SJL22-SM 金融数据密码机
系列产品技术白皮书

北京江南歌盟科技有限公司

二０二０年九月

声　明

《SJL22-SM 金融数据密码机系列产品技术白皮书》第 8.0i 版。

本手册由北京江南歌盟科技有限公司编写（以下简称歌盟科技），仅赠送给用户和合作伙伴参阅。歌盟科技保留对本书的所有权和解释权，任何公司和个人未经允许，不得擅自使用、复制、修改、传播本书的内容。歌盟科技保留有对本书进行重新修订的权利，随时可能对本书中的打印错误、与最新资料不符之处、内容的更新等做必要的修改，这些不再另行通知，但全部编入新版白皮书内。

联系方式：http://www.gemen.com.cn/contact.htm

北京江南歌盟科技有限公司

二〇二〇年九月

目 录

图

表

此页无正文

1 前言

SJL22-SM 金融数据密码机系列产品是适应国内、国际金融业务安全发展趋势而设计的一种在应用级上与 RACAL（THALES）密码机兼容*并具有自身特色的*新型金融数据密码机产品。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-SM 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。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。

首先，SJL22-SM 金融数据密码机系列产品作为主机型的安全设备，提供给主机基于金融业务应用不同处理环节上的不同安全需求。国内传统的金融数据密码机在保证金融信息安全上，只是提供了保证 PIN 的私密性和报文完整性的功能，随着信息技术的飞速发展，大量的敏感数据在金融网络中的传输以及在相应业务系统数据库中的存储也需要得到安全的保障。SJL22-SM 金融数据密码机在保障金融信息安全上*不但可保证信息的私密性、完整性，还支持信息的安全存储以及安全传输。*

第二，作为金融数据加密产品密钥的安全至关重要，SJL22-SM 金融数据密码机系列产品为高安全强度的完整的TDEA三层密钥管理体系，主密钥的长度为192位，并严格遵循专钥专用的原则：支持多达 50 组长度为 192 位的主密钥集合，每组主密钥有其专用的目的；支持多样性的密钥管理机制，包括本地主密钥，密钥交换密钥、工作密钥、DUKPT 以及 PKI 体系的公、私钥。管理体系的高度安全性、灵活性，是 SJL22-SM 金融数据密码机优于传统金融数据密码机的一大特点。

第三，产品的设计严格遵循国际金融行业的安全标准和规范，可完全满足 VISA/MasterCard 国际信用卡组织向加入的各成员组织的安全要求，支持 TDES 加密。

对于如何保证国际卡（发卡和外卡收单）交易的安全，VISA/MasterCard 国

际信用卡组织向加入的各成员组织提出了如下的基本要求：

2003年1月1日以后，所有新安装的ATM（包括替换的ATM），必须支持“TDES（三重 DES）”。

2004 年 1 月 1 日以后，所有新开发的 POS PIN 接收设备（包括替换设备）必须支持“TDES”。

2003 年 6 月 1 日以后，所有支持 DES 的 POS PIN 接收设备，必须符合 VISA“TDES”的要求。

2007 年 7 月 1 日以后，所有的 ATM 应支持“TDES”。

2007 年 7 月 1 日以后，所有从支持“TDES”设备产生的交易，从发起节点至 VISA 国际信用卡组织必须采用 TDES 加密。

2010 年 7 月 1 日以后，所有的 POS PIN 接收设备应支持“TDES”。

更多相关内容请参见： *http://international.visa.com/fb/vendors/pin/*

本文主要针对银行卡业务的特点，并参照国际金融电子资金传送的有关规范与应用特点，叙述了 SJL22-SM 金融数据密码机特点、提供的功能及在银行卡网络的安全应用。目的在于有效的保证信用卡网络中信息的安全传输和正常交易，防止各种欺诈行为的发生，切实的维护银行的信誉，保障客户的利益。

2 产品设计原则及规范

2.1 设计目标

1、 SJL22-SM 金融数据密码机系列产品在体系设计上综合国内外金融密码机产品设计的全部优点，采用严格的三层密钥管理体系，支持密钥长度为 192 位高强度的多组本地主密钥集合，体现“专钥专用”的设计原则。

2、 严格遵循国际金融行业的安全标准与规范（ISO/ANSI/FIPS 以及 VISA/ECBS 等），完全与国际金融业务安全体系对接。

3、 将传统的金融数据密码机完成的两种主要功能扩充至四种功能。

- PIN 的私密性（传统功能）
- 数据传输的完整性（传统功能）
- 数据传输的安全性（扩充功能）
- 本地数据存储的安全性（扩充功能）

4、 在算法的选择上，采用***以国家专用算法（SSF33/SSF10/SCB2）为主、结合国际兼容通用算法（公开密钥算法 RSA；数字签名算法 SHA-1，SHA-224，SHA-256，SHA-384，SHA-512，MD2，MD4，MD5，RIPE-MD128， RIPE-MD160， RIPE-MD256， RIPE-MD320，ISO-10118-2 等以及相应的 HMAC 算法；对称算法 DES/TDES/AES）***的多密码算法共存，并提供算法的转换功能和机制。

5、 在硬件平台的选择上，采用可控的安全计算机平台技术，使用物理安全、访问控制安全、用户安全、安全传输和管理安全等相关技术，确保 SJL22-SM 金融数据密码机系列产品整体上的保密性、完整性和可控性。

6、 SJL22-SM 金融数据密码机系列产品的研发成功，不但能完全满足国内日益增加的国际卡业务交易的安全需求。而且还可满足国际上的金融业务安全需求，并具备适应新技术、新标准、新规范的可扩展能力。

2.2 设计思想

SJL22-SM 金融数据密码机系列产品在研发过程中，综合参考了国内外金融业务数据安全产品方面已有的先进的开发研究成果；严格遵循国际金融行业业务安全规范，引进与自主创新相结合，最终目的是形成具有国际竞争能力的、具有自主产权的国产化的金融数据安全产品（***软著登字第 033528 号，登记号：2005SR02027***）。产品的设计严格遵循以下原则：

2.2.1 先进性

产品设计立足于高起点，在技术上紧跟国际先进水平，采用先进设计思想，硬件设计中坚持采用符合时代发展的新技术、新工艺。在 SJL22-SM 金融数据密码机系列产品的设计中分别采用了：

- 选用新型、新功能集成电路芯片
- IC 卡技术
- 软件内核加密机制
- 密钥存储器容错设计机制
- 可编程物理接口协议机制
- 直流工作电压检测及自动处理
- 侵害密码自动销毁（Tamper Resistance）机制

在结构设计上采取集成工程设计思想，结构简洁合理，提高了设备的可靠性和可维护性。

2.2.2 成熟性

SJL22-SM 金融数据密码机系列产品的研发，是基于公司的技术人员多年 RACAL（THALES）密码机及部分命令兼容产品技术支持及售后服务经验、国产密码机的研发支持经验，以及对国际金融行业安全技术发展的跟踪研究、国际金融行业安全的各种规范和标准的熟知等方面的基础上开发的产品，因此，产品无论是功能上还是物理安全及稳定性、可靠性上，均在原主流产品之上。

2.2.3 规范性

SJL22-SM 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

2.2.4 高安全性

- SJL22-SM 金融数据密码机系列产品设计上充分考虑安全性问题，主密钥为多达 50 组、长度为 192 bits 的高强度密钥集合，采用“专钥专用”的密钥使用原则和严格的三层密钥管理体系；支持双长度、三长度密钥的 TDEA 加密

- 密钥管理的双重访问控制(Dual Control)机制
- 重要或敏感的终端管理操作或联机命令的调用采用授权/双重授权机制
- 双重保护技术（Dual Protection）确保密码机能够防辐射、防刺探，使得密码机物理安全性在业内达到领先水平（专利申请号：2004200880380）
- 双重授权技术（Dual Authorization），给用户对敏感操作提供了更可靠的手段
- 密码机密钥管理访问的物理安全机制（设置面板锁）
- 采用物理的侵害自动销毁密钥（Tamper Resistant）机制来保证密钥的安全；严格符合 FIPS 140-2 级别 3 的安全要求
- 物理电气接口信号的过流过压保护等多种安全保护措施，确保 SJL22-SM 金融数据密码机系列产品从体系结构到物理结构的整体安全性

2.2.5 可靠性

由于金融业务具有实时性与连续性的特点，因此可靠性是设备的一个重要指标。密码机在硬件的设计上，采用具有创新的设计技术手段，主机采用符合工业标准的嵌入式结构，整体设计上抗冲击、抗振动；密钥管理采用字符终端的方式，使密码机更象黑盒子，有效的减少设备的故障率，极大的提高了设备的可靠性和稳定性。

2.2.6 通用性

在功能上，符合 VISA/MasterCard 国际信用卡组织的要求，能完全与 RACAL（THALES）密码机在应用级上兼容，满足目前银行国际卡业务所要求的规范和标准，同时还支持 IC 卡业务安全体系以及手机银行业务安全体系，在接口方面，适应各种主机通讯接口及不同的通信协议。多安全体系、多通讯协议可并行工作。

2.2.7 系列化

SJLL22 金融数据密码机设计有高、中、低三个档次系列产品，以满足金融业务不同功能、不同性能、不同主机类型的需求。使用 SJL22-SM 金融数据密码机系列产品作为商业银行业务网络中的应用密码设备的最大优点是：除和其他厂商的密码设备互联互通外，采用和 RACAL（THALES）密码机兼容的高速变种加密机制使得 SJL22-SM 金融数据密码机系列产品自身形成一套封闭的安全体系，大大增强了金融业务系统的安全性。

同时，密码机的设计符合绿色环保的标准，低噪音、低功耗、无辐射，采用无公害的元器件。

下面是 SJL22-SM 金融数据密码机系列产品外观图：

图 2-1 SJL22-SM金融数据密码机（高端专用型）外观图

图 2-2 SJL22-SM金融数据密码机（高端通用型）外观图

图 2-3 SJL22-SM金融数据密码机（中端）外观图

图 2-4 SJL22-SM金融数据密码机（网点型）外观图

3 密码机安全机制

依据密钥安全管理的规则，SJL22-SM 金融数据密码机系列产品提供了如下的安全机制，从物理安全性、逻辑安全性等多方面实现了作为密码产品在整体上对安全的需求。

3.1 物理安全机制

SJL22-SM 金融数据密码机系列产品设计为高安全性的加密设备，对于密钥管理，采用双重访问控制，严格依据 FIPS 140-2 的安全级别 3 的要求，采用侵害自动销毁密钥机制，在提高密码机自身的安全防护上以及保证密钥的安全上，采用了相应的实现机制。

3.1.1 采用硬件密钥存储部件

SJL22-SM 金融数据密码机系列产品内设置独立的硬件存储部件，划分为不同的区域，分别用于保存 LMKs（Local Master Keys，以下简称为 LMKs）以及其他各类密钥及敏感数据。密钥存储部件上的密钥存储器采用低功耗 SRAM 芯片，使用 3.6V 锂电池供电，硬件设计上可维持 10 年密钥不丢失。密钥存储部件从硬件设计上采用了防辐射、防探测的安全机制；采用硬件冗余、硬件仲裁及校验等容错/恢复机制，以确保密钥的正确性与完整性。密码机采用重工业钢机箱，设计有多个物理联动传感器，在警戒状态下，任何企图侵害密码机的行为，均会触动传感器装置，而启动密钥销毁机制，自动销毁保存在密钥存储器中的所有密钥。

密钥存储器的容量最大为 128K（***可扩充为 256K***），提供用户可存储 192 位长密钥 2730 个，128 位长密钥 4096 个，64 位长密钥 8192 个（剩余密钥空间预留扩充功能用）。

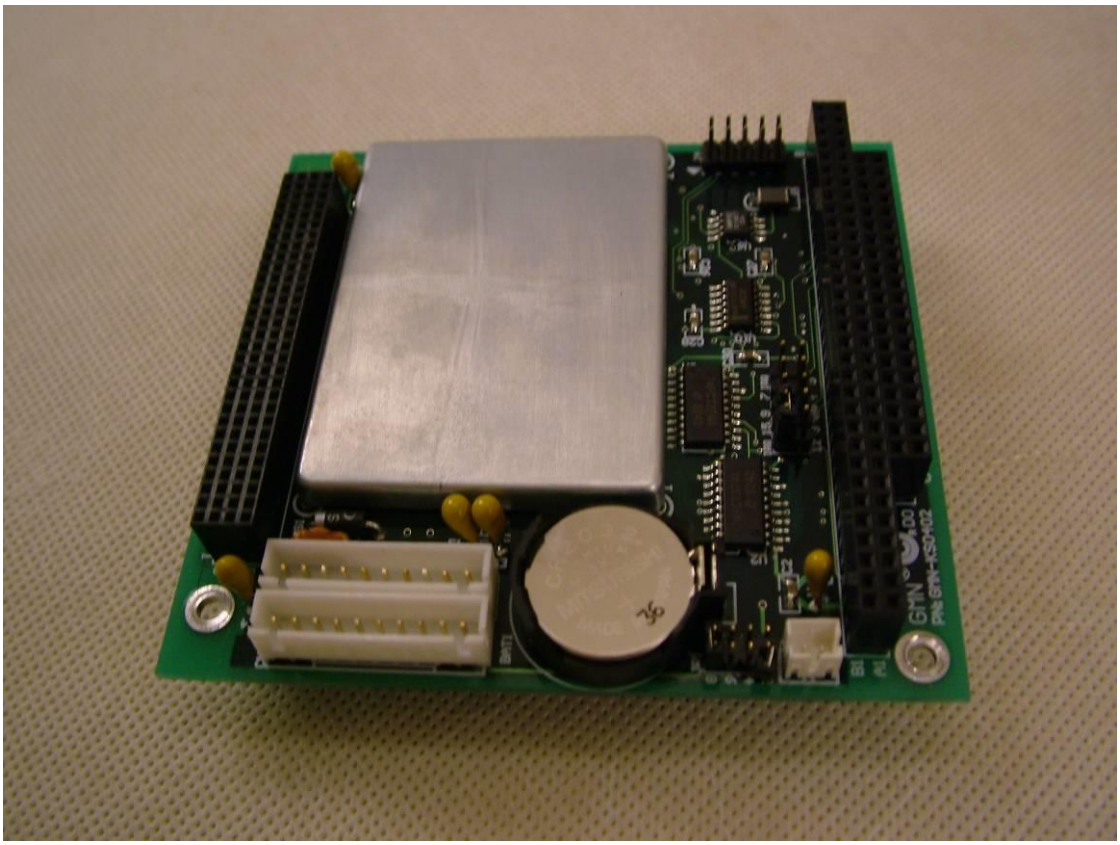


图 3-1 密钥卡结构示意图

3.1.2 设置硬件配置参数存储区

密码机的所有配置参数均保存在密钥存储部件的非易失性存储器 FRAM 内，其容量最大为 8K Bytes。

3.1.3 采用硬件算法部件

用于 SJL22-SM 金融数据密码机系列产品的算法运算。采用 PCI 总线（2.2 规范）接口，实现对称算法（国家专用算法 SSF33、SSF10、SCB2；国际算法 DES/TDES，AES）的加解密运算；PKI 体系的 RSA 密钥对生成，公/私钥的加/解密运算以及采用 MD5/SHA-1 等 13 种 HASH 算法进行摘要运算；使用硬件随机数发生器等。

3.1.4 采用双重保护机制

一个 TRSM（Temper Resistant security module）设备可由一个或多个 TRSM 组成（引自 ANSI X9.24），基于 ANSI X9.24 标准的这样一种理念，密码机在硬件的设计上采用了如下的措施。

3.1.4.1 设置密封锁

机仓安全锁：

SJL22-SM 高端设计于机箱后部两侧位置，共两把。钥匙由两人分别保管，以保证对密码机物理访问的双重控制，便于对密码机的安全管理。

SJL22-SM 中、低端设计于机箱后侧，并加装锁防护装置。在警戒状态下，机仓一旦被打开将会触发机箱内设置的**限位传感开关**，自动销毁密钥存储卡中保存的本地主密钥、用户密钥、敏感数据及重要安全参数。

操作面板安全锁（***注：SJL22-SM 高端密码机设有，其它型号无***）：共一把。密码机在日常的管理与使用中，需要频繁的对管理端口、IC 卡装置、脱机开关、警戒状态开关进行操作。增加操作面板安全锁可保证只有授权人员才能使用，从而避免无关人员的非法操作。（参考图，如有变动以实物为准）。

