**用户手册**

**（通用产品类）**

产品名称： 科盾服务器密码机

认证委托方：深圳科盾量子信息科技有限公司

2022年 6 月 22 日

**版权声明**

国家密码管理局商用密码检测中心（以下简称“本中心”）拥有对本材料及其中内容的全部知识产权，受法律保护。

未经本中心书面许可，任何单位和个人不得以任何方式或理由对本材料的任何部分进行复制、修改、抄录、传播，或向第三方分发。

凡侵犯本中心版权等知识产权的，必依法追究其法律责任。

我们定期检查本材料的内容，在后续版本中会有必要的修正。

本材料以及其修改权、更新权及最终解释权均属本中心。

用户手册

描述产品满足的GM/T 0028-2014《密码模块安全技术要求》安全等级，支持的密码算法、软硬件环境、具备功能、主要技术指标和操作指南，指导用户安装、使用产品。对于密码卡、智能密码钥匙、智能IC卡、密码机等基础类密码产品，应提供包含主要函数接口/指令集等内容的二次开发手册。

用户手册中提及的密码算法、主要功能、密码部件应与前述技术工作总结报告和安全性设计报告内容一致。

**目 录**

[**1.** **简介** 1](#_Toc106695838)

[**1.1.** **主要功能** 1](#_Toc106695839)

[**1.2.** **技术指标** 2](#_Toc106695840)

[**1.1.** **密码运算速度** 2](#_Toc106695841)

[**1.2.** **永久密钥存储能力** 3](#_Toc106695842)

[**1.3.** **密码服务能力** 3](#_Toc106695843)

[**1.4.** **管理检测功能** 3](#_Toc106695844)

[**1.5.** **工作条件** 3](#_Toc106695845)

[**1.6.** **可靠性指标** 3](#_Toc106695846)

[**1.7.** **外形尺寸** 4](#_Toc106695847)

[**2.** **安装** 4](#_Toc106695848)

[**2.1.** **装箱清单** 4](#_Toc106695851)

[**2.2.** **外观简介** 4](#_Toc106695852)

[**2.2.1.** **前面板** 4](#_Toc106695856)

[**2.2.2.** **后面板** 5](#_Toc106695857)

[**2.3.** **设备安装** 6](#_Toc106695858)

[**2.4.** **使用前检查** 7](#_Toc106695859)

[**3.** **初始化和日常管理** 7](#_Toc106695860)

[**3.1.** **服务器密码机初始化** 7](#_Toc106695862)

[**3.1.1.** **出厂管理修改** 7](#_Toc106695863)

[**3.1.2.** **管理员初始化** 8](#_Toc106695864)

[**3.1.3.** **管理密钥初始化** 10](#_Toc106695865)

[**3.2.** **日常运维管理** 11](#_Toc106695866)

[**3.2.1.** **密钥管理** 12](#_Toc106695867)

[**3.2.2.** **密钥备份与恢复** 17](#_Toc106695868)

[**3.2.3.** **设备管理** 19](#_Toc106695869)

[**3.2.4.** **设备自检** 21](#_Toc106695870)

[**3.2.5.** **日志管理** 23](#_Toc106695871)

[**4.** **注意事项** 24](#_Toc106695872)

安全等级，支持的密码算法、软硬件环境、具备功能、主要技术指标和操作指南，指导用户安装、使用产品。对于密码卡、智能密码钥匙、智能IC卡、密码机等基础类密码产品，应提供包含主要函数接口/指令集等内容的二次开发手册。

用户手册中提及的密码算法、主要功能、密码部件应与前述技术工作总结报告和安全性设计报告内容一致

* 1. **简介**

深圳科盾量子信息科技有限公司生产的科盾服务器密码机是具备二级安全的应用层数据密码机，是一个物理安全的实体，能够实时地为密码业务应用系统提供密钥管理、消息验证、数据加密、签名的产生和验证、密钥协商等密码服务，保证数据从产生、传输、接收到管理这一系列过程的安全性、有效性、完整性、不可抵赖性。可应用身份认证、数据加密、数据完整性保护等多种应用场景。在部署应用中，一台服务器密码机可以为多个应用系统提供密码服务或密钥管理，当单台密码机的处理能力难以满足主机系统的使用要求时，可以采用密码机群集，由多台密码机同时为一个应用系统提供统一的密码运算和密钥管理服务。为确保密码机使用的安全，密码机应当与主机安装于同一机柜或同一机房中，防止敏感数据的泄漏。服务器密码机典型部署模式如下图所示：



1. **科盾服务器密码机典型部署模式**
   1. **主要功能**

科盾服务器密码机是应用层节点数据密码机，是一个物理安全的实体，能够实时地为密码业务应用系统提供密钥管理、消息验证、数据加密、签名的产生和验证、密钥协商等密码服务，保证数据从产生、传输、接收到管理这一系列过程的安全性、有效性、完整性、不可抵赖性。

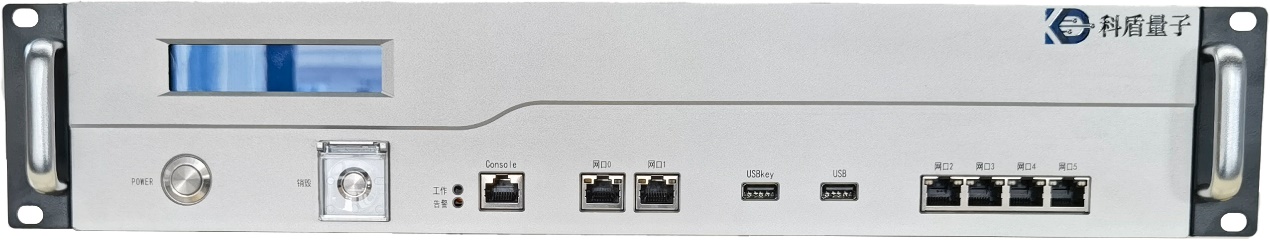
密码机采用天津国芯的CCUPH2002 PCI-E密码卡实现国产密码算法和密钥管理的支持。服务器密码机主要功能特点如下：

