

签名验签服务器 用户手册

目 录

版本历史	1
1 引言	2
2 总体设计	3
2.1 需求概述	3
2.2 功能列表	3
3 登录	4
3.1 账号密码登录	4
3.2 证书登录	5
4 首页	6
5 用户管理	7
5.1 用户管理	7
5.2 角色管理	11
5.3 部门管理	15
6 应用管理	18
6.1 应用管理	18
7 签名验签	22
7.1 容器管理	22
7.2 签名日志	27

8 基本配置	32
8.1 证书链管理	32
8.2 CA 信息配置	35
8.3 密钥管理	42
9 日志管理	48
9.1 操作日志	48
9.2 登录日志	49
9.3 业务日志	50
9.4 系统日志	51
9.5 证书日志	52
10 系统管理	54
10.1 字典管理	54
10.2 菜单管理	54
10.3 参数设置	55
10.4 统计分析	55

版本历史

版本号	修改内容	修订日期	修订人
1.0	初始版本、详细说明签名验签服务器平台功能使用方法	2023.01.05	

1 引言

本文档主要描述签名验签服务器平台功能的使用方法。

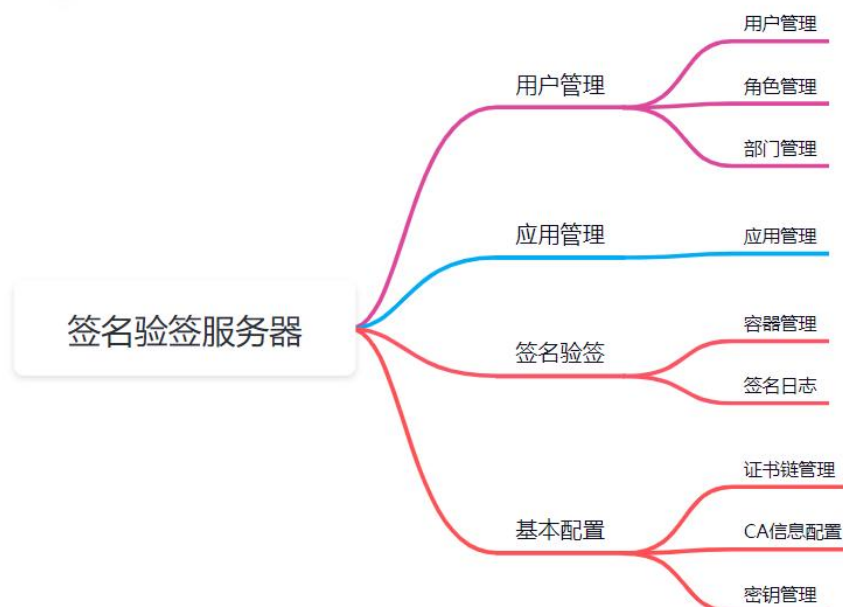
2 总体设计

2.1 需求概述

签名验签服务器，主要是一个管理平台，里面包含的模块有首页、用户管理、应用管理、签名验签、基本配置、日志管理、系统管理等。

2.2 功能列表

签名验签服务器主要分为用户管理模块、应用管理模块、签名验签、基本配置、系统管理等五个子模块，具体的功能列表如下所示。



3 登录

3.1 账号密码登录

- 1、输入用户名、密码、验证码，点击登录



签名验签服务器

V1.5.0

账号密码登录 证书登录

用户名

密码

验证码

登录

© 2020 签名验签服务器

3.2 证书登录

- 1、输入 UKEY 密码，点击登录



The screenshot displays the login interface for the '签名验签服务器 V1.5.0' (Signature Verification Server V1.5.0). The interface is framed by a blue border. At the top center is a blue circular logo containing a white shield with a star. Below the logo, the text '签名验签服务器' and 'V1.5.0' are centered. Two tabs are present: '账号密码登录' (Account Password Login) and '证书登录' (Certificate Login), with the latter being the active tab. Under the '证书登录' tab, there is a text input field with the placeholder '请输入UKEY密码' (Please enter UKEY password) and a lock icon on the right. Below the input field is a green icon of a USB UKEY. At the bottom of the input area is a large green button labeled '登录' (Login). The footer of the interface shows the copyright notice '© 2020 签名验签服务器'.

4 首页

- 1、点击左侧菜单栏的首页可以查看当前版本信息。



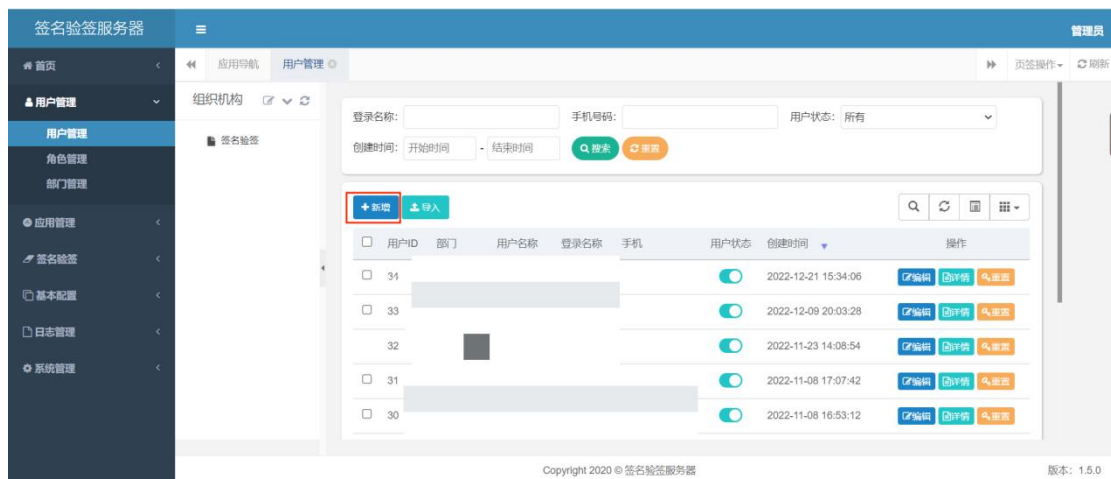
5 用户管理

5.1 用户管理

- 1、点击用户管理，可以查看当前系统下的所有用户。



- 2、点击新增，可以添加新的用户。



签名验签服务器

应用管理 用户管理 添加用户

基本信息

*用户名: 请输入用户名

*用户类型: 管理员

证件类型: --请选择证件类型--

登录账号: 请输入登录账号

用户状态: ☒

管理员证书: 上传文件 未选择任何文件

角色: [Avatar]

*归属部门: 请选择归属部门

手机号码: 请输入手机号码

证件号: 请输入证件号

登录密码: 请输入登录密码

邮箱: 请输入邮箱

其他信息

备注:

Copyright 2020 © 签名验签服务器 版本: 1.5.0

3、点击导入，可以批量添加新的用户。

签名验签服务器

应用管理 用户管理

组织机构 签名验签

登录名称: 手机号码: 用户状态: 所有

创建时间: 开始时间 - 结束时间 搜索 重置

+新增 导入

用户ID	部门	用户名	登录名称	手机	用户状态	创建时间	操作
34					☒	2022-12-21 15:34:06	编辑 删除 重置
33					☒	2022-12-09 20:03:28	编辑 删除 重置
32					☒	2022-11-23 14:08:54	编辑 删除 重置
31					☒	2022-11-08 17:07:42	编辑 删除 重置
30					☒	2022-11-08 16:53:12	编辑 删除 重置

Copyright 2020 © 签名验签服务器 版本: 1.5.0

导入用户数据

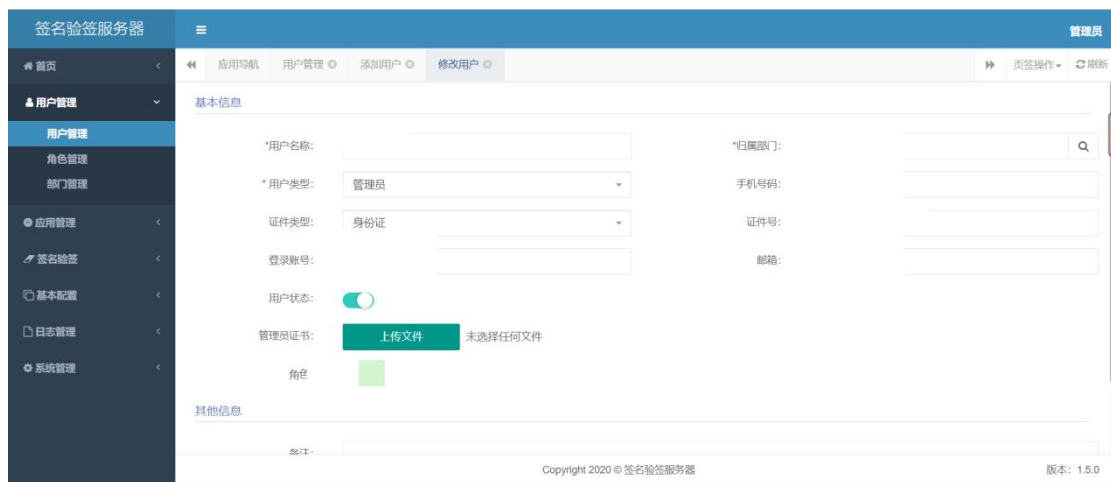
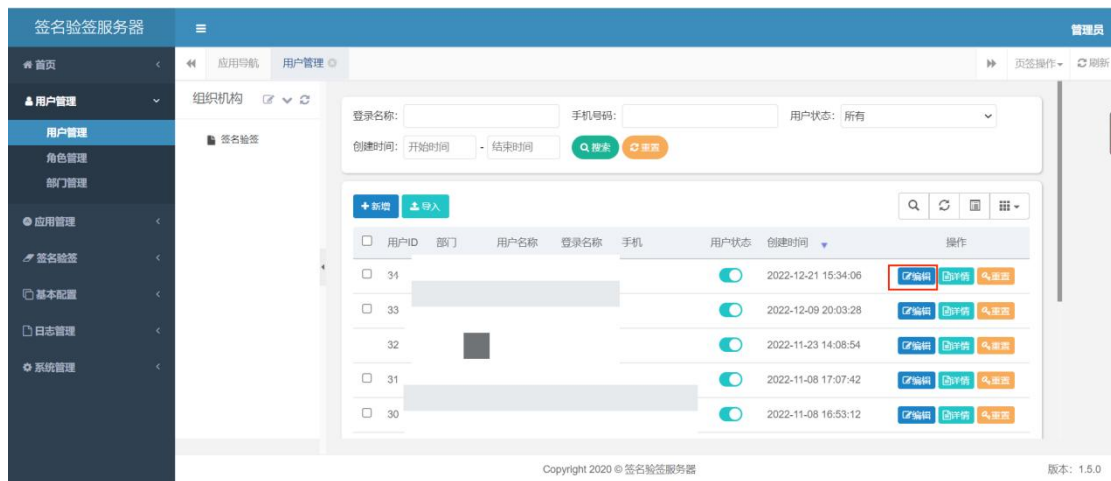
选择文件 未选择任何文件

☐ 是否更新已经存在的用户数据 下载模板

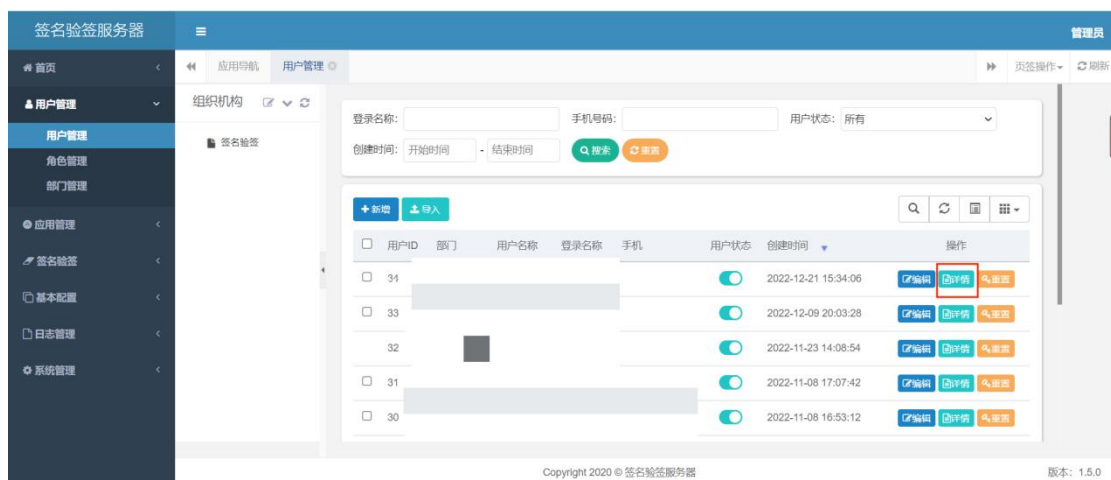
提示: 仅允许导入“xls”或“xlsx”格式文件!

导入 取消

4、点击编辑，可以对用户进行编辑。



5、点击详情，可以查看当前用户详细信息。



用户详细

用户Id:

部门Id:

登录名:

用户名:

用户状态:

证件类型:

关闭

6、点击重置，可以重置当前用户密码。

签名验签服务器

应用管理

用户管理

用户管理

角色管理

部门管理

应用管理

签名验签

基本配置

日志管理

系统管理

组织机构

签名验签

登录名称:

手机号码:

用户状态: 所有

创建时间: 开始时间 - 结束时间

搜索

重置

+新增

导入

用户ID

部门

用户名

登录名称

手机

用户状态

创建时间

操作

☐	34					2022-12-21 15:34:06	编辑 详情 重置
☐	33					2022-12-09 20:03:28	编辑 详情 重置
☐	32					2022-11-23 14:08:54	编辑 详情 重置
☐	31					2022-11-08 17:07:42	编辑 详情 重置
☐	30					2022-11-08 16:53:12	编辑 详情 重置

重置密码

登录名称:

输入密码:

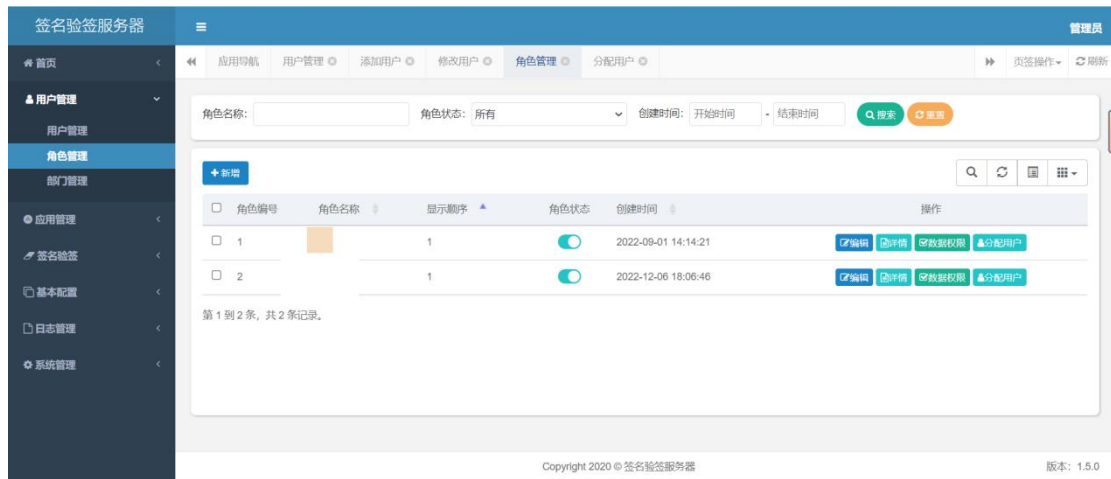
确定

关闭

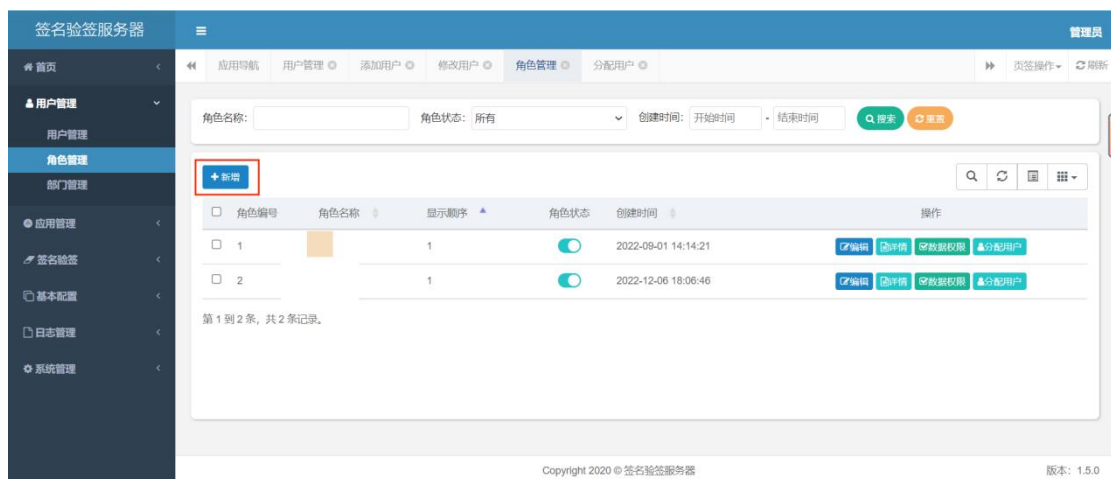
10

5.2 角色管理

1、点击角色管理，可以看到当前系统下所有的角色。



2、点击新增，可以添加新的角色，可以选择对应的菜单权限控制。



添加角色

*角色名称:

*显示顺序:

状态:

☒

备注:

菜单权限

☐ 用户管理
 ☐ 应用管理
 ☐ 签名验签
 ☐ 基本配置
 ☐ 日志管理

确定

关闭

3、点击编辑，可以对当前角色进行编辑。

签名验签服务器

应用管理

用户管理

添加用户

修改用户

角色管理

分配用户

角色名称:

角色状态: 所有

创建时间: 开始时间 - 结束时间

搜索

重置

+ 新增

角色编号	角色名称	显示顺序	角色状态	创建时间	操作
1		1	☒	2022-09-01 14:14:21	编辑 删除 分配权限 分配用户
2		1	☒	2022-12-06 18:06:46	编辑 删除 分配权限 分配用户

