

翼安签名验签服务器 用户手册



山东华翼微电子技术股份有限公司

| 版本更新记录表 | | | | | | | |
|---------|-------|--------|------|--|--|--|--|
| 序号 | 版本号 | 版本更改说明 | 更改日期 | | | | |
| 1 | V1. 0 | 首次发布 | | | | | |
| 2 | | | | | | | |
| 3 | | | | | | | |
| 4 | | | | | | | |
| 5 | | | | | | | |
| 6 | | | | | | | |
| 7 | | | | | | | |
| 8 | | | | | | | |
| 9 | | | | | | | |
| 10 | | | | | | | |

声 明

版权声明

本文档的版权属山东华翼微电子技术股份有限公司所有。

本文档的版权受到中华人民共和国国家法律和国际公约的保护。未经书面许可,任 何单位和个人不得以任何形式或通过任何途径非法使用、拷贝、修改、扩散本文档的全 部或部分内容。

特别提示

我们做了大量的努力使本文档尽可能的完备和准确,但疏漏和缺陷之处在所难免。 任何人或实体由于本文档提供的信息造成的任何损失或损害,山东华翼微电子技术股份 有限公司不承担任何义务或责任。

山东华翼微电子技术股份有限公司保留未经通知用户对本文档内容进行修改的权利。

联系我们

如果您对本文档有任何疑问、意见或建议,请与我们联系。对您的帮助,我们十分 感激。

公司电话: 0531-66680161

公司邮箱: shandonghuayi@holichip.com

公司地址:山东济南高新区舜泰北路 933 号 19 层



| 1 | 概述 | | 1 |
|---|-----|--------------------|----|
| | 1.1 | 简介 | 1 |
| 2 | 产品 | 安装说明 | 1 |
| | 2.1 | 安装环境要求 | 1 |
| | 2.2 | 产品安装 | 1 |
| 3 | 产品 | 操作说明 | 1 |
| | 3.1 | 应用实体管理 | 9 |
| | 3.2 | 数据备份恢复 | 20 |
| | | 3.2.1 数据备份 | 20 |
| | | 3.2.2 数据恢复 | 24 |
| | 3.3 | 双机热备管理 | 28 |
| | 3.4 | 用户管理 | 31 |
| | | 3.4.1 系统用户管理 | 31 |
| | | 3.4.2 restful用户管理 | 37 |
| | 3.5 | 设备管理 | 41 |
| | | 3.5.1 初始化 | 41 |
| | | 3.5.2 系统升级 | 43 |
| | | 3.5.3 设备信息 | 43 |
| | | 3.5.4 重启/关机 | 44 |
| | | 3.5.5 系统配置 | 45 |
| | | 3.5.6 时间源设置 | 53 |
| | | 3.5.7 服务管理 | 55 |
| | | 3.5.8 设备自检 | 56 |
| | 3.6 | 证书管理 | 57 |
| | | 3.6.1 证书查询设置 | 57 |
| | | 3.6.2 CA证书管理 | 58 |
| | | 3.6.3 CRL管理 | 59 |
| | | 3.6.4 用户证书管理 | 61 |
| | | 3.6.5 设备证书管理 | 62 |
| | | 3.6.6 证书验证管理 | 68 |
| | | 3.6.7 证书同步设置 | 69 |
| | | 3.6.8 数字信封管理 | 70 |
| | 3.7 | 日志管理 | 72 |
| | | 3.7.1 日志设置 | 72 |
| | | 3.7.2 日志审计(仅审计员可见) | 74 |
| | | 3.7.3 故障日志 | 79 |
| | 3.8 | 预警管理 | 82 |
| | | 3.8.1 预警设置 | 82 |
| | | 3.8.2 预警列表 | 83 |
| | 3.9 | 国标密钥管理 | 85 |



| 4 5 | 初始化配量常见问题及 | | |
|--------|------------|----------|----|
| | 対体化両里 | 学友心体住田止雨 | 05 |
| | 3.9.5 | 私钥权限码 | 94 |
| | 3.9.4 | 密钥批量管理 | 92 |
| | 3.9.3 | 对称密钥 | 90 |
| | 3.9.2 | RSA密钥 | |
| | 3.9.1 | SM2密钥 | 85 |
| | | | |



1 概述

1.1 简介

签名验签服务器严格按照国家密码管理局 GM/T 0029-2014《签名验签服务器技术 规范》等技术规范进行设计,产品已取得国家密码管理局商用密码检测中心颁发的商用 密码产品认证证书,支持国家密码管理局认可的密码算法,能够为各类系统提供数据签 名和验签、基于数字证书的身份认证、基于数字证书的加解密等安全保护,以保证关键 业务信息的真实性、完整性和不可否认性。产品可以应用于电子商务、CA 认证中心、 网上银行等服务器端,提供高强度和高效率的密码服务。

2 产品安装说明

2.1 安装环境要求

产品为 2U 机架式服务器,安装前须准备 2U 机位、2 个 AC220V/50Hz 交流电源插座、 设备接入网络环境(设备 IP 地址、路由、安全策略等)。

2.2 产品安装

签名验签服务器部署在局域网内,只为局域网内的应用实体和用户服务,不能接入 互联网,为局域网外的用户使用。

设备部署可以是一台应用服务器对应一台签名验签服务器,也可以一对多、多对一、 多对多。

3 产品操作说明

将测试 PC 的 IP 配置为 192. 168. 3. *网段后,浏览器访问 https://192. 168. 3. 3, 进入登录页面。系统首次打开登录页面如 0,**默认登录用户名 fisherman,口令 fisherman** 及验证码。

注意:此处默认登录用户名及口令为可配置,即可根据实际情况自定义默认用户 名及口令。





图3-1 默认登录页面

首先点击【**下载工具**】,如0,弹出后下载Setup.exe程序。执行安装程序完成组件 安装。如0。



图3-2下载工具



| 👸 安装程序 - UKEY服务管理控件 | _ | | \times |
|---|-----------------------------|-------|----------|
| 选择额外任务 您想执行什么额外任务 ? | | C | |
| 选择您希望安装程序安装 UKEY服务管理控件 时执行的额外任 步 继续安装。 | 务,再归 | 点击 下一 | |
| ☑ 创建桌面快捷方式图标 | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| <上一步® 下一步 | ; (<u>N</u>) > | 取 | 消 |

图3-3安装程序

安装完成后重新刷新网页,输入验证码后,点击【登录】按钮即可登录。如0。

| 签名验签服务器 | 器 (V2.0.0) |
|---|--|
| 产品用于在服务端为应用实体提供基于PKI体系和数字证书的数字签名、验证签名等运算功能。保证关键业务信息的真实性、完整性和不可否认性。 ▲ 高性能 ◆ 兼容性 ◆ 高性能 ◆ 兼容性 ◆ 运行态势监控 ◆ 敏感信息防护 | 你好, 欢迎登录 UKEY登录 ※ K1426230906B1126 ● ◎刷新 ▲ 输入PIN码 ● ● 输入PIN码 ● ● 输入验证码 ● ● 输入验证码 ● ● 第入验证码 ● ● 第入验证码 ● |
| | |

图3-4默认用户登录



用户默认用户登录之后进入首页,如图3-5。该页面显示当前系统的基本信息,主 要包括以下四项:

数量信息:

显示用户数量、证书数量、实体数量和并发连接数。

系统状态:

显示管理员访问次数统计和系统资源占用情况。

网络状态:

显示当前设备各网口的网络状态。

模块状态:

显示设备的加密卡状态。

| ★ 主界面 ▲ 用户管理 ~ | ● 0 用户数量 | | 0 证书数量 | 0 实体数量 | の #发连接 |
|---|----------------|-----------|------------------|------------------|---|
| | 七日内管理员访问统计 | | | | ③ 系统持续运行封问: 0天0小8142分58秒 |
| | 1 0.42 0.43 | 0 0104 | 0-45 01-48 | © ⊙ Q. A. A ★≡ | 系统操作监测 CPU CPU CPU CPU CPU CPU 使用 の ドゲの の ドゲの の の の の の の の の の の の の の |
| | | | | | 模块状态 |
| | 网络状态实时监控 | 岡口名称 | IP地址 | | -RUA: IF |
| | ••• | eth0 | 192.188.3.95 | 1, 0.02Mbps | |
| | ••• | eth1 | 192.168.4.3 | 14 0.00Mbps | |
| | | eth2 | 192.168.5.3 | †4 0.00Mbps | |
| | ••• | eth3 | 192.168.6.3 | †4 0.00Mbps | |

图3-5 默认用户首页

点击左侧导航栏【用户管理】下的【系统用户管理】菜单添加新用户,如0。点击 "新建用户"按钮,插入UKEY到电脑,点击"刷新"会在用户令牌显示插入的UKEY序列 号,如图3-7。

| 华 翼很 HUAYI MICRO | 散电- -ELECTRONI | F cs | | | | |
|----------------------------|-------------------|----------------|--------------------|---------|--------------|----------|
| ▲ 士田西 | | | | | | |
| 二 用户管理 | ^ | 用户管理 | | | ↑ 首页 | / 系统用户管理 |
| ◎ 系统用户管理 | | 用户列表 | 角色 初志 | + 新建用户 | 口令有效期设置 器 | |
| | | | 12 件数5年 石田子 | 页数目: 10 | 0-0共0 区 | < > >1 |
| | | | | | | |
| | | | | | | |
| | | | 图3-6系统用户管理 | | | |
| 亲 | 新建用 | 户 | | | \times | |
| | 0 | 请输入 | 8填项进行用户添加 | | | |
| | *选 | 择角色: | ● 管理员 ○ 操作员 ○ 审计员 | | | |
| | *用 | 户令牌: | K1426190507B4069 • | の刷新 | | |
| | * 솟 | 牌口令: | 输入口令 | | | |
| | | | 带*星号的数据项为必填项 | | | |

图3-7新建用户

【审计员】,点击【确定】按钮完成用户添加。如0。

输入令牌口令(默认口令12345678),选择该用户是【管理员】、【操作员】还是

确定

取消



| 新建用户 | | | × |
|---------------|-------------------|-------|---|
| i 请输入: | 必填项进行用户添加 | | |
| *选择角色: | ● 管理员 ○ 操作员 ○ 审计员 | | |
| *用户令牌: | K1426190507B4069 | ▼ ○刷新 | |
| *令牌口令: | | | |
| | 带*星号的数据项为必填项 | | |
| | | 确定取消 | |

图3-8新建用户

在系统用户管理功能中创建管理员、操作员、审计员用户,并绑定Ukey后,点击右 上角用户图标,选择"退出系统"如0,退出默认用户访问界面,再次进入系统登录页 面,如0。



图3-9退出系统





图3-10 登录页面

选择要登录的UKEY序列号,输入UKEY口令和验证码,点击【登录】。管理员登录成 功之后进入管理员界面首页,如0。

| ★ 主界面 | | 3 | | 0 | • 0 | <i>.</i> 0 |
|-----------------------------|-------|------------|-----------|--------------|-------------------------|-------------------------|
| 🔲 应用实体 | 本管理 | 用户数量 | | 证书数量 | 实体数量 | 并发连接 |
| 数据备份 | 分恢复 | 七日内管理员访问统计 | | | | ⑤ 系统持续运行时间:0天0小时45分10秒 |
| ₊→ 双机热备 | S管理 | | | | @ 🔿 🍳 🕴 | 3 ♠ = |
| ▲ 用户管理 | E ~ | 2 | | | / | 系统硬件监测 |
| ⁰✿ 设备管理 | ∎ v | | | | | - $ -$ |
| ☞ 征书管理 | ∎ v | 1 | | | | CPU 内存 硬盘 1% 18% 37% |
| > 日志管理 | ŧ v | | | | | CPU使用率 内存使用率 硬盘使用率 |
| ▲ 预警管理 | ŧ v | 01-02 0 | • 1-03 | 01-04 01-05 | 01-05 01-07 | 01-08 |
| Or 国标密钥 | 月管理 ~ | | | | | 模块状态 … |
| | | 网络状态实时监控 | | | | |
| | | 阿口間标 | 网口名称 | IP地址 | 当前阿速 | RAGE. IFW |
| | | ••• | eth0 | 192.188.3.95 | 1 0.00Mbps | |
| | | ••• | eth1 | 192.168.4.3 | 1, 0.00Mbps | |
| | | ••• | eth2 | 192.168.5.3 | 1, 0.00Mbps | |
| | | • | eth3 | 192.168.6.3 | † ₄ 0.00Mbps | |

图3-11 管理员首页

操作员登录成功之后进入操作员管理首页,如0。



| ^ | 主界面 应用实体管理 | | 3 用户数量 | | 0 证书数量 | 0 实体数量 | ジ 0 #发连续 |
|--------------------------------------|---------------|---|------------------|-------|--------------|-------------------------|-------------------------|
| Ð | 数据备份恢复 | | 七日内管理员访问统计 | | | | ③ 系统持续运行时间:0天0小时46分34秒 |
| $\stackrel{\rightarrow}{\leftarrow}$ | 双机热备管理 | | | | | | A = |
| °¢ | 设备管理 | v | 2 | | | | 系统硬件监测 |
| 17 | 证书管理 | ~ | | | | | |
| | 日志管理 | ~ | 1 | | | | CPU 内存 硬盘 1% 18% 37% |
| | 预警管理 | ~ | | | | | |
| 01 | 国标密钥管理 | ~ | 0 01-02 01-03 | 01-04 | 01-05 | 01-08 01-07 | 01-08 |
| | | | | | | | 模块状态 |
| | | | 网络状态实时监控 | | | | |
| | | | 阿口附标 | 网口名称 | IP地址 | 当前阿速 | |
| | | | ••• | eth0 | 192.188.3.95 | 1 0.00Mbps | |
| | | | ••• | eth1 | 192.168.4.3 | ‡ 0.00Mbps | |
| | | | m | eth2 | 192.168.5.3 | 1, 0.00Mbps | |
| | | | m | eth3 | 192.168.6.3 | τ ₁ 0.00Mbps | |

图3-12 操作员首页

审计员登录成功之后进入审计员管理首页,如0。

| ★ 主界面 ▶ 日志管理 ~ | 3 用户数量 | | 0 证书数量 | ● 实体数量 | ジ 0 _{井发连续} |
|---|--|-----------|------------------|-------------------------|-------------------------------|
| | 七日内管理员访问统计 | | | | ③ 系统持续运行时间: 0天0小时45分55秒 |
| | 21100_0014201430014300143001430014300143001430000000000 | 0 0104 | 0.05 01.05 | | |
| | | | | | 模块状态 |
| | 网络状态实时监控 网口图师 | 周口名称 | IP地址 | | 卡状态: 正常 |
| | in the second se | eth0 | 192.188.3.95 | 14 0.06Mbps | |
| | | eth1 | 192.168.4.3 | 1_ 0.00Mbps | |
| | | eth2 | 192.168.5.3 | 1 ₁ 0.00Mbps | |
| | I | eth3 | 192.168.6.3 | †4 0.00Mbps | |

图3-13 审计员首页

点击右上角用户图标,除了可对当前登录用户进行退出外,还可进行密码修改操作, 点击"修改密码",弹出修改界面如0。输入原口令以及新口令之后,点击确定即可完 成密码修改。



| | ● 管理员 K1426190507B4069 ● 修改密码 ● 退出系统 |
|---------------|--|
| 修改口令 | × |
| i 请输入! | 原口令和新口令进行口令修改 |
| *用户令牌: | K1426190507B4069 🗸 |
| *原口令: | 输入原口令 |
| *新口令: | 输入新口令 |
| *确认新口令: | 确认新口令 |
| | 带。星号的数据项为必填项 |
| | 确定取消 |

图3-14 修改口令

3.1 应用实体管理

应用实体管理页面显示应用实体的基本信息,包括应用实体名、密钥类型、密钥索 引号、密钥长度、签名证书状态、加密证书状态、加密密钥对状态、应用实体状态,界 面如 0。



用户手册

| 应用实体管理 | | | | | | | | | ↑ 首页 / 应用实体管理 |
|--------|--------------|--------|------------|-----|---------------|---------------------|---|-----------------|--------------------|
| 应用名称: | 输入应用实体名称进行 | 一搜索 | 2 査询 (2 重要 | | | | | | |
| 应用实体列表 | | | | | | | | + 新增应用实体 | ■粉成用实体 / 体衣PDF签章图片 |
| | arus-sete199 | warden | 3 | 255 | ₩±4ETD 使得入 | anniha LE TB 未登入 | (1993) (中日日日) (日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日 | 不可用 每页数目: 10 | #### #2 |

图3-15应用实体注册

新增应用实体时,点击"新增应用实体"按钮,选择密钥类型,输入应用名称、私 钥权限码、密钥索引号,点击【确定】。界面如 0。



| 新增应用实体 | | \times |
|-----------|---|----------|
| 1 应用实体基本信 | 高息。 19月1日——————————————————————————————————— | |
| *密钥类型: | ● SM2 ○ RSA | |
| *应用名称: | 测试SM2应用 | |
| *私钥权限码: | ••••• | |
| *确认私钥权限码: | ••••• | |
| *密钥索引号: | 1 | |
| 带相号的 | 数据项为必填项 | |
| | 确定取消 | i |

图3-16新增应用实体

点击【确定】即可完成应用实体的注册,应用实体对应密钥号的私钥权限码也会被 创建,此时会弹出"创建应用实体完成,但不可用,请在应用实体信息管理中完成其他 操作",需要导入证书应用实体才可用。界面如0。

警告

Х

确定

创建应用实体完成,但不可用,请在应用实体信息管理中完成其他操 作!



