ICS 35.040
L 80
备案号:55613—2016

GM

中华人民共和国密码行业标准

GM/T 0045—2016

金融数据密码机技术规范

Specifications of financial cryptographic server

2016-03-28 发布　　2016-03-28 实施

国家密码管理局　　发布

目　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由密码行业标准化技术委员会提出并归口。

本标准主要起草单位：成都卫士通信息产业股份公司、无锡江南计算机技术研究所、兴唐通信科技股份有限公司、山东得安信息技术有限公司、北京三未信安科技发展有限公司、北京江南天安科技有限公司。

本标准主要起草人：李元正、张世雄、黄锦、张所成、徐明翼、王妮娜、郑海森、高志权、李国、马晓艳。

金融数据密码机技术规范

1 范围

本标准定义了金融数据密码机的相关术语，规定了金融数据密码机功能要求、接口要求、硬件要求、业务要求、安全性要求和检测要求等内容。

本标准适用于金融数据密码机的研制、使用，也适用于指导金融数据密码机的检测。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件，凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 4943 信息技术 设备(包括电气事务设备)的安全

GB/T 9813—2000 微型计算机通用规范

GB/T 17964 信息技术 安全技术 分组密码算法的工作模式

GM/T 0002 SM4 分组密码算法

GM/T 0003 SM2 椭圆曲线公钥密码算法

GM/T 0004 SM3 密码杂凑算法

GM/T 0005 随机性检测规范

GM/T 0006 密码应用标识规范

GM/T 0009 SM2 密码算法使用规范

GM/T 0028 密码模块安全技术要求

JR/T 0025 中国金融集成电路(IC)卡规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

金融数据密码机 financial cryptographic server

在金融领域内，用于确保金融数据安全，并符合金融磁条卡、IC 卡业务特点的，主要实现 PIN 加密、PIN 转加密、MAC 产生和校验、数据加解密、签名验证以及密钥管理等密码服务功能的密码设备，也称为主机加密机(HSM)。

3.2

对称密码算法 symmetric cryptographic algorithm

加密和解密在算法和密钥上相同或可相互推导的密码算法。

3.3

非对称密码算法 asymmetric cryptographic algorithm

使用两种相关变换和非对称密钥对的密码算法，一种是由公开密钥定义的公开变换，另一种是由私有密钥定义的私有变换。两种变换具有以下特性：给定公开密钥，得出私有密钥在计算上是不可行的。

