手写信息数字签名系统服务端管理平台用户手册

(V1.3.7)

北京数字认证股份有限公司
北京市海淀区北四环西路 68 号双桥大厦 15 层
TEL：086-010-58045600
FAX：086-010-58045678
邮政编码：100080

目录

欢迎使用.....4
版权声明.....5
阅读指南.....6
名词解释.....6
约定.....7
第 1 章 产品简介.....8
1.1 产品简述.....8
1.2 产品架构视图.....9
第 2 章 管理使用说明.....10
2.1 前提条件.....10
2.2 用户登录.....11
2.2.1 证书方式.....11
2.3 主界面及功能模块介绍.....11
2.4 初始向导.....12
2.4.1 系统管理员添加.....13
2.4.2 系统 IP 端口初始化.....13
2.4.3 单位证书管理.....14
2.4.4 时间戳配置.....16
2.4.5 设备证书下载.....17
2.4.6 信任根证书下载.....17
2.5 签名管理.....18
2.5.1 表单模板管理.....18
2.5.2 基于表单模板签名规则.....19
2.5.3 基于 PDF 文件签名规则.....20
2.6 服务与配置.....21
2.6.1 服务启动与关闭.....21
2.6.2 系统时间同步.....21
2.6.3 服务日志管理.....22
2.7 数据与审计.....22
2.7.1 事件证书统计.....22
2.7.2 平台日志审计.....23
2.8 用户管理.....24
2.8.1 角色管理.....24
2.8.2 用户管理.....25
2.9 高级管理.....27
2.9.1 系统备份与恢复.....27
2.9.2 信任链管理.....28
2.9.3 事件证书 URL 配置.....30
2.9.4 集群同步配置.....31
2.9.5 服务器同步管理.....32

2.10 出库管理 32
2.10.1 出库信息配置 32
2.10.2 代理 ip 配置 34

第 3 章 服务热线 34

第 4 章 常见 FAQ 34

欢迎使用

欢迎您使用手写信息数字签名系统管理平台，本手册可以帮助您快速了解和掌握手写信息数字签名系统管理平台各项功能和具体的操作方法，如果本手册能为您提供帮助，带来便利，我们将深感欣慰。如果您在使用过程中，遇到了问题，或对我们产品有好的建议，可以：

- 致电客户服务热线 4007001900；
- 或访问公司网站：www.bjca.org.cn

与我们联系，对您提出的问题或建议，我们表示衷心地感谢。

版权声明

本手册著作权属北京数字认证股份有限公司所有，在未经本公司许可的情况下，任何单位或个人不得以任何方式对本手册的部分或全部内容擅自进行增删、改编、节录、翻印、改写。

北京数字认证股份有限公司

©2017

阅读指南

本手册可以帮助您快速了解和掌握 PDF 签章服务器系统（以下简称 AnySign）的各项功能和具体的操作方法。

- 本手册主要包括四个部分，本节阅读指南引导您了解本手册的主要内容、快速使用说明、阅读中的注意事项以及手册约定；
- 第 1 章产品简介，向您介绍本产品的产品简述、系统实体关系图和管理员权限说明；
- 第 2 章详细描述管理员的操作方法，指导管理员的日常系统管理工作。
- 第 3、4 章节向您解答本产品使用中可能遇到的常见问题处理方法，以及售后维护热线说明。

名词解释

名词	说明
XSS	手写信息数字签名系统
PDF	是一种电子文件格式，由 Adobe 公司开发而成。
手写数字签名	手写信息数字签名系统手写数字签名是一款应用于公众签名确认场景，为个人顾客提供无纸化可信手写签名服务的安全产品。电子单证转换成标准格式（PDF 或 XML），可实现个人手写和机构数字签名（签章），由事件型数字证书进行签字人手写数字签名。
数据签名	SDS 签名实质就是对数据进行签名，然后返回签名数据包，即电子单证转换成数据字节，调用一次性数字证书进行签字人数字签名。
时间戳签名	是数字签名技术一种变种的应用。是一个经加密后形成的凭证文档，它包括三个部分： （1）需加时间戳的文件的摘要（digest）； （2）DTS 收到文件的日期和时间； （3）DTS 的数字签名。
USBKEY	存储用户数字证书的硬件介质。

约定

约定标识	说明
!	此符号代表警告提示，需要读者特别注意该内容。
?	此符号代表对内容进行特别说明或解释。
*	此符号在界面中所对应的输入框或选择框为必填项或必选项

第 1 章 产品简介

1.1 产品简述

有效的提高运营效率和降低经营成本是各类企事业组织所共同追寻的目标。无纸化方案不但可以降低业务中的纸张耗材成本，还可以帮助您和您的顾客打破物理时空的束缚，享受信息化带来的提速效应。在这当中，可靠的电子签名无疑给无纸化应用带来一针定心剂，使您在体验业务优化的同时，免除了无纸化中合法、可靠、安全等问题的后顾之忧。手写信息数字签名系统即这样一款帮您摆脱纸张束缚的无纸化手写数字签名应用产品。PKI 应用体系与手写签名的有效结合，在保护无纸化业务签名的合法效力同时，也更符合个人的签名习惯及实际业务的场景需求。产品重点面向大众化的个人签字场景，让业务签名脱离纸张制约，节省耗材及管理成本，提高业务办理效率。无论是政务、电信、保险或医疗等应用领域，无论是在营业厅、窗口柜台，手写信息数字签名系统管理平台用户手册甚至是客户家中的签名确认场所，手写信息数字签名系统将为您带来权威可信、绿色环保的服务体验，为您实现经济、安全、高效的综合效益提升。

系统视图如下所示：

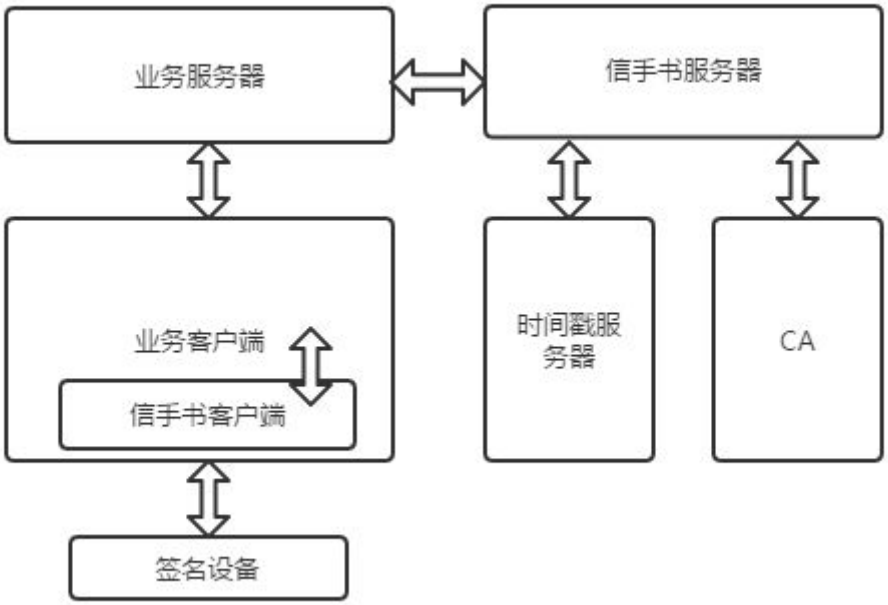


图 系统视图

1.2 产品架构视图

手写信息数字签名系统签名产品主要包括接口层、业务层和资源层。手写信息数字签名系统客户端集成在客户业务系统，调用接口层接口，接口层接口再调业务层的接口，实现签名业务，签名业务层调签名组件和签名库，完成整个业务。产品架构视图如下所示：

