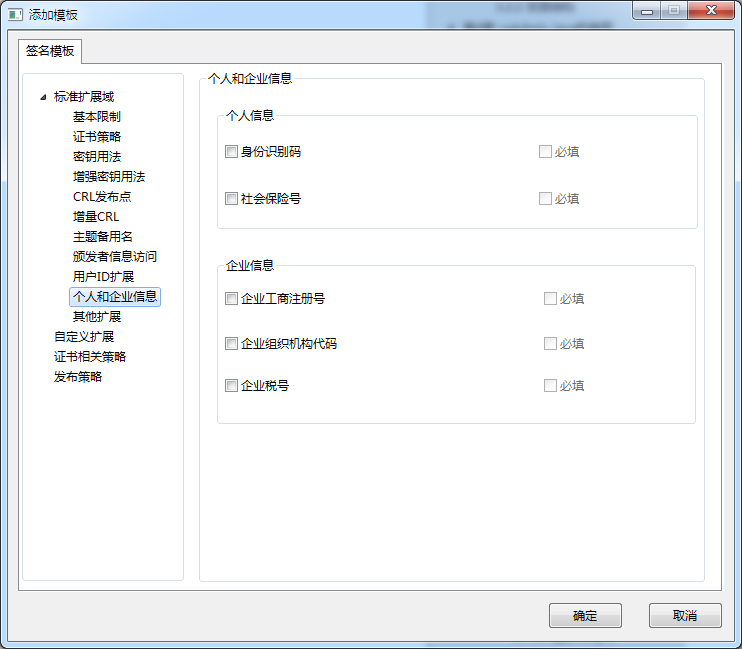


**用户ID扩展（自定义扩展）**



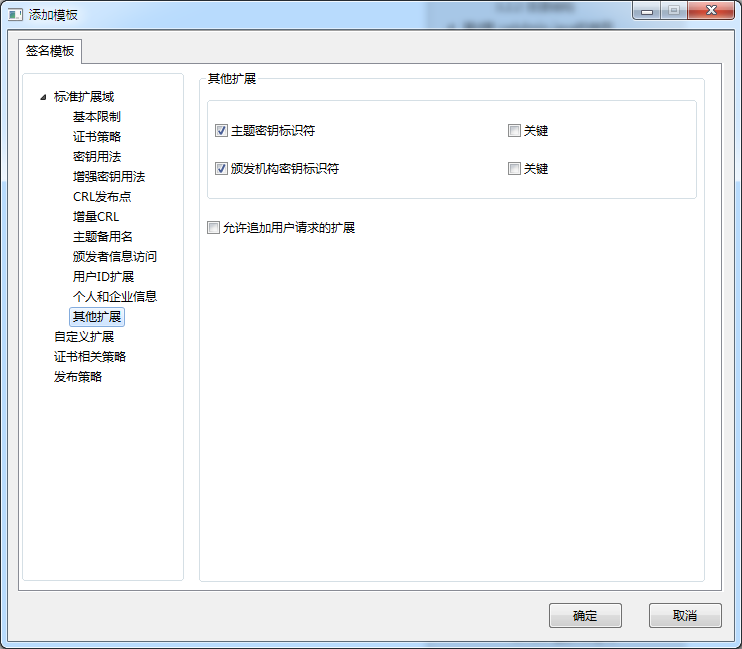
将用户uuid信息的内容作为此扩展内容，扩展的oid为此输入的自定义oid。

**个人和企业信息（国密定义的扩展）**



参见国密《0015-2012 基于SM2密码算法的数字证书格式规范》5.2.4.2.18及后续内容

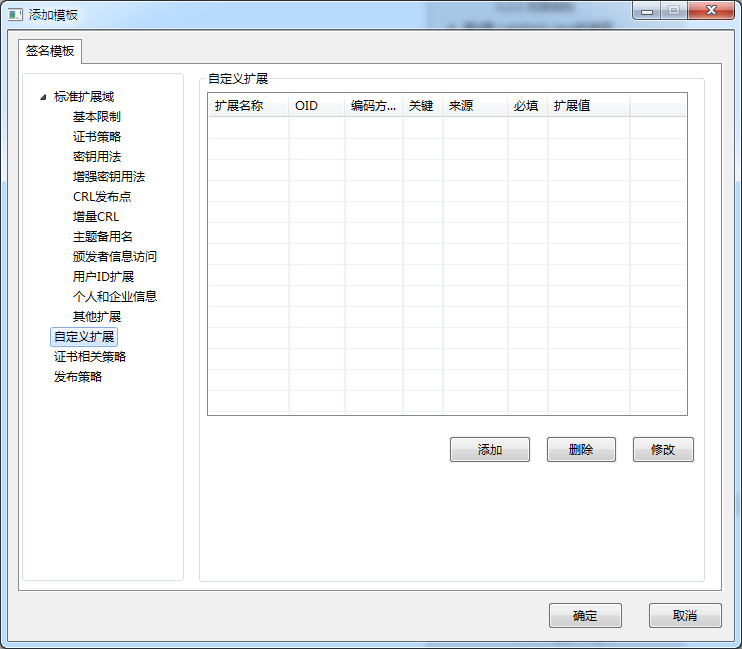
**其它扩展**



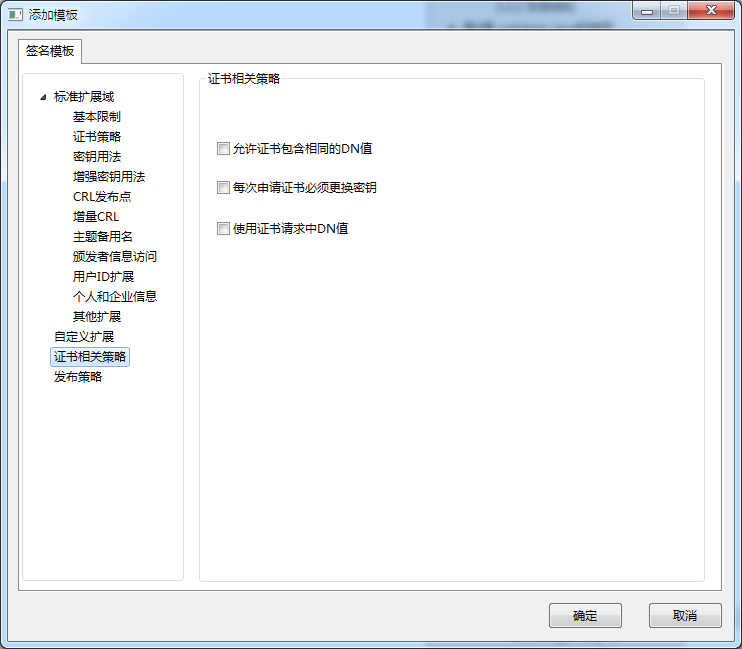