1. 数据加解密：支持SM1、SM4分组密码算法以及SM2 非对称算法加解密；
2. 数字签名/验证：支持SM2公钥密码算法；
3. 密钥协商：支持SM2算法的密钥协商；
4. 杂凑运算：支持SM3运算；
5. 密钥库安全存储功能：通过密码卡安全存储密钥；
6. 提供数字物理噪声源芯片生成随机数；
7. 具有手动密钥自毁功能；
8. 具有图形化配置管理功能；
9. 采用智能密码钥匙作为管理员认证介质，实现管理员多因子认证；
10. 支持密钥备份恢复功能；
11. 具有系统算法自检、状态检测及报警功能；
12. 具备软件完整性保护和校验功能；
13. 主机接口采用太网接口，通信协议采用TCP/IP协议。
    1. **技术指标**
    2. **密码运算速度**
14. SM2签名：21000次/秒
15. SM2验证：22000次/秒
16. SM2加密：10Mbps
17. SM2解密：20Mbps
18. SM1/SM4算法运算速度：800 Mbps
19. SM3杂凑运算速度：850 Mbps
    1. **永久密钥存储能力**
20. 用户SM2密钥对：64对
21. 密钥加密密钥:64条
    1. **密码服务能力**
22. 网络接口传输速率：100/1000Mbps自适应
23. 并行处理用户数：1024个
24. 提供密码设备标准接口
25. 客户端API支持主流国产平台以及主流Windows平台
    1. **管理检测功能**
26. 支持智能密码钥匙管理
27. 提供配置管理工具
28. 提供定期自检和手动检测功能
29. 支持第三方密钥管理
    1. **工作条件**
30. 额定工作电压： 220V±10％ ，50Hz±3
31. 工作环境温度： 0℃～40℃
32. 工作环境相对湿度：30％～90％ RH(40℃)
33. 存贮环境温度：-40℃～55℃
34. 存贮环境相对湿度：20％～93％ RH(40℃)
35. 大气压力：86～106KPa
    1. **可靠性指标**
36. 平均无故障工作时间：≥20000小时
37. 使用寿命: 大于10年
    1. **外形尺寸**
38. 2U标准机箱
39. 重量：小于10KG
40. 外壳结构：工业钢
    1. **安装**
42. 1. **装箱清单**

打开设备包装箱后，按装箱明细表检查以下部件是否齐全。

1. 科盾服务器密码机一台
2. 智能密码钥匙6个
3. 用户手册一本
4. 220V交流电源线两根
5. 串口线一根
6. 产品保修卡一张
7. 产品质量跟踪卡一张
8. 服务记录表一张
9. 顾客满意度调查表一张
10. 机架螺钉一套（4个螺钉和4个螺母）
11. 随机光盘一张
    1. **外观简介**
12. 2. 1. **前面板**

服务器密码机前面板如下图所示：



1. 服务器密码机前面板图

前面板各部件的功能如下：

1. USB2.0接口

* USB接口用于管理员身份鉴别，密钥备份与管理。
* USBKey接口（保留）。

1. 液晶屏

* 服务器密码机运行状态描述显示输出。

1. 状态灯

* 工作指示灯：服务器密码机加电正常运行时，工作灯点亮。
* 告警指示灯：异常状态指示。当服务器密码机处于非正常状态时或者没有进行初始化时，报警灯亮，可结合液晶屏显示输出判断密码机故障信息。

1. 控制台串口

串行通信接口。通过串口登录服务器密码机的接口，密码机运维人员可以通过该端口登录密码机进行检修。

1. 业务网口

服务器密码机接入网络交换设备的接口。一般将第六个网络端口作为配置管理口，其余五个网络端口可提供密码服务业务。

1. 销毁按钮

用于销毁密钥。触发销毁按钮时，服务器密码机内部未受保护密钥将全部销毁。

1. 复位开关

用于对服务器密码机进行复位。

* + 1. **后面板**

服务器密码机后面板如下图所示：



1. 服务器密码机后视图

后面板各部件的功能如下：

1. 交流电源插孔

服务器密码机220V交流电源输入。密码机提供双电源供电，有两个电源插孔。

1. 机仓锁

对服务器密码机内的部件进行物理防护。用户请勿私自打开，否则可能造成严重后果。

1. 机舱接地柱

用于连接机柜接地端。

* 1. **设备安装**

服务器密码机的高度为2U，宽度为19英寸，能直接安装在19英寸标准机柜内。

安装过程如下：

1. 将服务器密码机放置在托盘上，移动服务器密码机使密码机前面板的四个开孔与机柜导槽的开孔对齐；
2. 用机架螺钉将服务器密码机前面板固定在机柜导槽上；
3. 用保护地电缆将服务器密码机的机仓接地柱（在服务器密码机后面板）和机柜的接地端连接在一起，以提高服务器密码机的安全性和抗电磁干扰能力；
4. 将机柜内的网线插入业务网口；
5. 用两根电源线将服务器密码机分别连接到机柜内的主、备220V交流电源上。
   1. **使用前检查**

检查项目如下：

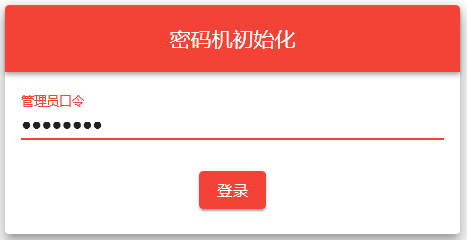
1. 服务器密码机应水平放置，机架螺钉不松动；
2. 服务器密码机器左右两侧应有良好的通风环境；
3. 服务器密码机业务网口插入网线后网口指示灯亮；
4. 后面板电源模块上的指示灯应点亮。
   1. **初始化和日常管理**