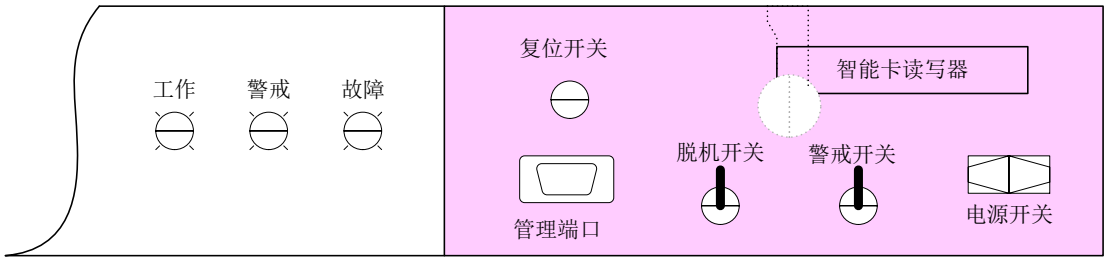


图 3-2 机箱前面板物理锁保护区示意图

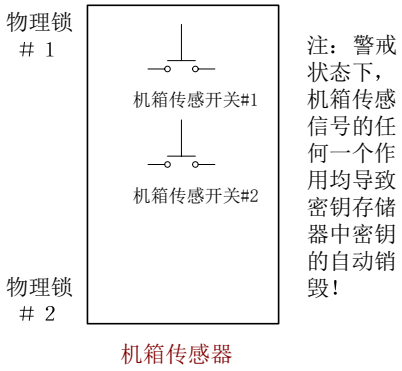


图 3-3 机箱传感器示意图

3.1.4.2 设置防护罩

密码机机箱内的关键部件在设计上加装了防辐射、防刺探工业钢制安全防护罩，使密码机具有能够防止非法攻击的物理特性如：***渗透以电子数据存储的数据、非授权修改内部操作、采用被动式的窃听模式来探测、记录或修改安全数据等。***（专利申请号：2004200880380，外观专利号：ZL2004 3 0078726.4）

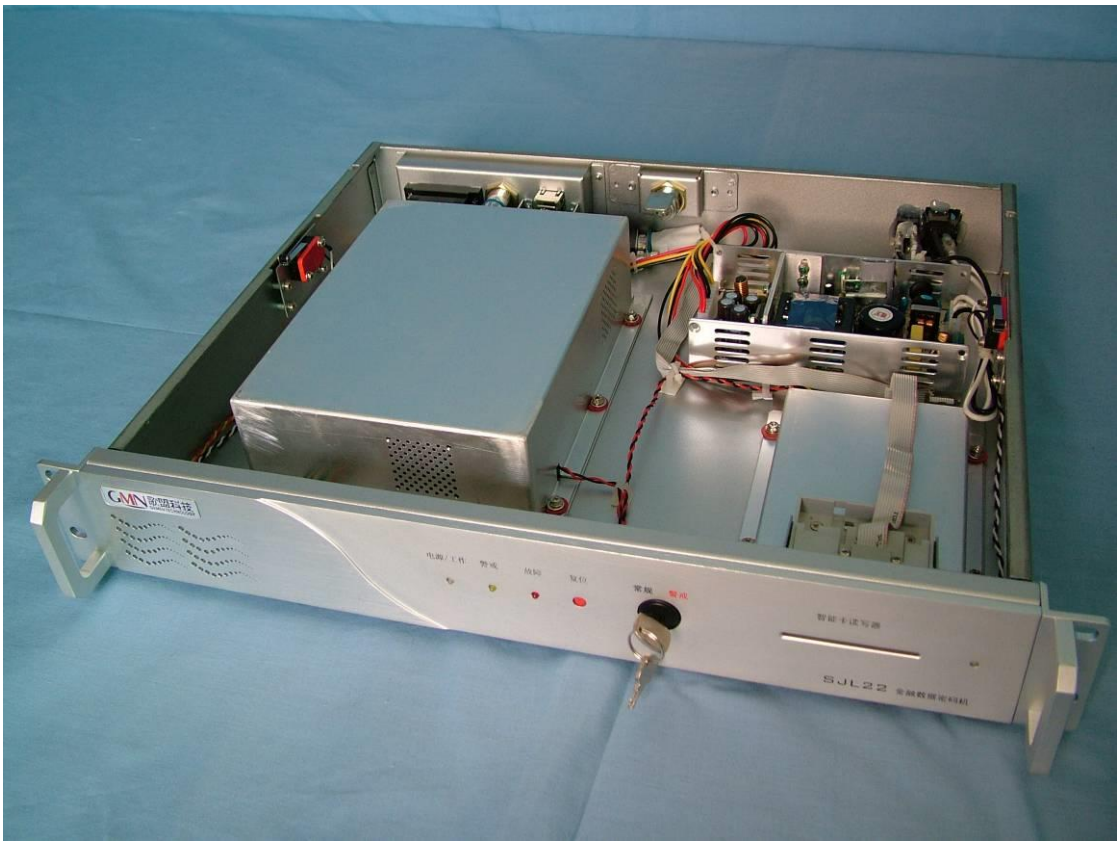


图 3-4 密码机的双重保护机制

3.2 随机数生成方式

SJL22-SM 金融数据密码机系列产品使用两种随机数产生方式：1、硬件随机数发生器——利用物理噪音源产生真随机数作为密钥成分或密钥。2、伪随机数发生器——采用双长度密钥的 ANSI X9.17/ANSI X9.31 伪随机数发生器产生随机数作为密钥成分或密钥。

3.3 密码机工作状态

SJL22-SM 金融数据密码机系列产品提供以下两种工作状态：

- 常规状态
- 警戒状态

常规状态不启用*侵害自毁密钥机制*（Tamper Resistance 机制），主要应用在金融业务应用系统开发阶段使用，便于用户的开发测试。

警戒状态启用*侵害自毁密钥机制*，使密码机具有在受到非法侵害时（如打开机盖等），而导致销毁保存在密码机中的主密钥/用户密钥、重要安全参数等的物理及逻辑特性。

密码机在前面板上设置有“常规状态”与“警戒状态”转换钥匙开关，用来控制密码机由常规状态进入警戒状态及主密钥的销毁。

3.4 密码机工作模式

SJL22-SM 金融数据密码机系列产品提供联机、脱机、授权以及双重授权四种工作模式，配合上述两种工作状态构成十二种密码机运行状态，加电或复位后的缺省状态为联机状态。

密码机在联机状态下才可进行正常的金融交易的安全处理（该状态下也可启动管理终端进行部分密钥管理操作）；转动密码机前面板上的 Toggle 开关（或密码机背面的钥匙开关）可使密码机进入脱机状态，该状态主要用于对密码机进行系统管理和关键的密钥管理操作。触动密码机面板上的“Reset”按钮可使密码机重新进入联机状态。

密码机的授权状态采用双重控制机制通过专人操作才能进入，授权状态为客户提供了客户主机使用密码机某些敏感指令以及使用敏感终端管理命令时的访问控制。授权状态任何时候均可通过联机指令（RC）或终端管理命令（C）解除。

双重授权状态用于更高安全级别的操作，是在授权状态的基础上，通过管理命令（AD）进入。可使用终端管理指令（CD）解除双重授权状态返回授权状态；***双重授权机制警示密码机使用者该状态下密码机的使用会带来不安全因素，用后应尽快解除该状态。***

3.5 密码机安全参数管理

SJL22-SM 系列密码机通过管理终端可对密码机的应用安全参数进行配置管理，提供了客户自行定制密码机应用安全机制的便利性。该功能通过密码机终端管理指令“CS”实现，CS 指令需要在密码机脱机状态下执行。为能够更清晰的阐述密码机的各项安全管理机制的实现，下面对“CS”命令的各功能项进行详细说明：

表 3-1 安全参数管理配置表

序号	功能内容	说 明	备 注
1.	配置个人标识码(PIN)长度(4-12)	配置应用系统中使用的 PIN 长度，密码机有关 PIN 的联机命令需要检查此项内容	
2.	设置回显(oN/oFF)	终端管理操作中，通过此项设置可隐藏输入的明文内容。	在多人操作密码机的情况下，有效地防止了密钥或敏感数据明文的泄漏
3.	Atalla ZMK 变种支持(oN/oFF)配置	用于限制是否允许密码机与 Atalla 密码机互通互联	在可控的前提下，与 Atalla 安全体系的密码机对通
4.	用户存储区密钥长度配置(S/D/T)	根据业务系统中密钥的长度，配置用户存储区的大小，合理的使用用户存储区中的密钥存储空间	用户存储区中的数据在密码机关掉电源后，会自动清除
5.	***警告：该操作过程将清除密码机中主密钥，还继续吗? [Y/N]***	后面各项安全参数的配置将会涉及基于密码机内的 LMKs 的整个应用安全体系的安全，因此，如果继续操作，密码机会提示：“***请将警戒钥匙开关转到警戒位置***”以及“***请将警戒钥匙开关转到常规位置***”，完成这两步操作后，密码机内中的 LMKs 会被清除掉。 如果中断操作，则后续的安全参数不会发生改变。	*一旦密码机内的密钥被清除掉后，则需要重新导入 LMKs，通过这种方式最大程度的保证了 LMKs 的安全，有效的防止了安全参数的非授权改变，使得对密码机关键安全参数的配置都是可控的。*
6.	密钥存储区密钥长度配置	根据业务系统中密钥的长度，配置用户存储区的大小，合理的使用密	密码机关掉电源后，密钥存储区中

	(S/D/T)	钥存储区中的密钥存储空间	的数据还保留，所以需要安全机制来保障安全
7.	选择个人标识码(PIN)明文(Y/N)	如 3.9 节中描述	
8.	配置是否允许 ZMK 转换命令执行(Y/N)	如 3.8.5 节中描述	
9.	配置是否允许 ANSI X9.17 方式导入(Y/N)	如 3.8.4 节中描述	
10.	配置是否允许 ANSI X9.17 方式导出(Y/N)	如 3.8.4 节中描述	
11.	配置是否允许终端 PIN 加密	银行网点用密码机需要对明文 PIN 加密	
12.	禁止检查十进制转换表	在 IBM 3624 方式下允许对十进制转换表的检查与否	
13.	禁止加密十进制转换表	在 IBM 3624 方式下允许对十进制转换表的加密与否	
14.	配置是否允许扩展密钥校验值输出	RACAL 密码机某些指令设计时不输出密钥校验值，应用时一个功能需多次访问密码机，影响效率	参见“SJL22-SM 金融数据密码机开发手册”相关部分
15.	配置用户申请函存储空间	用于批量处理用户申请函时，存储用户申请函数据	
16.	ZMK 长度配置	用于与原 RACAL 安全体系兼容	
17.	配置使用 LMK 加密 PIN 时的加密算法 A/B	提供给磁条卡业务中两种不同的 PIN 加密方式。两种算法所涉及的输入数据 PAN 和 PIN 明文。	建议使用 B 算法
18.	配置密码机授权方式	提供给用户选择口令授权的方式或 IC 卡授权的方式	
19.	RSA 选件密钥类型兼容 THALES	提供给 RSA 命令选项兼容 THALES 4 字节密钥类型或传统 3 字节密钥类型的选项	
20.	最小 HMAC 验	允许对 HMAC 输出支持 5~20 字节	

	证字节数长度	的最小输出选项	
21.	允许 PKCS#11 方式导入和导出 HMAC 密钥	允许对 HMAC 密钥按 PKCS#11 方式的密文导入导出	
22.	允许 ANSI X9.17 方式导入和导出 HMAC 密钥	允许对 HMAC 密钥按 ANSI X9.17 方式的密文导入导出	

3.6 密钥管理的授权机制

SJL22-SM 金融数据密码机系列产品密钥管理的授权与双重授权通过以下两种方式来进行：

- 口令授权方式： 采用由 2 个或 3 个（依厂商设定）16 位字符口令字按先后顺序输入密码机授权
- IC 授权卡方式： 采用 2 张或 3 张（依厂商设定）授权卡按先后顺序插入密码机授权的方式进行授权

密码机的授权方式可通过管理命令来配置。密码机进入授权状态可由 2 人或 3 人进行，厂商可根据用户要求设定参与密码机授权的人数。厂商一旦设定，用户不能自行改变。

密码机的授权可通过主密钥成份卡或授权卡进行。授权卡可通过主密钥成份卡使用终端管理命令（CO）单独制作。

授权卡和主密钥成份卡的区别是：授权卡只做身份识别用。主密钥成份卡既用来识别身份又保存主密钥成份信息。

授权卡可单独制作，仅用于授权是使用，授权卡上不保存任何密钥成份信息。

3.7 隐蔽键（^）

使用字符终端进行密钥管理时，使用者任何时候可通过按下 Shift+6（即^字符）键来隐藏随后的输入字符。该键在多人输入密钥明文时尤为重要。

3.8 密钥管理安全机制

密钥的安全管理包括密钥在其整个生存周期内的管理与保护。所谓密钥生存周期（密钥有效期），即“密钥的生成—密钥的使用—密钥的废弃—密钥的销毁”这样一个过程周期。该部分所指的密钥为 KEK(密钥交换密钥，在本体系中称为 ZMK/TMK)以及其下属层的工作密钥。

密码机 LMKs 的管理在后续相关章节中专门进行说明。

3.8.1 TMK/ZMK 产生

SJL22-SM 金融数据密码机系列产品提供两种产生方式，一种是采用双重访问控制的方式产生，双重控制意味着此类操作至少需要两个人。比较典型的是在生成密钥时，第一个人登录到管理终端，在密码机内随机生成密钥的第一个成份（产生的结果可以为密文、明文、一半或三分之一密钥或以明文的方式写入 IC 中）。然后第二人登录到管理终端，在密码机内随机生成密钥的第二个成份，产生的成份由成份的持有人保管，根据密钥成份的个数依次类推。在需要合成密钥时，再分别登录到管理终端，依据密钥的合成方式（密文、明文、一半或三分之一密钥或 IC 卡的方式）在密码机内部合成密钥。这种方式保证了新产生的密钥不会被单独的一个人掌握或控制。

3.8.2 工作密钥产生

工作密钥通常是由密码机在内部随机生成，并输出在某个主密钥组加密下的密文以及密钥交换密钥下加密的密文。该种方式主要用于产生在线分发的工作密钥，其生命周期短暂，更换频繁。

3.8.3 密钥存储与备份

密码机产生的各种类型的密钥均由指定的主密钥组加密并保存于主机数据库中或保存在密码机内的密钥存储区中，保存在密码机内的密钥同时受密码机的侵害自毁密钥（Tamper Resistant）安全机制来保证安全。**密钥存储在数据库中的存储方式在需要进行多机热备的情况下，使得密钥的同步更新简单易行。密钥存储在密码机中虽然提高了密码机的安全性但也给频繁交换密钥时各密码机中密钥的同步带来了极大的开销甚至不可操作。因而，在后一种情况下，建议使用随时准备（"Ready for Use"）替换的冷备份方式。另外，对密码机的可靠性也提出了更严格的要求。**

SJL22-SM 金融数据密码机系列产品还提供密钥成份在 IC 卡中保存的功能。该种方式使得相同体系的密码机间的密钥分发安全、简单、易行。同时还提供密钥以密文的形式保存在密钥 IC 卡中的功能，增加了密钥存储的安全性。

3.8.4 密钥导入导出安全机制

SJL22-SM 金融数据密码机系列产品支持两种加密方式：**TDEA 变种加密与 ANSI X9.17 方式加密**。其中 ANSI X9.17 主要用于相同体系密码机的或不同体系的密码机间密钥的导入或导出。密钥的导入导出主要用于工作密钥的在线分发，即通讯的双方利用协商好的 KEK，来保证工作密钥的同步。

根据银行业务系统的不同以及安全级别的不同，SJL22-SM 金融数据密码机系列产品提供密钥以 ANSI X9.17 方式导入导出控制这一安全机制，该安全机制的实现是通过终端管理命令 CS 来配置是否允许密钥导入或是否允许密钥导出。客户可根据自己业务系统的安全体系需求，进行配置。典型的情况是，如果是密钥的发起方，则只允许密钥导出，而不允许导入；如果是密钥的接受方，则只允许密钥导入，而不允许导出。银行系统的业务模式多种多样，安全机制的采用需要配合具体的情况而定。

密钥的导入/导出管理控制主要用于不同厂商间密码机的互联互通。SJL22-SM 金融数据密码机系列产品的密钥变种机制使得自身形成一个封闭

的密码体系，大大提高了应用系统的安全性。宛如，不同地方的方言导致同样是中国人但不同地域的人互相不能沟通的道理一样。

3.8.5 ZMK 转换安全机制

初始的 ZMK 是由通讯的双方通过双重访问控制机制协商产生的，采用人工的方式进行安装的。与工作密钥相比，虽然 ZMK 生存周期比较长，但也需要定期地进行更换。

在已经存在初始 ZMK 的基础上，可采用在线的方式进行 ZMK 的更新。但由于 ZMK 为加密其他密钥的密钥，其安全级别较高，因此，为确保在线更换过程的安全性，密码机提供保证 ZMK 转换的安全机制，该安全机制的实现是通过终端管理命令来配置是否允许进行 ZMK 的转换，这种机制可防止假冒通讯节点的接入。

3.9 PIN 管理安全机制

银行业务安全系统在开发测试阶段，需要密码机提供联机指令，完成由 PIN 密文解密出明文的功能。而这一功能在业务系统正式投产之后，对客户主机数据库中保存的 PIN 的安全是一种极大的威胁。

因此，密码机提供输出 PIN 明文的控制机制，通过终端管理命令来配置是否允许输出 PIN 明文，配合授权机制（即解密出 PIN 明文的指令需要密码机在授权状态下才能够完成）更有效的保证了 PIN 的私密性。

3.10 算法概述

在加密算法的使用上，银行在他们的自助终端和主机之间使用国家专用的金融数据加密算法 SSF33、 SSF10 或 SCB2；但国际卡业务所有传送到外卡中心的交易一定要符合 VISA/MasterCard 国际信用卡组织要求的 TDEA 加密。因此，SJL22-SM 金融数据密码机系列产品从加密体系上***提供不同密码算法之间加密数据的转换功能***。

