服务器密码机用户手册

SJJ1920-G

北京神州龙芯集成电路设计有限公司

V1.0

目 录

1. 产品介绍

1.1.产品简介

服务器密码机是由神州龙芯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。

客户端应用程序通过调用服务器密码机提供的标准 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服务器密码机所提供的安全功能。服务器密码机 API 接口遵循《GM/T 0018-2012 密码设备应用接口规范》，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

密钥生成与管理：支持通过物理噪声源生成 256 位 SM2 密钥对和 1024/2048 位 RSA 密钥对，采用由国家密码管理局审批使用的物理噪声源产生器芯片生成的随机数。

密钥的安全存储：设备内可存储 SM2 密钥对（包含签名密钥和加密密钥对）和 RSA 密钥对，并且私钥部分受设备主密钥的加密保护。

数据加密和解密：支持 SM1 和 SM4 密码算法的 ECB 和 CBC 模式的数据加密和解密运算。

消息鉴别码的产生和验证：支持基于 SM1 和 SM4 密码算法的 MAC 产生及验证。

数据摘要的产生和验证：支持 SHA-1、SHA-256、SM3 等杂凑密码算法。

数字签名的产生和验证：可以根据需要利用内部存储的 SM2 密钥对或外部导入 SM2 私钥对请求数据进行数字签名。

物理随机数的产生：采用由国家密码管理局审批使用的物理噪声源产生器芯片生成的随机数。

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

支持国产密码算法：采用安全先进的密码模块，符合国家密码管理机构的要求，全面支持 SM1、SM2、SM3、SM4 等标准密码算法。

支持多种操作系统：应用服务器与服务器密码机之间采用 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：服务器密码机 API 接口遵循《GM/T 0018-2012 密码设备应用接口规范》，通用性好。

三层密钥结构：采用“设备保护密钥-用户密钥-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。

支持连接密码及访问白名单：通过连接密码和白名单的支持，实现了服务器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。

2. 操作指南

2.1.服务器密码机安装

1.打开服务器密码机包装，对照“装机清单”，检查服务器密码机设备以及配件是否齐全，从包装箱中取出服务器密码机，并把它固定好。

2.使用电源线连接电源。

3.打开服务器密码机电压开关，启动服务器密码机。

4.准备一台 PC 机作为服务器密码机的管理终端，使用网线连接到服务器密码机的“网口 1”或者“网口 2”，修改管理终端的 IP 地址，使其 IP 地址与服务器密码机的 IP 地址在同一个网段。

注：服务器密码机两个网口的默认出厂 IP 为绑定模式：192.168.1.2，使用两个网口中的任何一个网口都可以，服务器密码机的子网掩码默认为 255.255.255.0。

