
SJJ1012 服务器密码机

用户技术手册

北京三未信安科技发展有限公司

V2.1

欢迎使用三未信安服务器密码机

Copyright (c) 2010 sansec

版权所有

本出版物的内容将做不定期性的变动，且不会另行通知。更改的内容将不会补充到本出版物。且会在本手册发行新版本时予以付梓印刷。本公司不做任何明示或默许担保，其中包括本手册的内容的适售性或符合特定使用目的的默许担保。

本公司依中华人民共和国著作权法，享有及保留一切著作之专属权力，未经北京三未信安科技发展有限公司事先书面同意，不得对本手册有增删、改编、翻印、改造或仿制的行为。

北京三未信安科技发展有限公司

2011 年 7 月

目 录

1	产品介绍.....	1
1.1	产品简介	1
1.2	产品功能	1
1.3	产品特点及关键技术.....	2
2	基本概念.....	3
3	快速使用指南.....	4
4	安装密码机.....	5
4.1	安装密码机	5
4.2	管理密码机	5
4.3	安装向导	6
5	系统管理.....	10
5.1	查看设备基本信息.....	10
5.2	查看/修改设备维护信息	10
5.3	查看设备运行信息.....	10
5.4	查看/修改网络配置.....	11
6	权限管理.....	12
6.1	查看登录状态	12
6.2	用户登录	12
6.3	用户注销	12
6.4	管理员管理	12
6.4.1	增加管理员.....	12
6.4.2	删除管理员.....	13
6.5	操作员管理	14
6.5.1	增加操作员	14
6.5.2	重置操作员口令	14
6.6	修改 IC 卡口令	14
6.7	查看权限设置表.....	15
7	密钥管理.....	16
7.1	RSA 密钥管理.....	16
7.1.1	产生密钥对	16
7.1.2	删除密钥对	16
7.1.3	设置私钥访问控制码	16
7.2	ECC(SM2) 密钥管理.....	17
7.2.1	产生 ECC 密钥对	17
7.2.2	删除 ECC 密钥对	17
7.2.3	设置私钥访问控制码	17
7.3	对称密钥管理.....	18
7.3.1	产生对称密钥.....	18
7.3.2	删除对称密钥.....	18
7.4	销毁密钥	19
8	服务管理.....	20

8.1	查看服务状态	20
8.2	修改服务配置	20
8.3	白名单管理	20
8.4	启动/停止服务	21
9	备份和恢复	22
9.1	备份密钥向导	22
9.2	恢复密钥向导	23
附录 A	常见问题	25
附录 B	主要技术指标	26
附录 C	权限设置表	28
附录 D	安全须知	29
附录 E	技术支持	30

1 产品介绍

1.1 产品简介

SJJ1012 服务器密码机（以下简称密码机）是由北京三未信安科技发展有限公司自主研发的高性能密码设备，能够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签名/验证、加密/解密的要求，保证传输信息的机密性、完整性和有效性，同时提供安全、完善的密钥管理机制。

密码应用系统通过调用密码机提供的标准 API 函数来使用密码机的服务，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《公钥密码基础设施应用技术体系 密码设备应用接口规范（试行）》标准接口规范，通用性好，能够平滑接入各种系统平台，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。

1.2 产品功能

- **RSA 密钥生成与管理：**可以生成 1024/2048/3072/4096¹位 RSA 密钥对，采用由国家密码管理局批准使用的物理噪声源产生器芯片生成的随机数。
- **ECC 密钥生成与管理：**可以生成 256 位 ECC 密钥对。
- **密钥的安全存储：**设备内可存储 RSA/ECC 密钥对（包括签名密钥对和加密密钥对），并且私钥部分受系统保护密钥的加密保护。
- **数据加密和解密：**支持 SM1、SM4 和 SSF33 等国产算法²的 ECB 和 CBC 模式的数据加密和解密运算，同时也支持 3DES、AES 等国际通用算法。
- **消息鉴别码的产生和验证：**支持基于 SM1、SM4、SSF33、3DES、AES 等算法³的 MAC 产生及验证。
- **数据摘要的产生和验证：**支持 SM3、SHA-1、SHA224、SHA256、SHA384、SHA512 等杂凑算法。
- **数字签名的产生和验证：**可以根据需要利用内部存储的 RSA/ECC 密钥对或外部导入 RSA/ECC 私钥对请求数据进行数字签名。
- **数字信封功能：**支持基于 RSA/ECC 密码算法的数字信封功能，并支持由内部

¹ 不同型号的密码机配置不同，支持的 RSA 算法最大密钥长度可能不同。

² 不同型号的密码机配置不同，支持的国产算法种类可能不同。

³ 同上。

密钥保护到外部密钥保护的数字信封转换功能。

- **物理随机数的产生：**采用由国家密码管理局批准使用的物理噪声源产生器芯片生成的真随机数。
- **用户访问权限控制：**具有用户管理功能，提高了密码设备自身的安全性。
- **密钥备份及恢复：**支持基于秘密共享技术的密钥的备份和恢复功能，保证了安全应用系统的安全性和可靠性。