3.4

杂凑算法　hash algorithm

一种将任意长度的消息压缩到某一固定长度的消息摘要的算法。

3.5

加密　encrypt;encryption

通过加密算法对明文进行变换产生密文的过程。

3.6

解密　decrypt;decryption

与加密过程相逆的过程,通过解密算法将密文转换成明文。

3.7

物理安全环境　physically secure environment;PSE

设计的具有访问控制机制或其他安全机制的环境,防止密钥泄露或存储的其他秘密数据泄露等。

3.8

物理防护　physical protection;PP

用物理手段保护硬件密码设备及其密钥或敏感信息。

3.9

主密钥　master key;MK

处于层次化密钥结构中的最顶层,用于其下层密钥的保护。

3.10

次主密钥　secondary master key;SMK

处于层次化密钥结构中的第二层,主要用于其下层密钥的产生或保护。

3.11

密钥分离　key separation;KS

保证每种密码操作只采用指定的密钥类型,例如,MAC 密钥只能用于产生消息认证码。

3.12

数据密钥　data key;DK

保护 PIN 和计算 MAC 的密钥,包括 MAC 密钥(MAK)和 PIN 密钥(PIK),也称为工作密钥。

3.13

密钥校验值　key check value;KCV

通过不可逆转算法计算的结果值,用于密钥完整性检验。校验值是通常在密钥下采用不可逆转算法计算一个任意串的结果。

3.14

个人识别码　personal identification number;PIN

在金融业务中,授权请求消息中认证持卡人的一种数字身份标识码,在交易时 PIN 只包含十进制数字,在登录时,可支持数字、大小写字母、标点符号。

3.15

密钥装载　key loading;KL

手工或电子手段将密钥传递到金融数据密码机中的过程。

3.16

手工密钥分发　manual key distribution;MKD

一种用密码信封等非电子手段进行密钥分发的方式。

3.17

手工密钥注入　manual key entry;MKE

用键盘输入的方式把密钥数据注入到金融数据密码机。

3.18

密钥分散　key dispersion;KD

由次主密钥或子密钥生成下级密钥的过程。

3.19

密钥分量　key componet;KC

多个合成完整密钥的密钥成分。

3.20

密码键盘　PIN pad;PP

用于输入个人识别码的一组数字和命令按键。

4　缩略语

下列缩略语适用于本文件。

AMK	应用主密钥	(Application Master Key)
API	应用编程接口,简称应用接口	(Application Program Interface)
ARPC	授权响应密文	(Authorization Response Cryptogram)
ARQC	授权请求密文	(Authorization Request Cryptogram)
CBC	(分组密码的)密码分组链接(工作方式)	(Cipher Block Chaining)
CFB	(分组密码的)密码反馈(工作方式)	(Cipher Feedback)
CK	主控密钥	(Control Key)
DK	数据密钥	(Data Key)
ECB	(分组密码的)电子密本(工作方式)	(Electronic Codebook)
Hash	散列函数运算,又称杂凑运算	(Hash Algorithm)
HSM	主机加密机	(Host Security Machine)
LMK	本地主密钥	(Local Master Key)
MAC	消息认证码	(Message Authentication Code)
MAK	MAC 计算密钥,属于数据密钥	(MAC Key)
OFB	(分组密码的)输出反馈(工作方式)	(Output Feedback)
PAN	主账号	(Primary Account Number)
PIN	个人识别码	(Personal Identification Number)
PIK	PIN 加密密钥,属于数据密钥	(PIN Key)
TMK	终端主密钥	(Terminal Master Key)
TPK	终端 PIN 加密密钥	(Terminal PIN Key)
TAK	终端 MAC 计算密钥	(Terminal MAC Key)
TEK	终端加密密钥	(Terminal Encrypt Key)
ZMK	区域主密钥	(Zone Master Key)
ZPK	区域 PIN 加密密钥	(Zone PIN Key)
ZAK	区域 MAC 计算密钥	(Zone MAC Key)
ZEK	区域加密密钥	(Zone Encrypt Key)

5 功能要求

5.1 密码算法

5.1.1 对称密码算法

金融数据密码机应配用 SM4 对称密码算法，SM4 密码算法的实现遵循 GM/T 0002。

为满足与原有系统兼容要求或与其他系统（例如：外卡系统）互联要求，也可支持国际标准 DES/3DES/AES 密码算法及国家密码管理主管部门认可的其他算法。

对称密码算法的工作模式应遵循 GB/T 17964，至少应包括 ECB 和 CBC 两种模式。

对称密码算法主要用于 PIN 加密、PIN 转加密、MAC 计算、数据加解密和密钥保护。

5.1.2 公钥密码算法

金融数据密码机应配用 SM2 非对称密码算法，SM2 密码算法的实现遵循 GM/T 0003，算法的使用遵循 GM/T 0009。

为满足与原有系统兼容要求或与其他系统（例如：外卡系统）互联要求，金融数据密码机也可支持国际标准 RSA 密码算法及国家密码管理主管部门认可的其他算法。RSA 密码算法模长应满足国际银行卡组织评估建议的长度并能扩展。

非对称密钥算法主要用于数字签名和验签、密码信封、密钥分发。

5.1.3 杂凑算法

金融数据密码机应配用 SM3 杂凑算法，SM3 杂凑算法的实现遵循 GM/T 0004。另外，SM2 密码算法应用在数字签名验签和计算消息认证码时，算法要求配用 SM3 杂凑算法，在 SM2 密码算法中使用的 SM3 杂凑算法的实现遵循 GM/T 0003。

