

SJL22 系列金融数据密码机

集群系统技术白皮书



北京江南歌盟科技有限公司

二〇〇四年二月

目 录

第一章 系统概述	1
第二章 前台功能说明	2
第三章 后台功能说明	11
第四章 系统特点	13

第一章 系统概述

SJL22 系列金融数据密码机集群系统是歌盟科技目前面向银行主机加密模式所开发的一套集多机热备、负载均衡、用户管理和实时监控为一体的密码机应用平台。该系统针对本公司 SJL22 系列金融数据密码机的特点量身定做，从而大大加强了本公司密码机产品在银行应用系统中的可靠性和处理速度，同时也为银行在监控和管理密码机方面提供了前所未有的方便，从而为银行面向客户提供稳定、高效的金融服务创造了良好的基础。

SJL22 系列金融数据密码机集群系统分为前后台两个部分组成，前台为银行提供实时的监控和管理功能；后台是整套集群系统的核心部分，用于分发、传递、处理各种交易和命令请求，同时负责维护整套集群系统的正常运作。

前台监控功能通过图形化的界面向银行动态展现密码机的详细状态，如：密码机的实时状态、密码机的负载状况、密码机的流量、密码机的授权状况等等，同时也为银行提供了动态操作后台集群系统的接口，使得银行操作人员在应对紧急情况的时候能够拥有更大的灵活性，就整套前台监控系统所提供的功能而言，国内目前同类产品中尚属首创。

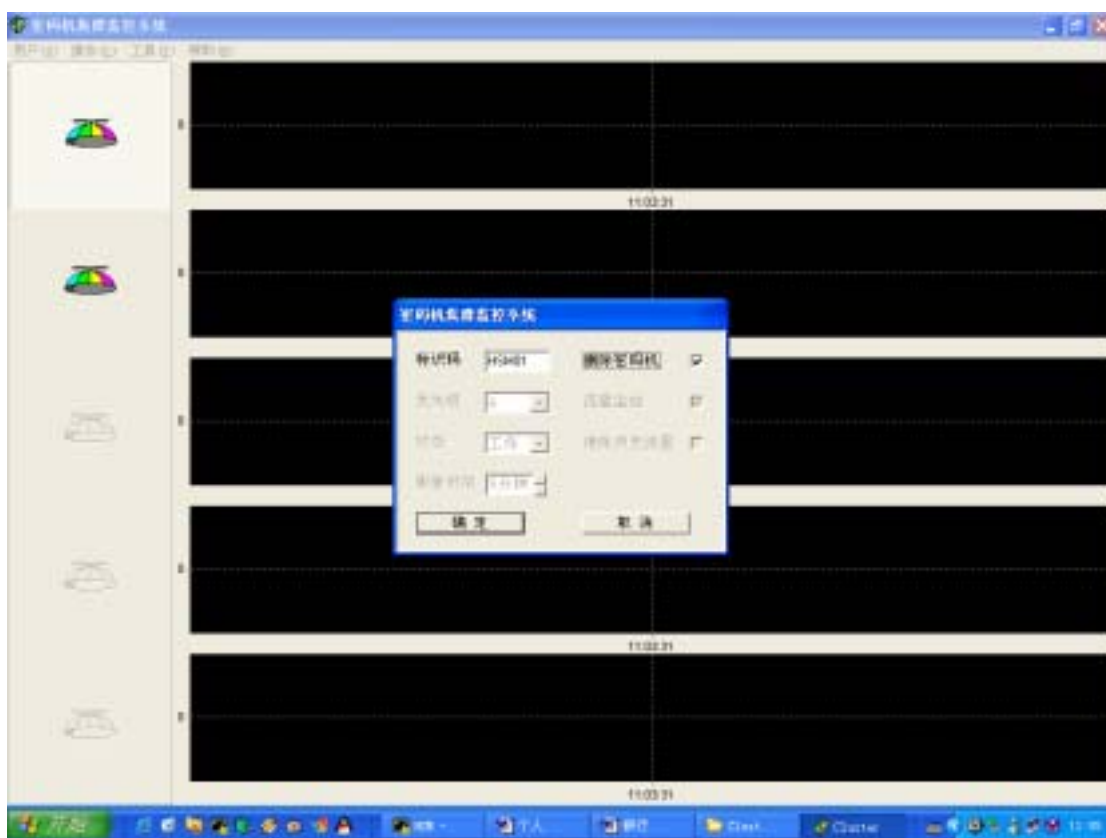
后台核心部分基于 Unix 系统自身提供的通讯机制和竞争模式，对所有处于集群系统模式的密码机进行了统一管理和监控，同时可以将所有监控的信息通过监控 Server 传递给前台的监控端。后台核心部分的另一主要功能是确保处于集群模式的密码机高效的工作，充分发挥负载均衡优势，并保证密码机的热备切换。