第 1 到 2 条, 共 2 条记录。

Copyright 2020 © 签名验签服务器

版本: 1.5.0

修改角色

*角色名称:

*显示顺序:

状态:

☒

备注:

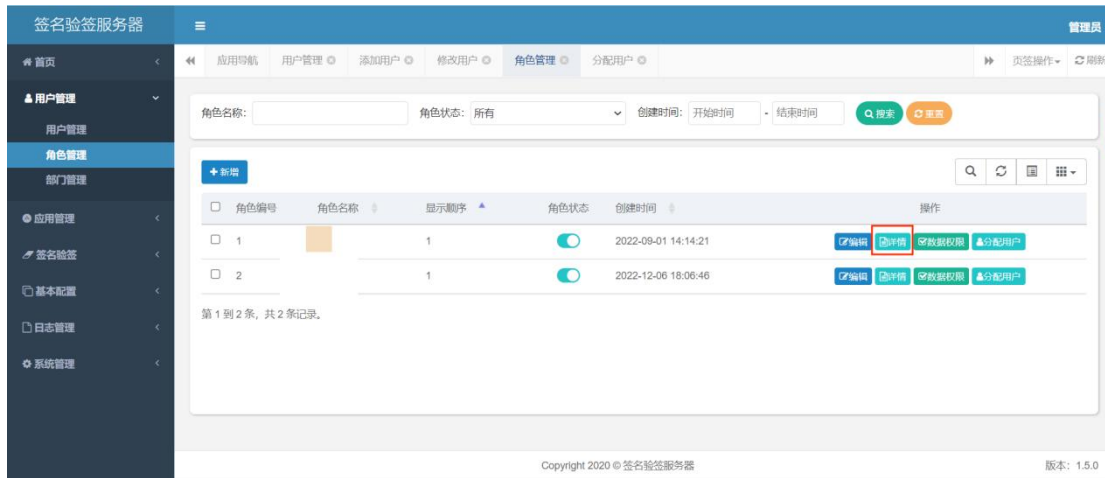
菜单权限

☒ 用户管理
 ☒ 应用管理
 ☒ 签名验签
 ☒ 基本配置
 ☒ 日志管理

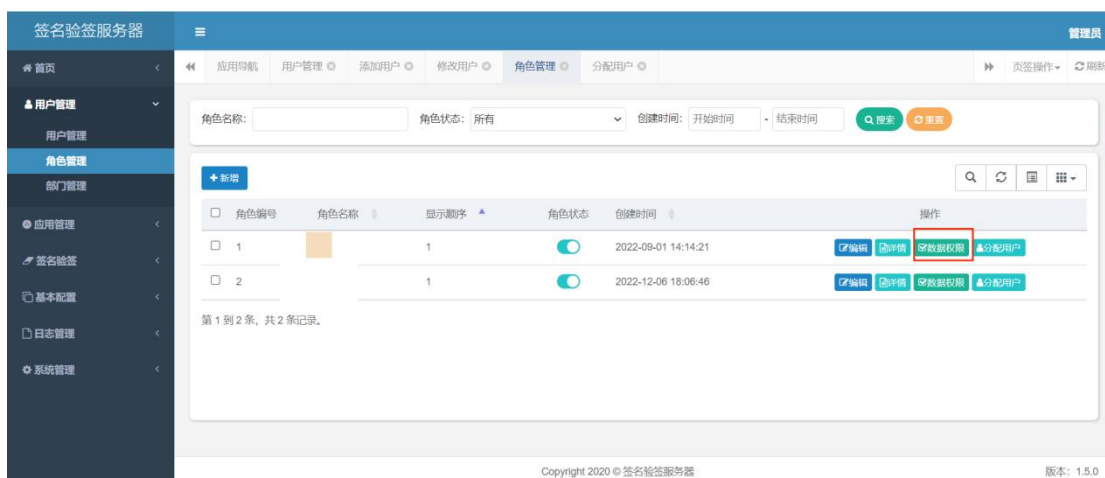
确定

关闭

4、点击详情，可以查看当前角色详细情况。



5、点击数据权限，可以查看当前角色所拥有的操作系统的权限。



分配数据权限

角色名称:

权限字符:

数据范围:

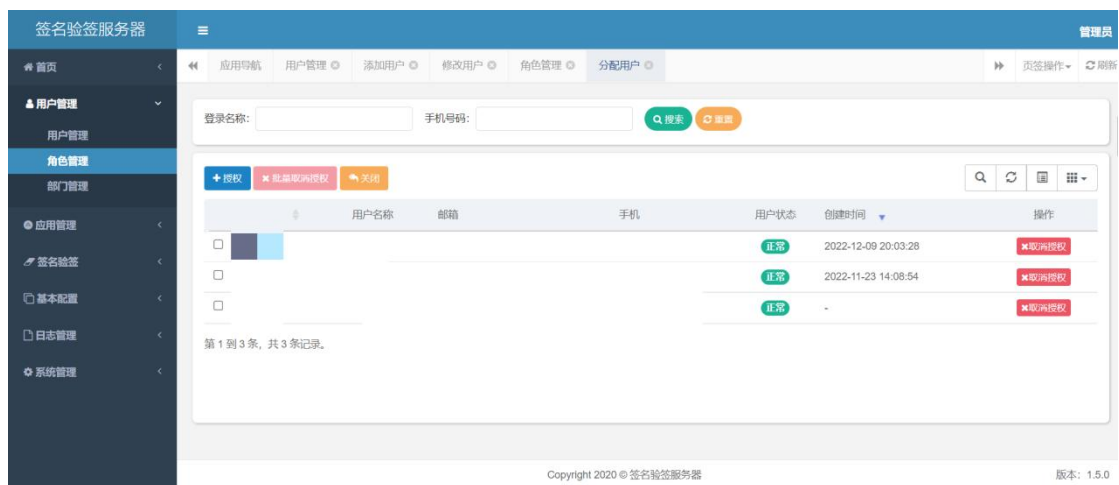
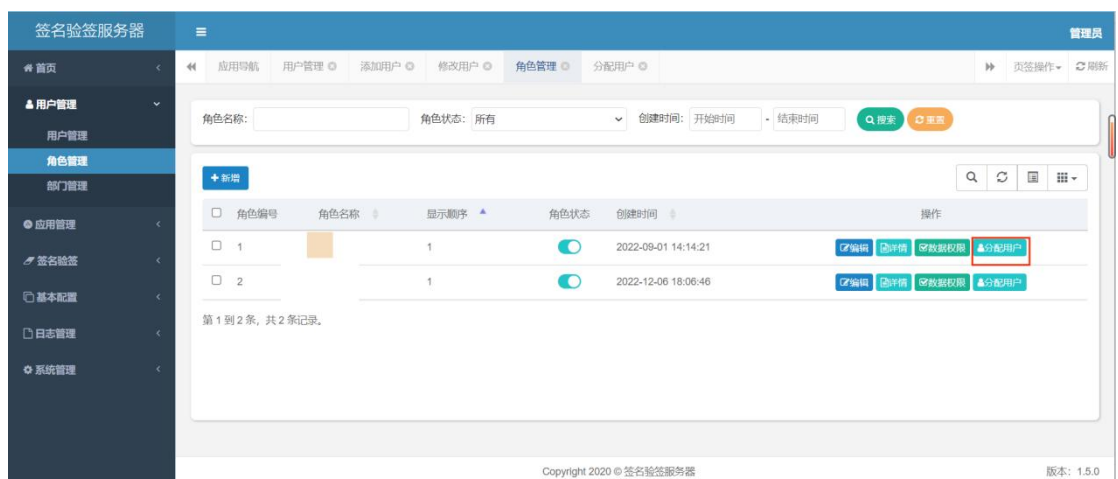
全部数据权限

❗ 特殊情况下，设置为“自定数据权限”

确定

关闭

6、点击分配用户，可以对角色分配用户，可以对所分配的用户进行授权。



5.3 部门管理

1、点击部门管理，可以看到当前系统所拥有的所有部门。



2、点击新增或添加下级部门，可以增加新的部门。



添加部门

上级部门:

*部门名称:

*显示排序:

负责人:

联系电话:

邮箱:

部门状态:

☒ 正常
 ☐ 停用

确定

关闭

3、点击编辑，可以对当前部门进行编辑。

签名验签服务器

应用管理

用户管理

添加用户

修改用户

角色管理

分配用户

部门管理

应用管理

签名验签

基本配置

日志管理

系统管理

部门名称:

部门状态: 所有

搜索

重置

新增

展开/收缩

部门名称	排序	状态	创建时间	操作
	0	正常		编辑 添加下级部门 部门详情

Copyright 2020 © 签名验签服务器

版本: 1.5.0

修改部门

上级部门:

无

*部门名称:

*显示排序:

0

负责人:

联系电话:

邮箱:

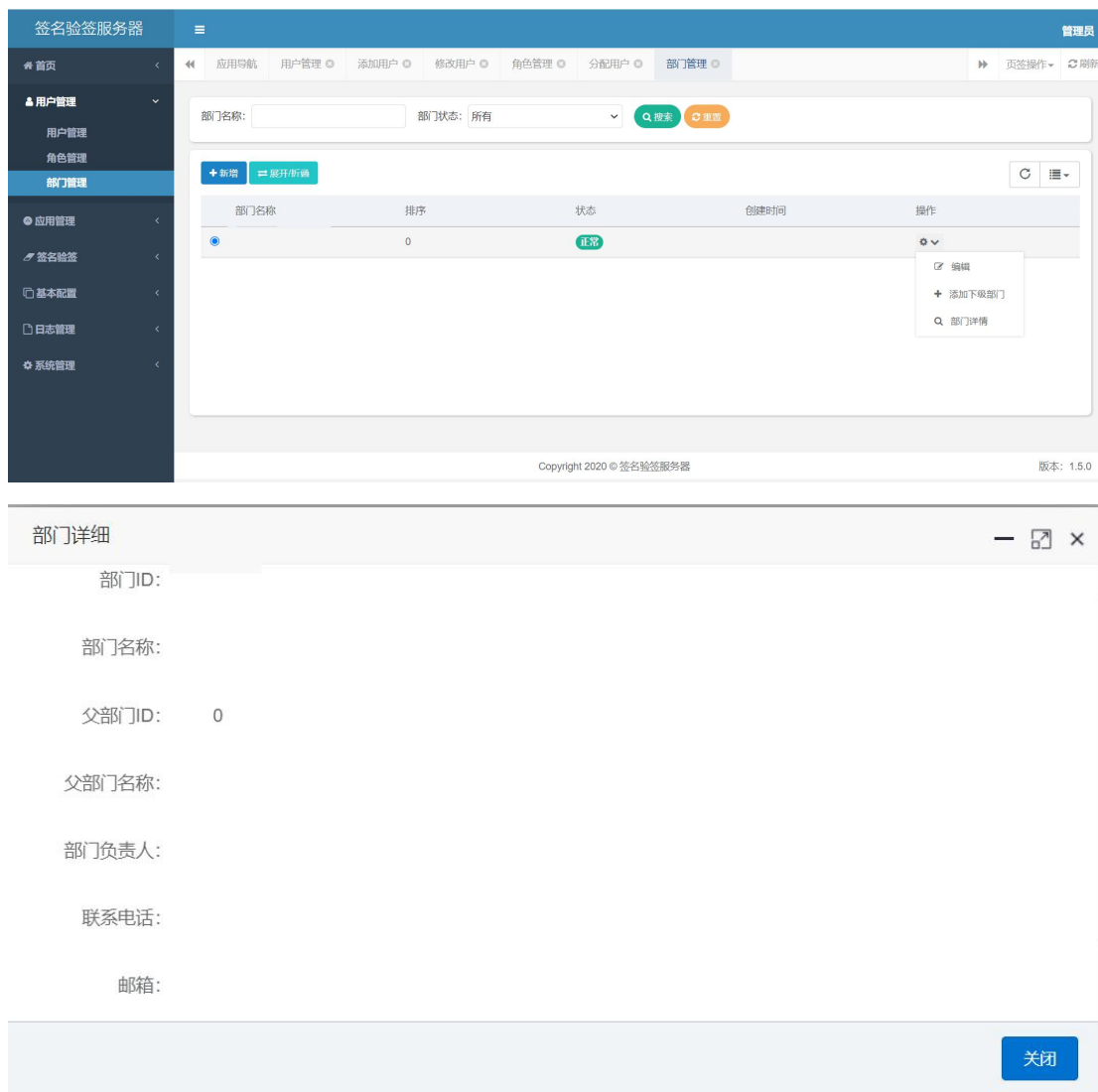
部门状态:

☒ 正常
 ☐ 停用

确定

关闭

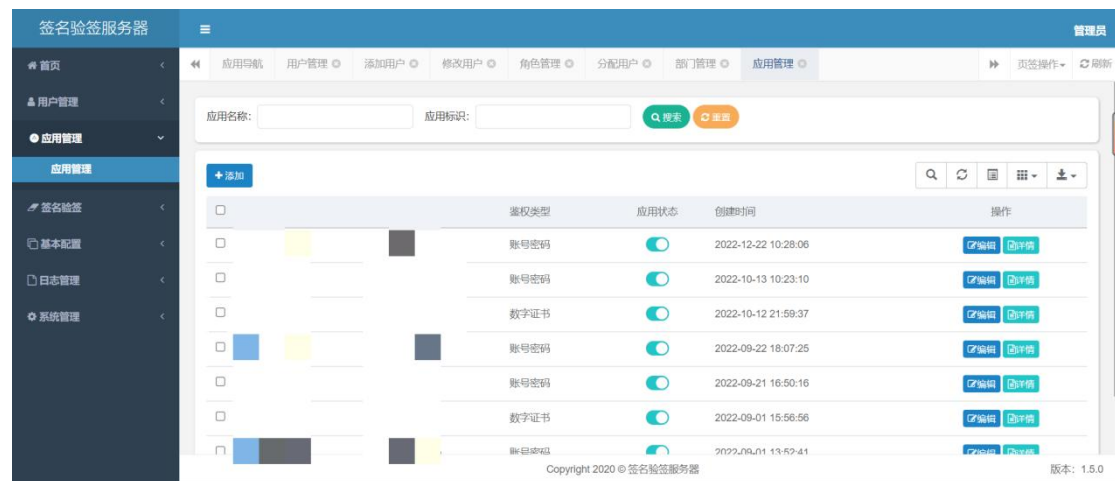
4、点击部门详情，可以查看当前部门详细。



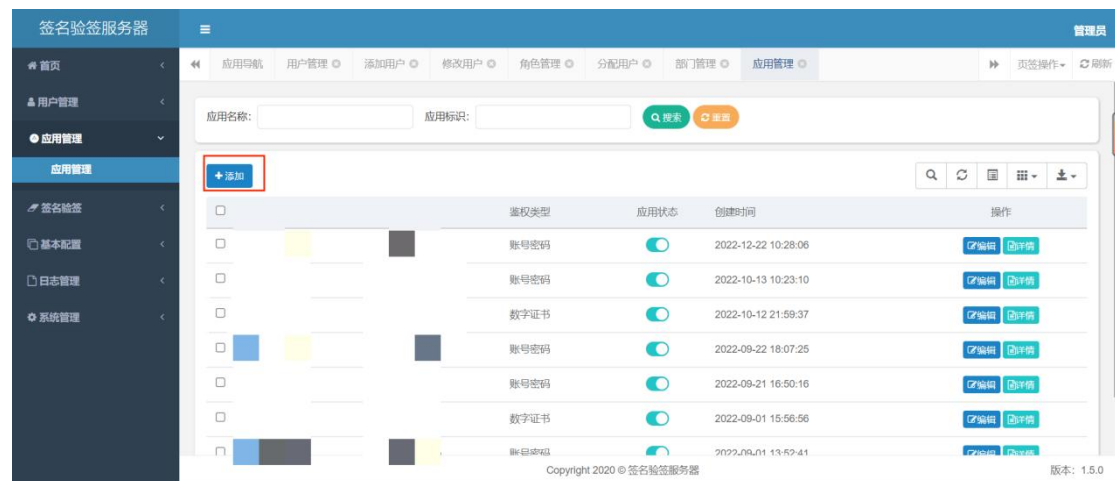
6 应用管理

6.1 应用管理

1、点击应用管理，可以查看当前系统全部应用列表。



2、点击添加，可以添加新的应用。





添加应用系统

*应用名称:

*应用标识:

*鉴权方式: 通信密码

*通信密码:

鉴权模块: ☐ 签名验签 ☐ 用户管理

IP白名单开关: ☐

确定 关闭

1. 在添加新的应用时，添加的应用名称是作为应用名使用，应用标识是作为这个应用唯一标识。

2. 鉴权方式主要有两种：

1. 通信密码，主要通过应用标识及通信密码一起进行鉴权。

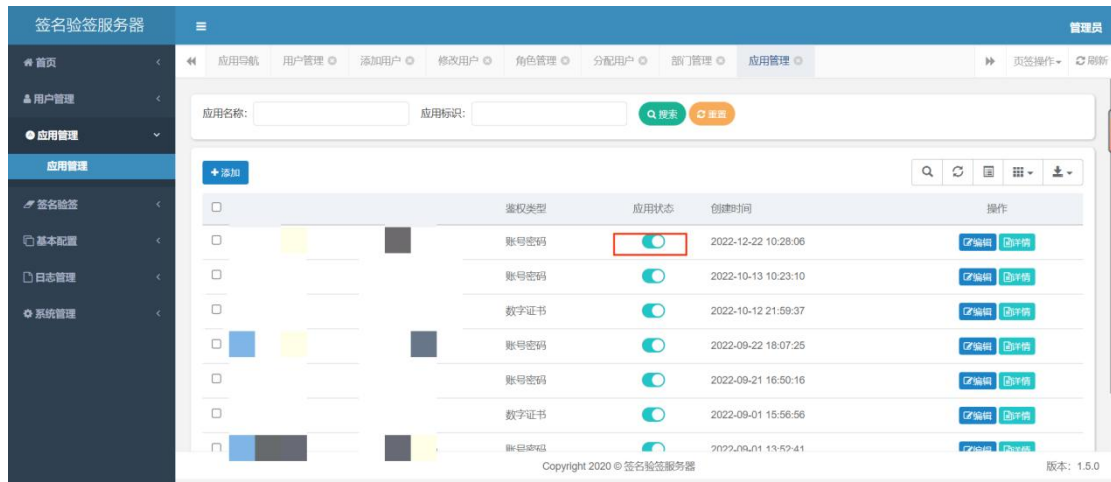
2. 数字证书，鉴权时通过应用标识及数字证书进行鉴权，鉴权方式是通过应用标识、签名值、签名原文进行鉴权。