为满足与原有系统兼容要求或与其他系统（例如：外卡系统）互联要求，金融数据密码机也可支持国际标准 SHA-1 密码算法及国家密码管理主管部门认可的其他算法。

杂凑算法用于数字签名和验证、杂凑值生成和验证。

5.2 密钥管理

5.2.1 基本要求

密钥管理是金融数据密码机的核心功能，保护密钥在产生、安装、存储、使用、备份、恢复整个生命周期安全。

金融数据密码机应具有明确的密钥保护措施。

金融数据密码机应具有防止密钥类型混用的防护措施，例如：计算消息认证码时，如果参与 MAC 计算的密钥是 PIK，设备应拒绝操作并立即返回错误。

5.2.2 密钥结构

金融数据密码机采用三层密钥机制，分别为主密钥、次主密钥和数据密钥等三层。密钥层次如图 1 所示。

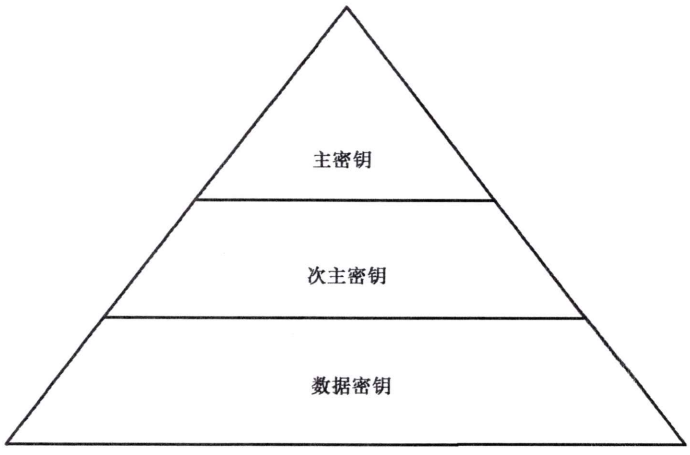

图 1　密钥结构图

主密钥是一种密钥加密密钥，其主要作用是保护密钥的安全传输和存储。主密钥的存储应采用强安全措施，不能以明文方式出现在密码机外。

次主密钥是一种密钥加密密钥，其主要作用是保护数据密钥的安全传输、分发和存储。次主密钥应加密保护后才能出现在密码机外。

数据密钥是实际保护金融业务数据安全的密钥，数据密钥应加密保护后才能出现在密码机外。

金融数据密码机中的密钥应分层保护，保护原则为“自上向下逐层保护”。主密钥保护次主密钥，次主密钥保护数据密钥。

5.2.3　密钥存储

金融数据密码机中主密钥应安全存储，可采用加密存储或微电保护存储方式。主密钥只能在系统备份时才能导出密码机，备份介质中存储的主密钥应遵循多段、多人方式，每段分人、分别保存的原则。

次主密钥和数据密钥只能在主密钥的保护下才能存储在密码机外。

采用微电保护存储方式时，密钥可以明文方式存储。应设计有销毁密钥的触发装置，当触发装置被触发时，销毁存储的所有密钥。

5.2.4　密钥注入

如果主密钥和次主密钥由外部设备产生，应采用手工密钥注入的方式导入到密码机中。

密钥不允许以明文形态完整地出现在金融数据密码机之外。明文形态的密钥在通过密码信封、码单、IC 卡、USB KEY 等形式输出时，应具有完整的管理措施保证非授权人员不能接触到明文密钥。