3.10.1专用算法

使用国家密码管理委员会批准的专用算法—SSF33/SSF10/SCB2，算法的具体性能指标如下：

SSF33：

1、为对称密码体系，分组加密算法

2、数据分组的长度为 128 bits

3、密钥长度为 128 bits

4、算法的运算速度达到 40Mbps/秒以上

SSF10：

1、为对称密码体系，分组加密算法

2、数据分组的长度为 64 bits

3、密钥长度为 128 bits

4、算法的运算速度达到 25Mbps/秒以上

SCB2：

1、为对称密码体系，分组加密算法

2、数据分组的长度为 128 bits

3、密钥长度为 128 bits/192 bits/256bits

3.10.2国际兼容算法

使用国家密码管理委员会批准使用的 DES/TDES/AES 算法，算法的性能指标具体如下：

DES/TDES：

1、能够与国际通用的金融数据加密算法兼容

2、采用对称密码体系，分组加密算法

3、数据分组的长度为 64 bits

4、密钥长度支持 64bits/128 bits/192 bits

5、算法的运算速度上达到 40M/秒以上

AES：

1、为对称密码体系，分组加密算法

2、数据分组的长度为 128 bits

3、密钥长度为 128 bits/192 bits/256bits

支持 RSA(数据填充方式支持 PKCS#1, OAEP, PSS, ANSI X9.31, EMV2000 等)算法，哈希算法支持 SHA-1，SHA-224，SHA-256，SHA-384，SHA-512，MD2，MD4，MD5，RIPE-MD128，RIPE-MD160，RIPE-MD256，RIPE-MD320，ISO-10118-2 等算法以及相应的 HMAC 算法，RSA 算法密钥模长支持 192 至 2048 位连续可调，满足目前***金融界全球推广的 EMV 2000 智能卡业务***的要求。

4 密钥管理方案

4.1 三层密钥体系

SJL22-SM 金融数据密码机系列产品密钥体系采用较之国内普遍使用的金融数据密码机体系更为合理、安全性更为可靠的三层密钥管理体系。LMK 由国内普遍使用的金融数据密码的三个成份合成扩充为由 2～9 个成份集合成，并支持 192 位长度的高强度主密钥。每个主密钥成份集生成时，由密码机在内部依据 ANSI X9.17 随机数生成算法离散成 50 组主密钥成份集保存在 IC 卡上。

欧洲银行标准委员会关于密钥管理有如下的建议：不管是对称密钥还是非对称密钥，均应专钥专用。因此 SJL22-SM 金融数据密码机系列产品在密钥管理体系的设计上，使得密码机内保存有 50 组的 LMKs，不同的 LMK 组加密不同功能的数据或密钥。这样一旦某个密钥泄密，不会影响到其它密钥的安全性。这种体系结构的优点是：LMKs 的安全性不完全依赖于管理制度，而是首先从技术上对密钥的安全性进行了充分的考虑。

在密钥体系结构的设计上，采用严格的三层密钥管理，如下图所示：

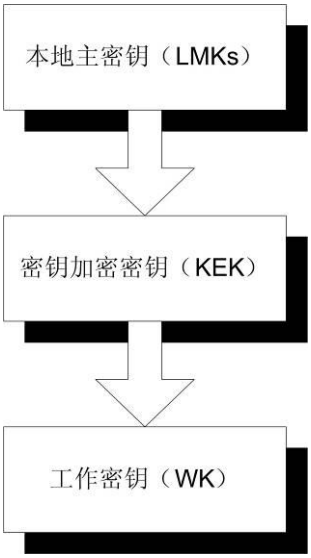


图 4-1 三层密钥管理体系

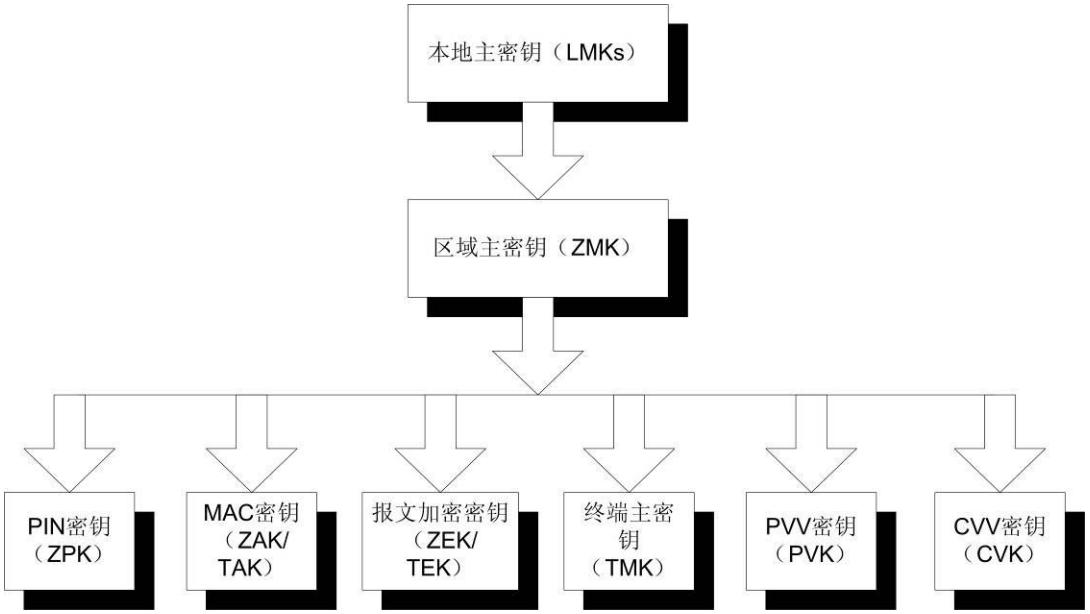


图 4-2 共享网络中的密钥分级管理

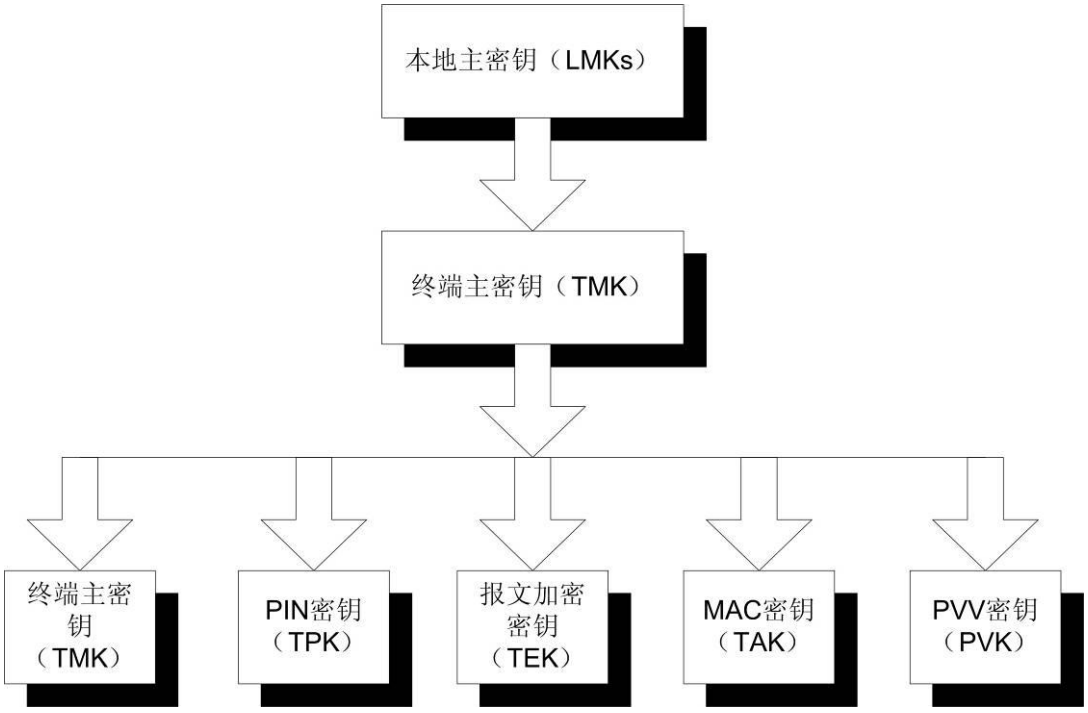


图 4-3 本地网络中的密钥分级管理

为保证保存在密码机内的 LMKs 的安全性，SJL22-SM 金融数据密码机系列产品***密钥管理体系不提供也不允许密钥或成份的导出功能（这是采用与国内其它同行业厂商截然不同的理念）***。这样在任何情况下，任何接触到密码机的人员都无法由密码机直接获得 LMKs 或其成份。在高度安全应用模式下由于采用了侵害销毁密钥机制，因此只要保证了 LMK 成份卡和密钥生成要素的安全，就能够保证主密钥的安全性，其结果是保证业务系统的安全性。

4.2 密钥类型

SJL22-SM 金融数据密码机系列产品的三层密钥管理体系中包含的密钥类型如下：

1、本地主密钥 LMKs

LMKs 限定为三长度密钥，分三个部分，每个部分由 16 位的 16 进制字符组成。所有在本地保存的密钥和数据均需要在 LMKs 下加密之后，保存在主机系统中。常用的各组密钥的功能如下表所示：

表 4-1 本地主密钥功能一览表

DEC Index	HEX Index	Key Type	LMK triplet	描　　述
00	00		000-002	密码机进入授权状态时使用的三个授权口令 ，(密码机设置为口令授权方式时使用)
01	01		003-005	用于主机数据库中存储的 PIN 的加密
02	02	00	006-008	1、加密ZMK与双长度的ZMKs 2、以变种的方式加密 ZMK 成份
03	03	01	009-011	用于加密 ZPK
04	04		012-014	用于产生随机数
05	05		015-017	用于密码机缓冲区中的密钥加密
06	06		018-020	用户产生的初始安全码，用于产生所有的其他主密钥组
07	07	02	021-023	1、用于加密TMK TPK PVK 2、以变种的方式加密 CVK
08	08	03	024-026	用于加密 TEK
09	09	04	027-029	用于加密用户申请函的用户参考号

10	0A	05	030-032	在变种的方式下加密 'not on us' PVK 与 CVK
11	0B	06	033-035	加密 Watchword 密钥.
12	0C	07	036-038	加密 ZTK
13	0D	08	039-041	加密 ZAK
14	0E	09	042-044	加密 TDK
15	0F	0A	045-047	加密 ZEK；以变种的方式加密*区域 IV Keys 和 ZEK 成份*
16	10	0B	048-050	加密 TEK；以变种的方式加密*终端 IV Keys 和 TEK 成份*
17	11	0C	051-053	加密 RSA 私钥
18	12	0D	054-056	公钥和验证数据的 MAC 密钥
19	13	0E	057-059	预留。
20	14	0F	060-062	*加密 DSK – 数据存储密钥. 以变种的方式加密 DS IV 密钥和 DSK 成份*
21	15	10	063-065	DEK: 用于加密需要本地安全存储的数据，*以变种的方式加密 IV 密钥和 DEK 成份*
22	16	11	066-068	加密 LPK（IPK）密钥。
23	17	12	069-071	预留。
24	18	13	072-074	预留。
25	19	14	075-077	预留。
26	2A	15	078-080	预留。
27	2B	16	081-083	预留。
28	2C	17	084-086	预留。
29	2D	18	087-089	预留。
30	2E	19	090-092	预留。
32	2F	1A	093-095	预留。
32	20	1B	096-098	预留。
33	21	1C	099-101	EMV2000 发卡命令密钥类型：0
34	22	1D	102-104	EMV2000 发卡命令密钥类型：1
35	23	1E	105-107	EMV2000 发卡命令密钥类型：2
36	24	1F	108-110	EMV2000 发卡命令密钥类型：3
37	25	20	111-113	EMV2000 发卡命令密钥类型：4
38	26	21	114-116	EMV2000 发卡命令密钥类型：5
39	27	22	117-119	EMV2000 发卡命令密钥类型：6
40	28	23	120-122	EMV2000 发卡命令密钥类型：7
41	29	24	123-125	EMV2000 发卡命令密钥类型：8

42	2A	25	126-128	EMV2000 发卡命令密钥类型：9
43	2B	26	129-131	EMV2000 发卡命令密钥类型：A
44	2C	27	132-134	EMV2000 发卡命令密钥类型：B
45	2D	28	135-137	EMV2000 发卡命令密钥类型：C
46	2E	29	138-140	EMV2000 发卡命令密钥类型：D
47	2F	2A	141-143	EMV2000 发卡命令密钥类型：E
48	30	2B	144-146	EMV2000 发卡命令密钥类型：F
49	31	2C	147-149	预留。

2、Zone Master Key (ZMK) 区域主密钥

Zone Master Key (ZMK)是加密密钥用的密钥，适用于共享网络中，它可以在共享网络中两个(或多个)通讯网点之间以成份的形式进行人工分配且保持双方的对称性，共享网络中任何两个通讯网点之间均共用不同的 ZMK。ZMK 用于加密底层需要传送的数据密钥，这样远地密钥就能自动在线地进行交换(无须人工干预)。该密钥可以长期不更改，通常二年更新一次 。本地存储时，ZMK 是在一组 LMK 下加密保存于主机数据库或密码机内的密钥存储区中。

3、Zone PIN Key(ZPK) 区域 PIN 密钥

区域 PIN 密钥是一个数据加密密钥，适用于共享网络，它通过 ZMK 加密在两个(或多个)通讯网点之间进行自动分配，ZPK 用于加密两个通讯网点之间需传输的 PIN，这样就实现了 PIN 的保密。ZPK 需要经常性地定期更改，在本地存储时，它是是在一组 LMK 下加密的。

4、Zone Authentication Key (ZAK) 区域认证密钥

区域认证密钥是一个数据加密用的密钥，适用于共享网络。它通过 ZMK 加密在两个(或多个)通讯网点之间进行自动分配。ZAK 用于两个通讯节点之间传送信息时，生成和校验一个信息认证代码(Message Authentication Code)，从而达到信息认证的目的。ZAK 需要经常性地更换，通常每天更换一次，本地存储时通过一对 LMK 进行加密。

5、Zone Encryption Key(ZEK) 区域加密密钥

区域加密密钥是一个数据加密密钥，适用于共享网络，它通过 ZMK 加密在两个(或多个)通讯网点之间进行自动分配，ZEK 用于加密两个通讯网点之间需传输的敏感数据，实现交易报文的安全传送。ZEK 需要经常性地定期更改，在本地存储时，它是是在一组 LMK 下加密的。

6、Terminal Master Key (TMK) 终端主密钥

终端主密钥是一个加密密钥用的密钥，适用于终端网络中。可以人工地或自动地在以前安装过 TMK 的基础上分配给通讯的双方且保持双方之间的对称性，它用于在终端网络内将新产生的 TMKS 或底层的数据加密用的密钥加密，然后由主机端传输到 ATM 或 POS 或其它相似的终端。TMK 可以具体业务安全体系确定更新的时间，本地存储时通过一组 LMK 进行加密。

7、Terminal PIN Key (TPK) 终端 PIN 密钥

终端 PIN 密钥是一个数据加密用的密钥，适用于终端网络中，它是在终端网络内通过 TMK 加密，由终端数据受理者自动分配到终端且保持通讯双方之间的对称性。TPK 用于加密在终端网络内终端和终端数据受理者之间传送的 PIN。本地存储时通过一对 LMK 进行加密的。TPK 需要经常性地定期更换，通常每天更换一次。

8、Terminal Authentication Key (TAK) 终端认证密钥

终端认证密钥是一个数据加密用的密钥，适用于终端网络。它在终端网络内通过 TMK 加密由终端数据受理者自动分配到终端或通过 ZMK 加密由终端数据受理者自动分配到交换中心。TAK 用于终端网络内终端与终端数据受理者之间传送信息时，生成和校验一个信息认证代码(Message Authentication Code)，从而达到信息认证的目的。TAK 需要经常性地更换，通常每天更换一次，本地存储时通过一对 LMK 进行加密。

9、Terminal Encryption Key(TEK) 终端加密密钥

终端加密密钥是一个数据加密密钥，适用于终端网络，它通过 TMK 加密在终端和前置机之间进行自动分配，TEK 用于加密终端和前置机之间需传输

的敏感数据，实现交易报文的安全传送。TEK 需要经常性地定期更改，在本地存储时，它是是在一组 LMK 下加密的。

10、PIN Verification Key (PVK) PIN 校验密钥

PIN 校验密钥是一个数据加密密钥，用于生成和校验 PIN 校验数据，同时校验一个 PIN 的可靠性。传送时 PVK 通过 TMK 或 ZMK 加密；存放本地时，它通过一对 LMK 加密。

11、Card Verification Key (卡校验密钥)

卡校验密钥(CVK)类似于 PIN 校验密钥，仅仅是用卡的信息取代了 PIN。

12、Data Storage Key (数据存储密钥)

