北京江南歌盟科技有限公司

SJL22 金融数据密码机系列产品介绍

SJL22 金融数据密码机系列产品，除满足当今国际/国内银行界磁 条卡/存折以及将来国际 IC 卡（符合 EMV2000 规范）业务的安全需求外，还完全与国际主流的 RACAL(THALES)加密体系兼容（密钥管理体系和主机命令体系），符合国际金融行业的安全规范，是国内成功应用于金融业 EMV2000 迁移的唯一产品。内嵌国内金卡、IC 卡应用体系、网上银行应用体系、PKI 应用体系及 EMV 96/2000 标准应用体系可与 RACAL（THALES）应用体系同时运行，加上多通讯协议可并行工作，因此，一台 SJL22 金融数据密码机具备的功能相当于同行业其它厂商多台密码机具备的功能。SJL22 金融数据密码机系列产品，采用无风扇无机械部件低功耗绿色技术设计思想，使整机稳定性、可靠性大大增强。

本公司永远保持不断发展、完善和提高自己的产品的理念，持之以恒地追求同行业领先的技术优势，给我们的用户永远提供一流技术的产品。欢迎热衷于本产品的用户来电来函和我公司联系。

SJL22 金融数据密码机系列产品目前支持的具体功能如下：

一、SJL22 金融数据密码机系列产品技术特点

1、密码算法

- 国家专用算法（SSF33/SSF10/SCB2）与经国家批准使用并兼容国际加密规范的算法（DES/3DES/AES）可并行处理，其中国家专用算法 SSF33/SSF10 与国际兼容算法 DES/3DES/AES 之间可相互转换。
- 数据加密算法符合 ANSI X3.92–1981 标准
- 三重数据加密算法：操作模式符合 ANSI X9.52–1998 标准
- 数据加密算法，操作模式符合 ANSI X3.106-1983 标准
- 密钥管理符合 ANSI X9.17 金融机构密钥管理（批处理）标准以及 ANSI X9.24-2002(零售)标准
- 采用物理噪音生成真随机数，伪随机数生成算法符合 ANSI X 9.17/ANSI X9.31 标准
- 公开密钥算法采用 RSA；数字签名算法使用 SHA-1，SHA-224，SHA-256，SHA-384，SHA-512，MD2，MD4，MD5，RIPE-MD128，RIPE-MD160，RIPE-MD256，RIPE-MD320，ISO-10118-2 等算法
- HMAC 算法支持 HMAC-SHA-1，HMAC-SHA-224，HMAC-SHA-256，

HMAC-SHA-384，HMAC-SHA-512，HMAC-MD2，HMAC-MD4，HMAC-MD5，HMAC-RIPE-MD128 ， HMAC-RIPE-MD160 ， HMAC-RIPE-MD256 ，HMAC-RIPE-MD320，HMAC-ISO-10118-2 等算法

2、密钥管理机制

- 密码机内共保存有 50 组本地主密钥，支持 192Bits 长度本地主密钥。
- 主密钥的生成过程中，密码机不保存任何密钥成份和安全参数，使得密码机更为安全可靠；密码机不允许导出主密钥或其成份，解决了密码机的安全隐患；
- 主密钥的存储采用完整性校验以及硬件冗余机制，以保证主密钥的一致性
- 支持密码机更换本地主密钥时密文数据的转换功能
- RACAL 测试密钥下的高度兼容性方便用户应用开发中的调试
- ZMK 密钥长度 64/128 bits 可配置
- 支持 ZMK 的安全转换机制
- 支持 ANSI X9.17 加密方式下，密钥安全导入导出机制
- ZMK/TMK，ZPK/TPK，ZAK/TAK，ZEK/TEK 长度支持 64/128/192 bits
- 支持本地主密钥变种、TDEA 变种机制；ZMK/TMK 支持 Atalla 单字节以及双字节变种加密
- 采用哑终端密钥管理模式，终端通讯参数可配置，**密钥管理和联机交易**可并行处理；支持中文（本地语言）和英文（国际语言）两种操作界面，可动态选择两种语言中的任一种*
- 支持不同长度的密鈅分割及成份打印
- 支持敏感数据及密钥以索引模式（S/D/T 三种模式）存储于用户存储区中或密钥存储区中
- 支持 VISA Chip Card 专用命令
- 支持 DUKPT（Derived Unique Key Per Transaction）派生每交易唯一密钥机制