图3-17应用实体注册弹出框

应用实体列表显示所有注册的应用实体信息,包括应用实体信息的修改、签名/加 密证书的 P10 生成请求、签名/加密证书、加密密钥对的导入、签名/加密证书的下载、 pdf 签章验签、删除功能,界面如 0。

| 应用实 | 本管理 | | | | | | | | | ↑ 首页 / 应用实体管理 |
|-----|------|-----------|------|-----------|------|------|------|-------|----------|---|
| 应是 | 用名称: | 输入应用实体名称进 | 行搜索 | 9、査询 〇 亜重 | | | | | | |
| 应用实 | 体列表 | | | | | | | | + 新增应用实体 | ■ 删除应用实体 / 修改PDF签章图片 |
| | 序号 | 应用实体名称 | 密钥类型 | 密胡索引号 | 蜜铜长度 | 签名证书 | 加密证书 | 加密密钥对 | 状态 | 操作 |
| | 1 | 测试SM2应用 | SM2 | 3 | 256 | 未导入 | 未导入 | 未导入 | 不可用 | 修改 删除 更多操作 |
| | | | | | | | | | 每页数目: 10 | 1-1共1 に 生地P10満来 导入正书 下載正书 pd1怨章验答 |

图3-18应用实体功能操作

在想要操作的应用实体上,点击"修改",弹出对话界面,如 0,输入想要修改的 密钥类型、应用名称、私钥权限码、密钥索引号,点击确定,即可完成应用实体信息的 修改操作。



| 应用实体修改 | | \times |
|------------------|-------------|----------|
| i 应用实体基本保 | 急 | |
| *密钥类型: | ● SM2 ● RSA | |
| *应用名称: | 测试SM2应用 | |
| *私钥权限码: | ••••• | |
| *确认私钥权限码: | ••••• | |
| *密钥索引号: | 1 | |
| 带*星号的 | 数据项为必填项 | |
| | 确定取消 | Ĵ |

图3-19应用实体修改

在想要操作的应用实体上,点击"删除",弹出对话界面,如0,点击"确定",即 可删除对应的应用实体。



华翼微电子

图3-20应用实体删除

点击"更多操作"里的"生成 P10 请求", 弹出对话界面,如 0,输入部门、单位、城市、省份信息之后,点击【签名证书 P10 生成】、【加密证书 P10 生成】按钮,可以生成签名证书 P10 文件、加密证书 P10 文件并直接下载。



| 生成P10请求 | | × |
|---------------|------------------------|--------|
| i 请输入: | 必填项生成P10请求 | |
| *姓名: | 测试SM2应用 | |
| *部门: | | |
| *单位: | | |
| *城市: | | |
| *省份: | | |
| | 带*星号的数据项为必填项 | |
| | 签名证书P10生成 加密证书P10生成 取消 | μ μ |

图3-21生成P10请求

点击"更多操作"里的导入证书,弹出对话界面,如 0,可上传签名证书文件、加密证书文件、加密密钥对文件(P12 格式),上述文件需要分别导入,其中密码是指 P12 密码,需要手动填写。注:上传证书前需上传 CA 证书,具体可见 3.6.2CA 证书管理





图3-22导入证书

点击"更多操作"里的"下载证书",弹出证书下载窗口如 0,选择"下载签名证书"、"下载加密证书",可下载应用实体证书。



图3-23导入证书

点击"更多操作"里的"pdf 签章验签",弹出证书 pdf 签章/验签窗口如 0,上传 pdf 文件即可进行签章验签。



| pdf签章验签 | | | × |
|----------|-------|-------|----|
| PDF文件: 🕦 | | | |
| | | | |
| | PDF签章 | PDF验签 | 取消 |



PDF 签章:选择需要签章的 PDF 文件,点击【PDF 签章】即可签章 PDF,如0。签章 完成之后,会自动生成一个签章后的 PDF 文件,如0。

| pdf签章验签 | | | \times |
|----------------------------------|---------------------|-------|----------|
| PDF文件: 🕕 测试PDF.pdf | | | \odot |
| | PDF签章 图3-25PDF签章 | PDF验签 | 取消 |
| pdf签i 成功 PC 导入成功,已完成签章! | | 确定 | ×× |
| 📷 signed_23_测试Ppdf 🔺 | | | |

图3-26PDF签章完成

PDF 验签:选择自动生成的签章后的 PDF 文件,点击【PDF 验签】即可验签,如 0, 并弹出验签成功结果,如 0。





图3-28PDF验签完成

应用实体删除:勾选应用实体所在行前"□",可多选,点击【删除】,如0,在弹出的对话框中点击确定后可将应用实体删除,弹出对话框如0。

| 应用实 | 体管理 | • | | | | | | | | ↑ 首页 / 应用实体管理 |
|-----|------|------------|------|----------------|------|------|------|-------|----------|-------------------|
| 应用 | 用名称: | 输入应用实体名称进行 | フ捜索の | 査询 〇 重苦 | | | | | | |
| 应用实 | 体列表 | | | | | | | | + 新增应用实体 | ■ 删除应用实体 |
| | 序号 | 应用实体名称 | 密钥类型 | 废钥索引号 | 废钥长度 | 签名证书 | 加震证书 | 加密密钥对 | 状态 | 操作 |
| | 1 | 测试SM2应用 | SM2 | 3 | 256 | 未导入 | 未导入 | 未导入 | 不可用 | 修改 删除 更多操作 |
| | 2 | 测试SM2应用2 | SM2 | 4 | 256 | 未导入 | 未导入 | 未导入 | 不可用 | 修改 删除 更多操作 |
| | 3 | 测试SM2应用3 | SM2 | 5 | 256 | 未导入 | 未导入 | 未导入 | 不可用 | 修改 删除 更多操作 |
| | | | | | | | | | 每页数目: 10 | ▼ 1-3共3 I< < > >I |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

图3-29删除应用实体



| 确认 | × |
|--------------|-------|
| | |
| 确认删除所选应用实体吗? | |
| | 确定 取消 |

图3-30删除对话框

修改PDF签章图片:主要功能是替换系统原有签章图片进行PDF签章,界面如0,点 击按钮后弹窗如0.。可上传.bmp格式的图片作为pdf签章图片在签章后的pdf中进行展示。

| 应用实 | 体管理 | | | | | | | | | | ↑ 首页 | ī / 应用实 | 体管理 |
|-----|------|------------|------|-----------|------|------|------|-------|----------|-----------|------|-------------------|-----|
| 应用 | 用名称: | 输入应用实体名称进行 | 7搜索 | 9 査询 〇 重要 | | | | | | | | | |
| 应用实 | 体列表 | | | | | | | | + 新增应用实体 | ■ 删除应用实 | 体 🖊 | 修改PDF签) | 章图片 |
| | 序号 | 应用实体名称 | 密钥类型 | 密钥索引号 | 密钥长度 | 签名证书 | 加密证书 | 加密密钥对 | 状态 | | 操作 | | |
| | 1 | 测试SM2应用 | SM2 | 3 | 256 | 未导入 | 未导入 | 未导入 | 不可用 | 修改 | 删除 | 更多操作 | |
| | | | | | | | | | 每页数目: 1 | 0 🔹 1-1共1 | < | $\langle \rangle$ | > |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |

图3-31修改PDF签章图片



| 修改PDF签章图片 | × |
|-------------------------------|---|
| i 上传签章图片后,将替换系统原有签章图片进行PDF签章。 | |
| 签章图片: ◎ | |
| 上传取消 | |
| 图3-32上传签章图片 | |

3.2 数据备份恢复

选主要功能是实现对服务器数据的备份和恢复,界面内容如0。

| 数据备份恢复 | |
|----------------------------|--------------------------------|
| 数据备份 | 数据恢复 |
| \$ | \$ |
| 点由数据备份按相,登录Ukey完成数据备份。 | 点由数据仿复按钮,登录Ukey完成数据仿复。 数据恢复 |
| | |
| | |
| | |

图3-33数据备份恢复

3.2.1 数据备份

点击"数据备份"按钮,在弹出窗先点击【开始备份】按钮。界面如0。



| 登录Ukey | | × |
|---------------------|------|----|
| i 请插入Ukey依次输入口令进行登录 | | |
| | | |
| *UKEY1: | | 登录 |
| *UKEY2: | | 登录 |
| *UKEY3: | | 登录 |
| | | |
| *UKEY4: | | 登录 |
| *UKEY5: | | 登录 |
| 带*星号的数据项为必填项 | | |
| | | |
| 开始备份 | 完成备份 | 取消 |
| 图3-34开始备份 | | |

插入 UKey, 点击【刷新】按钮后显示 UKey 序列号。界面如 0。



| 登录Ukey | | | × |
|---------------|--------------------|------|----|
| i 请插入U | key依次输入口令进行登录 | | |
| *UKEY1: | K1426190507B4069 👻 | 刷新 | 登录 |
| *UKEY2: | - | | 登录 |
| *UKEY3: | - | | 登录 |
| *UKEY4: | - | | 登录 |
| *UKEY5: | ~ | | 登录 |
| : | 带*星号的数据项为必填项 | | |
| 开始备份 | | 完成备份 | 取消 |
| | 图3-35刷新 | | |

再点击【登录】按钮, 在弹出框页面输入 UKEY 对应口令后, 点击确定。界面如 0。



用户手册

| 登录Ukey | ; | × |
|------------|--------------------------|---|
| i 请插入Uke | ey依次输入口令进行登录 | |
| *UKEY1: | K1426190507B4069 🔹 刷新 登录 | |
| 输入口令 | × | |
| *口令: | | |
| | 确定取消 | |
| *UKEY5: | | |
| # ∗ | ¹ 星号的数据项为必填项 | |
| 开始备份 | 完成备份取消 | |

图3-36UKEY登录

顺着前面步骤依次把 5 个 Ukey 配置完成,备份密钥分割成 5 份,分别存储到 5 个 Ukey 中,完成全部密钥登录操作之后,点击【完成备份】按钮如 0,可将设备配置数据 及密钥以密文形式下载到本地。界面如 0。



| 登录Ukey | | | | | × |
|---------------|---|----------------|--------------|--------|---|
| 〕 请插入U | key依次输入口令进行登录 | | | | |
| *UKEY1: | K1426190507B4069 | ~ | | 登录 | |
| *UKEY2: | K1426230302B4970 | • | | 登录 | |
| *UKEY3: | K1426230302B4964 | • | | 受录 | |
| *UKEY4: | K1426230302B4963 | - | | 爱录 | |
| *UKEY5: | K1426221104B3964 | • | | 受录 | |
| 带*星号的数据项为必填项 | | | | | |
| 开始备份 | | | 完成备份 | 取消 | |
| 图3-37完成备份 | | | | | |
| | ABC12345678_2023_11_10_14_35_15.zip https://192.188.3.96/pro-api/downloadBacku | p?fileName=ABC | 12345678_202 | 3_11_1 | × |
| i | <u>在文件夹中显示</u> | | | | |

图3-38备份文件

3.2.2 **数据恢复**

点击【数据恢复】按钮,插入数据备份时所用到的 5 个 Ukey 中的任意 3 个 Ukey, 界面如 0。



| 登录Ukey | | | | | × |
|---------------|------------------|---|------|----|---|
| う 请依次捕 | 插入Ukey输入口令进行登录 | | | | |
| *UKEY1: | K1426190507B4069 | • | 刷新 | 登录 | |
| *UKEY2: | | - | | 登录 | |
| *UKEY3: | | • | | 登录 | |
| | 带*星号的数据项为必填项 | | | | |
| | | | 开始恢复 | 取消 | |

图3-39数据恢复

点击【登录】按钮,在弹出框页面输入 UKEY 对应口令后,点击确定。界面如 0。

| 登录Ukey | | × |
|----------------|---------------------|----|
| i 请依次插) | Ukey输入口令进行登录 | |
| | | _ |
| 输入口令 | | × |
| *口令: | ****** | |
| | 确定 | 取消 |
| ά π | *星号的数据项为必填项 开始恢复 | 取消 |



图3-40数据恢复登录

顺着前面步骤依次把 3 个 Ukey 配置完成之后,版本号则自动填入下拉列表中,选择需要恢复的版本号,并选择对应版本号的备份文件。界面如 0。

| 登录Ukey | | | | | × |
|----------------------|---------------------------|------------|---------|----|---|
| i 请依次据 | 積入Ukey输入口令进行登录 | | | | |
| *UKEY1: | K1426190524B4573 | • | | 登录 | |
| *UKEY2: | K1426221103B0300 | • | | 登录 | |
| *UKEY3: | K1424170223B4046 | • | | 登录 | |
| *版本: | BTS-XC5000-HG_2024_02_20_ | 09_48_07 | | • | |
| <mark>*</mark> 备份文件: | BTS-XC5000-HG_2024_0 | 2_20_09_48 | _07.zip | | |
| | 带*星号的数据项为必填项 | | | | |
| | | | 开始恢复 | 取消 | |

图3-41选择版本

点击【开始恢复】按钮,弹出确认提示框,如图 3-42。



| 登录Ukey | × |
|--|---|
| 请依次插入Ukey输入口令进行登录 | |
| *UKEY1: K1426190524B4573 ▼ 刷新 登录 | |
| *(确认 × 是否确认恢复到指定备份? 确定 取消 | |
| *备份文件: ① BTS-XC5000-HG_2024_02_20_09_48_07.zip | |
| ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● | |
| 开始恢复 | i |

图3-42恢复确认

点击【确定】后开始恢复,如0,恢复完成后提示重启设备后生效,如0。





3.3 双机热备管理

在选择双机热备功能状态开启模式下,才可配置双机热备功能;选中"启动双机热备"选项,选择主服务设备网口,输入主服务 IP、另一台热备设备 IP 地址、虚拟路由



ID, 点击"保存配置",完成此设备的双机热备配置,界面如 0。要真正实现双机热备 功能,还需要在另一台签名验签服务器上按上述配置完成双机热备配置,同时保证双台 设备间网络可达。注意:做双机热备的两台设备 IP 地址必须在同一网段,虚拟路由 ID 必须相同,且同一网段下如果存在多组双机热备,每组的虚拟路由 ID 必须互不相同, 建议使用主服务 ip 最后一组数作为虚拟路由 ID 可保证不与同网段其他组热备冲突。 配置双机热备前提条件:必须保证创建并使用相同的 Ukey 操作,同时建议分别初始化 两台设备,保证双机热备时两台设备数据一致。注:主、备双机热备配置完成之后,此 时并未数据同步,若实现数据同步两台设备需依次点击"开启数据同步"按钮。当开 启后会有主备状态的区分,双机热备功能状态分别为:已开启,当前为主机;已开启, 当前为备机,如0。开启过程如0。

| 双机热备管理 | | ♠ 首页 / 双机热备管理 |
|------------------|------------------|---------------|
| 热备设置 | | |
| 双机热备功能状态: | 已关闭 | |
| *双机热备功能设置: | ● 启动双机装备 ○关闭双机装备 | |
| * 主服务设备网口: | eth0 - | |
| * 主服务IP: | 192.168.3.5 | |
| * 另一台设备IP: | 192.168.3.207 | |
| * 虚拟路由ID(1-255): | 11 | |
| | ☐ 保存品面 ① 开启数据局涉 | |
| | | |

图3-45双机热备



| 热备设置 | | | | |
|------------------|---|--|--|--|
| 双机热备功能状态: | 已开启,当前为主机 | | | |
| * 双机热备功能设置: | ●启动双机热备 ○关闭双机热备 | | | |
| * 主服务设备网口: | eth0 - | | | |
| * 主服务IP: | 192.168.3.5 | | | |
| * 另一台设备IP: | 192.168.3.207 | | | |
| * 虚拟路由ID(1-255): | 11 | | | |
| | 保存配置 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ | | | |
| 图3 | -46开启数据同步 | | | |
| 正在开启数据同步 | | | | |
| 数据同步开启成功 | | | | |

图3-47数据同步开启成功

注意:数据同步开启后请访问主服务 IP 进行操作,请勿再访问子服务 IP 操作(详 情请看"常见问题及解答")。



关闭双机热备时选择"关闭双机热备",再点击保存配置,如0所示。

注意:关闭双机热备时,需访问两台设备的子服务IP,分别进行关闭操作,不可直接在主服务IP上进行关闭。若已开启数据同步,关闭双机热备后需手动重启才可继续操作设备。



图3-48关闭双机热备

3.4 用户管理

3.4.1 **系统用户管理**

系统用户管理显示当前系统所有用户的信息,具体显示内容包括用户角色、对应 UKEY 的序号、登陆状态,以及新建用户、设置用户口令过期天数、删除用户、修改口


令。界面如 0。

| 列表 | | | | + 新建用户 💠 口令有效期设置 🔟 删除用户 |
|----|------------------|-----|----|--|
| | 今講座列号 个 | 角色 | 状态 | 提作 |
| | K1426190507B4069 | 审计员 | 周线 | 修改口令 删除 |
| | K1426221103B0598 | 管理员 | 在线 | 修改口令 删除 |
| ו | K142623030284964 | 管理员 | 南战 | 様な口令 副除 毎页数目: 10 ▼ 1-3 共 3 (< < > > |
| | | | | |

图3-49系统用户管理

点击"新建用户"按钮,选择添加的用户角色(管理员、操作员或审计员),插入 Ukey,若未识别 Ukey 信息,可点击"刷新"按钮,输入令牌口令(默认口令 12345678), 以及新口令和确认新口令(新口令由 8-16 位数字、大小写字母或特殊字符的三种或三 种以上组合),点击"确定",即可完成新增管理员、操作员或审计员添加操作,操作界 面如 0。注:新口令与原令牌口令不能相同。



| 新建用户 | | \times |
|---------------|------------------------|----------|
| i 请输入! | 必填项进行用户添加 | |
| *选择角色: | ◉ 管理员 ○ 操作员 ○ 审计员 | |
| *用户令牌: | K1426230302B4964 ・ の刷新 | |
| *原口令: | ••••• | |
| *新口令: | ••••• | |
| *确认新口令: | ••••• | |
| | 带*星号的数据项为必填项 | |
| | 确定取消 | |

图3-50新建用户

点击"口令有效期设置"可设置用户口令过期天数。在用户口令过期天数输入天数, 点击【确定】完成用户口令过期天数配置(设置为0时关闭用户口令过期提醒)。如0。

| 口令有效期设置 | × |
|--------------|-------|
| 修改用户口令的有效期 | |
| *口令有效期: 10 | Ę |
| 带*星号的数据项为必填项 | |
| | 确定 取消 |



0.

