

# 翼安服务器密码机 用户手册

山东华翼微电子技术股份有限公司



用户手册

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



## 目 录

1	产品	概述 1
	1.1	产品简介1
2	产品	操作说明
	2.1	初次使用服务器密码机流程2
3	服务	器密码机操作配置
	3.1	服务器密码机服务配置5
		3.1.1 服务器密码机网络配置5
		3.1.2 路由配置
		3.1.3 Syslog配置7
		3.1.4 系统时间设置
		3.1.5 服务升级
	3.2	服务器密码机权限管理配置10
		3.2.1 管理员、审计员添加10
		3.2.2 用户删除
		3.2.3 注销所有用户13
		3.2.4 修改用户口令15
		3.2.5 白名单配置
	3.3	服务器密码机设备信息查看17
	3.4	服务器密码机秘钥管理
		3.4.1 设备主密钥更新
		3.4.2 RSA密钥添加/删除
		3.4.3 SM2密钥添加/删除
		3.4.4 SM9主密钥添加/删除
		3.4.5 SM9用户密钥添加/删除
		3.4.6 对称密钥添加/删除
		3.4.7 导出公钥
		3.4.8 P10证书
		3.4.9 P12证书
		3.4.10 密钥备份
	25	3.4.11 名钥恢复
	3.5 2.6	版介希省的机KeyStore能直官理41 取夕思家印机口士答理
	3.0	瓜分铅苦钙机口芯目埋
		3.0.1 服务品名码机口芯反量42 2.6.2 亩计本询
		3.6.2 审计 旦间
		3.6.5 审订
	37	5.0.4 审订删除
	3.2	₩77₩11₩74/₩112
	5.0	3.8.1 服务器密码机执备设置 //
		3.8.2 服务器密码机数据同步 50
	39	服务器密码机初始化 51



4	产品	常见错误分析及解决方法	60
	4.1	服务器密码机配置管理连接不上	.60
	4.2	服务器密码机服务连接不上	.60
	4.3	服务器密码机服务报错	.60



## 1 产品概述

#### 1.1 产品简介

翼安服务器密码机是由山东华翼微电子技术股份有限公司自主研发的高性能密码 设备,产品严格遵循国家相关产品技术规范进行设计,内置经国家密码管理局审批的高 速密码模块,支持国家密码管理局认可的密码算法,适用于各类密码安全应用系统进行 高速的、多任务并行处理的密码运算。可以满足应用系统数据的加密解密、签名/验证 的要求,实现应用的数据的机密性和完整性保护,同时可提供安全、完善的密钥管理机 制。

应用系统通过调用服务器密码机提供的API接口来使用密码服务,密码机API与密码 机之间的调用过程对上层应用透明,应用开发商能够快速的使用密码机所提供的安全功 能。密码机API接口符合密码产品标准接口规范,通用性好,能够满足大多数应用系统 的要求,在应用系统安全方面具有广泛的应用前景。



## 2 产品操作说明

## 2.1 初次使用服务器密码机流程

首先,通过IE10(其他浏览器可以根据浏览器提示进行)浏览器登录服务器密码机 IP(eth0默认是192.168.18.239): https://192.168.18.239,弹出如图1界面:

8	此网站的安全证书有问题。
	此网站出具的安全证书不是由受信任的证书颁发机构颁发的。 此网站出具的安全证书是为其他网站地址颁发的。
	安全证书问题可能显示试图欺骗您或截获您向服务器发送的数据。
	建议关闭此网页,并且不要继续浏览该网站。
	🥑 单击此处关闭该网页。
	😵 继续浏览此网站(不推荐)。
	● 更多信息

图 2

B 
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B
 B

单击"继续浏览此网站(不推荐)",进入用户登录界面如图2



当初次登陆加密机时,没有任何管理员的添加,所以默认用户名:admin,密码: admin,点击登录,可以进入配置页面。可以正常通过浏览器访问服务器密码机进行相 关配置操作。使用服务器密码机时需要从web页面首页下载客户端软件。首先点击客户 端下载,下载"客户端"软件setup.exe。

安装setup.exe控件,以便支持用户管理。操作步骤如下: 以管理员身份运行setup.exe,选择"下一步":



继续,下一步;



继续,下一步;

华翼微电子

🕑 安装程序 - UKEY服务管理控件	—		×
<b>选择额外任务</b> 您想执行什么额外任务 <b>?</b>		¢	
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,再点	话下—	
☑ 创建桌面快捷方式图标			
<上一步(B) 下一步	(N) >	取	肖



#### 继续,选择"安装";

🔗 安装程序 - UKEY服务管理控件		—	
<b>准备安装</b> 安装程序即将安装 UKEY服务管理控件。			
点击 安装 继续安装,点击 上一步 检查	4改变设置。		
开始菜单: 渔翁UKey组件			^
额外任务: 创建桌面快捷方式图标			
			_ v
×			
[	〈上一步圖 安	業()	取消

图 6

安装完成后,相关服务已经启动,后续可以进行用户管理等相关操作。

## 3 服务器密码机操作配置

#### 3.1 服务器密码机服务配置

#### 3.1.1 服务器密码机网络配置

对密码机的网络配置,需要满足管理员权限。初次登录,系统未添加管理员,登录 后权限默认为管理员权限。

单击左侧菜单栏"服务配置"按钮,并单击"网络配置"按钮,如图 7

选择网卡端口,输入IP和掩码,网关没有可以不输。每个网口可单独设置服务类型: "配置管理"用于web管理; "主服务"用于主服务调用。"兼容"模式即网口可同时 提供web管理和主服务调用。 "聚合"模式需要先选择需要配置的网口,配置好IP选择 聚合模式,单击修改,然后循环此操作,直到所有需要聚合的网口配置完成后,再重启



加密机。<mark>聚合模式为主备</mark>,端口号较小的为主口,IP以此端口为主。

IP配置完成后需要重启加密机后才能生效。点击设备管理菜单─>服务器重启,点 击服务器重启会提示设备重启启动,请稍等。设备重启后,加密机IP会变为修改后的IP。

设备信息菜单	当前位置: 服务配置>>网络配置	
密钥信息菜单	网络配置	
密钥管理菜单	网卡端口:	eth0 V
国标密钥信息	服务类型:	○ 管理 ○服务 ◎兼容 ○聚合
国标密钥管理	网络类型:	●IPv4 ○IPv6
密钥备份管理	IPv4:	192.168.18.239
服务配置菜单	子网掩码v4:	255.255.255.0
🔅 连接口令配置	IPv6:	2001:150:1800:1::10
◎ 网络配置	子网掩码v6:	64
	Mac地址:	10:0c:29:53:30:f2
<ul> <li>系统时间</li> </ul>	聚合物理网口:	无
<b>     TP</b> TP     T     T     T     T     T		
SNMP配置	设置	
1000 加約1/1/33 1000 服务升级		
KeyStore管理		
日志管理菜单		
设备监控菜单		
双机热备功能		
设备管理菜单		

图 7

#### 3.1.2 路由配置

对密码机的路由配置,需要满足管理员权限。

单击左侧菜单栏"服务配置"按钮,并单击"路由配置"按钮,如图8。

输入"目标网络"、"子网掩码"、"网关地址",点击"新增"即可添加路由信息,并且立即生效。选中需要删除的路由信息,然后点击"删除"按钮,即可删除当前路由信息,并且立即生效。



#### 3.1.3 Syslog配置

对密码机的syslog配置,需要满足管理员权限。 单击左侧菜单栏"服务配置"按钮,并单击"syslog配置"按钮,如图9。

HUAYI MICRO-ELECTRONICS			用户手册
设备信息菜单	当前位罢:服务配置>>syslog面證		
密钥信息菜单	syslog配置		
密钥管理菜单	服务器响地址:	192.168.6.169	
国标密钥信息	上报周期(单位:分钟):	10	
国标密钥管理	工10月8八十位-03447.	10	
密钥备份管理	设置		
权限管理菜单			
服务配置菜单			
🔅 连接口令配置			
🔅 网络配置			
🔅 路由配置			
io syslog配置			
◎ 系统时间			
○ NTP配置			
◎ 服务1/133 ◎ 服务升级			
KeyStore管理			
日志管理菜单			
设备监控菜单			
双机热备功能			
设备管理菜单			

#### 3.1.4 系统时间设置

对密码机的时间配置,需要满足管理员权限。

单击左侧菜单栏"服务配置"按钮,并单击"时间配置"按钮,如错误!未找到引用源。0。可查看和设置服务器的系统时间。





#### 3.1.5 服务升级

华翼微电子

对密码机的服务升级,需要满足管理员权限。

单击左侧菜单栏"服务配置"按钮,并单击"服务升级"按钮,如错误!未找到引用源。1。可进行服务器的本地升级,升级包需要由厂家提供。

![](_page_14_Figure_0.jpeg)

3.2 服务器密码机权限管理配置

### 3.2.1 管理员、审计员添加

单击左侧菜单栏"权限管理"按钮,在配置终端(指个人笔记本电脑,不是服务器 密码机)USB口中插入key并单击"用户添加"按钮,如图12。

设备信息采甲	当前位置: 权限管理>>用户添加		
密钥信息菜单	系统用户添加		
密钥管理菜单	系统用户角色:	●管理员 ○操作员 ○审计员	
国标密钥信息	田白公園・		
国标密钥管理			
密钥备份管理	~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	请输入8-10个字付	
权限管理菜单		添加用户	
👤 用户添加			
▶ 用户管理			
👱 白名单管理			
服务配置菜单			
KeyStore管理			
日志管理菜单			
设备监控菜单			
双机热备功能			
设备管理菜单			

选择管理员角色,用户口令默认为12345678,点击"添加用户"按钮,成功后会在 "用户管理"中显示已添加的管理员。输入口令后,再单击"登录"按钮,如图13。 添 加用户必须满足管理员权限,即有半数以上的管理员登陆。

![](_page_16_Picture_1.jpeg)

登录口令输入添加的管理员口令,默认是12345678。登录成功后会提示登录成功。 同时会修改登录状态为"已登录"。

把添加管理员的key做上标记,然后拔掉key,重新插入下一个key进行管理员添加,步骤与第一个相同。

请依次使用如上方法添加五个管理员。

华翼微电子

当有半数以上的管理员登陆时,即获得管理员权限,如果管理员状态显示"未登录" 即使加密机内部含有半数以上的管理员,也不具有管理员权限。

添加完5个管理员后,单击左侧菜单栏添加用户,添加审计管理员。审计管理员的 权限是可以查看审计日志,进行审计操作以及删除审计日志。添加审计管理员方法与添 加管理员相同。