3、PIN 、MAC 及 CVV 的生成及验证

- PIN 长度 4～12 可配置
- 支持国际卡业务通用的 IBM 3624 PIN 加密/验证算法
- 支持 ANSI X9.8，ISO 95641 DP1/Format 0/1/2/3，IBM/Diebold ATM，Doctel ATM，PLUS network 等 7 种 PIN 加密算法
- PIN BLOCK 支持长度 64/128/192Bits 的加密密钥

- 可根据用户特殊需求扩充专用 PIN 加密算法*
- 支持 VISA PVV/CVV 及 MasterCard CVC 生成及验证
- 支持 American Express CSCK 专用命令，防止磁条卡的非法复制
- 支持单长度密钥（64 bits）的 ANSI X9.9 及双长度密钥（128Bits）的 ANSI X9.19 MAC 算法，支持多种 MAC 生成验证方式

4、传输加密功能

- 提供应用系统报文加密传输的功能，支持 DEA/TDEA 的多种加密模式（ECB CBC CFB OFB），灵活的实现了不同格式（“Binary”或“Expanded Hex”）的大数据块报文，以密文的方式在两个通讯的节点之间进行安全传输。

5、数据安全存储功能

- 提供应用系统数据安全存储的需要，支持 DEA/TDEA 的多种加密模式（ECB CBC CFB OFB），灵活的实现了的大数据块的报文，以密文的方式在某个本地主密钥组 LMK 下（DEK——Data Encryption Key）或某个本地主密钥组 LMK 加密的数据密钥 DSK 下（Data Storage Key——数据存储加密密钥）下加密存储。

6、打印功能

- 支持密码信函、密码申请信函及密钥信函打印功能，串行端口通讯参数和通讯格式可配置（支持通讯速率 300~115200bps，支持 7N1，7O1，7E1，8N1，8O1 及 8E1 等多种通讯格式）
- 支持中文密钥及密码信函打印功能，支持 AS/400、ES/9000 环境的 IBM cp1386-1388 字符集中文字符(简体中文扩充 GBK 规范)打印功能*
- 支持 HP 兼容的激光条形码打印功能
- 标准配置：串行端口和并行端口（注：打印时使用串口或并口可配置）*

7、主机接口

- 支持 TCP/IP 协议，10/100M 自适应
- 具备跨网段使用时网关设置功能*
- 具备客户端访问密码机的 IP 地址过滤和 MAC 绑定功能*
- TCP 套接字连接数量可配置，最大 4096 个连接*
- 主机接口可扩充串口，支持异步协议及 RACAL 透明异步协议（支持通讯速率 300~115200bps，支持 7N1，7O1，7E1，8N1，8O1 及 8E1 等多种通讯格式）

——可通过管理程序配置*

- 具备独立的密钥管理端口、主机端口、打印端口，支持多种通讯协议并行工作（最多可同时支持 TCP/IP，Async 等两种通讯协议）*

8、稳定性及安全性：

- 系统研发基于高稳定性的、优化的专用操作平台，运行极其稳定
- 硬件设计符合 FIPS 140-2 LEVEL 3 标准，具有高安全性.
- 常规和警戒两种工作状态，提高了密码机的安全等级。在警戒工作状态下，任何试图对密码机的侵害都会启动物理障碍装置自动销毁密码机内保存的密钥（Tamper-Resistant Mechanism）；如：密码机打开机箱会自动清除保存于其内的密钥。
- 联机/脱机、授权/双重授权、警戒工作模式便于密码机的安全维护和密钥管理，加强了密码机的安全管理措施
- 关键联机命令及密钥导入/导出/转换等管理命令需在授权状态下处理，提供授权配置功能
- 双重控制下可选择的 IC 授权卡和口令字授权两种机制，使得密码机的使用和日常管理更为安全灵活
- 物理双重保护机制保证密码防刺探、防辐射
- 用户可自行个性化 IC 卡，具有丰富的卡片管理功能。支持的卡片包括主密钥成份卡、密钥成份卡、授权卡、密钥存储卡、测试密钥卡、维护管理卡及升级卡（厂家专用）