数据存储密钥 DSK 是用来加密本地保存的敏感数据，主要目的是保证金融敏感信息的安全存储。

13、*Base Derivation Key（基础派生密钥）

用于 DUKPT 传输密钥机制，实现大量的 POS 系统每交易使用唯一的密钥。

14、Local PIN Key（本地 PIN 密钥）

本地 PIN 密钥又称发卡行 PIN 密钥（Issuer PIN Key）。本地 PIN 密钥 LPK 是用来验证从网络中接收的客户 PIN 和保存在主机数据库中指定格式 PIN 的正确性的专用密钥，保存在主机数据库中的 PIN 是按指定的 PIN 格式（01~06）生成的 PIN 数据块。

4.3 密钥类型表

在密钥体系的实际应用中，为方便 LMK 密钥组的使用，严格把 LMK 密钥组与其下加密的密钥对应起来，建立了密钥类型表。将常用的 LMK 密钥组按从小到大的顺序排序，每个序号由两位十六进制数组成。考虑到 LMK 变种的存在，在每个序号前增加一位，代表 LMK 变种的序号。从而将密钥类型表扩充到三位。每个三位的序号代表不同的密钥，如 001 表示密钥为 ZPK。

密钥类型表如下表所示：

表 4-2 密钥类型表

LMK Triplet / Variant	LMK Pair / Variant	LMK Triplet code	0	1	2	3	4	5	6	7	8	9
000-002	00-01											
003-005	02-03											
006-008	04-05	00	ZMK	ZMK (Comp)	KML							
009-011	06-07	01	ZPK									
012-014	08-09											
015-017	10-11											
018-020	12-13											
021-023	14-15	02	PVK TPK TMK				CVK CSCK					
024-026	16-17	03	TAK									
027-029	18-19	04										
030-032	20-21	05										
033-035	22-23	06	WWK									
036-038	24-25	07										
039-041	26-27	08	ZAK									
042-044	28-29	09	BDK	MK-AC	MK-SMI	MK-SMC	MK-DAK	MK-DN				
045-047	30-31	0A	ZEK	ZE-IV	ZEK (Comp)							
048-050	32-33	0B	TEK	TE-IV	TEK (Comp)							
051-053	34-35	0C	RSA-SK									
054-056	36-37	0D	RSA-PMK									RSA-SMK
057-059	38-39	0E										
060-062	40-41	0F	DSK	DS-IV	DSK (Comp)							
063-065	42-43	10	DEK	DE-IV	DEK (Comp)							
066-068	44-45	11	LPK(IPK)									
069-071	46-47	12										
072-074	48-49	13										
075-077	50-51	14										
078-080	52-53	15										
081-083	54-55	16										

084-086	56-57	17										
087-089	58-59	18										
090-092	60-61	19										
093-095	62-63	1A										
096-098	64-65	1B										
099-101	66-67	1C										
102-104	68-69	1D										
105-107	70-71	1E										
108-110	72-73	1F										
111-113	74-75	20										
114-116	76-77	21										
117-119	78-79	22										
120-122	80-81	23										
123-125	82-83	24										
126-128	84-85	25										
129-131	86-87	26										
132-134	88-89	27										
135-137	90-91	28										
138-140	92-93	29										
141-143	94-95	2A										
144-146	96-97	2B										
147-149	98-99	2C										

4.4 基准测试密钥

SJL22-SM 金融数据密码机系列产品提供 2 组基准测试主密钥,以利于安全业务系统开发阶段的调试，第 1 组测试主密钥主要是为了和 RACAL 兼容，第 2 组测试主密钥为三长度测试密钥。50 组测试密钥的明文分别如下所示：

表 4-3 基准测试主密钥集#1

LMK 组	基准测试主密钥集#1			LMK 对
000-002	EAAB 4012 9F1A B977	5E2A 5DD7 B0B6 08E1	EAAB 4012 9F1A B977	00-01
003-005	2020 2020 2020 2020	3131 3131 3131 3131	2020 2020 2020 2020	02-03
006-008	4040 4040 4040 4040	5151 5151 5151 5151	4040 4040 4040 4040	04-05
009-011	6161 6161 6161 6161	7070 7070 7070 7070	6161 6161 6161 6161	06-07
012-014	8080 8080 8080 8080	9191 9191 9191 9191	8080 8080 8080 8080	08-09
015-017	A1A1 A1A1 A1A1 A1A1	B0B0 B0B0 B0B0 B0B0	A1A1 A1A1 A1A1 A1A1	10-11
018-020	C1C1 0101 0101 0101	D0D0 0101 0101 0101	C1C1 0101 0101 0101	12-13
021-023	E0E0 0101 0101 0101	F1F1 0101 0101 0101	E0E0 0101 0101 0101	14-15
024-026	1C58 7F1C 1392 4FEF	0101 0101 0101 0101	1C58 7F1C 1392 4FEF	16-17
027-029	0101 0101 0101 0101	0101 0101 0101 0101	0101 0101 0101 0101	18-19
030-032	0202 0202 0202 0202	0404 0404 0404 0404	0202 0202 0202 0202	20-21
033-035	0707 0707 0707 0707	1010 1010 1010 1010	0707 0707 0707 0707	22-23
036-038	1313 1313 1313 1313	1515 1515 1515 1515	1313 1313 1313 1313	24-25
039-041	1616 1616 1616 1616	1919 1919 1919 1919	1616 1616 1616 1616	26-27
042-044	1A1A 1A1A 1A1A 1A1A	1C1C 1C1C 1C1C 1C1C	1A1A 1A1A 1A1A 1A1A	28-29
045-047	2323 2323 2323 2323	2525 2525 2525 2525	2323 2323 2323 2323	30-31
048-050	2626 2626 2626 2626	2929 2929 2929 2929	2626 2626 2626 2626	32-33
051-053	2A2A 2A2A 2A2A 2A2A	2C2C 2C2C 2C2C 2C2C	2A2A 2A2A 2A2A 2A2A	34-35
054-056	2F2F 2F2F 2F2F 2F2F	3131 3131 3131 3131	2F2F 2F2F 2F2F 2F2F	36-37
057-059	0101 0101 0101 0101	0101 0101 0101 0101	0101 0101 0101 0101	38-39
060-062	2020 2020 2020 2020	3131 3131 3131 3131	2020 2020 2020 2020	40-41
063-065	4040 4040 4040 4040	5151 5151 5151 5151	4040 4040 4040 4040	42-43
066-068	6161 6161 6161 6161	7070 7070 7070 7070	6161 6161 6161 6161	44-45
069-071	8080 8080 8080 8080	9191 9191 9191 9191	8080 8080 8080 8080	46-47
072-074	A1A1 A1A1 A1A1 A1A1	B0B0 B0B0 B0B0 B0B0	A1A1 A1A1 A1A1 A1A1	48-49
075-077	C1C1 0101 0101 0101	D0D0 0101 0101 0101	C1C1 0101 0101 0101	50-51
078-080	E0E0 0101 0101 0101	F1F1 0101 0101 0101	E0E0 0101 0101 0101	52-53
081-083	1C58 7F1C 1392 4FEF	0101 0101 0101 0101	1C58 7F1C 1392 4FEF	54-55
084-086	0101 0101 0101 0101	0101 0101 0101 0101	0101 0101 0101 0101	56-57
087-089	0202 0202 0202 0202	0404 0404 0404 0404	0202 0202 0202 0202	58-59

090-092	0707 0707 0707 0707	1010 1010 1010 1010	0707 0707 0707 0707	60-61
093-095	1313 1313 1313 1313	1515 1515 1515 1515	1313 1313 1313 1313	62-63
096-098	1616 1616 1616 1616	1919 1919 1919 1919	1616 1616 1616 1616	64-65
099-101	1A1A 1A1A 1A1A 1A1A	1C1C 1C1C 1C1C 1C1C	1A1A 1A1A 1A1A 1A1A	66-67
102-104	2323 2323 2323 2323	2525 2525 2525 2525	2323 2323 2323 2323	68-69
105-107	2626 2626 2626 2626	2929 2929 2929 2929	2626 2626 2626 2626	70-71
108-110	2A2A 2A2A 2A2A 2A2A	2C2C 2C2C 2C2C 2C2C	2A2A 2A2A 2A2A 2A2A	72-73
111-113	2F2F 2F2F 2F2F 2F2F	3131 3131 3131 3131	2F2F 2F2F 2F2F 2F2F	74-75
114-116	0101 0101 0101 0101	0101 0101 0101 0101	0101 0101 0101 0101	76-77
117-119	2020 2020 2020 2020	3131 3131 3131 3131	2020 2020 2020 2020	78-79
120-122	4040 4040 4040 4040	5151 5151 5151 5151	4040 4040 4040 4040	80-81
123-125	6161 6161 6161 6161	7070 7070 7070 7070	6161 6161 6161 6161	82-83
126-128	8080 8080 8080 8080	9191 9191 9191 9191	8080 8080 8080 8080	84-85
129-131	A1A1 A1A1 A1A1 A1A1	B0B0 B0B0 B0B0 B0B0	A1A1 A1A1 A1A1 A1A1	86-87
132-134	C1C1 0101 0101 0101	D0D0 0101 0101 0101	C1C1 0101 0101 0101	88-89
135-137	E0E0 0101 0101 0101	F1F1 0101 0101 0101	E0E0 0101 0101 0101	90-91
138-140	1C58 7F1C 1392 4FEF	0101 0101 0101 0101	1C58 7F1C 1392 4FEF	92-93
141-143	0101 0101 0101 0101	0101 0101 0101 0101	0101 0101 0101 0101	94-95
144-146	0202 0202 0202 0202	0404 0404 0404 0404	0202 0202 0202 0202	96-97
147-149	0123 4567 89AB CDEF	FEDC BA98 7654 3210	0707 0707 0707 0707	98-99
Password 1 = 0101 0101 0101 0101 Password 2 = NOW IS THE TIME FOR A Password 3 =0303 0303 0303 0303				

密钥校验值为：93A196A2FC6C82B6

表 4-4 基准测试主密钥集#2

LMK 组	基准测试主密钥集#2			LMK 对
000-002	EAAB 4012 9F1A B977	5E2A 5DD7 B0B6 08E1	0123 4567 89AB CDEF	00-01
003-005	2020 2020 2020 2020	3131 3131 3131 3131	0123 4567 89AB CDEF	02-03
006-008	4040 4040 4040 4040	5151 5151 5151 5151	0123 4567 89AB CDEF	04-05
009-011	6161 6161 6161 6161	7070 7070 7070 7070	0123 4567 89AB CDEF	06-07
012-014	8080 8080 8080 8080	9191 9191 9191 9191	0123 4567 89AB CDEF	08-09
015-017	A1A1 A1A1 A1A1 A1A1	B0B0 B0B0 B0B0 B0B0	0123 4567 89AB CDEF	10-11
018-020	C1C1 0101 0101 0101	D0D0 0101 0101 0101	0123 4567 89AB CDEF	12-13
021-023	E0E0 0101 0101 0101	F1F1 0101 0101 0101	0123 4567 89AB CDEF	14-15

024-026	1C58 7F1C 1392 4FEF	0101 0101 0101 0101	0123 4567 89AB CDEF	16-17
027-029	0101 0101 0101 0101	0101 0101 0101 0101	0123 4567 89AB CDEF	18-19
030-032	0202 0202 0202 0202	0404 0404 0404 0404	0123 4567 89AB CDEF	20-21
033-035	0707 0707 0707 0707	1010 1010 1010 1010	0123 4567 89AB CDEF	22-23
036-038	1313 1313 1313 1313	1515 1515 1515 1515	0123 4567 89AB CDEF	24-25
039-041	1616 1616 1616 1616	1919 1919 1919 1919	0123 4567 89AB CDEF	26-27
042-044	1A1A 1A1A 1A1A 1A1A	1C1C 1C1C 1C1C 1C1C	0123 4567 89AB CDEF	28-29
045-047	2323 2323 2323 2323	2525 2525 2525 2525	0123 4567 89AB CDEF	30-31
048-050	2626 2626 2626 2626	2929 2929 2929 2929	0123 4567 89AB CDEF	32-33
051-053	2A2A 2A2A 2A2A 2A2A	2C2C 2C2C 2C2C 2C2C	0123 4567 89AB CDEF	34-35
054-056	2F2F 2F2F 2F2F 2F2F	3131 3131 3131 3131	0123 4567 89AB CDEF	36-37
057-059	0101 0101 0101 0101	0101 0101 0101 0101	0123 4567 89AB CDEF	38-39
060-062	2020 2020 2020 2020	3131 3131 3131 3131	0123 4567 89AB CDEF	40-41
063-065	4040 4040 4040 4040	5151 5151 5151 5151	0123 4567 89AB CDEF	42-43
066-068	6161 6161 6161 6161	7070 7070 7070 7070	0123 4567 89AB CDEF	44-45
069-071	8080 8080 8080 8080	9191 9191 9191 9191	0123 4567 89AB CDEF	46-47
072-074	A1A1 A1A1 A1A1 A1A1	B0B0 B0B0 B0B0 B0B0	0123 4567 89AB CDEF	48-49
075-077	C1C1 0101 0101 0101	D0D0 0101 0101 0101	0123 4567 89AB CDEF	50-51
078-080	E0E0 0101 0101 0101	F1F1 0101 0101 0101	0123 4567 89AB CDEF	52-53
081-083	1C58 7F1C 1392 4FEF	0101 0101 0101 0101	0123 4567 89AB CDEF	54-55
084-086	0101 0101 0101 0101	0101 0101 0101 0101	0123 4567 89AB CDEF	56-57
087-089	0202 0202 0202 0202	0404 0404 0404 0404	0123 4567 89AB CDEF	58-59
090-092	0707 0707 0707 0707	1010 1010 1010 1010	0123 4567 89AB CDEF	60-61
093-095	1313 1313 1313 1313	1515 1515 1515 1515	0123 4567 89AB CDEF	62-63
096-098	1616 1616 1616 1616	1919 1919 1919 1919	0123 4567 89AB CDEF	64-65
099-101	1A1A 1A1A 1A1A 1A1A	1C1C 1C1C 1C1C 1C1C	0123 4567 89AB CDEF	66-67
102-104	2323 2323 2323 2323	2525 2525 2525 2525	0123 4567 89AB CDEF	68-69
105-107	2626 2626 2626 2626	2929 2929 2929 2929	0123 4567 89AB CDEF	70-71
108-110	2A2A 2A2A 2A2A 2A2A	2C2C 2C2C 2C2C 2C2C	0123 4567 89AB CDEF	72-73

111-113	2F2F 2F2F 2F2F 2F2F	3131 3131 3131 3131	0123 4567 89AB CDEF	74-75
114-116	0101 0101 0101 0101	0101 0101 0101 0101	0123 4567 89AB CDEF	76-77
117-119	2020 2020 2020 2020	3131 3131 3131 3131	0123 4567 89AB CDEF	78-79
120-122	4040 4040 4040 4040	5151 5151 5151 5151	0123 4567 89AB CDEF	80-81
123-125	6161 6161 6161 6161	7070 7070 7070 7070	0123 4567 89AB CDEF	82-83
126-128	8080 8080 8080 8080	9191 9191 9191 9191	0123 4567 89AB CDEF	84-85
129-131	A1A1 A1A1 A1A1 A1A1	B0B0 B0B0 B0B0 B0B0	0123 4567 89AB CDEF	86-87
132-134	C1C1 0101 0101 0101	D0D0 0101 0101 0101	0123 4567 89AB CDEF	88-89
135-137	E0E0 0101 0101 0101	F1F1 0101 0101 0101	0123 4567 89AB CDEF	90-91
138-140	1C58 7F1C 1392 4FEF	0101 0101 0101 0101	0123 4567 89AB CDEF	92-93
141-143	0101 0101 0101 0101	0101 0101 0101 0101	0123 4567 89AB CDEF	94-95
144-146	0202 0202 0202 0202	0404 0404 0404 0404	0123 4567 89AB CDEF	96-97
147-149	0123 4567 89AB CDEF	FEDC BA98 7654 3210	0123 4567 89AB CDEF	98-99
Password 1 = 0101 0101 0101 0101 Password 2 = NOW IS THE TIME FOR A Password 3 = 0303 0303 0303 0303				

密钥校验值为：D8D3 36CA 8D27 D543

4.5 密钥管理操作方式

SJL22-SM 金融数据密码机系列产品的终端管理操作方式具有如下的特点：

- SJL22-SM 金融数据密码机系列产品采用字符终端（哑终端）的密钥管理操作方式。字符终端的特点是操作者不可能截获操作过程中任何通讯数据，***减少了安全隐患***。另外，采用字符终端进行密钥管理也不需要增加采用其他密钥管理方式（如采用键盘和 LCD）所需的额外硬件接口设备，从而提高了密码机硬件整体的可靠性和稳定性，减少了故障率。
- 提供密钥存取/访问的双重控制机制，使得对涉及密钥安全的任何操

作都需要在严格授权的情况下才能够执行。

- 终端操作简单易懂，通过任意一个连接到密码机控制端口的字符终端即可进行配置管理和密钥管理的各种操作。操作界面简洁易懂，方便客户对密码机进行管理。

4.6 LMKs 管理机制

LMKs 为用于加密其他密钥的密钥，其在整个生存期内的安全管理至关重要。下面简要说明其安全管理机制。

4.6.1 产生方式

密码机采用双重控制机制实现主密钥的管理，以防止单独某个人独自生成或取得密钥信息。通常由二至九位银行官员分别通过密码机提供的终端操作界面产生自己的密钥成份，并在口令字的保护下保存到符合 ISO 7816 的 IC 卡中，每个成份 IC 卡可复制多份。