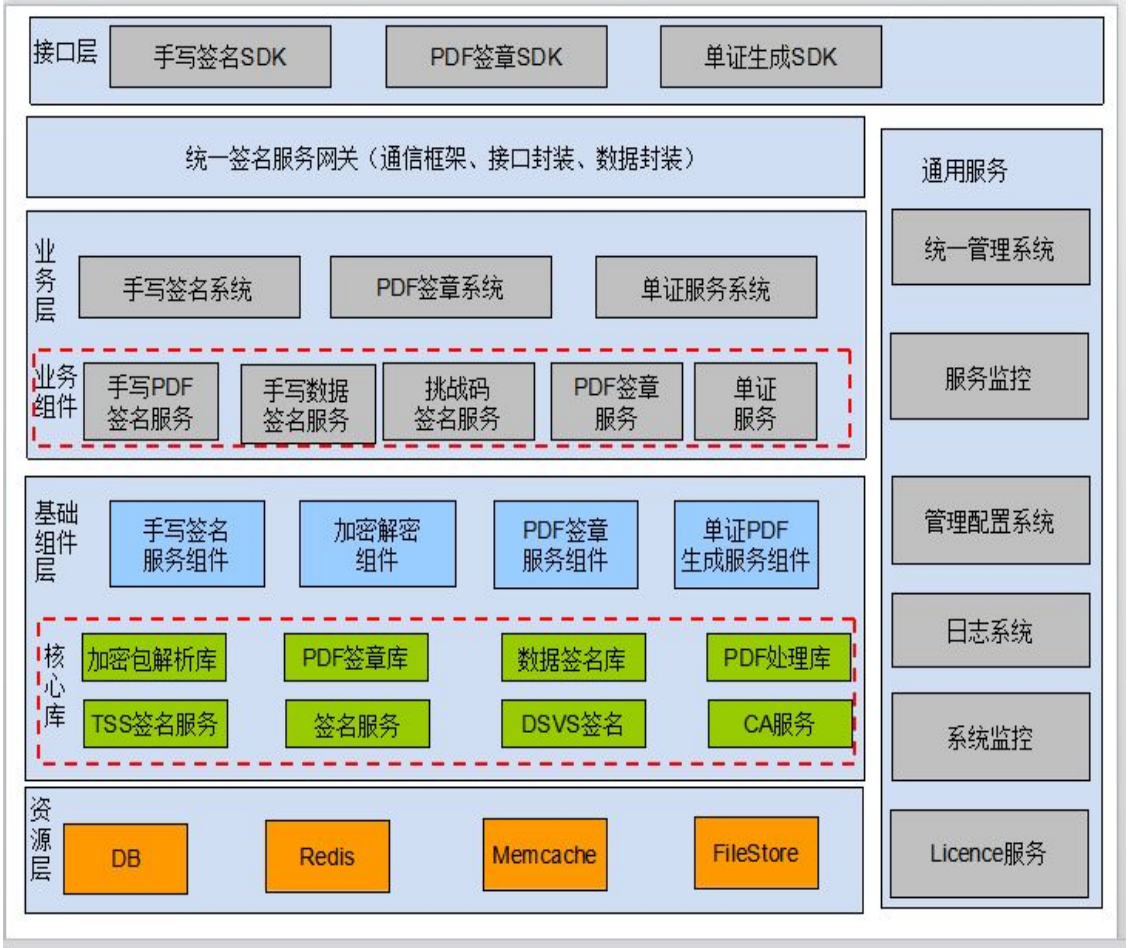


图 产品架构视图

第 2 章 管理使用说明

2.1 前提条件

1. 如果用户使用数字证书登录，需要在本地安装证书应用环境，点击登录首页中的【下载证书应用环境】，下载安装即可。
2. 管理员要使用 IE 9 版本的浏览器。

2.2 用户登录

系统管理员、普通用户在得到合法凭证后可以登录手写信息数字签名系统管理平台。在浏览器的地址栏中输入：http://服务地址:服务端口（手写信息数字签名系统默认是 192.168.1.1），访问手写信息数字签名系统管理平台的登录页面。服务地址和服务端口根据实际情况修改。登录方式：证书方式。

2.2.1 证书方式

在登录的客户端上插入存储管理员数字证书的 USBKey，系统自动将用户的证书显示在下拉列表中，用户输入证书口令，并点击【登陆】。如下图所示：

图 证书登录方式

使用证书登录时，登录的客户端一定要安装北京 CA 的证书应用环境。

2.3 主界面及功能模块介绍

登录成功后进入管理员的工作界面，如下图。此时，管理员就可以开展工作了。

工作界面主要分三大部分，分别为系统 logo、菜单功能栏、主操作界面：

（1） 系统 logo:显示产品名称、版本、管理员姓名等信息：

（2） 菜单功能栏：菜单功能栏包括以下 7 个功能模块：

- ✓ **初始向导**：包括系统管理员添加、系统 IP 端口初始化、单位证书管理、时间戳配置、设备证书下载以及信任根证书下载，方便管理人员首次使用系统。
- ✓ **签名管理**：包括表单模板管理、基于表单模板签名规则和基于 PDF 文件的签名规则。
- ✓ **服务与配置**：包括服务启动与关闭、系统时间同步以及服务日志管理。
- ✓ **数据与审计**：包括事件证书统计与平台日志审计。用于记录平时管理平台的工作状态。
- ✓ **用户管理**：包括角色管理与用户管理。可以实现对管理平台的用户与角色进行添加，删除，修改及授权等功能。
- ✓ **高级管理**：包括系统备份与恢复、信任链管理、事件证书同步 URL 配置、集群同步配置以及服务器同步管理等。
- ✓ **出库管理**：包括出库信息配置。

(3)主操作界面

每个功能模块有不同的操作界面，下面会对每个功能模块进行详细介绍。

2.4 初始向导

操作使用说明：登录系统后，点击【初始向导】-【系统管理员添加】，您可以添加新的管理员，从证书中获取。如下图所示：

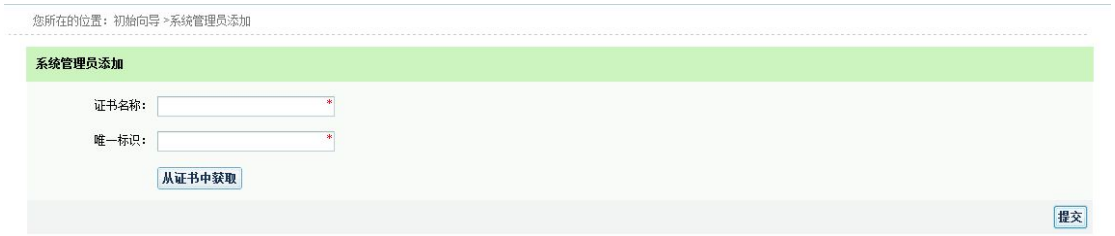


图 添加管理员

强烈建议您在首次使用本系统时完成初始化配置工作，并根据初始化向导的指引，在完成所有配置项后重启服务。

2.4.1 系统管理员添加

本模块用于添加系统管理员，您可以将您或其他用户添加为管理员，以便今后可以登录使用该系统。如果您需要再次添加管理员，或对现有管理员进行修改或删除操作，可以参考 2.9.2 小节用户管理模块。