1.3 产品特点及关键技术

- **支持多种操作系统：**应用服务器与密码机之间采用 TCP/IP 协议进行通信，可支持多种主流的操作系统，如 MS Windows 系列，Linux 系列，Solaris、AIX、HP-UX 等 Unix 操作系统。
- **支持标准接口：**密码机 API 接口符合《公钥密码基础设施应用技术体系 密码设备应用接口规范（试行）》标准接口规范，通用性好。同时支持 PKCS#11、MS-CSP、JCE 等国际标准接口。
- **三层密钥结构：**采用“系统保护密钥-用户密钥（卡内 RSA/ECC 密钥对/KEK）-会话密钥”的三层密钥保护结构，保证用户密钥及应用系统的安全性。
- **安全密钥存储：**保证关键密钥在任何时候不以明文形式出现在设备外，密钥备份文件也受到专用备份密钥的保护。
- **支持连接密码及白名单：**通过连接密码和白名单的支持，实现了密码机对应用服务器的授权认证，进一步提高了系统的安全性。
- **密钥使用授权：**每对 RSA/ECC 密钥对对应一个授权保护码，以保证不同密码应用系统调用同一台密码设备时的密钥安全性。

2 基本概念⁴

- **设备编号**：设备标签上的产品序号，是由生产日期、生产批次、流水号组成的一串数字编号，与设备型号组合使用可唯一标识某一密码设备。
- **设备型号**：国家密码管理机构批准使用的密码产品型号。
- **数字信封**：一种数据的封装方式，在该方式下使用数据加密密钥保护数据，使用接收者加密公钥保护数据加密密钥。
- **数字签名**：附加在数据上的签名数据，或是对数据所作的密码变换，用以确认数据来源及其完整性，防止被他人伪造或者签发者否认。
- **密钥部件（密钥分量）**：至少两个随机或伪随机产生的、有密码密钥特点（例如，格式，随机性）的参数之一，其中密码密钥由一个或多个这样的参数组合而成。例如，通过模 2 加的方法形成一个密码密钥。
- **密钥分割**：将密钥分给多人掌管，并且必须有一定人数的掌管密钥的人同时到场才能恢复密钥。
- **密钥加密密钥（KEK）**：用于对会话密钥或文件密钥进行加密时采用的密钥。又称辅助（二级）密钥(Secondary Key)或密钥传送密钥(key Transport key)。通信网中的每个节点都分配有一个这类密钥。
- **密钥索引**：在密码设备或安全系统内表示密钥位置的数值。
- **签名私钥**：用于签名计算的私有密钥。
- **加密私钥**：用于实现数据保密性的私有密钥。
- **私钥访问控制码**：用于获取私钥使用权限的口令字。
- **对称密钥/秘密密钥**：在采用对称密码技术时，一组特定实体使用的密钥。
- **会话密钥**：密钥管理中的最低一层密钥，这种密钥只在一次会话和一个受限时间内使用，比如终端上的一次用户会话，完毕就销毁。

⁴ 来自《中华人民共和国国家标准 密码相关术语》

3 快速使用指南

a) 安装密码机

详细参考“4 安装密码机”的“安装密码机”部分。

b) 运行管理工具

详细参考“4 安装密码机”的“管理密码机”部分。

c) 安装向导

详细参考“4 安装密码机”的“安装向导”部分。

d) 管理员及操作员

详细参考“6 权限管理”的“管理员管理”、“操作员管理”部分。

e) 修改 IC 卡口令

详细参考“6 权限管理”的“修改 IC 卡口令”部分。

f) RSA 密钥管理

详细参考“7 密钥管理”的“RSA 密钥管理”部分。

g) ECC 密钥管理

详细参考“7 密钥管理”的“ECC 密钥管理”部分。

h) 对称密钥管理

详细参考“7 密钥管理”的“对称密钥管理”部分。

i) 网络配置

详细参考“5 系统管理”的“查看/修改网络配置”部分。

j) 启动/停止服务

详细参考“8 服务管理”的“启动/停止服务”部分。

k) 服务参数配置

详细参考“8 服务管理”的“修改服务配置”部分。

l) 备份与恢复

详细参考“7 密钥管理”的“备份和恢复”部分。

m) 销毁密钥

详细参考“7 密钥管理”的“销毁密钥”部分。

4 安装密码机

4.1 安装密码机

- a) 打开密码机包装，对照“装机清单”，检查设备配件是否齐全。
- b) 从包装箱中取出密码机主机，并将设备固定到安装位置⁵。
- c) 使用电源线连接电源。
- d) 打开密码机电源开关，启动密码机。

4.2 管理密码机

- a) 准备一台 PC 机作为管理终端，使用网线连接到密码机的“网口 2”或“网口”⁶
- b) 修改管理终端的 IP 地址，与密码机 IP 地址为同一个网段。密码机默认地址为：