主密钥成份生成后在未投入生产前，任何成份卡的泄漏或丢失不会给密码机带来安全隐患。一旦成份卡参与密码机主密钥的重构，则应对各成份卡严格管理。

SJL22-SM 金融数据密码机系列产品采用 ANSI X9.17 伪随机数方式生成 50 组 LMK 成份组。

主密钥 LMKs 生成要素：

秘密值 A：16 位十六进制数字（64bits）

秘密值 B：16 位十六进制数字（64bits）

秘密值 C：16 位十六进制数字（64bits）

时间因子：8 位十进制数字（mmddHHMM）

参与者顺序号：1~9

主密钥 LMKs 生成要素中的三个秘密值，建议由人工输入，也可由密码机随机生成。人工输入方式产生的 LMKs 成份，一旦出现主密钥成份卡丢失

的情况，可通过重新输入各要素来进行恢复；但采用密码机随机生成的方式，则不可能通过上述方式来恢复，因此必须严格加强对各 LMK 成份卡的备份管理。

生成主密钥成份时，密码机中并不保存主密钥或成份，也不将中间结果保存在密码机中。

第 1~3 位（依厂商设定）成份的持有者也是口令授权机制的口令字的持有者，密码机可通过管理命令由主密钥成份卡生成密码机授权卡。密码机授权卡中不包含任何主密钥信息。

4.6.2 LMKs 的验证

由于 SJL22-SM 金融数据密码机系列产品采用 50 组 192bits 长度的主密钥集合，主密钥的正确性即完整性验证方式不适宜采用常规加密“0”的方式。我们采用 DEA 的 MDC（Message Detection Code）模式，类似于 MD5/SHA1。另外，单个主密钥的正确性验证采用了奇偶校验码。

SJL22-SM 金融数据密码机提供两种主密钥的验证方式，来完成主密钥的正确性验证。一种是使用终端管理命令 **V**，通过验证主密钥的校验值来确定密码机中主密钥的正确性；另一种方式是由主机系统发送联机指令 **NC**，通过验证主密钥的校验值来确定密码机中主密钥的正确性。另外，主密钥错误也会启动密码机故障灯指示。

4.6.3 导入方式

当密码机投产时，由二至九位银行官员分别通过密码机的终端管理操作界面，利用管理命令 LK，将上步生成并保存于 IC 卡中的各主密钥成份集导入密码机中。密码机不提供密钥成份导出功能。***一旦主成份成份卡参与生产系统密码机主密钥的构成，则应对其进行严格管理。***

4.6.4 LMKs 更新机制

主密钥有一定的生存周期，即“密钥的生成－密钥的使用－密钥的废弃－密钥的销毁”。LMKs 通常是 2~3 年更换一次。为方便银行业务系统转换新旧主密钥加密下的数据，SJL22-SM 金融数据密码机系列产品提供了在更新主密钥时，旧主密钥密钥以及敏感数据的自动转换机制：即设置旧密钥存储区，当需要更换主密钥时，临时保存旧主密钥于该密钥存储区域中，利用密码机提供的联机指令方便的完成由旧主密钥加密下的各种数据、密钥转换到新的主密钥下加密。一旦转换完毕，应立即清除旧密钥存储区（通过联机命令）。

具体过程如下图所示：

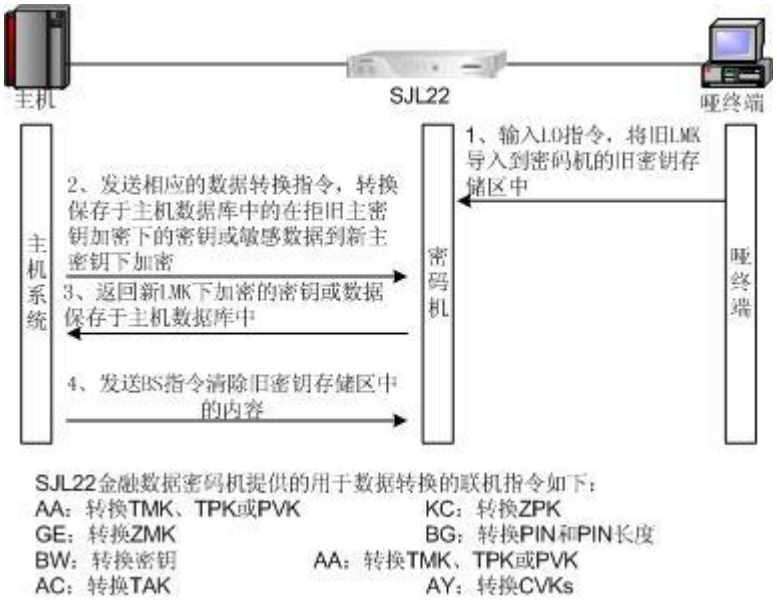


图 4-4 更新LMKs时数据转换流程

4.7 IC 卡管理机制

IC 卡（*本文中所有出现的 IC 卡均指智能 CPU 卡*）本身具有很高的安全性，在此基础上，SJL22-SM 金融数据密码机系列产品提供了完善的 IC 卡管理机制，具体如下：

卡片共分七类：

主密钥成份卡——提供空白卡由用户自行格式化。用于保存合成主密钥的

各个成份，2～9 个成份可选；主密钥成份生成时，可选择复制多个卡片作为备份保管。管理程序也提供了授权状态下复制主密钥成份卡的功能。

授　权　卡 ——提供空白卡由用户自行格式化。仅用于密码机的授权，不保存任何主密钥成份信息，不能复制，只能在主密钥成份卡（成份一、成份二或成份三）的持卡人的授权下才可完成授权卡的制作。

密钥成份卡 ——提供空白卡由用户自行格式化。用于保存除主密钥以外的其他各类密钥的成份，用于该密钥的合成，每一类密钥的成份数量由 1～9 或 2~9 个可选；密钥成份卡生成时可选择复制卡片以用于备份保管。管理程序也提供了授权状态下复制密钥成份卡的功能。

密钥存储卡 ——提供空白卡由用户自行格式化，用于保存用户/密钥存储区中的密钥。用户可有选择的备份指定索引区间内的密钥于密钥存储卡中。

测试密钥卡 ——由厂家产生，随机附带。用于保存测试用本地主密钥集合，该测试主密钥集合的每组密钥的明文可公开提供给客户，便于业务应用系统开发过程中的安全体系调试。

维护管理卡 ——由厂家产生，厂商专用。用于密码机核心程序的升级维护或功能配置管理。维护管理必须在密码机脱机状态下进行，也就是说密码机功能管理须在厂商授权的监督下使用。

程序升级卡 ——由厂家产生，厂商/代理商专用。用于密码机核心程序的升级维护管理。升级维护管理必须在密码机脱机状态下进行。

密码机随机附带多张（近 20 张）空白 IC CPU 卡片，客户可根据系统的安全需求制定相应的 IC 卡管理规范，如客户可自行定义卡片的类型，为卡片

进行格式化（个人化）管理，包括卡片的生成日期、用户标识、发卡机构标识、卡片类型标识、卡片保护口令等。为保护卡片的安全，卡片口令由持卡人自己选定并严格保管。所有的 IC 卡在使用时，均需要输入保护口令，一旦三次输入口令错误，卡片将被锁定并废弃原有功能。要使用被锁定的 IC 卡片，只能对卡片重新格式化。

4.8 TDEA 加密机制

随着计算机处理能力的飞速发展，对单长度密钥的破译很容易实现。由此，采用单长度密钥加密需要向双长度和三长度密钥加密过渡升级。

SJL22-SM 金融数据密码机系列产品联机指令支持单长度，双长度和三长度密钥的 TDEA 加密。

如果是单长度密钥，则直接用密钥进行加密或解密；如果是双长度密钥，加密的过程是用左半部分的密钥加密，再用右半部分密钥解密，最后再用左半部分密钥加密，解密过程相反；如果是三长度密钥，加密的过程是用第一部分密钥加密，再用第二部分密钥解密，最后用第三部分密钥再加密，解密过程相反。三长度 TDEA 加密支持标准的 ANSI X9.52 模式。

4.8.1 密钥标识

SJL22-SM 金融数据密码机系列产品的终端控制命令、主机指令是通过密钥的第一个字符来识别密钥长度的：

- 如果密钥的第一个字符是（0~9 或 A~F）的 16 进制字符，则该密钥为单长度密钥；当 ZMK 配置为双长度密钥时，ZMK 密钥第一个字符也是（0~9 或 A~F）的 16 进制字符，但仍被识别为双长度密钥。
- 如果密钥第一个字符是“K”、“I”、“k”或“i”,则表示密钥是以索引的方式存储在用户存储区或密钥存储区的单长度密钥。
- 如果密钥的第一个字符是除（0~9 或 A~F）的 16 进制字符、“K”和“I”以外，则该字符是密钥标识符（U、X——双长度；T，Y——三长度），用来标识密钥长度以及加密机制。密钥机制标识适用于双长度密钥

和三长度密钥加密，加密密钥必须是 LMKs 、双长度或三长度的输入/输出密钥。

4.8.2 密钥机制

ANSI X9.17 模式：

密钥机制的标识符如下：

X——双长度 DEA 密钥

Y——三长度 DEA 密钥

双长度或三长度密钥的每个密钥单独的采用 ECB 模式加密。这种机制只适用于密钥的输入/输出，需要配合终端控制命令 CS 来完成执行。

Variant 模式：

该密钥机制的标识符如下：

U——双长度加密密钥

T——三长度加密密钥

双长度或三长度密钥的每个部分均单独的采用 ECB 模式加密。根据被加密密钥是双长度密钥还是三长度密钥，采用不同的变种模式，对于双长度密钥，在密钥的右半部分进行变种；对于三长度密钥，在密钥的中间部分进行变种。变种模式共有 5 种。变种模式应用于双长度和三长度密钥加密。这种机制适用于 LMK 密钥下加密，以及密钥的输入/输出。

双长度密钥变种方式： 双长度密钥的第一部分—A6

双长度密钥的第二部分—5A

三长度密钥变种方式： 三长度密钥的第一部分—6A

三长度密钥的第二部分—DE

三长度密钥的第三部分—2B

例如：

1、双长度密钥：

给定的双长度加密密钥：XXXX XXXX XXXX XXXX YYYY YYYY YYYY YYYY

双长度密钥： AAAA AAAA AAAA AAAA BBBB BBBB BBBB BBBB

A6 与密钥的前两个字节 Y 异或后对密钥 AAAA AAAA AAAA AAAA 加密。

5A 与密钥的前两个字节 Y 异或后对密钥 BBBB BBBB BBBB BBBB 加密。

2、三长度密钥：

给定的双长度加密密钥：XXXX XXXX XXXX XXXX YYYY YYYY YYYY YYYY

三长度密钥： AAAA AAAA AAAA AAAA BBBB BBBB BBBB BBBB CCCC CCCC CCCC CCCC

6A 与密钥的前两个字节 Y 异或后对密钥 AAAA AAAA AAAA AAAA 加密。

DE 与密钥的前两个字节 Y 异或后对密钥 BBBB BBBB BBBB BBBB 加密。

2B 与密钥的前两个字节 Y 异或后对密钥 CCCC CCCC CCCC CCCC 加密。

5 产品基本结构

SJL22-SM 金融数据密码机系列产品整体结构的设计是基于平台式的设计思想，采用模块化的实现方式，主要由命令处理模块、命令解释模块、多个支持不同协议的通讯模块、密钥管理模块、升级模块、算法模块以及密钥存储模块等组成。密钥存储模块的设计采用具有侵入自动销毁功能的硬件装置，并和硬件设备的物理障碍（如：行程检测装置，开箱检测装置等）联动使用，密钥存储装置的容量取决于内置密码算法的数量。

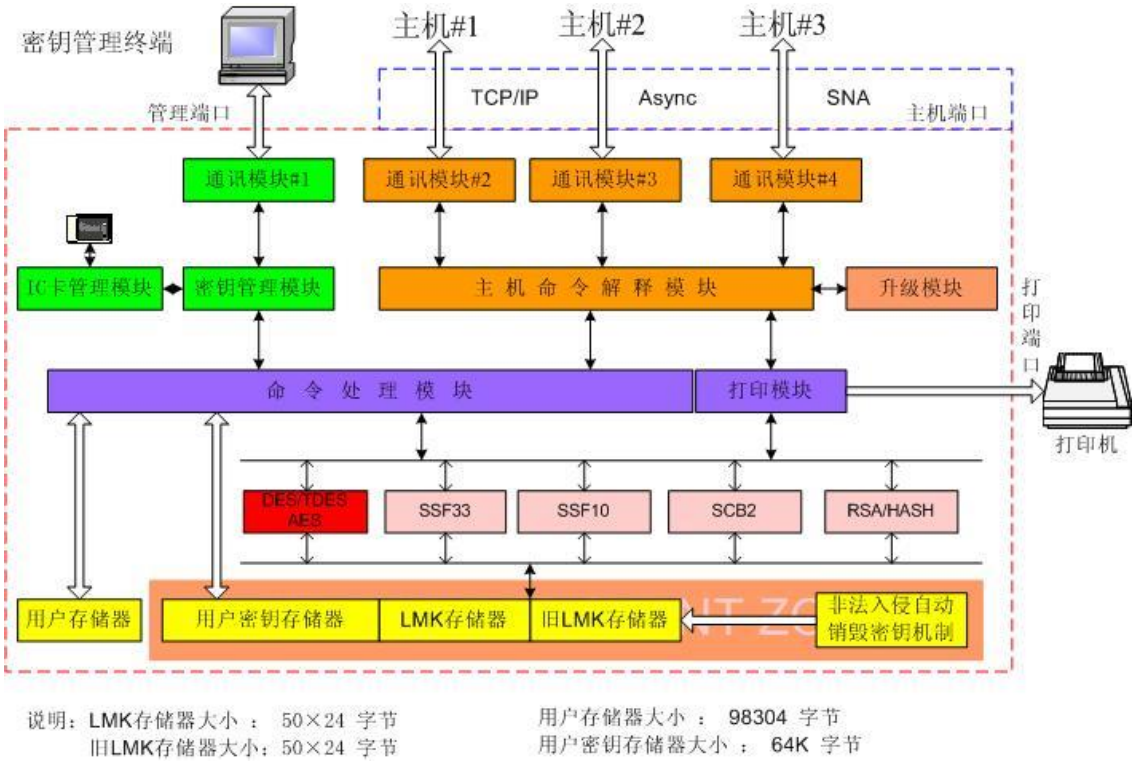


图 5-1 SJL22-SM金融数据密码机系列产品系统结构示意图

密码机系统模块与硬件模块共同实现了一个完整的 SJL22-SM 金融数据密码机系列产品系统。具体如下：

1、通讯模块

通信模块支持 ASYNC、SNA、TCP/IP 等通信协议，并可分析各种数据结构，实现和主机之间的通讯，TCP/IP 传输速率 10 Mbps、100 Mbps、1000 Mbps（根据用户要求特定）；ASYNC 传输速率 2400 bps 至 115200 bps 可配置。同时支持主机的多协议并行工作机制。

2、IC 卡管理模块

实现与 IC 读写器间的通讯，完成 IC 卡的读写功能。采用 IC 卡实现对密码机操作人员的身份验证以及授权管理。只有合法身份者才有权访问或产生密钥。配有两张或三张授权卡（依客户要求由厂商出厂时设定），分别由专人负责掌管。密码机进行关键的、敏感的操作时，需要由专人对密码机进行授权，在授权状态下执行。

3、密钥管理模块

与管理端口进行通讯，接收管理终端命令，在 IC 卡管理模块和命令处理模块的配合下，实现终端管理的各项操作。该模块主要完成两项工作: (1)密钥管理：产生 LMK 成份及导入；产生机内随机数，并通过运算和各种校验手段形成新的各类密钥，在相应的 LMK 下加密后提供给主机使用。(2)对密码机系统进行管理，如网络管理、打印管理、系统配置等等

4、主机命令解释模块

扫描并分析通讯模块接收的主机指令，并判断指令格式的正确性，如果不正确，返回相应错误类型的错误代码；如果指令格式正确，在命令处理模块的配合下，完成主机指令的调用。

5、升级模块

用于完成密码机各种核心程序的更新工作。

6、打印模块

配合主机命令解释模块，调用相应的算法模块，接收主机发送的打印指令，与打印机之间以并行或串行协议进行通讯，完成主机打印请求。如实现 PIN 明文、密钥明文打印到连接于密码机打印端口的打印机上。并行或串行打印模式可设置。