图3-51口令有效期设置

勾选用户所在行前的"□",点击"删除用户"如 0,可将该用户删除。弹出框如

| 用户列表 | | | | + 新建用户 🗘 口令有效期设置 🗐 删除用 | Þ |
|------|------------------|-----|----|---------------------------|---|
| | 令跳床列号 个 | 角色 | 状态 | 操作 | |
| | K1426190507B4069 | 管理员 | 在线 | 修改口令 删除 | |
| | K1426221103B0598 | 管理员 | 商线 | 修改口令 删除 | |
| | 1 | | | 毎页数目: 10 ▼ 1-2 共 2 1< < > | |





点击用户列表中的"修改口令",可修改对应用户的口令(需插入该用户绑定的 Ukey),新口令不能和原口令相同且新口令和确认新口令必须一致,输入原口令、新口 令以及确认新口令后(口令由 8-16 位数字、大小写字母或特殊字符的三种或三种以上 组合),点击【确定】,验证通过后,即可完成用户 Ukey 口令的修改,界面如 0。



| 修改口令 | | × |
|--------------|------------------|---|
| i 请次插 | 入Ukey输入口令进行口令修改 | |
| *用户令牌: | K1426190507B4069 | |
| *原囗令: | ••••• | |
| *新口令: | •••••• | |
| *确认新口令: | •••••• | |
| | 带*星号的数据项为必填项 | |
| | 确定 取消 | |

图3-54修改口令

点击用户列表中的"删除"如 0,弹出提示框后,点击确定可单独删除对应的用 户信息,如 0。

| | | | 工 朝延用厂 ♥ Ц♥特30時後直 凹 動除用/ |
|------------------|-----|----|-----------------------------|
| ◇ ⇒ 读序列号 个 | 角色 | 状态 | 操作 |
| K1426190507B4069 | 管理员 | 在线 | 修改口令 删除 |
| K1426221103B0598 | 管理员 | 高线 | 修改口令 删除 |
| | | | 毎页数目: 10 ▼ 1-2 共 2 1< < > > |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |



图3-56删除提示框

3.4.2 **restful用户管理**

华翼微电子

restful 用户管理显示当前系统所有 restful 用户的信息,具体显示内容包括用户 名和备注信息,以及新建用户、删除用户、修改口令和用户搜索功能。如 0。

| restful用户管理 | | ♠ 首页 / restful用户管理 |
|----------------------|-----------------------------|--|
| 用户名: 输入搜索用户名称 | 备注: 输入搜索备注 Q 機索 Q 満空 | |
| 用户列表 | | +新建用户 圖 删除用户 |
| □ 用户名 个 | 备注 | 操作 |
| TestUser01 | | ●改口◆ 副除 每页成目: 10 ▼ 1-1 共1 I< < > >1 |

图3-57restful用户管理

点击"新建用户"按钮,输入用户名、口令和确认口令后,点击"确定",即可完成新增 restful 用户操作,用户名只能由 4 到 16 位(字母,数字,下划线,减号)组成,操作界面如图 3-57 图 3-58。



| 新建用户 | | × |
|--------------|--------------|---|
| i 请输入 | 必填项进行用户添加 | |
| *用户名: | TestUser01 | |
| *囗令: | ••••• | |
| *确认口令: | ••••• | |
| 备注: | 备注信息 | |
| | 带*星号的数据项为必填项 | |
| | 确定 取消 | |

图3-58新增restful用户

勾选用户所在行前的"□",点击"删除用户"如错误!未找到引用源。,可将该用 户删除。弹出框如 0。

| 用户名: 输入搜索用户名称 | 备注: 输入搜索备注 | Q 税款 O 测空 |
|----------------------|-------------------|-----------------------------|
| 用户列表 | | + 新建用户 🖀 新時用户 |
| ☑ 用户名 | 番注 | 操作 |
| TestUser01 | | 修改口令 删除 |
| TestUser02 | | 修改口令 删除 |
| TestUser03 | | 修改口令 翻除 |
| | | 毎页数目: 10 ▼ 1-3 共 3 < < > > |
| | | |
| | | |
| | | |
| | | |

图3-59选择用户





华翼微电子

图3-60用户删除

点击用户列表中的"修改口令",可修改对应用户的口令,输入新口令以及确认新口令后,点击【确定】,即可完成 restful 用户口令的修改,界面如 0。

| 修改口令 | | × |
|--------------|--------------|---|
| i 请输入 | 必填项进行用户口令修改 | |
| *用户名: | TestUser01 | |
| *新口令: | 输入新口令 | |
| *确认新口令: | 确认新口令 | |
| : | 带*星号的数据项为必填项 | |
| | 确定取 | 肖 |

图3-61修改口令

点击用户列表中的"删除" 如 0, 弹出提示框后, 点击确定可单独删除对应的用



户信息,如0。

| | 用户名: 输入搜索用户名称 | 编注: 输入搜索备注 | 9. 読友 〇 清空 |
|------|---------------|-------------------|-----------------------------|
| 用户列表 | ŧx | | + 新雄用户 富 副除用户 |
| | 用户名 | 备注 | 操作 |
| | TestUser01 | | 修改口令 副除 |
| | TestUser02 | | 修改口令 删除 |
| | TestUser03 | | 修改口令 删除 |
| | | | 毎页数目: 10 ▼ 1-3 共 3 < < > > |
| | | | |

图3-62删除用户

| 确认 | | × |
|----|---------------------|---|
| | | |
| | 确定要删除用户TestUser01吗? | |
| | 确定取 | 肖 |

图3-63删除提示框

搜索框中"用户名"和"备注"支持模糊查询,可按条件查询出对应的用户信息, 清空按钮用于重置查询条件,界面如0。

| 用户名: 01 | 备注: 输入搜索备注 | Q. 前主 C 消空 |
|------------|------------|---|
| 用户列表 | | + 新建用户 日 開始用户 |
| □ 用户名 | 酱注 | 操作 |
| TestUser01 | | 様改□◇ 無除 毎页数目: 10 ▼ 1-1 共 1 (< < > >) |



图3-64按条件搜索

3.5 设备管理

3.5.1 初始化

初始化设备需要先开启初始化功能,再点击【初始化设备】,才可进行设备初始化。 点击【开启初始化功能】,可以开启初始化设备功能;点击【关闭初始化功能】按钮, 可以关闭初始化设备功能,界面如 0。注:初始化会清除设备所有的用户、数据、配置 和密钥,初始化前请做好备份。

| 初始代 | ↑ 首页 / 设备管理 / 初始化 |
|--|-------------------|
| ● 开京(約)出化(5)第 ⑦ 約)出代(2)第 ◎ 美国(約)出代(2)第 | |
| | |
| | |

图3-65初始化设备

点击【开启初始化功能】后,【初始化设备】按钮为可点击状态,如 0,然后就可 以通过点击【初始化设备】进行设备初始化。



图3-66初始化设备

点击【初始化设备】后会弹出确认窗口,如0。点击确定后进行初始化,初始化完 成后弹出初始化完成提示,点击确定回到登录页面。如0,初始化过程大约需要一分钟。



| 确认 | × |
|---------------------------------|--------|
| 初始化会删除所有已产生的密钥、应用、证书、用户等数 续? | 据, 确定继 |
| 确定 | 取消 |
| 图3-67初始化确认 | |
| 完成 | |
| 初始化成功,请重新登录 | |
| | 确定 |
| | |

图3-68初始化完成

若禁用点击【初始化设备】,可点击【关闭初始化设备】如0 ,点击【关闭初始 化功能】后,【初始化设备】按钮为禁用状态,如0。



图3-70关闭初始化功能后



3.5.2 系统升级

系统升级页面可以使用升级包升级系统,界面如 0。点击【系统升级】,在弹出框 中选择升级文件,点击"开始升级",进行系统升级,界面如 0。

| 系统升级 | | ń i | 首页 / 设备管理 / 系统升级 |
|------------------------|-----------|------------------|-------------------------|
| 当前使用的系统版本为: 系统更新时间: | | | ★ 系统升级 |
| 升级记录 ◎ ゅう | 升级记录 | | |
| | 没有数据 | | |
| | | 每页数目: 10 ▼ 0-0 共 | 0 < < > > |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | 图3-71系统升级 | | |
| 系统升级 | | | × |
| i 请上传系统升级文件 | | | |
| | | | |
| *升级文件: 🔘 | | | |
| · | | | |
| 带*星号的数据项为必填 | 项 | | |
| | | 开始升级 | 取消 |
| | | | |

图3-72升级文件

3.5.3 设备信息

设备信息显示生产厂商信息、硬件版本信息、软件版本信息、产品序列号、设备名称信息。界面如 0。



| 4 | 签名验签服务器 | | ➡ 操作员,欢迎进入管理 | 里系统 |
|--------------------------------------|---------|--------|-------------------|---------------------------|
| A | 主界面 | | 设备信息 | |
| | 应用实体管理 | | | |
| Ð | 数据备份恢复 | | 基本信息 | |
| $\stackrel{\rightarrow}{\leftarrow}$ | 双机热备管理 | | 设备名 | 称: 签名验签服务器 |
| ° o | 设备管理 | ^ | 生产厂 | 商: 山东华翼微电子信息技术股份有限公司 |
| \bigcirc | 初始化 | | 硬件版 | 本: 飞腾 |
| \bigcirc | 系统升级 | | 软件版 | 本: V2.0.0.4421.240308_STD |
| 0 | 设备信息 | | 产品型 | 号: YASVS-2000 |
| \bigcirc | 重启/关机 | | 序列 | 号: 021501049240131B0414 |
| \bigcirc | 系统配置 | | | |
| \bigcirc | 时间源设置 | | | |
| \bigcirc | 服务管理 | | | |
| \bigcirc | 设备自检 | | | |
| | 证书管理 | \sim | ©2020-2024 山东华翼微电 | 子信息技术股份有限公司 版权所有 保留所有权利 |
| | | | | 图3-73设备信息 |

3.5.4 重启/关机

提供在重启/关机页面手动重启和关机的功能,界面如0。

| 重启/关机 | | | |
|-------|--|--|--|
| 设备重启 | | | |
| ♀ 重启 | | | |
| 设备关机 | | | |
| ○ 关机 | | | |

图3-74重启/关机界面

点击"重启",会弹出"设备正在重启,稍后请重新登录!"提示信息框,如0。点 击确定后,自动跳转至登录页面,待重启成功之后,用户可刷新登录页面重新登录。点 击"关机"后,会弹出"设备正在关机,无法正常使用!"提示信息框,如0。点击确 定后,自动退出登录。 **注:1、用户可不断刷新登录页面确认是否重启成功。2、为避** 免浏览器缓存,在登录之前可刷新登录页面,确定重启成功后,再登录。



用户手册

| 成功 | |
|------------------|----|
| 设备正在重启, 稍后请重新登录! | I |
| | 确定 |
| 图3-75重启提示 | 1 |
| 成功 | |
| 设备正在关机,无法继续使用! | |
| | 确定 |

图3-76关机提示

3.5.5 **系统配置**

系统配置页面包含"网络配置"、"路由配置"、"白名单配置"以及"时间配置"功能。界面如 0。

| 系统配置 | | ★ 首页 / 设备管理 / 系统配置 |
|----------|------------------|--------------------|
| 配置项 | | |
| 网络配置路由配置 | 白名单配置 时间配置 | |
| * 网卡端口 | 1: eth0 × | |
| * 网口类型 | 2: ●普通機式 ○聚合模式 | |
| * 网络类型 | 2: • IPV4 OIPV6 | |
| * IPV4 | 4: 192.188.3.96 | |
| * 子网掩辞 | 3: 255.255.255.0 | |
| * 默认网乡 | ŧ: 192.188.3.1 | |
| | ■ 保存配置 び 应用配置 | |
| | | |
| | | |
| | | |
| | | |



网络配置:网络配置可以配置设备的网络参数。选择网卡端口、网口模式、网络类型,输入 IP 地址、子网掩码、网关信息,点击【保存】,即可完成网络配置操作,IPV4 界面如 0, IPV6 界面如 0。网口模式选择聚合模式,可以将所有配置成聚合模式的网口 聚合为一个 IP, 界面如 0。

| 系统配置 | | ♠ 首页 / 设备管理 / 系統配置 |
|------|--|--------------------|
| 配置项 | | |
| 网络配置 | 路由配置 白名单配置 时间配置 | |
| | * 阿卡端口: eth0 * | |
| | * 网口樊型: ⑧ 普通機式 ○聚合機式 | |
| | * 网络类型: ④IPV4 〇IPV6 | |
| | IPV4: 192.188.3.99 | |
| | 子网境码: 255.255.255.0 | |
| | 默认网关: 192.188.3.1 | |
| | 6 保存配置 · · · · · · · · · · · · · · · · · · · | |
| | | |
| | | |
| | | |

图3-781PV4网络设置

| 系统配置 | | ↑ 首页 / 设备管理 / 系统配置 |
|------|-----------------------|--------------------|
| 配置项 | | |
| 网络配置 | 路由配置 白名单配置 时间配置 | |
| | * 网卡编曰: eth0 * | |
| | • 网口浅型: ● 普通模式 ○ 聚合模式 | |
| | * 网络类型: 〇IPV4 | |
| | IPV6: ae86:: | |
| | 前缀长: 64 | |
| | 默认网关: :: | |
| | | |
| | | |
| | | |
| | | |

图3-791PV6网络设置

用户手册

| 系统配置 | | ★ 首页 / 设备管理 / 系统配置 |
|----------|-----------------|--------------------|
| 配置项 | | |
| 网络配置路由配置 | 白名单配置 时间配置 | |
| * 网卡端口 | : eth0 - | |
| * 网口类型 | : 〇 普通模式 ④ 聚合模式 | |
| * 网络类型 | : OIPV4 | |
| IPV6 | : ae86:: | |
| 前缀长 | : 64 | |
| 默认网关 | £ | |
| | B 保存配置 · 应用配置 | |
| | | |
| | | |

图3-80聚合模式

配置聚合模式后,网卡端口新增"bond"选项,选择bond端口后可配置聚合模式以 及聚合IP等信息。其中聚合模式包括0[~]6七种模式分别是:0平衡轮循策略、1主-备份策 略、2平衡策略、3广播策略、4动态链接聚合、5适配器传输负载均衡、6适配器适应性 负载均衡,如0。。**注:除模式1以外其余模式需要路由器支持。**

| 配置项 | | |
|------|------------------|---------------|
| 网络配置 | 置 路由配置 | 白名单配置 时间配置 |
| | * 网卡端口: | bond |
| | *聚合模式: | 模式1 |
| | * 网络 <u>类型</u> : | |
| | IPV4: | 192.188.3.99 |
| | 子网掩码: | 255.255.255.0 |
| | 默认网关: | 192.188.3.1 |
| | | |
| | | ☐ 保存配置 |

图3-81聚合模式

网络配置需要重启设备后才会生效。如0。保存配置成功后,点击【应用配置】则



无需重启设备,会使当前网络配置立即生效。如0。注:请确认不同网口不在同一网段 内,否则可能导致网口的网络无法使用。

网络配置保存成功, 重启设备或应用配置后生效



应用确认

应用配置会使当前网络配置立即生效,是否确定要应用配置?



