安为科技

AnweiTech

视频安全密钥服务系统

用户手册

版权所有©北京安为科技有限公司 2021。保留一切权利。
本手册的任何部分，包括文字、图片、图形等均归属于北京安为科技有限公司（以下简称“北京安为”或“安为科技”）。未经书面许可，任何单位或个人不得以任何方式摘录、复制、翻译、修改本手册的全部或部分。除非另有约定，北京安为科技有限公司不对本手册提供任何明示或默示的声明或保证。

关于本产品

本手册描述的产品仅供中国大陆地区销售和使用。本产品只能在购买地所在国家或地区享受售后服务及维保方案，热线服务时间为 7*24 小时。

关于本手册

本手册仅作为相关产品的指导说明，可能与实际产品存在差异，请以实物为准。北京安为科技建议您在专业人员的指导下使用本手册。

责任声明

●在法律允许的最大范围内，本手册以及所描述的产品（包含其硬件、软件、固件等）均“按照现状”提供，可能存在瑕疵或错误。北京安为不提供任何形式的明示或默示保证，包括但不限于适销性、质量满意度、适合特定目的等保证；亦不对使用本手册或使用本产品导致的任何特殊、附带、偶然或间接的损害进行赔偿，包括但不限于商业利润损失、系统故障、数据或文档丢失产生的损失。

●您知悉互联网的开放性特点，您将产品接入互联网可能存在网络攻击、黑客攻击、病毒感染等风险，北京安为不对因此造成的产品工作异常、信息泄露等问题承担责任，但北京安为将及时为您提供产品相关技术支持。

●使用本产品时，请您严格遵循适用的法律法规，避免侵犯第三方权利，包括但不限于公开权、知识产权、数据权利或其他隐私权。您亦不得将本产品用于大规模杀伤性武器、生化武器、核爆炸或任何不安全的核能利用或侵犯人权的用途。

●如本手册内容与适用的法律相冲突，则以法律规定为准。

数据安全声明

●您在使用产品的过程中，将收集、存储与使用个人数据。安为科技在产品开发过程中，贯彻个人数据保护原则。

●作为数据控制者，您在收集、存储与使用个人数据时，须遵循所适用的个人数

据保护相关的法律法规，包括但不限于，对个人数据采取保护措施，例如，对设备进行合理的权限管理、加强设备应用场景的物理安全、定期进行安全评估等。

●本产品中未设置恶意程序、隐蔽接口，无未明示的功能模块等。

前 言

本手册描述了密钥管理系统产品的功能配置和操作，指导用户完成对产品的各功能配置和使用。

本节内容的目的是确保用户通过本手册能够正确配置和实现产品各功能。在使用此产品之前，请认真阅读产品手册并妥善保存以备日后参考。

适用产品

本手册适用于视频安全密钥服务系统。

目标用户

本手册主要针对用户为：

- 工程商
- 技术支持
- 终端用户

符号说明

符号	说明
	说明类文字，表示对正文的补充和解释。
	注意类文字，表示提醒用户一些重要操作或者防范潜在的伤害和财产损失危险。
	警告类文字，表示有潜在风险，不过不加避免，有可能造成伤害事故、设备损坏或业务中断。

安全注意事项

- 设备接入互联网可能面临网络安全问题，请您加强个人信息及数据安全的保护。当您发现设备可能存在网络安全隐患时，请及时与我们联系。
- 请您理解，您有责任合理配置所有的密码及其他相关产品安全设置，并妥善保管好您的用户名和密码。
- 使用设备前，请检查电源是否符合室内机所需的电源。
- 设备支持的环境请不要在高温、低温或者高湿度的环境下使用设备，具体温、湿度要求参见设备的参数表。

- 为了避免热量积蓄，请保持设备周边通风流畅。
- 请不要使物体摔落到设备上或大力振动设备，使设备远离存在磁场干扰的地点。避免将设备安装到表面振动或容易受到冲击的地方（忽视此项可能会损坏设备）。

第 1 章 产品简介

本产品作为基于密码技术的安全解决方案，专注于对称密钥与非对称密钥的全生命周期管理，覆盖商密算法（如 SM2/SM3/SM4）及国际算法，通过统一密钥管理能力，确保密钥生成质量、安全存储与高效分发，满足多应用、多业务场景需求。同时，产品集成 CA 证书管理功能，支持证书的申请、解析、及校验等全流程管理，确保身份认证的可靠性与数据传输的安全性，全面符合监管与合规要求。

核心功能特性

1.密钥全生命周期管理

采用多级密钥管理体系，覆盖密钥生成、存储、分发、撤销、归档、备份、恢复及销毁全流程，确保密钥安全可控。

支持商密算法（SM2/SM3/SM4）及国际算法，满足多样化业务场景需求。

2.丰富的接口与协议支持

遵循 GM/T 0051 规范，提供对称及非对称密钥管理接口。

3.高性能密钥分发

基于多任务异步并发架构，动态编排密钥请求，实现高并发、毫秒级低时延的密钥管理服务，保障业务连续性。

4.高稳定密钥存储

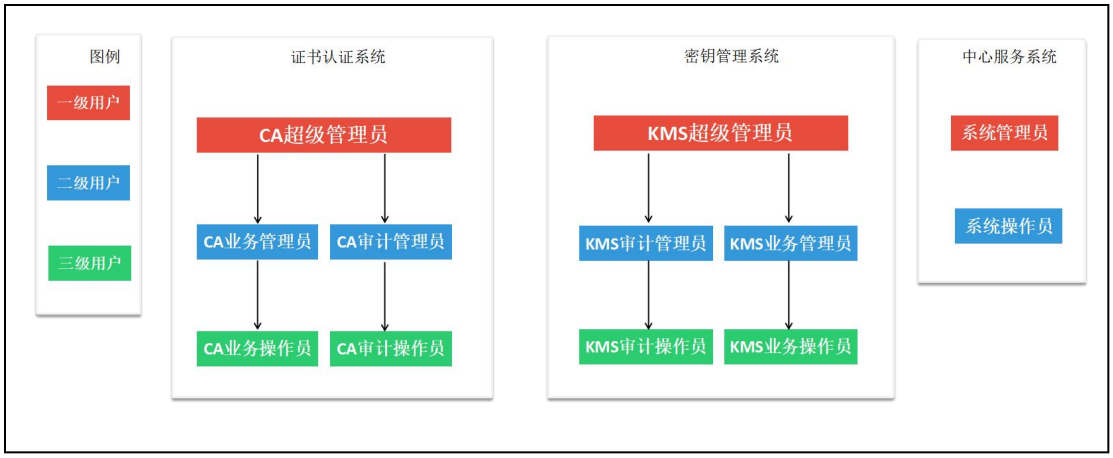
采用弹性扩容的存储服务框架，支持 30 万证书及 5 万密钥的安全存储。

提供密钥实时备份与定期备份机制，确保数据安全与可用性。

本手册详细介绍了产品管理平台的操作指南，包括密钥生成、存储、分发、撤销等全生命周期管理功能的配置步骤，帮助用户快速掌握产品使用与维护方法。

第 2 章 用户说明

在使用本系统之前，请务必了解本系统中的权限管理制度，方便您更好的使用该系统。



中心服务系统(SYS)

权限层级	角色名称	职责
一级	系统管理员	创建系统操作员，查看在线用户。
二级	系统操作员	系统监控，系统运维，日志存储

密钥管理系统（KM）

权限层级	角色名称	职责
一级	KMS 超级管理员	创建 KMS 业务管理员和审计管理员
二级	KMS 审计管理员	审计策略配置、全量操作日志审查、违规操作拦截处置 创建审计操作员
二级	KMS 业务管理员	创建 KMS 业务操作员
三级	KMS 审计操作员	日志管理
三级	KMS 业务操作员	配置密钥加密密钥 用户密钥 历史密钥 密钥归档记录

证书认证系统（CA）

权限层级	角色名称	职责
一级	CA 超级管理员	查看在线用户，创建 CA 业务管理员和 CA 审计管理员，可对其进行管理。
二级	CA 审计管理员	创建 CA 审计操作员。

二级	CA 业务管理员	查看在线用户，创建 CA 业务操作员，可对其进行管理。
三级	CA 审计操作员	日志管理
三级	CA 业务操作员	CA 证书 证书申请 已签发证书列表 证书 CRL 管理 证书归档 证书解析校验