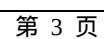
第二章 前台功能说明

1. 动态操作密码机

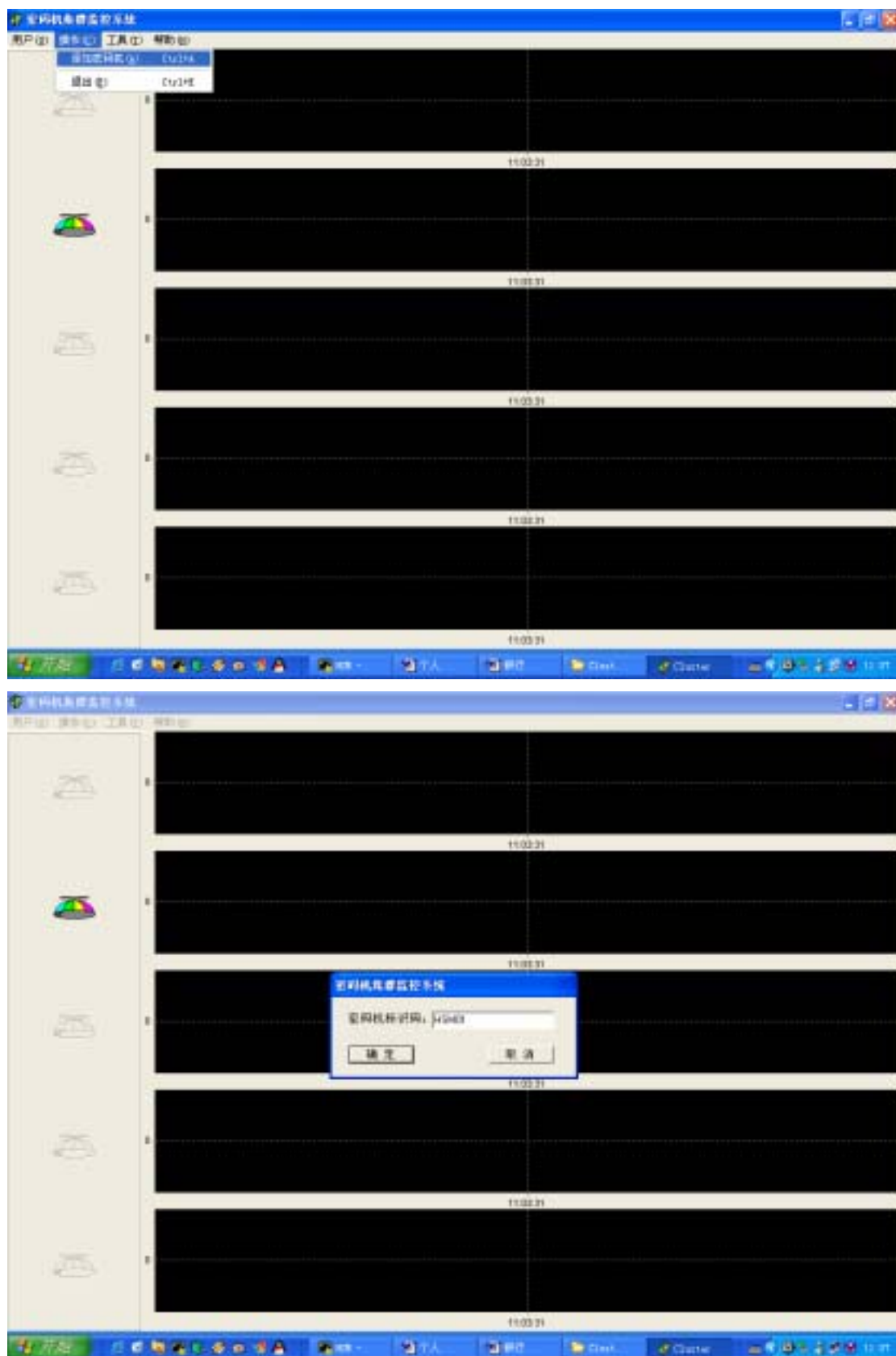
本系统最大的一个特点在于摒弃了传统密码机的静态操作模式，采用全动态模式进行处理。本集群系统无需任何附加手段，从根本实现原理上吻合了银行 7*24 不间断的模式。