在系统管理员添加界面，填写管理员信息，并单击【提交】添加管理员。您也可以直接从证书中获取管理员信息，单击【从证书中获取】，系统会自动读取当前证书用户姓名和证书唯一标识：

带*标记的输入框为必填项，请完整输入对应信息。

证书唯一标识为证书详细信息中 OID 为 2.16.840.1.113732.2 这一项的值。具体操作方法可以使用客户端证书管理工具打开证书，然后点击查看证书，在弹出的窗口中选择详细信息选项卡，从中找到域为 2.16.840.1.113732.2 的那项的值，就是这里需要输入的唯一标识。

2.4.2 系统 IP 端口初始化

根据提示配置系统 IP/端口的相应参数，点击【确定】，系统会自动重启加载相应设置，重启后完成初始化配置。如下图所示：

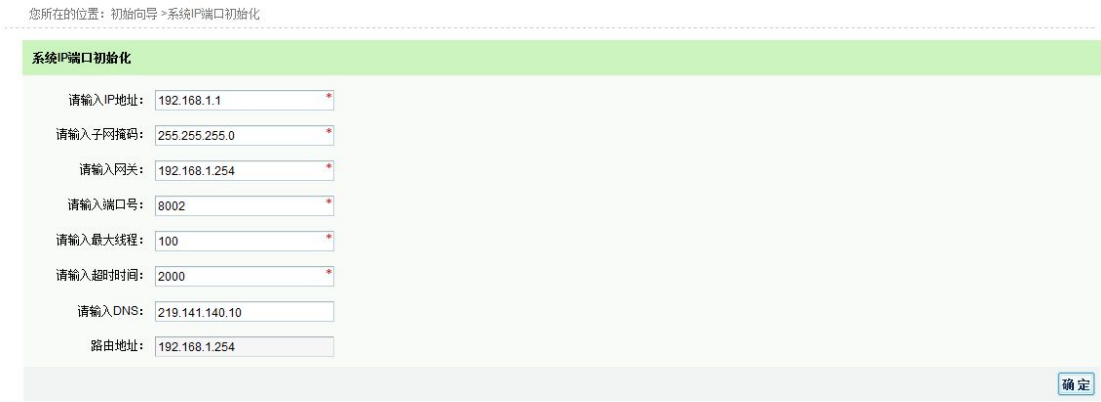


图 系统 IP 端口初始化

带*标记的输入框为必填项，请完整输入对应信息。

2.4.3 单位证书管理

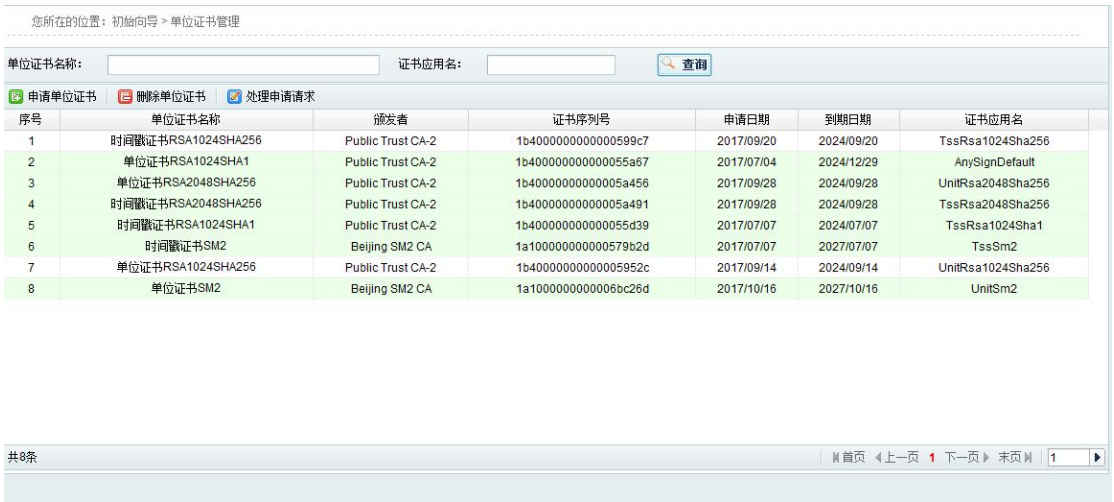


图 单位证书管理列表

当业务需要机构签章时（例如机构、企业、电信公司等），需要在服务端配置签名/签章所用的单位数字证书，实现签名时的密钥运算。单位证书全部在手写信息数字签名系统服务器上申请产生，CA 中心处理证书申请签发单位数字证书，将证书导入到手写信息数字签名系统服务器上完成单位证书的配置。添加新的单位证书后，需要在签名规则中选择该证书。

1、申请单位证书

点击【申请单位证书】，输入所需申请的单位证书信息，如下图所示：

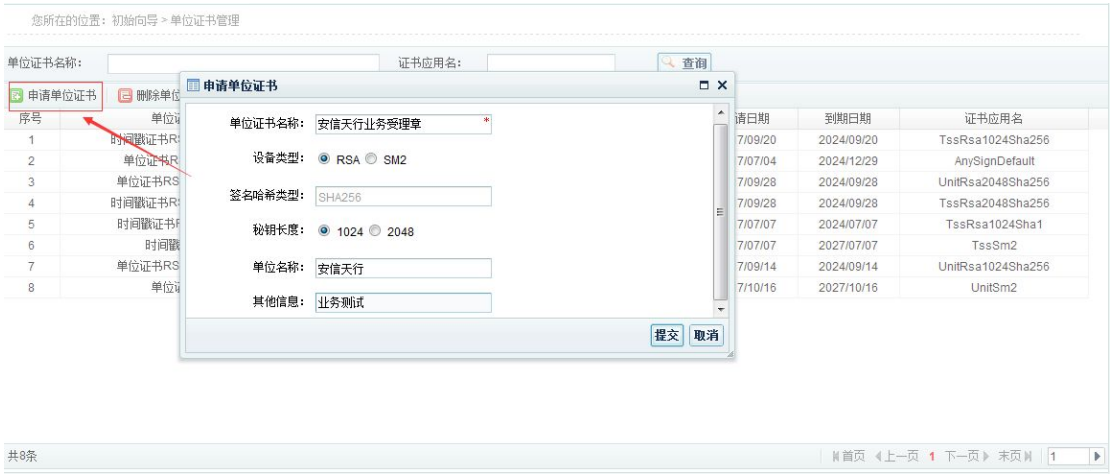


图 申请单位证书

设备类型为单位证书的算法类型，请根据项目需求选择 RSA 或 SM2 算法，当选择 RSA 时，签名哈希类型与出库管理-->出库信息配置-->CA 服务信息配置中的签名哈希算法一致，选择秘钥长度，信息输入完成后，点击提交。如下图所示：