服务器密码机的初始化和日常管理流程下图所示：



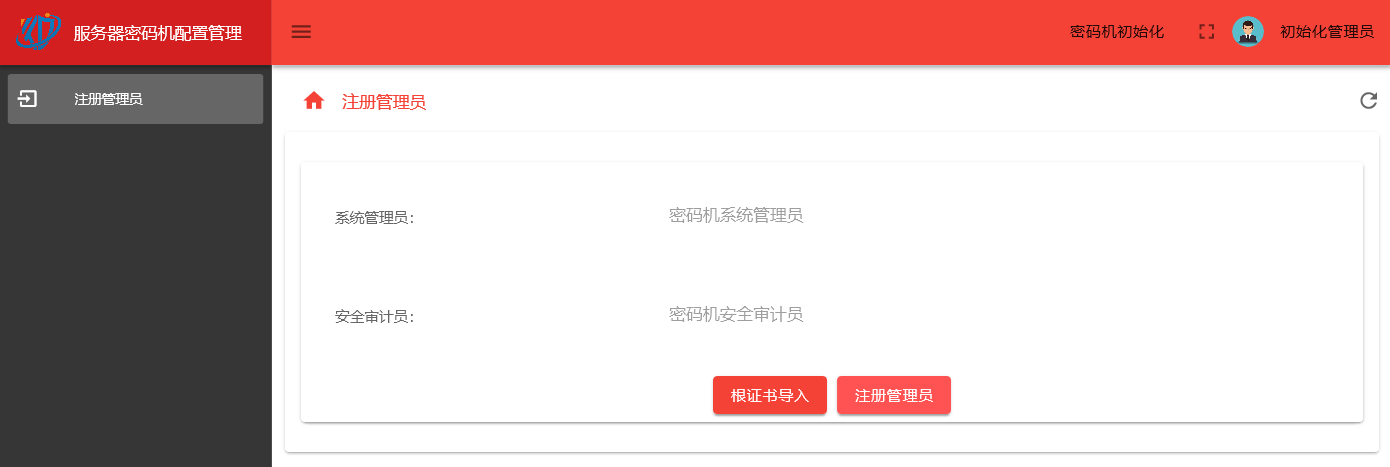
1. 服务器密码机的初始化和日常配置流程图
2. 1. **服务器密码机初始化**
      1. **出厂管理修改**

在服务器密码机开启后等待1-2分钟，管理终端计算机IP设置为192.168.1.X,其中1<X<255，连接网口5。在管理终端计算机浏览器输入http://192.168.1.1:8080/#/ms/init，初始化界面如下图所示：