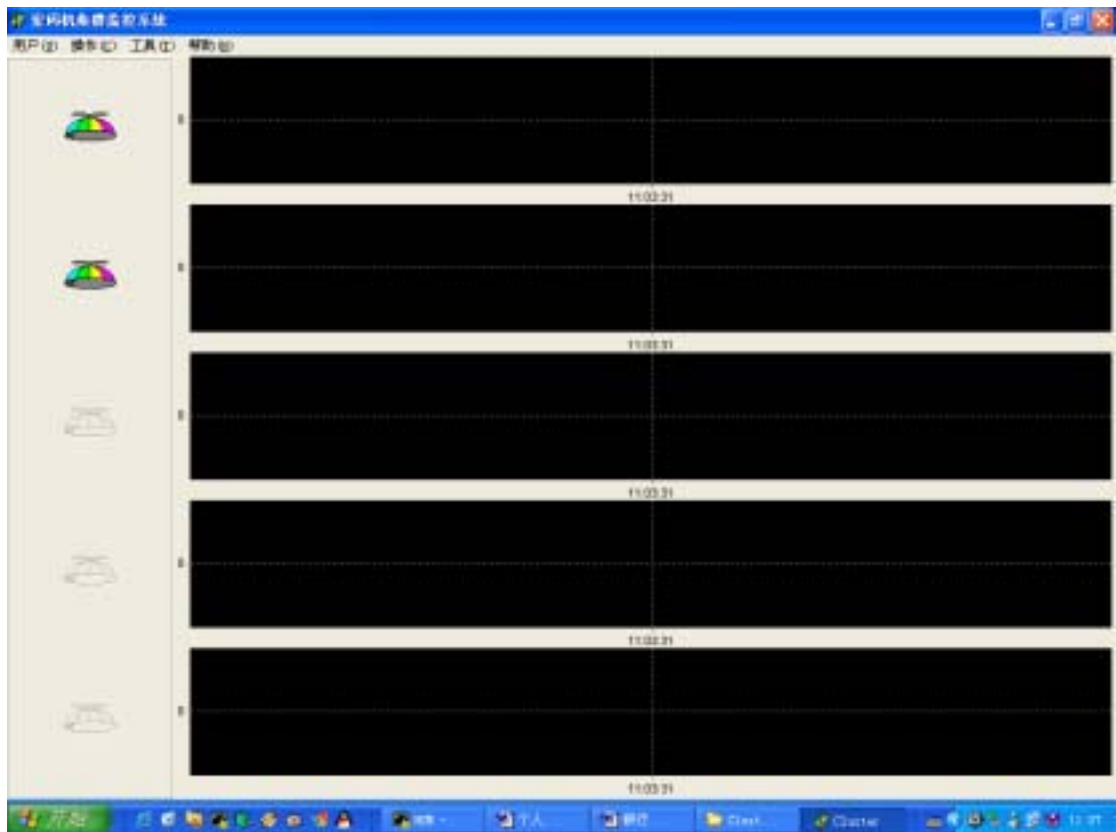
动态删除密码机



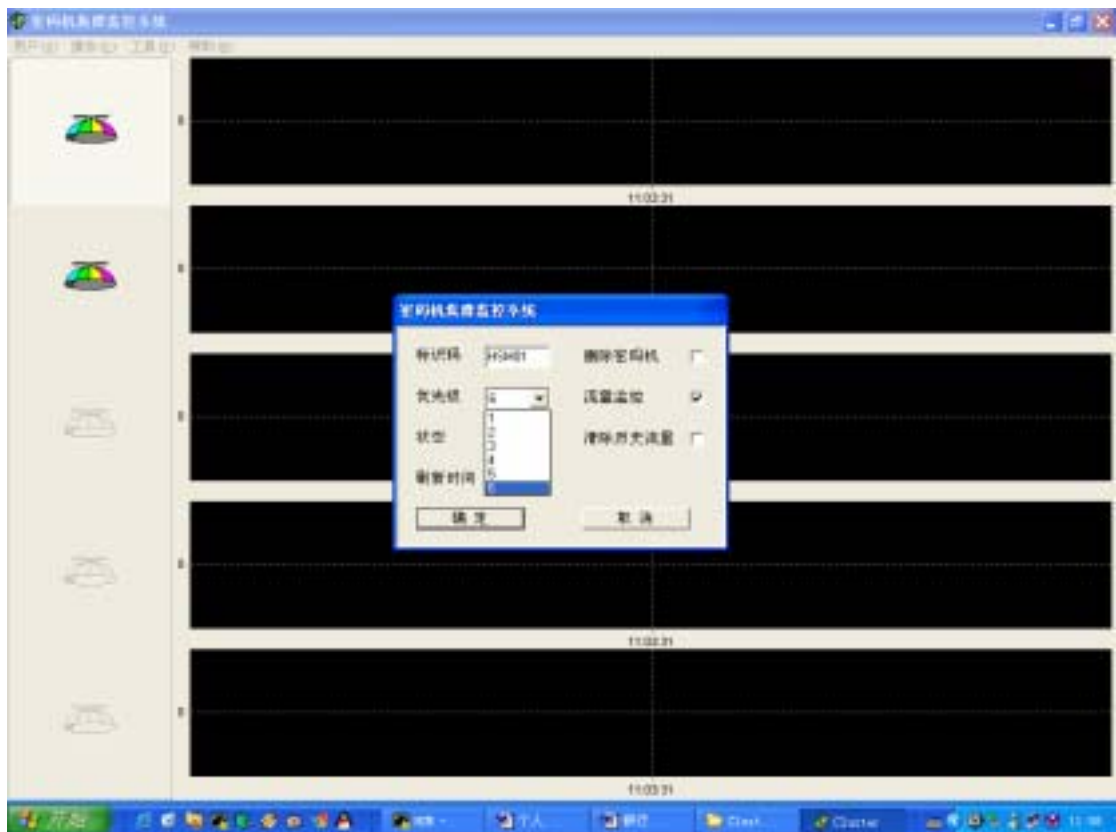


动态增加密码机

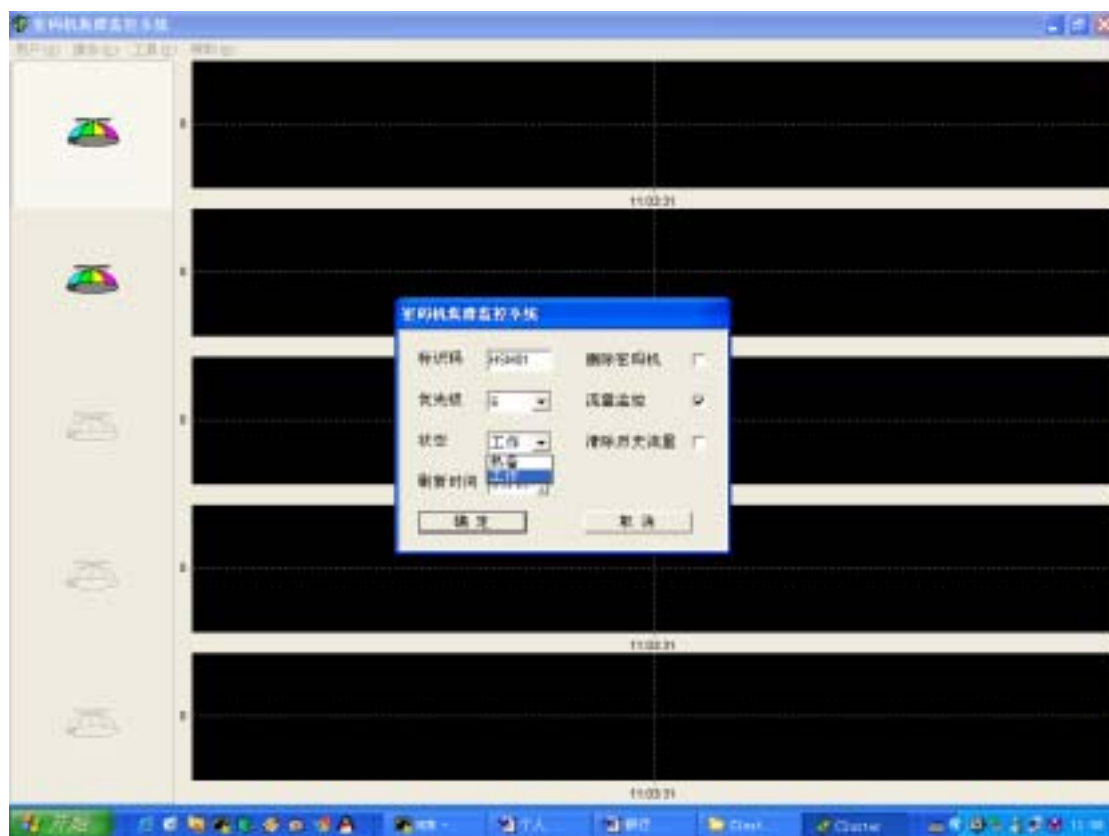