【主题密钥标识符】和【颁发机构密钥标识符】是RFC标准扩展。

如选择【允许追加用户请求的扩展】，将把p10中1.3.6.1.4.1.311.2.1.14下的扩展作为证书扩展。

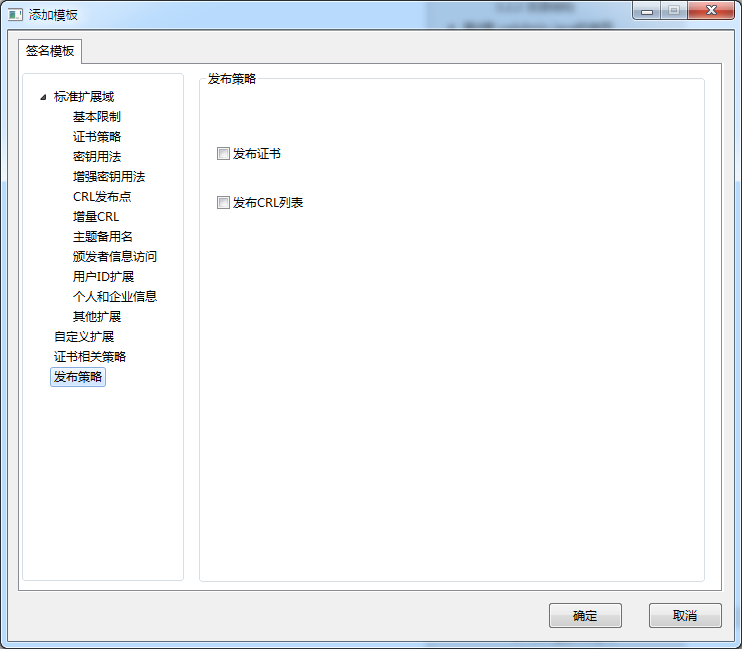
* 自定义扩展域



* 证书相关策略



* 发布策略



#### 添加加密模板

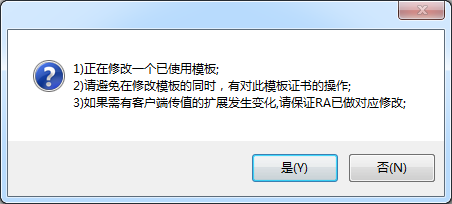
* 证书策略
* 密钥用法
* 增强密钥用法
* CRL发布点
* 增量CRL
* 主题备用名