第 3 章 安装控件

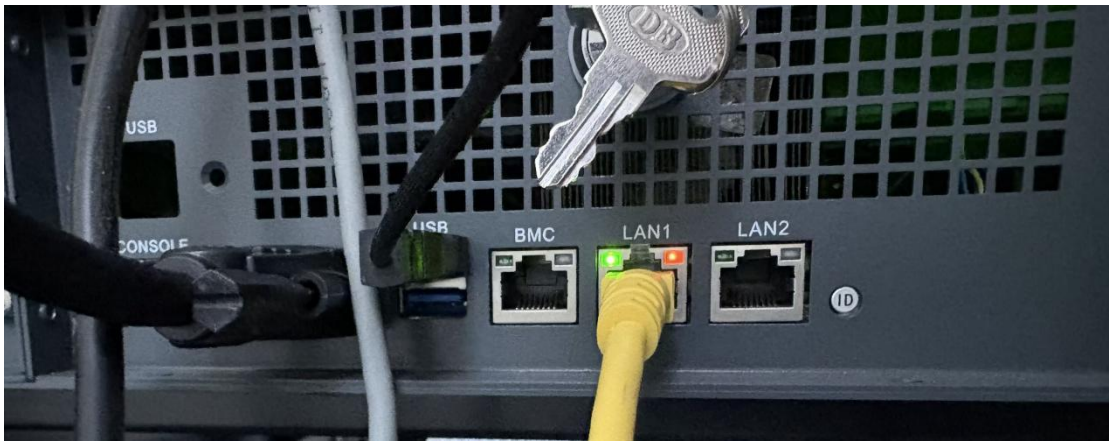
推荐运行环境：

谷歌浏览器（建议使用较新版本）。

连接管理口：

笔记本连接设备管理口，将笔记本地址设置为 192.168.100.xx（除 192.168.100.1 以外）。

管理口位置：



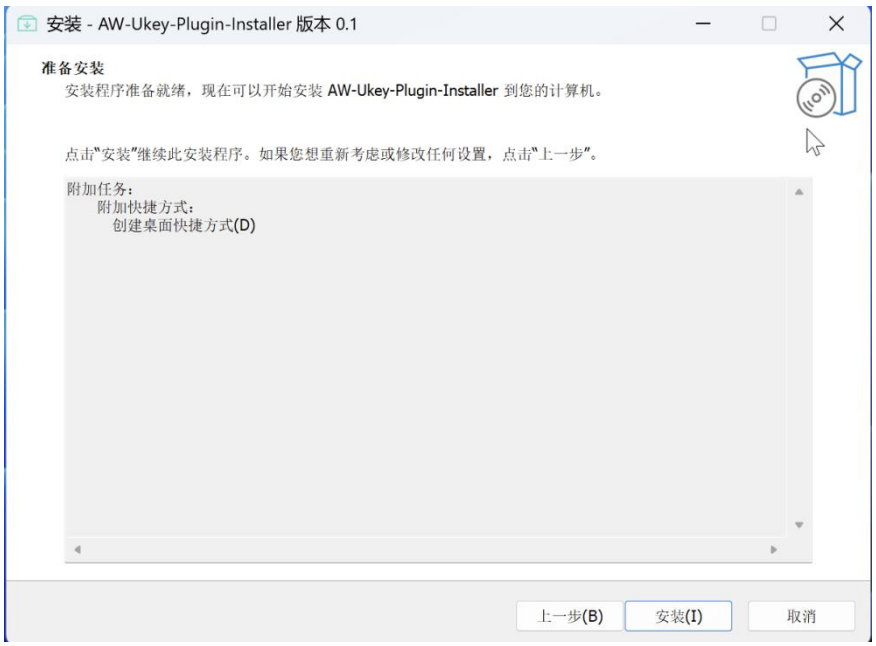
打开浏览器输入 https://192.168.100.1，进入到系统登录页面。

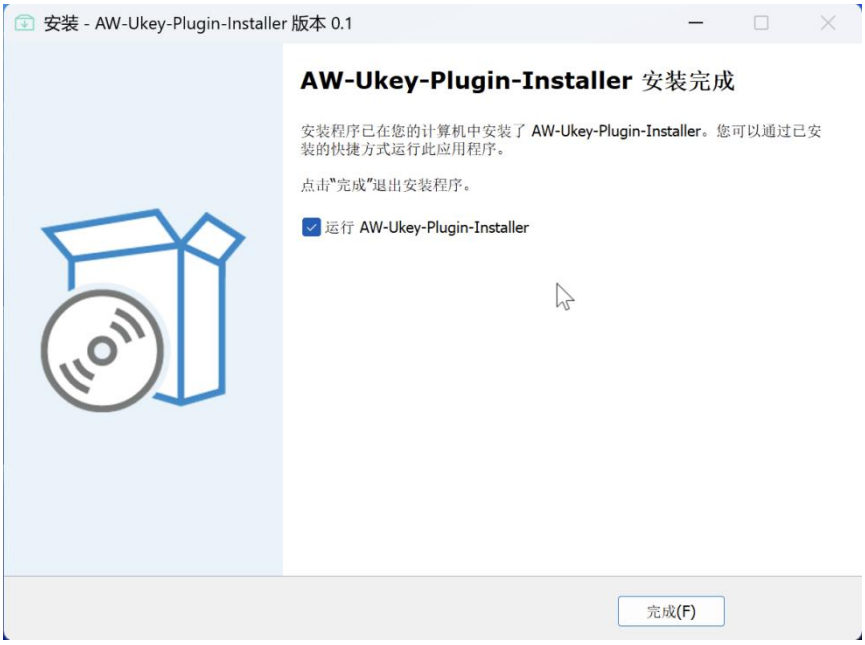
通过浏览器访问系统登录页面时，系统会自动提示安装控件，若没有自动下载，点击刷新或者点击网页顶端出现的 “请先下载安装后再登录系统！”中的“下载”，用管理员权限下载控件。

操作步骤

1.安装控件。右键以管理员的身份运行，弹出安装提示框，按照提示完成安装。

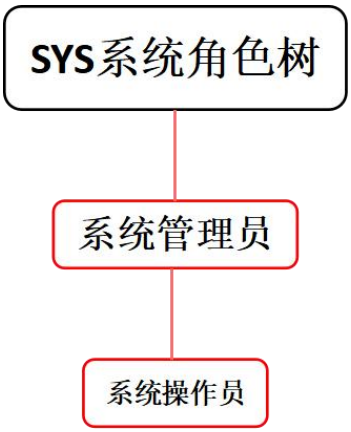

安装 - AW-Ukey-Plugin-Installer 版本 0.1
选择附加任务
您想要安装程序执行哪些附加任务？
选择您想要安装程序在安装 AW-Ukey-Plugin-Installer 时执行的附加任务，然后点击"下一步"。
附加快捷方式：
创建桌面快捷方式(D)
下一步(N)
取消


安装 - AW-Ukey-Plugin-Installer 版本 0.1
准备安装
安装程序准备就绪，现在可以开始安装 AW-Ukey-Plugin-Installer 到您的计算机。
点击"安装"继续此安装程序。如果您想重新考虑或修改任何设置，点击"上一步"。
附加任务：
附加快捷方式：
创建桌面快捷方式(D)
上一步(B)
安装(I)
取消


安装 - AW-Ukey-Plugin-Installer 版本 0.1
AW-Ukey-Plugin-Installer 安装完成
安装程序已在您的计算机中安装了 AW-Ukey-Plugin-Installer。您可以通过已安装的快捷方式运行此应用程序。
点击"完成"退出安装程序。
运行 AW-Ukey-Plugin-Installer
完成(F)


AW-Ukey-...

第 4 章 中心服务系统(SYS)