图 生成证书请求

系统提示证书请求生成成功，根据提示保存证书请求文件（txt 格式），将该文件提交 CA 中心，获得单位数字证书。

2、单位证书导入

当获得 CA 签发的单位证书后，点击【处理申请请求】，选中要导入的单位证书项，点击【导入证书】。如下图所示：

图 导入证书

如果采用“输入证书内容”方式导入证书，请粘贴证书 Base64 编码内容到相应信息框内，输入应用名，如果应用名为空，则默认取证书的序列号，点击【提交】完成导入证书；同时您也可以采用直接上传后缀为 cer 格式的证书文件的方式完成导入证书。

2.4.4 时间戳配置

在此模块中，您可以开启和关闭时间戳服务器签发时间戳以及外部设备进行签章两个功能，使用方法与【服务启动与关闭】类似。当启用时间戳服务器或外部设备服务后，需要选择或定义对应的应用配置。同时可以点击配置文件下载中的文件名下载配置文件，并使用配置文件上传功能上传配置文件。如下图所示：

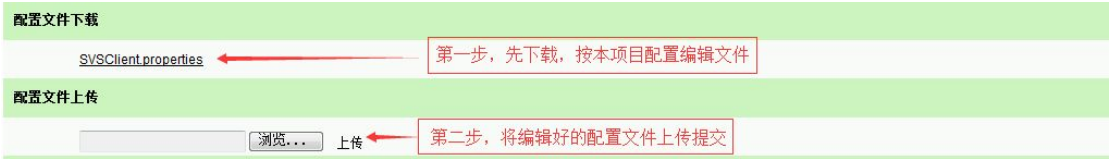
图 时间戳配置

当需要在 PDF 签名同时添加一个时间戳时，首先需要开启时间戳服务状态：

其次在时间戳应用配置中，选择对应的类型，当选择启用本地时间戳时，本地时间戳服务应用配置与 2.10.1 节 CA 服务信息配置中的 CA 类型和签名哈希算法一致，点击【提交】确认，如下图所示：

当不启用本地时间戳时，即选择在线时间戳，应用配置类型指向的是时间戳服务器的应用名，TSSDefault 默认代表 RSA 算法时间戳应用，TSSSM2 默认代表 SM2 算法时间戳应用，请根据您的项目算法需求选择。选中后，点击【提交】确认，如下图所示：

第三步，提交时间戳服务的配置文件。您需要首先下载默认的配置文件 SVSClient.properties，修改服务器地址 address1 和端口 port1，保存后上传配置文件：



上传配置文件成功后，时间戳的配置生效。

2.4.5 设备证书下载

在这里可以下载设备证书。如下图所示：

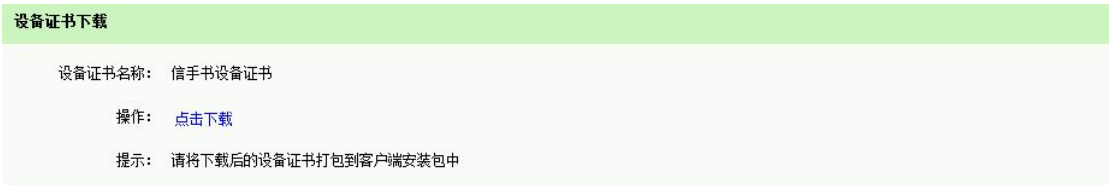


图 设备证书下载

点击【点击下载】，选择保存。如下图所示：

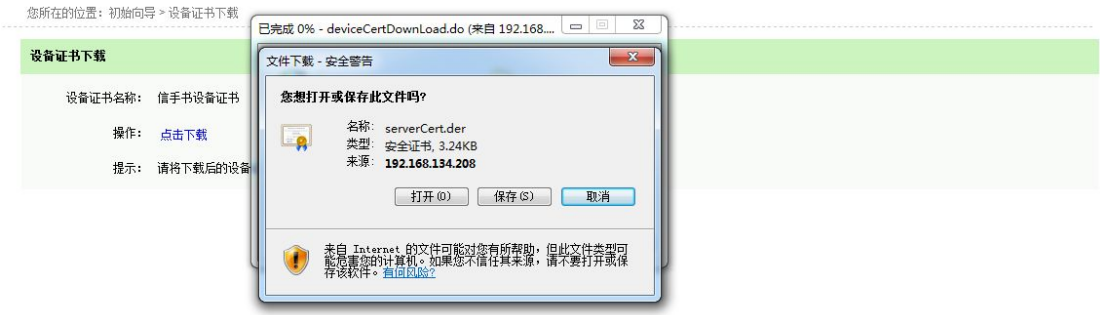


图 设备证书保存

2.10.4 中设备证书初始化之后，设备证书才能实现下载。

2.4.6 信任根证书下载

在这里可以对信任根证书进行下载，如下图所示：

2.5 签名管理

本模块用于配置手写信息数字签名系统服务器服务端签名相关策略，包括表单模板管理、基于表单模板和基于 PDF 文件的两种签名规则管理。

2.5.1 表单模板管理

手写信息数字签名系统产品支持基于表单模板+动态数据方式生成 PDF 格式文件，作为待签名的源文件。您可以将用于生成不同类型 PDF 的表单模板文件，通过表单模板管理提交到手写信息数字签名系统服务器上，并进行维护管理，如下图所示：

图 表单模版管理

在表单模板管理页面，您可以查找现有模板，查看模板内容，新建、修改或删除模板。点击【添加模板】，输入模板名称（在设置签名规则时将按模板名称匹配规则所对应的表单模板文件）并选择模板文件，如下图所示：

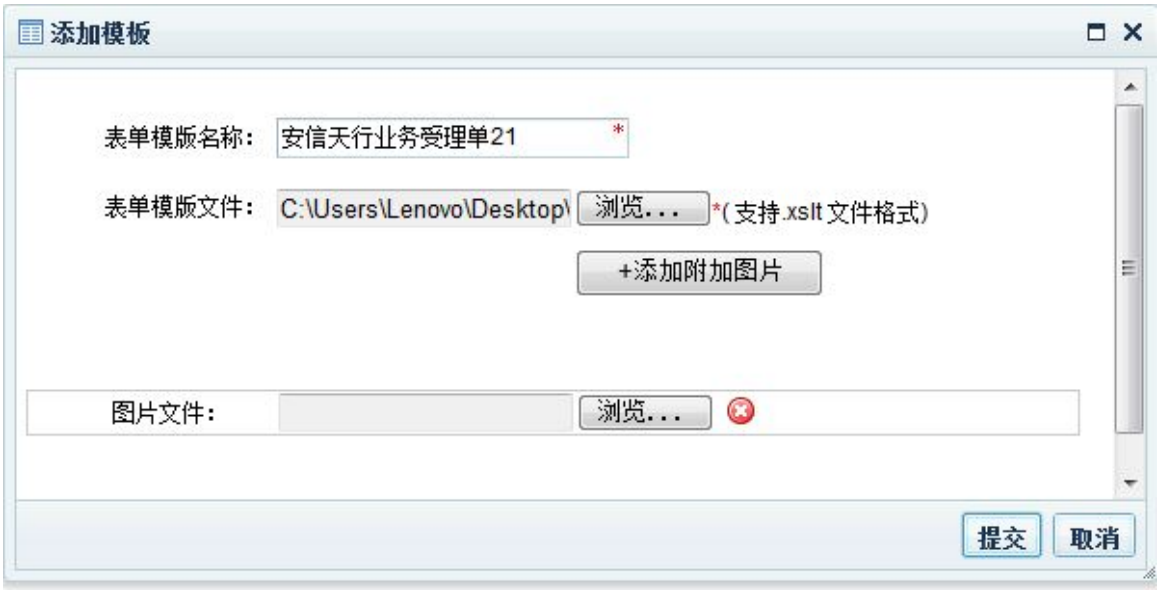


图 添加模板

手写信息数字签名系统支持 xslt 格式的表单模板，如果需要在模板中匹配图片（例如 LOGO 图），您可以在下面的图片文件中浏览添加所需图片。您还可以通过【查看模板】、【修改模板】功能实现对模板文件的查看和修改替换。