3. 在鉴权方式选择通信密码时，通信密码必填，鉴权方式选择数字证书时不需要填写通信密码。

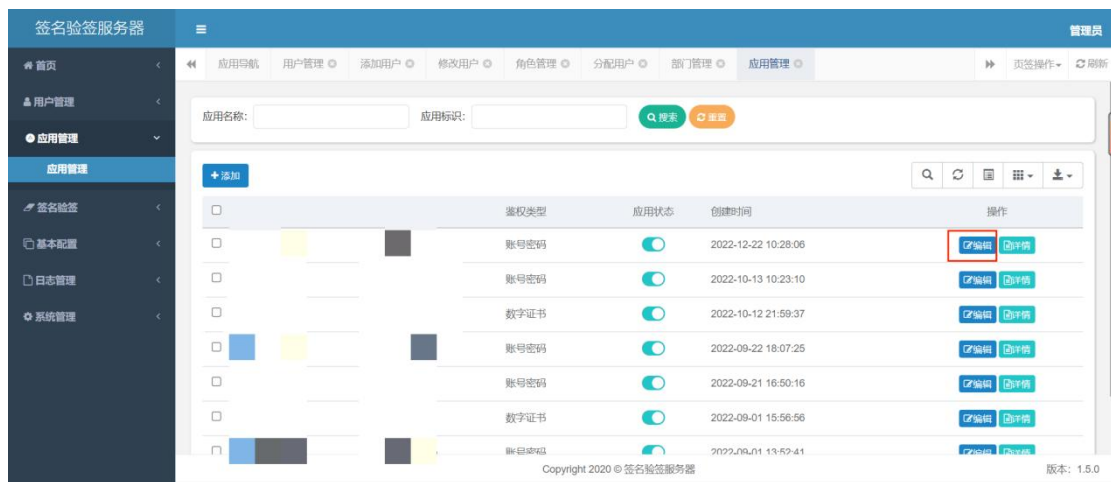
4. 鉴权模块可以选择签名验签及用户管理，通过选择的鉴权模块可以给应用设置鉴权权限。

5. ip 白名单开关主要作用就是设置白名单 ip 用户。

3、点击应用状态，可以选择关闭或开启应用。



4、点击编辑，可以对当前应用进行编辑。



修改应用系统

*应用名称:

*应用标识:

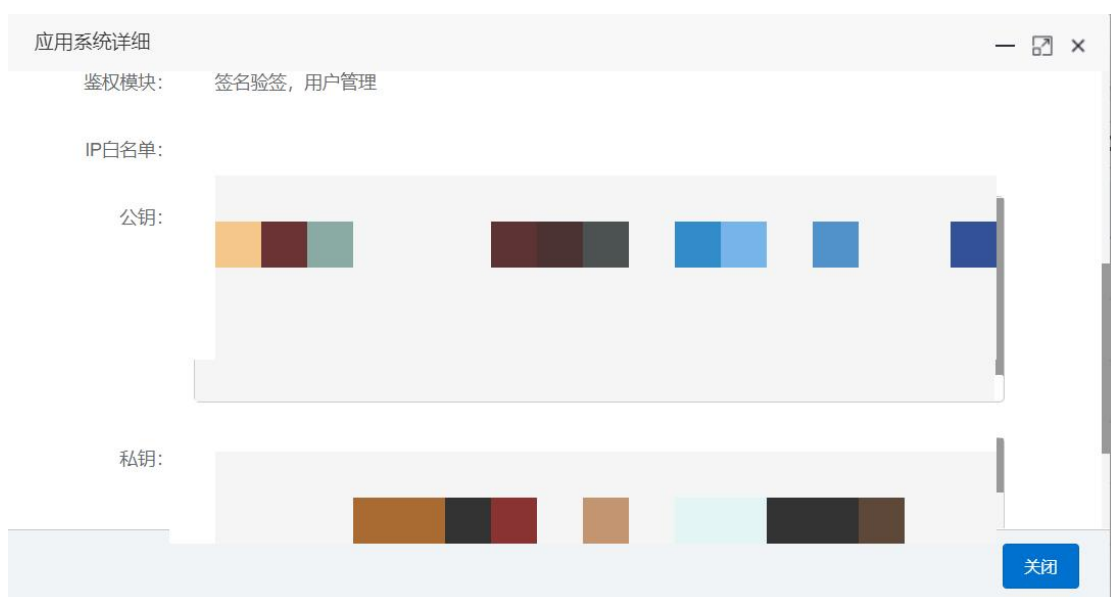
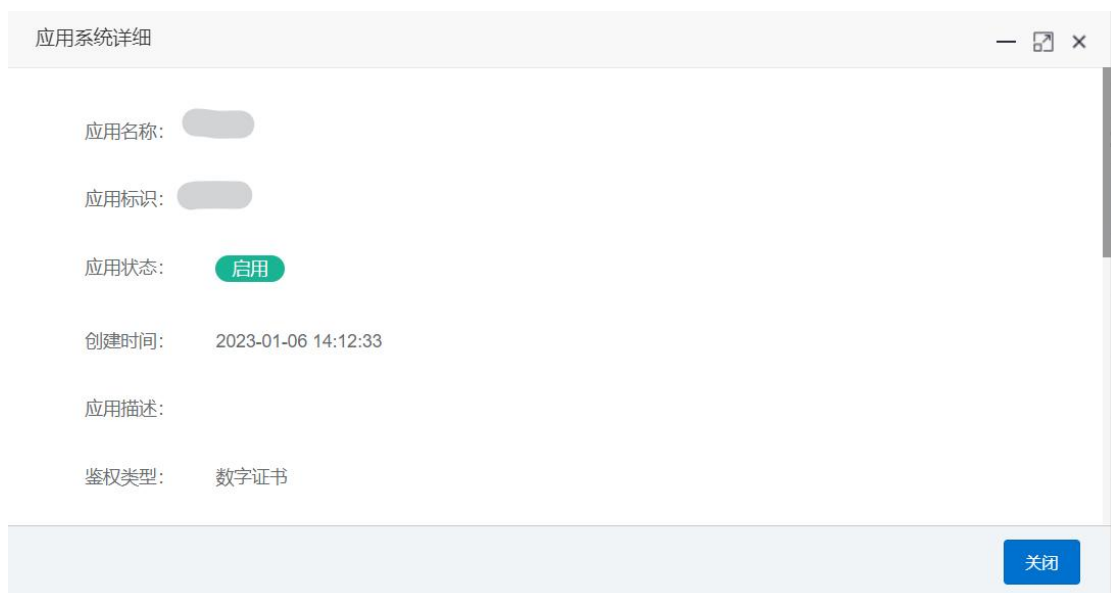
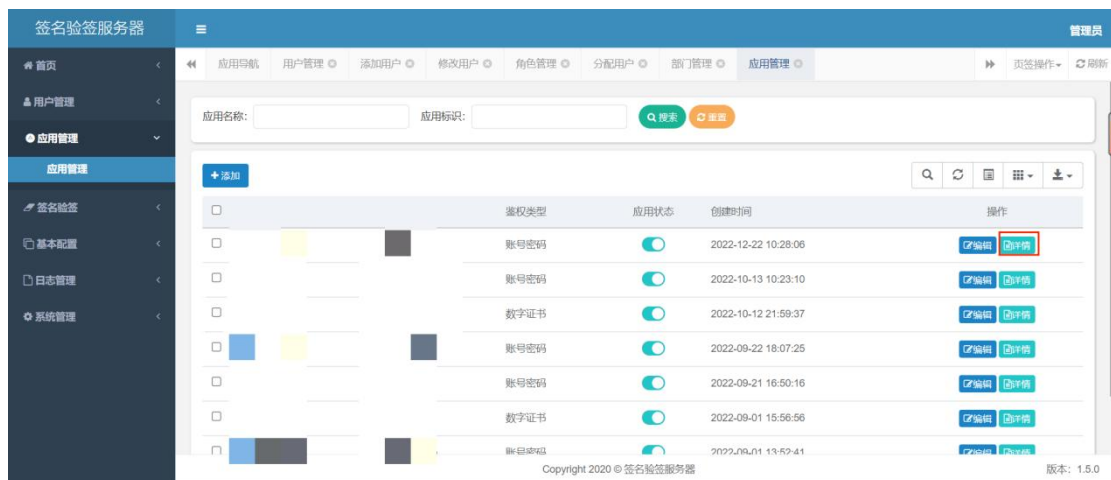
*鉴权方式:

*通信密码:

鉴权模块: ☐ 签名验签 ☐ 用户管理

IP白名单开关: ☐

5、点击详情，可以查看当前应用详细情况。



7 签名验签

7.1 容器管理

1、点击容器管理，可以看到当前系统下所有的容器列表。



2、点击添加，可以添加新的签名验签容器。



添加密钥容器

*容器名称:

*密钥算法:

*签名证书:

加密证书:

应用系统:

确定 关闭

1. 在添加密钥容器时，容器名称是随机生成的，但是也可以自己修改。
2. 密钥算法可以选择两种：RSA 算法和 SM2 算法。
3. 签名证书，签名证书主要是跟据你所选择的密钥算法，然后查找基本配置中密钥管理里对应算法的证书列表，选择你所需要的证书即可。
4. 加密证书，加密证书的选择与签名证书的选择方法一样，跟据对应的密钥算法选择自己所需要的证书。
5. 应用系统，应用系统所展示的是应用管理里添加的应用，添加你所需要的应用即可。

3、点击导入，可以批量导入容器并且申请证书。

签名验签服务器

应用管理 容器管理

容器名: 容器状态: 所有

☐	名	书CN	密钥算法	状态	操作
☐			RSA	☒	编辑 证书 删除
☐			RSA	☒	编辑 证书 删除
☐			RSA	☒	编辑 证书 删除

第 91 到 93 条, 共 93 条记录。 条记录每页

Copyright 2020 © 签名验签服务器 版本: 1.5.0

导入容器

*应用系统:

请选择

*密钥算法:

请选择

*签发CA:

请选择

*证书策略:

请选择

*有效期:

请选择

*批量文件:

上传文件

未选择任何文件

*批量模板:

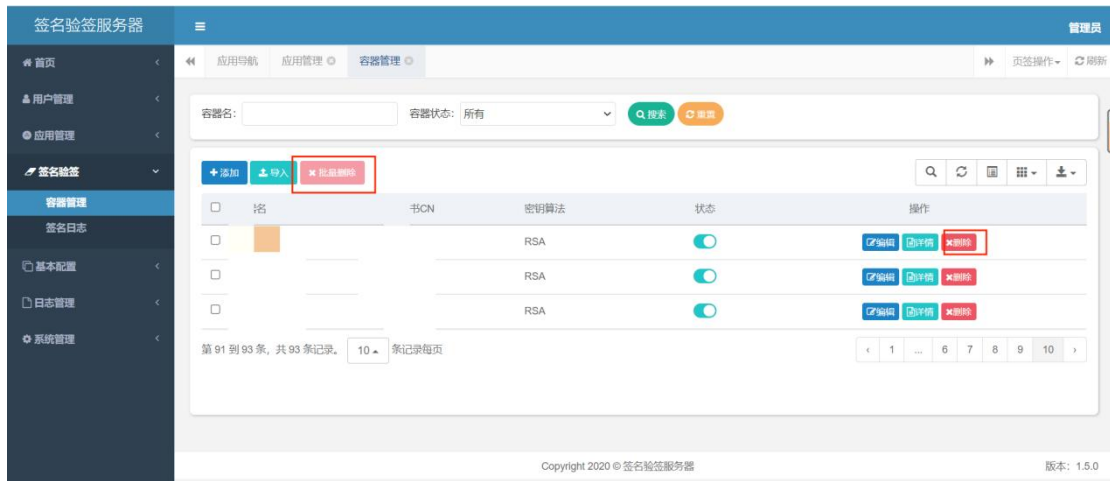
[下载模板](#)

确定

关闭

6. 应用系统：需要选择在应用系统里所添加的应用。
7. 密钥算法：密钥算法主要有 RSA 算法及 SM2 算法。
8. 签发 CA：需要选择基本配置里的 CA 信息配置中添加的 CA，申请证书的时候会到所添加的 CA 处申请证书。
9. 证书策略：证书策略选择的是在 CA 信息配置中的证书应用类型里配置的策略，且选择的策略密钥算法要与第二步选择的密钥算法保持一致。
10. 有效期：有效期主要与 CA 信息配置中的证书应用类型里配置的策略时添加，此处选择对应有效期即可。
11. 如果不知道批量导入的模板，选择下载模板即可得到批量导入模板。

4、点击批量删除或者删除，可以删除掉所选择的容器。



5、点击状态，可以选择关闭或启用容器。



6、点击编辑，可以对当前容器进行编辑修改。



修改密钥容器

*容器名称:

*密钥算法:

*签名证书:

加密证书:

应用系统:

确定

关闭

7、点击详情，可以查看当前容器详细情况。

签名验签服务器

应用管理

容器管理

容器名:

容器状态: 所有

搜索

新增

添加

导入

批量删除

Q

刷新

重置

导出

☐	名	书CN	密钥算法	状态	操作
☐			RSA	☒	编辑 详情 删除
☐			RSA	☒	编辑 详情 删除
☐			RSA	☒	编辑 详情 删除

第 91 到 93 条, 共 93 条记录。

10 条记录每页

<

1

...