4.1. 系统初始化

系统登陆地址：https://192.168.100.1/sys 。

若用户初次访问系统，则会进入系统管理员初始化页面。用于注册系统管理员账号，系统管理员账号可以创建系统操作员账号。

操作步骤

1. 安装成功后，插入 UKey，刷新界面，填写用户名、证书有效期。

2.点击盘符下拉框，成功枚举出用户 UKey 盘符，按照界面提示输入相应信息。

4.2. 系统管理员登录

操作步骤

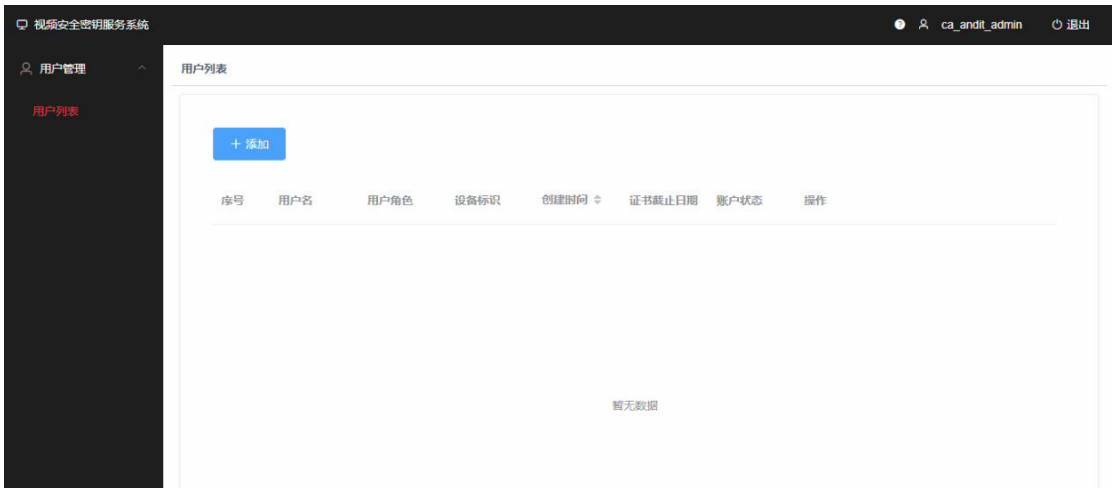
1. 通过浏览器访问平台地址，进入平台登录页面。

2. 插入 UKey，选择 UKey 盘符，输入登录 PIN 码、单击登录。

3. 登录成功，进入系统平台。

第 5 章 导航

导航栏是系统的导向，提供了有关系统的信息。熟悉导航的结构，可以更好的帮助用户理解此平台的功能。



5.1. 导航栏

在导航栏中，将光标移动至“帮助”上，点击帮助，可下载用户使用手册。

在上导航栏中，从左至右依次为：产品名称、帮助、账号信息。

（帮助）：

可下载产品用户手册。

下载平台证书列表：

单击下载平台证书列表，内含平台的 cer 证书。

账号信息：

单击账号用户名，下拉框中可修改 PIN 码、修改个人信息、查看版本信息、退出登录。

5.2. 资料下载

在导航栏中，将光标移动至  上，可下载用户使用手册。

5.3. 修改 PIN 码

在导航栏中，将光标移动至账号用户名上，弹出下拉框，单击修改 PIN 码。

输入旧登录 PIN 码，新登录 PIN 码，确认登录 PIN 码。

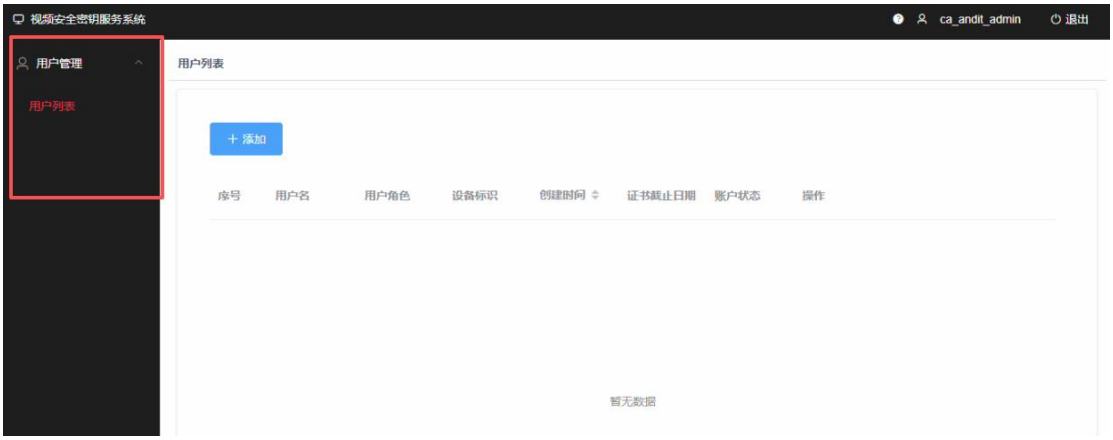
平台安全设置要求 PIN 码：6-16 位数字。

5.4. 修改个人信息

在导航栏中，将光标移动至账号用户名上，弹出下拉框，单击“修改个人信息”。修改完成后点击确定。

5.5. 左侧导航栏

左侧导航栏显示当前账号所拥有的功能。



查看平台信息

在导航栏中，将光标移动至账号用户名上，弹出下拉框，单击关于，查看当前版本信息、软件使用许可说明、开源软件说明。

单击**退出**，退出系统平台。

第 6 章 用户管理

本章功能所属角色为系统管理员，主要功能是用户的新增、删除、修改、查找、冻结、重置、为用户分配角色，同时还可以对锁死的子用户进行 UKey 解锁。

6.1. 添加用户

操作步骤

1. 在主页左侧导航栏中单击用户管理->用户列表。
2. 单击添加。
3. 依次输入提示信息，单击确定。

用户名：输入用户名。

用户角色：可添加角色为 CA 审计管理员、CA 业务管理员。

Ukey 序列号：选择 UKey 盘符。

证书有效期：可选择 3 年、5 年、10 年、20 年、30 年、50 年。

登录 PIN 码、确认登录 PIN 码：设置登录 PIN 码。

管理 PIN 码、确认管理 PIN 码：设置管理 PIN 码，管理 PIN 码用于解锁。

可选操作

1.编辑用户：单击操作栏的**编辑**，可修改用户角色、电话、邮箱。

2.查询用户：可根据用户名、用户角色、账户状态、创建时间、证书截止日期查询用户。

3.删除、冻结用户：单击操作栏的**删除、冻结**即可操作。

删除：删除当前选中用户。

冻结：冻结选中账号，冻结后账号不可登录，冻结后可以进行解冻操作。

4.重置密码：单击操作栏的**重置**，输入管理员密码，可重置用户密码。

5.UKey 解锁：如果当前的子角色在使用 UKey 登录时多次输错 PIN 码导致该 UKey 锁死，可在父角色列表的右上角 **UKey 解锁**进行解锁处理。

插入被锁定的 UKey，输入该 UKey 的用户名，并选择插入的盘符，点击确定进行解锁（再次使用该解锁 UKey 登录时需输入默认 PIN 码 123456）。

第 7 章 SYS 系统操作员

本章功能所属角色为系统操作员，系统操作主要为负责系统监控、系统运维、日志配置。

退出系统管理员账户，返回登录界面。

返回登陆页面，登陆在系统管理员角色下创建的系统操作员账户。

首次登陆提示修改密码，修改密码后请牢记。

该章节由系统操作员负责。例如：

控件管理：

控制插件的上传下载，前端支持通过 ukey 控件调用智能密码钥匙接口完成身份认证、用户证书存储、日志签名等功能，保证存储安全和密码运算安全。当旧版本插件出现漏洞等不安全因素时，可通过插件管理及时更新安全的插件来保障平台的安全性。

License 管理：

License 模块的主要提供预激活文件的下载与激活文件的上传。主要内容包括激活文件（用来检验 License 合法性）安装，预激活文件（用于离线生成激活文件）生成、解析校验激活文件等功能。

系统监控管理：

对服务信息进行监控，包含系统信息、CPU 信息、内存信息、网络状态以及磁盘信息。

配置管理：

包含 网络配置、日志配置、SSH 配置、服务重启。

7.1. 系统监控

在左侧导航栏中单击**系统监控**，可以查看当前设备 IP 地址、使用时长、操作系统信息、内存使用率、磁盘使用率、CPU 使用率。

7.2. 系统运维

7.2.1.网络配置

网络配置用于进行**网口配置**（启用或停用网口并配置相关 IP）。

7.2.2.系统升级

将系统从当前版本升级到新的版本，用于修复系统缺陷以及功能优化。系统升级将不会对现有数据进行覆盖与清除，升级过程中可能会重启部分服务，服务重启过程会出现短暂不可用。

注意

升级过程中请勿关闭或重启系统，同时系统升级的版本不低于当前系统版本。

选择本地升级。

同时支持查看已升级的历史记录。

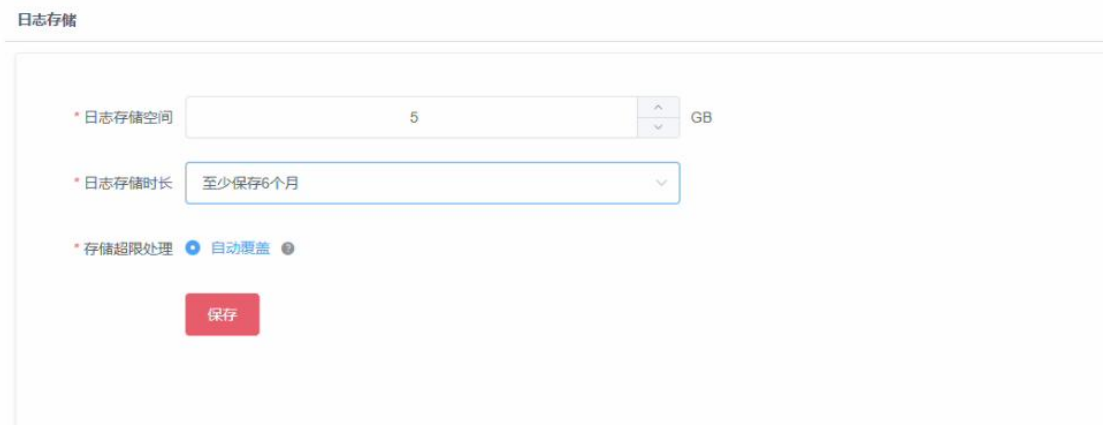
7.2.3.服务启停

可对系统服务进行重启，无需进入后台输入命令，重启过程中，系统正在运行的任务将中断，请谨慎操作。可开关 SSH 服务，开启 SSH 服务后，可远程 SSH 登录到平台服务。

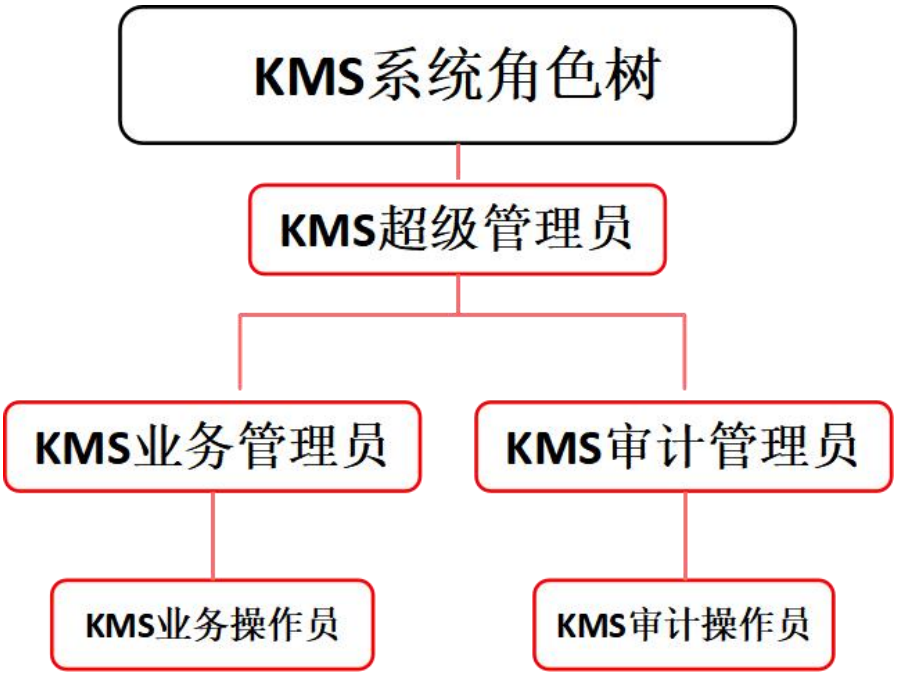
7.3. 日志配置

7.3.1. 日志存储

支持配置日志存储空间和存储时长。存储超期后系统选择自动覆盖。未超期日志则会默认进行本地保存。



第 8 章 密钥管理系统-KM



密钥管理系统用户划分为三层，KMS 超级管理员为一级用户，KMS 业务管理员和 KMS 审计管理员为二级用户，KMS 业务操作员和 KMS 审计操作员为三级用户。