2.5.2 基于表单模板签名规则

手写信息数字签名系统提供两种方式在服务器端对 PDF 文件进行单位签章，本小节介绍基于表单模板方式。表单模板签名方式是输入表单数据，先按模板生成 PDF，再按规则进行电子签章。选择【添加规则】，基于表单模板的签名规则配置信息可以分为表单模板信息、签名规则信息和签名图片位置设置，如下图所示：

图 添加模板规则

表单模板信息：本规则生成 PDF 文件所用的表单模板名称。选定某表单模板后，手写信息数字签名系统将先按模板和业务提交的数据生成 PDF 文件，再按相应的签名规则)进行 PDF 电子签章。

签名规则信息：本规则签名的基本属性。包括：

- 签名规则名称：用于为您这一类型签名规则命名
- 签名规则编号：手写信息数字签名系统每次服务端签名时将根据该编号匹配对应的签名规则
- 单位证书：该类型规则电子签章时所用的印章数字证书
- 签名图片：该类型规则电子签章在 PDF 中显示的印章图片
- 修改签名图片：修改该类型规则电子签章在 PDF 中显示的印章图片
- 不透明度：印章图片在 PDF 中显示的不透明度，如示例，数值越高，颜色越深

签名图片位置设置：设置印章图片在 PDF 文件中的加盖位置。定位可以选择精准坐标定位或关键字搜索定位。

2.5.3 基于 PDF 文件签名规则

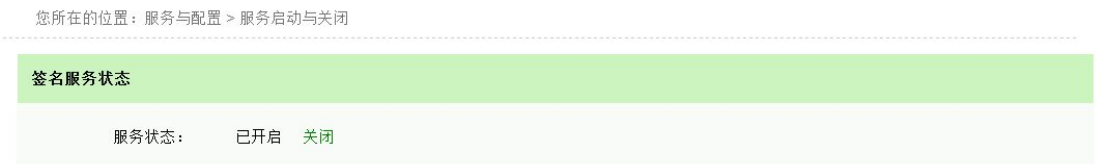
手写信息数字签名系统提供两种方式在服务器端对 PDF 文件进行单位签章，本小节介绍基于 PDF 文件签名方式。PDF 文件签名方式是输入已有的 PDF 文件，直接按规则进行电子签章。选择【添加规则】， 选择和填写签名规则相关参数设置。在签名规则设置上，基于 PDF 文件签名规则与表单模版签名规则方法相同，唯一区别是无需选择表单模板，如下图所示：

图 添加文件签名规则

2.6 服务与配置

2.6.1 服务启动与关闭

点击【开启】，即可开启服务；点击【关闭】，即可关闭签名服务。已开启如下图所示：



2.6.2 系统时间同步

您可以输入时间同步服务器的 IP 地址进行时间同步，点击【立即同步】或【确定】实现同步功能。如下图所示：

图 系统时间同步配置

2.6.3 服务日志管理

在服务日志管理中，你可以配置 SVSServer 的日志状态（开启或关闭），和 PDFServer 的日志级别，同时可以下载对应类型的日志文件。如下图所示：

图 服务日志管理

2.7 数据与审计

2.7.1 事件证书统计

点击【数据与审计】-【事件证书统计】，选择开始日期和结束日期，点击【查询】，就可以在查询结果中看到事件证书的统计结果。如下图所示：

图 事件证书统计

2.7.2 平台日志审计

点击【数据与审计】-【平台日志审计】，选择开始日期，结束日期，操作对象，操作类型，操作结果，操作人等查询信息，点击【查询】，就可以在查询结果中看到平台的日志记录。如下图所示：