IP 地址：192.168.10.12

子网掩码：255.255.255.0

<i>提示：为防止密码机预设 IP 地址与现有网络中的 IP 地址冲突，请先采用管理终端和密码机直连⁷的方式修改 IP 地址后再接入工作或测试网络。

- c) 打开 IE 或其他网页浏览器，输入密码机 IP 地址，如：<http://192.168.10.12>。



⁵ 安装到机架所需要的螺丝、导轨等配件不是标准配置

⁶ 部分型号只配备一个网口

⁷ 千兆网卡具有自适应功能，不需要专用的网线

<!=重要提示：由于是基于网络的管理方式，多台管理终端可同时连接密码机，但如果同时对密码机进行管理操作的话可能会导致不可预知的错误。

<!=重要提示：如果遇到不能访问的情况，或者忘记 IP 地址，请在用户光盘中找到《紧急维护手册》。

d) 打开登录界面后，使用用户名“swdsm”登录，默认登录密码是“swxa1234”，登录后即可进行管理配置。详细配置步骤可参考后续章节。



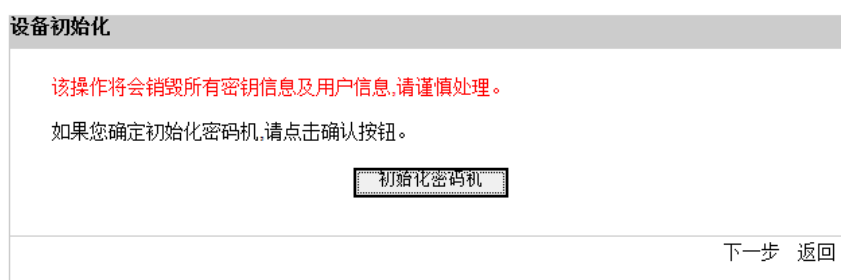
4.3 安装向导

在第一次使用密码机，可以使用管理程序的安装向导功能，逐步完成对加密机的基本配置。如果需要使用其他配置功能，可参考本章节其他管理操作说明。

安装向导提供以下主要配置功能：

a) **初始化密码机：**清空所有密钥及管理信息。

安装向导： [设备初始化](#) > 管理员 > 操作员 > 密钥管理 > 网络配置 > 服务配置 > 备份密钥 > 重启密码机



b) **增加管理员：**为保证设备的安全性、可靠性，及正常使用所有功能，建议设

置 3 个管理员（标准配置）。

安装向导：设备初始化 > [管理员](#) > 操作员 > 密钥管理 > 网络配置 > 服务配置 > 备份密钥 > 重启密码机

增加管理员

请将标记为“管理员”的IC卡按照正确的方向插入设备中，并输入IC卡保护口令。

PIN口令:

上一步 下一步

c) **增加操作员：**用于启动密码服务，增加 1 个操作员（标准配置）。

安装向导：设备初始化 > 管理员 > [操作员](#) > 密钥管理 > 网络配置 > 服务配置 > 备份密钥 > 重启密码机

增加操作员

请将标记为“操作员”的IC卡按照正确的方向插入设备中，并输入IC卡保护口令。

PIN口令:

上一步 下一步

d) **RSA 密钥管理：**产生安全应用系统需要的 RSA 签名密钥对或加密密钥对并保存在密码设备内部。

安装向导：设备初始化 > 管理员 > 操作员 > [密钥管理](#) > 网络配置 > 服务配置 > 备份密钥 > 重启密码机

产生内部RSA密钥对

根据索引指定位置，生成新的RSA密钥对。

密钥索引和或密钥索引范围(1~50)(用逗号分隔),例如:1,3,5-12	1-5
密钥用途	签名密钥对和加密密钥对 ▼
模长	1024 ▼

上一步 下一步

e) **ECC 密钥管理：**产生安全应用系统需要的 ECC 签名密钥对或加密密钥对并保存在密码设备内部。

安装向导: 设备初始化 > 管理员 > 操作员 > **密钥管理** > 网络配置 > 服务配置 > 备份密钥 > 重启密码机

产生内部ECC密钥对

根据索引指定位置，生成新的ECC(SM2)密钥对。

请输入密钥索引和/或密钥索引范围(1~50)(用逗号分隔)，例如：1,3,5-12

1,2,3,4,5

密钥用途

签名和加密

模长(bits)

256

产生密钥对

上一步

下一步

f) **网络配置**：查看或修改设备的网络配置参数。

安装向导: 设备初始化 > 管理员 > 操作员 > 密钥管理 > **网络配置** > 服务配置 > 备份密钥 > 重启密码机

网络配置信息

修改密码机网络地址。

注：修改后不能立即生效，需要重新启动密码机才能启用新的地址。

IP地址

192.168.10.12

子网掩码

255.255.255.0

默认网关

0.0.0.0

刷新

修改

上一步

下一步

g) **配置服务信息**：修改服务启动参数。

安装向导: 设备初始化 > 管理员 > 操作员 > 密钥管理 > 网络配置 > **服务配置** > 备份密钥 > 重启密码机

服务配置

修改服务配置信息。

注：修改后不能立即生效，需要重新启动密码机。

服务端口(默认值:8008)

8008

开机自动启动

自动启动

会话超时时间(分钟)(0~65535)

30

最大并发数(0~65535)

1024

服务连接密码

●●●●●●●●

服务启动口令(操作员卡口令)

●●●●●●●●

刷新

保存

上一步

下一步

h) **对客户机授权**：修改服务授权白名单，进行访问控制。

安装向导: 设备初始化 > 管理员 > 操作员 > 密钥管理 > 网络配置 > **服务配置** > 备份密钥 > 重启密码机

白名单管理

对客户端机器进行授权，只有在白名单中的IP地址才被允许访问密码服务。
注：当白名单为空时，允许所有IP访问。

添加到白名单

输入要授权的IP地址：

白名单状态

192.168.10.13	删除
192.168.10.15	删除

上一步

下一步

i) **备份密钥信息：**将密钥等重要信息加密后备份到文件中并妥善保管。

安装向导: 设备初始化 > 管理员 > 操作员 > 密钥管理 > 网络配置 > 服务配置 > **备份密钥** > 重启密码机

备份密钥

将启动密钥备份向导将密码机内的密钥备份到文件中，可用于部署多台密码机并行，或以后密码机出现故障时及时恢复系统。
注：本过程将会用到刚才初始化好的3张管理员卡。

[查看登录状态](#)