在以密文形态输出密钥时，确保密钥加密密钥的类型正确、密钥及密钥加密密钥在有效期内、密钥信息没有泄露。

需手工注入的明文形态密钥应采用分段传输、保存和注入，不同的密钥分量应由不同授权管理员分开保存；在注入密钥时，应至少由 2 名以上的授权管理员在注入现场共同完成。

5.2.5　密钥备份/恢复

金融数据密码机应具备主密钥、次主密钥的备份/恢复功能。备份操作产生的备份数据应以密文形式存储到存储介质中，加密备份数据的密钥应有安全机制保证其安全。

备份的密钥可以恢复到金融数据密码机中，同厂家的不同型号的金融数据密码机之间应能够互相备份恢复。密钥恢复操作只能在金融数据密码机内进行。

5.3 随机数

金融数据密码机应采用不少于2个硬件物理噪声源的产生随机数。产生的随机数应满足GM/T 0005的要求。

金融数据密码机配用的随机数发生器应通过送样检测、出厂检测、上电检测和使用检测等四个阶段的随机数检测：

a) 送样检测

依据GM/T 0005要求进行随机数送样检测。

b) 出厂检测

- 检测量：采集 50×10^6 比特随机数，分成50组，每组 10^6 比特；
- 检测项目：依据GM/T 0005要求进行检测；
- 检测通过标准：检测中如果有一项不通过检测标准，则告警检测不合格。允许重复1次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

c) 上电检测

- 检测量：采集 20×10^6 比特随机数，分成20组，每组 10^6 比特；
- 检测项目：依据GM/T 0005要求进行检测；
- 检测通过标准：检测中如果有一项不通过检测标准，则告警检测不合格。允许重复1次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

d) 使用检测

1) 周期检测

- 检测量：采集 4×10^5 比特随机数，分成20组，每组20 000比特；
- 检测项目：依据GM/T 0005规范中完成除离散傅立叶检测、线性复杂度检测、通用统计检测外的12项项目检测；
- 检测通过标准：检测中如果有一项不通过检测标准，则告警检测不合格。允许重复1次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效；
- 检测周期：检测周期可根据实际需求配置，但检测间隔最长不超过12 h。

2) 单次检测

- 检测量：根据实际应用时每次所采随机数大小确定，但长度不应低于128比特，且已通过检测的未用序列可继续使用；
- 检测项目：依据GM/T 0005规范中的扑克检测进行检测。当样本长度小于320比特时，参数 $m=2$；
- 检测通过标准：检测中如果不通过检测标准，则告警检测不合格。允许重复1次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

金融数据密码机在判定随机数发生器失效后，不能对外提供任何操作。

5.4 访问控制

金融数据密码机的启动、停止和配置只能由授权管理员完成；密码机应提供管理员身份鉴别机制。

金融数据密码机应提供网络访问控制机制，由安全员配置允许访问密码机的安全策略，至少应具有验证合法主机的IP地址的功能。

5.5 设备管理

5.5.1 设备自检

金融数据密码机应提供设备自检功能，设备自检包括密码算法正确性检查、随机数发生器检查、存

储密钥和数据的完整性检查等。

5.5.2 日志审计

金融数据密码机应提供日志记录功能，同时提供日志查看和日志导出功能。一条日志的内容中需包括日志的主体，日志产生时间等元素。日志分为下列3类管理：

a) 操作日志：记录管理员的操作行为，包括系统配置参数的修改等。
b) 管理日志：记录需审计的安全事件，包括管理员登录、密钥注入、密钥产生、密钥更新、密钥销毁、授权状态的切换等。
c) 运行日志：记录设备的运行工作状态，包括设备的异常、拒绝、报警等。