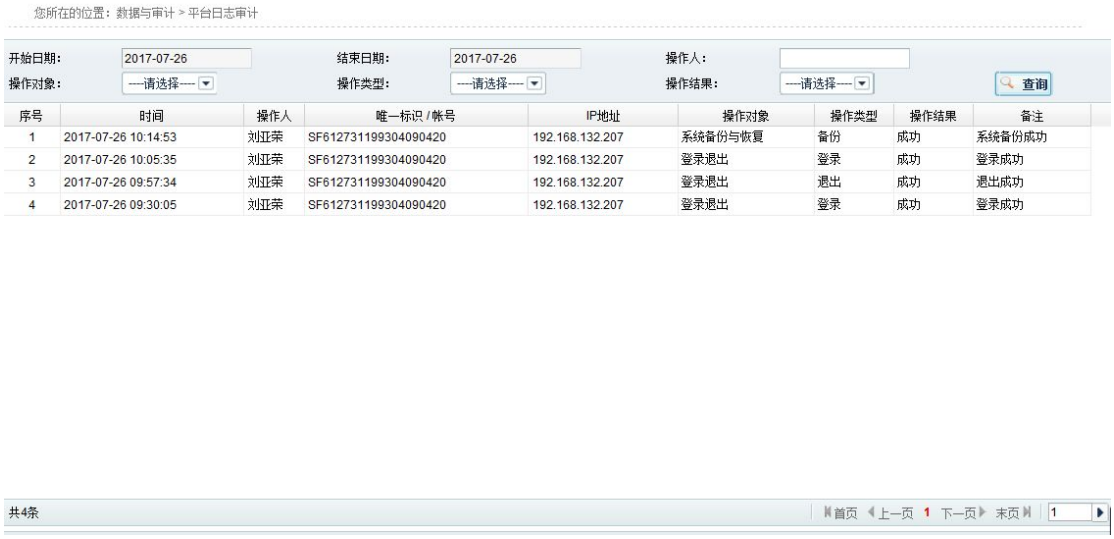


图 平台日志统计

2.8 用户管理

2.8.1 角色管理

点击【用户管理】-【角色管理】可以对角色进行添加，删除，修改，授权角色等操作。如下图所示：

图 角色管理

点击【添加角色】，输入角色名，点击【提交】，可以添加角色。如下图所示：

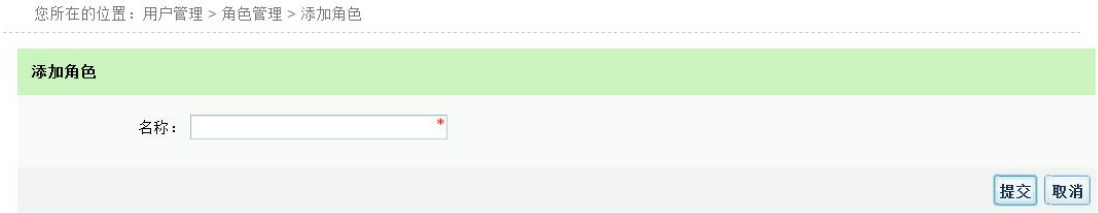


图 角色添加

选中想要修改的角色，点击【修改角色】，输入想要修改的角色名。点击【保存】，就可以修改角色。如下图所示：

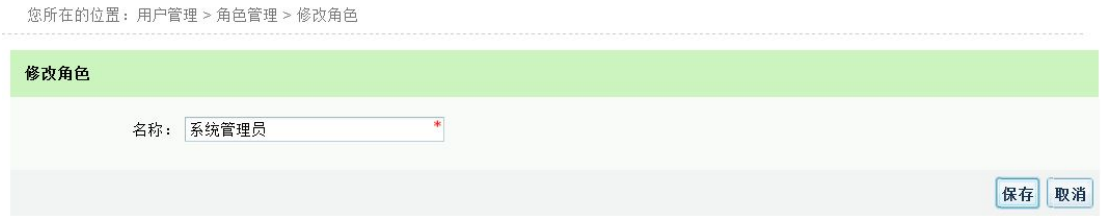


图 角色修改

选中想要删除的角色，点击【删除角色】，在弹出的提示框中选择【确定】，就可以删除选中的角色。如下图所示：

图 角色删除

选中想要授权的角色，点击【授权角色】，在弹出的对话框中选择授予的权限，点击【提交】，可以授权该角色。如下图所示：

图 角色授权

2.8.2 用户管理

点击【用户管理】-【用户管理】可以对用户进行添加，删除，修改等操作。下方显示当前系统中拥有的用户信息。如下图所示：

图 用户管理

点击【添加用户】，选择证书用户，证书用户可以直接从证书中获取用户信息，选择适当的角色（该用户所拥有的权限与此有关）。点击【提交】就可以添加新用户。如下图所示：

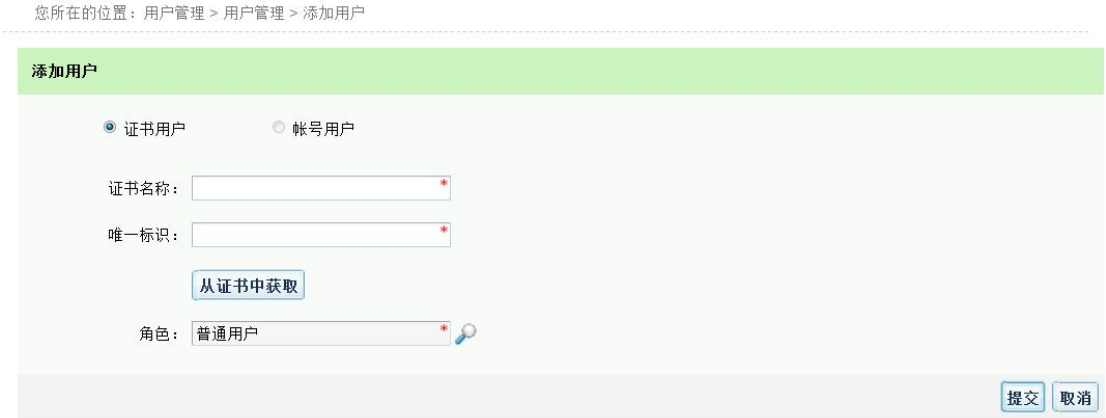


图 添加用户

选择需要删除的用户，点击【删除用户】，在弹出的确认框中点击【确定】。就可以删除用户。如下图所示：

图 删除用户

选择需要修改的用户，点击【修改用户】，即可进入修改页面。证书唯一标识和用户类型不能修改。点击【保存】确认修改。

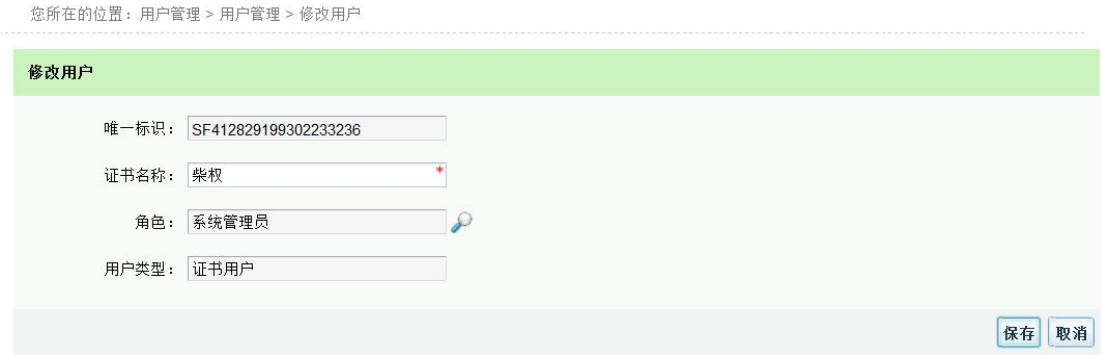


图 修改用户

2.9 高级管理

2.9.1 系统备份与恢复

此模块为您提供了备份与恢复功能，您可以备份手写信息数字签名系统服务器当前 BJCAROOT 下的一部分配置信息，保证系统瘫痪时的快速恢复。如下图所示：

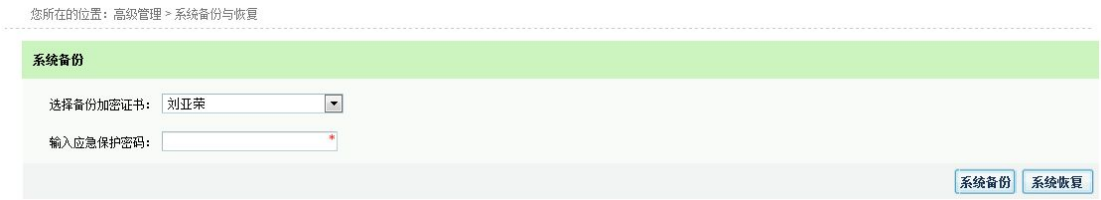


图 系统备份与恢复

选择备份加密证书以及输入应急保护码，点击【系统备份】。系统会弹出一个文件下载框，选择适当的路径保存备份文件。即完成备份。如果您想对系统进行恢复，点击【系统恢复】，系统跳转到恢复界面，如下图所示：

图 系统恢复

点击 选择备份文件的路径，上传您要恢复的备份文件；在恢复策略中，您可以选择使用证书恢复，也可以选择使用密码恢复。恢复策略中所使用的密码指的是您在备份中输入的应急保护密码。选择使用证书恢复，如下图所示：