2.2.启动管理程序

1. 打开连接到服务器密码机的计算机上的浏览器，输入网址 http://192.168.1.2 来访问服务器密码机管理系统。

2.输入出厂默认的用户名 Admin 和密码 Admin1234，登录到服务器密码机。

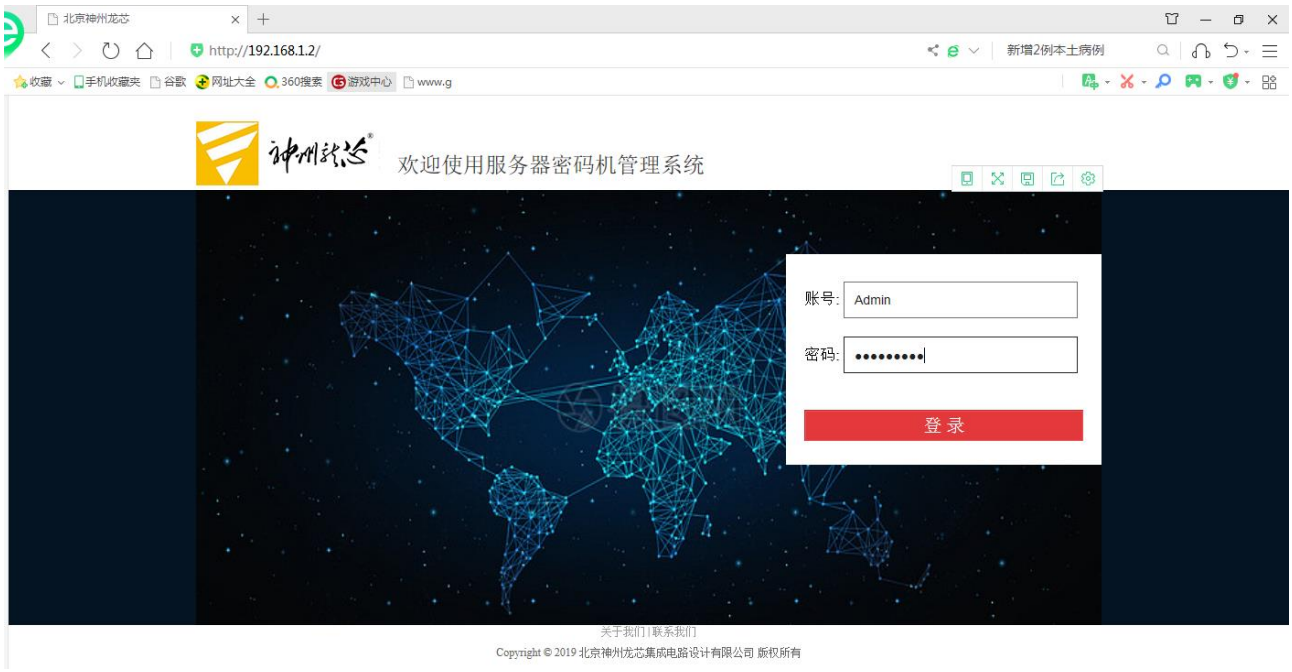


图 2-1 管理工具登录界面

登录成功后，就可以进入到服务器密码机管理系统首页，如图所示：

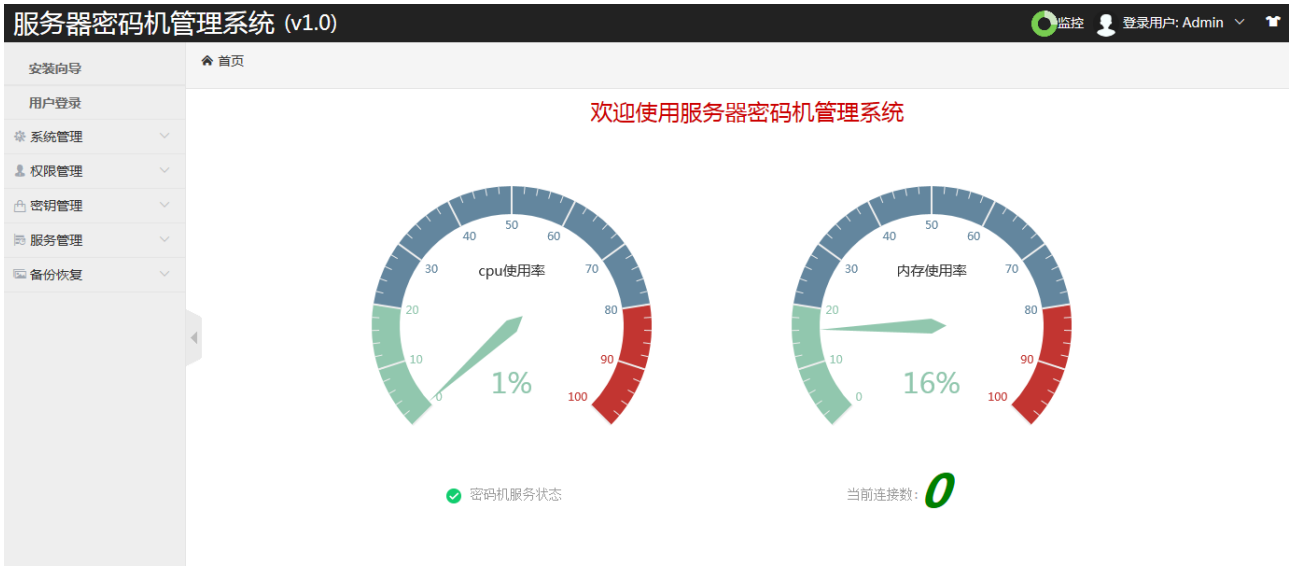


图 2-2 服务器密码机管理系统首页

注意：由于是基于网络的管理方式，所以允许多台管理终端同时连接服务器密码机。但是，如果多个管理终端同时对服务器密码机进行管理操作的话，可能会发生不可预知的错误。

2.3. 安装向导

第一次使用服务器密码机，可以使用服务器密码机管理系统的安装向导功能，逐步完成对密码机的基本配置。如果需要使用其他配置功能，可参考本文档其他管理操作说明。

安装向导提供以下主要配置功能：

a) 初始化密码设备：清空所有密钥及管理信息。

图 2-3 初始化密码机及销毁密钥

点击确定后，进入增加管理员界面

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（标准配置为 3 个管理员），把标记为“管理员”的 USBKey 按照正确的方向插入到服务器密码机的 usb 接口中，然后输入 USBKey 的 PIN 口令，USBKey 默认密码：12345678，单击“增加管理员”按钮。

图 2-4 增加管理员

成功添加 3 个管理员后，进入增加操作员界面。

c)增加操作员：用于启动密码服务，增加一个操作员（标准配置为 1 个操作员）。将标记为“操作员”的 USBKey 按照正确的方向插入设备的 usb 接口中，操作员 USBKey 的默认 PIN 口令为：12345678，输入口令，单击“增加操作员”按钮。

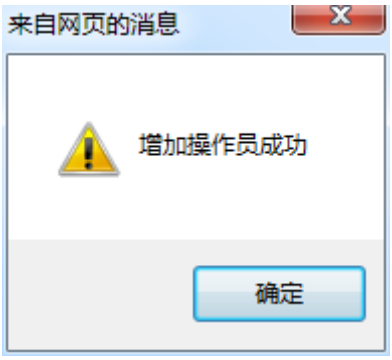
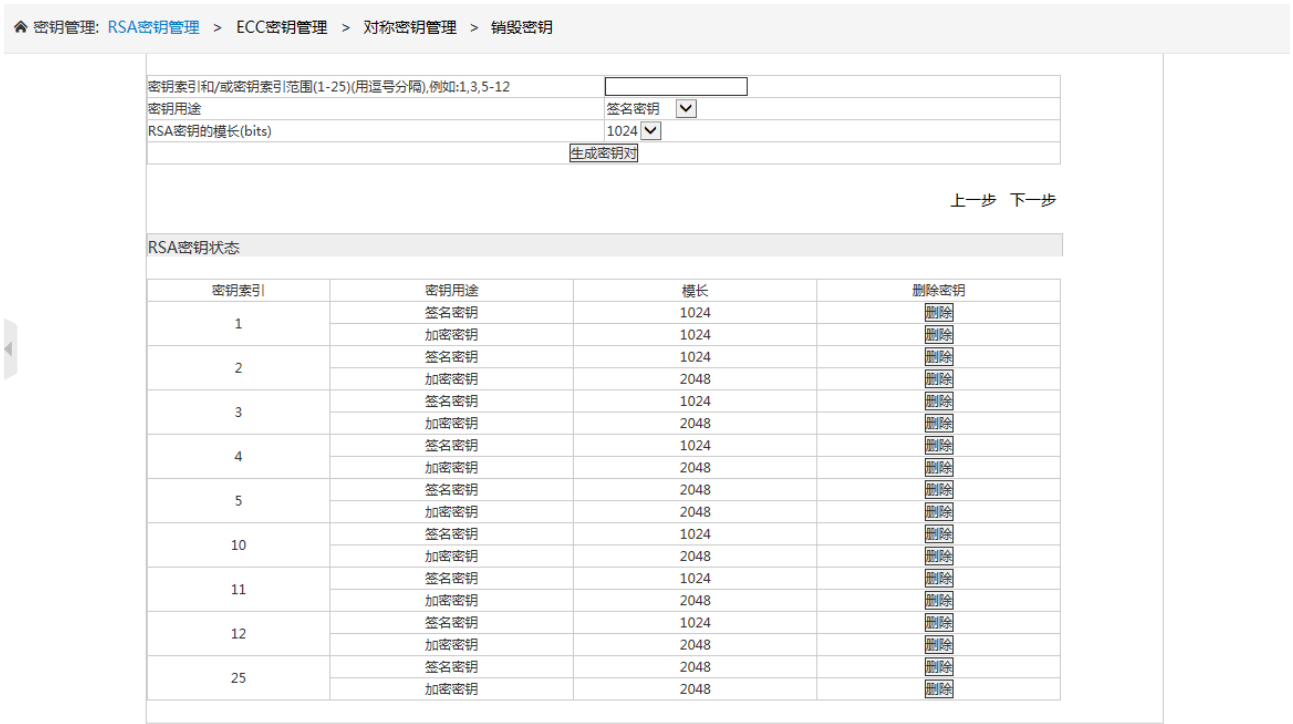


图 2-5 增加操作员

成功增加操作员后，单击下一步按钮，进入内部 RSA 密钥对管理界面。

d)内部 RSA 密钥对管理：产生签名密钥对或加密密钥对并保存在服务器密码机设备内部。在密钥索引和/或密钥索引范围输入框中，输入密钥索引，选择密钥用途和 RSA 密钥的模长，单击“生成密钥对”按钮，就可以看到成功生成的 RSA 密钥状态。如下图所示：



密钥索引	密钥用途	模长	删除密钥
1	签名密钥	1024	删除
	加密密钥	1024	删除
2	签名密钥	1024	删除
	加密密钥	2048	删除
3	签名密钥	1024	删除
	加密密钥	2048	删除
4	签名密钥	1024	删除
	加密密钥	2048	删除
5	签名密钥	2048	删除
	加密密钥	2048	删除
10	签名密钥	1024	删除
	加密密钥	2048	删除
11	签名密钥	1024	删除
	加密密钥	2048	删除
12	签名密钥	1024	删除
	加密密钥	2048	删除
25	签名密钥	2048	删除
	加密密钥	2048	删除