上一步

下一步

j) **重新启动密码机：**为确保所有设置已经生效，建议重新启动密码机。

<i>提示：安装向导中对网络配置和服务配置所作的修改需要重启密码机才能生效。

<i>提示：重新启动密码机时请将操作员卡插入设备中。

5 系统管理

5.1 查看设备基本信息

可查看厂商信息、设备编号、系统版本、支持算法等信息。

系统管理: [设备基本信息](#) > 设备维护信息 > 设备运行信息 > 网络配置信息

设备基本信息	
生产厂商	SANSEC
设备型号	SJJ0930
产品号	SH2U11-SC5S
设备序列号	2010101413301052
设备版本	v1.2.2

<i>提示：使用密码机过程中遇到问题需要技术支持时，提供以上信息将会帮助我们更快解决问题。

5.2 查看/修改设备维护信息

可以查看和修改设备维护方面的相关信息。

5.3 查看设备运行信息

可以查看设备当前运行情况，如密码服务是否正在运行，当前并发数和密码机的内存使用情况。

系统管理: 设备基本信息 > 设备维护信息 > [设备运行信息](#) > 网络配置信息

设备运行信息	
加密服务	未启动
当前并发数	0
内存占用率	47.51
刷新	

<!>重要提示：当前并发数持续增长，或者明显高于预计值，有可能是因为应用开发接口调用方式错误。

<!>重要提示：当内存占用率超过 80%，建议将密码机升级到更高性能的型号。

5.4 查看/修改网络配置

查看或修改设备的网络配置参数，如 IP 地址、网关等。

系统管理：设备基本信息 > 设备维护信息 > 设备运行信息 > [网络配置信息](#)

网络配置信息

IP地址	192.168.10.12
子网掩码	255.255.255.0
默认网关	0.0.0.0

<i>提示：当修改了 IP 地址时，需要关闭当前管理窗口，重新连接到新的地址。

<i>提示：部分型号配备了双网口，“网口 1”用于密码服务，“网口 2”用于设备管理。

6 权限管理

6.1 查看登录状态

选择“权限管理”或“用户登录”页面，即可查看当前管理员或操作的登录状态。

权限管理: [用户登录](#) > 用户管理 > 修改IC卡口令 > 查看权限表

用户登录
在此登录管理员或操作员
请输入IC卡PIN口令:

用户状态

当前权限状态	管理员权限	
管理员数目	3	
已登录管理员	2号:	注销全部管理员
操作员登录状态	未添加	注销全部操作员

6.2 用户登录

登录管理员或登录操作员。

在登录时请根据卡片标示的方向插入管理员口令卡并输入 IC 卡保护口令(PIN)。

<!>安全提示: 在出厂时所有用户卡的保护口令均被初始化为“12345678”，为保证系统的安全性，请及时通过“修改用户口令”功能修改该口令。

6.3 用户注销

在“用户登录”页面中有用户注销的选项，可以通过执行该功能释放管理员权限或操作员权限。

<!>安全提示: 在完成管理操作时，建议及时注销管理员，仅保留操作员登录状态即可正常使用密码机的密码服务及状态监控功能。

6.4 管理员管理

6.4.1 增加管理员

a) 选择“管理员管理”中的“增加管理员”功能。

权限管理: 用户登录 > [用户管理](#) > 修改IC卡口令 > 查看权限表

管理员管理		
序号	状态	操作
1号管理员	有效	删除
2号管理员	有效	删除
3号管理员	有效	删除
4号管理员	-	添加
5号管理员	-	添加

- b) 根据卡片标示的方向插入管理员口令卡。
- c) 输入 IC 卡保护口令（PIN），才能获得对 IC 卡的访问权限。

权限管理: 用户登录 > [用户管理](#) > 修改IC卡口令 > 查看权限表

添加管理员	
请将标记为“管理员”的IC卡安装正确的方向插入设备，并输入IC卡保护口令。	
PIN口令:	添加管理员
返回	

- d) 输入正确的口令后，即可完成新增管理员功能。

<!>安全提示: 该密码设备在设计时支持 1 到 5 个管理员，为保证密码设备的安全性及可靠性，建议设置 3 个管理员。

<!>安全提示: 在出厂时所有用户卡的保护口令均被初始化为“12345678”，为保证系统的安全性，请及时通过“修改用户口令”功能修改该口令。

6.4.2 删除管理员

在“用户管理”页面，点击“删除”，即可完成管理员删除。

权限管理: 用户登录 > [用户管理](#) > 修改IC卡口令 > 查看权限表

管理员管理		
序号	状态	操作
1号管理员	有效	删除
2号管理员	有效	删除
3号管理员	有效	删除
4号管理员	-	添加
5号管理员	-	添加

<!>安全提示: 当某张管理员卡丢失或认为其安全性存在隐患时，可通过“删除管理员”及“增加管理员”功能更新管理员。

6.5 操作员管理

6.5.1 增加操作员

根据卡片标识的方向插入操作员口令卡，并输入 IC 卡保护口令（PIN），即可完成新增操作员功能。

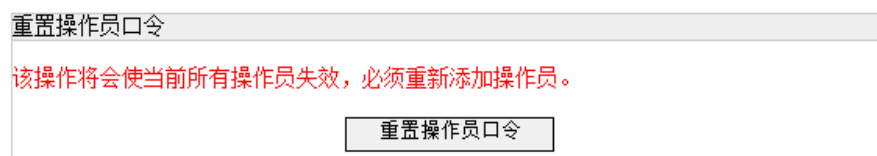


<!>安全提示：为保证设备的可扩展性，本设备支持 1 个以上的操作员，但标准配置为 1 个操作员。

<!>安全提示：在出厂时所有用户卡的保护口令均被初始化为“12345678”，为保证系统的安全性，请及时通过“修改 IC 卡口令”功能修改该口令。

6.5.2 重置操作员口令

重新设置设备内的操作员状态及登录密钥，执行该操作后目前已存在的操作员将全部失效，必须重新增加操作员。



<!>安全提示：操作员不提供类似于管理员管理时单独删除某个管理员的功能，如果出现操作员卡丢失的情况，为保证安全性，在增加新的操作员前必须重新初始化操作员口令。

6.6 修改 IC 卡口令

根据卡片标示的方向插入管理员口令卡并输入 IC 卡原保护口令和新口令，点击“修改口令”即可完成修改。

权限管理: 用户登录 > 用户管理 > [修改IC卡口令](#) > 查看权限表

修改IC卡口令

根据卡片标识的方向插入IC口令卡。

请输入原口令	
请输入8位新口令	
请再次输入新口令	

修改口令

<!\>安全提示：在出厂时所有用户卡的保护口令均被初始化为“12345678”，为保证系统的安全性，请及时通过“修改用户口令”功能修改该口令。

6.7 查看权限设置表

为方便使用，可以查看各项管理操作所需要的权限对应表。详细的权限表参考“附录 B 权限设置表”部分。

7 密钥管理

7.1 RSA 密钥管理

7.1.1 产生密钥对

本设备支持双密钥体制，每个索引位置对应两对 RSA 密钥对，分别是签名密钥对和加密密钥对，签名密钥对主要用于数字签名，加密密钥对一般用于数字信封或保护会话密钥的安全。

密钥管理: [RSA密钥管理](#) > [ECC密钥管理](#) > [对称密钥管理](#) > [销毁密钥](#)

内部RSA密钥对管理

生成RSA密钥对

密钥索引和/或密钥索引范围(1~50)(用逗号分隔),例如:1,3,5-12

密钥用途

RSA密钥的模长(bits)

生成密钥对

<i>提示：批量产生密钥对的时候，需要先删除所选范围内已经存在的密钥对。

<i>提示：不同型号的密码机可能支持的 RSA 算法最大模长不同，即有些型号密码机不支持 3072 和 4096 位密钥。

7.1.2 删除密钥对

点击“删除”即可删除指定密钥索引位置的 RSA 密钥对。

RSA密钥状态				
密钥索引	密钥用途	模长	删除密钥	修改私钥访问控制码
1	签名密钥	1024	删除	修改访问码
	加密密钥	1024	删除	
2	签名密钥	1024	删除	修改访问码
	加密密钥			
4	签名密钥	1024	删除	修改访问码
	加密密钥			

7.1.3 设置私钥访问控制码

密码设备应用接口在调用指定的 RSA 私钥时，必须先获取相应的私钥访问权限。每个密钥索引对应一个私钥访问控制码，即同一索引位置的签名私钥和加密私钥只需要设置一次私钥访问控制码即可。

RSA密钥状态				
密钥索引	密钥用途	模长	删除密钥	修改私钥访问控制码
1	签名密钥	1024	删除	修改访问码
	加密密钥	1024	删除	

密钥管理: [RSA密钥管理](#) > [ECC密钥管理](#) > [对称密钥管理](#) > [销毁密钥](#)

设置私钥访问控制码

设置应用系统用于获取私钥使用权限的口令字。

访问控制码(8个字符)

.....

重复访问控制码

.....

确定

返回

7.2 ECC(SM2) 密钥管理

7.2.1 产生 ECC 密钥对

与 RSA 密钥结构一样, 本设备支持双密钥体制, 每个索引位置对应两对 ECC(SM2) 密钥对, 分别是签名密钥对和加密密钥对, 签名密钥对主要用于数字签名, 加密密钥对一般用于数字信封或保护会话密钥的安全。

密钥管理: [RSA密钥管理](#) > [ECC密钥管理](#) > [对称密钥管理](#) > [销毁密钥](#)

内部ECC密钥对管理

生成ECC密钥对

请输入密钥索引和/或密钥索引范围(1~50)(用逗号分隔), 例如: 1,3,5-12

1,3,5-8

密钥用途

签名密钥

ECC密钥的模长(bits)