图 证书方式恢复

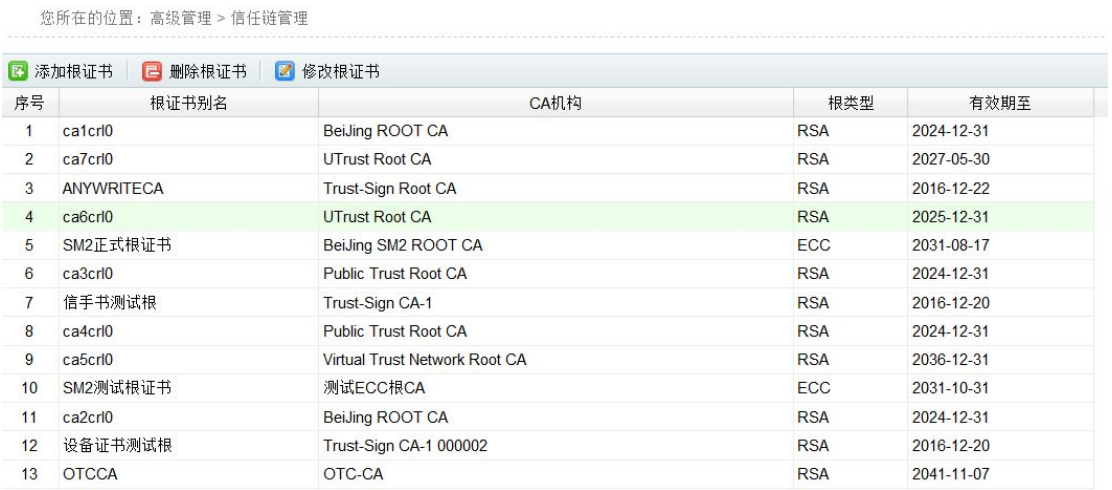
插入证书，输入证书口令，点击【系统恢复】即可。选择使用应急保护密码恢复，如下图所示：

图 口令方式恢复

输入应急恢复密码，点击【系统恢复】即可。

2.9.2 信任链管理

在此模块下可以实现根证书的添加，删除以及修改。如下图所示：



序号	根证书别名	CA机构	根类型	有效期至
1	ca1crl0	BeiJing ROOT CA	RSA	2024-12-31
2	ca7crl0	UTrust Root CA	RSA	2027-05-30
3	ANYWRITECA	Trust-Sign Root CA	RSA	2016-12-22
4	ca6crl0	UTrust Root CA	RSA	2025-12-31
5	SM2正式根证书	BeiJing SM2 ROOT CA	ECC	2031-08-17
6	ca3crl0	Public Trust Root CA	RSA	2024-12-31
7	信手书测试根	Trust-Sign CA-1	RSA	2016-12-20
8	ca4crl0	Public Trust Root CA	RSA	2024-12-31
9	ca5crl0	Virtual Trust Network Root CA	RSA	2036-12-31
10	SM2测试根证书	测试ECC根CA	ECC	2031-10-31
11	ca2crl0	BeiJing ROOT CA	RSA	2024-12-31
12	设备证书测试根	Trust-Sign CA-1 000002	RSA	2016-12-20
13	OTCCA	OTC-CA	RSA	2041-11-07

图 信任链管理

点击【添加根证书】，输入根证书别名，CA 名称，点击【浏览】选择根证书路径，然后点击【提交】，即可完成根证书的添加。如下图所示：

图 添加根证书

选中需要删除的根证书，点击【删除根证书】，在弹出的确认框中选择【确定】即可完成根证书的删除。如下图所示：

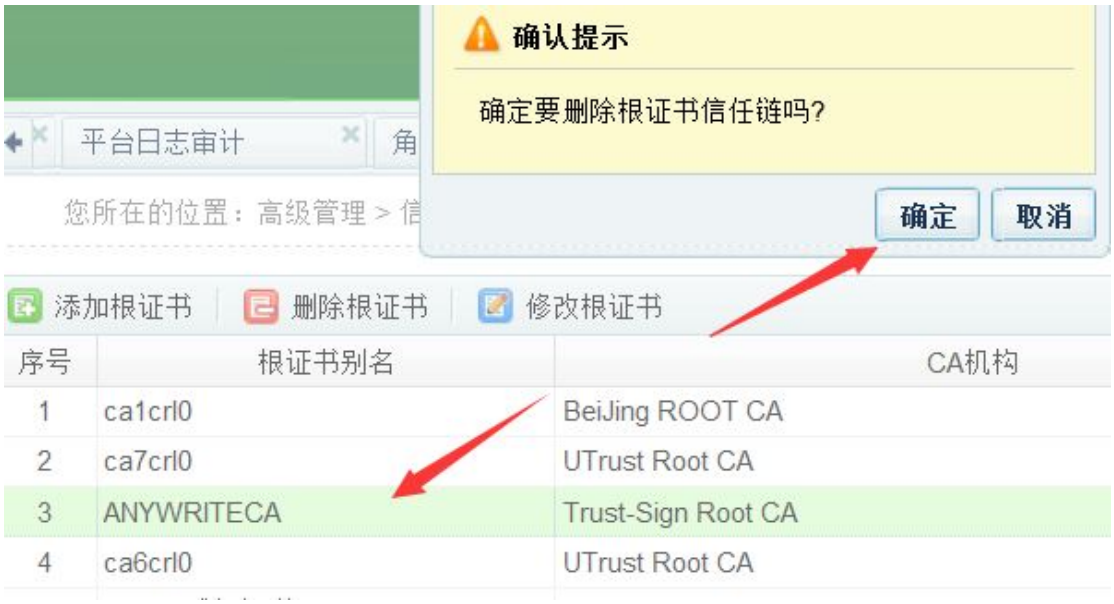


图 删除根证书

选择需要修改的根证书，点击【修改根证书】，在弹出的对话框中输入新的根证书别名，CA 名称，选择根证书路径。点击【保存】即可修改根证书。如下图所示：

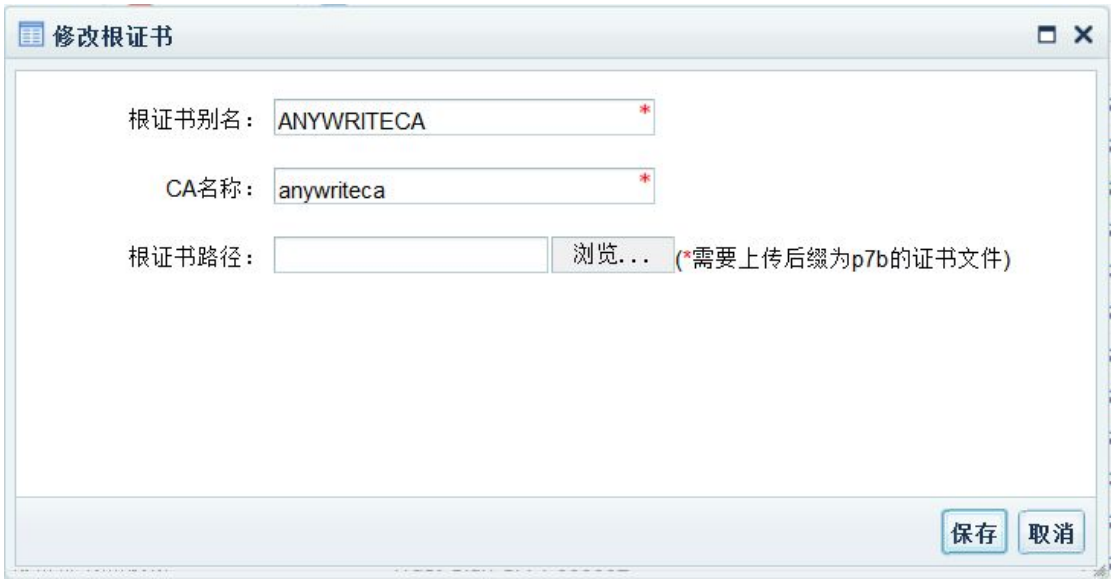


图 修改根证书

2.9.3 事件证书 URL 配置

点击【高级配置】-【事件证书 URL 配置】，可以对事件证书 URL 进行重新配置。如下图所示：

图 事件证书 URL 配置

根据需求选择 【使用本地签发证书】 或者 【使用公网签发证书】点击提交按钮，即可改变事件证书 URL 的配置。

2.9.4 集群同步配置

集群同步功能可以帮您更好的对多台手写信息数字签名系统系统集群模式下进行统一配置管理，本版本进群同步配置，同步范围包括“表单模板管理”、“基于表单模板签名规则”和“基于 PDF 文件签名规则”，当进行集群同步时，集群内其他服务器的表单模板配置和签名规则配置将按本机设置进行同步。（进行同步操作请见 2.10.6 服务器同步管理）如下图所示：