图 2-6 RSA 密钥对管理

单击“下一步”按钮，进入内部 ECC 密钥对管理界面。

e)内部 ECC 密钥对管理：产生 ECC 签名密钥对或加密密钥对并保存在服务器密码机设备内部。输入密钥索引或者密钥索引范围，选择密钥用途和 ECC 密

钥的模长，然后单击“生成密钥对”按钮。就可以看到成功生成的 ECC 密钥状态。如下图所示：

图 2-7 ECC 密钥管理

单击“下一步”按钮，进入对称密钥管理界面。

f)对称密钥管理：产生对称密钥并保存在服务器密码机设备内部。输入密钥索引或者密钥索引范围，选择密钥长度，单击“产生密钥”按钮。成功生成的对称密钥如下图所示：

图 2-8 对称密钥管理

单击“下一步”按钮，进入网络配置信息界面。

g)网络配置信息：查看或修改设备的网络配置参数。

图 2-9 网络配置信息

单击“下一步”按钮，进入服务配置信息界面。

h)服务配置信息：修改服务启动参数。

图 2-10 服务配置信息

单击“下一步”，进入备份密钥向导界面。

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。

图 2-11 密钥备份

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。

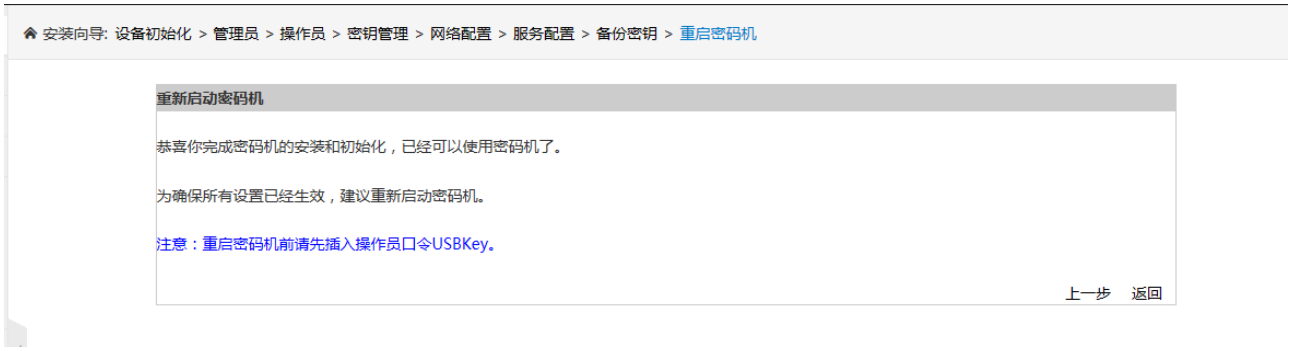


图 2-12 重启服务器密码机

注：在重新启动密码机前，请先插入操作员 USBKey。

3. 用户登录

在登录时请根据 USBKey 标示的方向插入管理员或者操作员 USBKey 并输入 USBKey 保护口令（PIN），默认密码：12345678，才能获得对 USBKey 的访问权限。