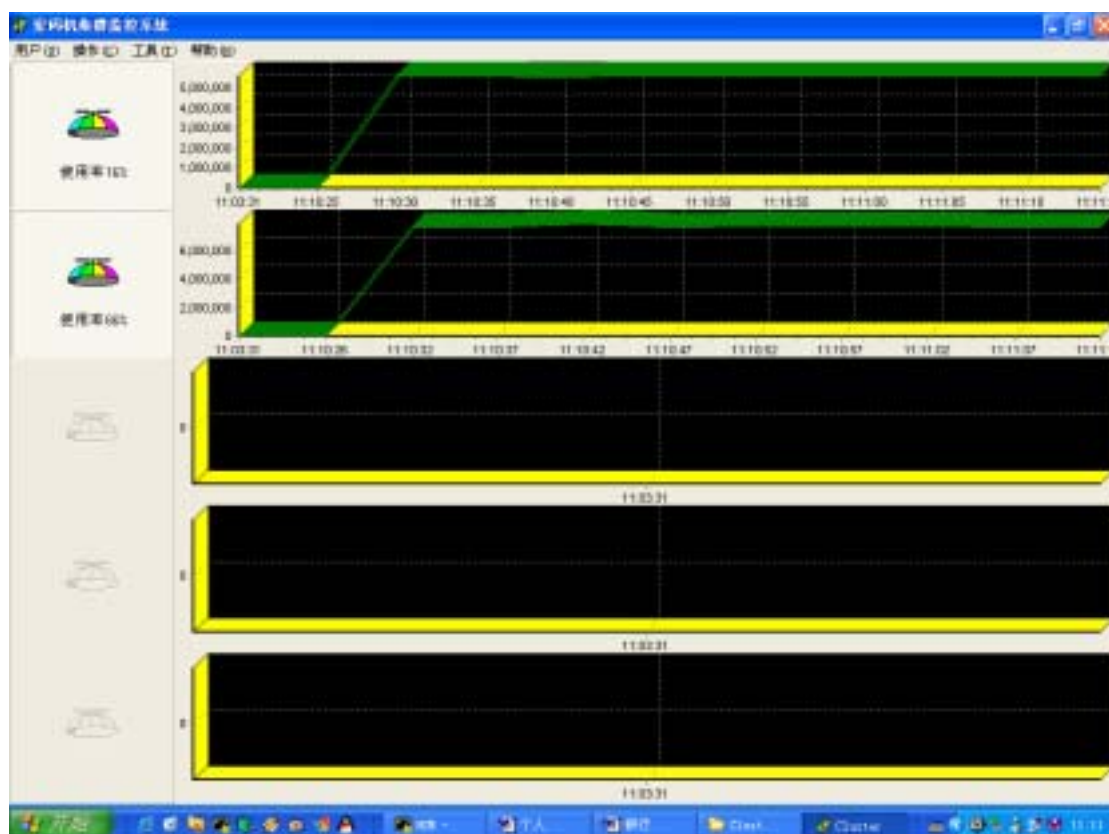
动态修改密码机优先级

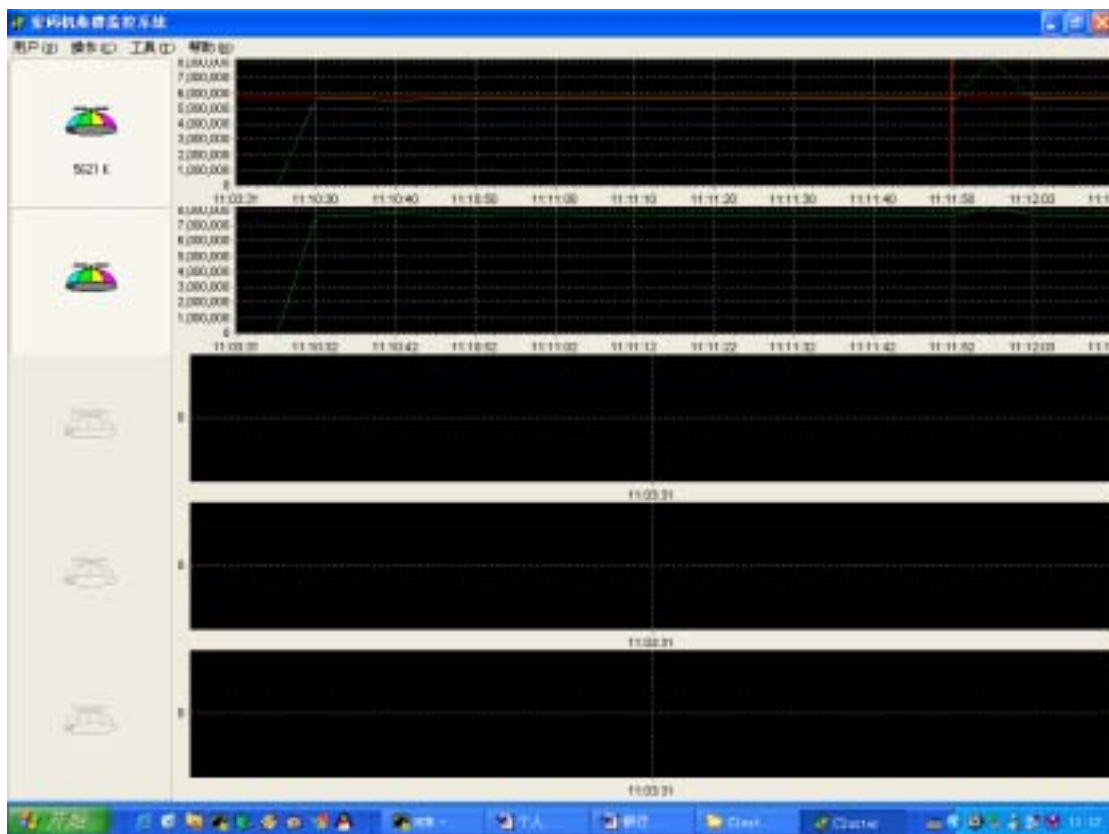


动态修改密码机状态