8.1. 管理员初始化

若用户初次访问密钥管理系统，则会进入初始化页面。用于注册一级账号：KMS 超级管理员账号，后续可通过初始化的一级账号创建二级账号，KMS 业务操作员和 KMS 审计操作员为三级用户，需要登入二级账户 KMS 业务管理员和 KMS 审计管理员注册。

操作步骤

1. 安装成功后，插入 UKey，刷新界面，填写用户名、证书有效期。

2. 点击盘符下拉框，成功枚举出用户 UKey 盘符，按照界面提示输入相应信息。

8.2. 角色登录

操作步骤

1. 通过浏览器访问平台地址，进入平台登录页面。

2. 插入 UKey，选择 UKey 盘符，输入登录 PIN 码、单击**登录**。

3. 登录成功，进入系统平台。

8.3. 业务管理(KMS-业务操作员)

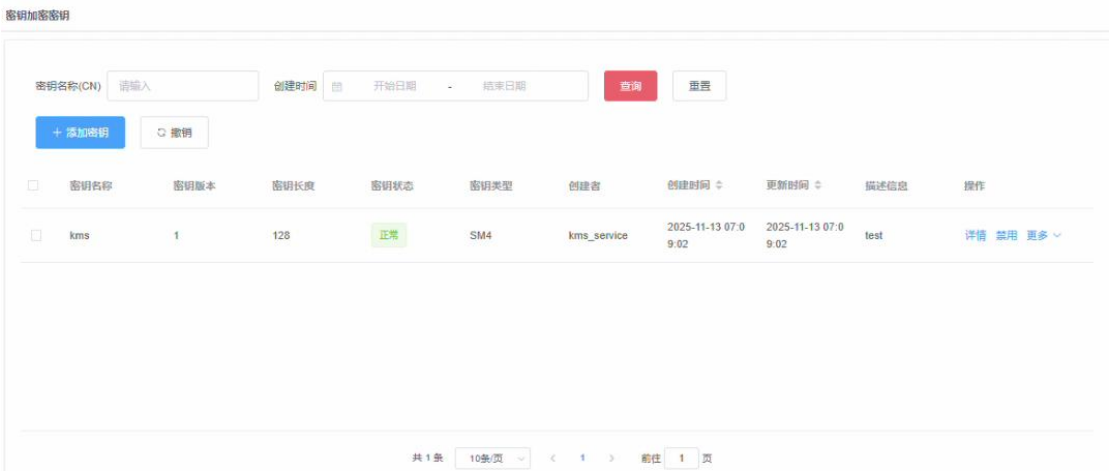
业务管理主要功能是管理密钥加密密钥和用户密钥。

本章功能所属角色为 KMS-业务操作员。

8.3.1.配置密钥加密密钥

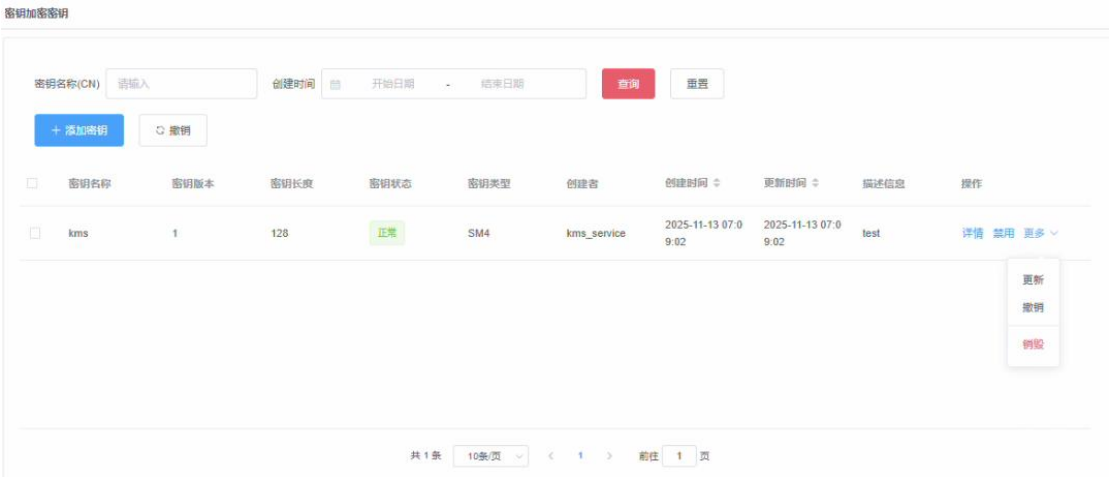
1. 密钥新增

点击**添加密钥**按钮，输入密钥名称和备注信息。点击**确定**生成密钥。



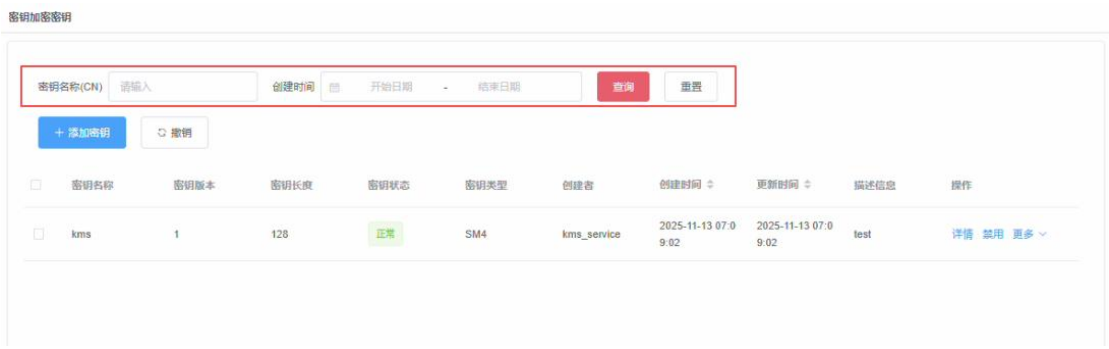
2. 禁用、更新、撤销、销毁功能

禁用、更新、撤销、销毁功能点击相应按钮并输入本业务操作员账户的 PIN 码进行二次认证后即可实现。



3. 查询功能

选择密钥名称和创建时间，填入搜索限制和索引即可完成查询。点击**重置**可重置搜索选项中的内容。



4. 详情功能