![](_page_17_Picture_1.jpeg)

## 3.2.2 用户删除

删除用户必须满足管理员权限,即有半数以上的管理员登陆。

删除用户时,在要删除的用户右侧单击"删除"按钮。如图14。

		124.133.2.85 确认删除用户?	显示			2024年05月13日 09:40:00 退出
设备信息菜单	当前位置: 权限管理				(确定) 取消	
密钥信息菜单	系统用户列表					
密钥管理菜单	席号 今機	「京利是	备色	状态	口今	容录 注销 删除
国标密钥信息						
国标密钥管理	1 K14	26221108B1694	管理员	未登录	*******	登录 注销 删除
密钥备份管理	注销所有用户					
权限管理菜单						
👤 用户添加						
▲ 用户管理						
14411111111111111111111111111111111111						
服务配置菜单						
KeyStore管理						
日志管理菜单						
设备监控菜单						
双机热备功能						
设备管理菜单						

图 34

#### 3.2.3 注销所有用户

在符合半数登陆的情况下,点击"注销所有用户",会同时注销管理员和审计员, 状态显示为"未登录"。如图15。

	•	124.133.2.85 确认注销所有用F	显示 <sup>コ</sup> ?			2024年05月1	3日 09:40:0	用 / <sup></sup> 5   退出
备信自亚单	当前位置: 权限	管理			确定取消			
相信息菜单	系统用户列表							
钥管理菜单	序号	今慶序列号	备色	状态		發音	注销	冊修余
标密钥信息		< #177735	мс	1/1/424	н×	巫水	-1H	003835
标密钥管理	1	K1426221108B1694	管理员	未登录	******	登录	注销	删除
钥备份管理	注销所有用户	<b>–</b>						
限管理菜单								
用户添加								
用户管理								
白名单管理								
务配置菜单								
eyStore管理								
志管理菜单								
备监控菜单								
机热备功能								
备管理菜单								

图 35

## 审计管理员注销后,将无法查看、审计、删除审计日志。如图16。

	目前操作需要日志审计	管理员权限		确定	2020年09月28日 18:19:06 退出
志闻	『计管理 > 曰志审计				-
LI V					
:	2020-09-28	结束时间:	2020-09-28		查询
	删除审计日志 删除全部审计				
	令牌序列号	操作信息		操作时间	审计状态
		L-	-页 下页 第1页	ī,共 <b>1</b> 页	

![](_page_19_Picture_1.jpeg)

#### 3.2.4 修改用户口令

单击"修改口令"按钮后,如图17。

当前	位置: 系统用户管理 >> 系统	用户管理	
令牌	中口令修改		
	用户令牌:	K1426200427B5260	
	原口令:	•••••	字母和数字的组合,大于8、小于16个字符
	新口令:	•••••	字母和数字的组合,大于8、小于16个字符
	确认新口令:	•••••	字母和数字的组合,大于8、小于16个字符
		修改	

图 37

在旧口令中输入USB KEY原有口令,新口令框中输入新口令,确认口令框中再输一次新口令。单击"修改"按钮完成口令修改。

#### 3.2.5 白名单配置

单击左侧菜单栏"权限管理"按钮,并单击"白名单管理"按钮,如图18。如果白 名单内没有任何IP则允许所有IP访问服务器密码机。

设备信息菜单	当前位置: 权限管理>>白名单管野	₽		
密钥信息菜单	白名单管理			
密钥管理菜单	网络类型:	●IPv4 ○IPv6		
国标密钥信息				
国标密钥管理				
密钥备份管理	结束1P:			
2 用户添加	增加IP地址			
▲ 用户管理 ▲ 白名单管理	序号	IP地址	刪除	
影配置菜单				
KeyStore管理				
志管理菜单				
设备监控菜单				
双机执备功能				
ALL REAL PROPERTY AND AND A REAL PROPERTY AND				

图 38

输入起始IP和结束IP,添加白名单成功后,只有白名单范围的ip地址,才允许访问加密机服务。如图19。

	起始 <mark>IP:</mark>	192.168.18.2	
	结束 <mark>IP</mark> :	192.168.18.30	
地址			
P地址	IPJt	地	删除

![](_page_21_Picture_0.jpeg)

#### 3.3 服务器密码机设备信息查看

单击左侧菜单栏"设备信息"按钮,进入设备信息查看页面,如图20。

设备信息菜单	当前位置:设备信息>>设备信则	
○ 设备信息	设备信息	
	生产厂商:	HUAYI
5 切信念来半 8 钥管理菜单	硬件版本信息:	CS-XC5000-FT
国标密钥信息	软件版本信息:	V2.0
国标密钥管理	产品序列号:	020201286230731B1622
密钥备份管理	非对称算法:	SM2 RSA1024 RSA2048 RSA3072 RSA4096 DSA DH ECP SM9
仅限管理菜单	对称算法:	SM1 SM4 3DES DES AES
<b>勝</b> 爾置菜单	杂凑算法:	SM3 SHA1 SHA224 SHA256 SHA384 SHA512
(eyStore管理		
日志管理菜単		
安备监控菜里		
X机热备功能		
设备管理菜甲		

图 20

单击左侧菜单栏"密钥信息"按钮,进入密钥信息查看页面,查看RSA密钥、SM2 密钥、SM9主密钥、SM9用户密钥、对称密钥,如错误!未找到引用源。-28。其中,如果 加密机支持SM9密钥,则SM9相关密钥信息页正常显示,如果不支持,则不显示。

	<u></u> 图 21										
当前位置:密钥信息>>SM2密钥信息											
SM2密钥											
0:[***]	1:[256]	2:[256]	3:[256]	4:[256]	5:[256]	6:[256]	7:[256]	8:[256]	9:[256]		
10:[256]	11:[256]	12:[256]	13:[256]	14:[256]	15:[256]	16:[256]	17:[256]	18:[256]	19:[256]		
20:[256]	21:[256]	22:[256]	23:[256]	24:[256]	25:[256]	26:[256]	27:[256]	28:[256]	29:[256]		
30:[256]	31:[256]	32:[256]	33:[256]	34:[256]	35:[256]	36:[256]	37:[256]	38:[256]	39:[256]		
40:[256]	41:[256]	42:[256]	43:[256]	44:[256]	45:[256]	46:[256]	47:[256]	48:[256]	49:[256]		
50:[256]	51:[256]	52:[256]	53:[256]	54:[256]	55:[256]	56:[256]	57:[256]	58:[256]	59:[256]		
60:[256]	61:[256]	62:[256]	63:[256]	64:[256]	65:[256]	66:[256]	67:[256]	68:[256]	69:[256]		
70:[256]	71:[256]	72:[256]	73:[256]	74:[256]	75:[256]	76:[256]	77:[256]	78:[256]	79:[256]		
80:[256]	81:[256]	82:[256]	83:[256]	84:[256]	85:[256]	86:[256]	87:[256]	88:[256]	89:[256]		
90:[256]	91:[256]	92:[256]	93:[256]	94:[256]	95:[256]	96:[256]	97:[256]	98:[256]	99:[256]		
100:[256]	101:[***]	102:[***]	103:[***]	104:[***]	105:[***]	106:[***]	107:[***]	108:[***]	109:[***]		
110:[***]	111:[***]	112:[***]	113:[***]	114:[***]	115:[***]	116:[***]	117:[***]	118:[***]	119:[***]		
120:[***]	121:[***]	122:[***]	123:[***]	124:[***]	125:[***]	126:[***]	127:[***]	128:[***]	129:[***]		
130:[***]	131:[***]	132:[***]	133:[***]	134:[***]	135:[***]	136:[***]	137:[***]	138:[***]	139:[***]		

图 2	冬	2	•
-----	---	---	---

ㅋㅋ													
RSA	ISA密钥信息												
	0:[****]	1:[1024]	2:[2048]	3:[1024]	4:[1024]	5:[1024]	6:[1024]	7:[1024]	8:[1024]	9:[1024]			
	10:[1024]	11:[1024]	12:[1024]	13:[1024]	14:[1024]	15:[1024]	16:[1024]	17:[1024]	18:[1024]	19:[1024]			
	20:[1024]	21:[1024]	22:[1024]	23:[1024]	24:[1024]	25:[1024]	26:[1024]	27:[1024]	28:[1024]	29:[1024]			
	30:[1024]	31:[1024]	32:[1024]	33:[1024]	34:[1024]	35:[1024]	36:[1024]	37:[1024]	38:[1024]	39:[1024]			
	40:[1024]	41:[1024]	42:[1024]	43:[1024]	44:[1024]	45:[1024]	46:[1024]	47:[1024]	48:[1024]	49:[1024]			
	50:[1024]	51:[1024]	52:[1024]	53:[1024]	54:[1024]	55:[1024]	56:[1024]	57:[1024]	58:[1024]	59:[1024]			
	60:[1024]	61:[1024]	62:[1024]	63:[1024]	64:[1024]	65:[1024]	66:[1024]	67:[1024]	68:[1024]	69:[1024]			
	70:[1024]	71:[1024]	72:[1024]	73:[1024]	74:[1024]	75:[1024]	76:[1024]	77:[1024]	78:[1024]	79:[1024]			
	80:[1024]	81:[1024]	82:[1024]	83:[1024]	84:[1024]	85:[1024]	86:[1024]	87:[1024]	88:[1024]	89:[1024]			
	90:[1024]	91:[1024]	92:[1024]	93:[1024]	94:[1024]	95:[1024]	96:[1024]	97:[1024]	98:[1024]	99:[1024]			
	100:[1024]	101:[****]	102:[****]	103:[****]	104:[****]	105:[****]	106:[****]	107:[****]	108:[****]	109:[****]			
	110:[****]	111:[****]	112:[****]	113:[****]	114:[****]	115:[****]	116:[****]	117:[****]	118:[****]	119:[****]			
	120:[****]	121:[****]	122:[****]	123:[****]	124:[****]	125:[****]	126:[****]	127:[****]	128:[****]	129:[****]			
	130:[****]	131:[****]	132:[****]	133:[****]	134:[****]	135:[****]	136:[****]	137:[****]	138:[****]	139:[****]			

当前位罟: 密钼信息 >>RSA密钼信息

![](_page_22_Picture_4.jpeg)

用户手册

![](_page_23_Picture_0.jpeg)