7、用户存储器

提供单独的物理存储区域，以索引的方式保存用户敏感数据或密钥于密码机中，密码机关机或重新启动后，用户存储区中的内容不存在。

8、密钥存储器

提供单独的物理存储区域，以索引的方式保存用户敏感数据或密钥于密码机中，密码机关机或重新启动后，密钥存储区中的内容仍然存在。其存储

内容在非法入侵自动销毁密钥机制的保护之下。

9、算法模块

密码机内置多种国家密码管理委员会批准使用的算法芯片,用于完成密码运算。为密码机的主要功能之一。由通讯的双方按约定密钥，采用某种算法对 PIN 进行加／解密及信息验证，以达到保护数据安全的目的。该设计支持多套加密算法是本机的一大特点。密码算法 1 和密码算法 2 均由硬件设计实现，因此运算速度快、可靠性高。用户在选购密码机时，可按需要安装一种算法或两种算法或多种算法。

10、命令处理模块

配合密钥管理模块以及主机命令解释模块完成密钥的访问、算法的调用，分析主机传入的函数数据内容，执行主机命令，调用各算法，完成加密、解密、验证、产生密钥等操作。

11、LMKs 存储器

密钥的存储采取了容错技术,针对不同的算法提供不同的密钥存储区域，LMKS 密钥器的内容在侵害自毁密钥机制的保护之下。

12、侵害自毁密钥保护模块

SJL22-SM 金融数据密码机系列产品设计为严格符合 FIPS 140-2 级别 3 的要求，使得密码机处在“警戒”的状态下，对于以下的情况提供对密码机内密钥的保护机制：来自网络中的扫描、探测，非法操作密码机、非正常的电压/温度波动以及移动密码机等。

6 产品技术特点

SJL22-SM 金融数据密码机系列产品，完全与国际上主流的 RACAL 加密体系应用级兼容，符合国际金融行业的安全规范。其所支持的功能具体如下：

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 X9.17/ANSI X9.31 标准
- 公开密钥算法采用 RSA（模长从 192 位至 2048 位连续可变）；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

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，支持国际主流制卡设备供应商 DataCard, NBS , G&D EMV 发卡命令集
- 支持 DUKPT（Derived Unique Key Per Transaction）派生每交易唯一密钥机制

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

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。

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。

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）*

主机接口

- 支持 TCP/IP 协议，10/100M 自适应,可根据客户特殊需求,扩充 1000M 以太网接口

- 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）*

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）

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 RACAL 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
- 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
- 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
- 支持公私钥对明/密文、PKCS#8 格式公私钥对明/密文以索引的方式导入、导出密码机
- 支持明/密文成份方式（如：p，q 两个成份、n，p 两个成份和 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***

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、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**
- **支持芯片卡（EMV 卡）联机验证及 Script Downloading 功能**
- 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 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

备注：带*的项目为 SJL22-SM 金融数据密码机系列产品加密体系区别于国际 RACAL 体系特有的功能与特点

7 系列产品说明

SJL22-SM 金融数据密码机系列产品包括高端（专用型和通用型）、中端、低端（网点型）三个档次，支持多应用安全体系，包括兼容 RACAL 兼容指令集、IC 应用指令集、JK 指令集以及手机银行相关指令集。各档次产品在安全机制、处理性能等方面稍有不同之处，下面主要从这两方面详细对比说明：

7.1 磁条卡安全体系密码机

1、 物理安全机制

表 7-1物理安全机制对照表

对比内容	高端产品	中端产品	低端产品
FIPS140-2 级别三的要求	符合 在警戒状态下掉电/开箱均销毁密钥	符合 掉电不销毁密钥 不论何种状态下开箱均销毁密钥	符合 掉电不销毁密钥 不论何种状态下开箱均销毁密钥
操作面板物理锁	专用型：有 通用型：无	无	无
机箱锁/锁防护装置	专用型：两把/无 通用型：两把/有	一把/有	一把/有
硬件的密钥存储部件	存储密钥/参数	存储密钥/参数	存储密钥/参数
硬件的算法部件	SSF33/SSF10/SCB2 DES/TDES/AES RSA SHA-1， SHA-224，SHA-256，SHA-384，SHA-512，MD2，MD4，MD5，RIPE-MD128，RIPE-MD160，RIPE-MD256，RIPE-MD320，ISO-10118-2	SSF33/SSF10/SCB2 DES/TDES/AES RSA SHA-1， SHA-224，SHA-256，SHA-384，SHA-512，MD2，MD4，MD5，RIPE-MD128，RIPE-MD160，RIPE-MD256，RIPE-MD320，ISO-10118-2	DES/TDES/AES SHA-1， SHA-224，SHA-256，SHA-384，SHA-512，MD2，MD4，MD5，RIPE-MD128，RIPE-MD160，RIPE-MD256，RIPE-MD320，ISO-10118-2 HMAC-SHA-1，HMAC-SHA-224，HMAC-SHA-256，

	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	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	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
采用双重保护机制	有	有	有
随机数生成方式	硬件+伪随机数	硬件+伪随机数	硬件+伪随机数
密码/密钥信函打印	串口/并口	串口/并口	可订购并口
主机通讯协议	TCP/IP Async Transparent Async	TCP/IP Async Transparent Async	TCP/IP

2、 功能性安全机制

表 7-2功能性安全机制对照表

对比内容	高端产品	中端产品	网点型产品
密码机的工作状态	12 种	12 种	12 种
密码机的授权机制	2 或 3 人 智能卡/口令	2 或 3 人 智能卡/口令	2 或 3 人 智能卡/口令
应用安全功能	可包含 PIN 加密指令	可包含 PIN 加密指令	包含 PIN 加密指令，但不包含密码信函打印指令

3、 处理性能以及物理参数

表 7-3 性能参数对照表

对比内容		高端产品	中端产品	网点型产品
采用 TCP/IP 协议通讯时的吞吐量：（以 VISA PVV 验证例）		≥7000 次/秒	≥4500 次/秒	≥900 次/秒
电器参数	最大功耗	最大 50W	最大 35W	最大 15W
物理参数	实际尺寸 单位：mm	专用型 450×430×88 通用型 450×430×68	365×430×68	345×215×68
	重量	8KG	8KG	4KG
	颜色	黑+银白色	黑+银白色	黑+银白色
环境参数	工作温度	0℃~50℃	0℃~50℃	0℃~50℃
	储藏温度	-40℃~60℃	-40℃~60℃	-40℃~60℃
	相对湿度	5%~90% 非凝结	5%~90% 非凝结	5%~90% 非凝结

7.2 IC 卡安全体系密码机

表 7-4 IC卡体系密码机对照表

对比内容		高端产品	中端产品	网点型产品
应用功能		可扩充发卡命令	可扩充发卡命令	不提供发卡命令
采用 TCP/IP 协议通讯时的吞吐量：（以 128 字节 ANSI X9.9 MAC 验证例）		≥9000 次/秒	≥6000 次/秒	≥1100 次/秒
电器参数	最大功耗	最大 50W	最大 35W	最大 15W
物理参数	实际尺寸 单位：mm	专用型 450×430×88 通用型 450×430×68	365×430×68	345×215×68
	重量	8KG	8KG	4KG
	颜色	黑+银白色	黑+银白色	黑+银白色
环境参数	工作温度	0℃~50℃	0℃~50℃	0℃~50℃
	储藏温度	-40℃~60℃	-40℃~60℃	-40℃~60℃
	相对湿度	5%~90% 非凝结	5%~90% 非凝结	5%~90% 非凝结

7.3 SJL22-SM 高端金融数据密码机

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。

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

7.3.1 SJL22-SM 高端产品前视外形图

图 7-1 SJL22-SM高端专用型前视图

图 7-2 SJL22-SM高端通用型前视图

7.3.2 SJL22-SM 高端产品前视整体外形图

图 7-3 SJL22-SM高端通用型整体视图

7.3.3 SJL22-SM 高端背视外形图

图 7-4 SJL22-SM高端通用型背视图

7.4 SJL22-SM 中端金融数据密码机

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。

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

7.4.1 SJL22-SM 中端前视外形图

图 7-5 SJL22-SM中端前视图

（外观专利号：ZL2004 3 0078726.4）

7.4.2 SJL22-SM 中端背视外形图

图 7-6 SJL22-SM中端背视图

7.5 SJL22-SM 金融数据密码机（网点型）

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。

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

7.5.1 SJL22-SM 网点型前视外形图

图 7-7 SJL22-SM网点型前视图

7.5.2 SJL22-SM 网点型背视外形图

图 7-8 SJL22-SM网点型后视图

8 系列产品应用

在银行卡信息安全保密方案中，硬件密码机是实现数据安全的关键（主要）部件，VISA/MasterCard 国际信用卡组织把它作为对入网用户考察的主要标准之一。硬件密码机是独立的、物理保密的、具有较高智能程度的专用密码装置。在其内部可实现金融通信网络所需要的各种密码功能。它作为主机型的加密设备与主机通过特定的通讯协议相连，快速完成主机所要求的各种安全功能要求。

8.1 密码机在金融业务网络中的应用

✧ 金融卡/折业务应用环境典型实例

典型的银行信用卡网络及密码机在网络中配置的拓扑结构可由下图所示。

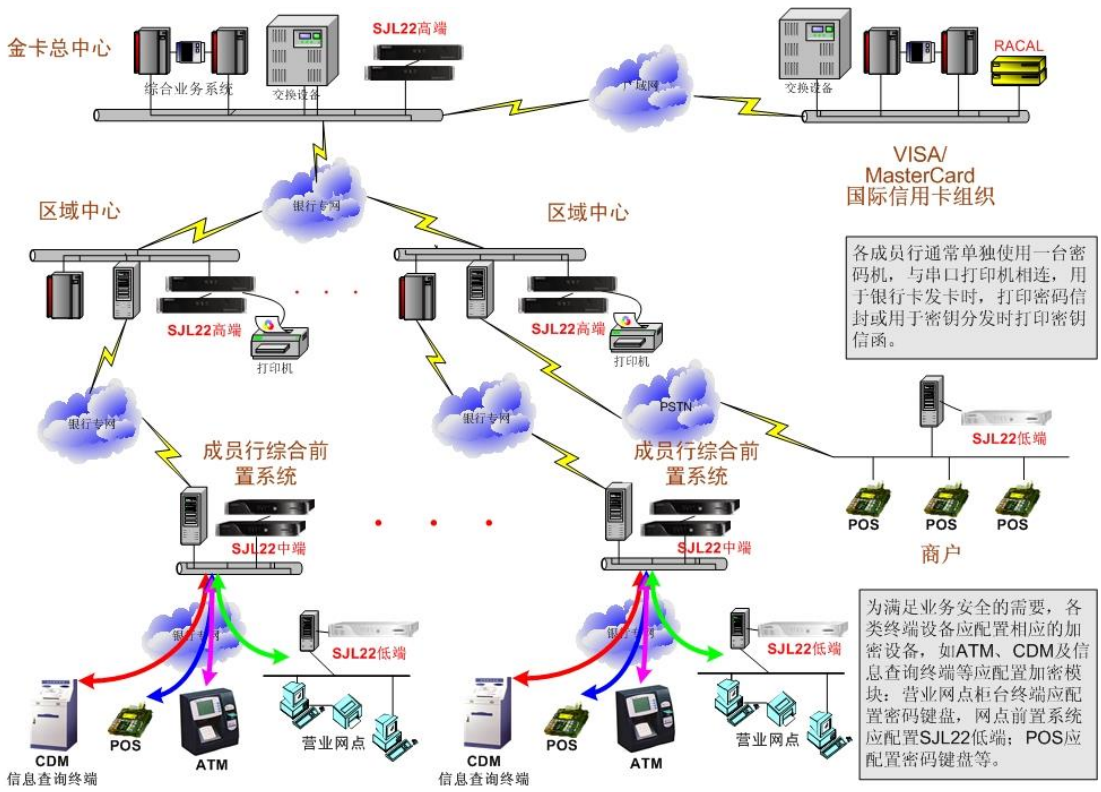


图 8-1 金融业务网络中密码机应用拓扑结构图

某个银行的 ATM、POS、CDM，*Information Terminal* 等自助服务终端均联结到本行的综合前置系统上，综合前置系统连到银行的业务主机上，各银行再上连

到交换中心主机系统上。

对整个网络而言，传输线路、主机、终端都是密码机安全防护的重点。因此要保证整个信用卡网络的安全，保证整个网络不出现可攻击的薄弱环节，密码机必须配置在交换中心主机、银行主机、商户 MIS 系统主机、ATM（可用带加密功能的 ATM ）、POS（可用带加密功能的 POS ）上，即网络的所有主要节点上。 不允许有密码盲区（或点）在网中出现，否则，将危及全网的安全。

SJL22-SM 金融数据密码机系列产品作为主机型的安全设备， 以 ASYNC、SNA 或 TCP/IP 协议与主机连接。每个节点上的主机可按照业务量的大小配置两台（其中一台热备份）或两台以上的密码机，供主机业务应用调用。

采用 SJL22-SM 金融数据密码机系列产品作为商业银行业务网络中的应用密码设备的最大优点是：**除和其他厂商的密码设备互联互通外，采用和 RACAL 密码机兼融的高速密钥变种机制使得 SJL22-SM 金融数据密码机系列产品自身形成一套封闭的密码体系，大大增强了金融业务系统的安全性**。