图 服务器集群配置

本界面用来设置参与集群同步管理的服务器，请您将所有集群服务器（包括本次访问的服务器）在本界面进行添加。如下图所示：

图 添加服务器

2.9.5 服务器同步管理

当需要进行集群服务器同步时，勾选接受同步的服务器，点击“集群服务器同步”，将当前的表单模板配置、签名规则配置同步到被勾选的服务器上。点击“数据库配置同步”将当前的数据库配置信息同步到被勾选的服务器上。你还可以通过服务器同步日志下载功能，下载集群内指定服务器的日志文件。如下图所示：

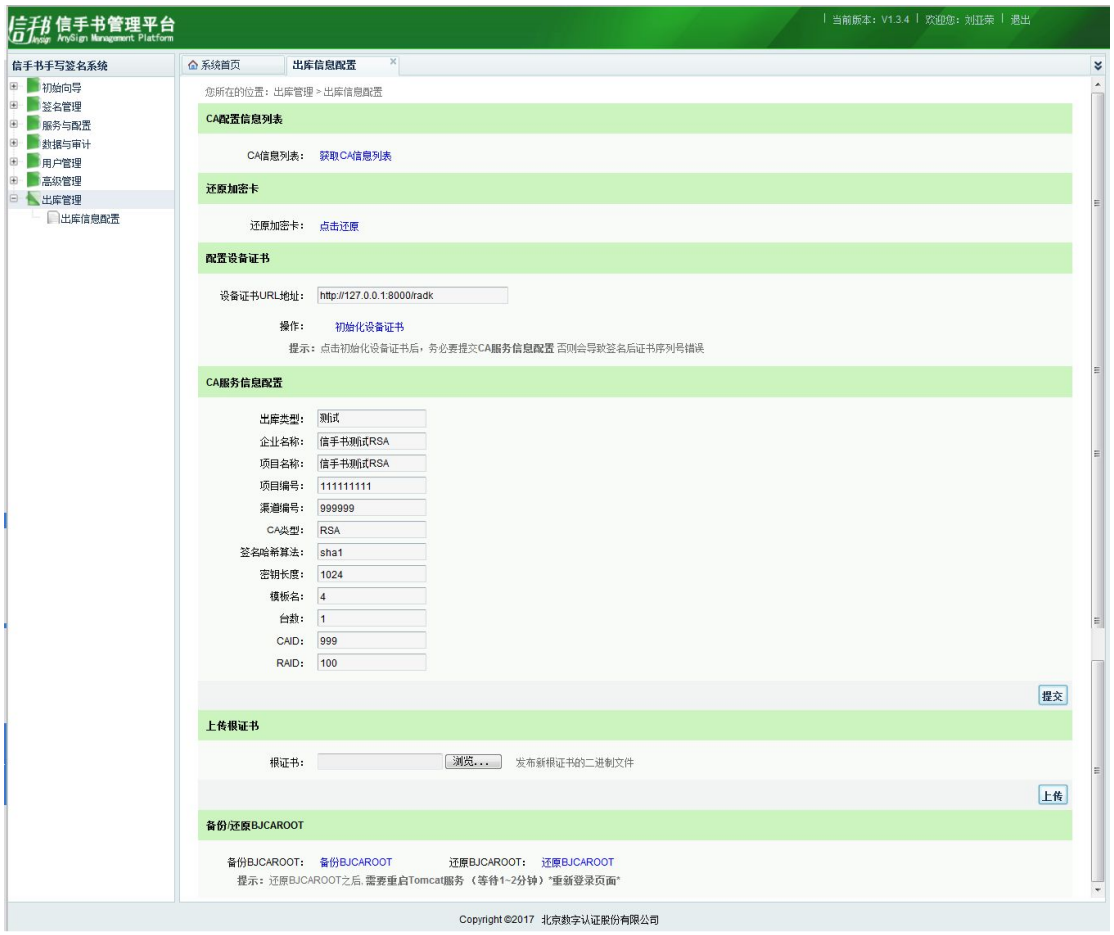
图 服务器同步管理

2.10 出库管理

2.10.1 出库信息配置

小提示：
本模块在产品出厂前配置，普通用户正常使用时请勿对本页面配置进行更改，以防造成系统无法正常使用！

出库信息配置用于服务器出厂配置，包括五个部分：获得 CA 信息列表、还原加密卡、配置设备证书、提交 CA 服务信息配置、上传根证书（非必填）、备份 BJCAROOT/还原 BJCAROOT。如下图所示：



CA 配置信息列表：点击【获取 CA 信息列表】，将手写信息数字签名系统需要出库的产品信息从手写信息数字签名系统生产管理系统中调用展示到 **CA 服务信息配置**中。

还原加密卡：点击【点击还原】，是将加密秘钥写入要出库的服务器中的加密卡中。

配置设备证书：点击【初始化设备证书】，通过本地 CA 签发设备证书，才能下载设备证书。

CA 服务信息配置：点击【提交】，目的是将列表信息配置到 CA 服务配置中。

上传根证书：上传信任根证书。

备份 BJCAROOT:点击【点击备份 BJCAROOT】，备份目的就是当服务器出现问题的时候可以把备份的 BJCAROOT 替换上。

还原 BJCAROOT:点击【点击还原 BJCAROOT】，目的是同一个项目多台服务出库时，保证设备证书不变。

2.10.2代理 ip 配置

生产人员在进行出库时，服务器默认 ip 为：192.168.1.1。由于出库时需要调用其他服务器中的地址，所以需要通过代理 ip 地址的方式来进行配置。

如下图所示：

svn 代理地址：输入 svn 的代理地址 ip。目的：是出库时备份 BJCAROOT 和还原 BJCAROOT 的时候需要调用 SVN 地址进行备份以及还原数据。

sftp 代理地址：输入 sftp 的代理地址 ip。目的：是出库时备份 BJCAROOT 和还原 BJCAROOT 的时候需要调用 SVN 地址进行备份以及还原数据。

生产运营系统代理地址：输入生产运营系统的代理地址 ip。目的：是出库时获取 CA 列表信息（调用接口）。

第 3 章 服务热线

如果您在使用过程中，遇到了问题，可以立即致电客户服务中心。

- 客户服务热线 4007001900；
- 或访问公司网站：www.bjca.org.cn

第 4 章 常见 FAQ

- **管理员登录时，插入证书介质后无法显示管理员名**

  请重新安装证书应用环境。