用户手册

当前位置: 密钥信息>>SM9主密钥信息

SM9主密钥

0:	E:[ 256 ]	1:	E:[ 256 ]	2:	E:[ *** ]	3:	E:[ 256 ]
	S:[ 256 ]		S:[ 256 ]		S:[ *** ]		S:[ 256 ]

冬	23
冬	Z3

当前位置: 密钥信息>>SM9用户密钥信息

SM9用户密钥													
0:	E:[ 256 ] S:[ *** ]	1:	E:[ 256 ] S:[ 256 ]	2:	E:[ *** ] S:[ 256 ]	3:	E:[ 256 ] S:[ 256 ]	4:	E:[ *** ] S:[ *** ]	5:	E:[ *** ] S:[ *** ]	6:	E:[ *** ] S:[ *** ]
7:	E:[ *** ] S:[ *** ]	8:	E:[ *** ] S:[ *** ]	9:	E:[ *** ] S:[ *** ]	10:	E:[ *** ] S:[ *** ]	11:	E:[ *** ] S:[ *** ]	12:	E:[ *** ] S:[ *** ]	13:	E:[ *** ] S:[ *** ]
14:	E:[ *** ] S:[ *** ]	15:	E:[ *** ] S:[ *** ]	16:	E:[ *** ] S:[ *** ]	17:	E:[ *** ] S:[ *** ]	18:	E:[ *** ] S:[ *** ]	19:	E:[ *** ] S:[ *** ]	20:	E:[ *** ] S:[ *** ]
21:	E:[ *** ] S:[ *** ]	22:	E:[ *** ] S:[ *** ]	23:	E:[ *** ] S:[ *** ]	24:	E:[ *** ] S:[ *** ]	25:	E:[ *** ] S:[ *** ]	26:	E:[ *** ] S:[ *** ]	27:	E:[ *** ] S:[ *** ]
28:	E:[ *** ] S:[ *** ]	29:	E:[ *** ] S:[ *** ]	30:	E:[ *** ] S:[ *** ]	31:	E:[ *** ] S:[ *** ]	32:	E:[ *** ] S:[ *** ]	33:	E:[ *** ] S:[ *** ]	34:	E:[ *** ] S:[ *** ]
35:	E:[ *** ] S:[ *** ]	36:	E:[ *** ] S:[ *** ]	37:	E:[ *** ] S:[ *** ]	38:	E:[ *** ] S:[ *** ]	39:	E:[ *** ] S:[ *** ]	40:	E:[ *** ] S:[ *** ]	41:	E:[ *** ] S:[ *** ]
42:	E:[ *** ] S:[ *** ]	43:	E:[ *** ] S:[ *** ]	44:	E:[ *** ] S:[ *** ]	45:	E:[ *** ] S:[ *** ]	46:	E:[ *** ] S:[ *** ]	47:	E:[ *** ] S:[ *** ]	48:	E:[ *** ] S:[ *** ]
49:	E:[ *** ] S:[ *** ]	50:	E:[ *** ] S:[ *** ]	51:	E:[ *** ] S:[ *** ]	52:	E:[ *** ] S:[ *** ]	53:	E:[ *** ] S:[ *** ]	54:	E:[ *** ] S:[ *** ]	55:	E:[ *** ] S:[ *** ]
56:	E:[ *** ] S:[ *** ]	57:	E:[ *** ] S:[ *** ]	58:	E:[ *** ] S:[ *** ]	59:	E:[ *** ] S:[ *** ]	60:	E:[ *** ] S:[ *** ]	61:	E:[ *** ] S:[ *** ]	62:	E:[ *** ] S:[ *** ]
63:	E:[ *** ] S:[ *** ]	64:	E:[ *** ] S:[ *** ]	65:	E:[ *** ] S:[ *** ]	66:	E:[ *** ] S:[ *** ]	67:	E:[ *** ] S:[ *** ]	68:	E:[ *** ] S:[ *** ]	69:	E:[ *** ] S:[ *** ]

图 24

图 26

设备信息菜单	当前位置:密钥信息>>DSA密钥信息									
密钥信息菜单	DSA密钥									
RSA密钥信息 PSM2密钥信息	0:[****] 1:[****] 2:[****] 3:[****] 4:[****] 5:[****] 6:[****] 7:[****] 8:[****] 9:[****]									
SM9主密钥信息	10:[****] 11:[****] 12:[****] 13:[****] 14:[****] 15:[****] 16:[****] 17:[****] 18:[****] 19:[****]									
SM9用户密钥信	20:[****] 21:[****] 22:[****] 23:[****] 24:[****] 25:[****] 26:[****] 27:[****] 28:[****] 29:[****]									
🥜 对称密钥信息	30:[****] 31:[****] 32:[****] 33:[****] 34:[****] 35:[****] 36:[****] 37:[****] 38:[****] 39:[****]									
<b>D</b> SA密钥信息	40:[****] 41:[****] 42:[****] 43:[****] 44:[****] 45:[****] 46:[****] 47:[****] 48:[****] 49:[****]									
<ul> <li>DH密钥信息</li> <li>ECP密钥信息</li> </ul>	50:[****] 51:[****] 52:[****] 53:[****] 54:[****] 55:[****] 56:[****] 57:[****] 58:[****] 59:[****]									
密钥管理菜单	60:[****] 61:[****] 62:[****] 63:[****] 64:[****] 65:[****] 66:[****] 67:[****] 68:[****] 69:[****]									
国标密钥信息	70:[****] 71:[****] 72:[****] 73:[****] 74:[****] 75:[****] 76:[****] 77:[****] 78:[****] 79:[****]									
国标密钥管理	80:[****] 81:[****] 82:[****] 83:[****] 84:[****] 85:[****] 86:[****] 87:[****] 88:[****] 89:[****]									
密钥备份管理	90:[****] 91:[****] 92:[****] 93:[****] 94:[****] 95:[****] 96:[****] 97:[****] 98:[****] 99:[****]									
权限管理菜单	100:[****] 101:[****] 102:[****] 103:[****] 104:[****] 105:[****] 106:[****] 107:[****] 108:[****] 109:[****]									
服务配置菜单	110:[****] 111:[****] 112:[****] 113:[****] 114:[****] 115:[****] 116:[****] 117:[****] 118:[****] 119:[****]									
日志管理菜单	120:[****] 121:[****] 122:[****] 123:[****] 124:[****] 125:[****] 126:[****] 127:[****] 128:[****] 129:[****]									
设备监控菜单	130:[****] 131:[****] 132:[****] 133:[****] 134:[****] 135:[****] 136:[****] 137:[****] 138:[****] 139:[****]									
双机热备功能	140:[****] 141:[****] 142:[****] 143:[****] 144:[****] 145:[****] 146:[****] 147:[****] 148:[****] 149:[****]									
设备管理菜单	150:[****] 151:[****] 152:[****] 153:[****] 154:[****] 155:[****] 156:[****] 157:[****] 158:[****] 159:[****]									
	160:[****] 161:[****] 162:[****] 163:[****] 164:[****] 165:[****] 166:[****] 167:[****] 168:[****] 169:[****]									

当前位置:	密钥信息>	> 对称密钥信息	3								
对称密钥	对称密钥信息										
	0:[32]	1:[32]	2:[**]	3:[**]	4:[**]	5:[32]	6:[**]	7:[**]	8:[**]	9:[**]	
	10:[32]	11:[**]	12:[32]	13:[**]	14:[**]	15:[**]	16:[**]	17:[**]	18:[**]	19:[**]	
	20:[**]	21:[**]	22:[**]	23:[**]	24:[**]	25:[**]	26:[**]	27:[**]	28:[**]	29:[**]	
	30:[**]	31:[**]	32:[**]	33:[**]	34:[**]	35:[**]	36:[**]	37:[**]	38:[**]	39:[**]	
	40:[**]	41:[**]	42:[**]	43:[**]	44:[**]	45:[**]	46:[**]	47:[**]	48:[**]	49:[**]	
	50:[**]	51:[**]	52:[**]	53:[**]	54:[**]	55:[**]	56:[**]	57:[**]	58:[**]	59:[**]	
	60:[**]	61:[**]	62:[**]	63:[**]	64:[**]	65:[**]	66:[**]	67:[**]	68:[**]	69:[**]	
	70:[**]	71:[**]	72:[**]	73:[**]	74:[**]	75:[**]	76:[**]	77:[**]	78:[**]	79:[**]	
	80:[**]	81:[**]	82:[**]	83:[**]	84:[**]	85:[**]	86:[**]	87:[**]	88:[**]	89:[**]	
	90:[**]	91:[**]	92:[**]	93:[**]	94:[**]	95:[**]	96:[**]	97:[**]	98:[**]	99:[**]	
1	100:[**]	101:[**]	102:[**]	103:[**]	104:[**]	105:[**]	106:[**]	107:[**]	108:[**]	109:[**]	
1	10:[**]	111:[**]	112:[**]	113:[**]	114:[**]	115:[**]	116:[**]	117:[**]	118:[**]	119:[**]	
1	120:[**]	121:[**]	122:[**]	123:[**]	124:[**]	125:[**]	126:[**]	127:[**]	128:[**]	129:[**]	
1	130:[**]	131:[**]	132:[**]	133:[**]	134:[**]	135:[**]	136:[**]	137:[**]	138:[**]	139:[**]	
					图 25	5					

![](_page_24_Picture_4.jpeg)

•

图 28

设备信息菜单	当前位置: 密钥信息	見>>ECP密钥信	息							
密钥信息菜单	ECP密钥									
RSA密钥信息 SM2密钥信息	0:[******]	1:[*****]	2:[*****]	3:[*****]	4:[*****]	5:[*****]	6:[*****]	7:[*****]	8:[*****]	9:[*****]
SM9主密钥信息	10:	11:	12:	13:	14:	15:	16:	17:	18:	19:
SM9用户密钥信	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]
	20:	21:	22:	23:	24:	25:	26:	27:	28:	29:
見 対称密钥信息	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]
	30:	31:	32:	33:	34:	35:	36:	37:	38:	39:
DSA密钥信息	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]
	40:	41:	42:	43:	44:	45	46.	47:	48:	49
P DH密钥信息	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]
	50:	51:	52:	53:	54:	55:	56:	57:	58:	59:
ECP密钥信息	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]
家细管调整单	60:	61:	62:	63:	64:	65:	66:	67:	68:	69:
密研官理楽甲	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]
	70:	71:	72:	73:	74:	75:	76:	77:	78:	79:
国标密钥管理	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]
	80:	81:	82:	83:	84:	85:	86:	87:	88:	89:
密钥备份管理	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]
	90:	91:	92:	93:	94:	95:	96:	97	98:	99:
权限管理菜单	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]
	100:	101	102:	103:	104:	105:	106:	107:	108:	109:
服务配置菜单	[******] 110:	$[^{******}_{111}]$	[******] 112	[******] 113	[******] 114	[******] 115	[******] 116:	[******] 117:	[******] 118	[******] 119
KeyStore管理	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]
	120:	121:	122	123:	124:	125	126:	127:	128:	129:
口志官理楽甲	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]
	130:	131:	132:	133:	134:	135:	136:	137:	138:	139:
双机热备功能	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]
	140:	141:	142:	143:	144:	145:	146:	147:	148:	149
设备管理菜单	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]	[******]
	150:	151:	152:	153:	154:	155:	156:	157:	158:	159:
	[******] 160	[******]	[******]	[******] 163	[******] 164	[******] 165	[******]	[******]	[******]	[******]