加密模板需要设置以上六项内容，其内容与签名模板内容一致，故不再显示，如果有需要，请参考4.7.4.4。

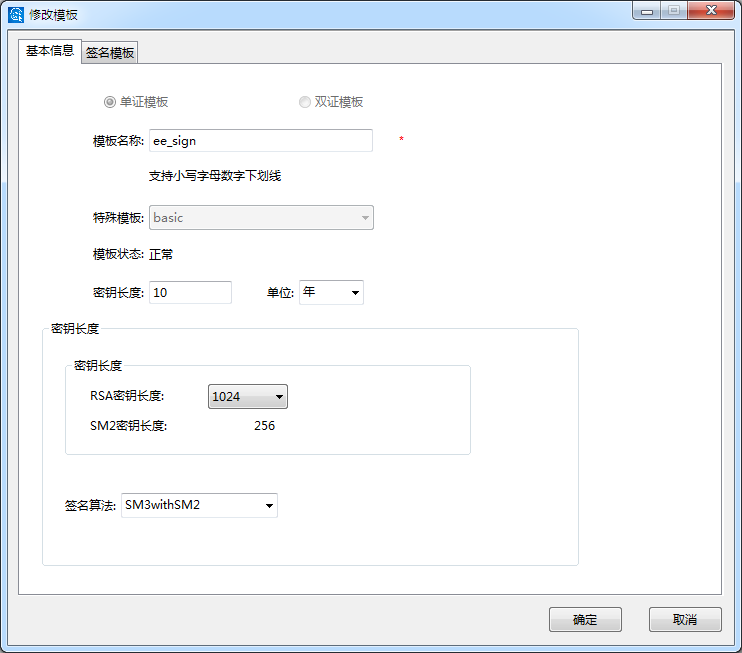
#### 修改模板

BA可以对模板进行修改，但双证模板不能改为单证，单证模板也不能改为双证，模板名也不可修改。（不建议对已使用中的模板做修改）

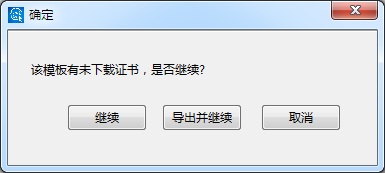
如果修改的模板状态为已使用，将提示：



点击【是】继续对模板进行修改。



根据需要对相关的信息修改，修改后点击【确定】将出现如下提示：



点击【继续】，对模板进行修改，但不保存之前待下载证书的信息；

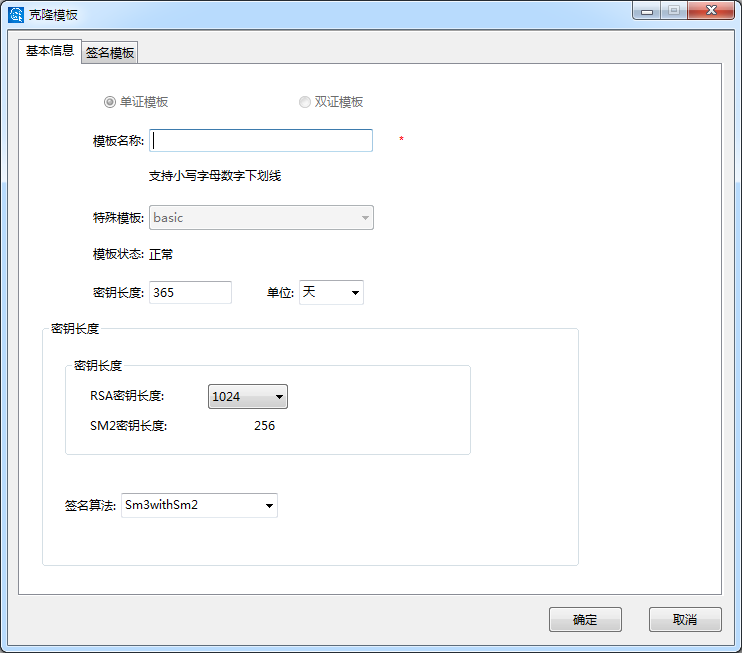
点击【导出并继续】，则先导出未下载的证书信息保存为文件再修改模板；

点击【取消】，不做修改；

**导出：**保存待下载证书的 CertDN、User ID、UserName为csv文件

#### 克隆模板

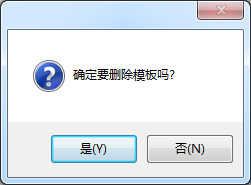
选中任意一个模板，右击选择【克隆模板】，会将选中模板的所有属性克隆到一个新的模板中来，管理员可以在这个模板的基础上设定新模板。



模板名称是必填项，且不能是已存在的模板名称，也不能是保留字。参考4.7.4.3。

#### 删除模板

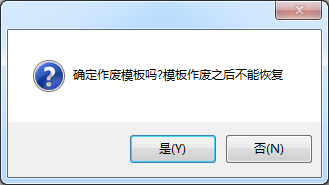
在一个模板没有被使用之前，BO可以将其删除，一旦被使用则不可以被删除。选中任意未使用模板，右击选择【删除模板】，提示如下图：



再次确认，将删除该模板。

#### 作废模板

未使用模板可以被作废，一旦被作废后，不可以恢复，不可以用来申请证书。对于已经成功申请但未下载的证书，在模板作废之后，仍然允许其下载。选中任意一个未使用模板，点击【作废模板】按钮，提示如下图：



再次确认即可作废该模板。

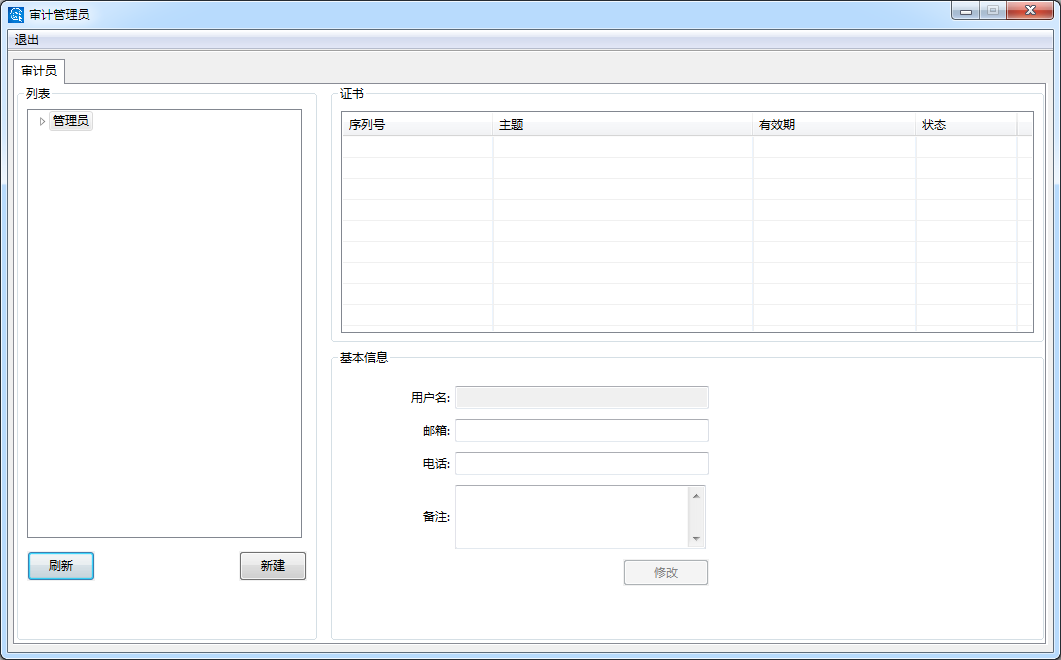
#### 特殊说明

CA-Server初始化为rsa算法时，请使用模板名为SECURE\_COMM的内置模板签发服务组件（如KMC Server）的通讯证书；

CA-Server初始化为国密算法时，请使用模板名为SECURE\_COMM，SECURE\_ENC \_COMM的模板，分别用于签发服务组件的身份证书和通讯证书。