X

图3-83应用配置

路由配置:路由地址的 IP 配置,需要配置 IP 地址、子网掩码和网关。如 0。

| 充配置 | | | | | ▲ 首页 / 设备管理 / 系統配 |
|-----------|-------------|---------------|-------------|--------------------------|--|
| 置项 | | | | | |
| 网络配置 路由配置 | 自名单配置 时间配置 | | | | |
| 路由列表 | | | | | + 新増 回 删除 |
| | 目标网络 | 子网播码/前缀 | 网关地证 | 网络类型 | 操作 |
| | 192.188.3.0 | 255.255.255.0 | 192.188.3.1 | ipv4 每页数目: 10 - 1-1 # | 1111年1日1日日 11日日 - 11日日 11日日 - 11日 11日日 11日日 1 |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |



点击【新增】按钮, 在弹出框中选择网络类型 IPV4 或 IPV6, IPV4: 输入目标网络、 子网掩码和网关地址; IPV6: 输入目标网络、前缀长度和网关地址。点击【确定】, 可 新增路由, 如 0。

| 新增路由 | | × | 新增路由 | | × |
|----------------|--------------|---|--------------|--------------|---|
| i 请输入: | 必填项进行路由添加 | | 请 输入4 | 必填项进行路由添加 | |
| * 网络类型: | ●IPv4 ○IPv6 | | * 网络类型: | | |
| *目标网络: | 输入目标网络 | | *目标网络: | 输入目标网络 | |
| *子网掩码: | 输入子网掩码 | | *前缀长度: | 输入前缀长度 | |
| * 网关地址: | 输入网关地址 | | *网关地址: | 输入网关地址 | |
| | 带中星号的数据项为必填项 | | 1 | 带"星号的数据项为必填项 | |
| | 确定 取消 | | | 确定 | j |

图3-851PV4/1PV6路由配置

勾选目标网络前的"□",可多选,点击【删除】即可删除选中路由地址,或点击列表操作列的"删除"如0。弹出删除确认框,如0。点击确定完成删除。

| 路由配置 路由列表 | 白名单配置 时间配置 | | | | +新增 国 删除 |
|---------------------|-------------|-----------------|-------------|---------------|----------------|
| ■ 序号 | 目标网络 | 子网编码/前缀 | 阿关地址 | 网络类型 | 操作 |
| 1 | 192.188.3.0 | 255.255.255.0 | 192.188.3.1 | ipv4 | 删除 |
| 2 | 192.188.3.2 | 255.255.255.255 | 192.188.3.1 | ipv4 | 题除 |
| | | | | 每页数目: 10 ▼ 1- | 3,#,3 K < > >I |



| 删除确认 | | × |
|--------------|----|----|
| 确认要删除选择的路由吗? | | |
| | 确定 | 取消 |

图3-87删除确认

白名单配置: 白名单的 IP 配置可以是 IP 网段或 IP 地址, 配置 IP 之后, 只允许白 名单中的设备访问服务器, 白名单之外的设备不允许访问, 如 0。(白名单列表为空时, 白名单功能关闭)

| 配置 | 顷 | | | | | |
|----|------|--------|-------|-------------------------------|--------------------|---------------------------------------|
| | 网络配置 | E 路由配置 | 白名单配置 | 时间配置 | | |
| | 白名单列 | し表 | | | | + 新増 圖 删除 |
| | | 序号 个 | | IP | 备注 | 操作 |
| | | 1 | | 192.168.18.140 | | 删除 |
| | | 2 | | 192.168.18.140-192.168.18.150 | | 删除 |
| | | | | | 每页数目: 10 - 1-2 共 2 | $ \langle \rangle \rangle > \rangle$ |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

图3-88白名单配置

点击【新增】,在 IP 栏输入 IP 或者 IP 段,可以在备注栏输入白名单备注,点击【确 定】,可新增白名单,如 0。



| 新增白名单 | | × |
|--------------|--------------|---|
| i 请输入 | 必填项进行白名单添加 | |
| *IP: | 输入白名单IP | |
| 备注: | 输入备注信息 | |
| | 带*星号的数据项为必填项 | |
| | 确定取消 | |

图3-89新增白名单

勾选白名单前的"□",点击【删除】即可删除选中白名单,或通过点击列表中操 作列的"删除",进行单个白名单的删除操作如 0。当删除的不是最后一个白名单时, 提示如 0。当最后一个白名单被删除时提示如 0。

| 置项 | | | | |
|----------------|-------------------------------|-----------|------------------|----------------|
| 网络配置路由配置 白名单配置 | 时间配置 | | | |
| 白名单列表 | | | | +新増 回 删除 |
| ☑ 序号个 | IP | | 酱注 | 操作 |
| Z 1 | 192.168.18.140 | | | 删除 |
| 2 | 192.168.18.140-192.168.18.150 | | 每页数目: 10 ¥ 1-2共2 | 部除 く く > > |
| | | | | |
| | | 图3-90删除白名 | 単 | |



华翼微电子

图3-92删除全部白名单

时间配置:时间可以配置当前系统时间,在设置系统时间输入栏输入系统时间,点 击【设置】,可修改系统当前时间。界面如 0。



| H | È | 千皿 | |
|---|---|----|--|
| 用 | 厂 | 十四 | |

| 路由配置 | 白名单配 | 医 时间配置 |
|--------|------------------|------------------------|
| | | |
| | | |
| * 当前系统 | 充时间: | ③ 2023-11-13 13:09:08 |
| * 设置系统 | 充时间: | ⑤ 请选择日期 |
| | | ∂ 设置 |
| | * 当前系统 * 设置系统 | * 当前系统时间: * 设置系统时间: |

图3-93时间配置

3.5.6 时间源设置

时间源配置包括 NTP 对时设置、北斗对时设置。界面如 0。注:设备分为带授时卡和不带授时卡两种版本,只有带授时卡的设备才会显示"北斗对时设置",否则不显示。

| 何勝设置項 NTP対时设置 NTP対时设置 C研究 1000545月288。1 | | | |
|--|---------|------|------------------------------|
| NTP対射设置 北斗对射设置 NTP対射设置 已开启 | | | |
| NTP対射设置 已开启 | | | |
| ANT DO-POT FORD | | | |
| INTEXSUS/ADMAN | 分钟 🖬 确定 | | |
| | | | |
| NTP对时列表 | | | + 新塔 圖 翻除 |
| 服务器IP | 端口号 | 对时周期 | 操作 |
| 192.168.3.209 | 123 | 1 | 题 除 |
| | | | 毎页数目: 10 ▼ 1-1 共 1 (< < > >) |
| | | | |

图3-94时间源配置

NTP 对时设置: NTP 对时列表内容为空时,代表未配置 NTP 对时,此时 NTP 对时设置显示为"已关闭"状态,如 0。

| NTP对时设置 已关闭 | | | | |
|-------------|-----|------|---|-------------|
| *NTP对时周期: 2 | 分钟 | 确定 | | |
| | | | | |
| NTP对时列表 | | | | |
| | | | | + 新増 回 删除 |
| ✓ 服务器IP | 端口号 | 对时周期 | | 操作 |
| | | 没有数据 | | |
| | | | (三) · · · · · · · · · · · · · · · · · · · | 0#0 K < N N |



图3-95已关闭

点击"新增"按钮,弹出对话框如 0,输入 NTP 服务器 IP 地址、点击"确定",即 可开启 NTP 对时设置,自动与 NTP 服务器进行时间同步。如 0 所示。

| 新增NTP对时设置 | | | | × |
|--|-----------------|-----------|----|----------|
| i 请输入必填现 | 贡新增NTP对时 | | | |
| *服务器IP: 输 | 入服务器IP | | | |
| 带*星 | 号的数据项为必填项 | | | |
| | | | 确定 | 取消 |
| | | 图3-96对时设置 | | |
| 时间源设置项 | | | | |
| NTP对时设置 北斗对时设置 NTP对时设置 已开启 | | _ | | |
| *NTP对时周期: 1 | 分钟 3 | 确定 | | |
| NTP对时列表 | | | | +新增 圖 删除 |
| □ 服务器IP | 端口号 | 对时周期 | | 操作 |
| 192.188.3.1 | 123 | 1 | | 删除 |

图3-97对时开启

NTP 对时周期输入框可修改 NTP 对时周期设置,点击"确定",即可修改所有服务器 IP 的对时周期。如 0 所示。



| 成功 | | | × |
|--|-----------------|----------------|---------------------------|
| 修改NTP对时周期 | 成功! | | |
| | | | 确定 |
| 时间游设置项 NTP対时设置 北斗对时设置 | | | |
| NTP均制设置 田府創 *NTP2时间期: 5 | <u> 위부</u> 립 예교 | | |
| NTP对时列表 | | | + 1677 8 1814 |
| 副务器IP 192.188.3.1 | 123 | 9105月1月1月 5 | iiift |
| | | | 每页数目: 10 ▼ 1-1共1 < < > > |

图3-98对时周期

北斗对时设置:点击"北斗对时设置"标签切换到北斗对时设置页面,如0所示。 输入北斗定时对时周期,点击"开启",即可自动与北斗卫星进行对时,时间同步。点 击"关闭",即可关闭北斗对时服务。

| 时间源设置项 | | | |
|---------|----------|---|----|
| NTP对时设置 | 北斗对时设置 | | |
| 北斗对时设置 | 已关闭 | | |
| * 363 | 斗定时对时周期: | 2 | 分钟 |
| 日 开启 | 日 关闭 | | |

图3-99北斗对时设置

3.5.7 **服务管理**

服务管理页面可配置 SSH、国密 SSH、国密 FTP、国密 SSL、SNMP 服务的开启和关闭。以及 SNMP 团体字的功能。如 0。

用户手册



| 服务管理 | | ♠ 首页 / 设备管理 / 服 |
|-------|---------------------|-----------------|
| 服务 | | |
| | * SSH: ① 已关闭 | |
| * [| e唐SSH: ① 已关闭 | |
| * | a密FTP: OD 已关闭 | |
| | 国密SSL: ① 日关闭 | |
| | SNMP: C 已开启 | |
| * SNM | value3 保存 | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

图3-100服务管理

点击按钮即可切换对应服务的开启和关闭状态。如0。



图3-101关闭/开启状态

点击【保存】即可保存 SNMP 团体名并生效,页面上显示修改后的 SNMP 团体名,如 0。注:从安全角度考虑,尽量避免将 snmp 的团体字修改为 public 这一默认值。



图3-102SNMP团体字

3.5.8 **设备自检**

设备自检页面中可以设置设备定时自检时间,设置时间后,每天到达设置时间后,



会自动进行自检。手动填写时间的时分,点击设置按钮进行设置,如0。

| 设备自检 | | ↑ 首页 / 设备管理 / 设备自检 |
|----------|------------------|--------------------|
| 设备自检 | | |
| 随机数自检: | 成功 | |
| SM1自检: | 成功 | |
| SM2自检: | 成功 | |
| SM3自检: | 成功 | |
| SM4自检: | 成功 | |
| 密钥完整性检测: | 成功 | |
| 数据完整性检测: | 成功 | |
| 卡状态自检: | 成功 | |
| 设备自检: | 成功 | |
| 上次自检时间: | 2023-11-13 12:00 | |
| 定时自检时间: | 🛱 12:00 × | |
| | □ 保存配置 ○ 手动自检 | |

图3-103设备自检

页面中显示自检结果,可以点击手动自检按钮手动执行一次自检,如0。

| 设备自检 | |
|----------|------------------|
| 随机数自检: | 成功 |
| SM1自检: | 成功 |
| SM2自检: | 成功 |
| SM3自检: | 成功 |
| SM4自检: | 成功 |
| 密钥完整性检测: | 成功 |
| 数据完整性检测: | 成功 |
| 卡状态自检: | 成功 |
| 设备自检: | 成功 |
| 上次自检时间: | 2023-11-13 14:46 |
| 定时自检时间: | 🗎 12:00 × |
| | □ 保存配置 ● 手动自检 |

图3-104手动自检

3.6 证书管理

3.6.1 **证书查询设置**

证书查询设置包括 OCSP 在线查询、CRL 自动更新两种方式的设置。选择 "OCSP 在 线查询",输入 OCSP URL 地址、点击 "保存",完成 OCSP 在线查询方式设置。界面如 0。

用户手册



| 证书會詢设置 | ★ 首页 / 证书管理 / 证书查询 |
|---|--------------------|
| 证书查询方式 | |
| OCSP在线查词 CRL自动更新 | |
| ・OCSP URL地址: http://192.168.100.30:8080/fm-ocsp/ocspServl | |
| * 支持证书OCSP在线验证: ○是 ⑧ 否 | |
| B Q# | |
| | |
| | |

图3-1050CSP在线查询

选择 "CRL 自动更新", 输入 LDAP 服务器的 URL 地址、基本 DN 信息,选择是否自动更新,点击"保存",完成 CRL 自动更新设置。界面如 0。

| 正书查询方式 | | |
|---------------|-----------------|-----------------|
| OCSP在线查询 CRLE | 自动更新 | |
| * LDAP URL | .地址: LDAP://192 | .168.100.30:389 |
| * 基乙 | ≴DN: c=cn | |
| * 自动 | 更新: ◉是 ○否 | |
| | 🖬 保存 | |
| | | |



3.6.2 CA证书管理

CA 证书管理包括 CA 证书、证书链的导入、证书信息展示和证书删除,支持多 CA 证书的导入。界面如 0。

| CA证书管理 | | | | | | | | ↑ 首页 / | 证书管 | e / C | A证书管 | 官理 |
|--------|----|----|-----|------|-----|-------|------|--------|-----|-------|---|------|
| CA证书列表 | | | | | | | | | Ð | 导入 | 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | life |
| ✓ 序号 | 类型 | 主題 | 颁发者 | | 有效期 | | | | | 操作 | | |
| | | | | 没有数据 | | | | | | | | |
| | | | | | | 每页数目: | 10 💌 | 0-0共0 | < | < | > | >1 |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

图3-107CA证书管理

点击【导入】, 在弹出框中选择证书类型, 以及证书或证书链文件, 点击"导入" 就可以导入 CA 证书或证书链。如 0 所示。

| 导入CA证书 | × |
|--------------------|---|
| i 请输入必填项导入证书或证书链文件 | |
| ★证书类型: | |
| *证书文件: ① | |
| 带*星号的数据项为必填项 | |
| 导入 取消 | |

图3-108导入CA证书

勾选证书所在行前的"□",点击【删除】,或者点击 CA 证书列表中操作列的"删除,"可以删除所选证书的信息。如 0。

| CA证书 | 管理 | | | | ★ 首页 / 证书管理 / | CA证书管理 |
|------|----|-----|---------------------------------------|---|---|--------|
| CA证书 | 列表 | | | | 日 导入 | 圓 删除 |
| | 序号 | 类型 | 主题 | 原茨吉 | 有效期 | 操作 |
| | 1 | SM2 | C=CN,ST=1,L=1,O=1,OU=21,CN=213 | C=CN,ST=山东甾,L=威海市,O=研发,OU=fisec,E=123@63.com,CN=子ca | 2022-09-10 00:00:00 - 2025-04-18 00:00:00 | 删除 |
| | 2 | RSA | C=CN,ST=1,L=1,O=1,OU=1,CN=冒烟测试RSA应用实体 | C=CN5,ST=SD5,L=WH5,O=FM5,OU=J5,CN=C5 | 2023-10-04 00:00:00 - 2024-10-18 00:00:00 | 删除 |
| | | | | 每页数目 | : 10 👻 1-2共2 🖂 < | > > |
| | | | | | | |
| | | | | | | |
| | | | | | | |

图3-109删除CA证书

3.6.3 CRL管理

CRL 管理包括 CRL 的导入、显示与删除功能,如 0。点击"CRL 导入"选择需要上传的 CRL 文件,再点击"导入"即可上传 CRL 文件。如 0。



| CRL管理 | | | | | ↑首页 / 证书管理 / CRL管理 |
|-------|-----|------|------|------------|--------------------------------------|
| CRL列表 | | | | | CRL导入回 副除 |
| ☑ 序列号 | 颁发者 | 算法类型 | 更新时间 | 下次更新时间 | 操作 |
| | | | 没有叙措 | 每页数目: 10 (| b0拱0 K < > >I |
| | | | | | |
| | | | | | |



| 导入CRL证书 | | | × |
|--------------|------|----|----|
| i 请输入必填项导入CR | L证书 | | |
| *CRL文件: 🕦 | | | |
| 带*星号的数据项 | 为必填项 | | |
| | | 导入 | 取消 |