设备信息菜单	当前位登	:密钥信息	見>>DH密钥信	記							
密钥信息菜单	DH密钥										
RSA密钥信息 P SM2密钥信息		0:[****]	1:[****]	2:[****]	3:[****]	4:[****]	5:[****]	6:[****]	7:[****]	8:[****]	9:[****]
SM9主密钥信息	1	0:[****]	11:[****]	12:[****]	13:[****]	14:[****]	15:[****]	16:[****]	17:[****]	18:[****]	19:[****]
SM9用户密钥信	2	0:[****]	21:[****]	22:[****]	23:[****]	24:[****]	25:[****]	26:[****]	27:[****]	28:[****]	29:[****]
🤎 对称密钥信息	3	0:[****]	31:[****]	32:[****]	33:[****]	34:[****]	35:[****]	36:[****]	37:[****]	38:[****]	39:[****]
✔ DSA密钥信息	4	0:[****]	41:[****]	42:[****]	43:[****]	44:[****]	45:[****]	46:[****]	47:[****]	48:[****]	49:[****]
CP密钥信息 CP密钥信息	5	0:[****]	51:[****]	52:[****]	53:[****]	54:[****]	55:[****]	56:[****]	57:[****]	58:[****]	59:[****]
密钥管理菜单	6	0:[****]	61:[****]	62:[****]	63:[****]	64:[****]	65:[****]	66:[****]	67:[****]	68:[****]	69:[****]
国标密钥信息	7	0:[****]	71:[****]	72:[****]	73:[****]	74:[****]	75:[****]	76:[****]	77:[****]	78:[****]	79:[****]
国标密钥管理	8	0:[****]	81:[****]	82:[****]	83:[****]	84:[****]	85:[****]	86:[****]	87:[****]	88:[****]	89:[****]
密钥备份管理	9	0:[****]	91:[****]	92:[****]	93:[****]	94:[****]	95:[****]	96:[****]	97:[****]	98:[****]	99:[****]
权限管理菜单	10	0:[****]	101:[****]	102:[****]	103:[****]	104:[****]	105:[****]	106:[****]	107:[****]	108:[****]	109:[****]
服务配置菜单	11	0:[****]	111:[****]	112:[****]	113:[****]	114:[****]	115:[****]	116:[****]	117:[****]	118:[****]	119:[****]
日志管理菜单	12	0:[****]	121:[****]	122:[****]	123:[****]	124:[****]	125:[****]	126:[****]	127:[****]	128:[****]	129:[****]
设备监控菜单	13	0:[****]	131:[****]	132:[****]	133:[****]	134:[****]	135:[****]	136:[****]	137:[****]	138:[****]	139:[****]
双机热备功能	14	0:[****]	141:[****]	142:[****]	143:[****]	144:[****]	145:[****]	146:[****]	147:[****]	148:[****]	149:[****]
设备管理菜单	15	0:[****]	151:[****]	152:[****]	153:[****]	154:[****]	155:[****]	156:[****]	157:[****]	158:[****]	159:[****]
	16	0:[****]	161:[****]	162:[****]	163:[****]	164:[****]	165:[****]	166:[****]	167:[****]	168:[****]	169:[****]

![](_page_25_Picture_5.jpeg)

![](_page_26_Picture_0.jpeg)

单击左侧菜单栏"国标密钥信息"按钮,进入密钥信息查看页面,查看国标格式的 RSA密钥、SM2密钥、对称密钥,如图29-30。

当前位置:	国标密钥信息>	>国标F	RSA密钥信息										
国标RSA密	胡信息												
1:	E:[2048] S:[1024]	2:	E:[****] S:[****]	3:	E:[****] S:[****]	4:	E:[****] S:[****]	5:	E:[****] S:[****]	6:	E:[****] S:[****]	7:	E:[****] S:[****]
8:	E:[****] S:[****]	9:	E:[****] S:[****]	10:	E:[1024] S:[****]	11:	E:[****] S:[****]	12:	E:[****] S:[****]	13:	E:[****] S:[****]	14:	E:[****] S:[****]
15:	E:[****] S:[****]	16:	E:[****] S:[****]	17:	E:[****] S:[****]	18:	E:[****] S:[****]	19:	E:[****] S:[****]	20:	E:[****] S:[****]	21:	E:[****] S:[****]
22:	E:[****] S:[****]	23:	E:[****] S:[****]	24:	E:[****] S:[****]	25:	E:[****] S:[****]	26:	E:[****] S:[****]	27:	E:[****] S:[****]	28:	E:[****] S:[****]
29:	E:[****] S:[****]	30:	E:[****] S:[****]	31:	E:[****] S:[****]	32:	E:[****] S:[****]	33:	E:[****] S:[****]	34:	E:[****] S:[****]	35:	E:[****] S:[****]
36:	E:[****] S:[****]	37:	E:[****] S:[****]	38:	E:[****] S:[****]	39:	E:[****] S:[****]	40:	E:[****] S:[****]	41:	E:[****] S:[****]	42:	E:[****] S:[****]
43:	E:[****] S:[****]	44:	E:[****] S:[****]	45:	E:[****] S:[****]	46:	E:[****] S:[****]	47:	E:[****] S:[****]	48:	E:[****] S:[****]	49:	E:[****] S:[****]
50:	E:[****] S:[****]	51:	E:[****] S:[****]	52:	E:[****] S:[****]	53:	E:[****] S:[****]	54:	E:[****] S:[****]	55:	E:[****] S:[****]	56:	E:[****] S:[****]
57:	E:[****] S:[****]	58:	E:[****] S:[****]	59:	E:[****] S:[****]	60:	E:[****] S:[****]	61:	E:[****] S:[****]	62:	E:[****] S:[****]	63:	E:[****] S:[****]
64:	E:[****] S:[****]	65:	E:[****] S:[****]	66:	E:[****] S:[****]	67:	E:[****] S:[****]	68:	E:[****] S:[****]	69:	E:[****] S:[****]	70:	E:[****] S:[****]

图 29

当前位盂: 臣	谢怀密钥信息>	>国标SI	MZ密钥信息										
国标SM2密销	脂息												
1:	E:[ 256 ] S:[ 256 ]	2:	E:[ *** ] S:[ 256 ]	3:	E:[ 256 ] S:[ *** ]	4:	E:[ *** ] S:[ *** ]	5:	E:[ 256 ] S:[ *** ]	6:	E:[ 256 ] S:[ *** ]	7:	E:[ *** ] S:[ *** ]
8:	E:[ *** ] S:[ *** ]	9:	E:[ *** ] S:[ *** ]	10:	E:[ 256 ] S:[ *** ]	11:	E:[ *** ] S:[ *** ]	12:	E:[ *** ] S:[ *** ]	13:	E:[ *** ] S:[ *** ]	14:	E:[ *** ] S:[ *** ]
15:	E:[ *** ] S:[ *** ]	16:	E:[ *** ] S:[ *** ]	17:	E:[ *** ] S:[ *** ]	18:	E:[ *** ] S:[ *** ]	19:	E:[ *** ] S:[ *** ]	20:	E:[ *** ] S:[ *** ]	21:	E:[ *** ] S:[ *** ]
22:	E:[ *** ] S:[ *** ]	23:	E:[ *** ] S:[ *** ]	24:	E:[ *** ] S:[ *** ]	25:	E:[ *** ] S:[ *** ]	26:	E:[ *** ] S:[ *** ]	27:	E:[ *** ] S:[ *** ]	28:	E:[ *** ] S:[ *** ]
29:	E:[ *** ] S:[ *** ]	30:	E:[ *** ] S:[ *** ]	31:	E:[ *** ] S:[ *** ]	32:	E:[ *** ] S:[ *** ]	33:	E:[ *** ] S:[ *** ]	34:	E:[ *** ] S:[ *** ]	35:	E:[ *** ] S:[ *** ]
36:	E:[ *** ] S:[ *** ]	37:	E:[ *** ] S:[ *** ]	38:	E:[ *** ] S:[ *** ]	39:	E:[ *** ] S:[ *** ]	40:	E:[ *** ] S:[ *** ]	41:	E:[ *** ] S:[ *** ]	42:	E:[ *** ] S:[ *** ]
43:	E:[ *** ] S:[ *** ]	44:	E:[ *** ] S:[ *** ]	45:	E:[ *** ] S:[ *** ]	46:	E:[ *** ] S:[ *** ]	47:	E:[ *** ] S:[ *** ]	48:	E:[ *** ] S:[ *** ]	49:	E:[ *** ] S:[ *** ]
50:	E:[ *** ] S:[ *** ]	51:	E:[ *** ] S:[ *** ]	52:	E:[ *** ] S:[ *** ]	53:	E:[ *** ] S:[ *** ]	54:	E:[ *** ] S:[ *** ]	55:	E:[ *** ] S:[ *** ]	56:	E:[ *** ] S:[ *** ]
57:	E:[ *** ] S:[ *** ]	58:	E:[ *** ] S:[ *** ]	59:	E:[ *** ] S:[ *** ]	60:	E:[ *** ] S:[ *** ]	61:	E:[ *** ] S:[ *** ]	62:	E:[ *** ] S:[ *** ]	63:	E:[ *** ] S:[ *** ]
64:	E:[ *** ] S:[ *** ]	65:	E:[ *** ] S:[ *** ]	66:	E:[ *** ] S:[ *** ]	67:	E:[ *** ] S:[ *** ]	68:	E:[ *** ] S:[ *** ]	69:	E:[ *** ] S:[ *** ]	70:	E:[ *** ] S:[ *** ]

![](_page_27_Picture_1.jpeg)