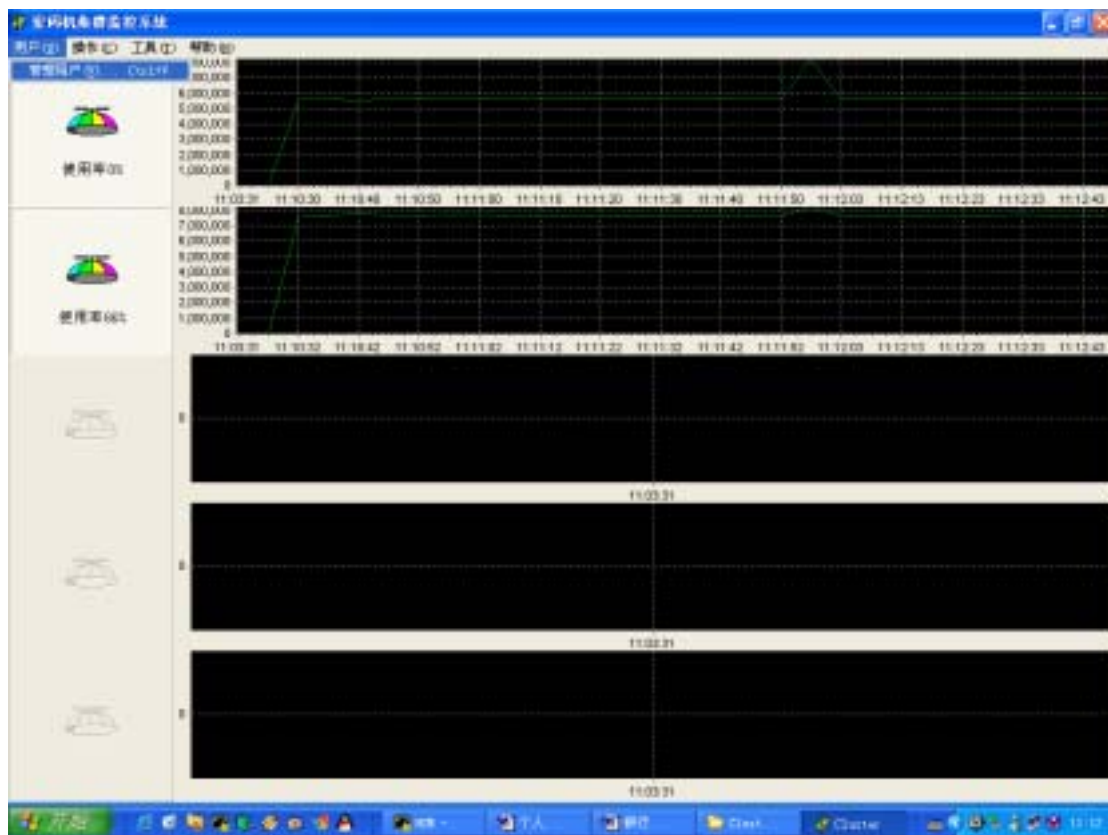


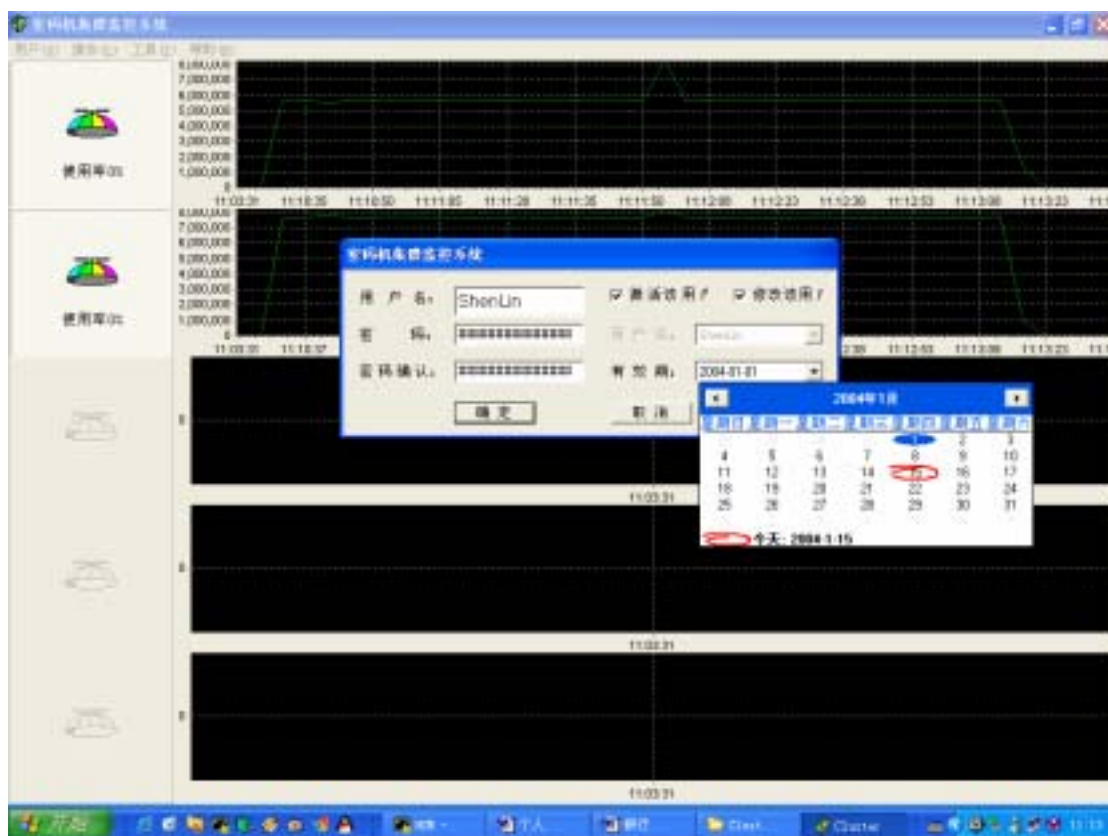
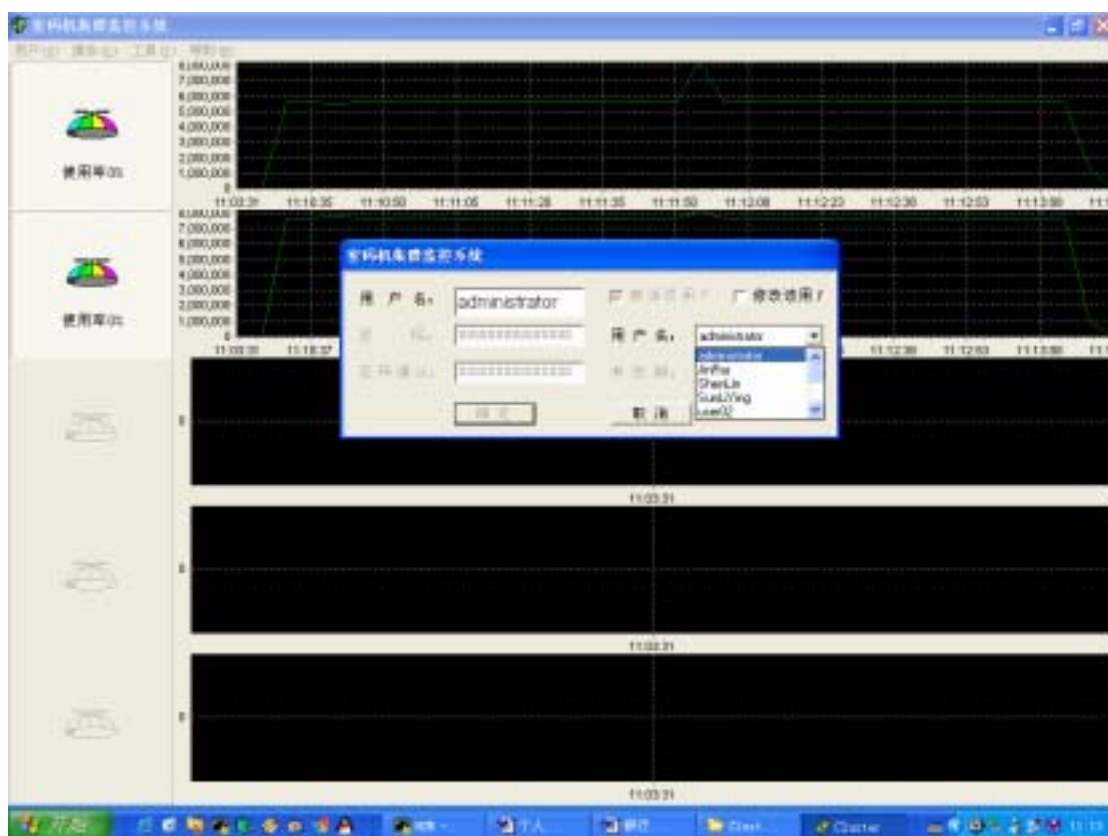
2. 动态监控密码机