查看当前管理员或操作员的登录状态。

图 3-1 用户登录界面

增加登录的管理员或操作员数目

输入 USBKey 的 PIN 口令，点击“用户登录”。

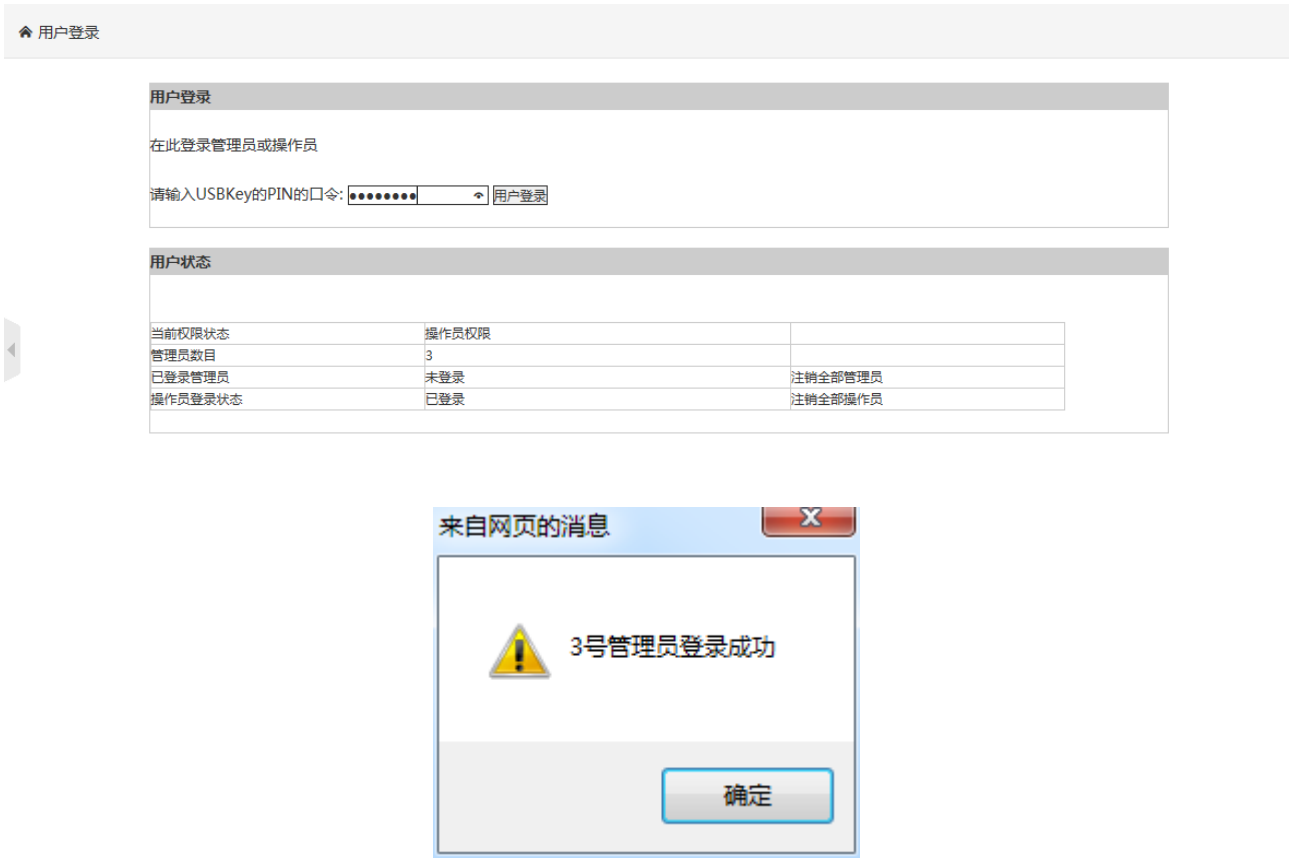


图 3-2 增加登录的管理员或操作员

注销全部管理员或全部操作员，选择需要注销全部管理员或注销全部操作员，点击相应的注销按钮。注销后，相应的管理员或者操作员的登录状态为未登录。

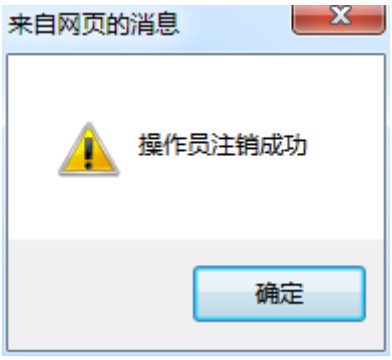


图 3-3 注销成功信息提示

4. 系统管理

4.1. 设备基本信息查看

可查看生产厂商、设备型号、产品号、设备序列号等信息。

图 4-1 设备信息查看

4.2. 查看/修改设备维护信息

用户可以查看和修改设备维护方面的相关信息。

图 4-2 修改设备信息

4.3. 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。

图 4-3 多网卡绑定，多个网口共享一个 IP 地址

图 4-4 不绑定多网卡的 IP 地址配置

注：当修改了 IP 地址后，修改后的 IP 地址不能立即生效，需要重新启动服务器密码机才能启用新的地址。

双网卡绑定后，多个网口共享一个地址，网卡工作在主设备模式下实现网络冗余。

4.4. 修改系统登录口令

用户可以修改服务器密码机管理系统的登录口令。输入原口令，然后在输入两次一样的新的口令，单击“修改口令”按钮即可。

图 4-5 修改登录口令

4.5. 设备自检

点击“设备自检”按钮，可以检查设备的状态。

图 4-6 设备自检

4.6. 查看日志

可以查看服务器密码机进行的各种操作。

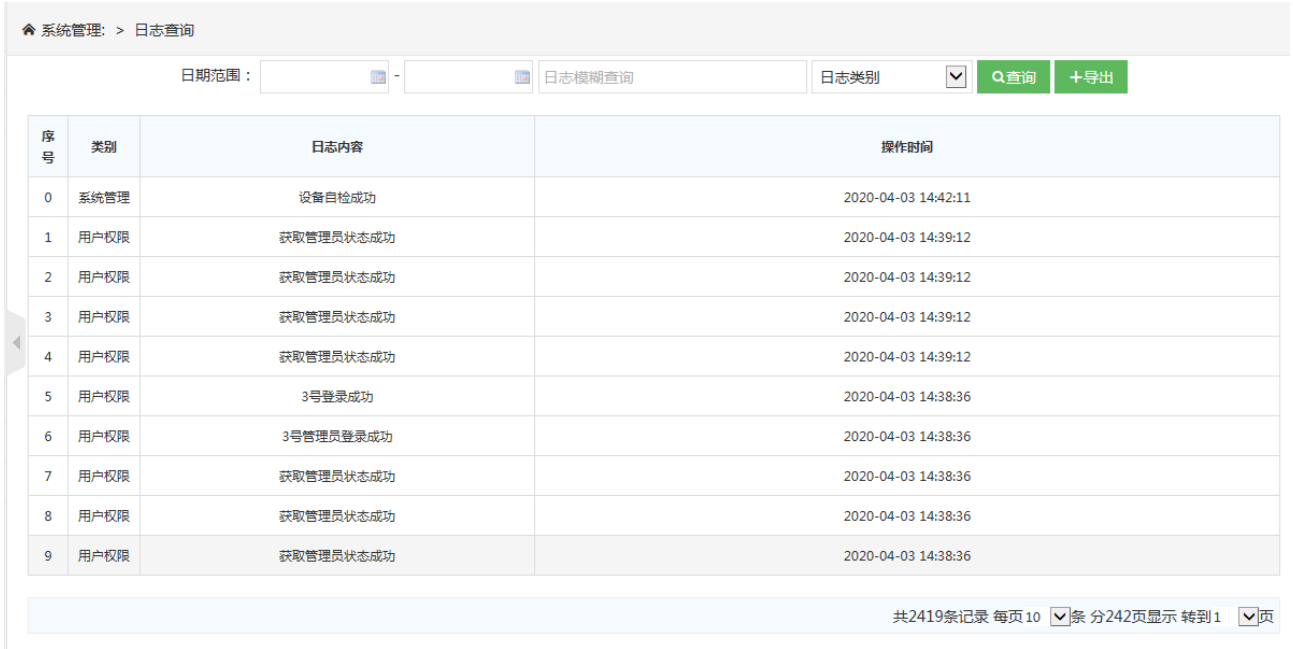


图 4-7 查看日志