#### 3.4 服务器密码机秘钥管理

#### 3.4.1 设备主密钥更新

单击左侧菜单栏"密钥管理",并单击"管理密钥"按钮,如图31。单击网页中"管 理密钥初始化"按钮,完成密钥初始化。设置设备主密钥需要满足管理员权限。

设备信息菜单	当則位立: 密钥官理>>官理密钥
密钥信息菜单	管理密钥
密钥管理菜单	
🔅 管理密钥	
🔅 设备密钥	
🔯 RSA密钥	
🔅 RSA密钥批	
里	
o SM2密钥	
SM2密钥批	
童	
🔅 SM9主密钥	
🔅 SM9用户密	
钥	
🔯 对称密钥	
🔅 对称密钥批	
里	
🔅 公钥导出	
<b>读</b> P10证书	
<b>读</b> P12证书	
🔯 DSA密钥	
DH密钥	
🔅 ECP密钥	
国标密钥信息	
国标密钥管理	·

图 31

#### 3.4.2 RSA密钥添加/删除

对密钥的添加、删除操作,需要满足管理员权限。

单击左侧菜单栏"密钥管理"按钮,进入"RSA密钥"页面如图32。输入密钥号并选择模长,可进行RSA密钥的生成与删除。

![](_page_28_Picture_1.jpeg)

华翼微电子

图 32

单击左侧菜单栏"密钥管理"按钮,进入"RSA密钥批量"界面如图33。输入密钥号范围,选择模长之后,可进行RSA密钥的批量生成与删除。

	当前位责: 密钥管理>>RSA密钥批理
家钥伫自苏单	RSA实组版图
當胡信息米半	
密钥管理菜单	樓长: ● 1024 ○ 2048 ○ 3072 ○ 4096
◎ 管理密钥	起始來知号:
Q 设备密钥	
o RSA密钥	终止密钥号:
Q RSA密钥批	指数: 65537 🗸
里 一里	
O SM2密钥	批量生成密钥 批量删除密钥
SM2密钥批	
里	
ONOH 合物	
SM9用户密	
2. 刘称密钥机	
里 小細尼山	
○ 公明寺正	
国标密钥信息	
国标密钥管理	

![](_page_29_Picture_0.jpeg)

#### 3.4.3 SM2密钥添加/删除

对密钥的添加、删除操作,需要满足管理员权限。

单击左侧菜单栏"密钥管理"按钮,进入"SM2密钥"页面如图34。输入密钥号可进行SM2密钥的生成与删除。

设备信息菜单	当前位置:密钥管理>>SM2密钥
密钥信息菜单	SM2密钥
密钥管理菜单	
○ 管理密钥	密钥号:
🔅 RSA密钥	生成治明
🔯 RSA密钥批	
里	
of SM2密钥	
🔅 SM2密钥批	
里	
SM9主密钥	
SM9用户密	
钥	
◎ 対称密钥	
222 刘利岱钥机	
▲ 从知己中	
2 の守出 2 の守出	
<b>0</b> P12证书	
o DSA密钥	
o DH密钥	
🔯 ECP密钥	
国标密钥信息	
国标密钥管理	

图 34

单击左侧菜单栏"密钥管理"按钮,进入"SM2密钥批量"界面如图35。输入密钥号范围可进行SM2密钥的批量生成与删除。

登着信息菜单       当前位置: 密钥管理>>SM2密钥批量         密封管理菜单       34台密拐号:         會 语電密調       後止密拐号:         會 珍念密钥       後止密钥号:         會 SM2密钥       後止密钥号:         ● SM2密钥       後止密钥         ● SM2密钥       ●         ● SM2密<       ●         ● SM2密       ●         ● SM2密       ●         ● SM2密       ●         ● SM2密       ●         ● SM2 (如用)       ●         ● SM2 (如用)       ●         ● SM2 (如用)       ●         ● SM2 (如用)       ●         ● SM3(1)       ●         ● SM3(2)       ●         ● P1024H       ●         ● F104H <th>HUAYI MICRO-ELECTRONICS</th> <th></th> <th>用户手册</th>	HUAYI MICRO-ELECTRONICS		用户手册
	设备信息菜单	当前位置: 密钥管理>>SM2密钥批量	
<ul> <li>法給密期号:</li> <li>送給密期号:</li> <li>送給密期号:</li> <li>送給密期号:</li> <li>送給密期号:</li> <li>送金密期</li> <li>送上密期号:</li> <li>送加密期</li> <li>送加密期</li> <li>送加密期</li> <li>ジロ空期</li> <li>ジ目の正书</li> <li>ジロ空邦</li> <li>ジロ空邦</li> <li>ジロ空邦</li> <li>ジロ空期</li> <li>ジロ空期</li> </ul>	密钥信息菜单	SM2密钥批里	
<ul> <li>○ 日本部</li> <li>○ ○本密钥</li> <li>○ ○ ○本密钥</li> <li>○ ○ ○ ○ ○ ○</li> <li>○ ○ ○ ○</li> <li>○ ○ ○ ○</li> <li>○ ○ ○ ○</li> <li>○ ○ ○</li> <li>○ ○ ○</li> <li>○ ○ ○ ○</li> <li>○ ○ ○ ○</li> <li>○ ○ ○ ○</li> <li>○ ○ ○ ○ ○</li> <li>○ ○ ○ ○ ○</li> <li>○ ○ ○ ○ ○ ○ ○</li> <li>○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○</li></ul>	密钥管理菜单	起始密钥号:	
※ SA密钥       #里生麻密钥       #里生麻密钥       #里無影響       #         第       SM2密钥       #	<ul> <li>↓</li> <li>↓</li></ul>	终止密钥号:	
<ul> <li>■ 10-100 1000</li> <li>● 10-1000</li> <li>●</li></ul>	RSA密钥     RSA密钥     RSA密钥	批單生成密钥 批單刪除密钥	
SM2密钥         SM2密钥         SM9主席目         SM9主席目         SM9自户密         J称密钥         J尔称密钥         J尔尔雷         J印         JT         J	里		
SM2密钥此         U         SM9主密钥         SM9自户密         SM9用户密         JM杯密钥         JM杯密钥比         JM不密钥比         JM不密钥比         U         V         SM9自户密         JM杯密钥         SM9自户密         JM杯密钥         SM9自户密         P10正书         P12证书         SM目空         P12证书         SM名         P12证书         SM目空         P12证书         SM目空         P12证书         SM目空         P12证书         SM3         SM1         SM1         SM1         SM1         SM1         SM1          SM1	of SM2密钥		
I       I         I       I <td< td=""><td>☆ SM2密钥批</td><td></td><td></td></td<>	☆ SM2密钥批		
<ul> <li>NP 生活明</li> <li>SM9用户密</li> <li>列称密钥</li> <li>列称密钥</li> <li>刘称密钥</li> <li>刘称密钥</li> <li>刘称密钥</li> <li>型 「</li> <li>「</li> <li>P10正书</li> <li>P12正书</li> <li>P12正书</li> <li>P12正书</li> <li>P12正书</li> <li>P12正书</li> <li>P12正书</li> <li>ECP密钥</li> </ul>	里 200 主应知		
<ul> <li>Interface</li> <li>Interfac</li></ul>	<ul> <li>SM9里密朝</li> <li>SM9用户密</li> </ul>		
<ul> <li>対称密钥</li> <li>対称密钥</li> <li>対称密钥</li> <li>対称密钥</li> <li>対称密钥</li> <li>型</li> <li>公明导出</li> <li>ジロ荘书</li> <li>P12证书</li> <li>P13本</li> <li>D5A密钥</li> <li>D5A密钥</li> <li>DF密钥</li> <li>ECP密钥</li> </ul>	钥		
図称密钥批         単         ② 公明导出         ④ P10证书         ④ P12证书         ④ DSA密钥         ④ DH密钥         ● ECP密钥	◎ 对称密钥		
<ul> <li>里</li> <li>公親导出</li> <li>ジロ正书</li> <li>ジロ正书</li> <li>ジロン正书</li> <li>ジロン正书</li> <li>ジロンボー</li> <li>ジロン</li></ul>	🔯 对称密钥批		
公期导出         ②       P10证书         ③       P12证书         ④       DSA密钥         ④       DH密钥         ④       CP密钥	里		
P10证书              P12证书              DSA密钥              OH密钥              OH密钥	🔯 公钥导出		
・ロンボキ         ・ロン         ・ロ         ・ロ         ・ロン         ・ロ         ・ロ         ・ロ	🔅 P10证书		
OSA密朝                  OH密朝                  OH密朝                 OECP密朝	🔅 P12证书		
<ul> <li>☑ DH密钥</li> <li>☑ ECP密钥</li> </ul>	🔯 DSA密钥		
✿ ECP密钥	or DH密钥		
	🔅 ECP密钥		
	围起家知管理		

#### 3.4.4 SM9主密钥添加/删除

SM9主密钥的添加、删除操作,需要满足管理员权限。

单击左侧菜单栏"密钥管理"按钮,进入"SM9主密钥"页面。如果此设备算法类型不支持SM9密钥,则相关菜单选项为灰色,不可操作。如图36所示。

华翼微电子 HUAYI MICRO-ELECTRONICS		用户手册
设备信息菜单	当前位置:密钥管理>>SM9主密钥	
密钥信息菜单	SM9主密钥	
密钥管理菜单	密钥号:	
<ul> <li>☆ 管理密钥</li> <li>☆ 込み応知</li> </ul>	密钥类型:	
して して して して して して して して して して		
o RSA密钥批	生成密钥 删除密钥	
量		
of SM2密钥		
M2密钥批		
童		
▲ SM9主密钥		
🏠 SM9用户密		
钥		
🔯 对称密钥		
🔅 对称密钥批		
里		
◎ 公钥导出		
P10证书		
○ P12证书		
ODSA密钥		
o ECP密钥		
国标密钥信息		
国标密钥管理		

若此设备算法类型支持SM9密钥操作,在密钥号输入框中输入指定密钥号,密钥类型可以选择加密密钥、签名密钥,单击"添加"按钮,完成SM9主密钥添加;在密钥号输入框中输入指定密钥号,单击"删除"按钮,完成SM9主密钥删除。如图37。

HUAYI MICRO-ELECTRONICS		用户手册
设备信息菜单	当前位置:密钥管理>>SM9主密钥	
密钥信息菜单	SM9主密钥	
密钥管理菜单	密钥号: 1	
管理密钥		
○ 设备密钥		
o RSA密钥	十 武态组 叫哈会态组	
● KSA密钥批		
E SM2寧钼		
SM2密钥批		
₫		
o SM9主密钥		
SM9用户密		
3		
◎ 对称密钥		
对称密钥批		
₫ 小細島忠		
► P10证书		
o P12证书		
of DSA密钥		
of DH密钥		
■ ECP密钥		
标密钥信息		
国标密钼管理		