5.5.3 远程管理

在有远程集中管理需求时，金融数据密码机可具有设备远程集中管理功能，设备管理功能的实现应符合密码设备相关管理规范的要求。

5.6 设备初始化

金融数据密码机的初始化，应包括产生管理员并授权、管理员按授权进行系统配置、产生并安装密钥、进行密钥备份。

设备的初始化不能由厂商进行。

5.7 设备自检

金融数据密码机应在启动过程中进行自检，在其他时间也可进行周期或手动自检，自检项包括：

a) 对密码运算部件等关键部件进行正确性检查。
b) 对随机数进行随机性检查。
c) 对存储的密钥等敏感信息进行完整性检查。

在检查不通过时应报警并停止工作。

6 硬件要求

6.1 物理接口

金融数据密码机应设置独立的服务接口和管理接口，分别用于密码服务和设备管理，接口的功能不能交叉混用。接口可采用以太网、USB、串口或者其他接口形式。

6.2 状态指示器

金融数据密码机应提供设备上电、工作、故障的状态指示。

6.3 随机数发生器

随机数产生器应采用国家密码管理主管部门批准使用的器件。

6.4 环境适应性

金融数据密码机的工作环境应符合GB/T 9813—2000中5.8要求。

6.5 可靠性

金融数据密码机的平均无故障工作时间应不低于10 000 h。

7 安全业务要求

7.1 基本要求

金融数据密码机通过应用编程接口对用户提供密码服务，实现密码功能。

根据应用的不同，应用编程接口可划分为磁条卡应用，IC 卡应用和基础密码运算服务。

在业务功能中，针对密钥和 PIN 的计算，其算法工作模式均采用 ECB 模式。针对数据的计算，其算法工作模式均采用 CBC 模式，且首块 IV 为全‘0’。使用 SM2 算法的操作应遵循 GM/T 0009 的要求。

金融数据密码机的应采用模块化设计，不同功能模块不能相互影响。

7.2 数据报文接口

7.2.1 数据缩写

数据标识缩写见表 1。

表 1 数据标识

标识	说明
n	可变长度域
A	字母数字字符，包括任何 ASCII 字符
H	十六进制字符，‘0’～‘9’和‘A’～‘F’
N	十进制数字字符，‘0’～‘9’
B	二进制字符(字节)，X’00 to X’FF

7.2.2 变量约定

变量名约定见表 2。

表 2 变量名约定

变量名	含义
Nh	用户在加密机中设定的消息头长度
Nt	用户在加密机中设定的消息尾长度

7.2.3 传输约定

数值数据按从高到低的字节序传输；其他数据按从前往后、从左往右的顺序传输。

7.3 业务功能要求

7.3.1 磁条卡应用

7.3.1.1 产生密钥

通过随机产生或分散产生的方式生成指定类型密钥分量，并将密钥分量写入 IC 卡或打印到密钥

信封。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“X0”
模式	1	A	‘0’—产生随机密钥； ‘1’—产生分散密钥。
介质类型	2	A	‘00’—没有存储介质 ‘01’—写入 IC 卡 ‘10’—打印密钥信封 ‘11’—打印密钥信封和写入 IC 卡 ‘12’—SM2 公钥加密 其他保留，用于扩展其他方式
密钥类型	1	A	‘1’—LMK，‘2’—ZMK，‘3’—MAK ‘4’—PIK，‘5’—TMK，‘6’—CVK ‘7’—PVK，‘8’—WWK，‘9’—TGMK ‘A’—ZEK ……
算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留，用于扩展其他算法类型
分量个数	1	A	标识分量序号。‘1’～‘9’：表示第一段～第九段；
密钥长度	4	A	‘0000’～‘0099’(产生密钥长度)，仅当模式＝‘0’存在
数据密钥	1A＋32H	H	用于分散的根密钥，仅当模式＝1 时存在
分散次数	1	A	‘1’～‘3’，仅当模式＝1 时存在
分散数据 1	16	H	分散因子 1。仅当模式＝‘1’时存在。和密钥分量个数对应
…	…	…	…
分散数据 n	16	H	分散因子 N，仅当模式＝‘1’时存在。
公钥长度	4	A	当介质类型＝‘12’时存在
公钥	N	B	输入 SM2 公钥。当介质类型＝‘12’存在
打印份数	1	A	打印密钥信封时存在
打印字段 0	N	A	不包含“；”
分隔符	1	A	值为“；”，打印字段结束符
打印字段 1	N	A	不包含“；”
…	…	…	…
打印字段 n	N	A	最后一个打印字段，不包含“；”
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“X1”
状态代码	2	N	正常为“00”，其他为错误
密钥	1A＋32	H	LMK 加密密钥
密文长度	4	N	密文长度(当介质类型＝‘12’时存在)