9、RSA 相关功能

- 产生 RSA 公私钥对，模长介于 192~2048Bits 之间连续可变
- 支持全部标准 RACAL（THALES）RSA 指令集，如 ES、EY 指令等
- 支持全部标准 EMV2000 发卡指令集
- 支持多种填充标准，如 PKCS1，OAEP，PSS，ANSI X9.31，EMV 2000 等数据填充模式
- 支持无符号及有符号整型两种公私钥 DER 编码
- 支持强素数的生成和基于强素数的公私钥生成
- 支持 CRT 模式运算
- 摘要算法支持 SHA-1，SHA-224，SHA-256，SHA-384，SHA-512，MD2，MD4，

MD5，RIPE-MD128，RIPE-MD160，RIPE-MD256，RIPE-MD320，ISO-10118-2 等算法

- 支持对数据进行 RSA 签名及验证
- 支持对数据进行 RSA 加解密运算
- 支持公私钥对，PKCS8 格式公私钥对以索引的方式导入、导出密码机
- 支持明/密文成份方式（如：p，q 两个成份，n，p 两个成份及 n，q 两个成份等）的 RSA 密钥对导入
- 支持 DEA 密钥的分散、数据完整性验证及应用密文的生成及验证等
- 以 1024Bits 模长为标准，性能指标如下（高端机型）：

  1) 产生公私钥对：3.5对/秒
  2) 签名： 180次/秒
  3) 验证： 2700次/秒

- **支持 DataCard、NBS 及 G & D EMV2000 卡个人化系统安全需求**

10、其它功能

- 支持 RACAL 报文头处理功能，最大长度 255 字节（0*～255）
- 支持 RACAL 报文尾处理功能（可选），最大长度 128 字节
- ASCII、EBCDIC 及 IBM1388 三种字符集可配置
- ***支持多字符集下 MAC 处理及报文加密的二进制方式处理模式***
- 支持多应用安全体系并行工作。目前密码机可同时支持金卡应用体系、RACAL（THALES）体系、IC 卡应用安全体系、金卡应用安全体系、网上银行安全体系、PKI 应用安全体系及 EMV 96/2000 标准安全体系。
- **支持香港网上银行，JETCO（银通），EPSCO（八达通），ATM 安全应用要求**
- IC 卡应用安全体系下可支持不同厂商的专用密钥母卡导入
- 可按客户应用需求快速提供 RACAL（THALES）主机命令及国内体系命令的复合命令*
- 低功耗、无辐射、无噪音，符合绿色环保要求

二、SJL22 金融数据密码机系列产品

SJL22 金融数据密码机高端产品

该机型分专用型和通用型两种产品，专用型适合多密码算法环境。适用于商业银行总行数据中心，银联总部数据中心以及各行业总部数据中心要求高处理性能和多密码算法等环境。

SJL22 高端(专用型)产品外形

SJL22 高端(通用型)产品外形

1、接口规范：

接口方式：RJ-45 & RS-232
最大传输速率：TCP/IP10M/100M 自适应； 异步为 115,200 bps
MTBF：≥ 30,000 小时

2、电器特性：

工作电压：100~230V
工作电流：1~0.5A
频率：50~60 Hz
功耗：最大 50W

3、物理特性：

专用型
实际尺寸：450 mm × 430 mm × 88 mm
通用型
实际尺寸：450 mm × 430 mm × 68 mm
包装尺寸：632 mm×572 mm×240 mm