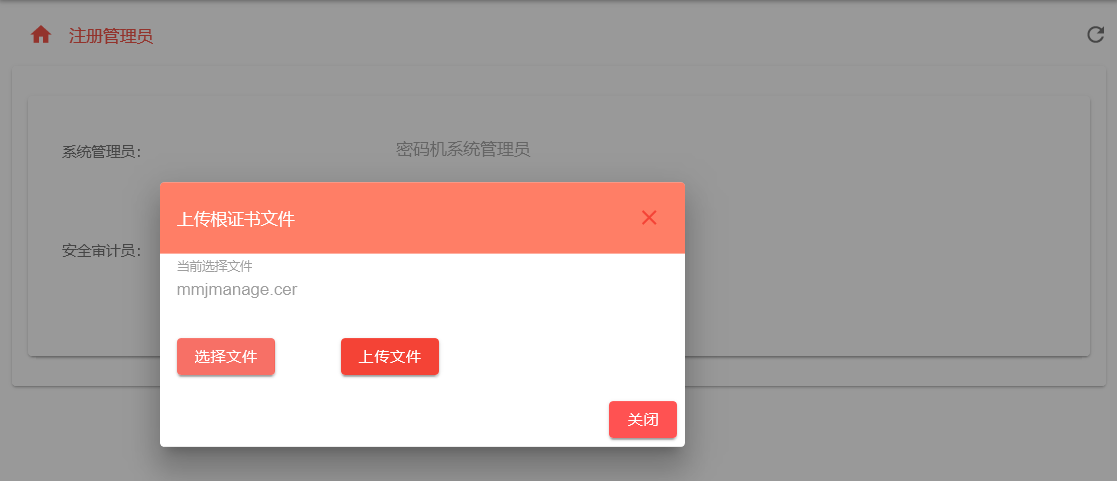
1. 密码机出厂初始登录

输入管理员口令：1qaz@WSX，进入服务器密码机配置管理页面。首先进行密码机初始化。密码机初始化页面如下图所示：



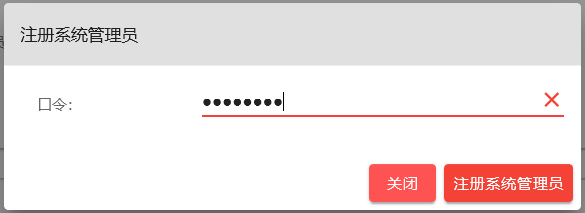
1. 密码机初始化页面
   * 1. **管理员初始化**

在初始化页面，点击根证书导入导入证书，如图7所示：



1. 根证书导入

在初始化页面，点击注册管理员，在下图页面中输入口令，并在服务器密码机上插入管理员智能密码钥匙（密码机配套设备）：



1. 系统管理员注册页面

系统管理员制作完成后，拔出系统管理员介质，插入介质制作安全审计员，安全审计员制作界面如下图所示：

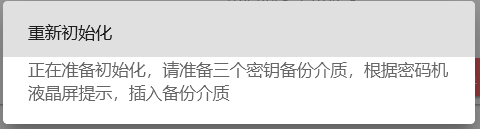


1. 安全审计员注册页面

系统管理员及安全审计员初始化完成后，请妥善保管好管理员介质，并记住管理员口令。

* + 1. **管理密钥初始化**

在初始化页面中，点击密码机初始化，显示以下界面：

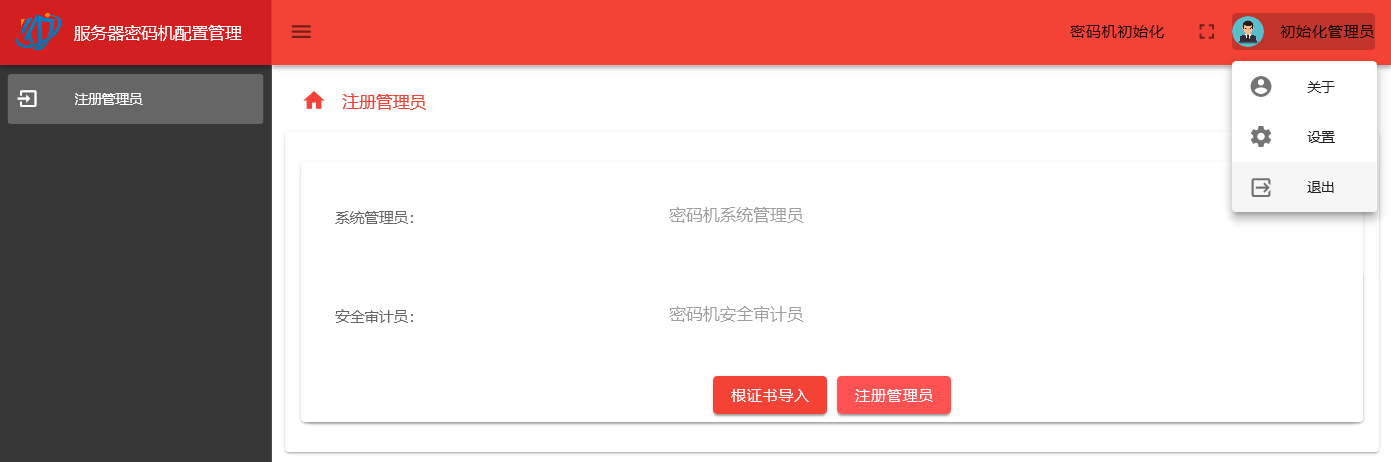


1. 密码机初始化

密钥备份介质采用智能密码钥匙，为便于设备管理，建议将设备管理员和设备操作员分别作为密钥备份介质。根据液晶屏提示，依次插入三个管理密钥分量存储介质。管理密钥生产过程中，液晶屏显示：拔掉当前介质，插入备份介质2…，

拔出当前介质，插入另一个备份介质，管理密钥生成完毕，液晶屏显示：管理密钥初始化：操作成功。

服务器密码机初始化完成后，退出初始化管理界面，进入正常使用模式。



1. 退出初始化管理页面
   1. **日常运维管理**

日常运维管理包括密钥管理、密钥备份与恢复、设备自检、设备管理和日志管理，需要设备管理员或设备操作员权限。根据登录管理员的不同，展示不同的管理菜单。

（1）设备管理员管理菜单：密钥管理、密钥备份与恢复、设备自检、设备管理。

（2）设备操作员管理菜单：设备管理、日志管理。

登录<http://IP:8080/#/ms/login>，在服务器密码机上插入系统管理员或安全审计员介质，在下图所示界面输入管理员口令（IP为服务器密码机管理地址，在设备出厂初始化时设置）：