6

7

8

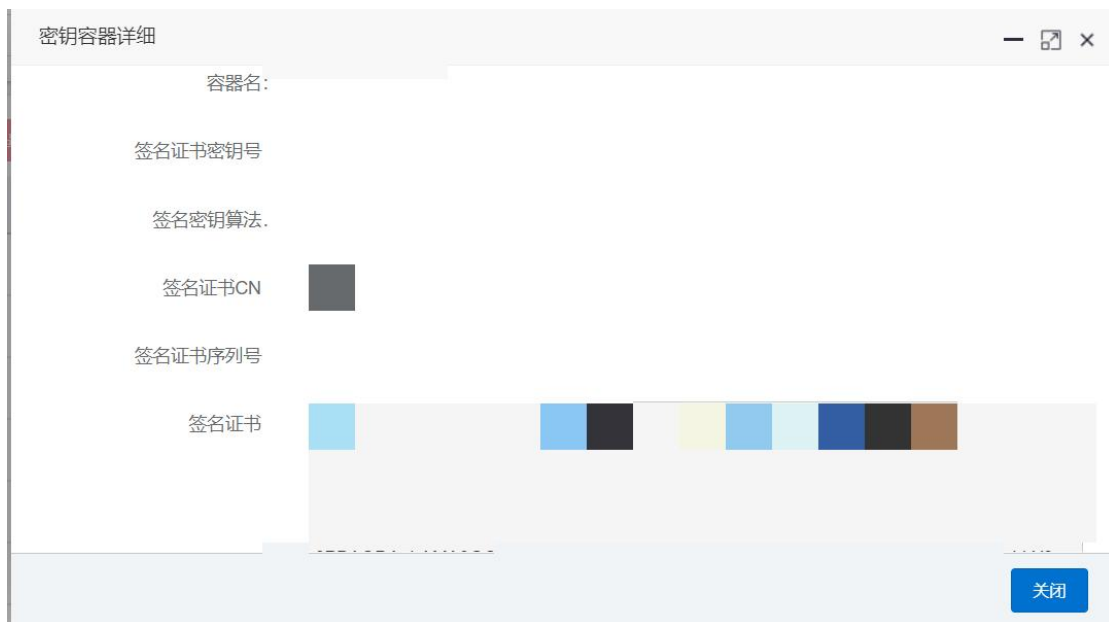
9

10

>

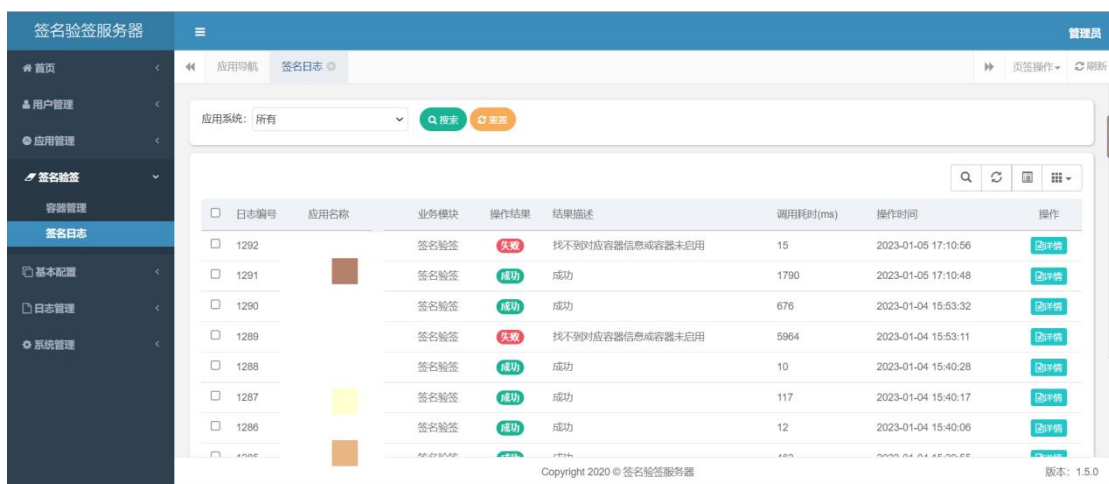
Copyright 2020 © 签名验签服务器

版本: 1.5.0

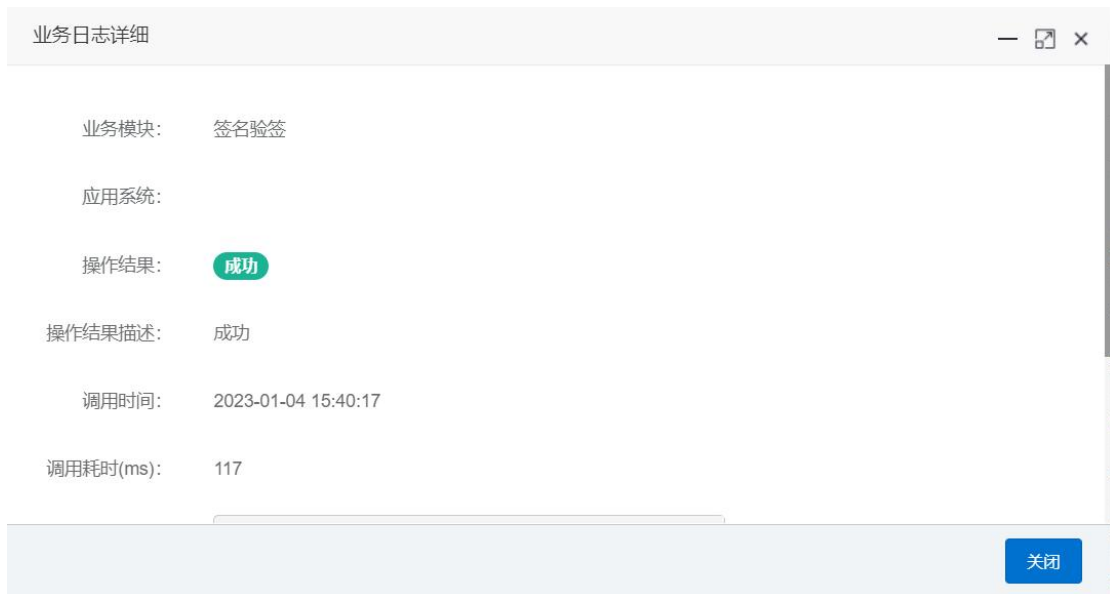


7.2 签名日志

- 1、点击签名日志，可以查看到当前系统下所有的签名验签日志记录。

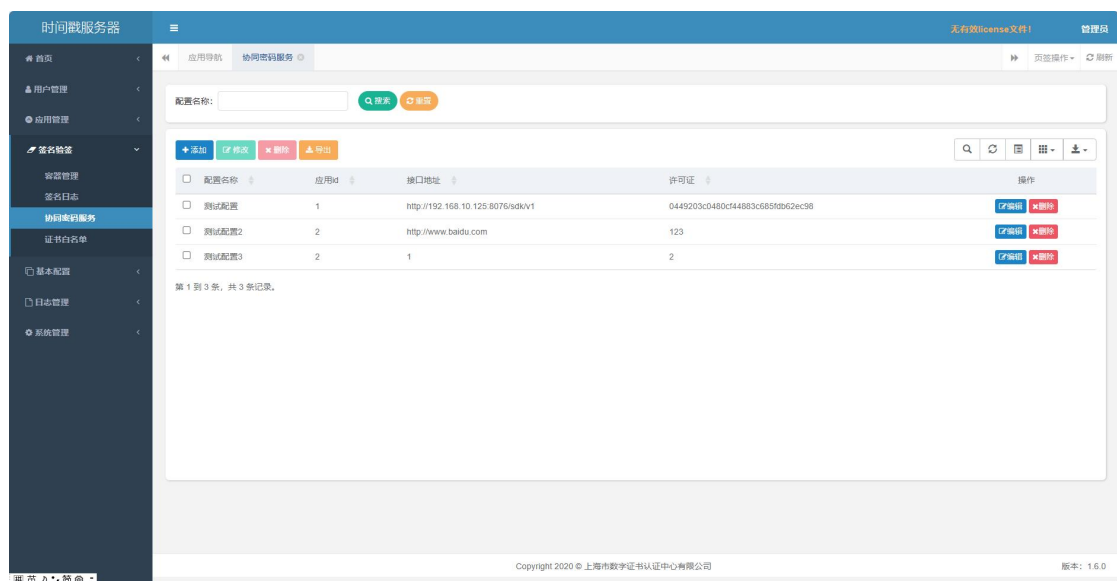


- 2、点击详细，可以查看当前记录的详细信息。



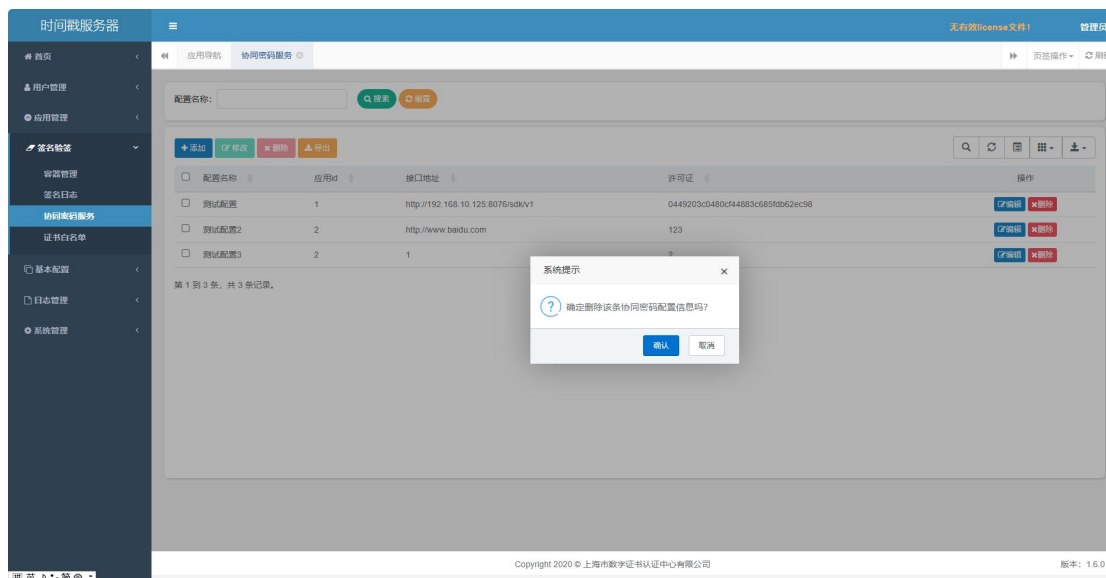
7.3 协同签名配置

1、点击协同密码服务即可查看当前系统所有的协同密码服务配置。



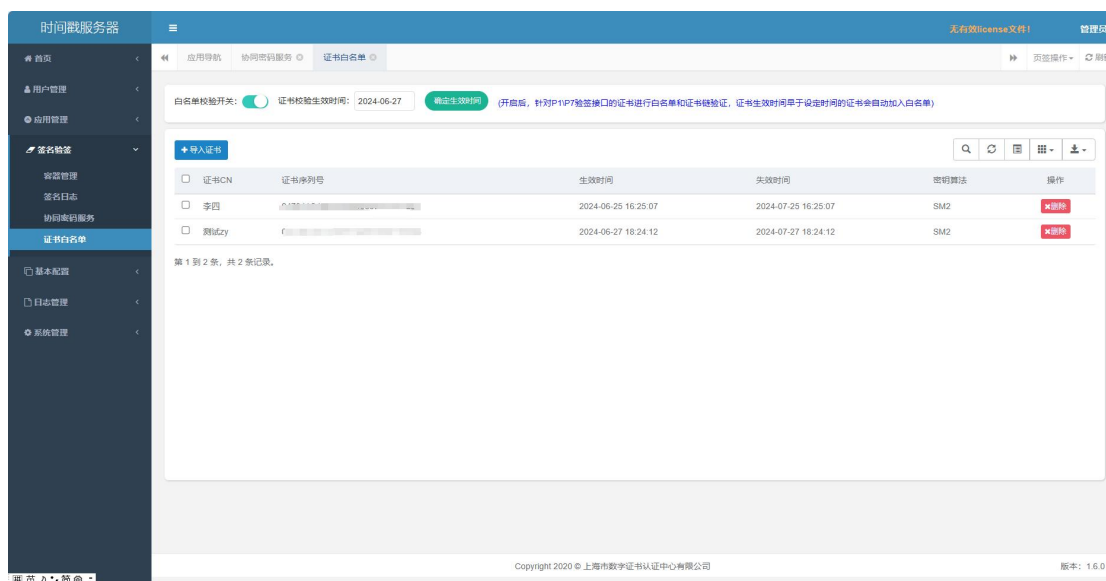
2、点击添加即可添加协同服务。配置名称可以自己指定，且不能重复。其余配置由对接方提供。



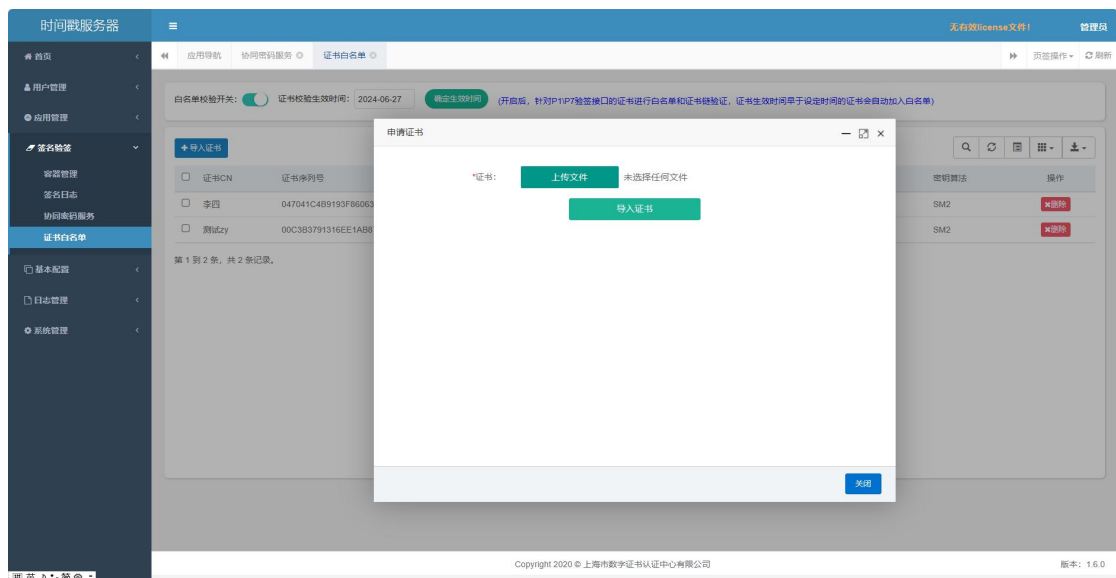


7.4 证书白名单配置

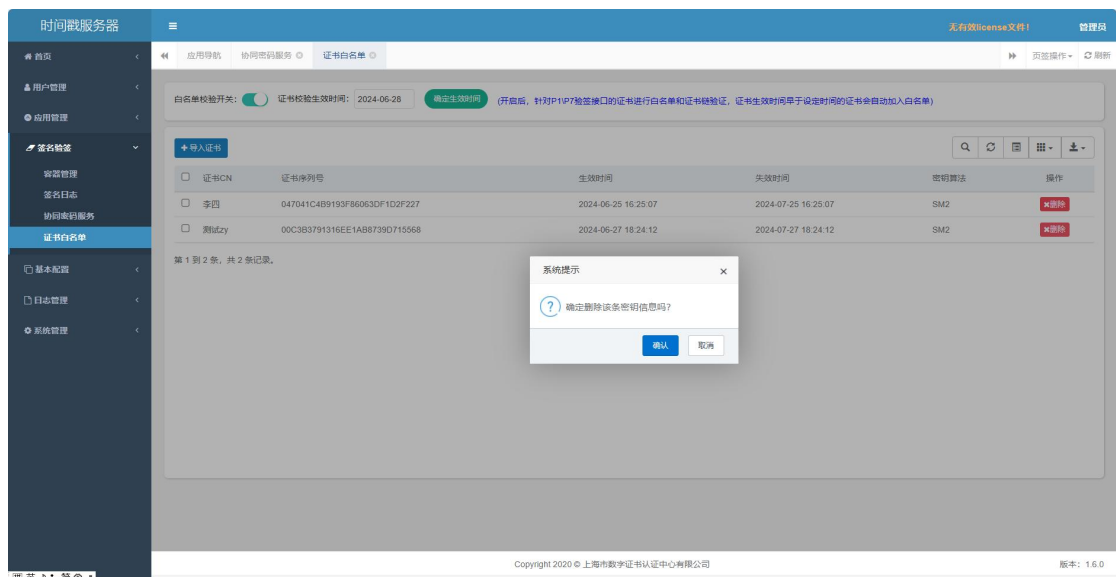
1、点击证书白名单配置即可显示当前系统所有的白名单证书。可以手动导入证书；开启白名单校验和确定证书校验生效时间后，针对 P1\P7 验签接口的证书进行白名单和证书链验证，证书生效时间早于设定时间的证书会自动加入白名单。