图3-111导入CRL

勾选 CRL 所在行前的"□",点击右上"删除"按钮,或者点击 CRL 列表里操作列的删除,即可将选中的 CRL 删除。界面如 0。

| CRL管理 | | | | | ♠ 首页 / 证书管理 | / CRL管理 |
|-------|------------|---|------------|---------------------|---------------------|-----------------------------|
| CRL列表 | | | | | 包 CRL导入 | ■ 删除 |
| | 9 | 颁发者 | 算法类型 | 更新时间 | 下次更新时间 | 操作 |
| 040 | 0402022c5c | C=CN,ST=山东省,L=威海市,O=研发,OU=fisec,E=123@63.com,CN=子ca | Sm3WithSm2 | 2023-05-22 15:00:00 | 2023-05-23 15:00:00 | 删除 |
| | | | | 每页数目: | 10 - 1-1 共 1 区 区 | \rightarrow \rightarrow |
| | | | | | | |
| | | | | | | |

图3-112CRL删除



3.6.4 **用户证书管理**

用户证书管理包括用户签名证书、加密证书的导入、用户证书查询和用户证书删除 功能,界面如 0。

| 用户证书 | 书管理 | | | | | | | | | | 🕈 首页 / 证 | 日本管理 /) | 用户证书管理 |
|------|-----|-------|---------------------|-------------|----|------------------|------|--------------------------|--------------------------|------|-------------|----------|----------------------|
| | 主题: | 输入关键字 | F进行搜索 | 证书状态: | 全部 | • | 오 搜索 | ○ 清空 | | | | | |
| 用户证书 | 书列表 | | | | | | | | | | 3 | 〕证书导入 | 间 删除 |
| | 序号 | 类型 | 主題 | | | 序列号 | | 有效期 | | | 状态 | | 操作 |
| | 1 | SM2 | C=CN,ST=1,L=1,O=1,O | U=21,CN=213 | | 73976004f33969d0 | | 2022-09-10 00:00:00至2025 | -04-18 00:00:00 每页数目: | 10 - | 正常 1-1共1 | ic c | 期除 > > |

图3-113用户证书管理

点击【证书导入】,选择证书类型和用户证书文件就可以导入用户证书,如0。

| 用户证书导入 | × |
|----------------------|------|
| 请输入必填项导入用户证书 | |
| *证书类型: 💿 签名证书 🔘 加密证书 | |
| *证书文件: 🕦 | |
| 带*星号的数据项为必填项 | |
| | 导入取消 |

图3-114导入用户证书

输入对应的"主题",选择证书状态,点击【搜索】按钮显示所对应的信息,【清空】 可以清除输入的内容。如 0。

| 主题: | 输入关键字进行搜索 | 证书状态: | 全部 | ♥ 建数 ○ 消空 |
|-----|-----------|-------|----|--|
| | | | | 图3-115用户证书搜索 |



勾选证书所在行前的"□",可多选,点击右上角【删除】按钮可以删除所选证书 的信息,或点击用户证书列表中操作列的删除,可以删除对应证书。如0,点击【删除】, 提示是否删除的确认框,如0。



图3-117证书删除确认框

3.6.5 **设备证书管理**

设备证书管理包括设备密钥的 P10 文件生成及设备证书的导入,其中设备密钥固定 密钥索引号为 0,设备证书包括为设备签名证书和设备加密密钥(P12 格式)的导入。 如 0。

| 华翼微电子 ITATI MICRO-ELECTRONICS | | | | | Ę | 目户手册 |
|----------------------------------|----|---------|----------------|------------|----------------------|------|
| 设备证此管理 | | | | | ★ 首而 / 江北管理 / 沿名江北 | 管理 |
| | | | | | HX / CPBE / KBCP | |
| 议备址书列表 | 進明 | 应列号 | ✿ 管理密钥生成 主题 | | 2 设备加密密钥导入 首 部 退作 | |
| | XE | ב נייהו | 没有数据 | DANKET | 2011 1- | |
| | | | | 每页数目: 10 👻 | 0-0共0 < > | м |
| | | | | | | |
| | | | | | | |

图3-118设备证书管理

点击【管理密钥生成】按钮,在弹出框中展示管理密钥的状态(管理密钥默认为已 生成状态),点击【生成】可以重新生成管理密钥。如 0。

| 管理密钥生成 | | | × |
|--------|----------|---|-----|
| • 点击生 | 成可生成管理密钥 | | |
| * 状态: | 已生成 | Ŧ | 成取消 |

图3-119管理密钥生成

点击设备证书管理页面的【生成 P10】,在弹出框中选择密钥类型后,点击弹出框中的"生成 P10"按钮,如 0。如果密钥已经生成会提示"密钥已经生成,继续密钥将覆盖重新生成"如 0。点击"确定"后弹出生成 P10 框,输入姓名、部门、单位、城市、省份点击【提交】,可生成设备 P10 请求文件,如 0。下载窗口如 0。



| 生成P10 | | × |
|--------------------|-------|----------|
| i 请输入必填项生成设备密钥P10 | | |
| * 密钥类型: ○RSA ()SM2 | | |
| * 密钥号: 0 |] | |
| | 生成P10 | 取消 |
| 图3-120生成P10 | | |
| 确认 | | \times |
| 密钥已经生成,继续密钥将覆盖重新生成 | | |
| | 确定 | 取消 |
| 图3-121重复生成提示框 | | |



| 生成P10 | × |
|-----------------|---|
| i 请输入必填项生成P10请求 | |
| *姓名: | |
| *部门: | |
| *单位: | |
| *城市: | |
| *省份: | |
| 带*星号的数据项为必填项 | |
| 提交取消 | i |
| 图3-122生成P10(2) | |
| 确认 | × |
| 生成P10成功,是否下载? | |
| 确定 | É |



点击【设备证书导入】选择要导入的设备证书如0,点击【导入】就可以导入设备 证书,导入成功后证书会显示在下方设备证书列表中。界面如0。



| 设备证书导入 | × |
|----------------|------|
| i 请输入必填项导入设备证书 | |
| * 文件路径: 🕕 | |
| 带*星号的数据项为必填项 | |
| | 导入取消 |
| | |

图3-124设备证书导入

| 设备证书管理 | | | | ↑ 首页 / 证书管理 / : | 设备证书管理 |
|--------|-----|------------------|--|---|-------------|
| 设备证书列表 | | | | ◆ 管理密明生成 ◆ 生成P10 回 设备证书导入 回 设备加密密明导入 | ■ 删除 |
| □ 序号 | 类型 | 序列号 | 主题 | 有效明 | 操作 |
| | SM2 | 551b41c8365f0141 | C=CN,ST=123,L=1323,O=123,OU=123,CN=123 | 2023-09-10 00:00:00至2025-04-18 00:00:00 每页数目: 10 * 1-1 共 1 I < < | ₩I₩ > >1 |

图3-125设备证书列表

点击【设备加密密钥导入】选择加密密钥文件,输入密码,点击【导入】就可以导 入设备加密密钥如0。



| 设备加密密钥导入 | | × |
|-----------|-----------------|----|
| i 请输入必填项导 | 注入设备加密密钥 | |
| * 加密密钥文件: | ● P12加密秘钥对.pfx | |
| * 密码: | ••••• | |
| 带*星号的 | 数据项为必填项 | |
| | 导入 | 取消 |

图3-126设备加密密钥导入

点击设备证书列表中的"删除"如0,弹出提示框后,点击确定可删除对应的设备 证书信息,如0。

| 设备证 | 设备证书管理 ↑ 首页 / 证书 | | | | | | | |
|--------|--------------------------|-----|------------------|--|---|----|--|--|
| 设备证书列表 | | | | | | | | |
| | 序号 | 类型 | 序列号 | 主题 | 有效期 | 操作 | | |
| | 1 | SM2 | 551b41c8365f0141 | C=CN,ST=123,L=1323,O=123,OU=123,CN=123 | 2023-09-10 00:00:00至2025-04-18 00:00:00 每页数目: 10 平 1-1 共 1 | | | |

图3-127删除设备证书





图3-128删除提示框

勾选证书所在行前的"□",可多选,点击右上角【删除】按钮可以批量删除所选 证书的信息如0。

| 设备证书管理 | | | | | ★ 首页 / 证书管理 / 设备证书管理 | | |
|--------|-----|-----|------------------|--|---|------|--|
| 设备证 | 书列表 | | | ◆ 曾理密明生成 | | 圆 删除 | |
| | 序号 | 类型 | 序列号 | 主题 | 有效期 | 操作 | |
| | 1 | SM2 | 551b41c8365f0141 | C=CN,ST=123,L=1323,O=123,OU=123,CN=123 | 2023-09-10 00:00:00至2025-04-18 00:00:00 | 删除 | |
| | 2 | RSA | 15f73d903b2a0a6b | C=CN,ST=测试省份,L=测试域市,O=测试单位,OU=测试部门,CN=测试设备证书 | 2024-01-01 00:00:00至2025-01-14 00:00:00 | 删除 | |
| | | | | | 毎页数目: 10 ▼ 1-2共2 < < | > > | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

图3-129设备证书多选删除

3.6.6 **证书验证管理**

华翼微电子

证书验证管理包括验证证书有效期、验证证书签名有效性、验证证书是否在 CRL 中功能,点击"保存",即可完成证书验证方式设置,界面如 0。
用户手册



| 证书验证管理 | ▲ 首页 / 证书管理 / 证书验证管理 |
|------------------------|----------------------|
| 证书验证 | |
| *验证证书有效期: | |
| *验证证书签名有效性:) 0 是 () 否 | |
| * 验证是否在CRL中: 〇是 ④否 | |
| B (97) | |
| | |
| | |

图3-130证书验证管理

3.6.7 **证书同步设置**

证书同步设置可以用于主服务向从服务进行证书同步,包括 CA 证书、CRL 证书以 及用户证书,这些证书的新增以及更新操作都会同步到从服务。选择是否是主服务器, 以及是否开启证书同步。主服务设置如图 3-131。注:只有主服务器开启了证书同步, 从服务才能进行连接。一台主服务器可以配置多台从服务器。证书的同步周期是 1 分钟。

| 证书同步设置 | ♠ 首页 / 证书管理 / 证书同步设置 |
|-----------------|----------------------|
| 同步设置 | |
| *是否是主服务器: ◎雪 ○否 | |
| * 开启证书同步: ⑧是 〇百 | |
| a (27) | |
| | |
| | |
| | |

图3-131证书同步设置

是否是主服务器选择否且开启证书同步选择是从服务"是否是主服务器"选择否, 即才可配置主服务 IP 和端口号信息,点击保存即可开启同步主服务器证书的功能如 0。 关闭证书同步功能仅需将"开启证书同步"选择"否",点击保存即可。



| 同步设置 | | | |
|------|----------|--------------|--|
| * 是 | 否是主服务器: | ○是◎否 | |
| * | 开启证书同步: | ●是○否 | |
| | * 主服务IP: | 192.188.3.88 | |
| | * 端口号: | 2022 | |
| | | 日 保存 | |
| | | | |

图3-132证书同步设置

3.6.8 **数字信封管理**

华翼微电子

数字信封管理包括生成数字信封和数字信封解封(注:仅支持 SM2)生成数字信封 需要先创建 SM2 应用实体并导入加密证书。如 0。

| 数字信封管理 | | | ♠ 首页 / 设备管理 / 数字信封管理 |
|--------|---------|--------|----------------------|
| 生成数字信封 | | | |
| | * 加密证书: | • | |
| | * 文件路径: | 0 | |
| | | â 2.18 | |
| 数字信封解封 | | | |
| | * 应用实体: | 213 * | |
| | * 文件路径: | 0 | |
| | | â M3t | |

图3-133数字信封管理

选择加密证书和所需文件,点击【生成】就可以生成数字信封。如0,数字信封文件生成成功,弹出是否下载弹出框,点击【确认】,下载数字信封文件,如0。



| 生成数字信封 | * 加密证书: C=CN,ST=sd,L=wh,O=fm,OU=ser,CN=Test86SM2 マ * 文件路径: ① 测试PDF.pdf ② | |
|--------|---|----------|
| | 图3-134生成数字信封 | |
| 确认 | | \times |
| 制作数学 | 信封成功, 是否下载! | |
| | 确定 | 取消 |

图3-135下载数字信封

选择应用实体和所需文件,点击【解封】就可以实现数字信封解封,如0。数字信 封解封后,会弹出是否下载原文数据的确认框,点击【确认】后,下载原文数据文件(文 件后缀为.txt),如0。

| 数字信封解封 | | |
|---------|-----------|---|
| * 应用实体: | Test86SM2 | • |
| * 文件路径: | | 8 |
| | ∂ 解封 | |

图3-136数字信封解封



| 确认 | | \times |
|---------------------|----|----------|
| 数字信封解封成功,是否下载原文件数据! | | |
| | 确定 | 取消 |
| | | |
| decDigitalEnvloptxt | | |

图3-137下载原文件

3.7 日志管理

3.7.1 日志设置

日志设置包括日志等级的设置、Syslog 主机地址、清除日志、下载主服务日志功能。界面如 0。

| 日志设置 | | ▲ 首页 / 日志管理 / 日志设置 |
|-------------|-----------------------|--------------------|
| 日志设置 | | |
| 日志等级: | DEBUG * | |
| Syslog主机地址: | 192.168.18.227 | |
| | ■ 成存设置 清除日志 ± 下载主服务日志 | |

图3-138日志设置

日志等级分为三个等级,分别错误日志 ERROR、调试日志 DEBUG、一般日志 INFO。 错误日志 ERROR:只记录页面操作错误或接口调用错误时的日志;

调试日志 DEBUG:记录重要功能调试信息的日志,同时包含错误日志 ERROR;

一般日志 INFO: 记录详细处理过程信息日志, 同时包含错误日志 ERROR 和调试日志 DEBUG。

界面如 0。选择日志等级,点击【保存设置】,可完成日志等级的修改。



| 日志管理 | | | |
|------|----------|-------|--|
| | 日志等级: | ERROR | |
| Sys | log主机地址: | INFO | |
| | | DEBUG | |
| | | ERROR | |

图3-139日志等级

若存在 Syslog 日志服务器,可在 Syslog 主机地址进行 IP 设置,点击【保存设置】,可完成配置。界面如 0。

| 日志管理 | | |
|------|-------------|---|
| | 日志等级: | ERROR |
| | Syslog主机地址: | 192.168.18.227 |
| | | □ 保存设置 □ 清除日志 土 下载主服务日志 |



点击【清除日志】,可对系统存储的日志数据进行删除。界面如0。

确认
送
该操作会删除所有的服务日志,确定执行?注:清除前请提前做好备份
取消



图3-141清除确认

点击【下载主服务日志】,可将系统主服务日志直接下载到本地。下载的文件如0。



图3-142下载日志文件

3.7.2 日志审计(仅审计员可见)

日志审计列表显示查询到的日志信息,包括令牌序列号、操作信息、操作时间、HMAC 和审计状态。界面如 0。

| 日志审 | t | | | | | ♠ 首页 | / 日志管理 / 日志审计 |
|-----|------|------------------|---------------------|---------------------|--|-----------|---------------|
| 起 | 上时间: | 田 开始日期 - 約 | ā束日期 令牌序列号 : | | Q. 施效 C 重面 | | |
| 日志列 | ŧ | | | | (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) | 导出XML 。 | 日志导出WEBTRENDS |
| | 序号 | 令牌序列号 | 操作信息 | 操作时间 | HMAC | 审计状态 | 操作 |
| | 8695 | K1426230302B4963 | 审计员登录成功 | 2024-01-08 11:28:13 | 41a2b9b48ca82dc76a1ef1f34534ca545505c48277f4d287619f1c94c8490057 | 未审计 | 审计 删除 |
| | 8693 | K1426221103B0598 | 证书验证失败 | 2024-01-05 12:15:26 | 0bedf7a33176a1b353c3521db675003a46701ed8d7827f6eca8db1ea78a82996 | 未审计 | 审计 删除 |
| | 8691 | K1426221103B0598 | 用户证书删除成功 | 2024-01-05 12:15:23 | d0e02416a13c602fc18cba58c8e2e96c4e3fd2520dbcdee3f862983468a503aa | 未审计 | 审计 删除 |
| | 8689 | K1426221103B0598 | 证书导入失败: 该证书标识已存在 | 2024-01-05 12:15:20 | d6468b2f02bfa2632539e5e3f6c061d7b011bc58269eebe328744c4fa30db348 | 未审计 | 审计 删除 |
| | 8687 | K1426221103B0598 | CA证书删除成功 | 2024-01-05 12:15:01 | dc8ec6eff931770d3cbff3017208830704f51f504d07f1cfa324d53e71e3b97b | 未审计 | 审计 删除 |
| | 8685 | K1426221103B0598 | CA证书删除成功 | 2024-01-05 12:14:59 | 558040efb35a9ea5c5acb1f18798ad1576e2838aae913466f51abfaaf887dba9 | 未审计 | 审计 删除 |
| | 8683 | K1426221103B0598 | 证书验证失败 | 2024-01-05 12:14:41 | 726d1187fdc892e7c2a91bdda529a98ecf749fc8145be40b25b2fd5735a5878a | 未审计 | 审计 删除 |
| | 8681 | K1426221103B0598 | 证书验证失败 | 2024-01-05 12:14:39 | 2281c1811aafbf528dbbe2e655a4ac9d19e12fdb7681fa28bd18e99bd3b9187d | 未审计 | 审计 删除 |
| | 8679 | K1426221103B0598 | 证书导入成功 | 2024-01-05 12:14:34 | a28067bd4748fb805ba5c938ea6f1c890e90359f7a4875177b2512100c400689 | 未审计 | 审计 删除 |
| | 8677 | K1426221103B0598 | 证书验证失败 | 2024-01-05 12:14:25 | cb4888c40c8ff91afb5af8369f12b15f18bce4474774384687ebc454475ab176 | 未审计 | 审计 删除 |
| | | | | | 每页数目: 10 👻 1- | 10 共 4203 | I< < > >I |