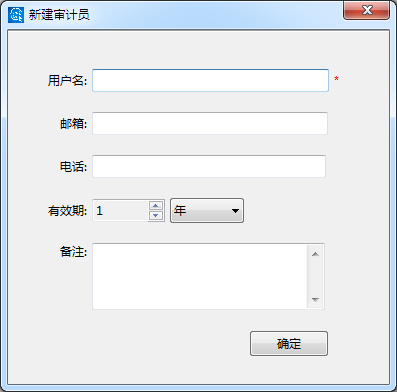
## 审计管理员功能

审计管理员主要负责审计员的管理。包括：新建审计员、查看审计员信息、修改审计员信息、作废审计员证书、重获审计员证书。



### 新建审计员

点击【新建】按钮，弹出对话框，依次填写审计员信息，其中用户名称、有效期为必填项，

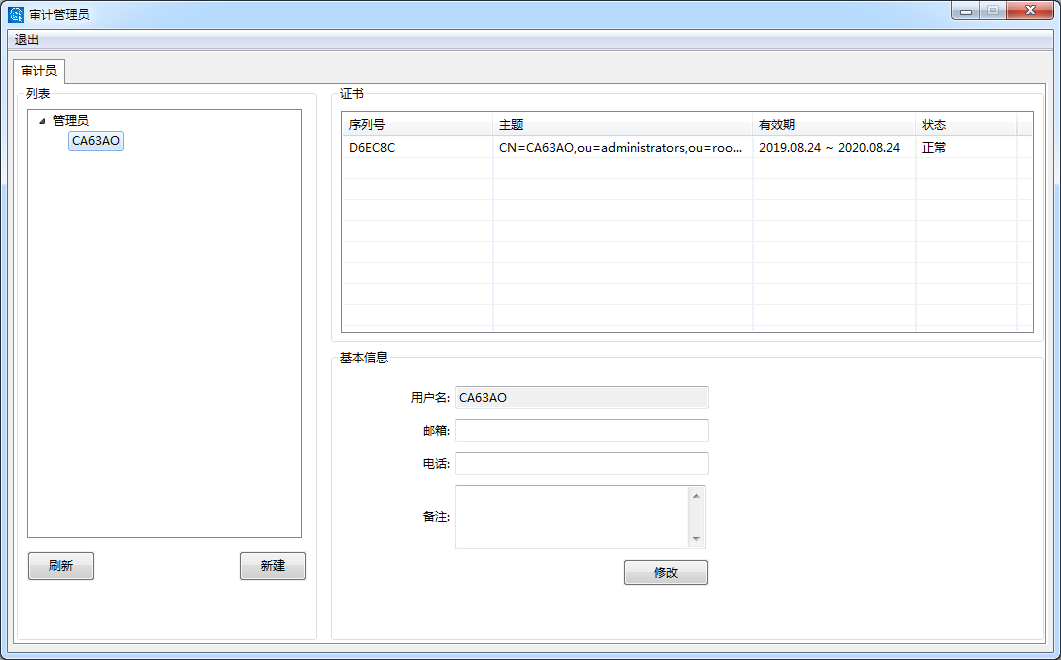


点击确定，选择路径后保存【两码文件】完成新建管理员操作。

完成新建管理员操作之后，在【登录页面】菜单栏选择【操作】/【下载管理员证书】利用该两码下载新的管理员证书到USBKey中，下载完成之后就可以使用该管理员的证书登录CA-Admin。