#### 3.4.5 SM9用户密钥添加/删除

SM9用户密钥的添加、删除操作,需要满足管理员权限。

单击左侧菜单栏"密钥管理"按钮,并单击"SM9用户密钥"按钮,进入SM9用户密 钥管理界面。如果此设备算法类型不支持SM9密钥,则相关菜单选项为灰色,不可操作。 如图38所示。

NO ELECTRONICS		用户于
设备信息菜单	当前位置: 密钥管理>>SM9用户密钥	
密钥信息菜单	SM9用户密钥	
密钥管理菜单	主座钥号:	
🍻 管理密钥		
😳 设备密钥	用尸密钥号:	
o RSA密钥	用户ID:	
RSA密钥批	密钥类型: ①加密密钥 〇签名密钥	
<ul> <li>◇ SM2密钥</li> <li>◇ SM2密钥批</li> <li>型</li> <li>◇ SM9主密钥</li> <li>◇ SM9用户密</li> <li>闭 对称密钥</li> <li>◇ 对称密钥</li> <li>型</li> </ul>	生成密钥 删除密钥	
<ul> <li>公明寺山</li> <li>第10征书</li> <li>第12征书</li> <li>DSA密钥</li> <li>DF密钥</li> <li>ECP密钥</li> </ul>		
国际密钥信息		

若此设备支持SM9算法,在密钥号输入框中输入指定主密钥号、用户密钥号、用户 id,密钥类型可以选择加密密钥、签名密钥,单击"添加"按钮,完成SM9用户密钥添 加;在密钥号输入框中输入指定用户密钥号,单击"删除"按钮,完成SM9用户密钥删 除。如图39。

![](_page_34_Picture_0.jpeg)

![](_page_34_Picture_1.jpeg)

用自动来干	3前12五:密钥官理>>5M9用户3	出租
<b>相信息菜单</b>	SM9用户密钥	
钥管理菜单	主密钥号:	1
管理密钥	田白漆钥号・	
设备密钥	用广面物与。	
RSA密钥	用户ID:	2
RSA密钥批	密钥类型:	●加密密钥 ○签名密钥
CMOSSER		
SM2密钥 SM2密钥	生成密钥  删除密钥	
SMQ主恋妇		
SM9里立物 SM9田白廠		
对称密钥		
对称密钥批		
公钥导出		
P10证书		
P12证书		
DSA密钥		
DHISSE		
2 D. 1 D. D. 1		
ECP密钥		

#### 3.4.6 对称密钥添加/删除

对密钥的添加、删除操作,需要满足管理员权限。 单击左侧菜单栏"密钥管理"按钮,并单击"对称密钥"按钮,如图40。

AICRO-ELECTRONICS		用户手
设备信息菜单	位置: 密钥管理>>对称密钥	
密钥信息菜单    对利	密钥	
密钥管理菜单	<b>应</b> 钮是:	
🄯 管理密钥		
◎ 设备密钥	密朝太度: 32 ▼	
◎ RSA密钥	生成率组 删除率组	
日本の日本の日本		
土 (1) SM2密钥		
i SM2密钥批		
里		
✿ SM9主密钥		
☆ SM9用户密		
钥		
2 对称密钥		
里		
☆ 公钥导出		
<b>读</b> P10证书		
✿ P12证书		
DSA密钥		
DH密钥		
ecp密钥		

添加/删除对称密钥时需要满足管理员权限,在密钥号输入框中输入指定密钥号, 密钥长度可选择8、16、24、32,单击"添加"按钮,完成对称密钥添加;

在密钥号输入框中输入指定密钥号,单击"删除"按钮,完成对称密钥删除。

单击左侧菜单栏"密钥管理"按钮,进入"对称密钥批量"界面,如图41。输入密 钥号范围,并选择号密钥长度可进行密钥的批量生成与删除。

![](_page_36_Picture_0.jpeg)

#### 3.4.7 导出公钥

单击左侧菜单栏"密钥管理"按钮,并单击"公钥导出"按钮,如图42。

华異微电于 HUAYI MICRO-ELECTRONICS		用户手册
设备信息菜单	当前位置: 密钥管理>>公钥导出 公钥号出	
<b>密钥管理菜单</b> <b>管理密钥</b>	算法: ●SM2 ○RSA 家钼号:	
◎ 设备密钥 ◎ RSA密钥 ◎ RSA密钥 ◎ RSA密钥批	导出公钥	
単 ☆ SM2密钥 ☆ SM2密钥 が SM2密钥批		
田     田     田     SM9主密钥     ひ     SM9用     戸密     SM9用     戸密     SM9用     P密     SM9     SM9用     P密     SM9     SM     SM9     SM9     SM9     SM9     SM9     SM9     SM9     SM     SM		
<ul> <li>钥</li> <li>动称密钥</li> <li>动称密钥</li> </ul>		
<ul> <li>♀ P10证书</li> <li>♀ P12证书</li> <li>♀ DSA密钥</li> </ul>		
DH密钥     DF密钥     ECP密钥		
国标密钥信息 国标密钥管理 ↓		

#### 3.4.8 P10证书

单击左侧菜单栏"密钥管理"按钮,进入"p10证书"管理页面。生成p10的密钥号 必须提前生成密钥。然后,选择密钥类型,填写密钥号,并根据实际需要,填写办法对 象、国家、省/自治区、县市、单位、部门。并单击"P10证书"按钮,如图43。

![](_page_38_Picture_0.jpeg)

设备信息菜单	当前位置: 密钥管理>>P10证书			
密钥信息菜单	P10证书			
密钥管理菜单	密钥类型:	●SM2 ○ RSA		
○ 管理密钥 ○ 沿条応知	密钥号:	1		
of RSA密钥	颁发对象:	FM	颁发对象建议长度为1-100个字符	
ot RSA密钥批	国家:	CN		
	省伯治区	山本公		
SM2密钥 SM2恋钥W	目前日本	山水自		
0112257010	兰 兰 兰 兰 兰 兰 兰 兰 兰 兰 兰 兰 兰 兰 兰 兰 兰 兰 兰	ST用印		
SM9主密钥	半位:	Нү		
of SM9用户密	制门:	A		
	产生P10			
♀️ 刈称密钥 ず 对称密钥批				
公钥导出				
● P10证书				
DSA密钥				
of DH密钥				
of ECP密钥				
标密钥信息				
副标率钼管理				

#### 3.4.9 P12证书

华翼微电子

使用P12证书的导入功能可以将P12文件中的密钥导入指定密钥号中。如图44。选择需要导入的密钥号,并填写口令,然后上传p12证书,选择"导入p12证书"。提示导入成功,则对应的密钥类型的密钥号位置会导入p12证书中保存的密钥信息。

![](_page_39_Picture_0.jpeg)

设备信息菜单	当前位置:密钥管理>>P12证书
密钥信息菜单	P12证书
密钥管理菜单	密钥号: (RSA密钥号范围1383, SM2密钥号范围: 11023)
🔯 管理密钥	
◎ 设备密钥	
o RSA密钥	证书: 选择文件 未选择任何文件
100 KSA密钥机	
重 ■ SM2密钥	⇒∧P120±+3
★ SM2密钥批	
童	
os SM9主密钥	
🔅 SM9用户密	
钥	
🔯 对称密钥	
◎ 对称密钥批	
里 八知己山	
9. 公钥寻山 10证书	
<b>0</b> P12证书	
ot DSA密钥	
 OH密钥	
🔯 ECP密钥	
国标密钥信息	
国标密钥管理	

#### 3.4.10 密钥备份

华翼微电子

对密钥的备份操作,需要满足管理员权限。

单击左侧菜单栏"密钥备份",并单击"密钥备份"按钮,如图45。

华翼微电子 HUAYI MICRO-ELECTRONICS			用户手册
迅冬仁白芸苗	当前位罟: 密钥备份管理>>密钥备	份	
<b>双周间芯米干</b>	实明 <u>条</u> 码		
密钥信息采甲	近初间仍		
密钥管理菜单	密钥备份开始按钮:	开始备份	
国标密钥信息	下载备份文件:	下载备份文件	
国标密钥管理	下载合制keystore	T # the the Charge	
密钥备份管理	1.#XTEIBUKCASCOLC.	15年0元E前JKeyStore	
密钥备份			
🛃 密钥恢复			
₽ 定制KeyStore版			
夏			
权限管理菜单			
服务配置菜单			
KeyStore管理			
日志管理菜单			
设备监控菜单			
双机热备功能			
设备管理菜单			
STR BADK I			

密钥备份操作需要添加五个管理员并登陆。单击"开始备份"按钮,提示"确定开 始进行备份吗",点击确定后,跳转进入"密钥备份"管理页面。如图46。

备信息菜单	当前位置: 密钥备份管理>>	密钥备份		
钥信息菜单	密钥备份			
<b>I管理菜单</b>	序号 令牌序列号	刷新	令牌口令	保存密钥
密钥信息	1 请选择令牌 🗸	刷新	请输入密码	保存密钥
密钥管理	2 请选择令牌 ✔	刷新	请输入密码	保存密钥
<b>胡爾份官理</b> 密钥备份	3 请选择令牌 🗸	刷新	请输入密码	保存密钥
密钥恢复 Contractor and the	4 请法择会牌 ✔	刷新	请输入密码	保存密钥
"王明KeyStore成	5	刷新	清給入変码	保在麥組
管理菜单		16793		M 11 11 10
配置菜单			通历	
rStore管理				
志管理菜单				
發监控菜单				
肌热备功能				

在配置终端插入USB KEY, 输入USB KEY口令,单击保存密钥。提示成功后插入下一个管理员USB KEY,重复此前操作。5个管理员密钥保存完成后,"备份"按钮可以点击,如图47。

当前位置:	当前位置:密钥备份管理>>密钥备份						
密钥备份							
序号	角色	令牌序列号	令牌口令	保存密钥			
1	管理员	K1424170223B0261	******	保存密钥			
2	管理员	K1424170223B0263	******	保存密钥			
3	管理员	K1424170223B0265	******	保存密钥			
4	管理员	K1424170223B0425	******	保存密钥			
5	管理员	K1424170223B0426	******	保存密钥			
			备份 ○旧版 ◎新版				
			图 47				

37

![](_page_42_Picture_1.jpeg)