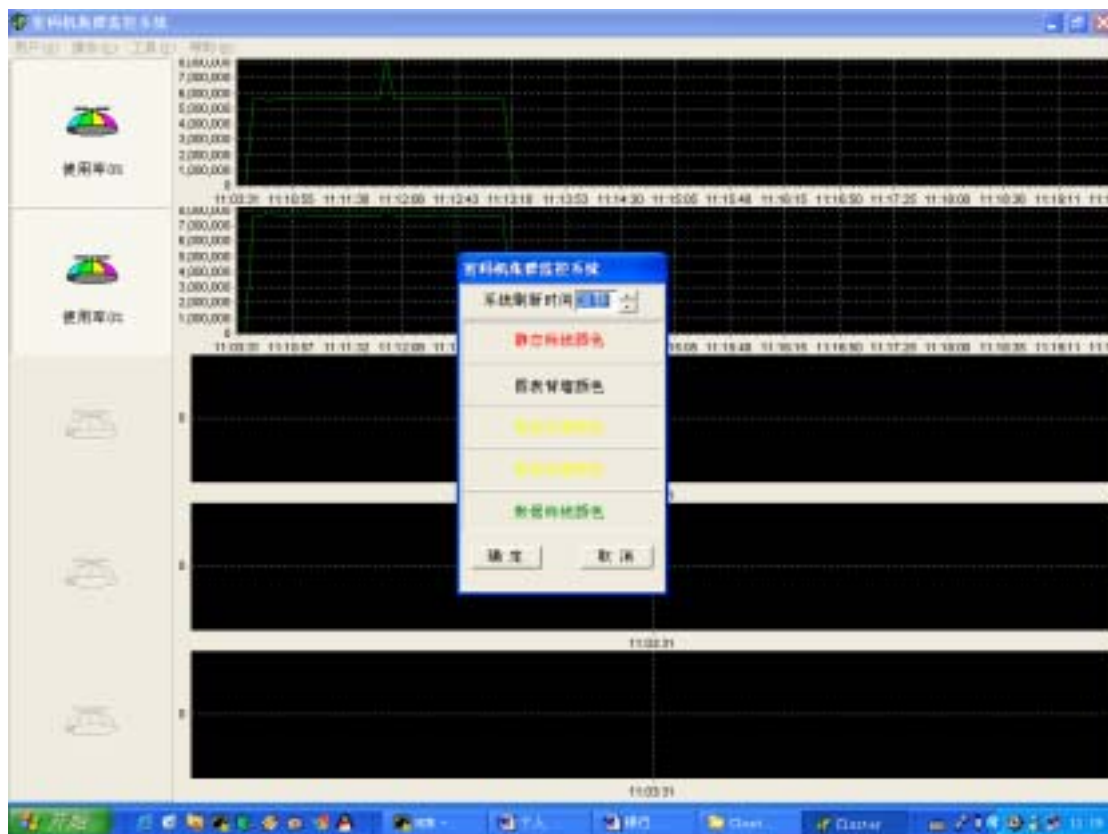
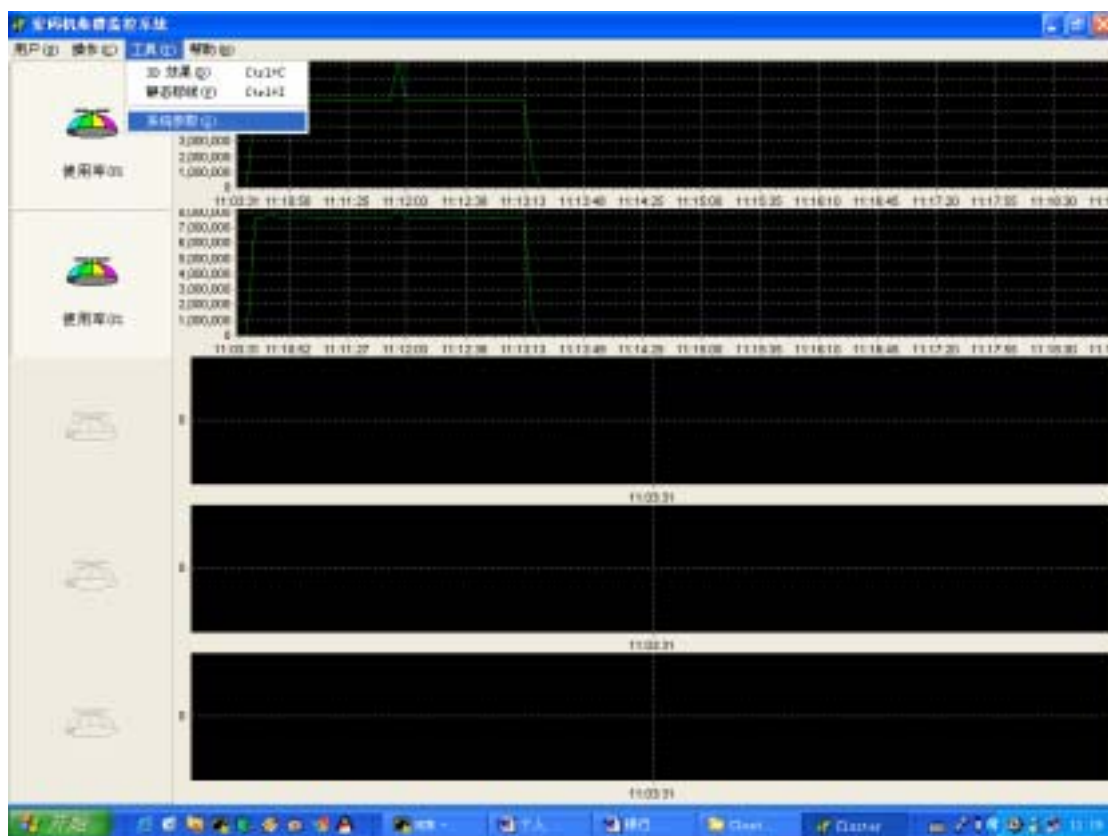