256

生成密钥对

<i>提示: 批量产生密钥对的时候, 需要先删除所选范围内已经存在的密钥对。

7.2.2 删除 ECC 密钥对

点击“删除”即可删除指定密钥索引位置的 ECC(SM2)密钥对。

ECC密钥状态				
密钥索引	密钥用途	模长	删除密钥	修改私钥访问控制码
1	签名密钥	256	删除	修改访问码
	加密密钥	256	删除	
3	签名密钥	256	删除	修改访问码
	加密密钥			
4	签名密钥	256	删除	修改访问码
	加密密钥			

7.2.3 设置私钥访问控制码

密码设备应用接口在调用指定的 ECC 私钥时, 必须先获取相应的私钥访问权限。每个密钥索引对应一个私钥访问控制码, 即同一索引位置的签名私钥和加密私钥只需要设置一次私钥访问控制码即可。

ECC密钥状态				
密钥索引	密钥用途	模长	删除密钥	修改私钥访问控制码
1	签名密钥	256	删除	修改访问码
	加解密密钥	256	删除	

密钥管理: [RSA密钥管理](#) > [ECC密钥管理](#) > [对称密钥管理](#) > [销毁密钥](#)

设置私钥访问控制码

设置应用系统用于获取私钥使用权限的口令字。

访问控制码(8个字符)

.....

重复访问控制码

.....

确定

返回

7.3 对称密钥管理

7.3.1 产生对称密钥

该密钥是一种对称密钥，既可作为密钥加密密钥（KEK）用于保护会话密钥的安全，也可直接用于数据加密，通过系统分割密钥的方法保证了两种应用的独立性，不会影响到数据或密钥的安全性。具体步骤如下：

密钥管理: [RSA密钥管理](#) > [ECC密钥管理](#) > [对称密钥管理](#) > [销毁密钥](#)

对称密钥管理

产生对称密钥

请输入密钥索引和/或密钥索引范围(1~200)(用逗号分隔)，例如：1,3,5-12

密钥长度(bits)

128

产生密钥

<i>提示：批量产生密钥的时候，需要先删除所选范围内已经存在的密钥。

7.3.2 删除对称密钥

根据提示，输入密钥索引，删除指定密钥索引位置的对称密钥。

删除对称密钥

密钥索引（1~200）

删除密钥

请输入密钥索引和/或密钥索引范围（用逗号分隔），例如：1,3,5-12

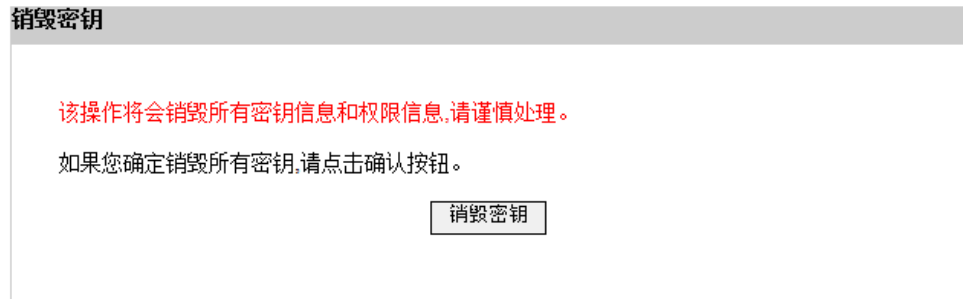
对称密钥状态

	1	2	3	4	5	6	7	8	9	10
0	128	0	128	0	128	256	256	256	256	0
10	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0

7.4 销毁密钥

该操作会销毁密码设备内的所有密钥及用户信息。

密钥管理: [RSA密钥管理](#) > [ECC密钥管理](#) > [对称密钥管理](#) > [销毁密钥](#)



<!--安全提示: 该功能不仅用于复位密码设备的初始状态,还可用于销毁设备内的所有密钥及用户文件。

8 服务管理

8.1 查看服务状态

用户可以查看服务的当前运行情况，包括负载和并发数等。

服务管理： [服务状态](#) > 服务配置 > 白名单管理 > 启动/停止服务

服务状态

服务运行状态	服务已启动
负载情况	0.0
当前并发数	0

刷新

8.2 修改服务配置

查看或修改服务的启动参数。

服务管理： 服务状态 > [服务配置](#) > 白名单管理 > 启动/停止服务

服务状态

注：修改后不能立即生效，需要重新启动服务或重启密码机。

服务端口(默认值：8008)	8008
开机自动启动	不启动
会话超时时间(分钟)(0~65535)	30
最大并发数(0~65535)	2048
服务连接密码	••••••••
服务启动口令(操作员卡口令)	••••••••

保存 刷新

<i>提示：如果服务已经启动，需要重新启动服务或重启密码机才能生效。

8.3 白名单管理

为保证密码设备的安全性，本设备支持白名单功能，用于控制客户机的访问权限。

服务管理: 服务状态 > 服务配置 > 白名单管理 > 启动/停止服务

白名单管理

对客户端机器进行授权，只有在白名单中的IP地址才被允许访问密码服务。
注：当白名单为空时，允许所有IP访问。
修改后不能立即生效，需要重新启动服务或重启密码机。

添加到白名单

输入要授权的IP地址:

添加

已成功添加到白名单列表中。

白名单列表

192.168.1.100	删除
192.168.1.101	删除

<！>安全提示：当白名单为空时，该功能自动失效，但为了保证应用系统的安全性，不建议采用该设置。

<i>提示：如果服务已经启动，则修改完成后必须重新启动服务才能生效。

<i>提示：IP 地址不支持通配符和网段，必须为独立 IP。

8.4 启动/停止服务

如果还未启动服务，可以选择“启动服务”。

服务管理: 服务状态 > 服务配置 > 白名单管理 > 启动/停止服务

启动服务

密码服务已停止!

