CA-Admin\_6.3 ***开发过程中遇到的问题：***

**2019-08-30** 自测完成，准备提交测试，禅道系统不太熟悉，推迟到 2019-09-02

**2019-08-30** 在本地代码修改了发现以下问题，并尝试修改：

2019-09-09

1. 提交给 测试 新的 jar 已完成
2. 产生 CA的证书请求，该怎么解释。 沟通完成，补充到 使用手册上
3. 下载RA证书，默认文件名为 用户名 已修改

1. 授权视图： 模板操作权限 修改为 证书操作权限（涉及BA、BO） 已修改

2. 不能进行 异常 状态的审计操作 已修改

1. 归档时间有问题， 使用手册说明

2019-09-11 （16）

1. 修改CA证书 复核异常 搞定
2. 检查 text 的长度 每个text 都有限制
3. 窗口显示 当前管理员用户名 登录使用的是证书，折中显示 cn 内容
4. KMC配置 CA 根证书 是不是不合理 等沟通
5. 历史库密钥统计 检查 内部名称为空 添加限制
6. 产生密钥 刷新 按钮 会判断 是否有 ca名称
7. 同一张证书 不同名 用户 替换 戴总给的 邮件两个文件 测试没问题
8. Ca内部名称和唯一标识 统一为 内部名称
9. BO 新增了 查看权限的操作 完成
10. 检查所有的 保存文件 默认名称， 完成
11. 复查之前修改过的 bug 完成

2019-09-17

1. 了解了 备用库密钥的使用规则 完成
2. 修复了之前测试提出的 bug 完成
3. 重点检查了 release key 的设计 和 超时时间的检查 完成

2019-09-18

1. 从 svn 拿 戴总的最新代码， 完成
2. 搭一套 RSA 的环境， 完成
3. 重现测试的 bug，并尝试解决 完成
4. 开始修改手册，争取完成一半
5. 增强日志下 验证操作签名值， 下载管理员证书 没有 reqCert 沟通
6. 增强日志下 验证签名失败 ， 完成

2019-09-23

1. 重构 BA视图 ，权限管理 添加 了 RA 管理 和 模板管理。 Ok

BO管理员分为两个角色 权限管理角色 和 证书管理角色。

权限管理角色 ： 通过 BA 对管理员授权 模板 或者 RA 来确定

证书管理角色： 通过 BA 对管理员授权 证书操作权限来确定

两者 不能同时授权给一个管理员。

1. CA更新 密钥之后，

CA系统设置的 KMC 信任证书仍然是 旧的根证书，验证 kmc 的身份证书

KMC\_Admin 设置的证书需要是新的根证书，与CA通信

使用脚本 启动程序，验证测试提出的所有bug

1. 禅道中的 bug 整理：
2. 创建/修改 管理员 时，电话、Email、备注检查。涉及长度和格式

BA(已验证) BO (已验证) AO (已验证) RA(已验证)

1. SA 作废/重获 BA证书，功能缺失。 已验证
2. 增强日志 审计，验证签名失败。 已验证
3. 下载RSA2048证书失败。 慢
4. SM2 使用正确的双证两码下载单证证书，提示失败，之后选择下载双证证书，仍然提示失败。 验证
5. 使用P10下载证书，勾选返回证书链，返回的结果 不是 p7b、 验证
6. 待下载的用户证书不能重新获取两码：功能缺失 验证
7. 添加 BO ，列表不能实时更新 信息 已验证
8. CA\_Admin 出现崩溃情况， openjdk错误 不能关闭窗口 使用中断开

模板 模块：

1. Cross\_ca模板 基本限制 》》证书链长度默认无值，应该勾选 无。 验证
2. 证书模板扩展项，可以添加非支持的格式信息，DIR 没有格式限制，
3. Scep 显示的特殊模板 名称 不符 ，应该是 scep 验证
4. 添加模板时，应该 给出默认允许的 签名算法值 验证
5. 添加同名 模板，会覆盖掉之前的模板 验证

KMC ——BUG：

证书重复添加或者修改: 已验证

1. 更新CA 根证书失败 RSA验证 SM2 验证
2. 历史密钥查询失败， RSA验证 SM2验证
3. 司法密钥恢复 RSA 测试成功 SM2验证
4. 修改管理员证书为 被使用的证书 RSA验证 SM2验证
5. **修改上传的证书为非连接CA签发的证书，使用 非CA签发的证书绑定到管理员 验证**
6. 添加 和 修改 为 已使用的证书重复（审计员） 验证
7. 查询历史密钥库失败，查询历史密钥失败， 权限异常 验证
8. 预产生密钥数量显示异常 验证
9. 使用非CA签发的证书登录KMC ，卡死 验证