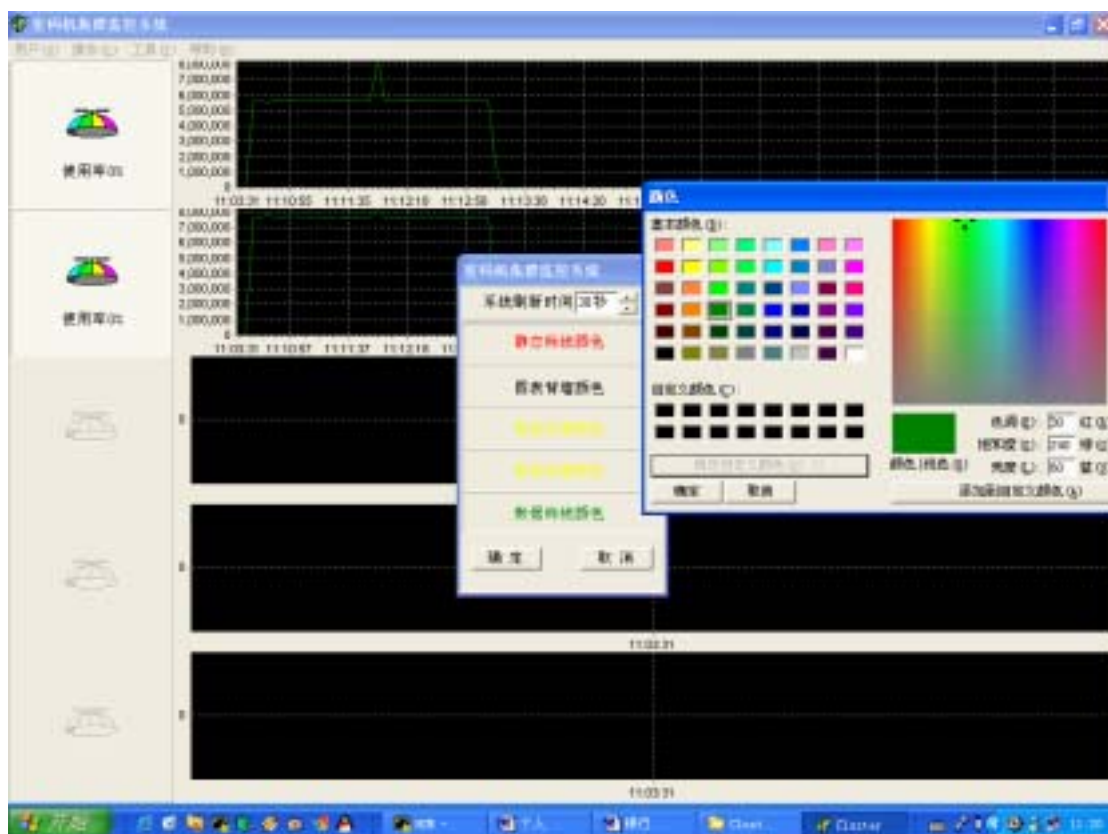
3. 动态用户管理





4. 系统参数调整





第三章 后台功能说明

本系统不仅在前台提供了操作界面，并且在后台也提供了相应的命令行操作，从而使银行的监控人员有更灵活的操作方式，后台对于密码机的操作仍然是全动态的，并可以在集群系统启动前静态的修改配置文件，来实现密码机属性的永久更改。

动态加入一台密码机

AddHsm 192.168.1.102 9010 HSM02

动态删除一台密码机

DelHsm 192.168.1.102 9010 HSM01

动态修改一台密码机的状态

ModifyHsm 192.168.1.102 9010 HSM02 0

ModifyHsm 192.168.1.102 9010 HSM02 3

修改为状态 0，表示进入工作状态，3 表示热备状态

动态修改一台密码机的优先级

ModifyPri 192.168.1.102 9010 HSM04 4

修改为优先级 4，优先级必须大于 0，且不能大于集群系统的最大支持标准

动态获取一台密码机的流量、负载、IP、端口、优先级

GetLoad 192.168.1.102 9010 HSM01

动态获取所有密码机的状态、集群允许最大优先级、集群支持的最大密码机数

GetState 192.168.1.102 9010

动态获取一台密码机的状态

GetState 192.168.1.102 9010 HSM01

动态获取当前集群中所有密码机的配置（序列号、版本号、主密钥校验值等）

GetAuth 192.168.1.102 9010

动态获取一台密码机的配置

GetAuth 192.168.1.102 9010 HSM01

启动集群系统

StartCluster [-c]

-c 表示只启动主控台，没有参数表示监控（如果有监控子系统的话）和主控全部启动

停止集群系统

StopCluster [-m]