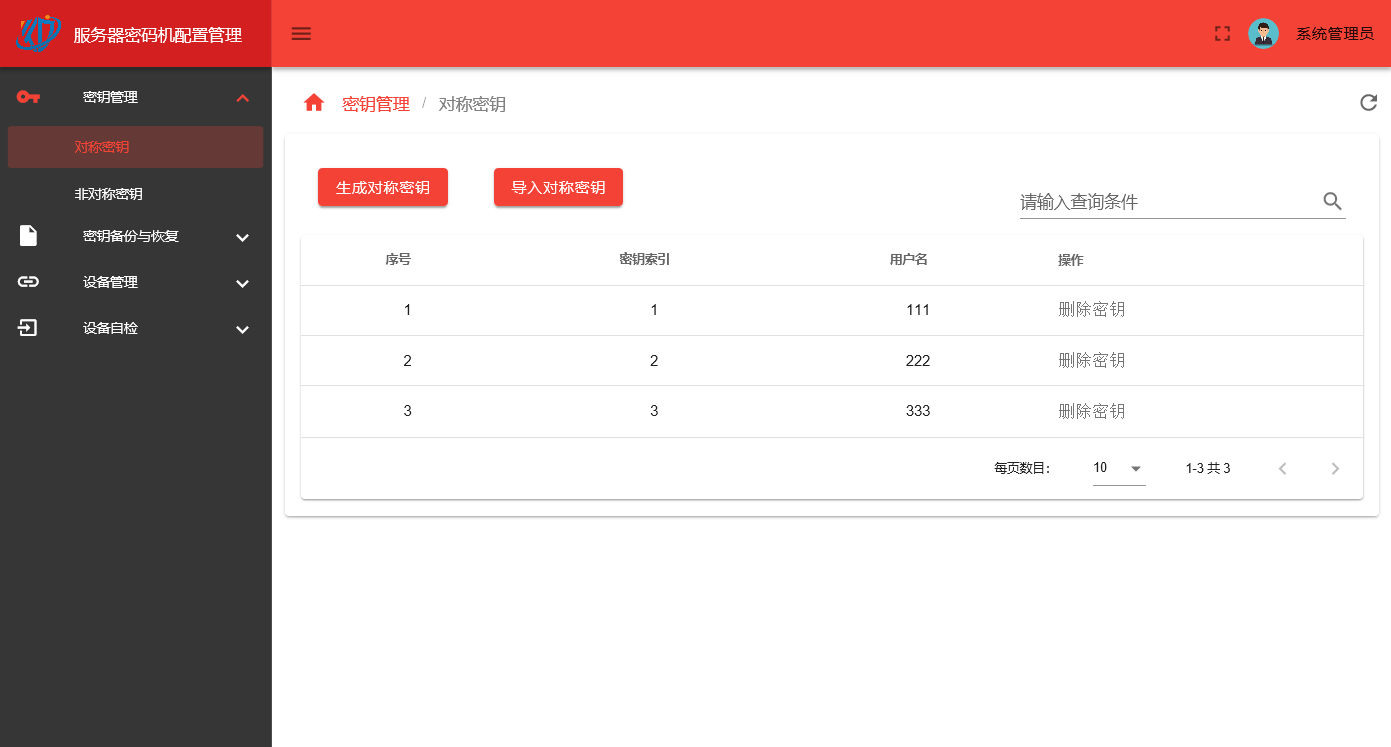
1. 管理员登录

根据输入的是系统管理员信息，还是安全审计员信息，进入相应的配置管理页面。

* + 1. **密钥管理**

密钥管理包括对称密钥管理和非对称密钥管理两个部分。

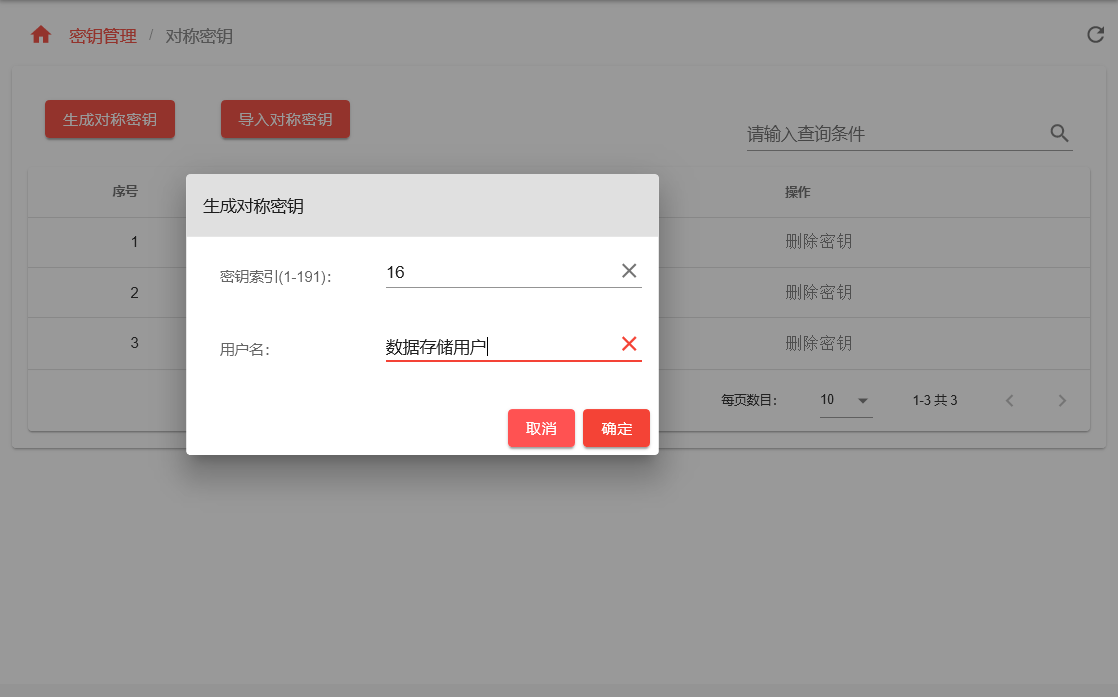
* + - 1. **对称密钥管理**

点击“对称密钥”菜单，显示服务器密码机中已经配置的对称密钥管理界面：

1. 服务器密码机对称密钥信息

上图中显示服务器密码机中对称密钥信息，索引号，对称密钥用户信息等。

点击“生成对称密钥”按钮，可以在服务密码机中生成对称密钥，并指定该对称密钥用户，便于服务器密码机密钥管理。对称密钥生成操作如下图所示：



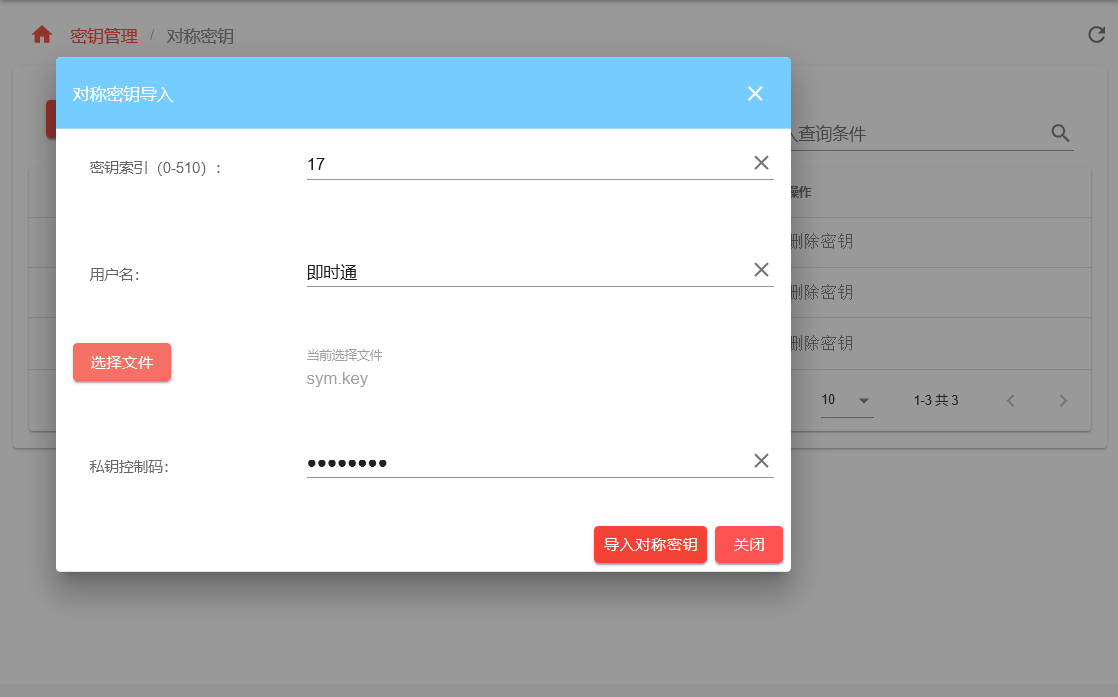
1. 对称密钥生成操作界面

产生对称密钥时，服务器密码机液晶屏会显示对称密钥产生情况，显示输出：

**（*用户名*）正在进行密钥管理操作**

**密钥管理操作完成**

密钥导入操作：点击“导入对称密钥”按钮，可以将外部对称密钥导入服务器密码机。对称密钥导入操作如下图所示：

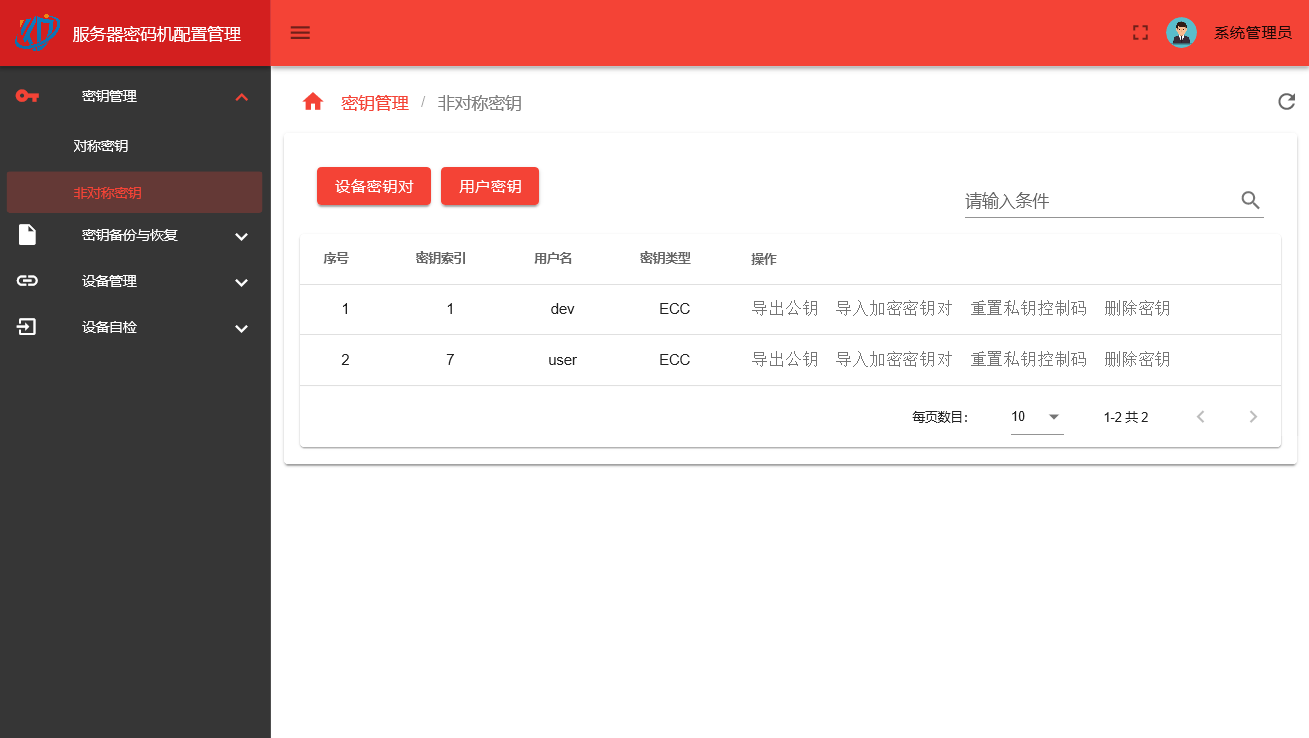
1.  对称密钥导入操作界面

服务器密码机液晶屏显示对称密钥导入情况。

密钥删除操作：点击“删除密钥”按钮，可以删除对应的密钥。

* + - 1. **非对称密钥管理**

点击“非对称密钥”菜单，显示服务器密码机中已经配置的非对称密钥管理界面：