2019-10-10 沟通

1. RSA 下中文乱码的问题
2. BO 角色的分级
3. RSA写入 加密证书失败，之后没有 catch 到异常。 例如 往 IE 写2048
4. 登录和下载证书比较慢，而且有时候有 超时，是不是通信的问题 搞定了

2019-10-11

1. 完善使用手册，
2. RSA 写入IE 2048证书失败， 试试 其他的csp ，

Base 不能写，报错信息： importEncX509Cert|4:CryptImportKey,80090005

Strong Enhanced 都可以写 RSA 2048的证书。

2019-10-12

1. 记载 gif 图片问题，
2. 测试 BO 查询证书问题，
3. 整理 手册，

2019-10-14

1. 检查 bug
2. 提交测试

2019-12-21

1. Admin的中英文显示问题：
2. 先补充配置文件， （上午） 搞定第一步，然后对之前的比较长的做处理
3. 逐个页面调整，尽可能的调整配置文件英文的长度 （下午）
4. 考虑下 实现什么布局方式：
5. 测试各种布局方式，做一个新的项目做测试（下午）
6. 使用布局方式显示页面测试，目的：在测试提出问题时，可以第一时间修改。
7. SWT/Jface， 跟同事沟通交流，看看他想听什么 （周一下午）
8. SWT/Jface 的 PPT： （周一----周四）、
9. 前言： 受众以及我的讲述重点。（周一）

本PPT 的内容是介绍一个大家普遍用的比较少的Java技术，少体现在课程教学上，体现在网络资料上，也体现在市场和产品上。很多有用Java来开发应用程序。主要是显示不美观，更主要的是 没有硬性需求，网易云音乐用的是JavaScript、更多的应用用，C、C++、VB 等。

1. 对这个技术的介绍，以及与相关技术的对比说明。（周一）

AWT---->Swing--->SWT/Jface ----> JavaFX

Swing 是Java语言的第一代桌面组件工具，

SWT/Jface 是Java语言的第二代桌面组件工具，著名的开源IDE-[eclipse](https://baike.baidu.com/item/eclipse/61703)就是用SWT开发的。

JavaFX 是Java语言的第三代桌面开发组件工具，带有Java的css效果。

一些技术性的书籍都会单独 有一章讲解Java的桌面开发组件，有可能是Swing，也有可能是SWT/Jface ，但还很少有人讲JavaFX，Java在08年发布版本的时候，发布了JavaFX的正式版。后续开始有一些人使用，但是现在相关资料还是很少，个人感觉在使用率上SWT/Jface >swing>JavaFX，但至今只见过eclipse。 应该还是因为没有很多的业务场景必须用到Java。而我们这次使用Java的SWT/Jface开发Admin 客户端程序，也是因为国产系统的推广，需要我们的客户端产品同时兼容windows 和 中标麒麟系统（中标麒麟系统是基于centos定制的国产系统）。

（CA组产品，CA\_Server是一个S端产品，也就是服务器端产品，CA\_Admin是一个C端产品，也就是桌面应用，应用程序，所以我们的产品是 C/S结构） 而RA是通过浏览器访问CA\_Server的，RA是一个B端产品，RA和CA\_Server的结构就是B/S结构。

这个技术的前景有没有，还不好说，如果国产系统推广比较成功，有某些产品可能会考虑下Java开发，只要Java不要放弃这条线，未来还是有可能的。而Java在18年发布了JavaFX 13的版本。

1. 对一个Demo 的简单项目框架做介绍，侧重对测试人员。（周一）
2. 对eclipse 环境下做开发的使用情况做介绍，入门。（重点） （周一）
3. 安装插件
4. 结合eclipse的Design 视图，实现拖拽式开发
5. 结合pdf 和 API 了解一些组件就可以了
6. 难度：布局、资料少
7. 优点：Java语言的逻辑和方法，全部都支持，非常完善
8. 对一些基础组件做介绍，结合 pdf 文档。（重点） （周三）
9. 对产品中使用到的 一些 技术做介绍。（为什么用、RA和Admin） （周三）
10. 实际使用演示做个一个小东西。（周三）