来自网页的消息
🛕 备份完成!
确定

然后单击"备份"按钮,等待备份完成,提示备份成功,如图48。

图 48

备份时,可选择备份为旧版本,或者新版本。旧版本备份文件兼容2015年之前的加密机服务器。新版本备份文件只能用于2015年之后的加密服务器中。

密钥备份完成后点击"下载备份文件"按钮,如图49,点击"保存"按钮,保存备 份文件到主机。请妥善保管该文件。本版本最多支持5次备份文件,用户管理的5把key 中只保留最新5次备份文件。

钥备份			
密钥备份开始按钮:	开始备份		
下载备份文件按钮:	下载备份文件	下载定制KeyStore	

图 49

#### 3.4.11 密钥恢复

![](_page_43_Picture_1.jpeg)

设备信息菜单	当前位置: 密钥备份管理>>密钥恢复			
密钥信息菜单	密钥恢复			
密钥管理菜单	1 选择备份文件			
国标密钥信息				
国标密钥管理	备份文件路径: 选择文件 未送	4择任何文件		
密钥备份管理				
名 密钥备份	2 恢复备份密钥			
P 密钥恢复 ○ chll/cn Charaelt	6 使田任音三个公娩即可恢复密组	1		
定制KeyStore版 有				
如明管理装备	序号 令牌序列号	刷新	令牌口令	取得密钥
收收官理采半	1 请选择令牌 🖌	刷新	请输入密码	取得密钥
KeyStore管理	2 请选择令牌 🗸	刷新	请输入密码	取得密钥
日志管理菜单	3 请选择令牌 🗸	刷新	请输入密码	取得密钥
设备监控菜单				
双机热备功能	备份文件版本: 请选择版本		~	
设备管理菜单	3 执行恢复操作			
	恢复			
	4			

单击左侧菜单栏"密钥管理"按钮,并单击"密钥恢复"按钮,如图50。

图 50

在进行密钥恢复功能前,请确认已经登录三个管理员。首先,选择备份文件,从五 个管理员KEY中任意选取三个即可完成恢复密钥的操作。在配置终端插入任意一个管理 员USB KEY,勾选对应的USB KEY序列号,输入USB KEY口令,单击"取得密钥"按钮, 提示成功后,插入下一个USB KEY,重复操作。获取3个密钥片段后,备份文件版本,可 以选择对应的备份文件版本,单击"恢复"按钮,如错误!未找到引用源。

![](_page_44_Picture_0.jpeg)

1 选择备伤	这件			
¥份文件路1	- 选择文件	axcsd1_2020_09_29_10_10_29.da	t	
○ 恢复备代 ● 使用任意 序号	注意的 一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個	<b>复密钥</b> ◇牌序列号	令牌口令	取得密钥
1	管理员	K1424170223B0261		取得密钥
2	管理员	K1424170223B0263		取得密钥
3	管理员	K1424170223B0265		取得密钥
4	管理员	K1424170223B0425	•••••	取得密钥
5	管理员	K1424170223B0426	•••••	取得密钥
¥份文件版	t: axcsd1_20	20_09_29_10_10_29	•	

#### 单击"恢复"进入恢复界面如图52。

华翼微电子 HUAYI MICRO-ELECTRONICS

	2 密钥正在恢复中,请耐心等待 当前位置: 数据备份恢复 >> 数据恢复									
勎	据恢复									
	备份文件路径	: 选择文件 a	axcsd1_2020_09_29_10_10_29.dat							
	● 使用任意日	一个令牌即可恢复	密钥							
	序号	角色	令牌序列号	令牌口令		取得密钥				
	1	管理员	K1424170223B0261			取得密钥				
	2	管理员	K1424170223B0263			取得密钥				
	3	管理员	K1424170223B0265	•••••		取得密钥				
	4	管理员	K1424170223B0425	•••••		取得密钥				
	5	管理员	K1424170223B0426	•••••		取得密钥				

![](_page_45_Picture_1.jpeg)

恢复完成,提示恢复成功。如图53。

![](_page_45_Picture_3.jpeg)

图 53

完成后进入恢复界面,单击"恢复"完成密钥恢复操作。

3.5 服务器密码机KeyStore配置管理

对密码机的KeyStore配置,需要满足管理员权限。

单击左侧菜单栏 "KeyStore管理"菜单,并单击 "KeyStore配置"菜单,如错误! 未找到引用源。4。

设备信息菜单	当前位置: KeyStore管理>>KeyStore配置
密钥信息菜单	KeyStore配置
密钥管理菜单	KeyStore位置: ④默认 〇定制
国标密钥信息	KeyStore别名: FMKS
国标密钥管理	密钥类型:
密钥 角 衍 官 理 如 阳 管 珊 蒂 单	KeyStore口令:
服务配置菜单	确认KeyStore口令:
KeyStore管理	私钥别名:
KeyStore配置	私钥口令:
KeyStore操作	确认私钥口令:
口芯目理采半	· · · · · · · · · · · · · · · · · · ·
双机热备功能	<b>数字证书:</b> 选择文件 未选择任何文件
设备管理菜单	副畫KeyStore 测试已配置KeyStore
s://124.133.2.85/htm	l/keyStore/keystorecfg.html

![](_page_46_Picture_1.jpeg)

加密机内的KeyStore分默认和定制两种方式,如果对keystore没有特殊要求,选择 默认方式,如果需要keystore扩容,需选择定制方式。默认方式的KeyStore空间只有20K, 能够存放的Keystore数据较小,定制方式的KeyStore空间为20M,可以存放较多的数据。 客户根据自己的应用需求,灵活选择。KeyStore测试功能可以检查配置是否正确。

通过keystore配置页面,可以对keystore进行枚举、删除、和清空等操作,如图55

设备信息菜单	当前位置: KeyStore管理>>KeySto	re操作
密钥信息菜单	KeyStore操作	
密钥管理菜单	KeyStore位置:	●默认 ○定制
国标密钥信息	KeyStore口令:	
国标密钥管理	校举keyStore信息:	1928 kauShna
密钥备份管理	신네마스	
权限管理菜单	私钥别名:	
服务配置菜单	获取别名证书信息:	获取证书信息
KeyStore管理	删除别名:	删除别名信息
KeyStore配置	清空keyStore:	清空keyStore
KeyStore mit		
日志官理楽単		
设备监控采甲		
<b>双机热备功能</b>		
设备管理菜单		

图 55

#### 3.6 服务器密码机日志管理

#### 3.6.1 服务器密码机日志设置

单击左侧菜单栏"日志管理"按钮,并单击"日志管理"按钮,如图56。

<b>—</b>	·	-	HH
HH			
н	1.		
/ 14	/	~	/ -/ -

设备信息菜单	当前位置:日	志管理>>日志管理						
密钥信息菜单	日志管理							
密钥管理菜单		日志等级:	ODEBUG	OWARN		OFATAL		
标密钥信息		日志大小・	0	单位,	M。日志大小坊	5国为030M(不含	30)	
标密钥管理		Щжусл.		-12.	не <u>пре</u> зеля	2007 Jon Control 1-E	557	
的智慧的管理	设定等	级 清除日志	下载日志					
2限管理菜单								
务配置菜单								
eyStore管理								
志管理菜单								
日志管理								
备监控菜单								
!机热备功能								
<b>备管理菜单</b>								

默认日志等级为ERROR,加密机出错时打日志,日志文件大小默认2M,单击"设置等级"按钮可以修改日志等级和日志大小。单击"清除日志"可以将日志文件删除。单击 "下载日志"可以将日志文件下载到本地。

3.6.2 审计查询

华翼微电子

进行审计查询是,需要有审计管理员权限。选择开始时间和结束时间后,单击"查 询"按钮,如错误!未找到引用源。7。

开始时	间:	2020-09-28	结束时间: 2020-09-30	重直	
审	it	删除审计日志 删除全部审计	+		
		令牌序列号	操作信息	操作时间	审计状态
	1	K1424170223B0261	user login success	2020-09-28 18:17:24:902	审计未通过
	2	K142417022380261	add white list ip 192.168.18.2- 192.168.18.30 success	2020-09-28 18:23:19:692	审计未通过
	3	K1424170223B0261	delete white list ip 192.168.18.2- 192.168.18.30 success	2020-09-28 18:24:25:474	审计未通过
	4	K1424170223B0261	back up data success	2020-09-29 08:27:30:191	审计未通过
	5	K1424170223B0261	back up data success	2020-09-29 08:32:33:042	审计未通过
	6	K1424170223B0261	back up data success	2020-09-29 08:42:46:076	审计未通过
	7	K1424170223B0261	KeyStore config success	2020-09-29 08:50:00:805	审计未通过
	8	K1424170223B0261	back up data success	2020-09-29 10:11:30:416	审计未通过
	9	K142417022380261	del RSA key success	2020-09-29 10:11:55:542	审计未通过
	10	K1424170223B0261	del RSA key success	2020-09-29 10:11:55:614	审计未通讨

#### 3.6.3 审计

审计功能需要有审计管理员权限才能进行审计操作。选择需要审计的日志,单击"审 计"按钮,审计状态修改为"审计通过",如图58。

と異微 AYI MICRO-EI	电于 ECTRONIC	s			用户手册
前位置:	日志闻	时管理 > 日志审计			
计日志	列表				
开始田	间:	2020-09-28	請東时间: 2020-09-30	画査询	
ij	计	删除审计日志 删除全部审计	+		
		令牌序列号	操作信息	操作时间	审计状态
	1	K1424170223B0261	user login success	2020-09-28 18:17:24:902	审计通过
	2	K1424170223B0261	add white list ip 192.168.18.2- 192.168.18.30 success	2020-09-28 18:23:19:692	审计通过
	3	K1424170223B0261	delete white list ip 192.168.18.2- 192.168.18.30 success	2020-09-28 18:24:25:474	审计通过
	4	K1424170223B0261	back up data success	2020-09-29 08:27:30:191	审计通过
	5	K1424170223B0261	back up data success	2020-09-29 08:32:33:042	审计通过
	6	K1424170223B0261	back up data success	2020-09-29 08:42:46:076	审计未通过
	7	K1424170223B0261	KeyStore config success	2020-09-29 08:50:00:805	审计未通过
	8	K1424170223B0261	back up data success	2020-09-29 10:11:30:416	审计未通过
	9	K1424170223B0261	del RSA key success	2020-09-29 10:11:55:542	审计未通过
	10	K1424170223B0261	del RSA key success	2020-09-29 10:11:55:614	审计未通过