请将操作员卡安装正确的方向插入设备，然后点击[启动密码服务]按钮启动服务。

启动密码服务

如果服务已启动，可以按选择进行以下操作：

- 立即停止服务：**立即终止当前服务的所有进程。
- 重新启动服务：**立即结束当前所有服务，并重新启动新的服务进程。

服务管理: 服务状态 > 服务配置 > 白名单管理 > 启动/停止服务

停止服务

当前服务运行正常，请选择要进行的操作。

立即停止服务	强制停止所有服务
重新启动服务	强制停止服务，然后重新启动

21

9 备份和恢复

9.1 备份密钥向导

运行备份向导，产生备份密钥并分割导出，然后对 RSA 私钥、ECC 私钥、对称密钥的敏感信息通过该密钥加密保存到文件中，再将备份文件从密码机下载到本地并妥善保管。具体步骤如下：

- a) 登录半数以上的管理员，获得超级管理员权限。准备好用于保存备份密钥分量的 3 张管理员卡。

备份密钥: [准备开始](#) > [导出密钥分量](#) > 生成备份文件 > 导出备份文件

密钥备份向导

1、准备备份。

请登录管理员半数以上管理员,以满足备份所需管理员权限。
并准备好3张管理员口令卡。

[查看登录状态](#)

- b) 依次输出 3 个备份密钥分量，该过程需要插入用户卡并输入 PIN 口令。

备份密钥: 准备开始 > [导出密钥分量](#) > 生成备份文件 > 导出备份文件

密钥备份向导

2、输出备份密钥分量[1]。

请选择一张管理员卡根据正确的方向插入设备中，并输入保护口令。

请输入PIN口令:

- c) 完成密钥分量导出后，密码机会自动将密钥等数据使用备份密钥进行加密，并备份到文件中。
- d) 点击“下载文件”连接，即可将备份文件下载到本地，不建议自行修改备份文件的名称。

备份密钥: 准备开始 > 导出密钥分量 > 生成备份文件 > [导出备份文件](#)

密钥备份向导

6、导出备份文件。

密码机内的密钥信息已经备份到密钥备份文件中，点击下面链接，下载到本地并妥善保管。

[下载密钥备份文件\[swhsmbak.dat\]](#)

[下一步](#)

e) 完成该备份功能后将自动删除再密码机端的临时备份文件。

<!>安全提示：密钥备份文件和管理员口令卡一定要妥善保管。

<i>提示：备份文件导出保存是不建议修改文件名，必须保证恢复上传时保持现在的文件名称，否则可能不能正常恢复。

9.2 恢复密钥向导

运行恢复向导，将保存在管理员卡中的备份密钥分量合成，将备份文件中保存的密钥信息通过该密钥解密。具体步骤如下：

a) 执行密钥恢复功能，打开密钥恢复向导。

恢复密钥: [准备恢复](#) > 上传备份文件 > 导入密钥分量 > 完成

密钥恢复向导

1、准备恢复密钥。

请登录管理员半数以上管理员，已满足备份所需管理员权限。
并准备好3张备份时所用的管理员卡。

[查看登录状态](#)

[开始恢复](#)

b) 将备份文件上传到密码机，并确认文件名为“swhsmbak.dat”。

恢复密钥: 准备恢复 > [上传备份文件](#) > 导入密钥分量 > 完成

密钥恢复向导

2、上传备份文件。

请选择之前密钥备份过程中生成的密钥备份文件，并点击[上传]按钮。

[浏览...](#) [上传](#)

如果您已经上传了备份文件，选择[<下一步>](#)

c) 找到当时备份密钥时使用的管理员口令卡，选择任意 2 张管理员卡，分别导入备份密钥分量，该过程需要插入管理员卡并输入 PIN 口令。

恢复密钥: 准备恢复 > 上传备份文件 > [导入密钥分量](#) > 完成

密钥恢复向导

3、导入备份密钥分量[1]。

请选择任意一张管理员卡按照正确的方向插入设备中，并输入保护密码。

请输入PIN口令:

如果还未上传密钥备份文件，请点击[<上一步>](#)返回上传。

d) 密钥恢复向导将依次恢复备份文件中保存的信息。

恢复密钥: 准备恢复 > 上传备份文件 > [导入密钥分量](#) > [完成](#)

密钥恢复向导

5、完成密钥恢复。

恭喜你，已经成功将密钥恢复到密码机。
上传到密码机的密钥备份文件已删除。

返回

<!>安全提示：恢复密钥过程会破坏当前密码机内的密钥信息，请确定当前密钥是否继续使用，再决定是否恢复到当前密码机。

<i>提示：导入密钥备份文件时必须保证与当时备份导出时一致，默认备份文件名称为“swhsmbak.dat”。

附录 A

常见问题

1. 打开开关后不能加电

- a) 检查电源线接入是否正常；
- b) 检查机箱背面电源插口旁边的开关是否打开；

2. 如何判断密码机已经正常启动

开机后，预计十几秒或几十秒之后有“di”的一声，刚开机时的声音属于硬件自检。

3. 无法连接管理终端

- a) 检查是否存在密码机 IP 地址与其他设备冲突；
- b) 在管理终端使用“telnet xxx.xxx.xxx.xxx 80”命令检查是否已经启动管理服务；
- c) 是否记错了 IP 地址，可通过串口管理工具进行修改，详细看到用户光盘内的《紧急维护手册》