图3-143日志审计

可以通过输入令牌序列号或者日志时间,点击【搜索】按钮显示所对应的信息,点击【重置】按钮可以清除输入的查询条件。界面如 0。

| 审计管理 | | | | | | |
|-------|----------|------|--------|------|------|--|
| 起止时间: | □ 开始日期 - | 结束日期 | 令牌序列号: | Q 搜索 | ● 重置 | |
| | | | | | | |

图3-144日志查询

选择需要审计的日志所在行,勾选序号所在行前"□",可多选,点击【审计】,或 点击列表对应记录所在操作列的"审计"按钮,如0,日志审计完成之后,弹出日志审



计完成提示框(此处审计成功,为审计的操作成功,并不指审计结果),如0,日志审计 成功之后,审计状态为:审计通过,如0。若日志被篡改,则审计未通过,如0,序号 "37"原为"增加系统用户 K1426190507B4069 成功",被篡改为"删除系统用户 K1426190507B4069 成功",选择被篡改日志所在行,点击【审计】。审计完成之后,同 样弹出日志审计完成提示框,如0,日志审计失败之后,审计状态为:审计未通过,如 0。审计状态总共包括:未审计、审计通过、审计未通过(若日志被篡改,则审计未通 过)。

| 日志列表 | ų. | | | | ● 非計 回 删除 回 删除全部 也 日志导出CSV | 也 日志导出XML | 出 日志导出WEB | TRENDS |
|------|----|-----------|---------------|---------------------|--|-----------|-----------|--------|
| | 序号 | 令牌序列号 | 操作信息 | 操作时间 | НМАС | 审计状态 | 腰 | PE . |
| | 34 | fisherman | 清除主服务日志成功! | 2023-11-14 09:00:15 | 7c0ebc844008af1c079d68c1e04156b57c6598ad1e1ba5bedb086368b7e684cb | 未审计 | 审计 | 删除 |
| | 33 | fisherman | 数字信封解封成功! | 2023-11-14 08:33:54 | 2f3af1237aab2cb6aae65831eda8d40fc992608eb313243bb2c3c349d61ef76c | 未审计 | 审计 | 删除 |
| | 32 | fisherman | 数字信封解封成功! | 2023-11-14 08:33:29 | edca82499a6fe1a2e1a632982839ab826d2804cfa6d47f97da6f5f1c4921b34f | 未审计 | 审计 | 删除 |
| | 31 | fisherman | 数字信封解封成功! | 2023-11-14 08:32:54 | 4b13fca96d2677c795bcc40886e7e2c9ba98d4adbca8ddf0137c7e6a2501e562 | 来审计 | 审计 | 删除 |
| | 30 | fisherman | 数字信封解封成功! | 2023-11-14 08:32:48 | 57e3be5bb2cecc10f34d3828b3d25fc4c45f6c02e52275ca43046b8120034911 | 未审计 | 审计 | 删除 |
| | 29 | fisherman | 制作数字信封成功! | 2023-11-14 08:30:22 | c87398f83ae614801af54ae3b265e4d32a692dd9a9f498a444fcb4bc843cc47b | 未审计 | 审计 | 删除 |
| | 28 | fisherman | 管理员登录成功 | 2023-11-14 08:16:38 | fec2f25caa79b46fd9b4a824fb54819546c1c3ad6b27e11a6943c873ff5f82e9 | 未审计 | 审计 | 删除 |
| | 27 | fisherman | 1号密明导出SM2公钥成功 | 2023-11-13 16:47:54 | 250eb7fcdce9d41c760dbd0f827b8f5686e73c9cd2d5c6b79f272a8fccf6548f | 未审计 | 审计 | 删除 |
| | 26 | fisherman | 管理员登录成功 | 2023-11-13 16:47:42 | 00cddc9a025eb3423d4d7d5f72bdc007d351c2b91bdab59965c62c649a4366d2 | 末审计 | 审计 | 副除 |
| | 25 | fisherman | 管理员登录成功 | 2023-11-13 14:44:28 | 2abae22443032d85289ddefeb8bdae10211a8a63eb3db77c87c9544c843697a1 | 未审计 | 审计 | 删除 |
| | | | | | 每页数目: 10 | + 1-10共34 | 14 4 | > >1 |

图3-145审计日志



图3-146审计成功

| 日志列家 | 長 | | | | 会 申計 図 制除 図 制除全部 ▲ 日志导出CSV ▲ 日 | 志导出XML 📥 日編 | 5导出WEBTRENDS |
|------|----|-----------|---------------|---------------------|--|-------------|--------------|
| | 序号 | 令牌序列号 | 操作信息 | 接作时间 | HMAC | 审计状态 | 操作 |
| | 34 | fisherman | 清除主服务日志成功! | 2023-11-14 09:00:15 | 7c0ebc844008af1c079d68c1e04156b57c6598ad1e1ba5bedb086368b7e684cb | 审计通过 | 审计 删除 |
| | 33 | fisherman | 数字信封解封成功! | 2023-11-14 08:33:54 | 2f3af1237aab2cb6aae65831eda8d40fc992608eb313243bb2c3c349d61ef76c | 审计通过 | 审计 删除 |
| | 32 | fisherman | 数字信封解封成功! | 2023-11-14 08:33:29 | edca82499a6fe1a2e1a632982839ab826d2804cfa6d47f97da6f5f1c4921b34f | 审计通过 | 审计 删除 |
| | 31 | fisherman | 数字信封解封成功! | 2023-11-14 08:32:54 | 4b13fca96d2677c795bcc40886e7e2c9ba98d4adbca8ddf0137c7e6a2501e562 | 未审计 | 审计 删除 |
| | 30 | fisherman | 数字信封解封成功! | 2023-11-14 08:32:48 | 57e3be5bb2cecc10f34d3828b3d25fc4c45f6c02e52275ca43046b8120034911 | 未审计 | 审计 删除 |
| | 29 | fisherman | 制作数字信封成功! | 2023-11-14 08:30:22 | c87398f83ae614801af54ae3b265e4d32a692dd9a9f498a444fcb4bc843cc47b | 未审计 | 审计 删除 |
| | 28 | fisherman | 管理员登录成功 | 2023-11-14 08:16:38 | fec2f25caa79b46fd9b4a824fb54819546c1c3ad6b27e11a6943c873ff5f82e9 | 未审计 | 审计 删除 |
| | 27 | fisherman | 1号密钥导出SM2公钥成功 | 2023-11-13 16:47:54 | 250eb7fcdce9d41c760dbd0f827b8f5686e73c9cd2d5c6b79f272a8fccf6548f | 未审计 | 审计 删除 |
| | 26 | fisherman | 管理员登录成功 | 2023-11-13 16:47:42 | 00cddc9a025eb3423d4d7d5f72bdc007d351c2b91bdab59965c62c649a4366d2 | 未审计 | 审计 删除 |

图3-147日志审计通过结果



| 起] | 上时间: | □ 开始日期 | - 结束日期 令 牌序列号: | | Q 技次 C 重置 | | |
|------|------|-----------|--------------------------|---------------------|--|---------------|--------------|
| 日志列編 | ŧ | | | | ● 第計 回 影除 回 影除全部 当日志寺出CSV 当日 | 志导出XML 🛃 日洞 | 志导出WEBTRENDS |
| | 序号 | 令牌序列号 | 操作信息 | 操作时间 | HMAC | 审计状态 | 操作 |
| | 37 | fisherman | 删除系统用户K1426190507B4069成功 | 2023-11-14 09:26:11 | b03cc3d78d988eac7e4dc5536899fcc37fb0b223da0ebd0188803676ecd15c46 | 未审计 | 审计 删除 |
| | 34 | fisherman | 清除主服务日志成功! | 2023-11-14 09:00:15 | 7c0ebc844008af1c079d68c1e04156b57c6598ad1e1ba5bedb086368b7e684cb | 审计通过 | 审计 删除 |
| | 33 | fisherman | 数字信封解封成功! | 2023-11-14 08:33:54 | 2f3af1237aab2cb6aae65831eda8d40fc992608eb313243bb2c3c349d61ef76c | 审计通过 | 审计 删除 |
| | 32 | fisherman | 数字信封解封成功! | 2023-11-14 08:33:29 | edca82499a6fe1a2e1a632982839ab826d2804cfa6d47f97da6f5f1c4921b34f | 审计通过 | 审计 删除 |
| | 31 | fisherman | 数字信封解封成功! | 2023-11-14 08:32:54 | 4b13fca96d2677c795bcc40886e7e2c9ba98d4adbca8ddf0137c7e6a2501e562 | 未审计 | 审计 删除 |
| | 30 | fisherman | 数字信封解封成功! | 2023-11-14 08:32:48 | 57e3be5bb2cecc10f34d3828b3d25fc4c45f6c02e52275ca43046b8120034911 | 未审计 | 审计 删除 |
| | 29 | fisherman | 制作数字信封成功! | 2023-11-14 08:30:22 | c87398f83ae614801af54ae3b265e4d32a692dd9a9f498a444fcb4bc843cc47b | 未审计 | 审计 删除 |
| | 28 | fisherman | 管理员登录成功 | 2023-11-14 08:16:38 | fec2f25caa79b46fd9b4a824fb54819546c1c3ad6b27e11a6943c873ff5f82e9 | 未审计 | 审计 删除 |
| | 27 | fisherman | 1号密钥导出SM2公钥成功 | 2023-11-13 16:47:54 | 250eb7fcdce9d41c760dbd0f827b8f5686e73c9cd2d5c6b79f272a8fccf6548f | 未审计 | 审计 删除 |
| | | | | | 每页数目: 10 👻 | 1-10 共 36 🛛 🖂 | < > > |

图3-148日志篡改

审计成功!

图3-149审计动作完成

| 日志列 | ŧ | | | | 副除 圖除全部 也 日志导出CSV | ▲ 日志导出XML | 也 日志导出WE | BTRENDS |
|-----|----|-----------|--------------------------|---------------------|--|-----------|-----------------|---------|
| | 序号 | 令牌序列号 | 操作信息 | 操作时间 | HMAC | 审计状 | <u>تە</u> | 操作 |
| | 37 | fisherman | 删除系统用户K1426190507B4069成功 | 2023-11-14 09:26:11 | b03cc3d78d988eac7e4dc5536899fcc37fb0b223da0ebd0188803676ecd1 | 15c46 审计: | 未通过 审计 | 删除 |
| | 35 | fisherman | 对32 33 34 执行审计操作,审计通过 | 2023-11-14 09:21:30 | f71826d410be4c7bbca98f188e0849e35965e302603c3fcdb18f696ddfd8 | 5ee6 未审 | 审计 | 删除 |
| | 34 | fisherman | 清除主服务日志成功! | 2023-11-14 09:00:15 | 7c0ebc844008af1c079d68c1e04156b57c6598ad1e1ba5bedb086368b7e | e684cb 审计 | 通过 审计 | 删除 |
| | 33 | fisherman | 数字信封解封成功! | 2023-11-14 08:33:54 | 2f3af1237aab2cb6aae65831eda8d40fc992608eb313243bb2c3c349d61e | ef76c 👘 🕅 | 通过 审计 | 删除 |
| | 32 | fisherman | 数字信封解封成功! | 2023-11-14 08:33:29 | edca82499a6fe1a2e1a632982839ab826d2804cfa6d47f97da6f5f1c4921b | o34f 审计 | 通过 审计 | 删除 |
| | 31 | fisherman | 数字信封解封成功! | 2023-11-14 08:32:54 | 4b13fca96d2677c795bcc40886e7e2c9ba98d4adbca8ddf0137c7e6a2501 | 1e562 未审 | क्रि | 删除 |
| | 30 | fisherman | 数字信封解封成功! | 2023-11-14 08:32:48 | 57e3be5bb2cecc10f34d3828b3d25fc4c45f6c02e52275ca43046b812003 | 34911 未审 | 审计 | 删除 |
| | 29 | fisherman | 制作数字信封成功! | 2023-11-14 08:30:22 | c87398f83ae614801af54ae3b265e4d32a692dd9a9f498a444fcb4bc843cc | c47b 未审 | 计 审计 | 删除 |
| | 28 | fisherman | 管理员登录成功 | 2023-11-14 08:16:38 | fec2f25caa79b46fd9b4a824fb54819546c1c3ad6b27e11a6943c873ff5f82 | 2e9 未审 | 计 审计 | 删除 |
| | | | | | 每页数目: 10 | → 1-10共日 | 37 K K | > > |

图3-150审计未通过

选择需要删除的一项或多项,勾选序号所在行前"□",点击【删除】,或点击列表 对应记录所在操作列的"删除"按钮,如0,弹出确认提示框,如0,确定后可以删除 日志。

 \times



| 起止 | :时间: | □ 开始日期 - | 结束日期 令牌序列号: | | Q 搜索 C 重置 | | | |
|-----|------|------------------|--------------------------|---------------------|---|--------------|---------|------|
| 志列表 | ž | | | | (1) 日本時間(1) 日本時間(| 出XML 🕹 日夜 | 5导出WEBT | REND |
| - | 序号 | 令牌序列号 | 操作信息 | 操作时间 | HMAC | 审计状态 | 授 | 作 |
| ~ | 10 | K1426190507B4069 | 10号密钥生成SM2密钥对成功 | 2024-02-20 07:33:27 | 81a62a50f83ac84d6cb3ddee44aff9c6a9634ee2ac1ae33b4ff7f20b8f4cf89d | 未审计 | 审计 | 删除 |
| ~ | 9 | K1426190507B4069 | 8号密钥生成SM2密钥对成功 | 2024-02-20 07:33:24 | 783436ea3f5b00510617e98808395166f3bcb2421fb88bbd2d0de8bfbe0660c6 | 未审计 | 审计 | 删除 |
| | 8 | K1426190507B4069 | 增加应用实体成功 | 2024-02-20 07:33:19 | 4d73f50438f0cff6b6a5db69ae6a9216710347468e8189c21d09fadc2c55bffd | 未审计 | 审计 | 删除 |
| | 7 | K1426190507B4069 | 审计员登录成功1 | 2024-02-20 07:24:20 | 536eedcf9c6778cc2a3c75487c38420ada5f2e5ea67aef87efdbf0ed6c6d3a8a | 审计未通过 | 审计 | 删除 |
| | 6 | K1426221104B3964 | 増加系統用户K1426190507B4069成功 | 2024-02-20 07:24:08 | 4b6a757c6e9daceec4cc06acf3cf7b96b5737e490ffec057bd9147e94e741648 | 未审计 | 审计 | 删除 |
| | 5 | K1426221104B3964 | 管理员登录成功 | 2024-02-20 07:00:11 | 7ffc848398a427eccbe61e7b78160c6a9d8d23aa9c9cec3c01882ee60db96102 | 未审计 | 审计 | 删除 |
| | 4 | K1426221104B3964 | 增加应用实体成功 | 2024-02-20 06:52:44 | 963d5a7ab0736d6274b91a5d0e27254d4e15ecc607eb2542372f65618e410461 | 未审计 | 审计 | 删除 |
| | 3 | K1426221104B3964 | 管理员登录成功 | 2024-02-20 06:52:16 | 3660bf966298043e56d755df2bb68ac900dce47b60f033897463baf4bfa92c8a | 未审计 | 审计 | Ð |
| | 2 | fisherman | 增加系统用户K1426221104B3964成功 | 2024-02-20 06:52:09 | 36e0803d0442fcac8198f6c0a88d8408139ecd94d54e81fed7b443a39641c2c4 | 未审计 | 审计 | 删除 |
| | 1 | fisherman | 管理员登录成功 | 2024-02-20 06:52:03 | a2d808ce0cf99852b31b93571752f5907e05b6c16317d11990b2a099edca7fc7 | 未审计 | 审计 | 删除 |
| | | | | | 每页数目: 10 👻 1 | -10 共 10 🛛 🖂 | < 2 | > |