详情功能可查看该密钥加密密钥的详细信息。点击**详情**按钮即可查看。

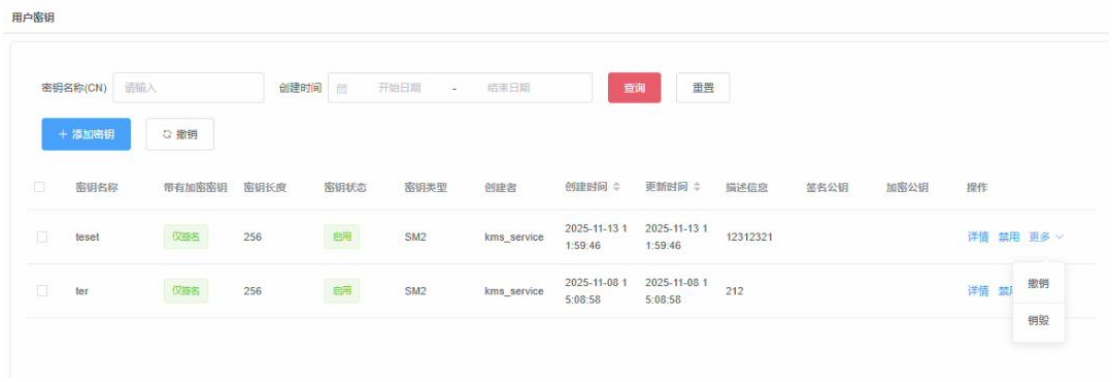
8.3.2.用户密钥

1. 密钥新增

点击**添加密钥**按钮，输入密钥名称、密钥用途和描述信息。点击**确定**生成密钥。

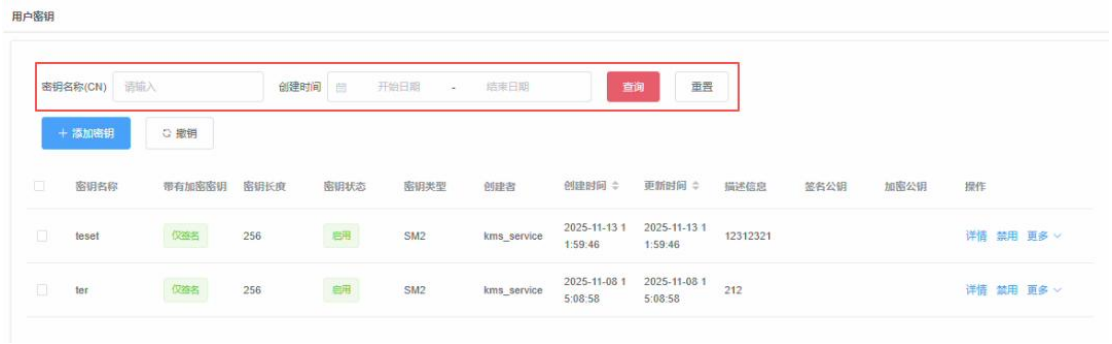
2. 禁用、撤销、销毁功能

禁用、撤销、销毁功能点击相应按钮并输入本业务操作员账户的口令即可实现。



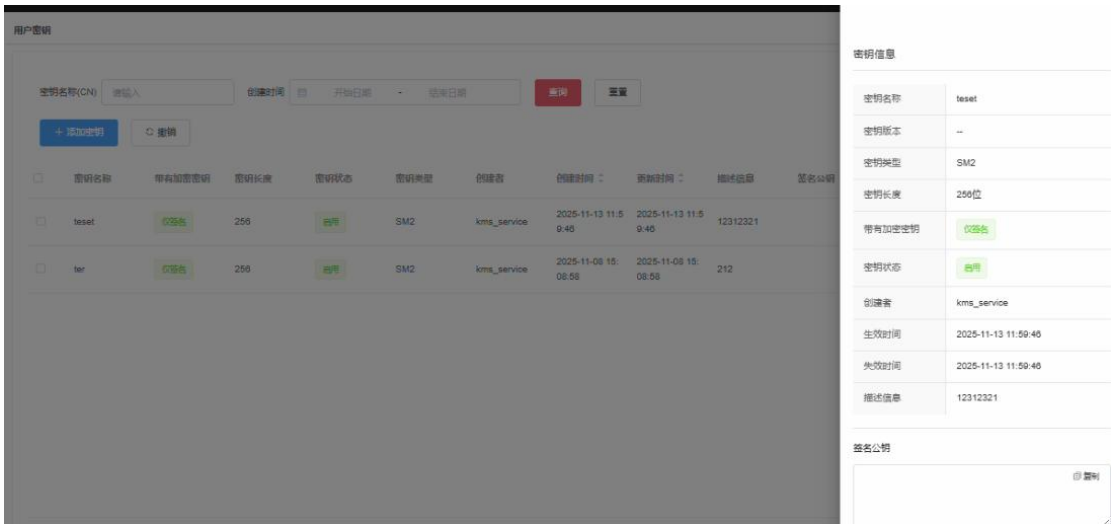
3. 查询功能

选择密钥名称和创建时间，填入搜索限制和索引即可完成查询。点击**重置**可重置搜索选项中的内容。



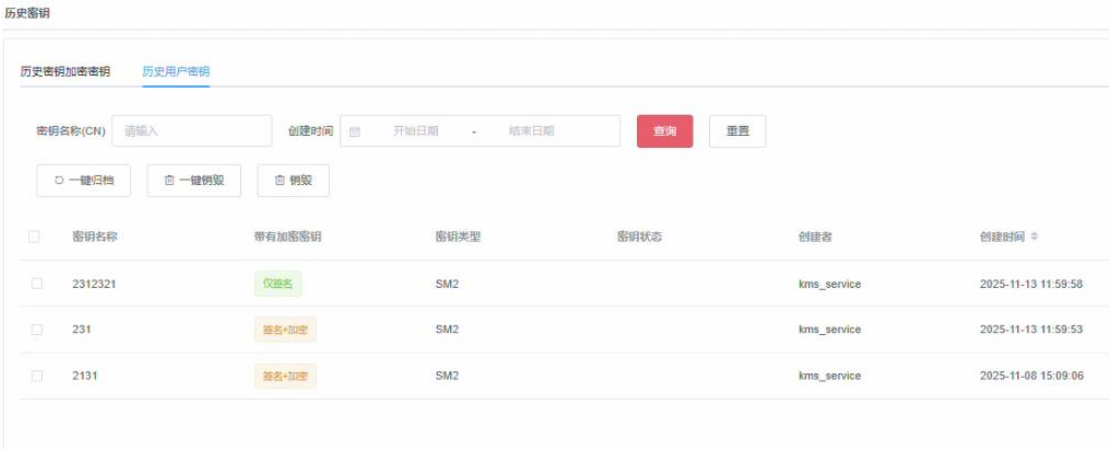
4. 详情功能

详情功能可查看该密钥加密密钥的详细信息。点击**详情**按钮即可查看。

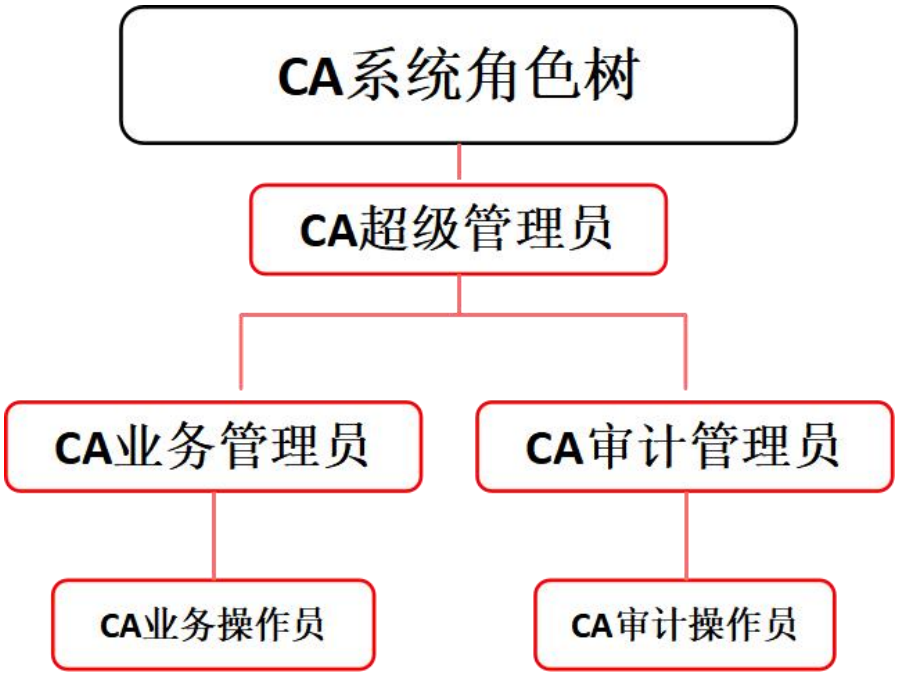


8.3.3.历史密钥

包括对历史密钥加密密钥、历史用户密钥的查询，归档和销毁功能。通过在创建时间、密钥名称中选择或填入搜索的条件和索引即可进行搜索。点击**重置**可重置搜索选选项中的内容。密钥销毁需要输入本业务操作员账户的口令。



第 9 章 证书认证系统-CA



9.1. 管理员初始化

若用户初次访问密钥管理系统，则会进入初始化页面。用于注册一级账号：证书认证系统用户划分为三层，CA 超级管理员为一级用户，CA 业务管理员和 CA 审计管理员为二级用户，CA 业务操作员和 CA 审计操作员为三级用户。