✧ **IC 卡应用环境典型实例**

下图为SJL22-SM 金融数据密码机系列产品在IC 卡应用业务中的典型应用示范：

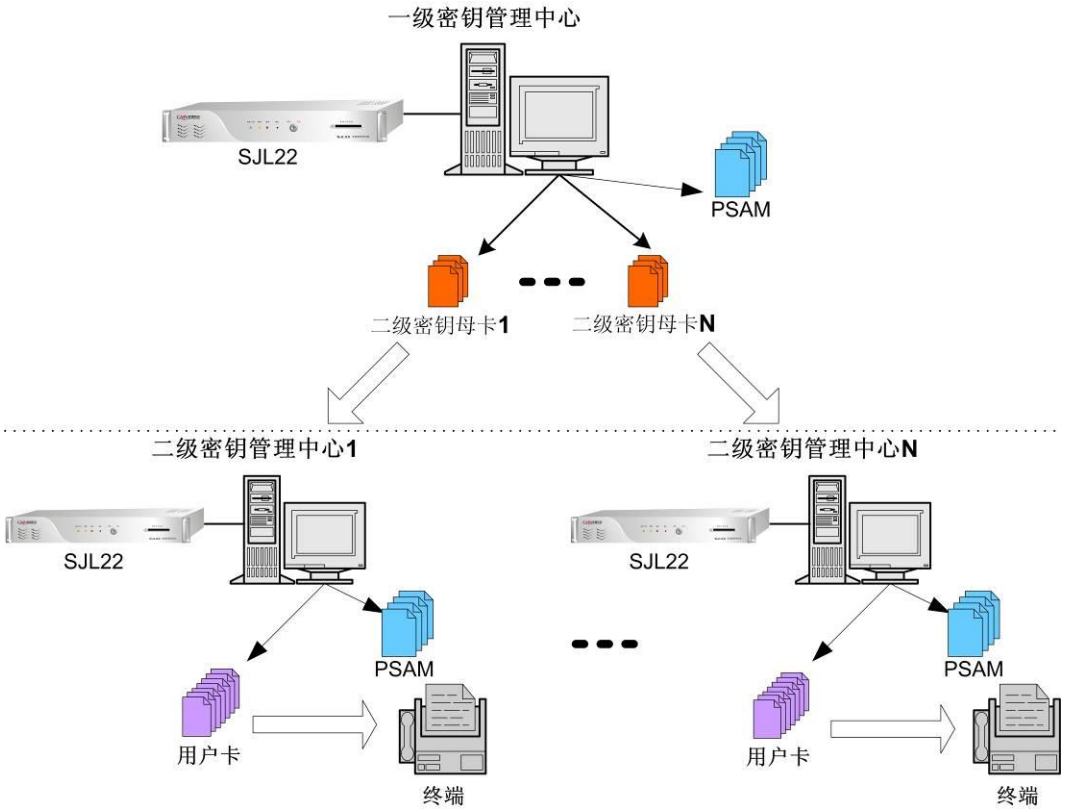


图 8-2 金融IC卡发卡业务中密码机应用拓扑结构图

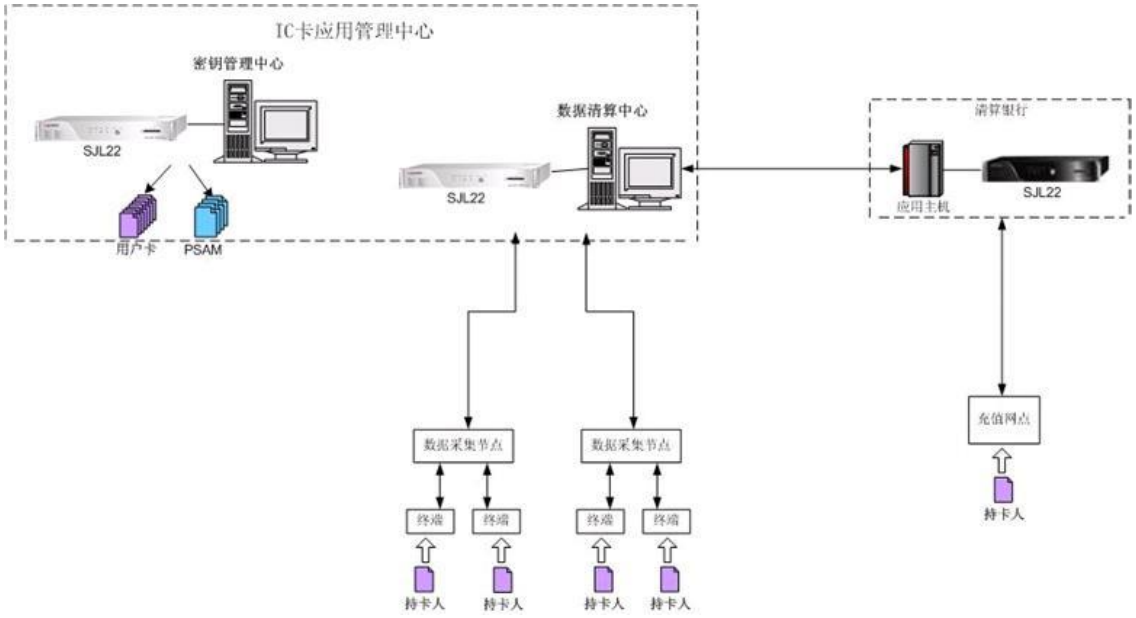


图 8-3 金融IC卡电子钱包业务中密码机应用拓扑结构图

✧ 代发卡业务应用环境典型实例

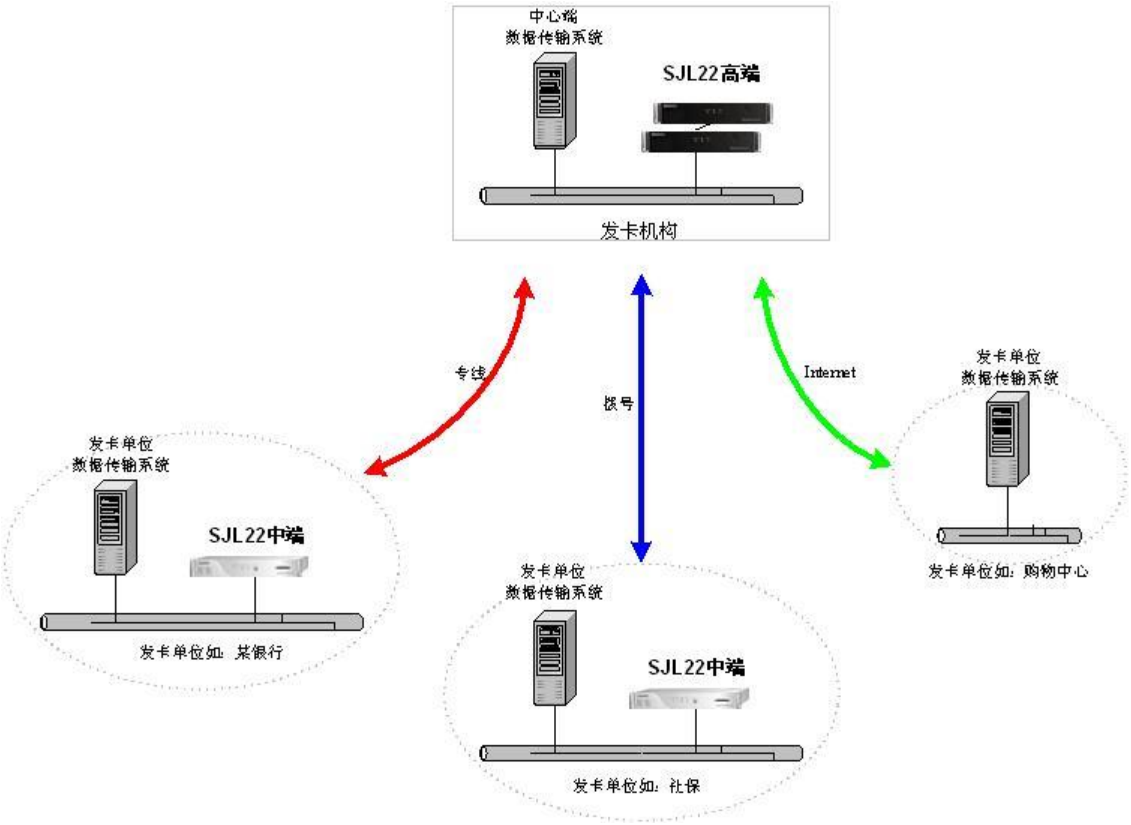


图 8-4 代发卡业务中密码机应用拓扑结构图

8.2 系列产品在金融业务网络中的主要作用

传统的金融数据密码机在保证金融数据安全上，围绕着数据的**私密性**和**完整性**，提供了相应的办能，这在一定程度上满足了 PIN 在传输和存储过程中的安全性以及报文的完整性。随着金融信息技术的飞速发展，关键敏感的数据既要在金融网络中频繁的传输交换、又要在应用系统数据库中进行存储。因此，保证金融信息在传输以及存储过程中，不会被非法窃取与篡改也是保障金融信息安全的一个重要组成部分。

SJL22-SM 金融数据密码机系列产品基于金融交易信息安全的需求，提供的主要功能是：保证信息的私密性和完整性，保证交易信息的**安全传输**以及金融敏感数据的**安全存储**。具体如下：

发卡过程：

1. 产生 PIN 并加密 PIN 保存于主机数据库中
2. 产生 VISA PVV、CVV/MasterCard CVV/美国运递 CSCK
3. 加密存储 PIN，提供多种 PIN 的存储方式
4. 打印密码信封或用户 PIN 申请函

交易过程：

1. 加密传输 PIN、在网络节点中转换 PIN
2. 提供不同加密模式的敏感数据加密传输
3. 提供消息鉴别码的产生、验证等，遵循 ANSI X9.9、ANSI X9.19 标准
4. 验证 VISA CVV 以及 MasterCard CVC/美国运通 CSC
5. 依据 PIN 的存储方式进行 PIN 的校验

密钥管理：

1. 产生随机密钥，遵循 ANSI X9.17 标准
2. 可产生并打印密钥成份，用于合成密钥令及密钥的分发
3. 提供密钥及敏感数据的安全存储机制
4. 加密密钥可同时支持 64、128、192 比特密钥，加密算法遵循 ANSI X3.106 标准
5. 提供密钥的校验、转换以及产生

8.3 系列产品工作过程简述

确保银行卡业务的安全，保证发卡行能正确的识别、受理用户的合法交易，PIN 作为一个关键要素，必须做到从发卡到交易的任何过程，均不能以明码的形式出现在 SJL22-SM 金融数据密码机系列产品以外的任何地方。

确保金融计算机网络的安全行之有效，必须做到任何人都不可能从计算机内或 SJL22-SM 金融数据密码机系列产品内得到有用的加密密钥。

SJL22-SM 金融数据密码机系列产品在银行卡业务网络中的工作流程可分三种情况描述如下：

发卡过程：

图 8-5 密码信封打印连接示意图

1、 SJL22-SM 金融数据密码机系列产品接到主机产生用户 PIN 的命令后，在内部用随机数自动产生(随机数产生附合 ANSI X9.17)一个 PIN 值；

2、 SJL22-SM 金融数据密码机系列产品在内部将 PIN 用 LMK_{02-03} 加密，把 PIN 的密文输出送给主机，主机接收后存入用户数据库中；

3、 主机调用 SJL22-SM 金融数据密码机系列产品指令将 PIN 的明码输出到通过串口或并口连在 SJL22-SM 金融数据密码机系列产品的专用打印机，打印在密码信封上。

密钥管理：

1、 LMK 的管理：

SJL22-SM 金融数据密码机系列产品投产时，首先产生并保存主密钥 LMKs 成份到 IC 卡上，（各类密钥的定义及使用，请参见第四部分：密钥管理）。在由 IC 卡导入到密码机中。LMKs 一旦在 SJL22-SM 金融数据密码机系列产品内形成，则永远不会以明文的形式出现在 SJL22-SM 金融数据密码机系列产品之外，亦不允许从密码机中导出。

LMKs 通常是 2 至 3 年更换一次。

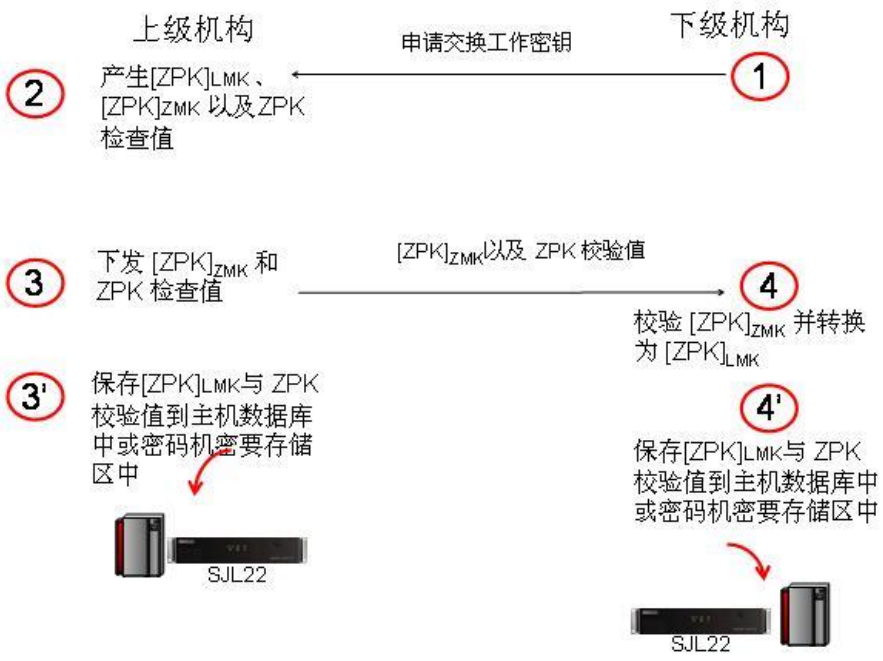
2、 ZMK/TMK 的管理

由通讯的双方协商产生 ZMK、TMK 密钥的方式。如果 ZMK、TMK 由 SJL22-SM 金融数据密码机系列产品生成，***可保存在密钥成份 IC 卡上或打印在密码信封上进行分发。***由通讯的双方分别通过终端的密钥管理方式在密码机内合成 ZMK 或 TMK 后，以密文的形式保存于各自的主机数据库中或密钥存储区中，供主机调用。

ZMK、TMK 通常是 1 至 2 年更换一次。

3、 工作密钥分发

工作密钥的分发通常分为下级机构申请或上级机构主动下发，下面主要以下级机构主动申请的模式进行阐述(假设通讯的双方已存在一个共同的 ZMK):



典型的密钥交换流程

图 8-6 工作密钥的在线分发

其他工作密钥的的分发流程与上述过程基本相同。

交易过程：

下图以一笔由自助终端—前置系统—帐务主机的交易为例，来说明典型的银行卡业务交易的安全流程。

图 8-7 典型的交易流程

1、 调用加密模块指令，用 TPK 加密 PIN

2、 调用加密模块指令，对关键数据用 TAK 产生 MAC

3、 前置系统调用密码机指令，用 TAK 对发送过来的报文验证 MAC

4、 如果验证 MAC 通过，调用密码机指令转换 PIN 由 TPK 加密为 ZPK 加密

5、 调用密码机指令用 ZAK 产生新的 MAC,发往帐务主机系统

6、 帐务主机系统调用密码机指令，用 ZAK 验证 MAC

7、 如果验证 MAC 通过，调用密码机指令进行 PIN 的校验

8、 对返回报文调用密码机指令用 ZAK 生成 MAC 发送给前置系统

9、 前置系统验证并转换 MAC（用 ZAK 验证，再用 TAK 生成），把报文发送给自助终端

10、自助终端用 TAK 验证 MAC,MAC 通过，受理此次交易，否则，返回拒绝受理的应答。交易中的应答消息不做加密，只做 MAC 验证。

以上描述是一种简化的银行卡交易模式，实际的金融交易业务流程多种多样，可根据具体的交易模式决定 SJL22-SM 金融数据密码机、终端加密模块

的配置以及密钥管理方式（如密钥的产生、分发、使用、保存等等），以确实保证金融交易的安全性。

9 主要性能指标

处理性能					
测试项目	数据长度	进程数	性能（笔/秒）		
			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 字节	4	>9000	>6000	>1100
MAC（ANSI X9.9）	256 字节	4	>8000	>5200	>1000
MAC（ANSI X9.9）	512 字节	4	>6400	>4000	>900
MAC（ANSI X9.19）	128 字节	4	>7000	>4500	>900
MAC（ANSI X9.19）	256 字节	4	>6500	>4000	>800
MAC（ANSI X9.19）	512 字节	4	>5200	>3200	>700
备注	主机：Linux 系统；Intel Pentium 4 CPU 2.60GHz；Memory 256M；长连接模式测试				

10 EMV 2000 项目迁移

本功能只有对选购了高速 RSA 加密部件才有效。

10.1 支持 RSA 功能

1、 支持 RSA 加密、解密功能

SJL22-SM 金融数据密码机能够实现 192 位—2048 位之间任意模长 RSA 公私钥加解密功能。

2、 支持 RSA (填充方式支持 PKCS#1,OAEP,PSS,ANSI X9.31,EMV2000 等)数字签名（SHA-1，SHA-224，SHA-256，SHA-384，SHA-512，MD2，MD4，MD5， RIPE-MD128， RIPE-MD160， RIPE-MD256， RIPE-MD320，ISO-10118-2）、认证功能

3、 支持 HMAC 算法：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

4、 支持公私钥对生成功能

SJL22-SM 金融数据密码机支持 192 位—2048 位之间任意模长 RSA 公私钥生成。

5、 支持随机数生成功能

SJL22-SM 金融数据密码机内部有物理噪声源发生器，可以生成满足要求的随机数。

6、 公私钥对导入导出密码机

支持公私钥对明/密文、PKCS#8 格式公私钥对明/密文以索引的方式导入、导出密码机

7、 公私钥对保存

SJL22-SM 金融数据密码机可内部保存公私钥 11 对（2048 位密钥）

10.2 RSA 性能指标

（一）B 算法加速卡 RSA 性能指标		
1．RSA 加密、解密	1024 位私钥	>= 180 次/秒
	公钥（65537/1024）	>= 2700 次/秒
	2048 位私钥	>= 50 次/秒
	公钥（65537/2048）	>= 90 次/秒
	公钥（3/2048）	>= 700 次/秒
2．RSA 签名、认证	1024 位私钥	>= 180 次/秒
	公钥（65537/1024）	>= 2700 次/秒
	2048 位私钥	>= 50 次/秒
	公钥（65537/2048）	>= 90 次/秒
	公钥（3/2048）	>= 700 次/秒
3．RSA 密钥对生成	1024 位(65537)	210 对/分钟 （由非强素数生成公私钥对）
	1024 位(65537)	150 对/100 秒 （由强素数生成公私钥对）
	2048 位(65537)	35 对/分钟（由非强素数生成公私钥对）
4．数据摘要算法	MD5 算法	55Mbps
	SHA1 算法	55Mbps

（二）A 算法卡 RSA 性能指标		
1．RSA 加密、解密	1024 位私钥	>= 2 次/秒 纯软件 >= 2.5 次/秒
	公钥(65537/1024)	>=150 次/秒 纯软件 >= 300 次/秒
	2048 位私钥	纯软件 >= 1 次/2.5 秒
2．RSA 签名、认证	1024 位私钥	>= 2 次/秒 纯软件 >= 2.5 次/秒
	2048 位私钥	纯软件 >= 1 次/2.5 秒
	公钥(65537/1024)	>= 150 次/秒 纯软件 >= 300 次/秒
3．RSA 密钥对生成	1024 位	1 对/3 秒 （由非强素数生成公私钥对）
4．RSA 密钥对生成	1024 位	1 对/5 分钟（由强素数生成公私钥对）
5．数据摘要算法	MD5 算法	55Mbps
	SHA1 算法	55Mbps

10.3 支持的 RSA 标准

1、支持全部标准 RACAL RSA 指令集，如 ES、EY 指令等

2、支持全部标准 RACAL EMV2000 发卡指令集

3、支持 PKCS#1，OAEP，PSS，ANSI X9.31，EMV 2000 等数据填充模式

4、支持无符号及有符号整型两种公私钥 DER 编码

5、支持强素数的生成和基于强素数的公私钥生成

6、支持 CRT 模式运算

10.4 支持的 EMV 发卡体系

1、 Datacard 公司 EMV 发卡体系

2、 NBS 公司 EMV 发卡体系

3、 G & D 公司 EMV 发卡体系

11 主要业绩

- **中国工商银行 澳门分行**选用 GM1130 金融数据密码机应用于打印密码信函业务
- 南京地铁项目中使用 SJL22-SM 金融数据密码机
- 东亚银行(中国)有限公司在银联人民币收单项目中使用 SJL22-SM 金融数据密码机
- **中国工商银行亚洲有限公司(香港)**选用 SJL22-SM 金融数据密码机和 GM1130 金融数据密码机应用于网上银行(Internet Banking)，JETCO，EPSCO,ATM 及核心业务
- **与神州数码融信软件有限公司**合作成功启动宁夏自治区农村信用联社卡中心项目
- 中标**廊坊市财税库行横向联网**项目安全集成
- 沧州市一卡通项目选用 SJL22-SM 金融数据密码机
- **SJL22-SM 金融数据密码机获 2006 年度密码科技进步奖（省部级）**
- 三门峡市商业银行选用 SJL22-SM 金融数据密码机作为业务系统核心设备
- 河南省农村信用联社采用 SJL22-SM 金融数据密码机
- 保定市城市信用社采用 SJL22-SM 金融数据密码机
- 中国石油天然气股份有限公司大连分公司加油卡项目选用 SJL22-SM 金融数据密码机
- “天津电子商务统一支付平台”中使用 SJL22-SM 金融数据密码机
- 柳州市商业银行“银行卡业务系统”采用 SJL22-SM 金融数据密码机
- 洛阳市商业银行采用 SJL22-SM 金融数据密码机