1. 服务器密码机非对称密钥信息

上图中显示服务器密码机中非对称密钥信息，索引号，对称密钥用户信息等。

点击“设备密钥对”按钮，可生成非对称设备密钥对。生成非对称设备密钥对操作如下图所示：



1. 非对称设备密钥生成操作界面

点击“用户密钥”按钮，可以在服务密码机中生成非对称用户密钥，并指定该对称密钥用户。非对称用户密钥生成操作如下图所示：

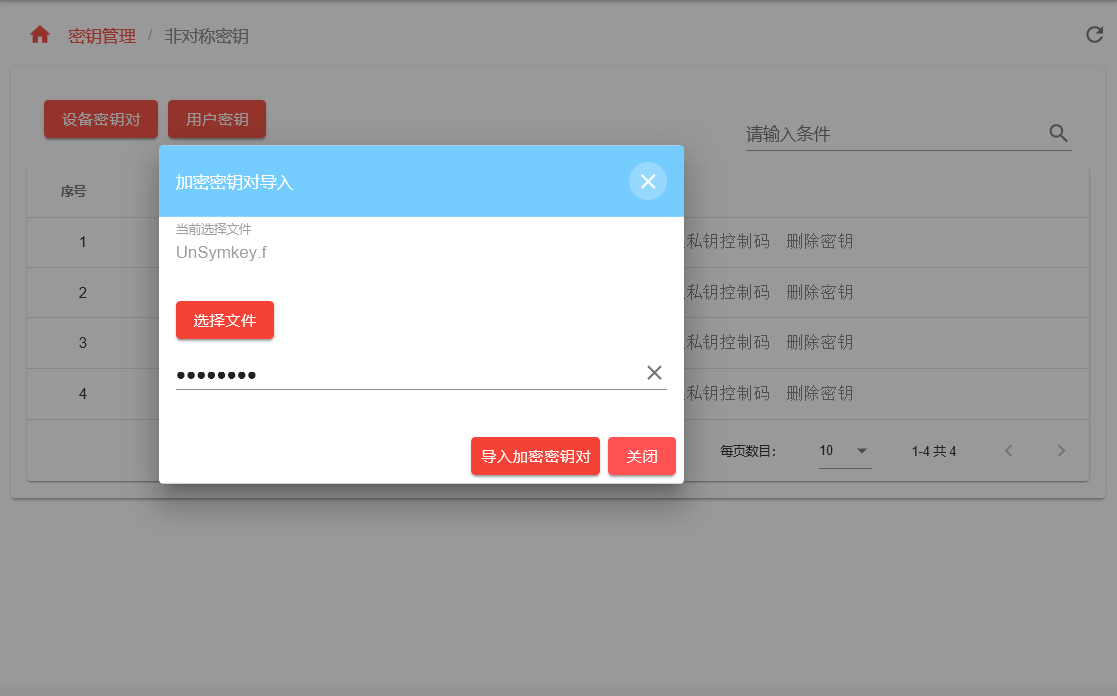


1. 非对称用户密钥生成操作界面

在非对称密钥管理页面的相应密钥后面，点击“导出公钥”按钮，可以将相应签名密钥对的公钥导出，并存入配置管理操作终端本地文件系统中，如下图所示（图中导出7号公钥）：

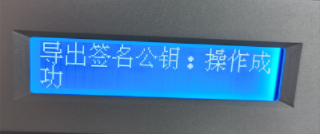
1.  非对称密钥公钥导出操作

在非对称密钥管理页面的相应密钥后面，点击“导入加密密钥对”按钮，可以将外部加密密钥对导入服务器密码机中。如下图所示：



1. 非对称加密密钥对导入操作

在上图中点击“选择文件”，选择第三方生成的加密密钥对文件，点击“导入加密密钥对”，完成加密密钥对导入。加密密钥对导入时液晶屏显示如下：



1. 非对称加密码密钥对导入液晶屏显示

密钥成功导入后，液晶屏显示：导出签名公钥：操作成功。

* + 1. **密钥备份与恢复**

可以将服务器密码机中的密钥定期备份，密钥恢复可以恢复服务器密码机密钥到备份时状态。

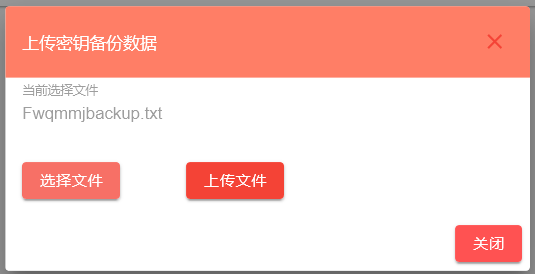