操作步骤

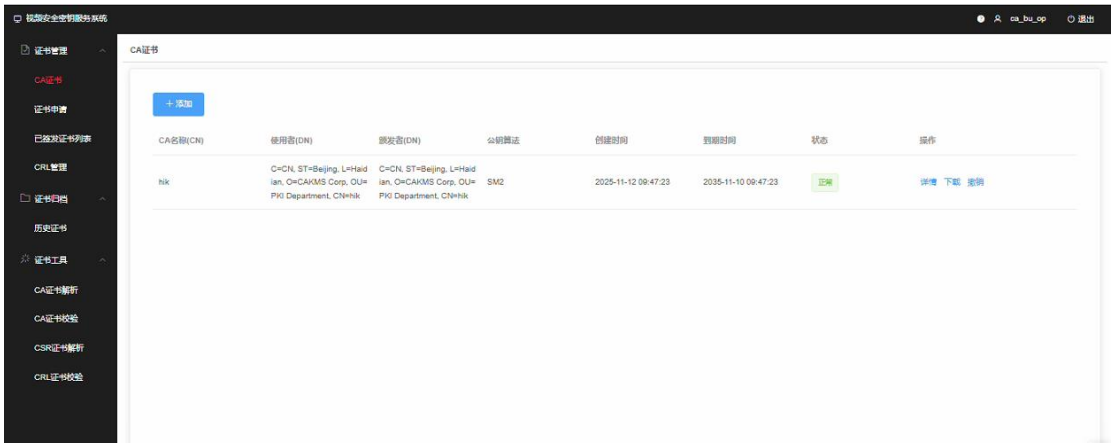
1. 安装成功后，插入 UKey，刷新界面，填写用户名、证书有效期。

2. 点击盘符下拉框，成功枚举出用户 UKey 盘符，按照界面提示输入相应信息。点击创建并下一步，系统管理员初始化完成，跳转登陆页面。

9.2. 证书认证系统

本节的功能所属角色为 **CA 业务操作员**。

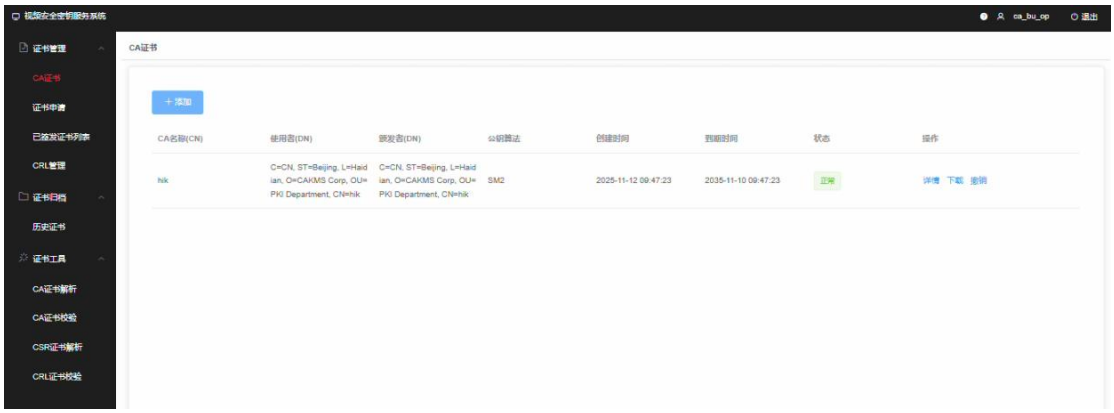
证书管理部分分为 CA 证书、证书申请、已签发证书列表、CRL 管理。



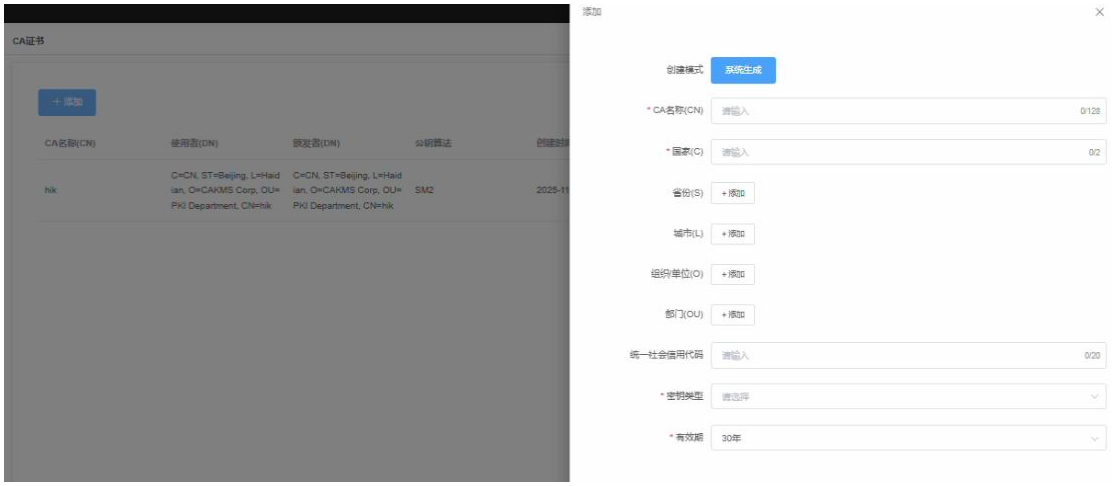
9.2.1.CA 证书

1. 新增 CA 证书。

系统生成自签 CA。

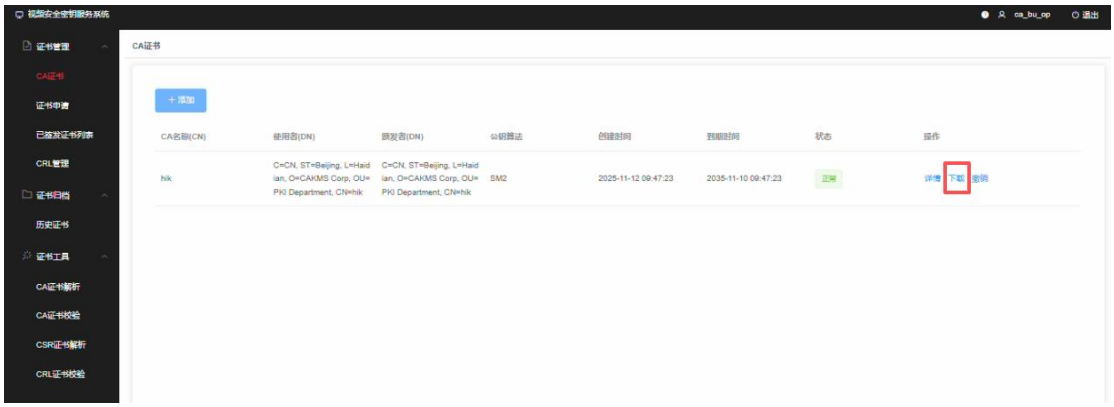


点击添加 CA 证书，填入 CA 名称、国家、密钥类型和有效期即可生成 CA 证书。



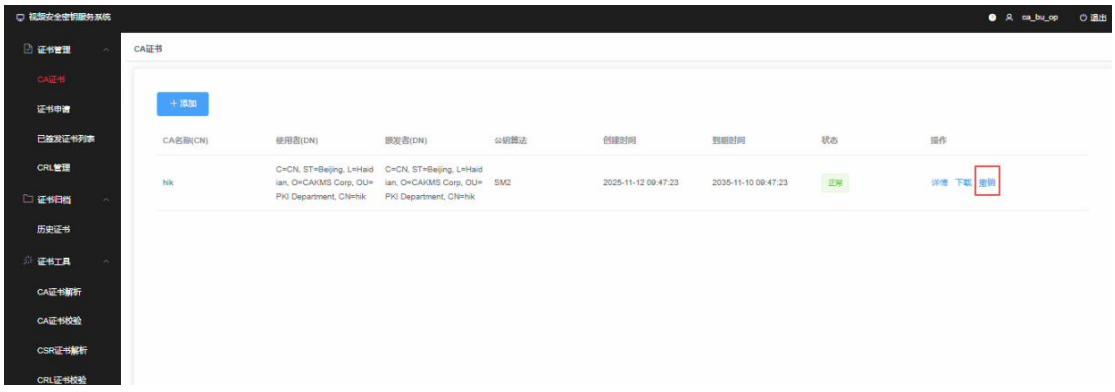
2.导出 CA 证书

点击 CA 证书对应的下载按钮，输入登录 PIN 码，点击确定即可导出证书。



3.撤销 CA 证书

点击 CA 证书对应的撤销按钮，输入本业务操作员账户的口令，点击确定即可撤销证书。



4.CA 证书详情

点击 CA 证书对应的**详情**按钮，即可查看本证书的详细信息。

9.2.2.证书申请

1.选择 CA 证书

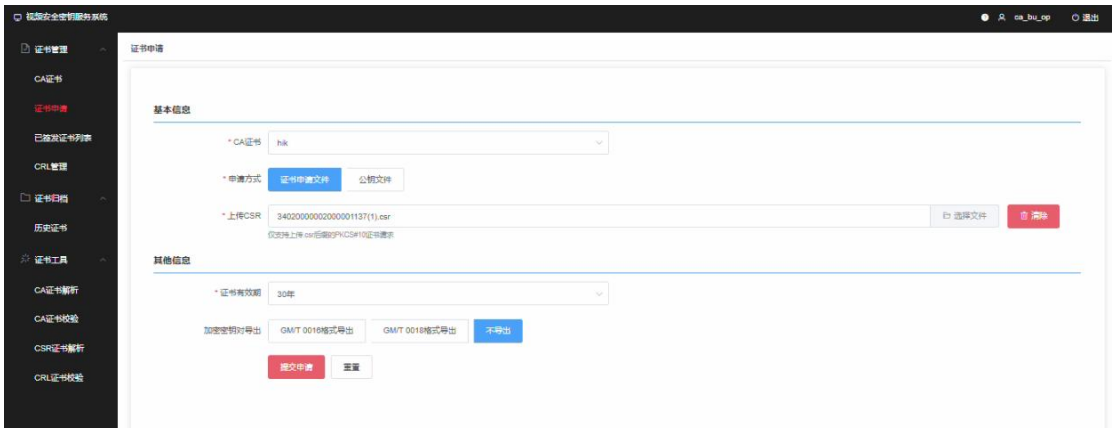
从 CA 证书下拉菜单中选择签发机构。

2.选择申请方式

证书请求文件：需上传 CSR 文件（在文本框中选择或输入路径）。

公钥文件：需提供公钥文件。

9.2.2.1. 证书请求文件申请



当选择证书请求文件申请时：

1.上传 CSR 文件

点击“上传 CSR”按钮，提交 PKCS#10 格式的证书请求文件（需提前在本地生成，包含公钥及申请者信息）。

2.设置有效期