重量：8 Kg
颜色：标准颜色，Black C
外壳结构：重工业钢

4、环境参数：

工作温度：0℃~50℃
存储温度：-40℃~60℃
相对湿度：5%~90% 非凝结

SJL22 金融数据密码机中端产品

该机型适用于商业银行省级分行数据中心，银联分支机构数据中心以及各行业分支机构要求中等处理性能和通用密码算法等环境。

SJL22 中端产品外形

1、 接口规范：

接口方式：RJ-45 & RS-232
最大传输速率：TCP/IP10M/100M 自适应；异步为 115,200 bps
MTBT：≥ 30,000 小时

2、电器特性：

工作电压：100~230V
工作电流：0.8~0.3A
频率：50 ~ 60 Hz
功耗：最大 35W

3、物理特性：

实际尺寸：365 mm × 430 mm × 68 mm
包装尺寸：632 mm×572 mm×240 mm
重量：8 Kg
颜色：标准颜色，Black C

外壳结构：重工业钢

4、环境参数：

工作温度：0℃~50℃
存储温度：-40℃~60℃
相对湿度：5%~90% 非凝结

SJL22 金融数据密码机低端（网点型）产品

该机型适用于商业银行储蓄所、网点，商场等要求低处理性能和通用密码算法等环境。

SJL22 低端（网点型）产品外形

1、接口规范：

接口方式：RJ-45
最大传输速率：TCP/IP10M/100M 自适应
MTBF：≥ 30,000 小时

2、电器特性：

工作电压：100~230V
工作电流：0.3~0.1A
频率：50~60 Hz
功耗：最大 15W

3、物理特性：

实际尺寸：345 mm × 215 mm × 68 mm
包装尺寸：430 mm×310 mm×200 mm
重量：4 Kg
颜色：标准颜色，White & Black
外壳结构：重工业钢

4、环境参数：

工作温度：0℃~50℃
存储温度：-40℃~60℃
相对湿度：5%~90% 非凝结

三、SJL22 金融数据密码机系列产品主要性能指标

测试项目	数据长度	进程数	性能（笔/秒）		
	字节		高端机	中端机	网点型
PVV		4	>7000	>4500	>900
DES PIN 转换		4	>7000	>4000	>800
3DES PIN 转换（Two Key）		4	>5000	>2800	>600
MAC（ANSI X9.9）	128	4	>9000	>6000	>1100
MAC（ANSI X9.9）	256	4	>8000	>5200	>1000
MAC（ANSI X9.9）	512	4	>6400	>4000	>900
MAC（ANSI X9.19）	128	4	>7000	>4500	>900
MAC（ANSI X9.19）	256	4	>6500	>4000	>800
MAC（ANSI X9.19）	512	4	>5200	>3200	>700

遵循国际标准　　：

SJL22 金融数据密码机系列产品在体系结构设计上以及硬件平台的设计上，遵循了以下的国际金融行业的安全标准：

- ANSI X3.92–1981: Data Encryption Algorithm
  ANSI X3.92–1981：数据加密算法
- ANSI X9.52–1998: Triple Data Encryption Algorithm: Modes of Operation
  ANSI X9.52–1998：三重数据加密算法：操作模式
- ANSI X3.106-1983: Data Encryption Algorithm, Modes of Operations, 1983.
  ANSI X3.106-1983：数据加密算法，操作模式
- ANSI X9.17–1995：Financial Institution Key Management (Wholesale) standard.
  ANSI X9.17–1995：金融机构密钥管理（批处理）标准
- ANSI X 9.9 1986 Financial Institution Message Authentication
  ANSI X 9.9 1986金融机构批处理报文鉴别
- ANSI X9.19 1986 Financial Institution Retail Message Authentication
  ANSI X 9.19金融机构零售报文鉴别
- ANSI X9.24–1998: Financial Services- Key Management Using the DEA
  ANSI X9.24–1998：金融服务—使用DEA的密钥管理
- ANSI X9.24 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
  ANSI X 9.24零售银行服务对称密钥管理（第一部分）：使用对称技术
- ANSI X9.66–200x (Draft): Security Requirements for Cryptographic Modules
  ANSI X9.66–200x (草案)：密码模块的安全要求
- ANSI X9.8–1995: Personal Identification Number (PIN) Management and Security, Part 1: PIN Protection Principles and Techniques
  ANSI X9.8–1995：个人标识码（PIN）的管理和安全，第一部分：PIN保护原则和技术
- ANSI X9.8–1995: Personal Identification Number (PIN) Management and Security, Part 2: Approved Algorithms for PIN Encipherment
  ANSI X9.8–1995：个人标识码（PIN）的管理和安全，第二部分：已批准的PIN加密算法