### 查看审计员信息

在视图左侧的列表选择某个审计员，【证书】和【基本信息】部分会显示对应的证书信息和管理员信息。如下图：

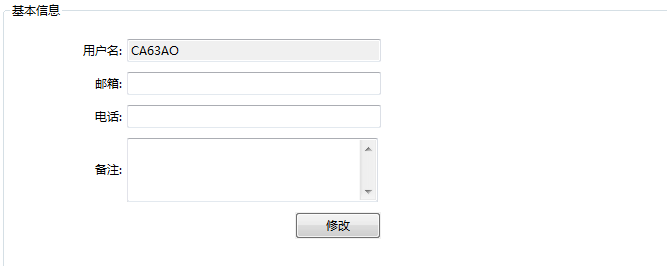


**证书信息：**序列号、主题、有效期、状态。

**基本信息：**用户名、邮箱、电话、备注。

### 修改审计员信息

选择要修改的审计员，在【基本信息】部分，可以修改邮箱、电话、备注，直接修改然后通过【修改】按钮提交，即可完成修改。



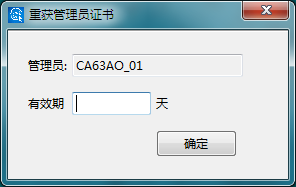
### 作废审计员证书

选中要作废的审计员，点击【作废审计员证书】按钮，经过确认操作之后，可将证书作废。

### 重获审计员证书

对于已作废的证书，可以进行重新申请证书操作。

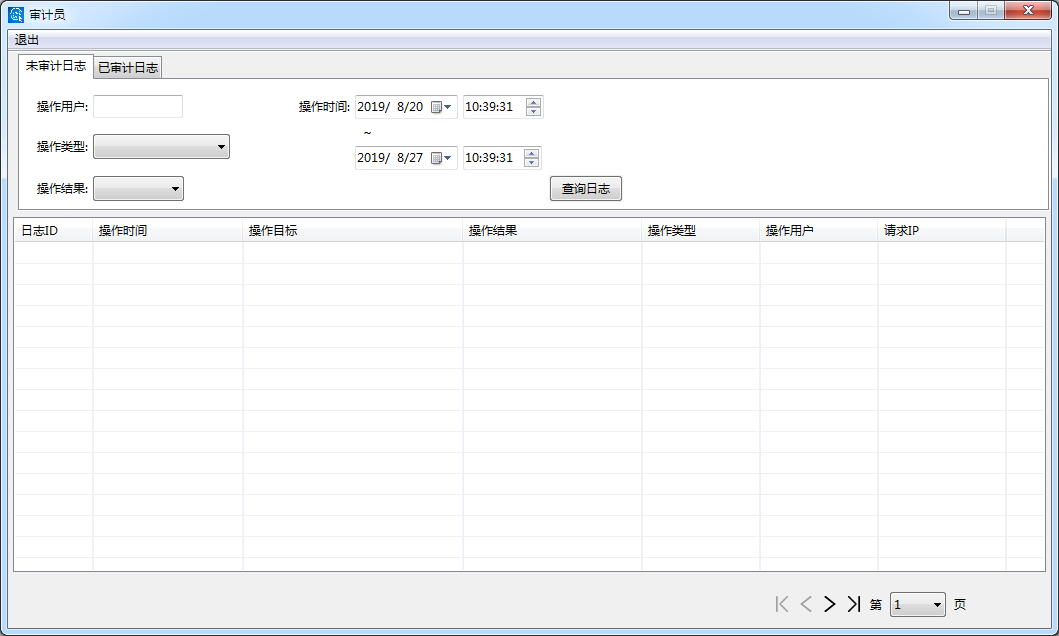
在审计员列表中，选中证书已作废的审计员，右击选择【重获管理员证书】，弹出对话框，填写申请有效期，点击确定，并保存两码用于下载证书。重获管理员证书如图：



保存文件值周，在【登录页面】菜单栏选择【操作】/【下载管理员证书】利用该两码下载新的管理员证书到USBKey中，下载完成之后就可以使用该管理员的证书登录CA-Admin。

## 审计员功能

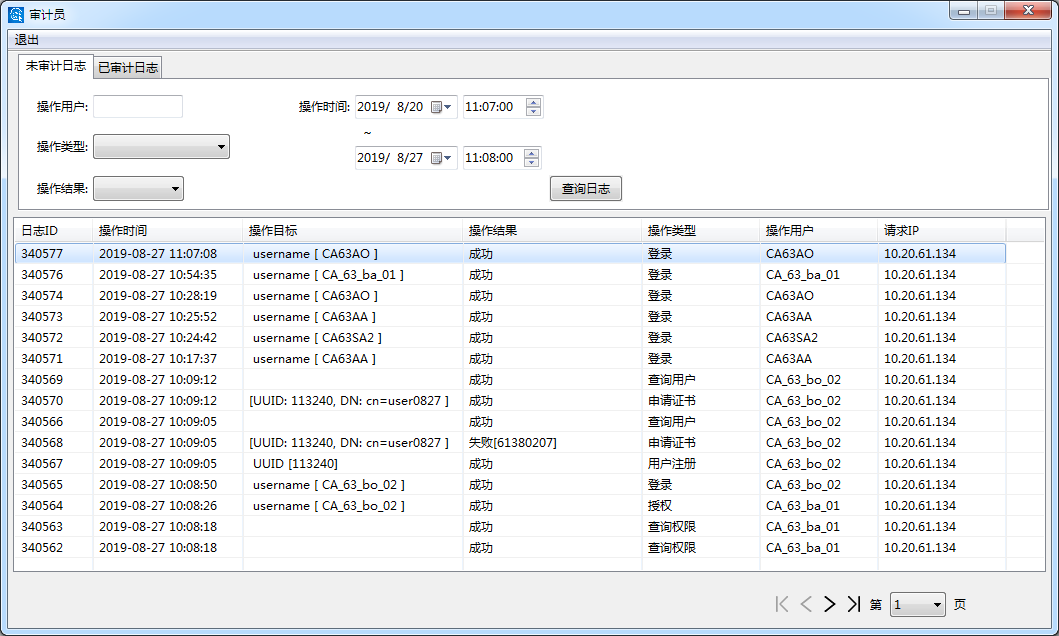
审计员负责对涉及系统安全的事件和各类管理和操作人员的行为进行审计和监督，负责查询和审计CA-Server操作记录。主要的功能有：查询待审计日志、查看日志详情、日志审计、查询已审计日志、设置日志归档任务、查询归档日志。审计员视图如下：



### 待审计日志

#### 查询待审计日志

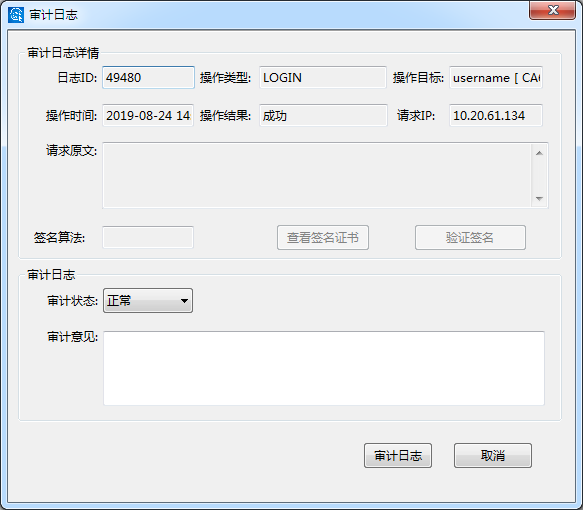
待审计查询日志必须设置查询条件（操作员、操作时间、操作类型、操作结果），即至少选择一个查询条件进行查询，也可进行多条件的组合查询，点击查询按钮后，则所有符合查询条件的日志信息将显示在日志列表中，如下图所示：