同时，可以根据查询条件，如按日期范围或者日志类别进行查询你所需要的日志，如下图所示：

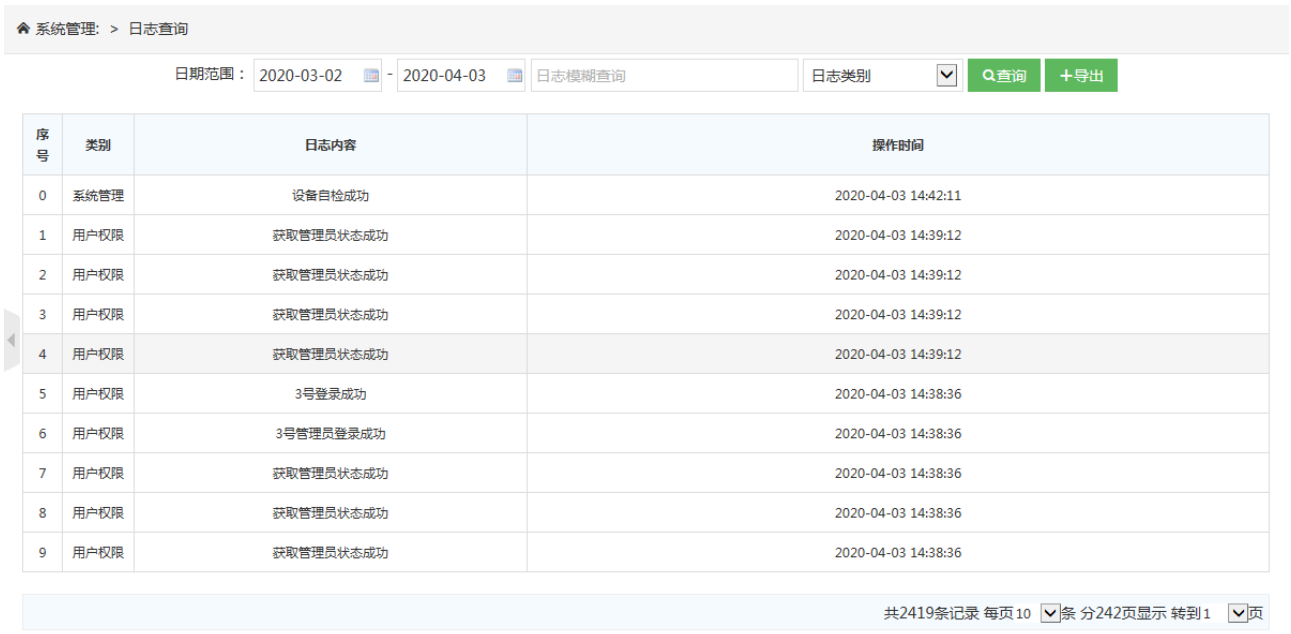


图 4-8 按时间查询日志

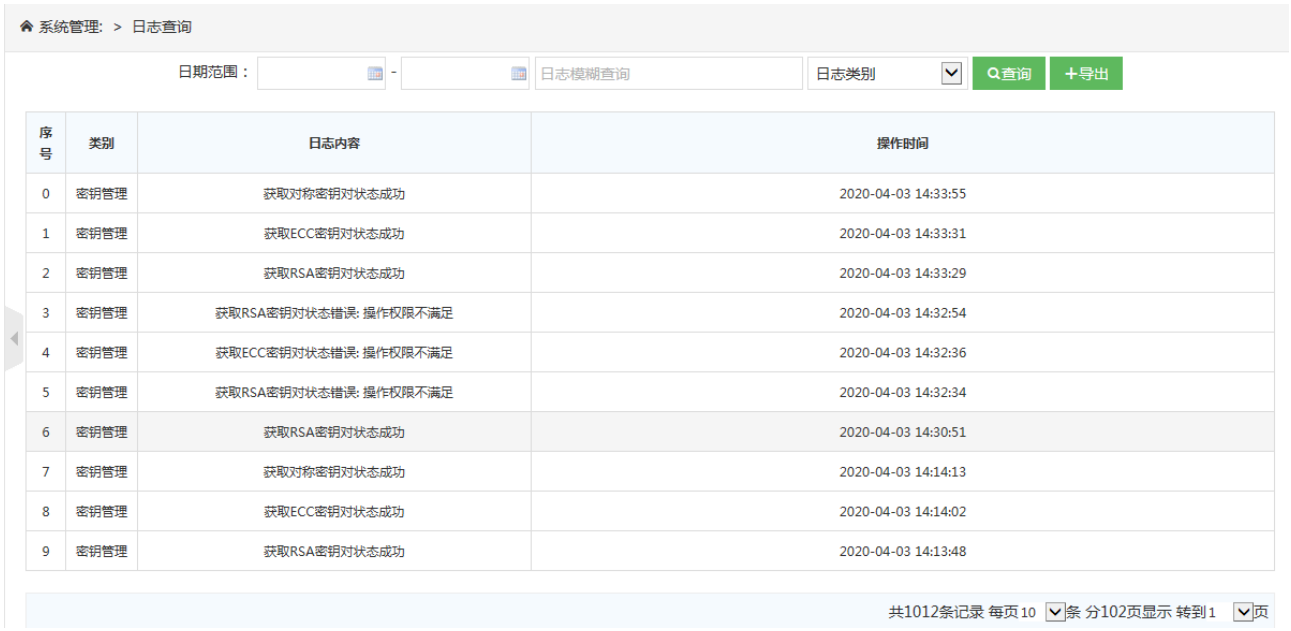


图 4-9 按日志类别查询日志

查询出来的日志，还可以通过点击“导出”按钮，保存到本地计算机上。

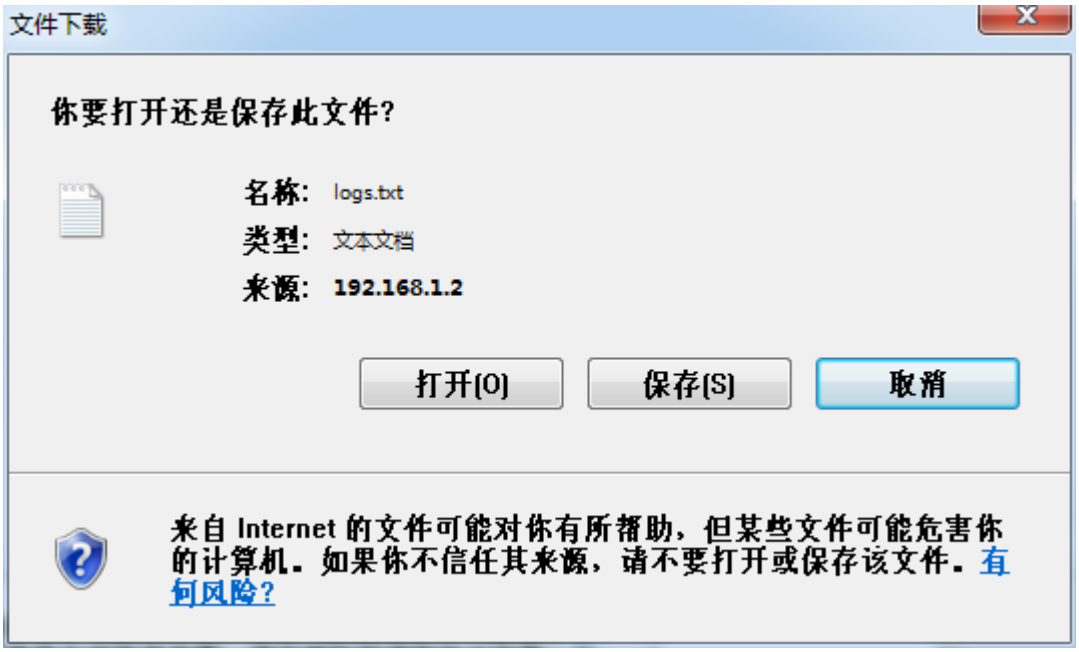


图 4-10 保存导出的日志

5. 权限管理

5.1. 用户管理

5.1.1 增加管理员

a) 选择“权限管理”中的“用户管理”功能。

图 5-1 用户管理功能

b)按照正确的方向插入管理员 USBKey，点击“添加”按钮。

c)输入 USBKey 保护口令（PIN），才能获得对 USBKey 的访问权限。

d)输入正确的口令后，点击“增加管理员”按钮，就可以成功完成增加管理员功能。

图 5-2 增加管理员

5.1.2 删除管理员

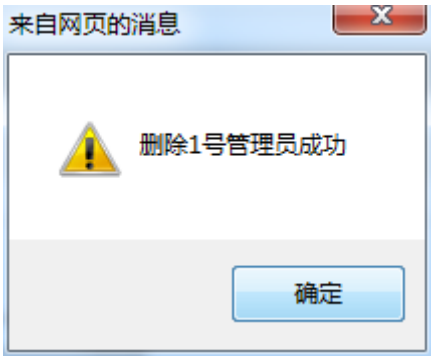


图 5-3 删除管理员

获得超级管理员权限后，在“用户管理”中，点击对应管理员后面的“删除”按钮即可删除。

注：当某张管理员卡丢失或者认为其安全性存在隐患时，可通过“删除管理员”或“添加管理员”功能更新管理员的状态。

5.1.3 增加操作员

a) 选择“操作员管理”中的“增加操作员”功能。

b)按照正确的的方向插入操作员 USBKey。

c)输入 USBKey 保护口令（PIN），才能获得对 USBKey 的访问权限。

d) 输入正确的口令后，点击“确定”按钮，即可完成新增操作员功能。

图 5-4 增加操作员

5.1.4 删除操作员

点击“删除操作员”按钮，删除当前所有的操作员。