-m 表示只停止监控，没有参数表示全部停止

清除制定的交易队列

ClearQ 192.168.1.102 9010 Req

ClearQ 192.168.1.102 9010 Resp

Req 表示交易请求队列，Resp 表示交易响应队列

读取集群系统信号灯值

ReadSem

读取集群系统内存状态

ReadShm

第四章 系统特点

1. 灵活性

歌盟科技密码机集群系统，具有很高的灵活性。

首先，集群系统的监控功能是可选插件（不在标准软件配置中）。银行客户可以根据自身的需要来选择是否需要监控功能，且无论客户是否定制了监控功能，集群系统都可以脱离监控单独运行。

其次，集群系统采用配置文件的方式来订制每台密码机的特定参数，且每台密码机拥有自己的配置文件，同时系统采用独立的主控配置文件和监控配置文件来决定密码机的启用和关闭以及监控的启用和关闭，这就保证了密码机的配置与集群系统的运行相对分离的灵活状态。

2. 透明性

首先，集群系统对客户完全透明，用户只需要使用集群系统自带的 API 函数即可完成与密码机的所有操作，无需关心通讯底层的任何操作，同时集群系统采用进程间通讯模式，因此用户无需关心长短连接和资源释放的问题；

其次，集群系统面向歌盟科技密码机完全透明，用户无需关心密码机的升级换代或体系更新问题。对于银行应用而言，集群系统对本公司密码机的优化和支持与密码机体系无关，客户调用的 API 也不会有任何更改，可以实现本公司密码机在客户系统端的无缝升级和移植。

3. 可用性

集群系统具有很高的可用性。

首先，提供了前台（Windows）图形化操作界面，为客户监控集群系统中的每台密码机的状态、负载、流量、授权等数据提供了横向和纵向的比较；

其次，系统在后台（Unix）提供了集群系统配套的工具包，可以动态的对集群系统中的密码机进行状态切换、查询、添加、删除、更改优先级、修改探测指令等操作，并提供针对查看集群系统本身资源和交易队列清空的工具（该功能为定制功能，不在标准软件配置中）。

4. 针对性

本套集群系统具有较强的针对性。

首先，根据歌盟科技的密码机的通讯和运算特点进行了全面优化处理，从而提高了本公司密码机的效率和稳定性，并对歌盟科技的密码机自动进行一致性校验和授权的动态最追踪；

其次，对于银行客户常用的统计手段（如 流量统计、负载统计）和应用系统（如前置系统）特点，也作了针对性的优化和设计，从而使得本套集群系统可以与银行任何常见的应用系统进行对接。系统自带完整的流水机制，该机制可以以文件方式记录完整交易过程，并通过集群自带的流水号生成功能保证密码机端交易的唯一性。

5. 通用性

本套集群系统在开发过程中，充分考虑到各家银行使用的现有加密机的状况，因此，在针对歌盟科技密码机优化版的基础上，又开发了通用版，可以适用各银行目前正在使用的绝大多数类型的加密机，通用版除了保留了负载均衡和多机热备的功能，并且提供了全面的监控功能和一致性校验功能，从而大大提高银行现有密码机应用的可靠性和安全性。

6. 安全性

考虑到密码机在银行系统中的重要性和 Windows 操作系统安全性相对较弱的实际情况，本套集群系统对安全部分作了专门的设计和處理。

首先，本套集群系统的前台监控部分采用了用户权限分级审查的方式，集群系统无论前后台都不保存密码明文，密码验证和存储采用与 Unix 登录类似的方法。用户存储使用独立的用戶文件，无论前台客户端或后台核心部分是否升级，只要用户的配置存储文件不变，那么当初建立的用户相关属性也不变，除非管理员手工修改。用户文件采用随机淹没的方式，没有任何明文出现。

其次，所有前后台交互通讯的报文，其格式都经过特殊定制和验证，对于非法连接的伪客户端和中途对报文的篡改具有较强的免疫力。

7. 扩展性

本集群系统采用插件似的功能定制方法，集群系统扩展性很强。

首先，集群系统可以根据客户要求随时方便的添加相应实用功能，而不影响系统的效率和稳定性。系统所有功能的实现，均采用消息指令模式，这就保证了集群系统升级后的完全向下兼容，目前消息指令有：定时类、触发类、命令行类、传输类和通知类五大类消息模式。

其次，集群系统通过核心部分的完善控制和基于 Unix 系统级的通讯保障，可以为客户实现多种外挂子系统的组合，如目前版本所提供可选子系统——监控子系统。同时集群系统所支持的密码机数量和每台密码机的数据通道也都具有很强的扩展性，本公司可以根据银行客户户交易量和交易类别的不同为机群设定不同的优化选项，从而为用户提供最佳的集群系统。（标准配置为支持 5 台密码机，每台密码机最多可以有 6 个数据通道）

8. 稳定性

由于歌盟科技密码机集群系统采用了二次探测、心跳轮寻，软切换通知等多种热备手段，因此比传统的密码机多机热备具有明显的可靠性优势。

首先，对于故障密码机集群系统具有一定的恢复能力，如果配备了监控子系统，密码机的所有切换动作和最新状态还会以图形化的方式反馈给密码机维护人员。

其次，集群系统充分发挥了多台密码机协调备份的优势，可以允许多台密码机同时故障，同时切换的要求，并且通过二次探测等恢复机制，可以将恢复后的故障机，自动带入热备状态，从而为银行业务系统稳定运行提供了更多的保证。

9. 高效性

本集群系统由于采用了负载均衡、通讯缓冲和读取竞争机制，因此有效的整合了集群系统中的各台密码机，从而提高了整体的处理性能。集群系统对比单台密码机或简单的双机热备功能的密码机组具有明显的抗压优势，可以在不影响处理效率的前提下，允许应用系统提交更大的并发请求和数据量，并且可以通过密码机优先级的调控，来合理分配待处理的任务，保证多台密码机的分摊处理。

10. 标准性

集群系统核心部分对于运算和处理要求较高，因此采用标准 C 程序编写，可以适应银行任何常见 UNIX 平台的移植，同时也保证了处理的高效性。前台监控部分为 Delphi6.0 开发，适用于 Win95（含 Win95）以上的任何服务器和个人桌面系统。前后台通讯，采用标准 TCP/IP 协议；核心进程间通讯和协调，采用标准的 System V IPC 通讯及 POSIX 标准的全双工管道通讯及信号机制。