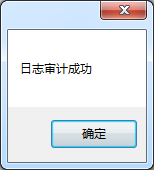
#### 查看待审计日志详情/日志审计

在查询出的日志列表中，选择任意一条记录右击选择【日志详情（审计）】，即可显示该条日志的详细信息。

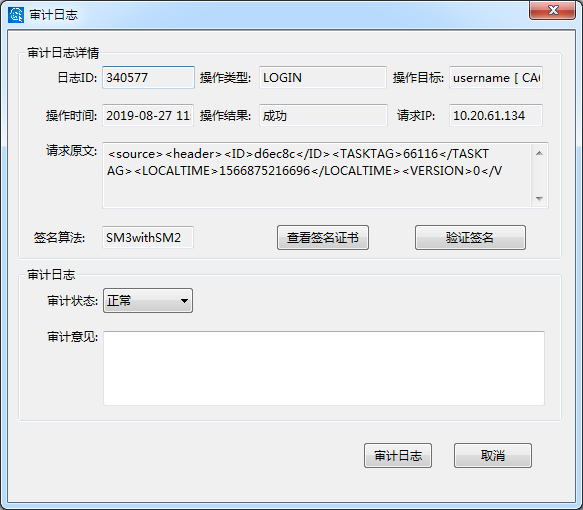
**没有开启增强日志的情况下，**示意图如图所示：



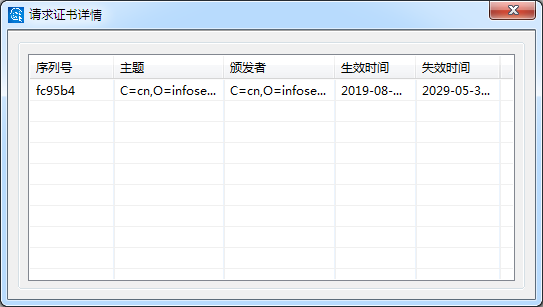
此时，可以做【审计日志】操作，选择【审计状态】，填写【审计意见】，点击【审计日志】按钮，即可审计。审计成功会有提示框。



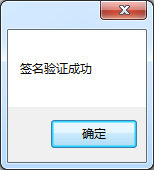
**开启增强日志的情况下，可以查看签名原文和请求证书、验证签名和审计日志。**显示如图：



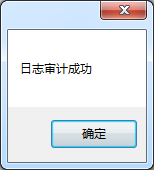
点击【查看签名证书】可以查看之前请求时的证书信息，如图：



点击【验证签名】，会使用签名原文和请求证书以及算法对签名值（签名值未显示）进行验证，验证通过有提示：



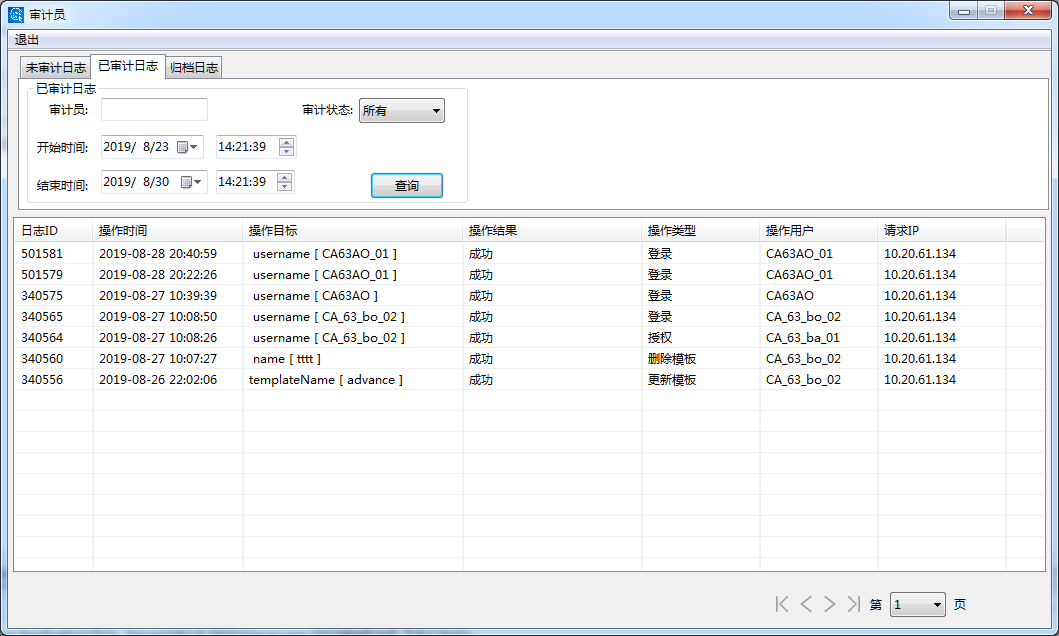
选择【审计状态】，填写【审计意见】，点击【审计日志】按钮，即可审计。审计成功会有提示框。