（Mp3 播放器、简版 QQ通信工具依靠远程桌面 源码放git）

1. 自己的作品，实际的工具，签名 验签工具。（周三晚上做一个简版的，周四征求意见）
2. 最有趣的地方，如果你是个做javaer 的开发者，或者说还不是个开发者，可以尝试一下用java做一些开发，不想C++ 那种做底层，需要考虑一些别的东西，java 是很成熟的语言了，你遇到的几乎所有问题都能找到答案。如果说刚学习的时候，抵触java，很大的可能是 因为只能看到命令行输出效果，枯燥且乏味。要想做个实际的东西，少不了要学前端，要搭服务器。如果你要做桌面上开发个 小程序，比如：任务清单啊、RSA算法签名加密验证啊，Base64编解码、16进制转换啊，都是很实用的东西。都可以试试。甚至用Java 写一个简单的socker通信都可以。
3. 总结：对这个培训的一个总结，如果你现在不想用或者没有什么想法，不要紧，当你有一天频繁的使用同一个操作的时候，你要回想一些 ，你可以直接做一个应用程序出来。
4. 了解 CA KMC 的配置文件， ①更新密钥之后需要做的处理，②学习配置文件

**待修改的部分：**

1. 代码中的问题：

1. 关于 超时时间的验证，释放key的验证，

2. 模板部分代码的优化，

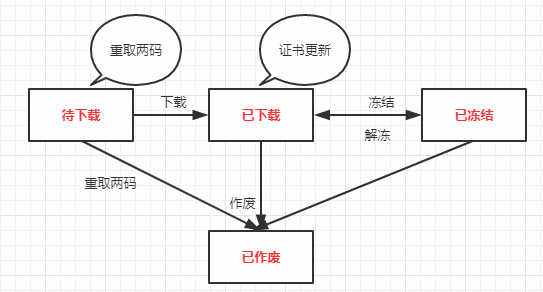
6. 修改管理员信息时，如果之前是 有内容的，比如 2222 如果删除掉 或者 写 “” ，提交之后都不会修改成，因为在插入数据库的时候，做了处理。

***开发中的重要逻辑问题：***

1. **证书的状态以及当前状态可以做的操作：**

**管理员证书**只有【作废】和【重获】功能。只有作废之后的证书才能重获。

**用户证书** 有 重取两码、更新证书、冻结证书、解冻证书、作废证书。



1. 模板的状态装换：

**模板的状态：** 已使用、未使用、

**模板的操作：**作废、删除、修改、查看、克隆

**已使用模板**不能 【作废】和【删除】

**已使用模板**可以【修改】，提示是否导出待下载证书信息，包括 certDN、user ID、userName

**未使用模板**支持 【作废】、【删除】、【修改】

作废模板不能恢复，作废模板和删除模板一个性质，只是还留存记录而已。

1. **密钥恢复的逻辑流程：**

**SM2：SM2的密钥恢复将加密私钥恢复到 Key中。**

1. 使用 KMC\_BO登录Admin，查询密钥，找到密钥
2. 开始密钥恢复，选择 司法密钥恢复员的证书
3. 输入PIN 调用Key做签名，
4. 选择 存储密钥的Key,完成写入操作。保存的名称：CatchPollKey

**RSA：RSA的密钥恢复将加密私钥恢复到Key中。**

1. 使用KMC\_BO登录Admin，查询密钥，找到密钥
2. 开始密钥恢复，选择 司法密钥恢复员的证书
3. 输入PIN 调用Key 做签名，
4. 选择保存密钥文件的路径，保存文件。
5. **证书下载的流程：**

Admin有两种下载证书的方式：输入P10 、本地产生P10.

**输入P10的方式**仅支持下载 SM2的单双证、RSA的单证。

**本地产生P10的方式**支持 SM2的单双证、RSA的单双证。

输入P10 下载证书，返回的结果以 视图的方式显示，勾选返回证书链，会返回证书链格式的证书信息。

本地产生P10下载证书，下载的结果直接写到 Key中。

1. **用户管理和用户证书下载：**

用户管理分为CA管理用户和RA管理用户：

☆ 如果CA管理用户 ，注册用户时，使用用户名注册用户，先查询是否存在，不存在，就产生一个uuid 作为用户的唯一标识，并返回两码。

☆ 如果是RA管理用户，注册用户时，直接使用用户名作为UUID 用户的唯一标识，并返回两码。

1. Key 的释放资源处理：

SM2 在登录时，登录失败发生异常， 释放 key。

登录成功，登录到某个管理员，等关闭管理员窗口时，释放。

RSA 在登录时，登录失败发生异常，不释放key。（因为 csp是static）

登录成功，登录到某个管理员，等关闭管理员窗口时，释放。

1. 产生证书请求失败：通过其他方式，检查USBKey是否可用，

运行异常排查：