4. 开机后密码服务未启动

- a) 检查是否打开了开机自动启动服务选项；
- b) 检查开机时是否已经能够插入正确的操作员口令卡；
- c) 重新配置服务启动口令；

附录 B

主要技术指标

	SJJ1012 (RE5000 型) 2U	SJJ1012 (RE200 型) 1U
非对称算法性能		
1024 位 RSA 密钥对生成	50 对/秒	5 对/秒
1024 位 RSA 签名速度	5000 次/秒	1000 次/秒
1024 位 RSA 验证速度	25000 次/秒	5000 次/秒
256 位 SM2 密钥对生成	350 次/秒	350 次/秒
256 位 SM2 签名速度	650 次/秒	650 次/秒
256 位 SM2 验证速度	180 次/秒	180 次/秒
对称算法性能		
SM1 算法加密/解密速度	110Mbps	50Mbps
AES 算法加密/解密速度	110Mbps	50Mbps
物理特性		
规格	2U	1U
外形尺寸（宽 x 深 x 高）	447x500x86mm	447x450x43mm
重量	13Kg	10.5Kg
电气特性		
工作电源	220V， 50Hz	220V， 50Hz
功耗	280W	150W
网络接口	RJ-45 10/100/1000Mb x2	RJ-45 10/100/1000Mb
工作协议	TCP/IP	TCP/IP
读卡器	符合 ISO/IEC7816-3 协议	
MTBF	大于 50000 小时	大于 50000 小时

环境参数		
工作温度	10℃-60℃	10℃-60℃
非凝结的工作湿度	5%-85%	5%-85%
存储温度	0℃-60℃	0℃-60℃
非凝结的存储湿度	5%-95%	5%-95%

附录 C

权限设置表

管理类别	操作项	所需权限
设备管理	查看设备基本信息	
	查看设备运行信息	操作员权限
	查看设备维护信息	
	修改设备维护信息	管理员权限
服务管理	启动服务	操作员权限
	停止服务	操作员权限
	修改服务配置	操作员权限
网络管理	重新启动网络	操作员权限
	修改网络配置	操作员权限
权限管理	查看登录状态	
	查看权限设置表	
	增加第一个管理员	
	增加管理员	超级管理员权限
	删除管理员	超级管理员权限
	增加操作员	超级管理员权限
	删除操作员	超级管理员权限
密钥管理	设置系统保护密钥	超级管理员权限
	查看 RSA 密钥对状态	操作员权限
	产生 RSA 密钥对	管理员权限
	删除 RSA 密钥对	管理员权限
	导入 RSA 密钥对	管理员权限
	设置 RSA 私钥访问控制码	管理员权限
	查看 ECC 密钥对状态	操作员权限
	产生 ECC 密钥对	管理员权限
	删除 ECC 密钥对	管理员权限
	导入 ECC 密钥对	管理员权限
	设置 ECC 私钥访问控制码	管理员权限
	查看对称密钥状态	操作员权限
	产生对称密钥	管理员权限
	删除对称密钥	管理员权限
	导入对称密钥	管理员权限
备份恢复	密钥备份	超级管理员权限
	密钥恢复	

附录 D

安全须知

1. 使用本产品前请仔细阅读安全须知。
2. 请遵照产品上的警告标志与说明。
3. 清洁时，先拔下电源插头。切勿使用化学清洁剂。
4. 切勿将产品靠近水源、火源。
5. 切勿将产品放于不稳定的推车、椅子或桌面上，以免产品滑落而损伤。
6. 使用本产品时，请留意标签上注明的电压类型。如果您无法确定，请洽询经销商或当地电力公司。
7. 请勿放置任何物品于电源线上，更勿将电源线放在出入口，以免遭到踩踏。
8. 使用延长线时，请注意其电源负荷度。插在同一延长线的电器总用电数不可超过延长线的电流负荷度。同时，同一插座的耗电量不可超过保险丝的负荷量。
9. 切勿将任何其他物品插入本产品的槽内，以免误触电路，造成短路、起火。同时，请勿泼洒任何液体到产品上。
10. 请勿自行维修产品。因为不当的拆卸，可能会导致触电或其他不良后果。因此，有任何维修问题，请接洽合格技术服务人员。
11. 遇到下列状况时，请将电源插头拔掉，并寻求合格维护人员的协助：
 - a. 电源线或插头有破损时
 - b. 液体侵入机身时
 - c. 依照指示操作，而产品仍无法正常运作时，您只能调整操作步骤中所提及的控制，因为如果调整不当，可能导致计算机受损，而且这些控制方式需要合格的技术人员，才能将计算机恢复到原来状况
 - d. 产品不小心掉落地面或外壳有任何损伤时
 - e. 产品功能明显改变，指明需要维修时

附录 E

技术支持

如果您在安装、使用三未信安密码产品时遇到问题，请及时致电技术支持中心。

技术支持中心：010-84109583

电子邮件：support@sansec.com.cn

公司网址：www.sansec.com.cn