图 5-5 删除操作员

5.2. 修改 USBKey 口令

a) 按照正确的方向插入管理员或者操作员 USBkey，输入 USBKey 原保护口令。

b) 输入新口令。

c) 再次输入新口令，点击“修改口令”按钮，完成口令修改。

图 5-6 修改 USBKey 口令

5.3. 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。

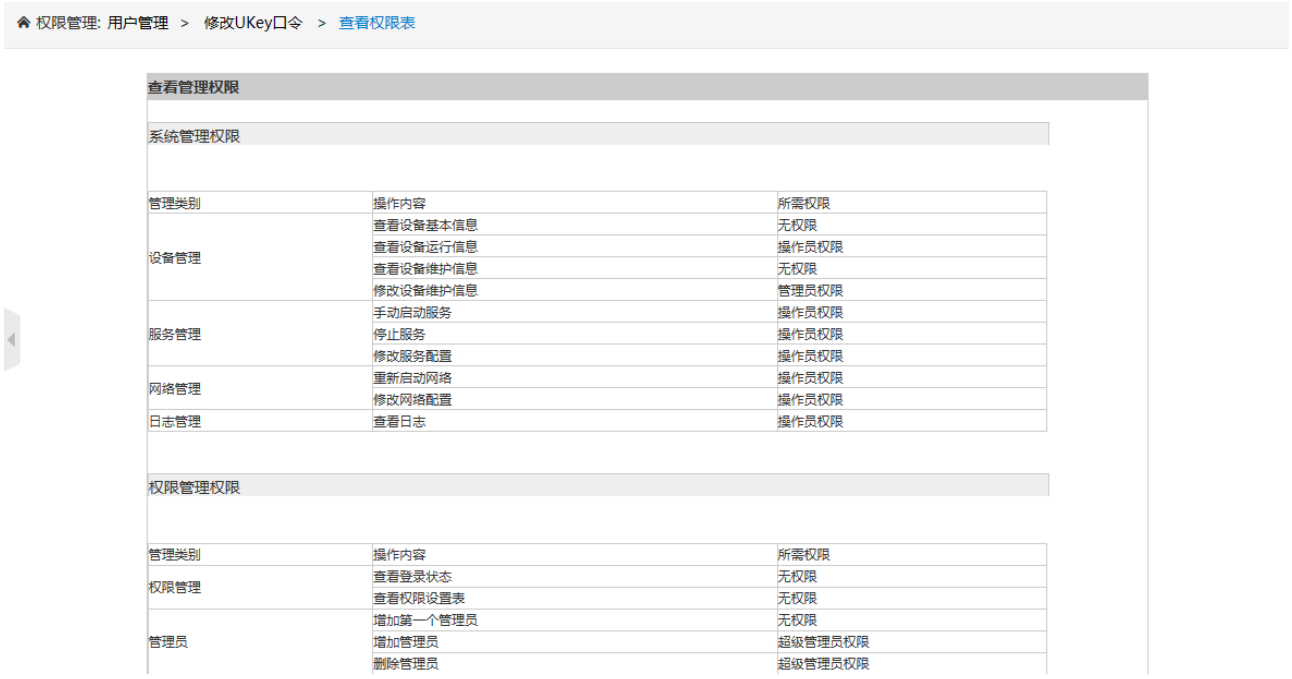


图 5-7 权限表查看

6. 密钥管理

6.1. RSA 密钥管理

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者保护会话密钥的安全。

6.1.1 产生 RSA 密钥对

具体的产生步骤如下：

a)根据提示的密钥索引范围，指定密钥位置；

b)选择密钥用途：签名密钥、加密密钥、签名密钥和加密密钥；

c)RSA 密钥的模长(bits)：1024、2048；

d)点击“生成密钥对”按钮，生成的密钥对将会被设备保护密钥加密后保存到密钥存储区。

图 6-1 指定密钥索引位置、密钥用途、密钥模长

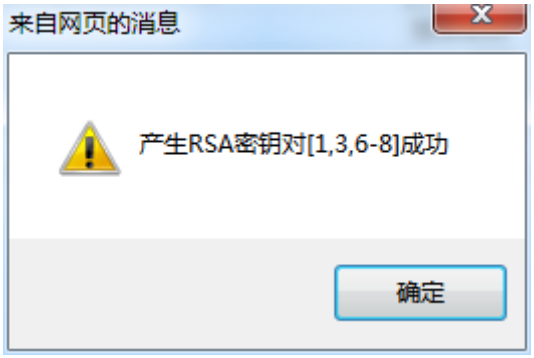
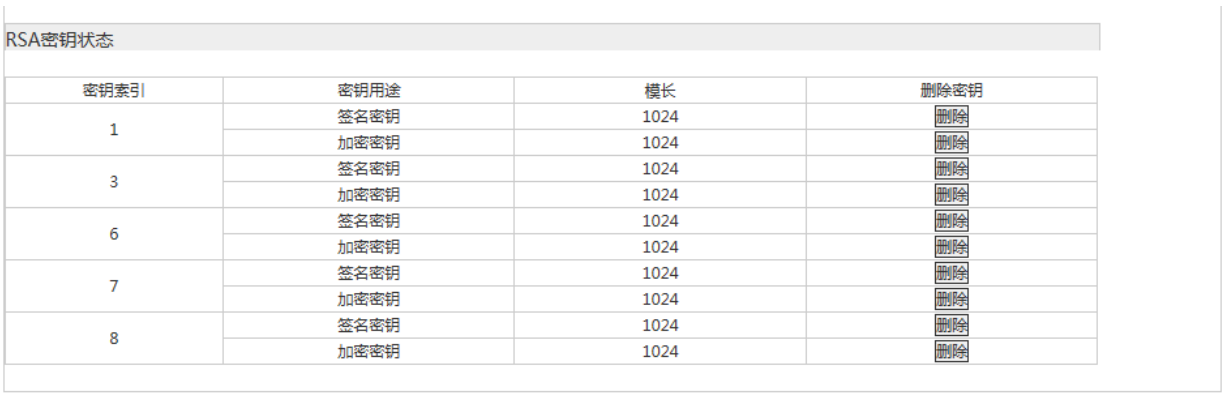


图 6-2 成功生成 RSA 密钥对



密钥索引	密钥用途	模长	删除密钥
1	签名密钥	1024	删除
	加密密钥	1024	删除
3	签名密钥	1024	删除
	加密密钥	1024	删除
6	签名密钥	1024	删除
	加密密钥	1024	删除
7	签名密钥	1024	删除
	加密密钥	1024	删除
8	签名密钥	1024	删除
	加密密钥	1024	删除