### 已审计日志

#### 查询已审计日志

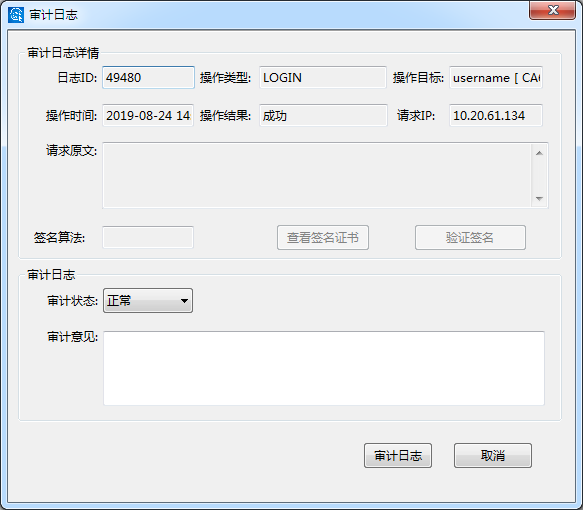
已审计日志必须设置查询条件（操作员、操作时间、操作类型、操作结果、审计员、审计时间、审计状态），即至少选择一个查询条件进行查询，也可进行多条件的组合查询，点击查询按钮后，则所有符合查询条件的日志信息将显示在日志列表中，如下图所示：



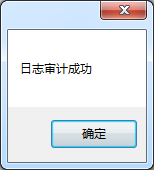
#### 查看审计日志详情/日志审计

在查询出的日志列表中，选择任意一条记录右击选择【日志详情（审计）】，即可显示该条日志的详细信息。

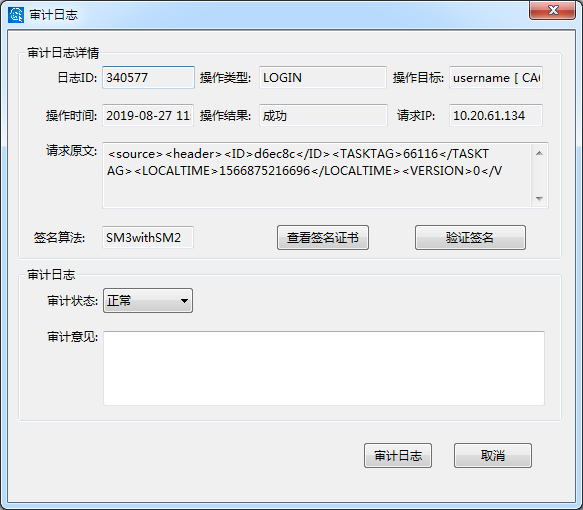
**没有开启增强日志的情况下，**示意图如图所示：



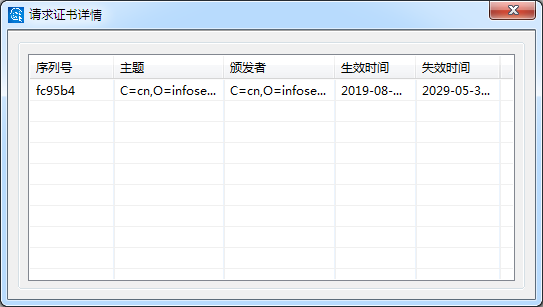
此时，可以做【审计日志】操作，选择【审计状态】，填写【审计意见】，点击【审计日志】按钮，即可审计。审计成功会有提示框。



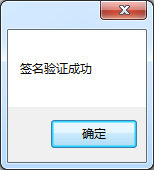
**开启增强日志的情况下，可以查看签名原文和请求证书、验证签名和审计日志。**显示如图：