图3-151日志删除





图3-152删除提示

点击【删除全部】,如0,弹出确认提示框如0,点击确定后可以删除所有日志。



| 日志列 | ŧ | | | | ● 毎日 ● 割除 ● 目表号出CSV ● 日表号 | ншXML 🕁 Е | 日志导出WEBTRENDS |
|-----|----|------------------|--------------------------|---------------------|--|-----------|---------------|
| | 序号 | 令牌序列号 | 操作信息 | 操作时间 | НМАС | 审计状态 | 操作 |
| | 10 | K1426190507B4069 | 10号密钥生成SM2密钥对成功 | 2024-02-20 07:33:27 | 81a62a50f83ac84d6cb3ddee44aff9c6a9634ee2ac1ae33b4ff7f20b8f4cf89d | 未审计 | 审计 删除 |
| | 9 | K1426190507B4069 | 8号密钥生成SM2密钥对成功 | 2024-02-20 07:33:24 | 783436ea3f5b00510617e98808395166f3bcb2421fb88bbd2d0de8bfbe0660c6 | 未审计 | 审计 删除 |
| | 8 | K1426190507B4069 | 增加应用实体成功 | 2024-02-20 07:33:19 | 4d73f50438f0cff6b6a5db69ae6a9216710347468e8189c21d09fadc2c55bffd | 未审计 | 审计 删除 |
| | 7 | K1426190507B4069 | 审计员登录成功1 | 2024-02-20 07:24:20 | 536eedcf9c6778cc2a3c75487c38420ada5f2e5ea67aef87efdbf0ed6c6d3a8a | 审计未通过 | 审计 删除 |
| | 6 | K1426221104B3964 | 增加系统用户K1426190507B4069成功 | 2024-02-20 07:24:08 | 4b6a757c6e9daceec4cc06acf3cf7b96b5737e490ffec057bd9147e94e741648 | 未审计 | 审计 删除 |
| | 5 | K1426221104B3964 | 管理员登录成功 | 2024-02-20 07:00:11 | 7ffc848398a427eccbe61e7b78160c6a9d8d23aa9c9cec3c01882ee60db96102 | 未审计 | 审计 删除 |
| | 4 | K1426221104B3964 | 增加应用实体成功 | 2024-02-20 06:52:44 | 963d5a7ab0736d6274b91a5d0e27254d4e15ecc607eb2542372f65618e410461 | 未审计 | 审计 删除 |
| | 3 | K1426221104B3964 | 管理员登录成功 | 2024-02-20 06:52:16 | 3660bf966298043e56d755df2bb68ac900dce47b60f033897463baf4bfa92c8a | 未审计 | 审计 删除 |
| | 2 | fisherman | 增加系统用户K1426221104B3964成功 | 2024-02-20 06:52:09 | 36e0803d0442fcac8198f6c0a88d8408139ecd94d54e81fed7b443a39641c2c4 | 未审计 | 审计 删除 |
| | 1 | fisherman | 管理员登录成功 | 2024-02-20 06:52:03 | a2d808ce0cf99852b31b93571752f5907e05b6c16317d11990b2a099edca7fc7 | 未审计 | 审计 删除 |
| | | | | | 每页数目: 10 👻 1 | -10 共 10 | < < > >1 |

图3-153删除全部



图3-154删除全部提示框

分别选择开始时间和结束时间,可导出所选时间段的日志信息。如0,然后点击【日 志导出】(三种格式可选)可以导出对应时间的日志文件,如0,时间不可为空。

| 日志审计 | | ↑ 首页 / 日志管理 / 日志审计 |
|-----------------------------------|-----------------|-------------------------------------|
| 起止时间: 2023-11-11 - 2023-11-15 令柳哼 | 列号: 〇 恵田 〇 施宏 | |
| 日志列表 | 2 #11 回 删除全部 | も 日志号出CSV も 日志号出XML も 日志号出WEBTRENDS |
| | | |







图3-156日志文件

3.7.3 故障日志

错误日志列表显示查询到的错误日志信息,包括操作时间、错误类型、设备 IP、 设备端口号、错误码、错误描述、和排查方法。界面如 0。

| 故障日初 | ā | | | | | | | ↑ 首页 | 【 / 日志管理 | / 故障日志 |
|------|-------|---------------------|-------|---------------|-------|------|------------------------|---------|----------|--------|
| 起 | 3止时间: | 一 开始日期 - 结束日期 | 错误类型: | 全部 | * | | | | | |
| | 设备IP: | 输入关键字进行搜索 | 端口号: | 输入关键字进行搜索 | | 错误码: | 前入关键字进行搜索 Q | 波次 〇 清空 | | |
| 故障日初 | 志列表 | | | | | | | | 日期除 | 圓 删除全部 |
| | 序号 | 操作时间 | 错误类型 | 设备IP | 设备端口号 | 错误码 | 错误描述 | | 操作 | |
| | 1 | 2024-01-06 19:32:52 | 证书API | 192.168.18.10 | 0 | 1 | OCSP连接异常java.net.Socke | | 排查方法 | 删除 |
| | 2 | 2024-01-05 19:32:52 | 证书API | 192.168.18.10 | 0 | 1 | OCSP连接异常java.net.Socke | | 排查方法 | 删除 |
| | 3 | 2024-01-04 19:32:52 | 证书API | 192.168.18.10 | 0 | 1 | OCSP连接异常java.net.Socke | | 排查方法 | 删除 |
| | 4 | 2024-01-03 19:32:52 | 证书API | 192.168.18.10 | 0 | 1 | OCSP连接异常java.net.Socke | | 排查方法 | 删除 |
| | | | | | | | 每页数目: 10 | ▼ 1-4共4 | < < | > >1 |
| | | | | | | | | | | |
| | | | | | | | | | | |

图3-157故障日志

可以通过选择起止时间、错误类型、设备 IP、端口号、错误码,点击【搜索】按钮显示所对应的信息,点击【清空】按钮可以清除输入的查询条件。界面如 0。

| 起止时间: | 🗐 开始日期 - 结束日期 | 错误类型: | 全部 | | | | |
|-------|---------------|-------|-----------|------|-----------|------|------|
| 设备IP: | 输入关键字进行搜索 | 端口号: | 输入关键字进行搜索 | 错误码: | 输入关键字进行搜索 | Q 捜索 | 다 清空 |

图3-158日志查询

选择需要删除的一项或多项,勾选序号所在行前"□",点击【删除】按钮,或选 点击对应记录"操作"列的"删除"按钮如 0,弹出确认提示框,如 0,确定后可以删 除日志。



| 志列表 | | | | | | | 圓 删除 | 圓 删除全部 |
|-----|---------------------|-------|---------------|--------|-----|------------------------|--------|-----------------------------|
| 序号 | 操作时间 | 错误类型 | 设备IP | 设备端口号 | 错误码 | 错误描述 | 操作 | |
| 1 | 2024-01-06 19:32:52 | 证书API | 192.168.18.10 | 0 | 1 | OCSP连接异常java.net.Socke | 排查方法 | 删除 |
| 2 | 2024-01-05 19:32:52 | 证书API | 192.168.18.10 | 0 | 1 | OCSP连接异常Java.net.Socke | 排查方法 | BH PO: |
| 3 | 2024-01-04 19:32:52 | 证书API | 192.168.18.10 | 0 | 1 | OCSP连接异常java.net.Socke | 排查方法 | 删除 |
| 4 | 2024-01-03 19:32:52 | 证书API | 192.168.18.10 | 0 | 1 | OCSP连接异常java.net.Socke | 排查方法 | 删除 |
| | | | | | | 每页数目: 10 👻 1-4 | 共4 < < | \rightarrow \rightarrow |
| | | | 图3 | -159删阝 | 余操俏 | Ę | | |
| 硝 | 认 | | | | | | × | |
| | | | | A | | | | |
| | | | 确注 | 定要删除 | È吗? | | | |
| | | | | | | 确定取 | 肖 | |

图3-160删除弹框

点击【删除全部】,如0,弹出确认提示框,如0,点击确定后可以删除所有日志。

| 故障日初 | 场利表 | | | | | | | 回 删除 回 删除全部 |
|------|-----|---------------------|-------|---------------|-------|-----|------------------------|--------------------|
| | 序号 | 操作时间 | 错误类型 | 设备IP | 设备端口号 | 错误码 | 错误描述 | 操作 |
| | 1 | 2024-01-06 19:32:52 | 证书API | 192.168.18.10 | 0 | 1 | OCSP连接异常Java.net.Socke | 排查方法 删除 |
| | 2 | 2024-01-05 19:32:52 | 证书API | 192.168.18.10 | 0 | 1 | OCSP连接异常Java.net.Socke | 排查方法 删除 |
| | 3 | 2024-01-04 19:32:52 | 证书API | 192.168.18.10 | 0 | 1 | OCSP连接异常Java.net.Socke | 排查方法 删除 |
| | 4 | 2024-01-03 19:32:52 | 证书API | 192.168.18.10 | 0 | 1 | OCSP连接异举Java.net.Socke | 排查方法 删除 |
| | | | | | | | 每页数目: 10 👻 1-4 共 | 4 < < > > |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

图3-161删除全部



华翼微电子

图3-162删除全部确认框

点击日志列表操作列的"排查方法"如0,弹窗可展示对应错误的解决方法信息, 如0。

| 障日表 | 志列表 | | | | | | | ■ 删除 | |
|-----|---------|---------------------|--------|---------------|---------|-----|-------------------------------------|---------------------------------|---------|
| | 序号 | 提作时间 | 错误类型 | 设备IP | 设备端口号 | 错误码 | 错误描述 | 操作 | |
| | 1 | 2024-01-06 19:32:52 | 证书API | 192.168.18.10 | 0 | 1 | OCSP连接异常java.net.Socke | 排查方法 | 翻网 |
| | 2 | 2024-01-05 19:32:52 | 证书API | 192.168.18.10 | 0 | 1 | OCSP连接异笨java.net.Socke | 排查方法 | 删除 |
| | 3 | 2024-01-04 19:32:52 | 证书API | 192.168.18.10 | 0 | 1 | OCSP连接异常java.net.Socke | 排童方法 | #199 |
| | 4 | 2024-01-03 19:32:52 | 证书5API | 192.168.18.10 | 0 | 1 | OCSP连续异常java.netSocke 每页数目: 10 + | <u>排重方法</u> 1-4 共 4 I< < | 田府 > |
| | | | | | | | | | |
| | | | | <u>&</u> |]3-163排 | 查方法 | 去 | | |
| 排 | 查方 | 法 | | |]3-163排 | 查方法 | 去 | | × |
| 排 | 查方 i | 法 | 的内容仅 | 图 |]3-163排 | 查方济 | 去 | | × |
| 排 | 查方 | 法 | 的内容仅 | 图 |]3-163排 | 查方法 | 去 | | × |
| 排 | 查方 | 法 | 的内容仅 | 图 |]3-163排 | 查方》 | 去 · | | × |

图3-164排查方法弹框(具体内容以实际显示为准)



3.8 预警管理

3.8.1 **预警设置**

预警阈值设置包括 CPU 占用率,内存占用率,磁盘占用率,并发连接数,网络负载, 是否允许邮件告警等等,可以通过设置阈值来发出警告,界面如 0。

| 预警阈值设置 | |
|--------------|-------|
| * CPU占用率(%): | 90 |
| * 内存占用率(%): | 90 |
| * 磁盘占用率(%): | 90 |
| * 并发连接数: | 90 |
| * 网络负载(%): | 90 |
| * 是否允许邮件告警: | ○是 ◎否 |
| | 保存 |

图3-165预警设置

"是否允许邮件告警"选择"是",则显示邮件服务器相关配置,如0。



| * 是否允许邮件告警 | ◎是○否 | |
|------------|------------|--|
| *邮件服务器IP: | | |
| * 邮件发送者: | | |
| * 邮件接收者: | | |
| | 保存 | |
| | | |
| | 图3-166邮件告警 | |

3.8.2 **预警列表**

预警列表可以处理相关预警信息,包括预警信息的显示、查询、删除以及清除全部, 界面如 0。

| 預營列表 | | ♠ 首页 | / 预警管理 / 预警列表 |
|--|---------------------|------------------|---------------|
| 起止时间: 🗈 开始日期 - 結束日期 孫警樂型: 全部 | ▼ Q 捜索 ○ 清空 | | |
| | | | 圓 清除 🛛 |
| □ 序号 预警信息 | 产生时间 | 是否发送邮件 | 操作 |
| □ 1 CPU占用率超过预警, 当前值: 100.0%, 阈值: 90.0% | 2023-11-13 09:13:42 | 未发送 | 删除 |
| | | 每页数目: 10 ▼ 1-1共1 | < < > > |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

图3-167预警列表

选择起止时间,和预警类型,点击【搜索】按钮显示所对应的信息,点击【清空】 按钮可以清除输入的查询条件。如 0。

| Ø | 华翼微电子 HUAYI MICRO-ELECTRONICS | | | | | | | | 用户手 | ≤册 |
|---|----------------------------------|--------|--------|-------|----|---|------|------|-----|----|
| | | | | | | | | | | |
| | 起止时间: | □ 开始日期 | - 结束日期 | 预警类型: | 全部 | • | Q 搜索 | ⊖ 清空 | | |

图3-168搜索

勾选预警列表所在行前的"□",可多选,点击【清除】可以删除所选预警信息, 或通过点击操作列的"删除",删除对应的预警信息。如图 3-169,点击【删除】会弹 出是否删除的确认提示框,如 0。





点击【删除全部】,弹出确认提示框,如0,点击确定后可以删除所有预警信息。



图3-171删除全部

3.9 国标密钥管理

华翼微电子

3.9.1 SM2密钥

SM2 密钥显示当前密钥号下的签名/加密密钥对情况,包括签名/加密密钥对的生成、 删除功能,界面如 0。

| SM2密钥 | | | | | | | | ↑首页 / 国标密 | 明管理 / SM2密钥 |
|---------------|---------------|---------------|---------------|---------------------|---------------|---------------|---------------|---------------------|---------------|
| 密钥列表 | | | | | | | | | |
| 1: E: [256] | 2: E: [256] | 3: E: [256] | 4: E: [256] | 5: E: [256] | 6: E: [256] | 7: E: [256] | 8: E: [256] | 9: E: [256] | 10: E: [256] |
| S: [256] | S: [256] | S: [256] | S: [256] | S: [256] | S: [256] |
| 11: E: [***] | 12: E: [256] | 13: E: [256] | 14: E: [***] | 15: E: [***] | 16: E: [***] | 17: E: [***] | 18: E: [***] | 19: E: [***] | 20: E: [***] |
| S: [***] | S: [256] | S: [256] | S: [***] | S: [***] | S: [***] | S: [***] | S: [***] | S: [***] | S: [***] |
| 21: E: [***] | 22: E: [***] | 23: E: [***] | 24: E: [256] | 25: E: [256] | 26: E: [***] | 27: E: [***] | 28: E: [***] | 29: E: [***] | 30: E: [256] |
| S: [***] | S: [***] | S: [***] | S: [256] | S: [256] | S: [***] | S: [***] | S: [***] | S: [***] | S: [256] |
| 31: E: [256] | 32: E: [256] | 33: E: [256] | 34: E: [256] | 35: E: [256] | 36: E: [256] | 37: E: [256] | 38: E: (256) | 39: E: [256] | 40: E: [256] |
| S: [256] | S: [256] | S: [256] | S: (256) | S: [256] | S: [256] |
| 41: E: [256] | 42: E: [256] | 43: E: [256] | 44: E: [256] | 45: E: [256] | 46: E: [256] | 47: E: [256] | 48: E: [256] | 49: E: [256] | 50: E: [256] |
| S: [256] | S: [256] | S: [256] | S: [256] | S: [256] | S: [256] |
| 51: E: [***] | 52: E: [***] | 53: E: [***] | 54: E: [***] | 55: E: [***] | 56: E: [***] | 57: E: [***] | 58: E: [***] | 59: E: [***] | 60: E: [***] |
| S: [***] | S: [***] | S: [***] | S: [***] | S: [***] | S: [***] |
| 61: E: [***] | 62: E: [***] | 63: E: [***] | 64: E: [256] | 65: E: [256] | 66: E: [256] | 67: E: [***] | 68: E: [***] | 69: E: [***] | 70: E: [***] |
| S: [***] | S: [***] | S: [***] | S: [256] | S: [***] | S: [256] | S: [***] | S: [***] | S: [***] | S: [***] |
| 71: E: [***] | 72: E: [***] | 73: E: [***] | 74: E: [***] | 75: E: [***] | 76: E: [***] | 77: E: [***] | 78: E: [***] | 79: E: [***] | 80: E: [***] |
| S: [***] | S: [***] | S: [***] | S: [***] | S: [***] | S: [***] |
| 81: E: [***] | 82: E: [***] | 83: E: [***] | 84: E: [***] | 85: E: [256] | 86: E: [***] | 87: E: [***] | 88: E: [256] | 89: E: [***] | 90: E: [***] |
| S: [***] | S: [***] | S: [***] | S: [***] | S: [256] | S: [***] | S: [***] | S: [256] | S: [***] | S: [***] |
| 91: E: [***] | 92: E: [***] | 93: E: [***] | 94: E: [***] | 95: E: [***] | 96: E: [***] | 97: E: [***] | 98: E: [***] | 99: E: [***] | 100: E: [***] |
| S: [***] | S: [***] | S: [***] | S: [***] | S: [***] | S: [***] |
| 101: E: [***] | 102: E: [***] | 103: E: [***] | 104: E: [***] | 105: E: [***] | 106: E: [***] | 107: E: [***] | 108: E: [***] | 109: E: [***] | 110: E: [***] |
| S: [***] | S: [***] | S: [***] | S: [***] | S: [***] | S: [***] |