2、点击导入证书，则可以添加白名单证书。



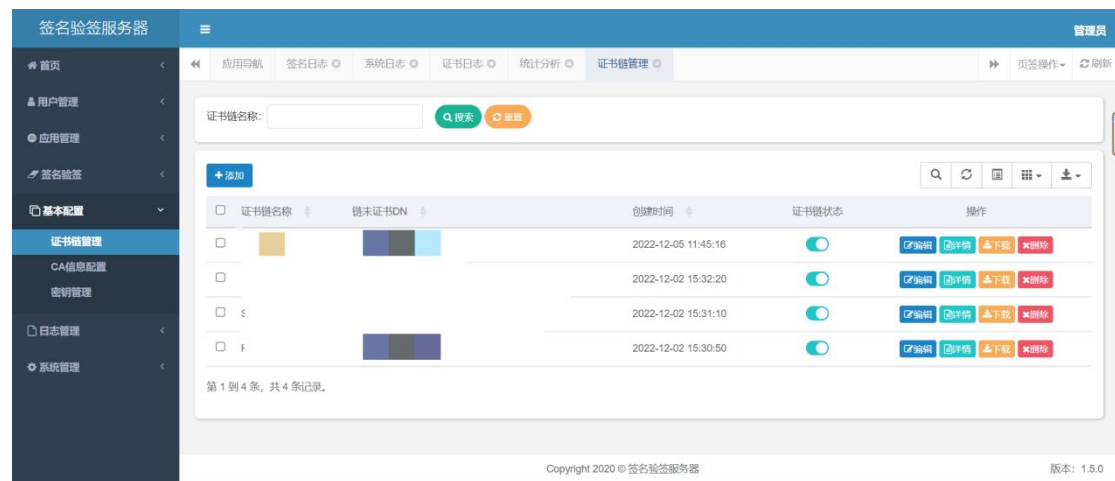
3、点击删除即可删除对应的白名单证书。



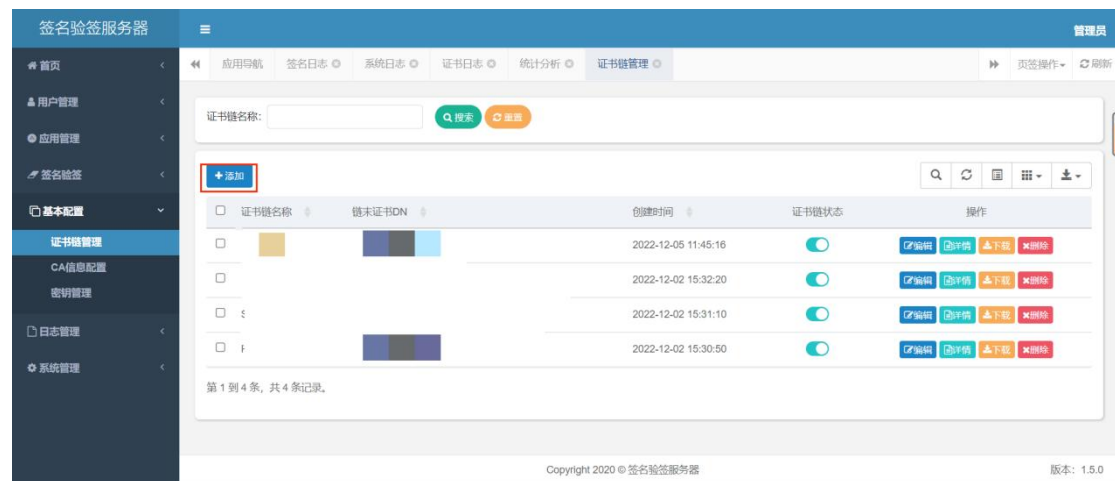
8 基本配置

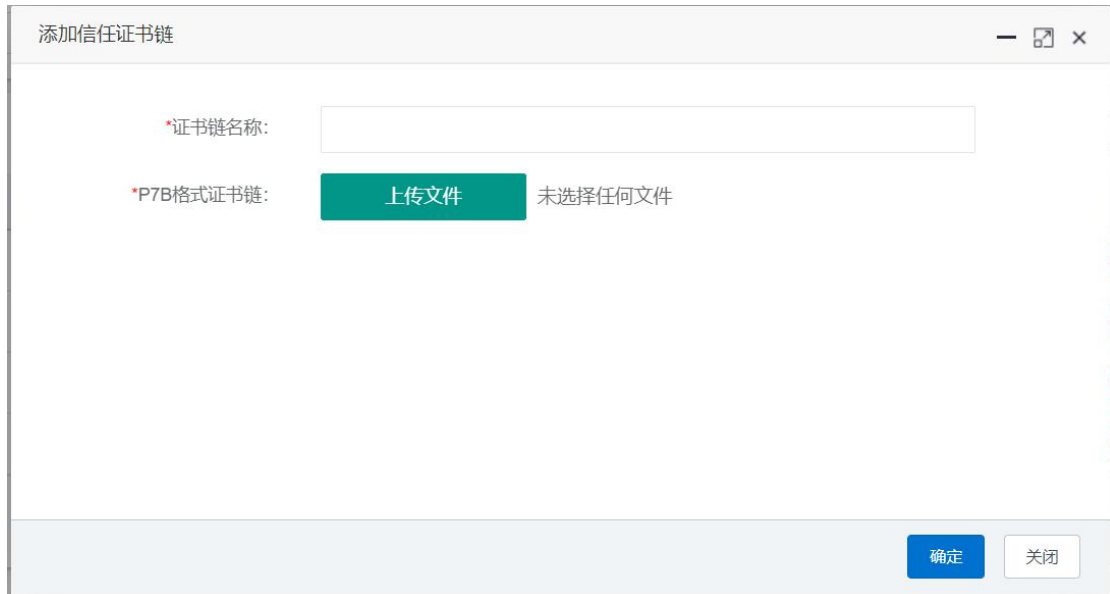
8.1 证书链管理

1、点击证书链管理，可以查看当前系统下添加的所有证书链。

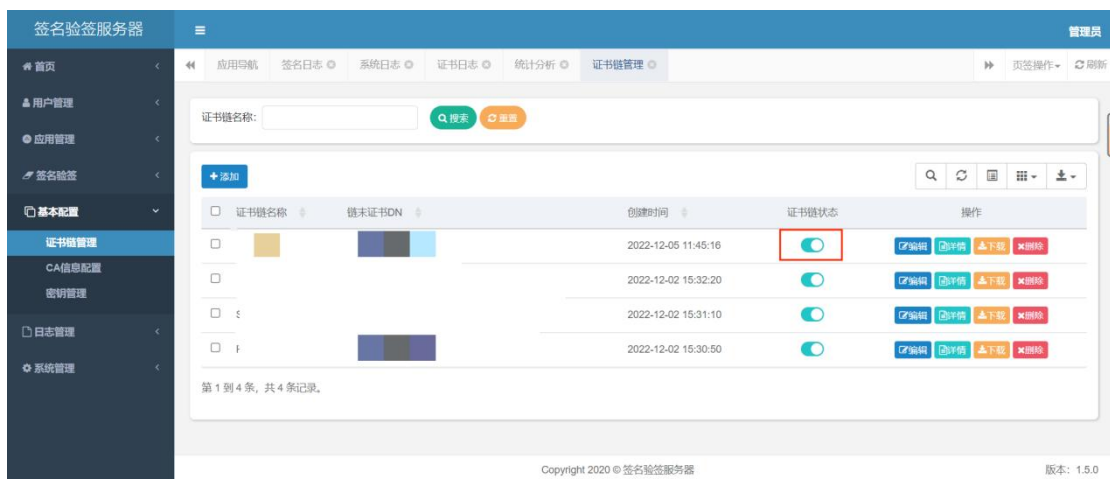


2、点击添加，可以添加新的证书链。

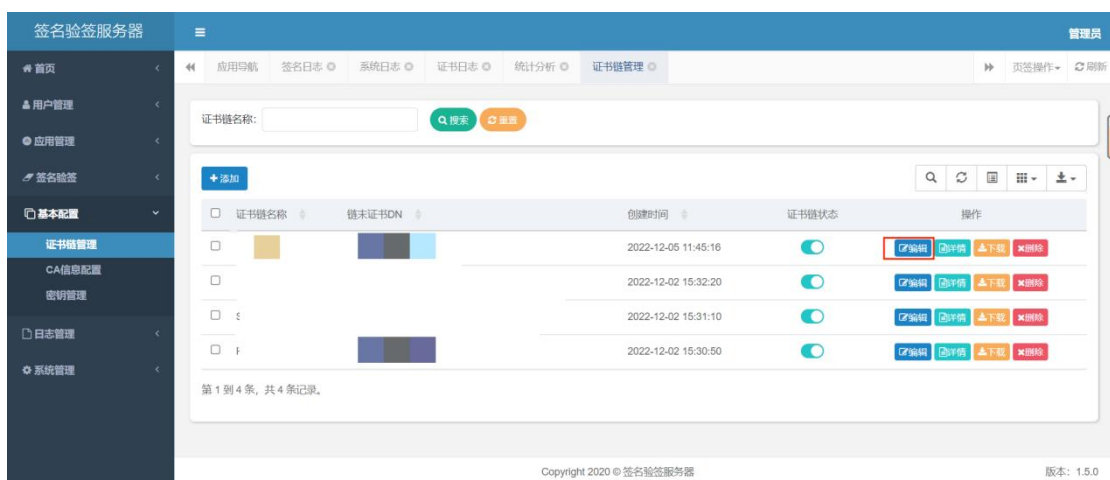




3、点击证书链状态，可以启用或者停用当前证书链。



4、点击编辑，可以对当前的证书链进行修改编辑。



修改信任证书链

*证书链名称:

p7b格式证书链:

上传文件

未选择任何文件

确定

关闭

5、点击详情，可以查看当前证书链的详细信息。

签名验签服务器

应用管理

用户管理

应用管理

签名验签

基本配置

证书链管理

CA信息配置

密钥管理

日志管理

系统管理

应用管理

签名日志

系统日志

证书日志

统计分析

证书链管理

证书链名称:

搜索

重置

+ 添加

证书链名称

链末证书DN

创建时间

证书链状态

操作

☐			2022-12-05 11:45:16	☒	编辑 详情 下载 删除
☐			2022-12-02 15:32:20	☒	编辑 详情 下载 删除
☐			2022-12-02 15:31:10	☒	编辑 详情 下载 删除
☐			2022-12-02 15:30:50	☒	编辑 详情 下载 删除

第 1 到 4 条, 共 4 条记录。

Copyright 2020 © 签名验签服务器

版本: 1.5.0

信任证书链详细

证书链id:

证书链名称:

链末证书DN:

证书链状态:

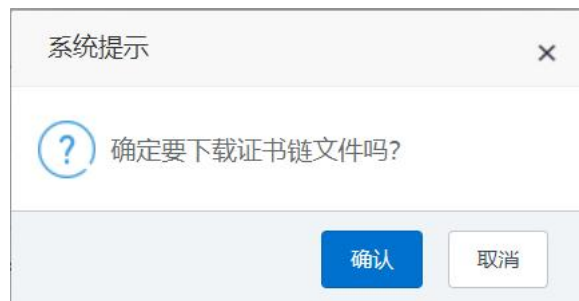
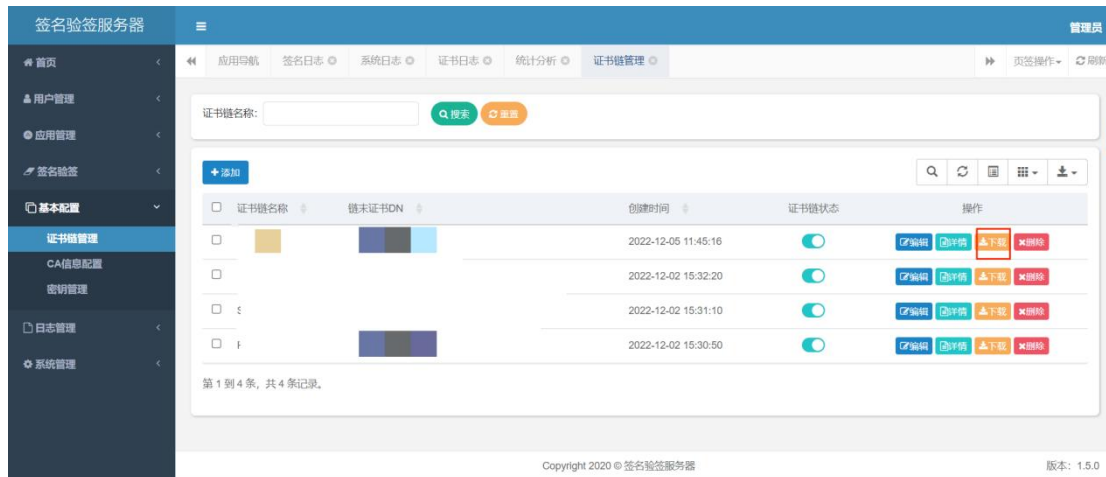
启用

创建时间:

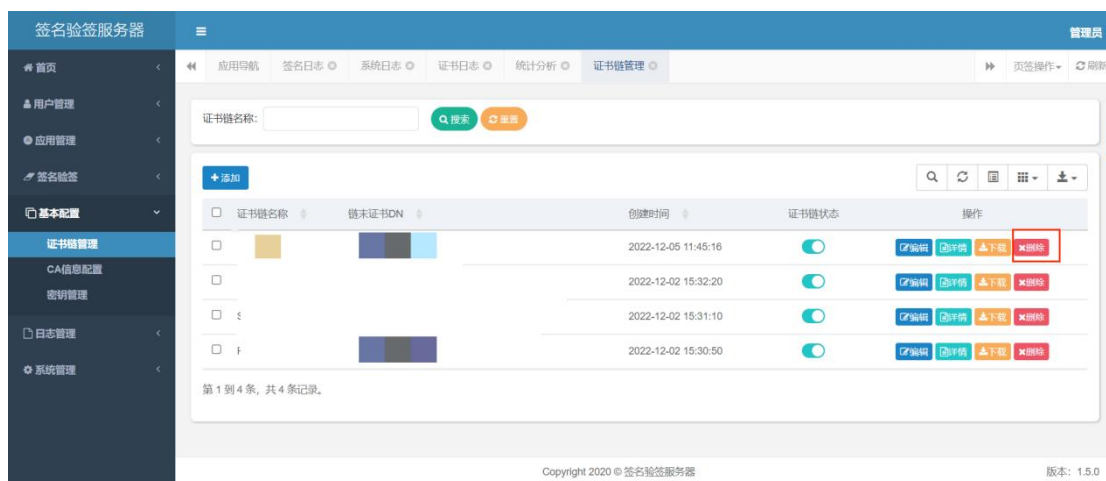
2022-12-05 11:45:16

关闭

6、点击下载，可以下载当前的证书链。

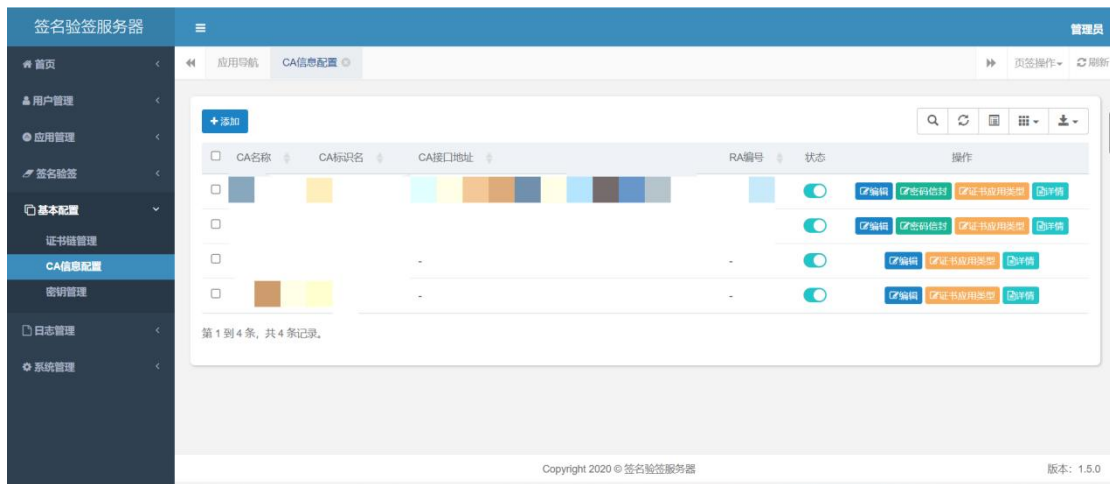


7、点击删除，可以删除当前的证书链。

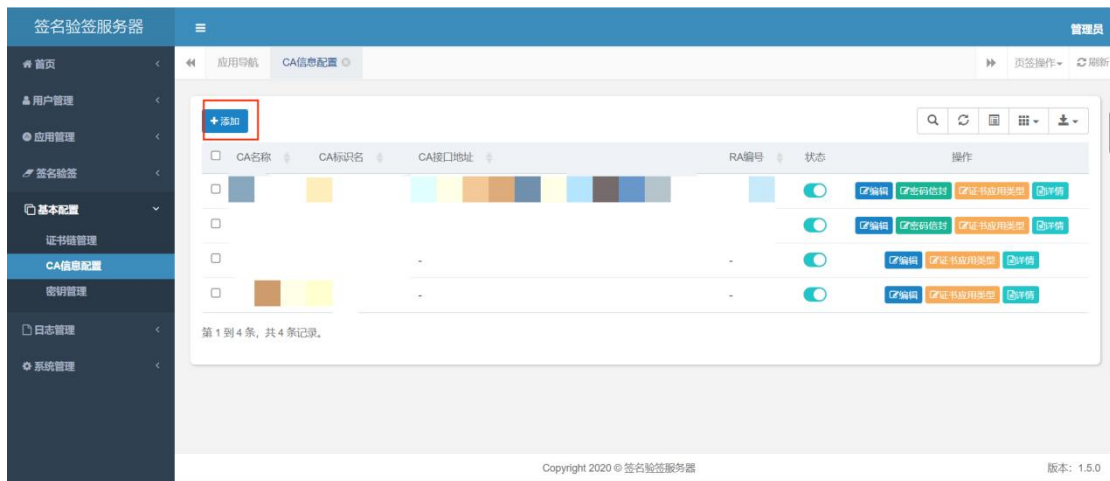


8.2 CA 信息配置

1、点击 CA 信息配置，可以查看当前系统下配置的所有 CA 列表。



2、点击添加，可以添加新的 CA。



添加CA配置

CA信息

*CA标识名: 内部CA

*CA名称:

*密钥算法: 请选择

*密钥长度: 请选择

*名称 (CN) :

单位 (O) :

确定 关闭

添加CA配置

CA信息

*CA标识名:

*CA名称:

*CA接口地址:

应用标识:

应用密码:

是否添加密码信封:

☒

*CA通讯证书:

上传文件

未选择任何文件

RA信息

*RA编号:

*RA证书:

上传文件

未选择任何文件

*RA证书密码:

确定

关闭

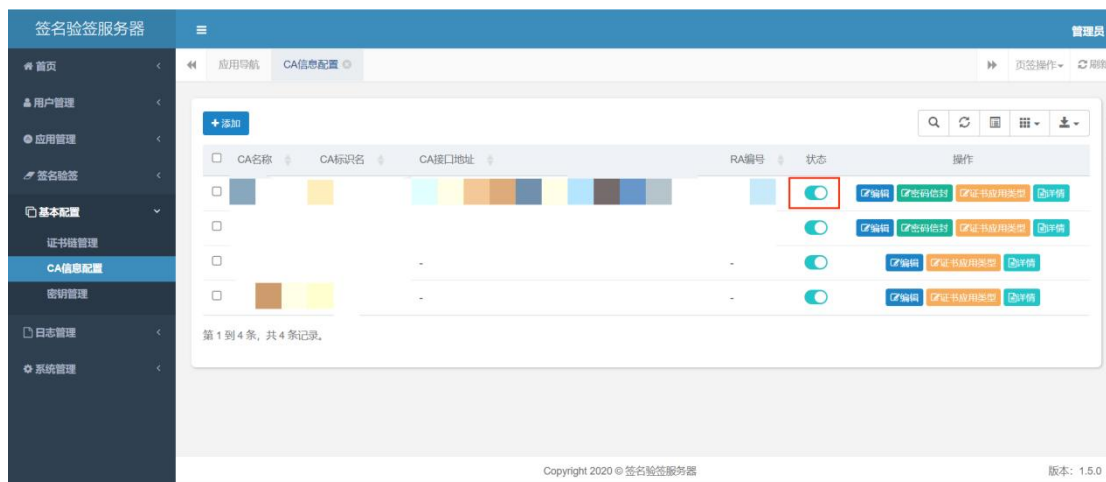
添加新的 CA 信息时，在第一步选择 CA 标识名时：

1. 选择内部 CA:当选择的 CA 标识名是内部 CA 时，必填项为 CA 名称、密钥算法、密钥长度、名称等即可，其中密钥算法中选择 RSA 算法时，其对应的密钥长度有 1024 及 2048 两个选项。当选择 SM2 算法时，密钥长度只有 256 一个选项。

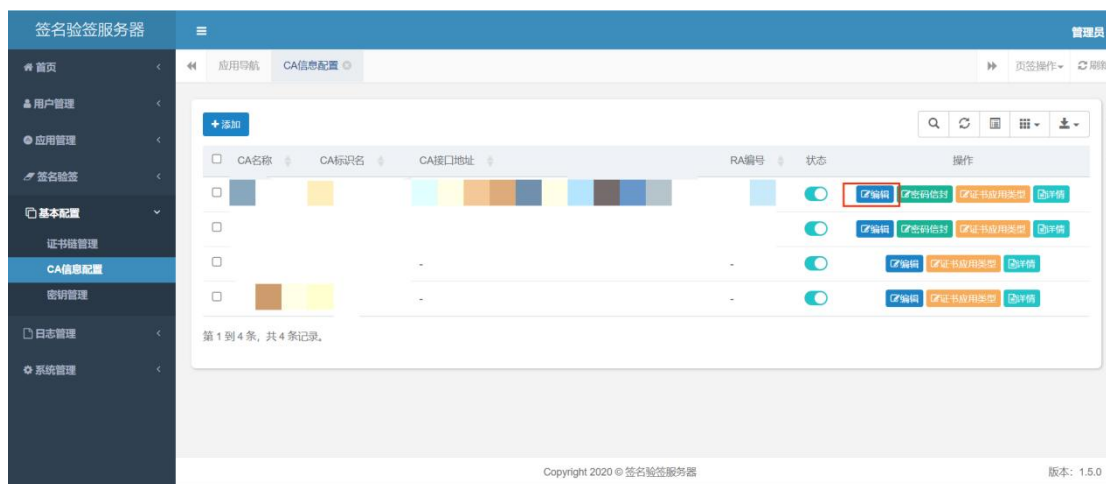
2. 选择其他 CA 时：

当 CA 标识名选择除了内部 CA 以外的标识名时，必填项有 CA 名称、CA 的接口地址、该 CA 的通讯证书、RA 编号、RA 证书、RA 的证书密码。其中 CA 通讯证书的格式是以以.cer 格式的证书，而 RA 证书是以.p12 格式的证书。

3、点击状态，可以启用或者关闭当前 CA。



4、点击编辑，可以对当前 CA 进行编辑。



修改CA配置

CA信息

CA标识名:

CA名称:

CA接口地址:

是否添加密码信封:

通讯证书:

上传文件

未选择任何文件

RA信息

RA编号:

RA证书:

上传文件

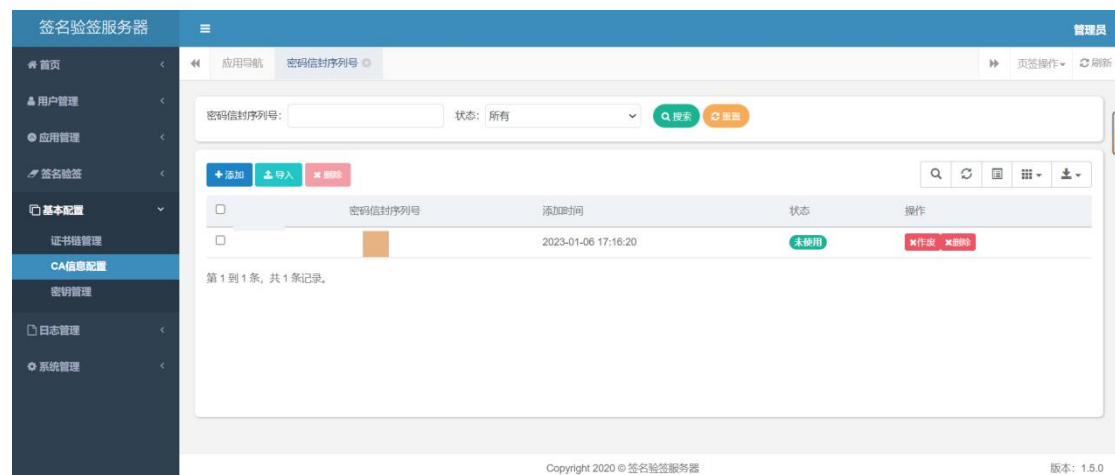
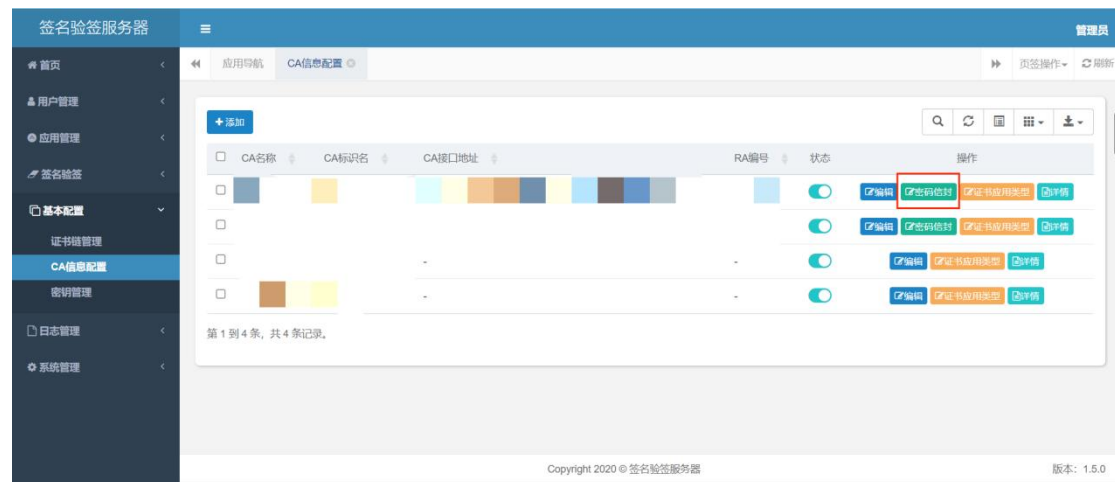
未选择任何文件

RA证书密码:

确定

关闭

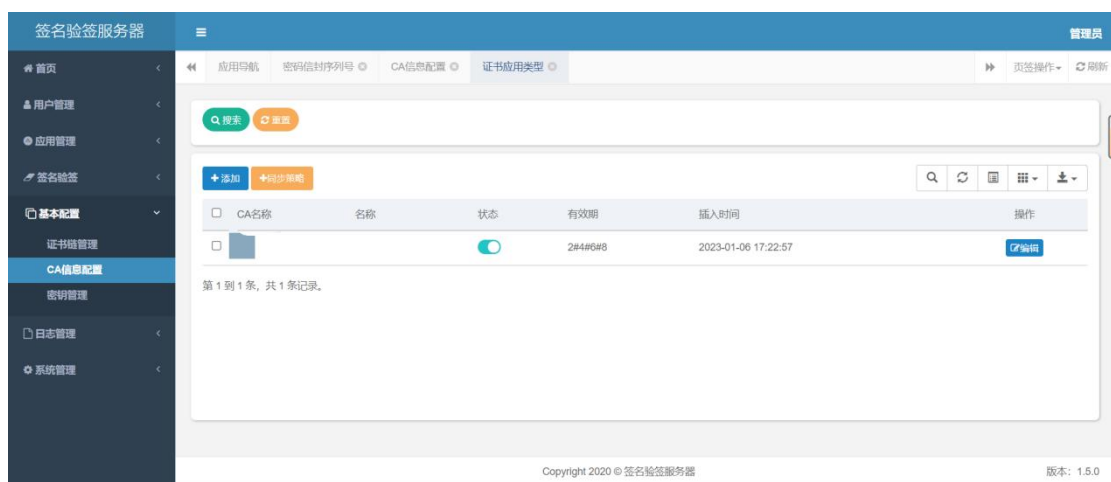
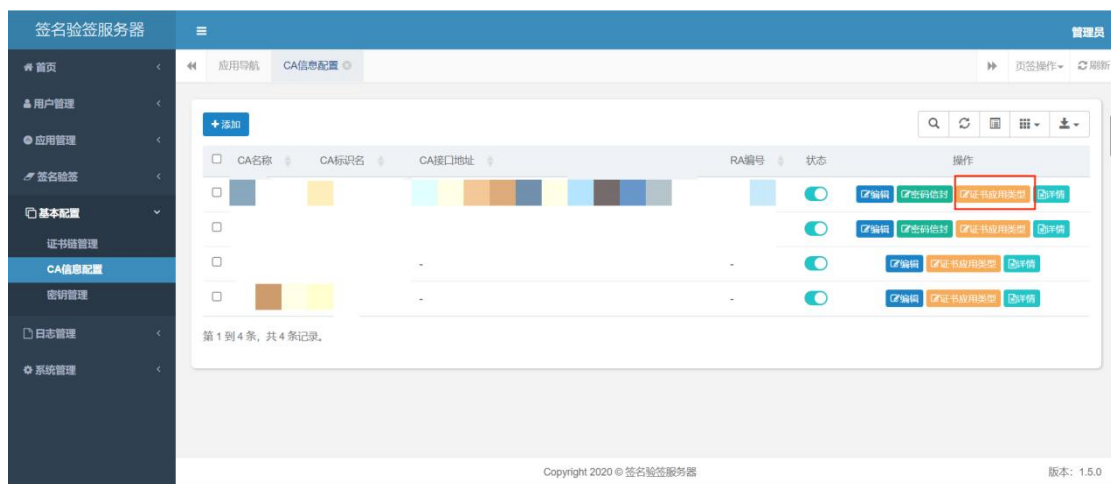
5、点击密码信封，可以进入当前 CA 的密码信封列表。



在密码信封列表中：

1. 点击添加，可以添加新的密码信封序列号。
2. 点击导入，可以批量导入密码信封序列号。
3. 点击删除，可以进行删除或者批量删除操作。
4. 点击作废，可以作废当前密码信封序列号。

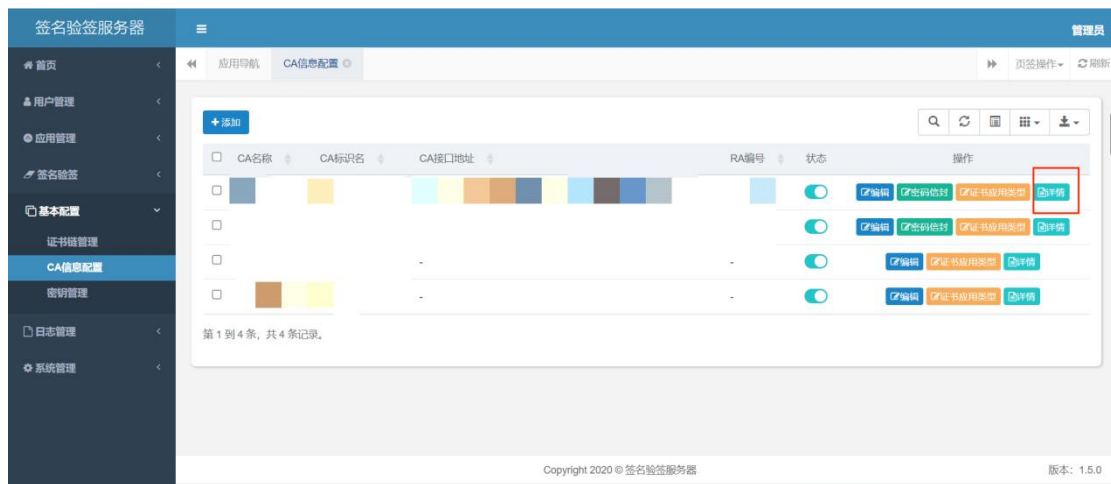
6、点击证书应用类型，可以进入当前 CA 的证书应用类型列表。



在证书应用类型列表中：

1. 点击添加，可以配置新的策略。
2. 点击同步策略，可以同步该 CA 的所有策略到当前列表。
3. 点击状态，可以启用或者停用当前策略。
4. 点击编辑，可以编辑修改当前策略。

7、点击详情，可以查看当前 CA 的详细信息。



CA配置详细

CA标识名:

CA名称:

CA接口地址:

状态: 启用

证书主题:

RA证书密码:

通讯证书:

关闭

8.3 密钥管理

- 1、点击密钥管理，可以查看当前系统下的所有密钥信息列表。

签名验签服务器

应用导航 密码信封序列号 CA信息配置 证书应用类型 密钥管理 页签操作 刷新

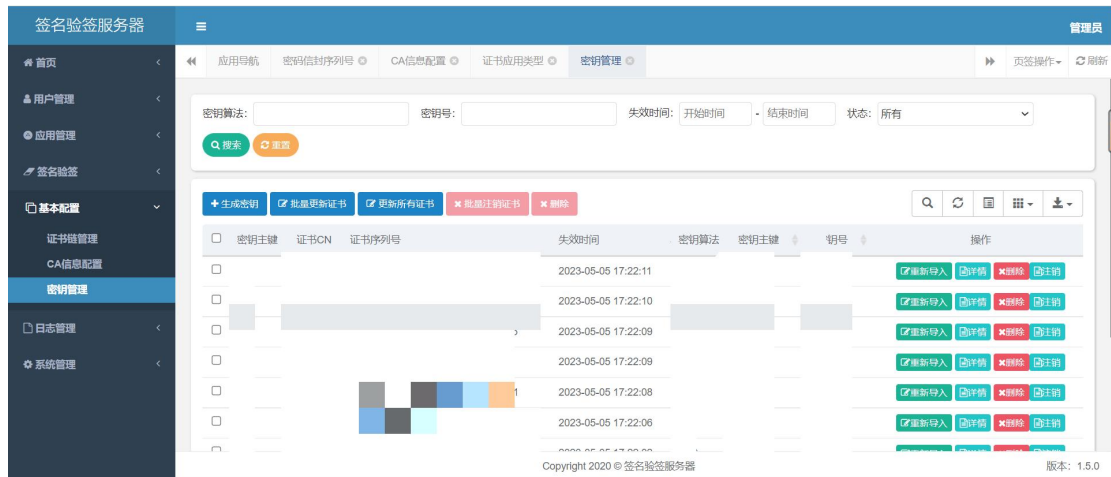
密钥算法: 密钥号: 失效时间: 开始时间 结束时间 状态: 所有

生成密钥 批量更新证书 更新所有证书 批量注销证书 删除

☐	密钥主键	证书CN	证书序列号	失效时间	密钥算法	密钥主键	密钥号	操作
☐				2023-05-05 17:22:11				重新导入 评估 删除 注销
☐				2023-05-05 17:22:10				重新导入 评估 删除 注销
☐				2023-05-05 17:22:09				重新导入 评估 删除 注销
☐				2023-05-05 17:22:09				重新导入 评估 删除 注销
☐				2023-05-05 17:22:08				重新导入 评估 删除 注销
☐				2023-05-05 17:22:06				重新导入 评估 删除 注销
☐				2023-05-05 17:22:05				重新导入 评估 删除 注销

Copyright 2020 © 签名验签服务器 版本: 1.5.0

- 2、点击生成密钥，可以生成新的密钥。



添加密钥

步骤1: 输入密钥信息

* 密钥算法:

请选择

* 密钥长度:

请选择

* 签名算法:

请选择

* 密钥号:

步骤2: 输入证书请求信息

* 名称 (CN):

单位 (O):

部门 (OU):

省份 (ST):

城市 (L):

EMAIL:

生成

43

步骤3: 保存证书请求文件

证书主题:

签名算法:

证书请求文件编码:

保存

步骤4: 申请证书

申请方式:

外部导入

* 证书文件:

上传文件

未选择任何文件

外部导入

关闭

添加密钥

— □ ×

步骤4: 申请证书

申请方式:

内部申请

* 签发CA:

请选择

* 证书策略:

请选择

* 有效期:

请选择

内部申请

关闭

添加密钥时，总共经过四个步骤：

步骤 1：输入密钥信息

1. 密钥算法：可以选择 RSA 算法和 SM2 算法。
2. 密钥长度：RSA 算法对应的密钥长度是 1024 和 2048，SM2 对应的密钥长度是 256。
3. 签名算法：RSA 算法对应的签名算法是 SHA256withRSA, SM2 算法对应的签名算法是 SM3withSM2。
4. 密钥号：密钥号可以自增长，也可以自己选择密钥号。