- FIPS PUB 140–2: Security Requirements for Cryptographic Modules. 2001
  FIPS PUB 140–2：密码模块的安全要求。2001
- ISO 13491–1: 1998 Banking – Secure cryptographic devices(retail), Part 1: Concepts, requirements and evaluation
  ISO 13491–1: 1998 金融业安全密码设备（零售），第一部分：概念，要求及评估
- ISO 13491–2: 2000 Banking – Secure cryptographic devices(retail), Part 2: Security compliance checklists for devices used in magnetic stripe card systems
  ISO 13491–1: 1998 金融业安全密码设备（零售），第二部分：用于磁条卡系统中设备安全符合对照表
- SO 9564–1: 1991 Personal Identification Number Management and security, Part 1: PIN Protection Principles and Techniques
  ISO 9564–1: 1991个人标识码的管理和安全，第一部分：PIN保护原则和技术
- ISO 9564–2: 1991 Personal Identification Number Management, Part 2: Approved Algorithms for PIN Encipherment
  ISO 9564–2: 1991个人标识码的管理和安全，第二部分：已批准的PIN加密算法
- ISO 11568–2: 1994 Banking Key Management (Retail), Part 2: Key Management Techniques for Symmetric Ciphers
  ISO 11568–2: 1994 银行业密钥管理（零售），第二部分：对称密码算法密钥管理技术
- ISO 11568–3: 1994 Banking Key Management (Retail), Part 3: Key Life Cycle for Symmetric Ciphers
- ISO 11568–3: 1994 银行业密钥管理（零售），第三部分：对称密码算法密钥生命周期
- ISO 11568–6: 1998 Banking Key Management (Retail), Part 6: Key Management Schemes
  I SO 11568–6: 1998 银行业密钥管理（零售），第六部分：密钥管理方案
- ISO 11770–2: 1996 Information Technology—Security Techniques— Key Management, Part 2: Mechanisms Using Symmetric Key Management Techniques
  ISO 11770–2: 1996 信息技术——安全技术——密钥管理，第二部分：采用对称密钥管理技术机制

- 欧洲银行标准委员会 ECBS TR406 V2 [September 2001] / V3[**SEPTEMBER 2003**]——加密算法使用与密钥管理指南
- 欧洲银行标准委员会 ECBS TR405——金融系统密钥恢复
- 中国金融 IC 卡卡片规范
- 中国金融 IC 卡应用规范

四、集群系统技术特点

歌盟集群系统是用于对密码机进行管理的一种软件平台，主要的功能是很好的实现了密码机的多机热备、负载均衡、集中监控以及密钥管理，主要技术特点如下：

- 透明性

对客户来说，用户向集群系统请求服务如同访问一台密码机，现有的业务系统无需进行任何修改即可应用到集群系统所提供的更高效稳定的服务；对开发者而言，集群下密码机的升级与集群系统软件无关；

- 灵活性

集群系统采用多个独立配置文件的方式订制集群系统的属性和各密码机的特定参数；

终端监控功能是可选插件，可根据客户自身的应用需求来选择是否需要此模块功能；

- 可扩展性

集群系统可在需要的时候增加新的密码机提供效率更高的服务；

- 可用性

集群系统提供了后台的管理软件，可方便的对系统的运行进行查询和管理；另外可选在前台监控软件以图形化方式提供更直观可用的监控管理界面；

密钥管理功能使用户不须再操心密钥更新过程中的繁琐处理，只要简单方便的应用本集群所提供的密钥管理界面和接口函数即可；

- 稳定性

集群系统实现多机热备功能，保证集群下的所有密码机中，只要有任意一台能够正常工作，则银行整套业务系统都不会受到影响，业务请求将被自动切换到正常密码机上处理，并且在多机热备的自动切换中，对应用系统而言是完全透明的，且对故障密码机集群系统会实时的向监控人员报警；

- 高效性

本集群系统实现了负载均衡，保证业务系统提交的所有任务能够以最优的方式分摊到群下各密码机中进行运算处理，从而缓解对某单台密码机的运算压力和通讯压力，更高效的体现集群的整体处理高效性；

- 可移植性

本集群系统采用标准 C 语言编写，在银行内任何常见的 UNIX 平台上体现为代码级兼容，不同系统下的应用可移植性高。

五、加密卡

1、主要特点

- 提供 1024 比特或 2048 比特的 RSA 签名/验证算法；
- 提供 MD5、SHA-1 两种 HASH 算法；
- 提供经国家密码管理局批准的物理噪声源（硬件随机数发生器），产生密钥种子；
- 支持 32 位 PCI 数据总线接口；
- 实现数据加密、数字签名和数据完整性验证；
- ***采用串口或 USB 接口，可外接 IC 卡读卡器及 UKey 实现身份认证、密钥备份和分发；***
- 支持多用户、多进程，支持 512 个工作密钥同时工作
- 支持 Windows9x、Windows NT、Linux 等多种操作系统

2、性能指标

- RSA 签名/验证速率： >1000 次/秒，>3500 次/秒
- RSA 密钥生成测试 ： 7 对/秒
- 分组加密（ECB） ： 100Mbps