图3-172国标SM2密钥

选择密钥号,点击密钥号,界面如 0,默认显示密钥号以及类型,点击生成密钥,



可生成签名密钥对或加密密钥对;点击删除,可将该密钥号内的签名密钥对或加密密钥 对进行删除。

| 密钥详情 | | |
|-------|------------------------------|---------|
| 密钥号: | 1 | |
| 类型: | 加密密钥 | |
| 🔓 生成图 | ☎钥 🔟 删除密钥 | 取消 |
| | 图2_172国 行 \$M2密钥生戓/删除 | |

点击【生成密钥】,则生成对应签名密钥对或加密密钥对,如果密钥已经存在,那

么生成密钥会覆盖原密钥。界面如 0。

| 密钥详情 | | × |
|------|--|---|
| M. | 确认 X X | |
| | 该密钥号下已存在密钥,修改会影响密钥正常使用,确认要覆盖密钥 号【1】的[加密]的密钥吗? | |
| E | 确定 取消 | |

图3-174覆盖生成

点击【删除密钥】,可以将对应密钥对删除。界面如 0。如果密钥不存在则不能删除。界面如 0。





3.9.2 RSA密钥

RSA 密钥显示当前密钥号下的签名/加密密钥对情况,包括签名/加密密钥对的生成、 删除功能,界面如 0。



用户手册

 \times

| RSA密钥 | | | | | | | | ↑首页 / 国标密 | 钥管理 / RSA密钥 |
|---------------|---------------|---------------|---------------|---------------|---------------------|---------------|---------------|---------------|---------------------|
| 密钥列表 | | | | | | | | | |
| 1: E: [2048] | 2: E: [***] | 3: E: [***] | 4: E: [2048] | 5: E: [2048] | 6: E: [2048] | 7: E: [2048] | 8: E: [2048] | 9: E: [2048] | 10: E: [2048] |
| S: [2048] | S: [***] | S: [***] | S: [2048] | S: [2048] | S: [2048] | S: [2048] | S: [2048] | S: [2048] | S: [2048] |
| 11: E: [***] | 12: E: [1024] | 13: E: [2048] | 14: E: [1024] | 15: E: [1024] | 16: E: [***] | 17: E: [***] | 18: E: [***] | 19: E: [***] | 20: E: [***] |
| S: [***] | S: [1024] | S: [2048] | S: [2048] | S: [1024] | S: [***] | S: [***] | S: [***] | S: [***] | S: [***] |
| 21: E: [***] | 22: E: [***] | 23: E: [***] | 24: E: [***] | 25: E: [***] | 26: E: [***] | 27: E: [***] | 28: E: [***] | 29: E: [***] | 30: E: [***] |
| S: [***] | S: [***] | S: [***] | S: [***] | S: [***] |
| 31: E: [***] | 32: E: [***] | 33: E: [1024] | 34: E: [1024] | 35: E: [***] | 36: E: [***] | 37: E: [***] | 38: E: [***] | 39: E: [***] | 40: E: [***] |
| S: [***] | S: [***] | S: [1024] | S: [1024] | S: [1024] | S: [***] | S: [***] | S: [***] | S: [***] | S: [***] |
| 41: E: [***] | 42: E: [***] | 43: E: [***] | 44: E: [***] | 45: E: [1024] | 46: E: [***] | 47: E: [***] | 48: E: [***] | 49: E: [***] | 50: E: [***] |
| S: [***] | S: [***] | S: [***] | S: [***] | S: [1024] | S: [***] | S: [***] | S: [***] | S: [***] | S: [***] |
| 51: E: [***] | 52: E: [***] | 53: E: [***] | 54: E: [***] | 55: E: [***] | 56: E: [***] | 57: E: [***] | 58: E: [***] | 59: E: [***] | 60: E: [***] |
| S: [***] | S: [***] | S: [***] | S: [***] | S: [***] |
| 61: E: [***] | 62: E: [***] | 63: E: [***] | 64: E: [***] | 65: E: [***] | 66: E: [***] | 67: E: [***] | 68: E: [***] | 69: E: [***] | 70: E: [***] |
| S: [***] | S: [***] | S: [***] | S: [***] | S: [***] |
| 71: E: [***] | 72: E: [***] | 73: E: [***] | 74: E: [***] | 75: E: [***] | 76: E: [***] | 77: E: [***] | 78: E: [***] | 79: E: [***] | 80: E: [***] |
| S: [***] | S: [***] | S: [***] | S: [***] | S: [***] |
| 81: E: [***] | 82: E: [***] | 83: E: [***] | 84: E: [***] | 85: E: [***] | 86: E: [***] | 87: E: [***] | 88: E: [***] | 89: E: [***] | 90: E: [***] |
| S: [***] | S: [***] | S: [***] | S: [***] | S: [***] |
| 91: E: [***] | 92: E: [***] | 93: E: [***] | 94: E: [***] | 95: E: [***] | 96: E: [***] | 97: E: [***] | 98: E: [***] | 99: E: [***] | 100: E: [***] |
| S: [***] | S: [***] | S: [***] | S: [***] | S: [***] |
| 101: E: [***] | 102: E: [***] | 103: E: [***] | 104: E: [***] | 105: E: [***] | 106: E: [***] | 107: E: [***] | 108: E: [***] | 109: E: [***] | 110: E: [***] |
| S: [***] | S: [***] | S: [***] | S: [***] | S: [***] |

图3-177RSA密钥

在密钥列表点击要管理的密钥号,显示密钥信息,界面如0。选择模长,点击"生 成密钥",可生成签名密钥对或加密密钥对;如果密钥已经存在,那么生成密钥会覆盖 原密钥。界面如0。

| 密钥详情 |
|------|
|------|

| 密钥号: | 13 | |
|------|---------------|----|
| 模长: | ● 1024 ○ 2048 | |
| 指数: | 65537 | • |
| 类型: | 加密密钥 | |
| L 生成 | 密钥 删除密钥 | 取消 |

图3-178RSA密钥生成/删除



用户手册



如果密钥不存在则不能删除,模长 2048 同理。界面如 0。





图3-181重复删除

3.9.3 对称密钥

对称密钥显示当前密钥号下密钥情况,界面如0。

| 对称密钥 | | | | | | | | | | | | | | | | • | 首页/ | 国标密钥管理 | / 对称密钥 |
|------|------|--------|-----|------|------|------|------|------|------|------|------|------|------|------|------|------|------|--------|--------|
| 密钥列表 | | | | | | | | | | | | | | | | | | | |
| 0: | [32] | 1: [| 32] | 2: | [32] | 3: | [32] | 4: | [32] | 5: | [32] | 6: | [32] | 7: | [32] | 8: | [32] | 9: | [32] |
| 10: | [32] | 11: [| 32] | 12: | [32] | 13: | [32] | 14: | [32] | 15: | [32] | 16: | [32] | 17: | [32] | 18: | [32] | 19: | [32] |
| 20: | [32] | 21: | 32] | 22: | [32] | 23: | [32] | 24: | [32] | 25: | [32] | 26: | [32] | 27: | [32] | 28: | [32] | 29: | [32] |
| 30: | [32] | 31: [| 32] | 32: | [32] | 33: | [32] | 34: | [32] | 35: | [32] | 36: | [32] | 37: | [32] | 38: | [32] | 39: | [32] |
| 40: | [32] | 41: | 32] | 42: | [32] | 43: | [32] | 44: | [32] | 45: | [32] | 46: | [32] | 47: | [32] | 48: | [32] | 49: | [32] |
| 50: | [32] | 51: [| 32] | 52: | [32] | 53: | [32] | 54: | [32] | 55: | [32] | 56: | [32] | 57: | [32] | 58: | [32] | 59: | [32] |
| 60: | [32] | 61: | 32] | 62: | [32] | 63: | [32] | 64: | [32] | 65: | [32] | 66: | [32] | 67: | [32] | 68: | [32] | 69: | [32] |
| 70: | [32] | 71: | 32] | 72: | [32] | 73: | [32] | 74: | [32] | 75: | [32] | 76: | [32] | 77: | [32] | 78: | [32] | 79: | [32] |
| 80: | [32] | 81: [| 32] | 82: | [32] | 83: | [32] | 84: | [32] | 85: | [32] | 86: | [32] | 87: | [32] | 88: | [32] | 89: | [32] |
| 90: | [32] | 91: [| 32] | 92: | [32] | 93: | [32] | 94: | [32] | 95: | [32] | 96: | [32] | 97: | [32] | 98: | [32] | 99: | [32] |
| 100: | [32] | 101: [| 32] | 102: | [32] | 103: | [32] | 104: | [32] | 105: | [32] | 106: | [32] | 107: | [32] | 108: | [32] | 109: | [32] |
| 110: | [32] | 111: [| 32] | 112: | [32] | 113: | [32] | 114: | [32] | 115: | [32] | 116: | [32] | 117: | [32] | 118: | [32] | 119: | [32] |
| 120: | [32] | 121: [| 32] | 122: | [32] | 123: | [32] | 124: | [32] | 125: | [32] | 126: | [32] | 127: | [32] | 128: | [32] | 129: | [32] |
| 130: | [32] | 131: [| 32] | 132: | [32] | 133: | [32] | 134: | [32] | 135: | [32] | 136: | [32] | 137: | [32] | 138: | [32] | 139: | [32] |
| 140: | [32] | 141: [| 32] | 142: | [32] | 143: | [32] | 144: | [32] | 145: | [32] | 146: | [32] | 147: | [32] | 148: | [32] | 149: | [32] |
| 150: | [32] | 151: [| 32] | 152: | [32] | 153: | [32] | 154: | [32] | 155: | [32] | 156: | [32] | 157: | [32] | 158: | [32] | 159: | [32] |
| 160: | [32] | 161: [| 32] | 162: | [32] | 163: | [32] | 164: | [32] | 165: | [32] | 166: | [32] | 167: | [32] | 168: | [32] | 169: | [32] |
| 170: | (32) | 171: 1 | 321 | 172: | 1321 | 173: | (32) | 174: | [32] | 175: | [32] | 176: | (32) | 177: | [32] | 178: | [32] | 179: | [32] |

图3-182对称密钥

在密钥列表点击要管理的密钥号,显示密钥信息,界面如0。



| 密钥详情 | | | × | |
|-------|----|--------|----|--|
| 密钥号: | 13 | | | |
| | | | | |
| 🔒 生成物 | 密钥 | 🗓 删除密钥 | 取消 | |

图3-183对称密钥生成/删除

点击【生成密钥】,则生成对称密钥,如果密钥已经存在,那么生成密钥会覆盖原密 钥。界面如0。

| 密钥详 | 确认 × | × |
|-----|-------------------------------|-----|
| | 该密钥号下已存在密钥,确认要覆盖密钥号【14】的的密钥吗? | |
| | 确定 取消 | , m |

图3-184重复生成

点击【删除密钥】,则删除对称密钥。界面如0。如果密钥不存在则不能删除。界面如0。



图3-185删除密钥



用户手册



图3-186重复删除

3.9.4 **密钥批量管理**

密钥批量管理,可以对可选范围内密钥进行批处理,包括RSA密钥、SM2密钥和对称密 钥,主要功能为"批量生成"和"批量删除",如0。

| 密钥账量管理 | ↑ 首页 / 国标密钥管理 / 密钥批量管理 |
|---------------------------|------------------------|
| 密钥批届管理 | |
| 密明类型: ●RSA密钥 ○SM2密钥 ○対称密钥 | |
| 密钥长度: ③1024 〇2048 | |
| 起始密钥号: | |
| 终止密钥号: | |
| ℃ 就嚴生成 目 批量删除 | |
| | |
| | |
| | |
| | |
| | |
| | |

图3-187批量密钥管理

选择需要批量管理的密钥类型和密钥长度,RSA 密钥长度可选 1024 和 2048,SM2 密钥默认长度为 256 不显示,对称密钥长度也为默认长度 32 且不显示,输入正确的起 始和终止密钥号,点击"批量生成"或"批量删除",如果当前范围内存在密钥,则会 弹出如 0 和 0 的确认弹出框,如果点击"确定"后生成或者删除操作将会覆盖该范围内 所有已生成的密钥。





当批量管理任务结束后弹出如0弹出框,表示批量管理任务已完成。



X

确定



当输入范围内不存在密钥时点击"批量删除"则会弹出如0的警告框。

警告

77-79号密钥不存在,无需删除!

图3-192批量密钥删除

3.9.5 私钥权限码

私钥权限码管理显示当前密钥的私钥权限码信息(私钥权限码在创建应用实体时配置)。可以通过输入密钥号,点击【查询】按钮显示所密钥号的私钥权限码信息,【清空】 可以清除输入的内容。界面如 0。



| 私钥权限码管理 | | | ↑ 首页 / 国标密钥管理 / 私钥权限码管理 |
|---------|--------|------|---------------------------|
| 密钥号: 请输 | 入密钥号 C | > 清空 | |
| 私钥权限码 | | | |
| 序号 | 废钥号 | 密钥类型 | 私钥仪限码 |
| 1 | 1 | SM2 | 12345678 |
| | | | 毎页数目: 10 ▼ 1-1共1 < < > > |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

图3-193私钥权限码管理

4 初始化配置签名验签使用步骤

(本管理界面配置默认选择密钥类型SM2,若为RSA,步骤相同,只需注意选择密钥类型) 1、 打开初始化登录界面,下载 UKEY 组件安装,安装成功之后,使用默认用户名

- fisherman 登录并新增管理员和审计员。(详见操作3产品操作说明)
- 2、 点击"证书管理"→"CA证书管理",导入 CA 证书(支持 cer 证书和证书链)。
 (详见操作 3.7.1 CA 证书管理)
- 3、 CA 证书导入成功之后,点击"证书管理"->"证书验证设置",进行证书验证 设置。默认设置为验证证书有效性和验证证书签名有效性。说明:若设置验证 是否在 CRL 中,需要点击"CRL 管理"导入 CRL 或点击"证书管理"->"证书 状态查询设置"设置 CRL 自动更新。(详见操作 3.7.2 证书验证设置/3.7.4CRL 管理/3.7.5 证书状态查询设置)
- 4、 点击"应用实体管理"->"应用实体注册",注册应用实体。
- 5、 应用实体注册成功之后,点击"应用实体管理"→"应用实体信息管理",选择 应用实体所在行,点击"生成 P10 请求",输入 P10 信息,点击"签名证书 P10



生成"和"加密证书 P10 生成"。成功之后下载签名 P10 和加密 P10 ,通过证书注册系统生成签名证书和加密证书,点击"导入证书",导入签名和加密证书 (详见操作 3.2 应用实体管理)

以上步骤成功操作完成之后,可正常使用签名验签服务器,若需其他功能,可 根据用户手册进行其他功能配置。

5 常见问题及解答

1、问:用户登录用户时,已经插入 Ukey,输入密码,点击登录却提示"令牌打开失败,请确认是否插入令牌!"。

答:因为由于登录时插入的 Ukey 部件版本可能比较低,不能立即识别。此时可点击 下拉列表,刷新 Ukey 的序列号,再点击登录即可。

2、问:私钥权限码管理中为什么只有私钥权限码的查看功能?

答:因为在应用实体注册的过程中,会有设置私钥权限码的步骤,应用实体注册过程 中密钥号对应的私钥权限码同步设置,应用实体删除过程中,对应密钥号的私钥权限 码也会同步删除。

3、问:时间配置中设置系统时间后,点击其他功能无反应?

答:因为系统设置 session 有效期为 30 分钟,如果设置的时间与当前时间相差 30 分钟以上,当前 session 有效期将失效,系统会自动退出当前用户登陆状态,此时需 重新执行登录系统操作。

4、问:设备提供数字签名、验签服务的准备工作有哪些?

答:设备已执行完成初始化;配置网络地址、设备时间;添加5个管理员、1个审计员;在证书管理功能模块中导入 CA 证书;在应用实体管理模块中注册应用实体,生成应用实体的签名密钥对和加密密钥对,设置私钥权限码(注意:此码用于调取密钥,不可丢失、遗忘,可在其它地方进行安全备份),导入应用实体的数字证书;应用实体依据 GM/T 0018-2012《密码设备应用接口规范》、GM/T 0029-2014《签名验签服务



器技术规范》标准进行 API 接口配置。

5、双机热备开启之后,点击数据同步,提示"数据同步失败",但是实际数据同步成功?

答: 在建立数据同步通道的过程中,有时会存在时间延迟,当查询数据同步是否建立时,若数据同步通道正在建立中,则会提示数据同步失败,过几分钟重新刷新页面再 次点击数据同步,若数据同步已经成功,则会给予成功提示,若仍然失败,则给予失 败提示。

6、数据同步开启正常运行中,登录子服务 IP 操作,无法正常同步数据?

答:数据同步开启后,需访问主服务 IP,请勿再访问子服务 IP 操作。因数据同步开 启后,会存在主备切换,本设备数据同步原理为"主同步从,从不能同步主",若数 据同步开启正常运作之后,仍然访问子服务 IP 操作,若恰巧访问的是从设备,从设 备记录日志等其他数据表 ID 会与主设备 ID 产生冲突,而导致数据同步失败。