- 丹东市商业银行采用 SJL22-SM 金融数据密码机
- 华北电网有限公司采用 SJL22-SM 金融数据密码机
- 湖北省两网互通工程中湖北省邮电局银联 2.0 系统改造项目选用 SJL22-SM 金融数据密码机
- 中国金融认证中心选用 SJL22-SM 金融数据密码机作为新一代中国金融认证根 CA（认证中心）的唯一密码设备
- 天津市地下铁路系统选定使用 SJL22-SM 金融数据密码机
- 重庆市市政交通一卡通项目选用 SJL22-SM 金融数据密码机
- 北京工业大学开始使用 SJL22-SM 金融数据密码机作为信息安全密码技术专用教学设备
- SJL22-SM 金融数据密码机成为中国工商银行 EMV 迁移项目中唯一使用的密码机

12 SJL22-SM 金融数据密码机系列与同类产品比较

金融数据密码机是用于保障金融业务安全的硬件密码设备，不仅要提供完善的、满足业务应用安全需求的各项功能，而且在自身的安全性设计上也应具有符合国际标准的安全机制。同时，密码机还必须具备高稳定性、高可靠性，以适应金融业务系统的连续性、实时性这一特点。

以下主要从密码机的物理安全机制、逻辑安全机制以及提供给应用系统的安全功能等几个方面，把 SJL22-SM 金融数据密码机与国内其他主流密码机进行比较，此章内容不作权威性比较，仅供参考。

一、 加密算法：

比较内容	SJL22-SM	国内其他厂商
1. 国家专用算法“SSF33 / SSF10 / SCB2”与“DES /3DES /AES”之间数据加密的转换功能	完全实现	不支持
2. 数据加密算法	符合 ANSI X3.92-1981 标准	符合
3. 三重数据加密算法	操作模式符合 ANSI X9.52-1998 标准	未知
4. 密钥管理标准	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	未知
5. 随机数生成方式	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	未知
6. 公开密码算法及数字签名算法	公开密码算法采用 RSA（模长从 192 至 2048 位连续可调）；填充模式支持：PKCS#1 v1.5，OAEP，PSS，ANSI X9.31 及 EMV2000 等；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	公开密码算法采用 RSA； 支持少数数字签名算法
7. HMAC 算法	支持 HMAC-SHA-1，HMAC-SHA-224，	不支持

	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	

二、 密钥管理机制

比较内容	SJL22-SM	国内其他厂商
1. 专钥专用	密码机内共保存有 50 组本地主密钥（Local Master Key，简称 LMK）	少于 30 对
2. LMK 的长度	192bits	128bits
3. LMKs 的产生	由 2~9 个成份合成，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，密码机产生 LMK 成份后，保存于专人保管的 IC-CPU 卡中。密码机投产时，再由成份卡导入到密码机中合成。***密码机不提供主密钥/成份的导出功能。***	由 3 个成份合成，在密码机内产生并保存，然后再由密码机导出至 A/B 卡中保存
4. LMK 成份的生成要素	由秘密值 A、B、C、成份序号、时间因子五个因子生成	由两个因子生成
5. LMK 存储介质	IC-CPU 卡，并采用完整性校验机制，以保证主密钥的一致性	逻辑存储卡
6. LMK 更新时数据的转换机制	提供，方便业务系统密钥更新	不支持
7. ZMK	ZMK 支持 64/128/192 位长度，并提供多种 ZMK 产生方式，具有安全的在线更新 ZMK 机制	不完善
8. TDEA 变种加密、LMK 变种加密以及 ZMK/TMK 单字节、双字节 ATALLA 变种密码机制	支持	不支持或不完善
9. ANSI X9.17 加密方式下，密钥的安全导入导出机制	支持	不支持或不完善
10. 密钥管理操作模式	采用字符终端的密钥管理模式，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	1、密码机面板操作模式，额外的零配件，降低了设备的稳定性和可靠性。

	语言中的任一种	2、Windows 终端管理方式，增加了不安全因素。
11. 密钥管理与联机交易并行处理	可以	不可以
12. 敏感数据以及 LMK 加密下的密钥存储模式	可保存在主机数据库中，或保存在密码机内的***密钥存储区***或***用户存储区***中。在密钥存储区存储的密钥索引标识为“**I，i**”，；在用户存储区中的索引标识为“**K，k**”。	保存在主机数据库中
13. VISA Chip Card 专用命令及 EMV 发卡指令	支持 VISA Chip Card 专用命令，支持国际主流制卡设备供应商 DataCard、NBS、G&D EMV 发卡命令集，***并成功应用于中国工商银行 EMV 发卡项目中***	不完善，无应用案例
14. DUKPT 派生每交易唯一密钥机制	支持（Derived Unique Key Per Transaction）DUKPT 派生每交易唯一密钥机制	不支持
15. 三层密钥管理体系	支持	不完善

三、 PIN、MAC 及 CVV

比较内容	SJL22-SM	国内其他厂商
1. PIN 长度 4~12 可配置	支持	功能不完善或固定 PIN 长度为 6
2. IBM 3624 PIN 加密及验证	支持	不完善
3. 支持的 PIN 数据块加密格式及密钥长度	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	提供 5 种格式，不能保障其正确性
4. 支持的卡校验方式	持 VISA PVV/CVV 及 MasterCard CVC 生成及验证、***扩展的美国运通 CSC 三种方式***	VISA CVV
5. MAC 的生成及验证	支持不同格式数据以 ANSI X9.9/ANSI X9.19 的方式生成及验证 MAC，***可自动根据密钥的长度选择 MAC 两种生成方式之一；支持多种 MAC 生成方式***	功能不完善
6. PIN 加密算法	内置两种 PIN 的加密算法。可根据用户特殊需求扩充 PIN 加密算法。	一种

四、 传输与存储加密

比较内容	SJL22-SM	国内其他厂商
1. 传输加密	提供应用系统报文加密传输的功能，支持	功能不完善

	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	
2. 数据安全存储	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），灵活的实现了大数据块的报文，以密文的方式在某个 LMK 下，或某个 LMK 下加密的数据密钥 DSK 下（Data Storage Key）加密存储	无

五、 主机接口

比较内容	SJL22-SM	国内其他厂商
1. TCP/IP 协议	支持 TCP/IP 协议，10/100M 自适应，可根据客户需求扩充 1000M 以太网接口	支持 TCP/IP 协议 10/100M 自适应
2. 跨网段访问时网关设置功能	支持	支持
3. 业务主机访问密码机的 IP 地址过滤和 MAC 地址绑定功能	支持	不支持
4. TCP 套接字连接数量	可配置，最大 4096 个连接	无配置功能，中端产品仅支持 8 个连接
5. 异步协议	支持标准的异步协议以及异步透明传输协议（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	功能不完善或固定通讯格式（8N1）
6. 多协议并行工作	具备独立的密钥管理端口、主机端口、串/并行打印端口。支持多种通讯协议并行工作，最多可同时支持 TCP/IP，Async，SNA 三种通讯协议	未提供或功能不完善

六、 稳定性及安全性

比较内容	SJL22-SM	国内其他厂商
1. 符合 FIPS140-2 LEVEL 3 标准	符合，如打开机箱即清除其内的密钥	开机箱不清密钥
2. 工作状态	设计有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主密钥	-

	（Tamper-Resistant Mechanism）	
3. 工作模式	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	-
4. 关键命令及密钥导入/导出/转换等管理命令在授权状态下处理	支持，并提供授权配置功能	不支持
5. 授权机制	支持 IC 卡/口令字两种授权方式，授权方式可配置。***授权卡以及口令字与 LMK 成份密切相关，用户可选择 2 人或 3 人授权***	卡授权，授权卡与主密钥成份无关，授权卡通用。
6. 双重授权机制	支持	无
7. 双重保护机制	支持	无
8. IC 卡管理功能	支持七种卡片（IC-CPU 卡）： 主密钥成份卡、 密钥成份卡、 授权卡、 密钥存储卡、 测试密钥卡（128/192bits）、 维护卡（厂家专用） 升级卡	支持三种卡片（存储卡）： A 卡 B 卡 C 卡

七、 打印功能

比较内容	SJL22-SM	国内其他厂商
1. 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*；支持密码信函、密码申请信函及密钥信函打印功能	功能不完善，某些特殊字体无法打印
2. 打印端口	打印时使用串行端口或并行端口可配置*，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）；打印机的使用厂商可配置	功能不完善或不支持
3. 打印条形码	支持 HP 兼容的激光条形码打印	不支持
4. 一行两个信函	支持一行打印两个密码信函	不支持
5. 管理端口打印信函	支持管理终端打印密码信函、密钥信函功能	不支持

八、 RSA 相关功能

比较内容	SJL22-SM	国内其他厂商

1. RACAL RSA 指令集	支持全部标准 RACAL（THALES）RSA 指令集，如 ES、EY 指令等	功能不完善
2. RACAL EMV2000 发卡指令集	支持全部标准 RACAL EMV2000 发卡指令集	未知
3. 填充标准	支持多种填充标准，如 PKCS#1，OAEP，PSS，ANSI X9.31，EMV 2000 等数据填充模式	不完善
4. 公私钥 DER 编码	支持无符号及有符号整型两种公私钥 DER 编码	未知
5. 强素数生成	支持强素数的生成和基于强素数的公私钥生成	不完善
6. CRT 模式运算	支持 CRT 模式运算	不完善
7. RSA 签名、验证及加解密运算	支持对数据进行 RSA 签名、验证及进行 RSA 加解密运算	不完善
8. 公私钥对的导入导出	支持公私钥对明/密文、PKCS#8 格式公私钥对明/密文及以索引的方式导入、导出密码机	未知
9. RSA 密钥对导入	支持明/密文成份方式（如：p，q 两个成份、n，p 及 n，q 两个成份等）的 RSA 密钥对导入	未知
10. 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	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	不完善
11. 性能指标	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	未知
12. 支持的 EMV 个人化系统	**支持 DataCard、NBS 及 G & D EMV2000 卡个人化系统安全需求**	部分支持，且不完善，没有应用案例

九、 其他功能

比较内容	SJL22-SM	国内其他厂商
1. 消息头	支持消息头处理，消息头长度 0~255 可配置	支持消息头处理
2. 消息尾	支持消息尾处理功能（可选项），最大长度 128 字节	不支持
3. 支持的字符集	ASCⅡ、EBCDIC 及 IBM1388 三种字符集可配置	ASCⅡ、EBCDIC 两种字符集可配置，功

		能不完善
4. 多安全体系支持	***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）应用体系、IC 卡应用安全体系、网上银行应用安全体系、PKI 应用安全体系及 EMV 96/2000 标准安全体系等。IC 卡应用体系根据属性定义一套命令体系同时支持 PBOC，建设部，劳动和社会保障部及石油加油卡等行业规范。	不支持
5. 多字符集 MAC 处理及报文加密	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	不完善
6. EMV 迁移安全需求的支持	支持多个个人化厂商的个人化发卡系统，支持 VISA、MasterCard 以及 PBOC2.0 三种 EMV 卡的卡片个人化安全需求。	功能不完善，尤其是 RSA 密钥对管理及使用上。
7. 特殊应用安全支持情况	支持香港网上银行，JETCO（银通），EPSCO（八达通），ATM 安全应用要求	
8. 产品的系列化	高中低端产品配合使用，形成了一个完整的、封闭的、高安全的密码体系。	不完善
9. 密码机扩充功能时，核心程序的升级方式	采用前台的升级程序，配合密码机核心程序中的升级模块方式、并在相应的安全机制控制下来实现，安全、可靠、简便、易操作	不完善，安全性低
10. 绿色环保设计	无噪音、无辐射、低功耗	无

SJL22-SM 金融数据密码机系列分为高、中、低端产品，采用 SJL22-SM 金融数据密码机系列产品作为商业银行业务网络中应用密码设备，其最大优点是：**除和其他厂商的密码设备互联互通外，采用和 RACAL（THALES）安全体系兼容的高速变种加密机制使得 SJL22-SM 金融数据密码机系列产品自身形成一套封闭的密码体系，大大增强了金融业务系统的安全性**。

13 附录一北京江南歌盟科技有限公司简介

北京江南歌盟科技有限公司（下称“歌盟科技”——http://www.gemen.com.cn）是在北京注册的实体公司。歌盟科技是一家专业从事金融信息安全技术发展研究、产品研发、生产销售与商业银行总体安全解决方案咨询服务及提供的高科技企业。

北京歌盟科技有限公司是于 2005 年 7 月在北京注册的实体公司。北京歌盟科技有限公司是歌盟科技在中国大陆地区密码产品的总代理商。北京歌盟科技有限公司是一家专业从事金融信息安全技术销售与售后技术支持，以及商业银行总体安全解决方案咨询服务及提供的高科技企业。

上海歌盟信息技术有限公司是于 2007 年 10 月在上海注册的实体公司。上海歌盟信息技术有限公司是歌盟科技密码产品在华东地区的销售服务窗口。上海歌盟信息技术有限公司是一家专业从事金融信息安全技术销售与售后技术支持，以及商业银行总体安全解决方案咨询服务及提供的高科技企业。

歌盟科技自主开发了应用在金融领域符合 VISA/MasterCard 新的国际卡业务规范(TDES、EMV2000)要求的 SJL22-SM 金融数据密码机系列产品及其配套的密码机机群系统。歌盟科技吸纳并汇集了一批优秀的科研、管理、技术人才，他们长期从事金融业务及金融信息安全领域的技术跟踪、应用规范、发展研究、咨询服务、软件开发及系统集成等，并在金融安全领域有着丰富的实践经验。

目前，歌盟科技和武汉大学在计算机应用、软件开发、网络与数据库、嵌入式系统、信息安全、智能卡应用等领域签署了双方合作协议。歌盟科技作为武汉大学的新技术应用推广单位，和武汉大学一道共同发挥各自的市场、技术和服务优势为业界做出自己的贡献。另外，歌盟科技作为福建瑞迪科技发展有限公司驻北京销售中心，继续为瑞迪科技过去、现在及将来的合作伙伴提供不断完善的技术支持和售后服务体系。

歌盟科技本着“创新技术、历练人才、营销市场、科学管理”的经营理念，以国家利益为重，以客户需求为本，提供金融安全领域用户全方位的技术服务。公司信奉“没有服务的服务才是最好的服务”的服务宗旨，向客户提供一流的技术、一流

的产品、一流的服务，一流的信誉。

歌盟科技将运用科学的企业管理手段，加强部门机构建设，提高科研技术水平，扩大市场营销范围，完善售前售后服务体系。在各有关部门和广大用户的支持和关怀下，为加快我国信息产业的现代化建设，做出应有的贡献。歌盟科技充满信心，通过公司全体员工的共同努力在金融安全领域成为有市场影响力的高科技企业。

歌盟科技全国各分支机构：

北京江南歌盟科技有限公司

北京歌盟科技有限公司

地 址: 北京市海淀区清缘西里水木天成 2 号楼 508
邮 编: 100192
电 话: +86-10-59870019/82753486
传 真: +86-10-59870419
客户投诉: +86-10-59870019 转 800
E-mail: **一般业务**: **contact@gemen.com.cn**
业务联系: **sales@gemen.com.cn**
技术支持: **support@gemen.com.cn**
客户投诉: **complain@gemen.com.cn**

华东地区代表处(上海歌盟信息技术有限公司)

地 址: 上海市张江高科技园区张衡路 429 号
上海交通大学信息安全学院南 101 室
邮 编: 201203
电 话: +86-21-50277279
传 真: +86-21-50277279
联系人: 陈国建
手 机: +86-13816331715
E-mail: gjchen@gemen.com.cn

华南地区代表处

地　址: 广州天河工业园建中路 62 号迪宝大厦一楼
邮　编: 510665
电　话: +86-20-85559119
传　真: +86-20-85559012
联系人: 彭军辉
手　机: +86-13924027125
E-mail: huanan@gemen.com.cn

华中地区代表处

地　址: 湖北省武汉市武汉大学计算机学院
邮　编: 430079
电　话: +86-27-68754862
传　真:
联系人: 张弛
手　机: +86-13507192543
E-mail: huazhong@gemen.com.cn

西北地区代表处

地　址: 兰州市贡元巷 15 号 806
邮　编: 730030
电　话: +86-931-3699220
传　真:
联系人: 黄明科
手　机:
E-mail: xibei@gemen.com.cn

东北地区代表处

地　址: 沈阳市和平区文化路 17 号金科大厦 5-13-2
邮　编: 110003
电　话: +86-24-23901508
传　真: +86-24-23908616
联系人: 丁毅
手　机: +86-13704023099
E-mail: dongbei@gemen.com.cn