图 6-3 生成的 RSA 密钥对状态

6.1.2 删除密钥对

删除指定密钥索引位置的 RSA 密钥对，弹出删除对话框，点击“确定”完成删除操作。

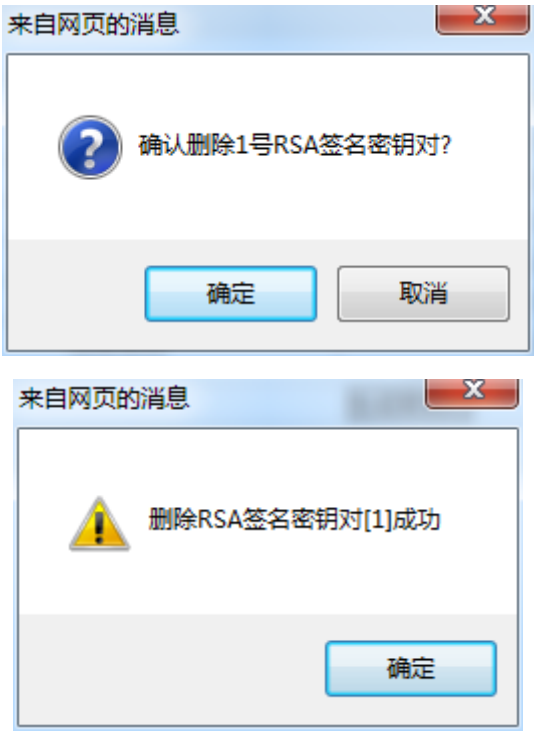


图 6-4 删除 RSA 密钥对

6.2. ECC 密钥管理

支持双密钥体制，每个索引位置对应两对 ECC 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。

6.2.1 产生 ECC 密钥对

具体的产生步骤如下：

a) 根据提示的密钥索引范围，指定密钥位置；

b) 选择密钥用途，也可以选择仅产生签名密钥对或加密密钥对；

c) 点击“生成密钥对”按钮，生成的密钥对将会被设备保护密钥加密后保存到密钥存储区。

图 6-5 指定密钥索引、密钥用途、密钥模长

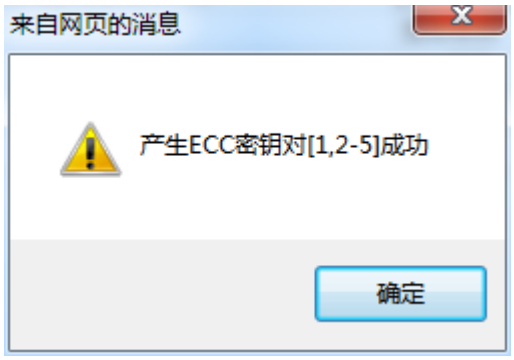
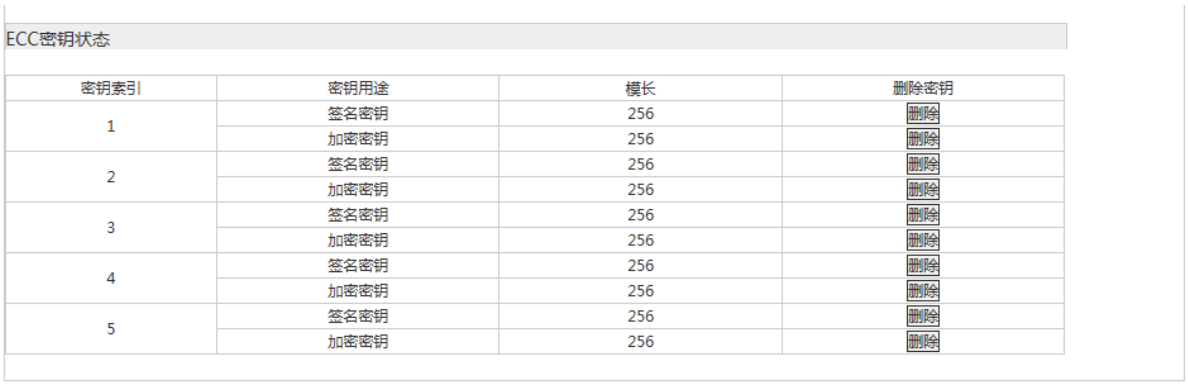


图 6-6 成功生成 ECC 密钥对



密钥索引	密钥用途	模长	删除密钥
1	签名密钥	256	删除
	加密密钥	256	删除
2	签名密钥	256	删除
	加密密钥	256	删除
3	签名密钥	256	删除
	加密密钥	256	删除
4	签名密钥	256	删除
	加密密钥	256	删除
5	签名密钥	256	删除
	加密密钥	256	删除

图 6-7 ECC 密钥对状态

6.2.2 删除 ECC 密钥对

删除指定密钥索引位置的 ECC 密钥对，弹出删除对话框，点击“确定”完成删除操作。

图 6-8 删除 ECC 密钥对

6.3. 对称密钥管理

6.3.1 产生对称密钥

a）输入要产生的对称密钥索引；

b）选择密钥长度（bits）：128、192、256；

c）产生密钥后将会被设备保护密钥加密后保存到密钥存储区。

图 6-9 指定密钥索引、密钥长度

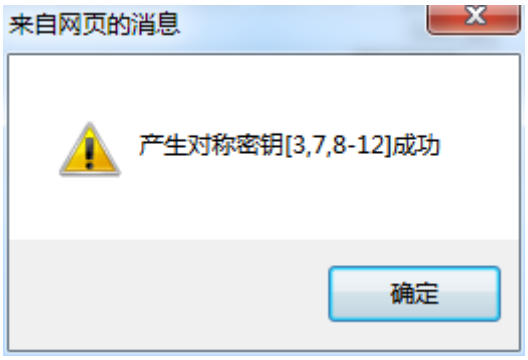


图 6-10 成功生成对称密钥

对称密钥状态

密钥索引	密钥长度	密钥删除
3	128	删除
7	128	删除
8	128	删除
9	128	删除
10	128	删除
11	128	删除
12	128	删除

图 6-11 对称密钥状态

6.3.2 导入对称密钥

输入密钥索引，然后输入十六进制的对称密钥，单击“导入密钥”按钮即可。

导入对称密钥

请输入密钥索引,密钥索引范围(1~100)	8
请输入十六进制的对称密钥(密钥长度为8的倍数且最长为32个字节)，例如：00010203	0001020304050607
导入密钥	

图 6-12 对称密钥导入

6.3.3 删除对称密钥

根据提示，删除过期或者废除的对称密钥。

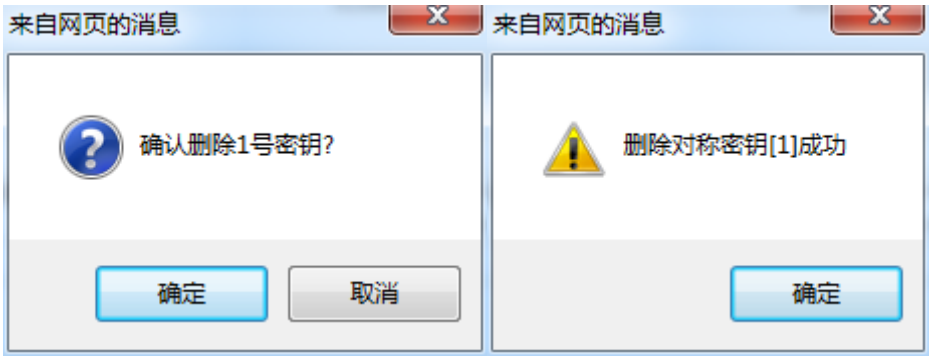


图 6-13 删除对称密钥

6.4 销毁密钥

该功能能销毁服务器密码机设备内的所有密钥以及用户信息。

图 6-14 销毁密钥

7. 服务管理

7.1. 查看服务状态

用户可以查看服务的当前运行情况，包括并发数及内存使用率。

图 7-1 设备服务状态

7.2. 修改服务配置

查看或修改服务的配置参数。修改步骤如下：

a)选择需要修改的项目，然后输入需要修改的值。

b)完成参数修改后，保存修改后的配置。

c)重启服务器密码机，修改生效。

图 7-2 修改服务配置

7.3. 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，用于进一步控制客户机的访问权限。

a)输入要授权的 IP 地址，点击“添加”按钮，即可把此 IP 地址添加到白名单中，可以合法的访问密码服务。

b)选择指定的 IP 序号，点击“删除”按钮即可从白名单中删除。

图 7-3 白名单管理

<!>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。

<!>重要提示：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。

7.4. 启动/停止服务

如果还未启动服务，可以选择“启动密码服务”。插入操作员 USBKey，单击“启动密码服务”即可。

图 7-4 启动密码服务

如果服务已启动，可以按选择进行以下操作：

1. 立即停止服务：立即终止当前服务的所有进程。

2. 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。

图 7-5 启动/停止服务

8. 备份恢复

8.1. 备份密钥

运行密钥备份向导，产生备份密钥并分割导出，然后对密钥的敏感信息通过该密钥加密保存到文件中。在将备份文件从服务器密码机下载到本地妥善保存。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 个管理员 USBKey。