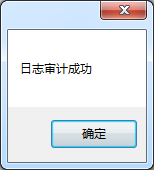
点击【查看签名证书】可以查看之前请求时的证书信息，如图：



点击【验证签名】，会使用签名原文和请求证书以及算法对签名值（签名值未显示）进行验证，验证通过有提示：

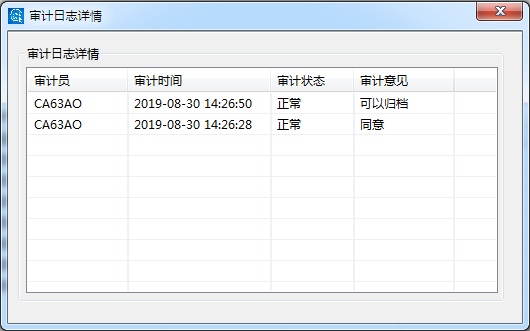


选择【审计状态】，填写【审计意见】，点击【审计日志】按钮，即可审计。审计成功会有提示框。



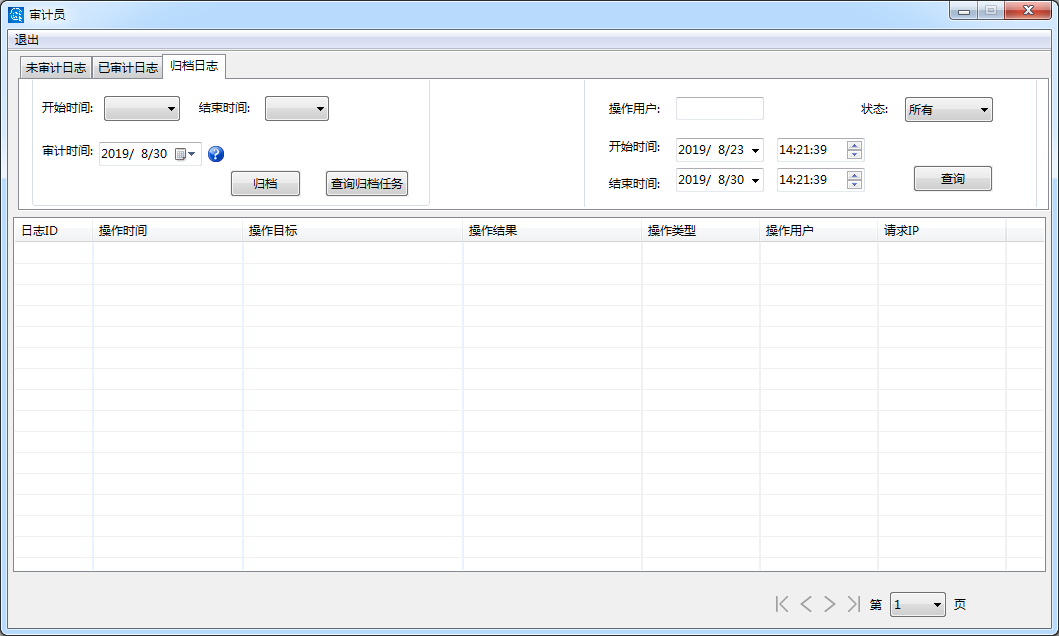
#### 查看日志审计详情

右击选择【审计详情】可查看该条日志的审计详情，如图所示：



### 日志归档

使用AO管理员登录系统，选择【归档日志】视图，显示如图：



#### 设置归档任务

对于已审计的日志，审计员可以对其进行【归档】操作，切换视图到【归档】，通过设置开始时间、结束时间、审计时间，然后点击【归档】即可设置归档任务。



**开始时间：**24小时制；

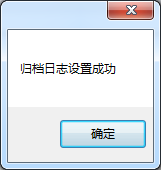
**结束时间：**24小时制；

**审计时间：**日期格式；

**归档任务的功能：**在每天的开始时间和结束时间之间，对设置的审计时间之前的已审计日志进行归档操作。

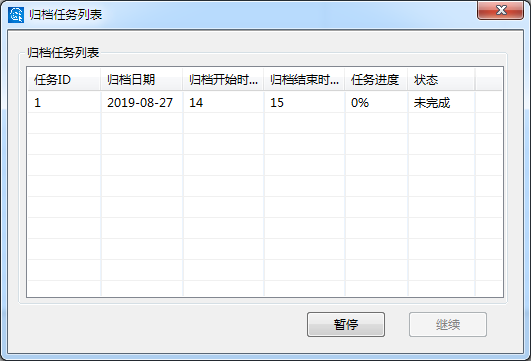
例如：开始时间为：14，结束时间为15，审计时间为：2019-08-27，设置归档任务。表示每天的14点到15点执行归档操作，对2019-08-27之前的所有已审计日志进行归档操作。

设置归档任务成功有提示信息如图所示：



#### 归档任务查看

系统只允许一个归档任务在进行，如已有归档任务在运行，可以通过点击右侧日志查询菜单项中归档任务查看按钮来进行查看和操作，如图所示：

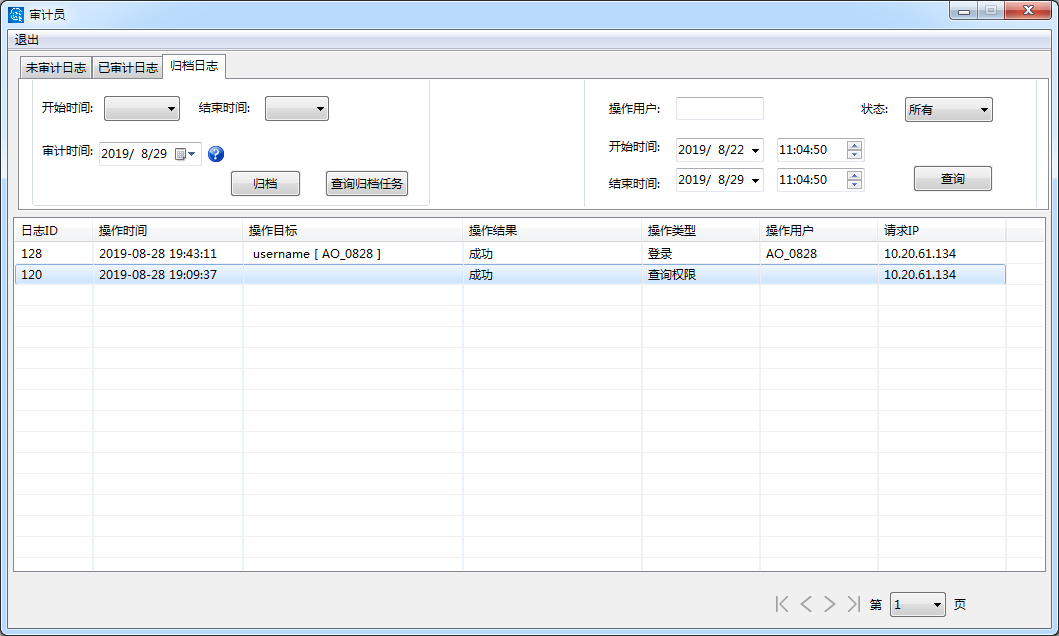


在该对话框中，可以查看归档任务在后台运行的状态，同时可以对该任务进行暂停与继续操作。

如果归档任务执行完成，就不能再查看归档任务了，【查看归档任务】只允许查看最新的未完成归档任务。

### 归档日志

该功能主要是对已归档的日志进行查询，查询日志必须设置查询条件（操作员、操作时间、状态），即至少选择一个查询条件进行查询，也可进行多条件的组合查询，点击查询按钮后，则所有符合查询条件的日志信息将显示在日志列表中，如下图所示：



## CA-Admin异常排查

1. 程序在运行过程中出现任何问题，请首先查询错误日志，错误日志文件在安装目录的log文件夹下。
2. 首先排查CA-Server、KMC-Server（涉及双证相关操作）是否运行正常。
3. 登录CA-Admin 失败：逐项确认【配置】中的IP地址、端口号、SSL是否勾选、CA根证书是否配置正确。
4. 登录CA-Admin 等待时间长，无反应，适当调节超时时间，调大等待服务器端响应，在SSL通信时，需要长一点的超时时间。

附录B：ＣＡ管理体系图