从下拉菜单中选择证书的有效期（如 1 年、3 年、5 年、10 年、20 年、30 年，需符合 CA 策略）。

3. 选择加密对导出格式（可选）

若需导出加密密钥，选择格式：

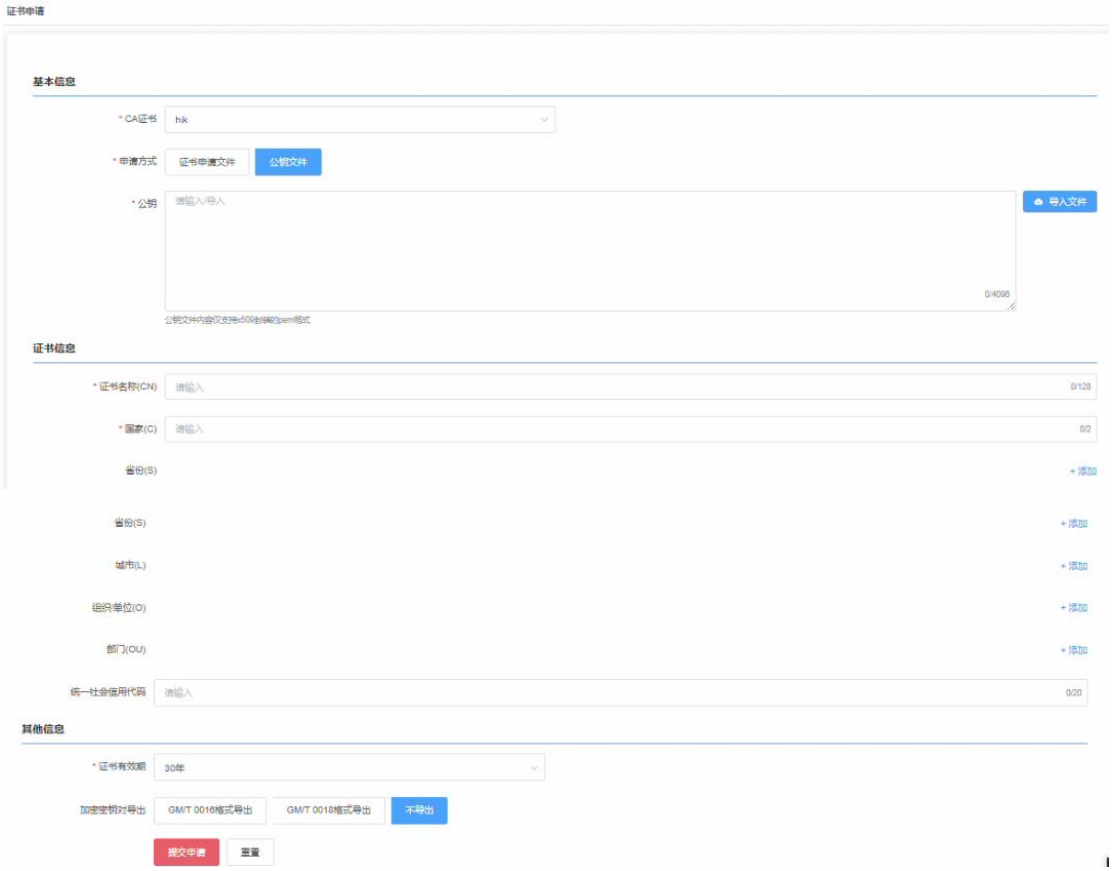
- GM/T 0016（国密 SKF 规范）
- GM/T 0018（国密 SDF 规范）

注意：只有 SM2 算法证书能选择导出加密密钥对，若选择不导出，则不会生成加密密钥对与加密证书。

4. 提交申请

确认信息无误后，点击“提交申请”按钮，等待 CA 审核签发证书。

9.2.2.2. 公钥文件申请



1. 输入/导入公钥文件

在指定输入框内粘贴公钥内容，或通过文件上传功能导入公钥文件。

2. 填写证书主体信息

证书名称（CN）：填写与公钥关联的实体名称（如服务器域名或个人姓名）。

地区信息：依次填写省份、城市、国家代码（如中国填 CN）。

组织信息：输入单位全称、部门名称（可选）。

统一社会信用代码：企业用户填写 18 位信用代码。

3. 设置有效期

从下拉菜单中选择证书有效期（如 1 年、3 年、5 年、10 年、20 年、30 年）。

4. 加密密钥对导出格式（可选）

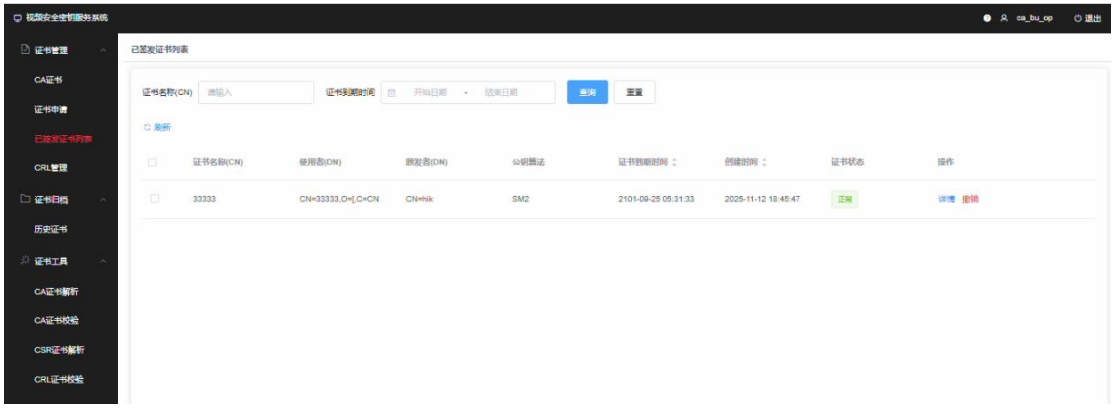
根据需求选择是否导出加密密钥对：

- **GM/T 0016**（国密 SKF 规范）
- **GM/T 0018**（国密 SDF 规范）
- **不导出：**仅生成签名证书。

5. 提交申请

确认信息无误后提交，等待 CA 机构审核签发证书。

9.2.3.已签发证书列表



核心功能

1. 证书信息展示

以表格形式列出已签发证书的详细信息，包括：

- **证书名称（CN）：**证书的通用名称
- **使用者（DN）：**证书持有者的可识别名称
- **颁发者（DN）：**证书颁发机构（CA）的可识别名称
- **公钥算法：**证书使用的加密算法（如 RSA、ECC 等）
- **证书到期时间：**证书的有效截止日期