* + - 1. **密钥备份**

点击“密钥备份”执行密钥备份，密钥备份完成后，加密后的密钥备份文件写入配置管理操作终端文件系统中，管理员安全保存该文件即可，如下图所示：



1. 密钥备份密文下载
   * + 1. **密钥恢复**

点击“密钥恢复”菜单，点击“密钥上传”，选择备份密钥文件（最新一次密钥恢复时生成的文件）：



1. 选择并上传密钥备份文件

文件上传成功后，在管理界面点击点击“密钥恢复”按钮，

密钥恢复成功后，管理界面显示：

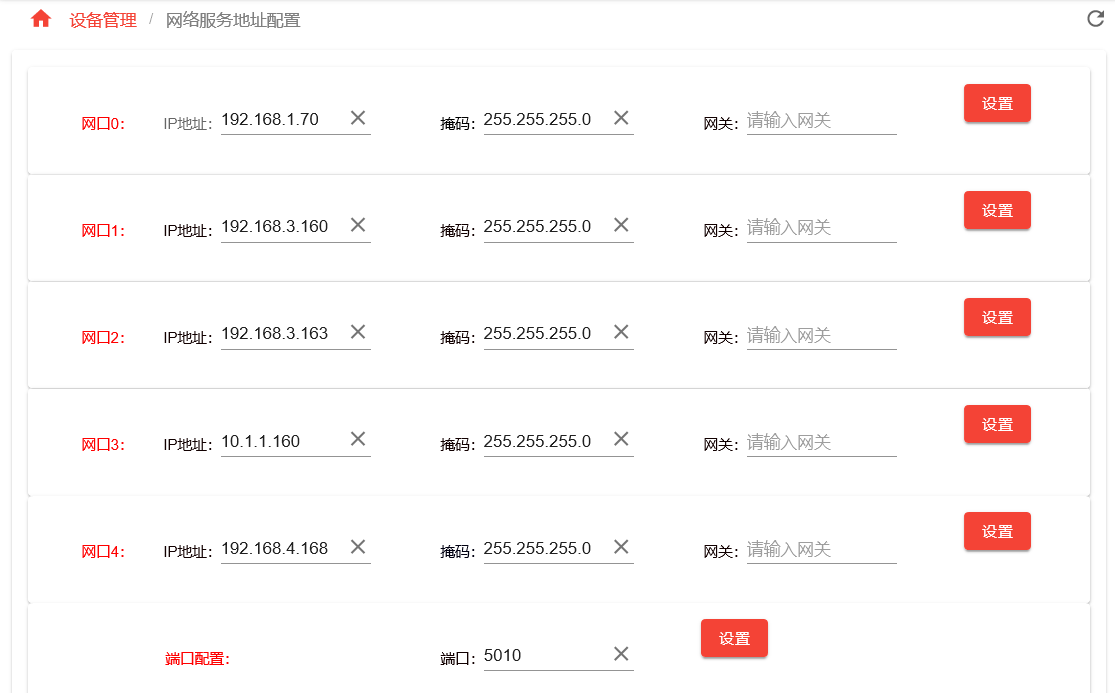


1. 密钥恢复成功界面显示
   * 1. **设备管理**

设备管理包括管理地址配置、网络服务地址配置、用户白名单管理、设备控制几个功能。

1. 网络服务地址配置

配置密码机五个业务网络接口地址。地址配置管理页面如下：

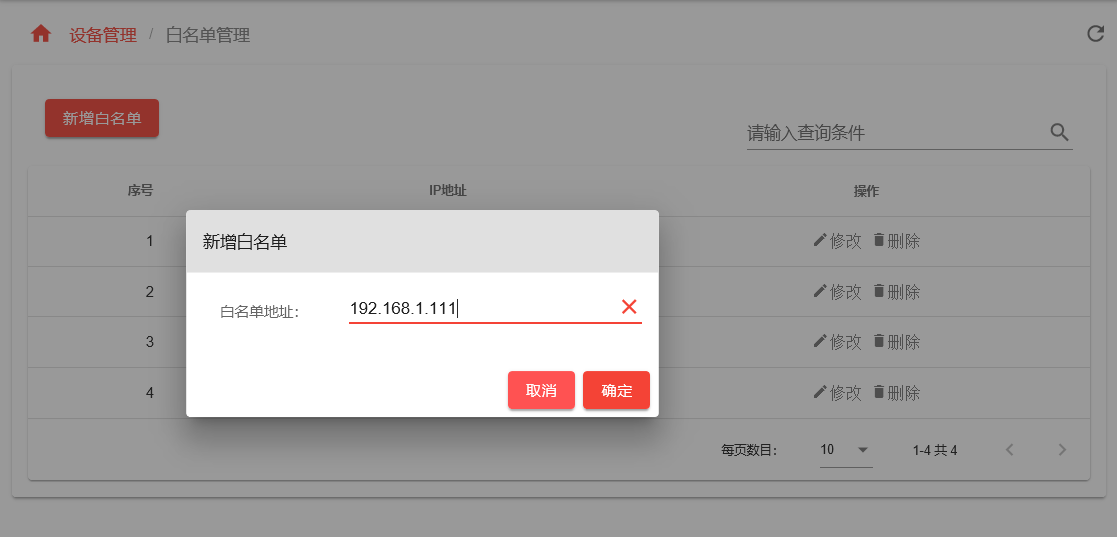


1. 服务器密码机设备信息

根据实际网络连接情况，设置相应的地址即可。

1. 白名单管理

配置可以使用服务器密码机的客户端地址信息。选择“白名单管理”菜单，显示当前的白名单地址。点击“新增白名单”按钮，可以添加白名单地址：



1. 白名单地址添加

在白名单地址后的“修改”和“删除”按钮，可以修改或删除该条地址信息。

* + 1. **设备自检**

在设备自检中设备点击设备信息查看，显示服务器密码机信息如下图所示：



1. 服务器密码机设备信息