步骤 2：输入证书请求信息，步骤 2 只有一个必填项，输入名称即可，其余选项看情况输入。

步骤 3：保存证书请求文件。

步骤 4：申请证书。

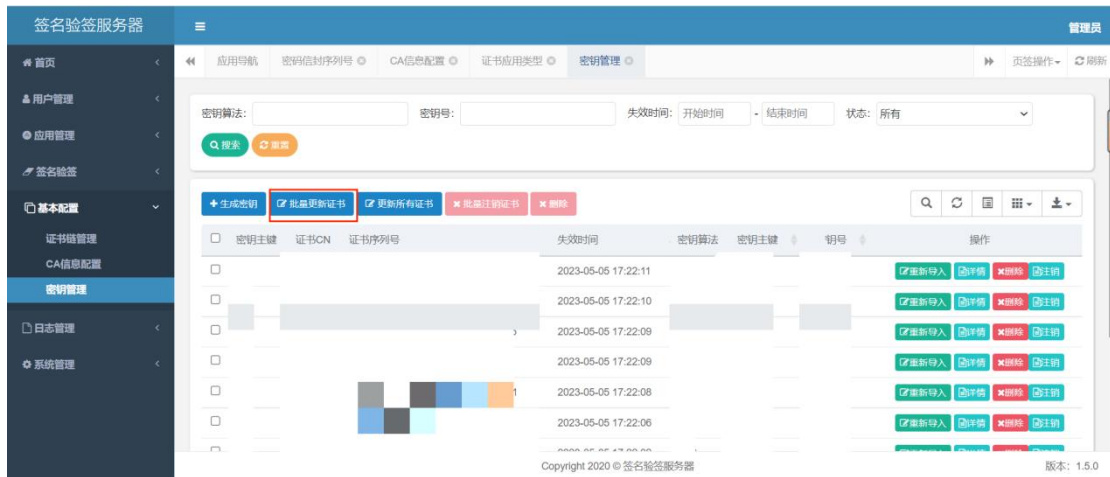
1. 申请方式：外部导入

申请方式选择外部导入时，需要跟据证书请求文件去申请.cer 格式的证书，然后导入。

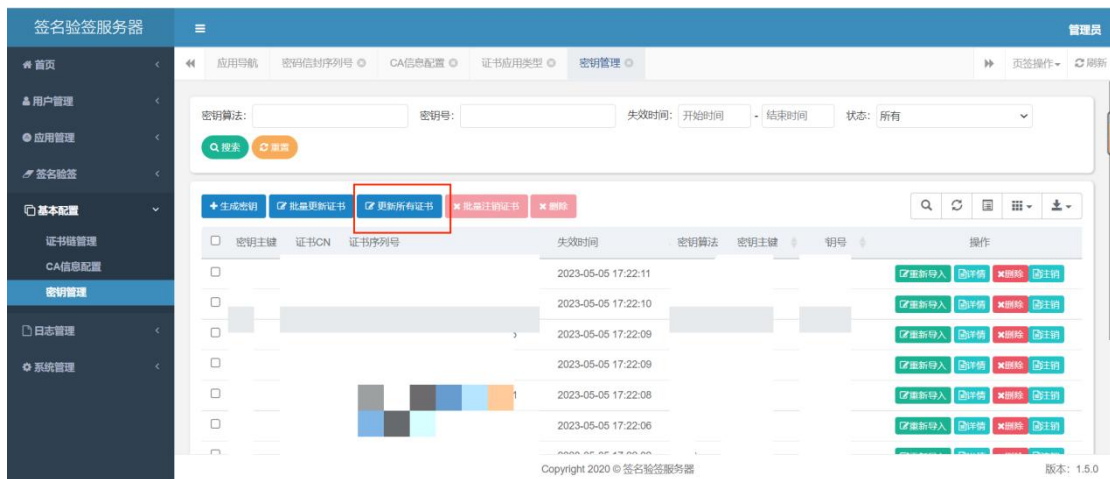
2. 申请方式：内部申请

申请方式是内部申请时，需要在 CA 信息配置模块先配置一个 CA,然后配置证书应用类型策略。如果该 CA 需要用到密码信封，也要配置密码信封序列号。

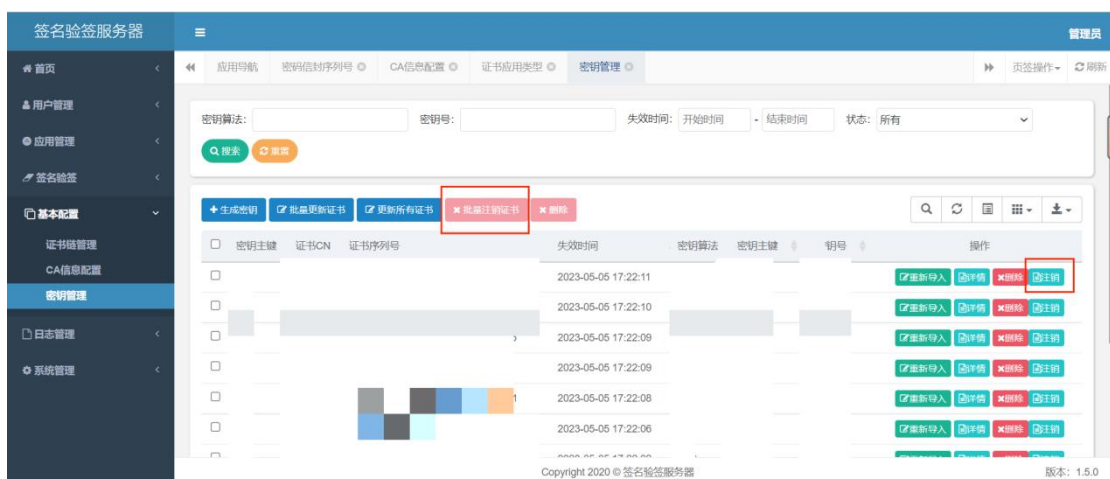
3、点击批量更新证书，可以跟据到期时间配置更新所选择的符合要求的证书。



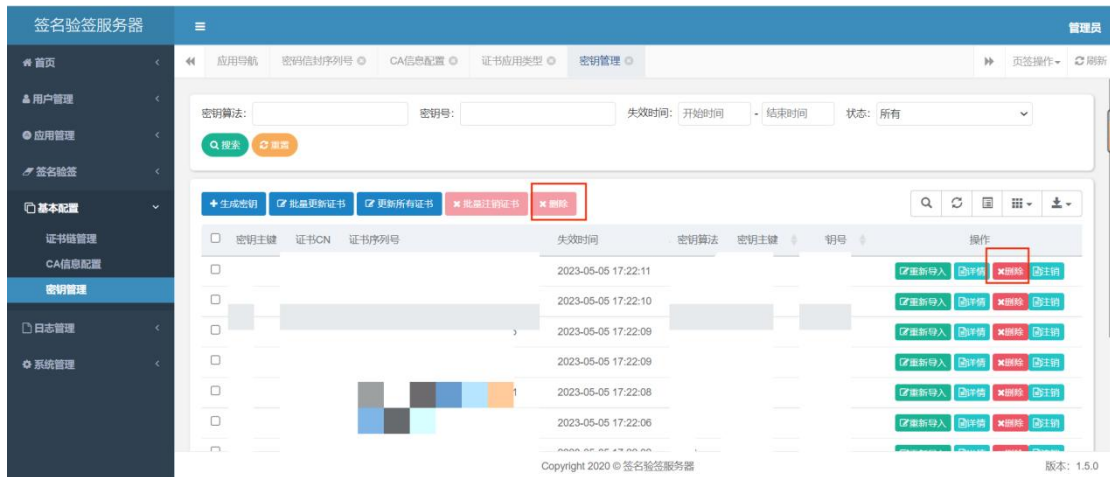
4、点击更新所有证书，可以对所有符合要求的证书进行更新。



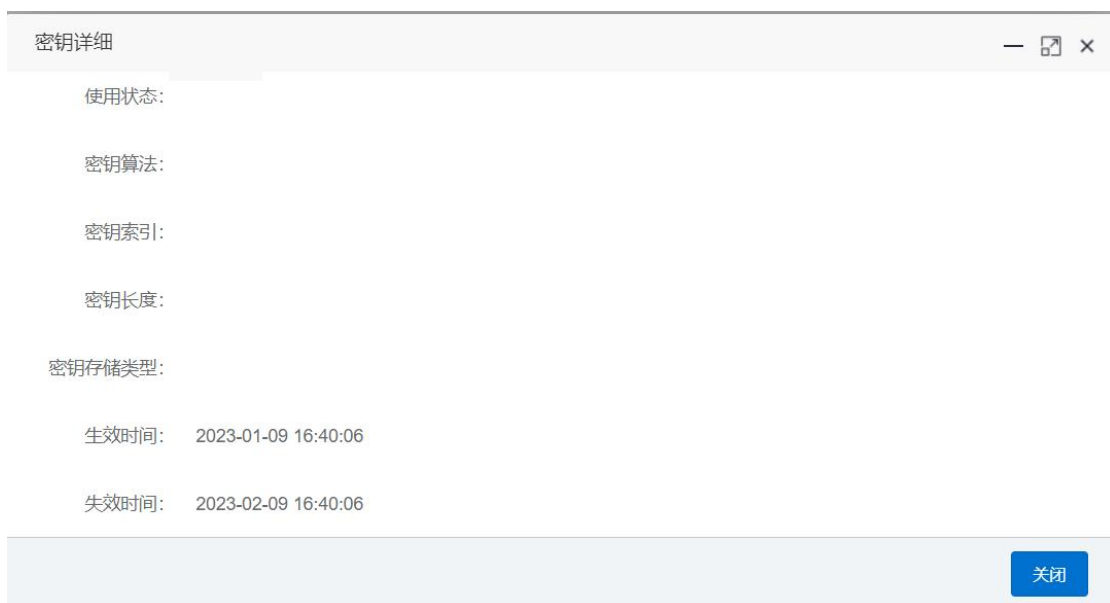
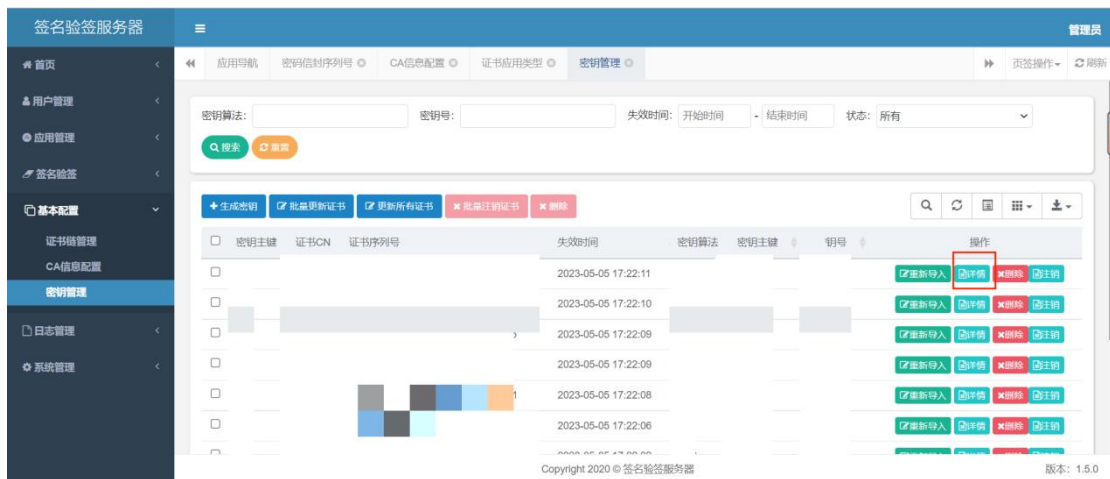
5、点击批量注销证书或注销，可以注销所选择的密钥。