• **创建时间：**证书签发的时间

• **证书状态：**当前状态（如有效、过期、吊销等）

2. 操作与交互

查询：支持按条件筛选证书

重置：一键清除所有筛选条件，恢复默认列表视图

对证书进行的操作：详情，撤销。

辅助特性

• **分页显示：**默认每页显示 10 条数据（当前界面提示“未找到数据”）

• **导航关联：**与左侧菜单中的其他功能（如证书申请、CA 证书管理等）形成完整证书生命周期管理流程

典型使用场景

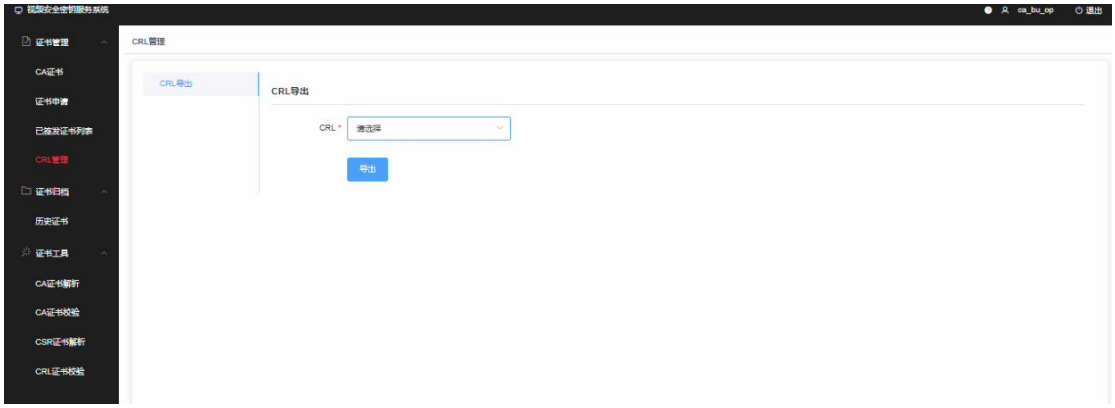
• 管理员需要快速查阅已签发证书的详细信息

• 监控证书有效期，及时处理即将过期的证书

• 验证证书颁发记录的合规性

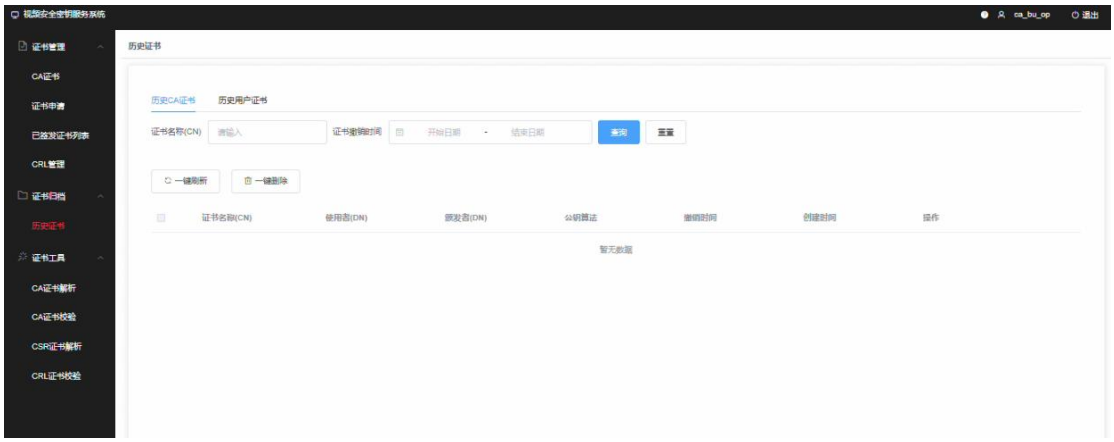
9.2.4.CRL 管理

在 CRL 选项中选择对应的选项，点击**导出**按钮即可导出 CRL。



9.3. 证书归档

9.3.1.历史证书



历史证书页面核心功能：

1. 分类查询

- 支持按名称/日期筛选 CA 和用户证书
- 分类展示证书关键信息（名称、颁发者、有效期、所使用的公钥算法等）

2. 批量处理

- 多选模式：可勾选多条记录
- 一键归档：支持批量归档选中证书

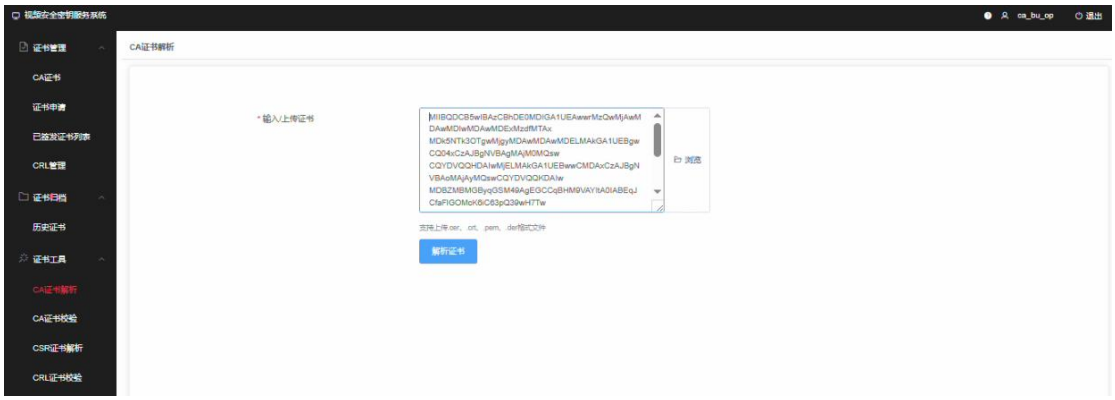
3. 分页展示

- 每页 10 条默认排序
- 底部显示总页数及数据总量

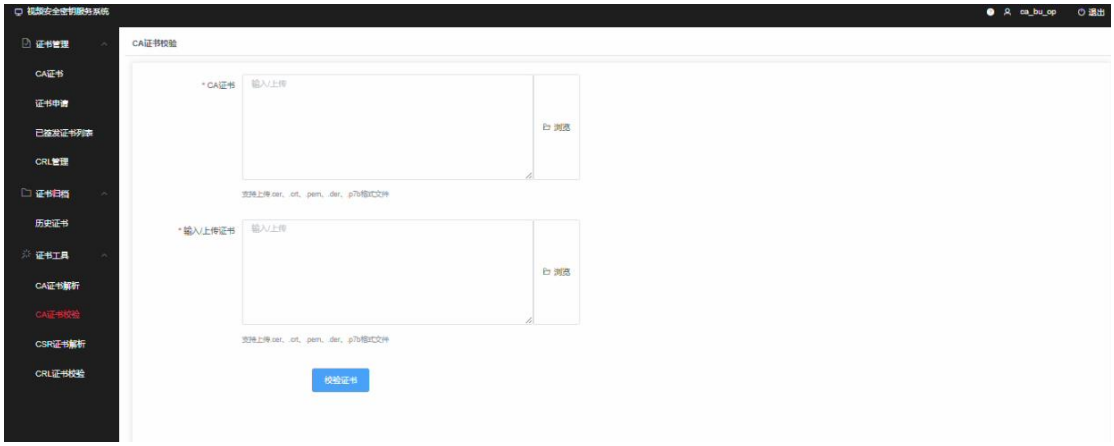
9.4. 证书工具

9.4.1.CA 证书解析

双击文本框后把证书文件粘贴证书文件内容的文本框中，或者点击文本框上传证书文件，点击查看证书内容即可进行证书解析。



9.4.2.证书校验



证书校验功能主要用于验证数字证书的有效性、完整性和可信度，确保证书未被篡改、过期或撤销。以下是详细功能描述：

1. CA 证书校验

用户需上传或输入受信任的根证书（CA 证书），格式支持.cer、.crt、.pem。

系统验证目标证书是否由该 CA 签发，确保证书链的可信性。

2.目标证书校验

用户上传待验证的证书文件（支持 .cer、.crt、.pem）。

系统检查证书的签名、有效期、扩展字段等基础信息是否合规。

3.校验流程

1）用户上传 CA 证书和目标证书。

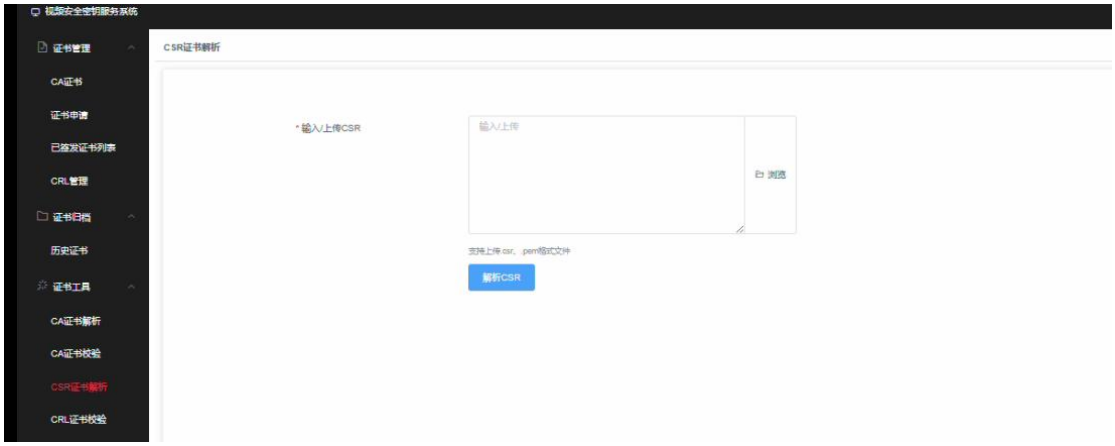
2）点击 “校验证书” 按钮，系统执行以下操作：

- 验证证书链完整性（CA 签名是否匹配）。
- 检查证书有效期（是否过期）。

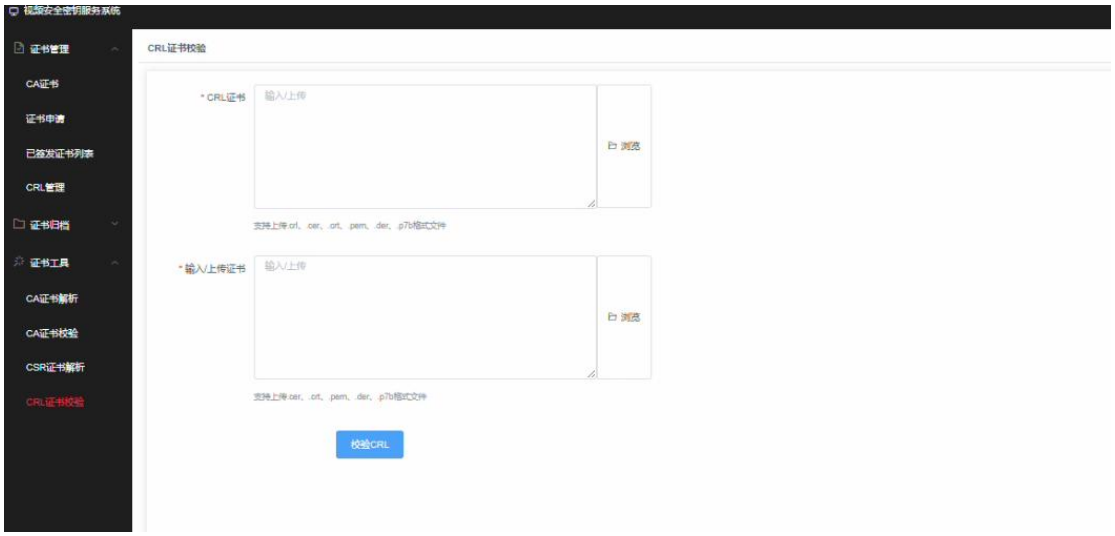
4.返回校验结果，及详细原因。

9.4.3.CSR 证书解析

双击文本框后把证书文件粘贴证书文件内容的文本框中，或者点击文本框上传证书文件，点击查看证书内容即可进行证书解析。



9.4.4.CRL 证书校验



证书校验功能主要用于验证数字证书的有效性、完整性和可信度，确保证书未被篡改、过期或撤销。以下是详细功能描述：

1. CRL 证书校验

用户需上传或输入受信任的 CRL 证书，格式（支持.crl）。

2.目标证书校验

用户上传待验证的证书文件（支持 .cer、.crt、.pem）。

系统检查证书的签名、有效期、扩展字段等基础信息是否合规。

3.校验流程

1）用户上传 CRL 证书和目标证书。

2）点击 “校验证书” 按钮，系统执行以下操作：

- 验证证书链完整性。
- 检查证书有效期（是否过期）。

4. 返回校验结果，及详细原因。