#### 3.6.4 审计删除

审计删除操作需要有审计管理员权限才能进行。选择需要删除的的日志,单击"删除审计日志"按钮,选中的日志将被删除,如错误!未找到引用源。9。

-	华翼微电子 HUAYI MICRO-ELECTRONICS			用户手册
	删除成功		2020± 确定	∓09月29日 10:45:19 │ 退؛
12 1	审计管理 > 日志审计			
	2020-09-28 删除审计日志 删除全部审计	结束时间: 2020-09-30	画査询	
	令牌序列号	操作信息	操作时间	审计状态
	K1424170223B0261	user login success	2020-09-28 18:17:24:902	审计通过
	K1424170223B0261	add white list ip 192.168.18.2- 192.168.18.30 success	2020-09-28 18:23:19:692	审计通过
	K1424170223B0261	delete white list ip 192.168.18.2- 192.168.18.30 success	2020-09-28 18:24:25:474	审计通过
ł	K1424170223B0261	back up data success	2020-09-29 08:27:30:191	审计通过
5	K1424170223B0261	back up data success	2020-09-29 08:32:33:042	审计通过
6	K1424170223B0261	back up data success	2020-09-29 08:42:46:076	审计未通过
	K1424170223B0261	KeyStore config success	2020-09-29 08:50:00:805	审计未通过
1	K1424170223B0261	back up data success	2020-09-29 10:11:30:416	审计未通过

点击"删除审计日志"按钮,可以逐条删除审计日志。

点击"删除所有审计日志"按钮,将会清除目前所有保存的审计日志。

3.7 服务器密码机监控

服务器密码机当前业务操作监控

单击左侧菜单栏"设备监控"按钮,并单击"监控服务"按钮,如错误!未找到引用源。0。

![](_page_51_Picture_0.jpeg)

可以每隔几秒钟看到服务器密码机所作的操作和当前服务器密码机并发连接数目。

3.8 双机热备

双机热备需要两台密码机服务器,一台为主机,一台为从机,正常状态下由主机提 供服务,从机保持与主机的数据同步。当主机因故停止运行后,从机自动切换为主机, 继续提供服务。主从机的数据同步依赖于网络,所以在使用此功能时务必保持主从机的 网络通讯正常。

#### 3.8.1 服务器密码机热备设置

单击左侧菜单栏"双机热备"按钮,并单击"热备设置"按钮,如错误!未找到引用源。。

HUAYI MICRO-ELECTRONIC	8		用.	户号
设备信息菜单	当前位置: 双机热备配置>>热备;	:置		
密钥信息菜单	热备设置			
密钥管理菜单	网口端口:	eth0 🗙		
标密钥信息	辺如执冬市能状态。	¥		
标密钥管理				
阿爾希份管理	XX机热备功能设置:		221.23112333333333333333333333333333333	
限管理菜单	网络类型:	●IPv4 ○IPv6 (仅输	入ip默认掩码为24,若要配置掩码,可输入形如"192.168.18.239/27")	
<b>影</b> 配置菜单	输入服务IP:	192.168.18.94		
eyStore管理	输入另一台设备IP:	192.168.18.90		
志管理菜单	虚拟路由ID(1-255):	61		
设备监控菜单				
Q机热备功能	双机热备配置			
▲ 热备设置				
▲ 数据同步				
设备管理菜单				

(一)、开启双击热备功能:

双机热备功能的开启,需要2台加密机A和B配合完成。选中网口端口,输入要进行 配置的网口、点击选中 "启动双机热备";随后输入 服务器 设备IP,另一台机器设 备的 IP,虚拟路由ID;点击 "双击热备配置" 按钮,来保存配置信息。重启加密机 服务器后,双机热备的设置才能生效。如图62所示。

备信息菜单	当前位置: 双机热备配置>>热备;	<u>殳署</u>
钥信息菜单	热备设置	
钥管理菜单	网口端口:	eth0 V
标密钥信息	─────────────────────────────────────	¥
际密钥管理	20加执冬市影识罕,	
钥备份管理	2000次1回9月1111100点:	
限管理菜单	网络类型:	●IPv4 ○IPv6 (仅输入IP默认摘码为24,若要酷告摘码,可输入形如"192.168.18.239/27")
务配置菜单	输入服务IP:	192.168.18.94
yStore管理	输入另一台设备IP:	192.168.18.90
志管理菜单	虚拟路由ID(1-255):	61
备监控菜单		
机热备功能	双机热备配置	
热备设置		
备管理菜里		

另一台加密机也需要进行类似的配置。

开启双机热备功能后,先启动的加密机会将自己的IP设置为双机热备服务设备的IP; 后启动的加密机则将自己的IP设置为从机IP 即 从服务设备的IP。如图63所示。

田	户	手	.₩
11	/	1	11/1

投备信息菜单	当前位置: 双机热备配置>>热备设置
密钥信息菜单	热省设置
密钥管理菜单	网口端口: eth0 V
国标密钥信息	双机热备功能状态: 关 关
国标密钥管理	双机热备功能设置: ④启动双机热备 〇关闭双机热备
密钥备份管理	网络类型: ◎IPv4 ○IPv6 (仅输入ip默认摘码为24,若要配置掩码,可输入形如"192.168.18.239/27")
服务配罟菜单	输入服务IP: 192.168.18.94
KeyStore管理	输入另一台设备IP: 192.168.18.161
日志管理菜单	虚拟路由ID(1-255): 61
双机热备功能       热备设置       数据同步       数据同步       设备管理菜单	双机热奋鶥活

注意:1)、虚拟路由ID,如果加密机A和B共同完成双机热备,那么两台加密机配置的虚拟路由ID应该一致,如果同一网络中,有多个主备组,那么他们的虚拟路由ID不能 重复

2) 、服务设备IP 要是一个非加密机A 和加密机B的局域网内没有使用的第三 方IP

(二)、关闭双机热备功能:

华翼微电子

首先,点击选中 "关闭双机 热备"来关闭双机热备功能;然后点击 "双击热备 配置" 按钮 ,来保存配置信息。重启加密机服务器后,双机热备的设置才能生效。

关闭双击设备功能后,加密机服务器会配置为自己原本的IP。

#### 3.8.2 服务器密码机数据同步

单击左侧菜单栏"双机热备"按钮,并单击"数据同步"按钮,如图64。

用户手册

设备信息菜单	当前位置: 双机热备功能>>数据同步
密钥信息菜单	数据同步
密钥管理菜单	数据同步
国标密钥信息	
国标密钥管理	
密钥备份管理	
权限管理菜单	
服务配置菜单	
KeyStore管理	
日志管理菜单	
设备监控菜单	
双机热备功能	
▲ 热备设置	
▲ 数据同步	
设备管理菜单	

图 64

3.9 服务器密码机初始化

华翼微电子

在设备出厂后,用户进行操作之前,需要进行设备初始化操作。连接后输入用户名 密码:默认用户名: admin,密码: admin,首先将服务器密码机ETH0网口接入网络,服 务器密码机默认连接IP地址是<u>https://192.168.18.239</u>。连接后输入用户名密码,如图 65:

![](_page_56_Picture_1.jpeg)

![](_page_56_Picture_2.jpeg)

输入用户名、密码后,点击登陆,进入管理界面如图66:

![](_page_57_Picture_0.jpeg)

![](_page_57_Figure_2.jpeg)

首先鼠标单击左侧菜单栏"设备管理",再单击"设备初始化"按钮,进入初始化 操作界面。如图67所示。

![](_page_58_Picture_1.jpeg)

华翼微电子

图 67

鼠标单击中间按钮"开启初始化功能",弹框提示"确定开启初始化功能",选择 确定之后,开启初始化成功后提示。然后,鼠标单击"初始化设备"按钮,如图68、 69所示。

![](_page_59_Picture_1.jpeg)

设备信息菜单	当前位置:设备管理>>设备初始化
密钥信息菜单	设备初始化
密钥管理菜单	开启初始化功能 初始化设备 关词初始化功能
国标密钥信息	注:初始化操作不会删除设备内密钥,只清除用户、审计日志、白名单、私钥权限码、定制KeyStore证书、非默认路由信息。
国标密钥管理	
密钥备份管理	
权限管理菜单	
服务配置菜单	
KeyStore管理	
日志管理菜单	
设备监控菜单	
双机热备功能	
设备管理菜单	
📑 设备初始化	
设备重启	

图 68

![](_page_59_Picture_4.jpeg)

点击确定后,页面回退到登录界面,需要重新输入账号: admin,口令: admin,重新登录进入加密机管理页面。注:初始化操作不会删除设备内密钥,只清除管理员、审计日志、白名单、定制KeyStore证书。

到此,初始化操作已经完成,需要重新启动加密机来达到初始化目的。单击左侧菜 单栏"设备重启"栏,选择"服务器重启"页面,如图70。

![](_page_60_Picture_0.jpeg)

![](_page_60_Picture_1.jpeg)

华翼微电子

图 70

等待机器重启完毕,可再次登陆web配置界面进行其他配置。登陆页面会变成如图71。

![](_page_61_Picture_1.jpeg)

![](_page_61_Picture_2.jpeg)

用户名变为已添加管理员的序列号,将任意管理员插入配置终端的usb接口中,并 在用户名处选择插入key的对应序列号,密码处输入对应的密码,默认是"12345678", 点击登陆后可以进入配置页面。否则不插入管理员无法进入配置页面。

![](_page_62_Picture_1.jpeg)

## 4 产品常见错误分析及解决方法

#### 4.1 服务器密码机配置管理连接不上

首先确认服务器密码机的ip地址输入正确。可通过ping命令来确定网络是否连接正常,有如下原因可导致网络连接不上:

- ◇ 客户端ip地址和服务器密码机连接网口对应的ip地址不在同一网段内。
- ◇ 服务器密码机配置了多个在同一网段的ip地址(服务器密码机的每个网口必须 设置不同ip网段)。
- ◇ 设置了新的ip地址后,没有重新启动服务器密码机,而导致ip没有修改。
- 4.2 服务器密码机服务连接不上

当服务器密码机配置管理可以连接, 而服务无法连接时, 可能有如下原因:

- ◇ 客户端配置文件没有放到系统目录下。
- ◇ 客户端配置文件中ip没有设置成连接服务器密码机的ip地址。
- ◆ 客户端配置文件的最后一行不是空行。
- ◆ 服务端口号8012被屏蔽。

#### 4.3 服务器密码机服务报错

在进行密钥生成、删除,备份、恢复操作时,需要管理员权限,否则报错。

![](_page_63_Picture_0.jpeg)