6、点击删除，可以选择删除所选择的密钥。



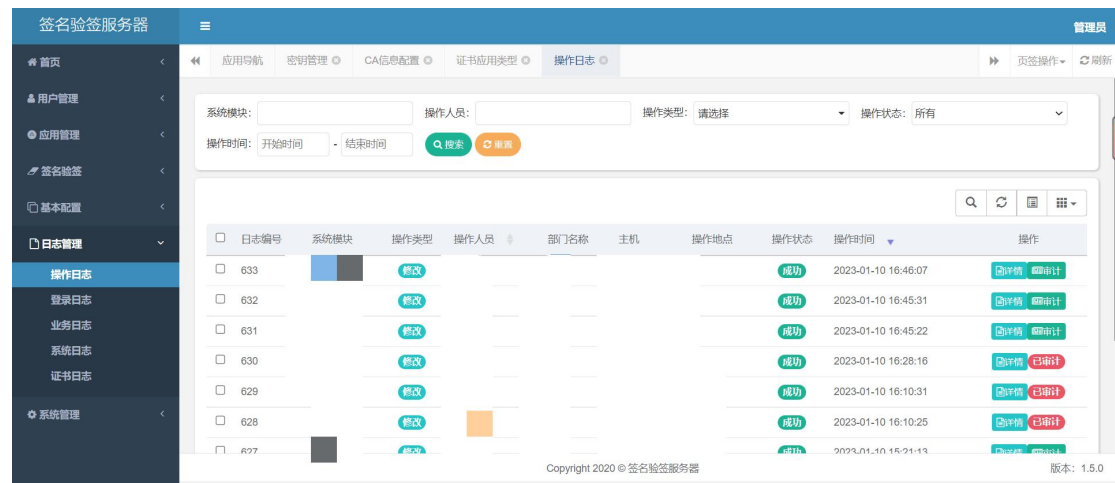
7、点击详情，可以查看当前密钥的详细信息。



9 日志管理

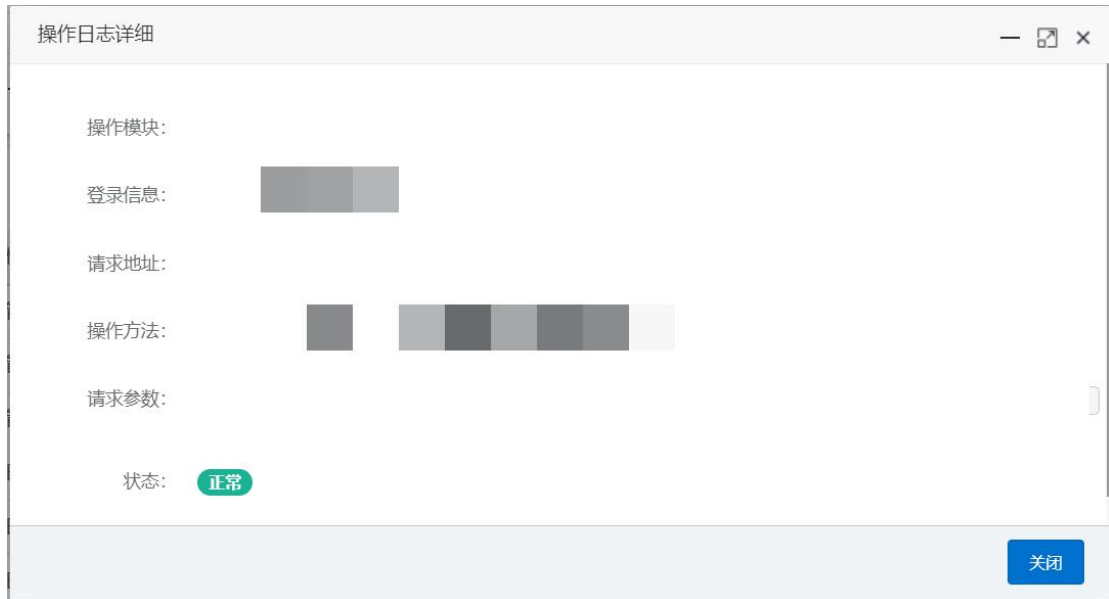
9.1 操作日志

1、点击操作日志，可以看到当前系统下所有操作日志列表。

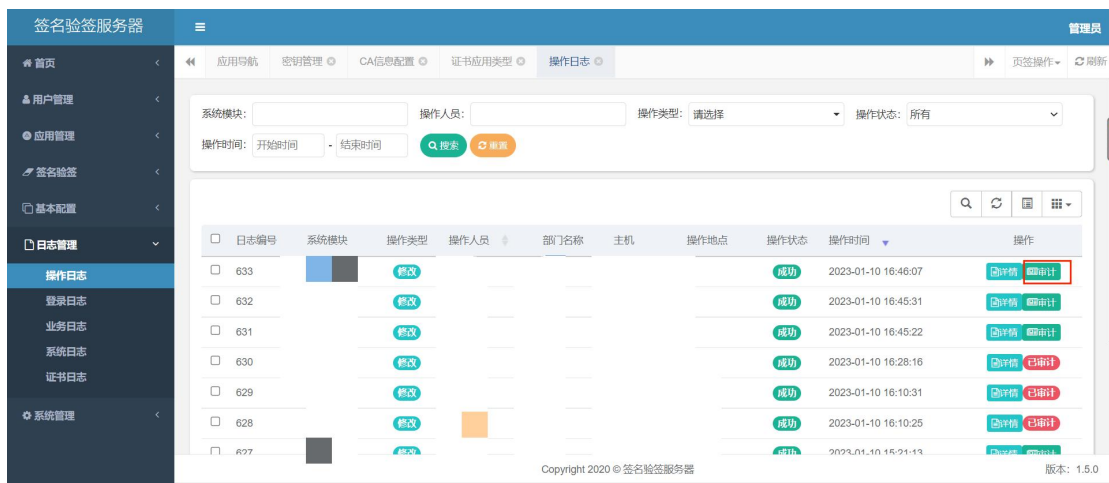


2、点击详情，可以看到当前日志的详细情况。



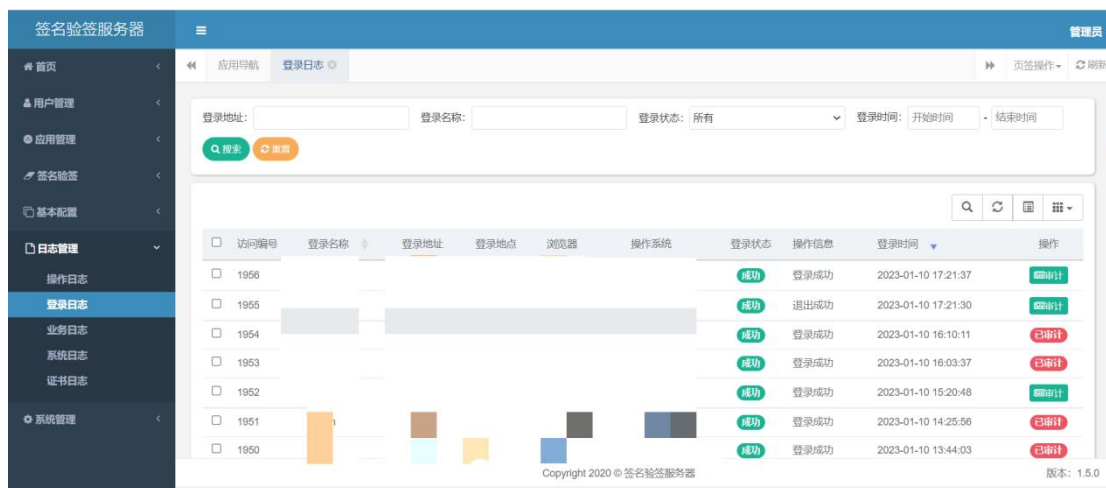


3、点击审计，可以对当前日志进行审计。

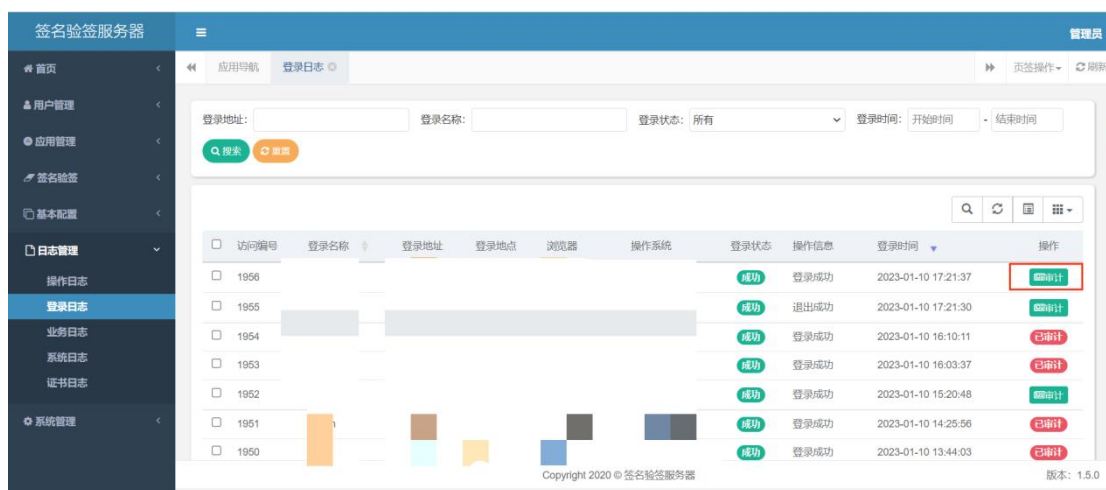


9.2 登录日志

1、点击登录日志，可以看到当前系统下所有的登录日志列表。

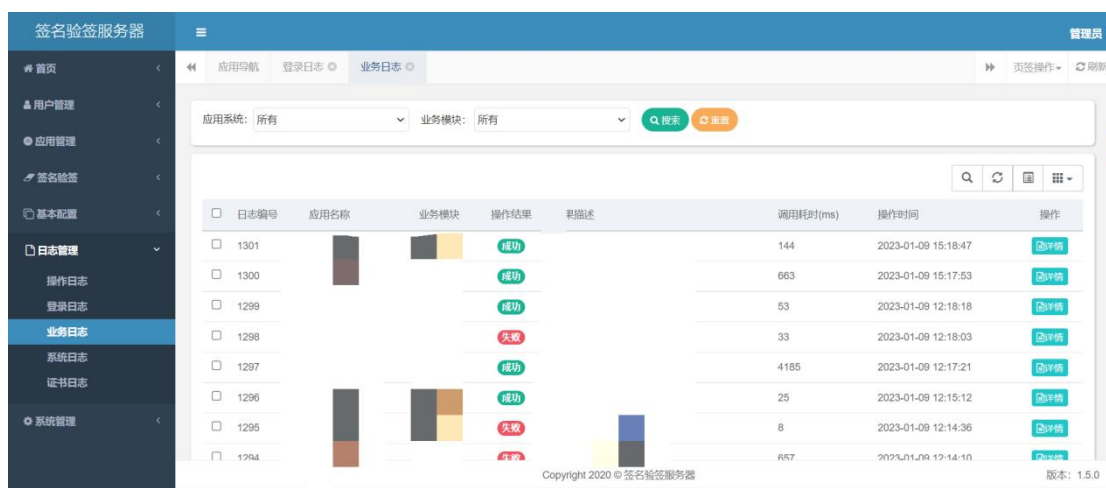


2、点击审计，可以对当前日志进行审计。

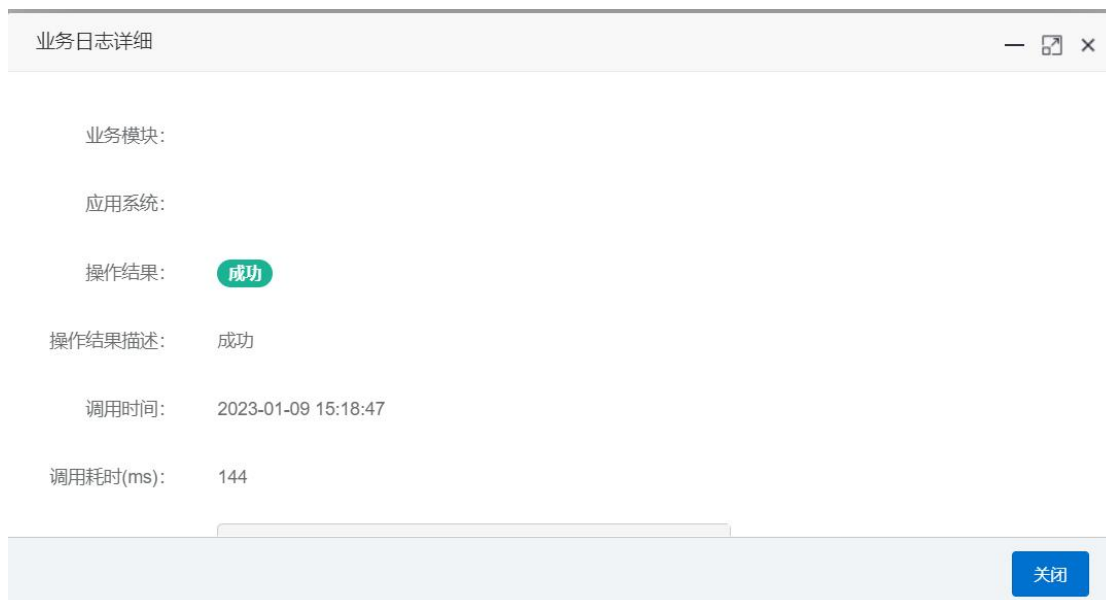
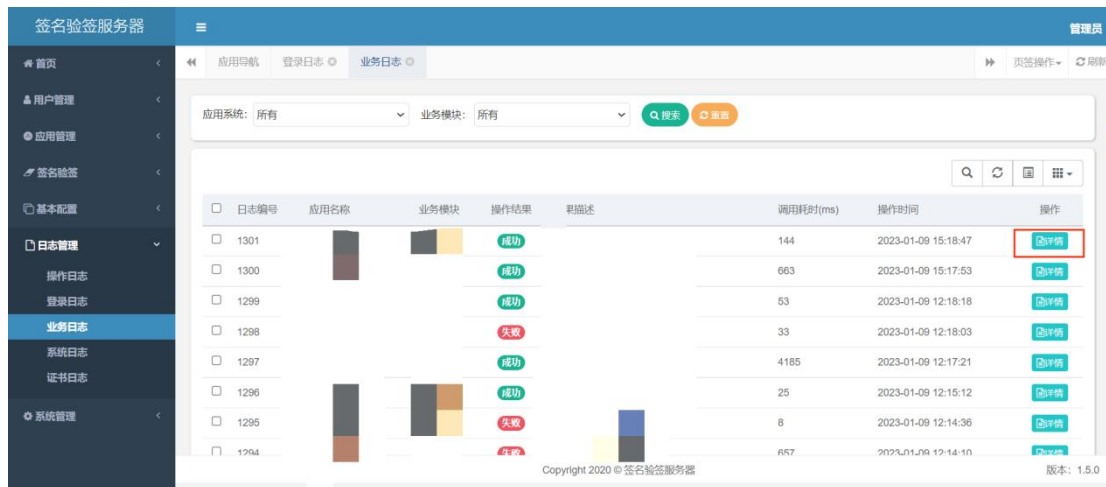


9.3 业务日志

1、点击业务日志，可以看到当前系统下业务日志列表。

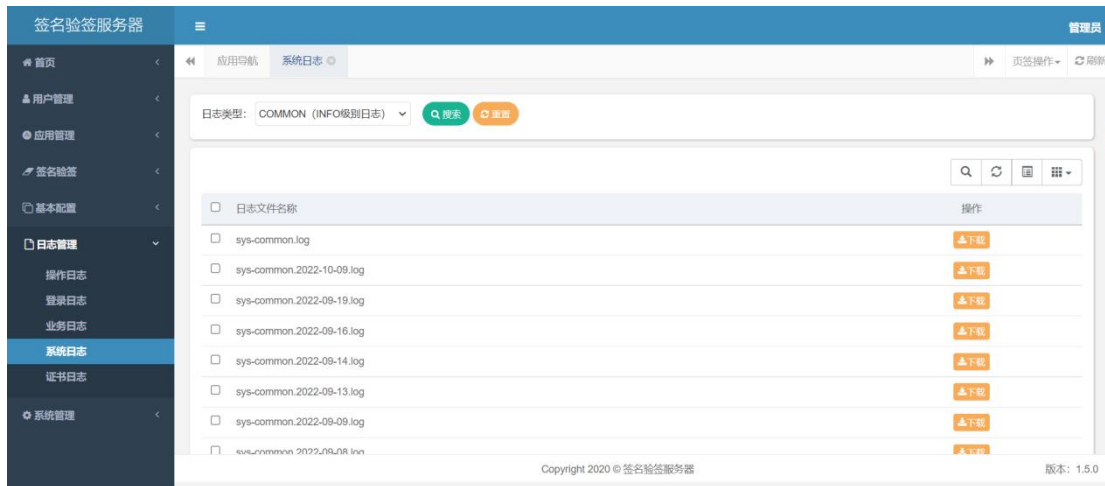


2、点击详细，可以看到当前业务日志详细。

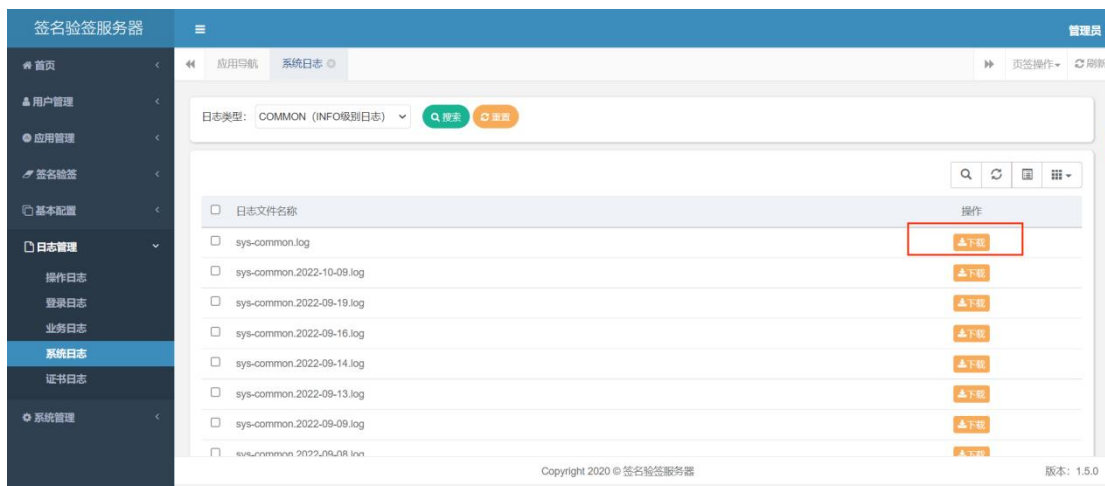


9.4 系统日志

1、点击系统日志，可以看到当前系统下系统日志列表。

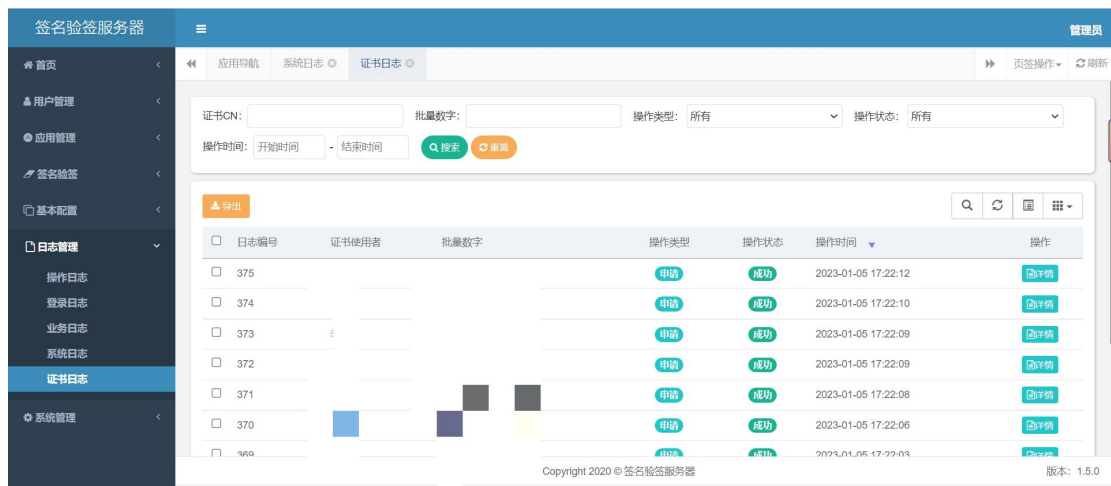


2、点击下载，可以下载当前系统日志。

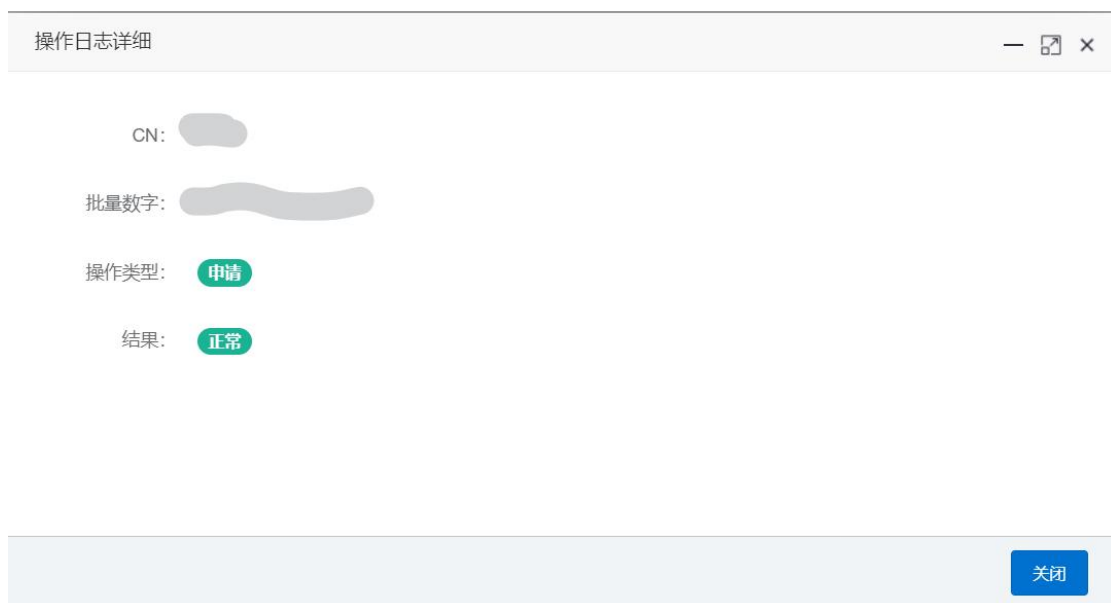
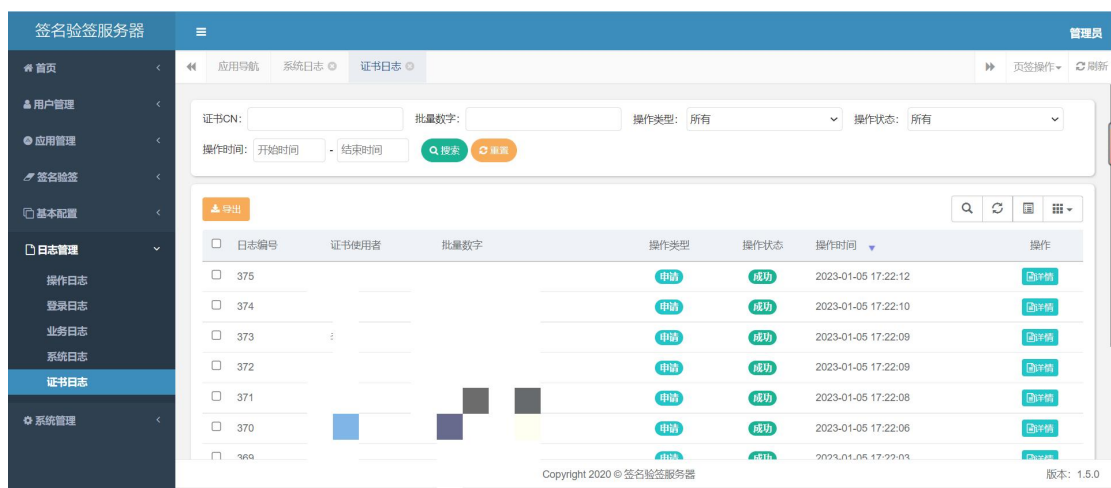


9.5 证书日志

1、点击证书日志，可以看到当前系统下所有的证书日志。



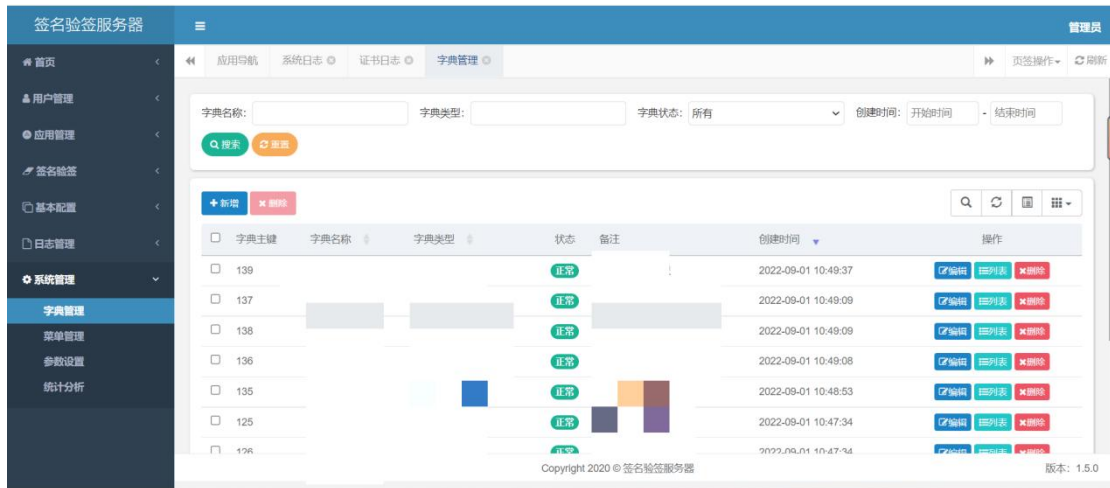
2、点击详情，可以看到当前日志的详细情况。



10 系统管理

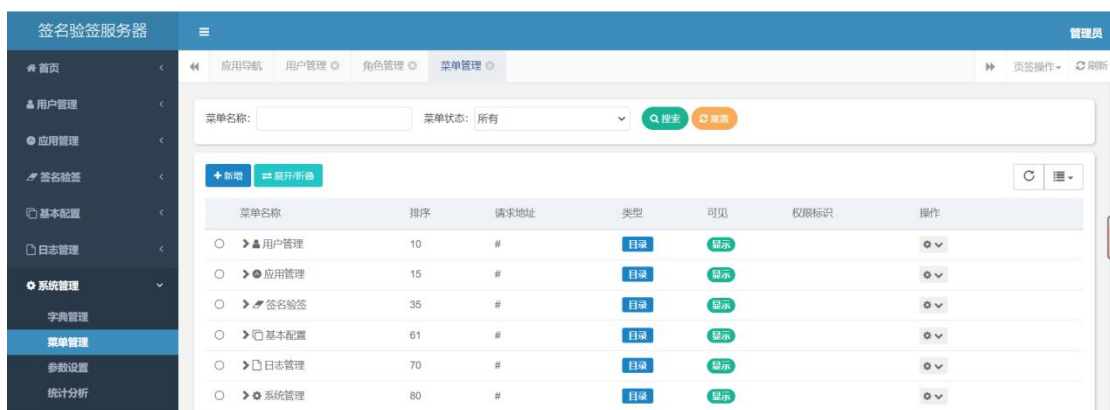
10.1 字典管理

1、点击字典管理，可以看到当前系统下所有的字典列表。



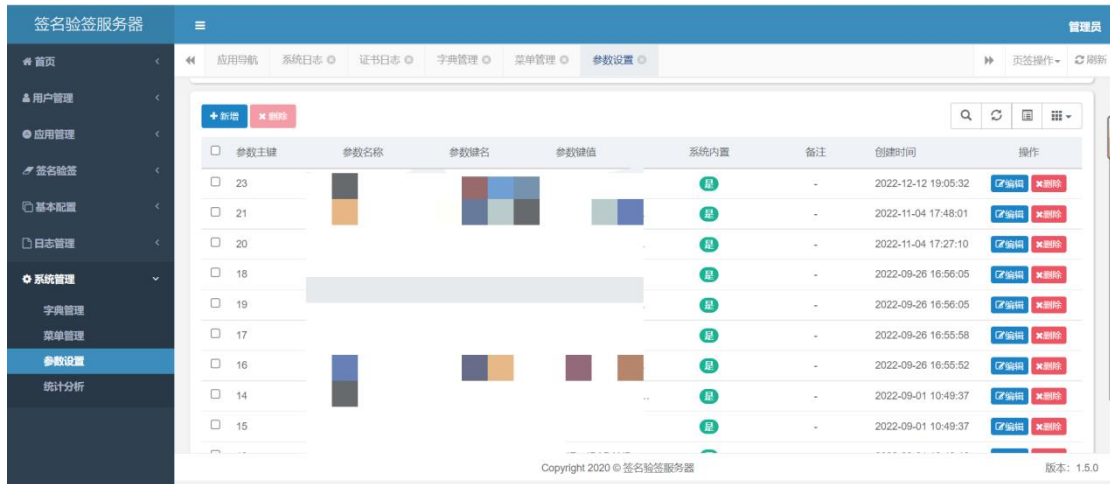
10.2 菜单管理

1、点击菜单管理，可以看到当前系统下所有菜单列表。



10.3 参数设置

- 1、点击参数设置，可以看到当前系统下所有参数列表。



10.4 统计分析

- 1、点击统计分析，可以看到当前系统日志统计分析图。