密文		H	公钥加密密文(当介质类型=‘12’时存在)
KCV	16	H	密钥校验值
消息尾	Nt	A	与输入相同

7.3.1.2 导入密钥

将密钥 从 ZMK 保护转为 LMK 保护。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“A6”
密钥类型	3	H	‘000’—ZMK;‘001’—ZPK;‘002’—TPK; ‘002’—PVK;‘002’—TMK;‘003’—TAK; ‘006’—WWK;‘008’—ZAK;‘009’—BDK; ‘00A’—ZEK;‘402’—CVK; ……
算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留,用于扩展其他算法类型
ZMK	1A+32H	H	用 LMK (04,05)加密
密钥	1A+32H	H	用 ZMK 加密
LMK 密钥方案	1	A	用 LMK 加密方式标志
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“A7”
状态代码	2	N	正常为“00”,其他为错误
LMK 密文	1A+32H	H	LMK 加密的密钥密文
KCV	16	H	密钥校验值
消息尾	Nt	A	与输入相同

7.3.1.3 导出密钥

将密钥 从 LMK 保护转为 ZMK 保护。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“A8”
密钥类型	3	H	‘000’—ZMK;‘001’—ZPK;‘002’—TPK; ‘002’—PVK;‘002’—TMK;‘003’—TAK; ‘006’—WWK;‘008’—ZAK;‘009’—BDK; ‘00A’—ZEK;‘402’—CVK; ……
算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留,用于扩展其他算法类型
ZMK	1A+32H	H	用 LMK (04,05)加密
密钥	1A+32H	H	用 LMK 加密

ZMK 密钥方案	1	A	用 ZMK 加密方式标志
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“A9”
状态代码	2	N	正常为“00”,其他为错误
ZMK 密文	1A+32H	H	ZMK 加密的密钥密文
KCV	16	H	密钥校验值
消息尾	Nt	A	与输入相同

7.3.1.4 合成 ZMK

由三个 ZMK 加密分量形成一个 ZMK,返回 LMK 加密后的密文,并计算校验值。

输入域	**长度**	**类型**	**备注**
消息头	Nh	A	
命令码	2	A	“GG”
算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留,用于扩展其他算法类型
ZMK 分量 1	1A+32H	H	ZMK 分量一,用 LMK(04,05)加密
ZMK 分量 2	1A+32H	H	ZMK 分量二,用 LMK(04,05)加密
ZMK 分量 3	1A+32H	H	ZMK 分量三,用 LMK(04,05)加密
分割符	1	A	可选项,值为“;”
ZMK 密钥方案	1	A	可选项,用 ZMK 加密方式标志
LMK 密钥方案	1	A	可选项,用 LMK 加密方式标志
KCV 类型	1	A	可选项, 0:输出的校验码为 16H; 1:输出的校验码为 6H。
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“GH”
状态代码	2	N	正常为“00”,其他为错误
ZMK 密文	1A+32H	H	用 LMK(04,05)加密
KCV	16	H	密钥校验值
消息尾	Nt	A	与输入相同

7.3.1.5 LMK 加密密钥

用 LMK 加密指定密钥。

输入域	**长度**	**类型**	**备注**
消息头	Nh	A	
命令码	2	A	“X2”

算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留，用于扩展其他算法类型
密钥类型	3	A	‘000’—ZMK；‘001’—ZPK；‘002’—TPK； ‘002’—PVK；‘002’—TMK；‘003’—TAK； ‘006’—WWK；‘008’—ZAK；‘009’—BDK； ‘00A’—ZEK；‘402’—CVK； ……
密钥方案	1	A	X/Y/Z(x=16；y=24；z=8)
索引	3	A	密钥在用户存储区域的索引
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“X3”
状态代码	2	N	正常为“00”，其他为错误
密钥密文	N	A	对应 LMK 加密的结果
消息尾	Nt	A	与输入相同