设备自检测试设备随机数的合规性，SM1,SM2,SM3SM4算法执行是否正确。点击相应的菜单选项，执行自检操作，密码机液晶屏显示目前自检状态。其中随机数合规性检测，随机数十二项随机数，检测时间较长，请耐心等待。设备自检完成后，自检结果显示在屏幕上：



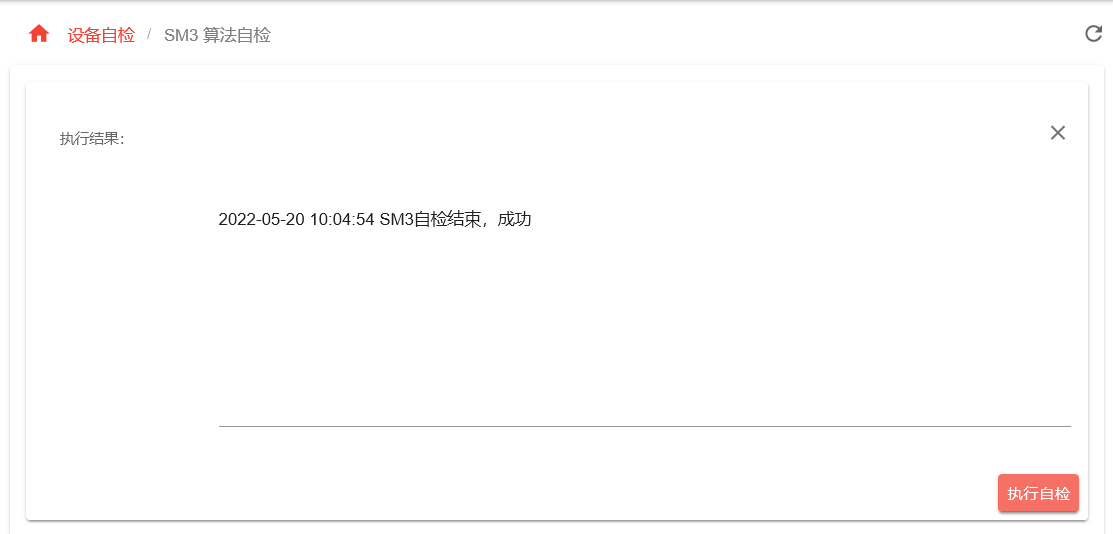
1. 随机数十二项自检结果显示



1. SM1算法自检结果显示



1. SM2算法自检结果显示



1. SM3算法自检结果显示



1. SM4算法自检结果显示
   * 1. **日志管理**

显示服务器密码机管理日志以及错误日志信息。点击管理日志菜单，显示如下日志信息：



1. 密码机日志管理

点击导出管理日志可将所有日志信息导出，如下图所示：



1. 导出管理日志操作

点击错误日志菜单，显示所有错误日志，点击导出错误日志可导出日志信息：



1. 密码机错误日志
   1. **注意事项**
2. 服务器密码机必须经过初始化后，才能为应用系统正常提供密码运算服务；
3. 服务器密码机每次重新开机，必须插入管理密钥分量载体，完成开机认证后，才能为应用系统正常提供密码运算服务；
4. 管理员关闭管理界面前，请退出管理员权限；
5. 严禁私自打开服务器密码机机箱，严禁带电插拔通信线缆；
6. 服务器密码机不能正常工作时，请填好保修单，及时与供应商联系，以便进行检查、维修；
7. 应妥善保存服务器密码机密钥备份载体，以防止备份载体损坏或者丢失给生产带来损失；
8. 若密钥备份载体损坏，严禁随便丢弃，必须交还给配发单位，由配发单位统一处理。