图 8-1 备份密钥

b) 依次输出 3 个备份密钥分量，该过程需要依次插入 3 个管理员 USBKey 并输入 PIN 口令。

图 8-2 输出备份密钥分量[1]

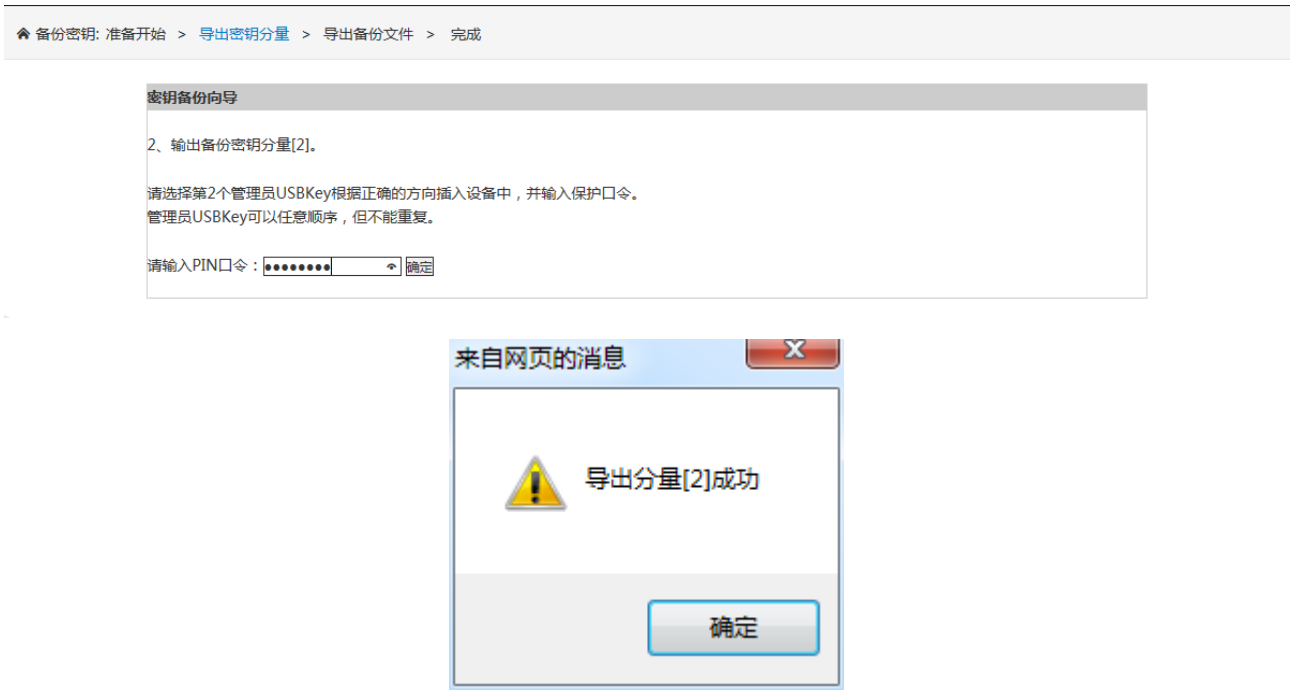


图 8-3 输出备份密钥分量[2]

图 8-4 输出备份密钥分量[3]

c)将密钥等数据使用备份密钥进行加密，并备份到文件中。右键点击“下载密钥备份文件[szlxsmbak.dat]”链接，选择“目标另存为...”，下载到本地并妥善保存。

图 8-5 导出备份文件

d)完成密钥备份。

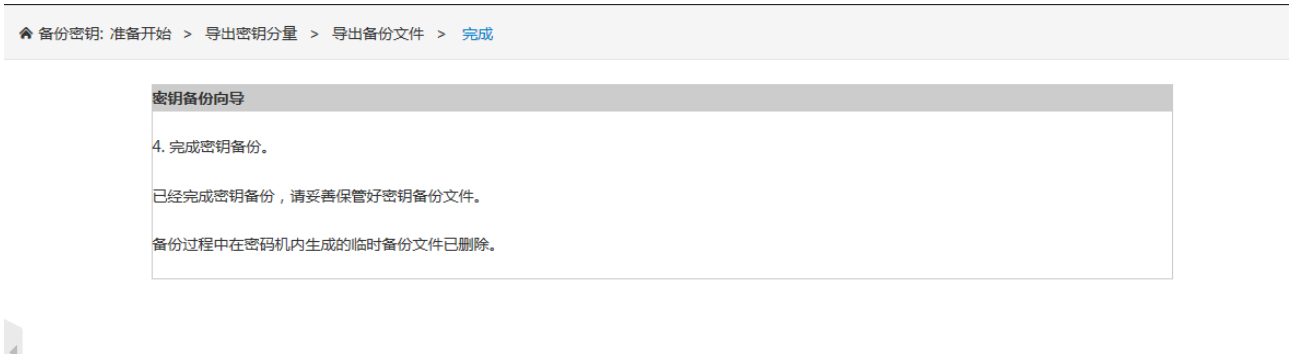


图 8-6 完成密钥备份

注意：文件导出保存时，建议不要修改备份文件的文件名，恢复密钥上传时保持现在的文件名，否则恢复密钥失败。

8.2. 恢复密钥

运行恢复向导，将保存在管理员 USBKey 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。

图 8-7 密钥恢复准备

b)选择之前密钥备份过程中生产的密钥备份文件，并点击[上传]按钮。

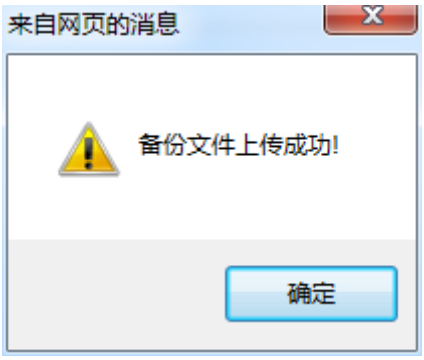


图 8-8 上传备份文件

c)依次导入任意 2 个备份密钥分量，该过程需要插入 2 个管理员 USBKey 并输入 PIN 口令。

图 8-9 导入备份密钥分量[1]

图 8-10 导入备份密钥分量[2]

d) 密钥恢复向导将依次恢复备份文件中保存的信息。

图 8-11 完成密钥恢复

注：恢复密钥过程会破坏当前服务器密码机内的密钥信息，必须确认好后，在进行密钥恢复。

导入密钥备份文件时，必须保证与当时备份导出时一致。