7.3.1.6 生成密钥校验值

计算送入加密机的密钥的校验值。

输入域	**长度**	**类型**	**备注**
消息头	Nh	A	
命令码	2	A	“KA”
算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留，用于扩展其他算法类型
密钥	1A+32H	H	LMK 加密加密的 ZMK 或 ZPK 或 TMK/TPK/PVK 或 TAK
密钥类型	3	N	‘000’—ZMK；‘001’—ZPK；‘002’—TPK； ‘002’—PVK；‘002’—TMK；‘003’—TAK； ‘006’—WWK；‘008’—ZAK；‘009’—BDK； ‘00A’—ZEK；‘402’—CVK； ……
分隔符	1	A	可选项，值为“；”，如果出现此域，则应同时出现以下三个参数，对于下面三个参数中未用到的参数，可以用 0 或有效值填充
ZMK 密钥方案	1	A	可选项，用 ZMK 加密方式标志
LMK 密钥方案	1	A	可选项，用 LMK 加密方式标志
KCV 类型	1	A	可选项， 0：输出的校验码为 16H； 1：输出的校验码为 6H。
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同

响应代码	2	A	“KB”
状态代码	2	N	正常为“00”,其他为错误
KCV	16	H	密钥校验值
消息尾	Nt	A	与输入相同

7.3.1.7 产生随机 PIN

产生随机 PIN,并用 LMK 加密保护输出。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“JA”
算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留,用于扩展其他算法类型
PAN	12	N	主账号去掉校验位的最后 12 位
PINLength	2	N	04-12
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“JB”
状态代码	2	N	正常为“00”,其他为错误
PIN 密文	7	N	用 LMK(02,03)加密
消息尾	Nt	A	与输入相同

7.3.1.8 加密 PIN

加密明文的 PIN。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“BA”
算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留,用于扩展其他算法类型
PIN	7	H	4～6 位数值数据,3～1 位“F”
PAN	12	N	主账号去掉校验位的最后 12 位
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“BB”
状态代码	2	N	正常为“00”,其他为错误
PIN 密文	7	N	用 LMK(02,03)加密,4～6 位明文 PIN,3～1 位“F”
消息尾	Nt	A	与输入相同

7.3.1.9 PIN 验证

通过比较明文 PIN 的方法验证由 ZPK 加密保护的 PIN 块。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“BE”
算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留，用于扩展其他算法类型
ZPK	1A+32H	H	LMK(06,07)加密
PIN 块	32	H	ZPK 加密
PIN 格式	2	N	PIN 块格式
PAN	12	N	主账号去掉校验位的最后 12 位
PIN	7	N	LMK(02,03)加密
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“BF”
状态代码	2	N	正常为“00”，其他为错误
消息尾	Nt	A	与输入相同

7.3.1.10 PIN 块从 ZPK 到 LMK

将 PIN 块 由 ZPK 保护转化为 LMK 保护。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“JE”
算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留，用于扩展其他算法类型
ZPK	1A+32H	H	LMK (06,07)加密
PIN 块	32	H	ZPK 加密(PIN 块的密文)
PIN 格式	2	N	
主账号	12	N	
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“JF”
状态代码	2	N	正常为“00”，其他为错误
PIN	7	N	LMK(02,03)加密
消息尾	Nt	A	与输入相同

7.3.1.11 PIN 块从 TPK 到 LMK

将 PIN 块 由 TPK 保护转化为 LMK 保护。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“JC”
算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留，用于扩展其他算法类型
TPK	1A+32H	H	LMK(14,15)加密
PIN 块	32	H	TPK 加密
PIN 格式	2	N	PIN 块格式
PAN	12	N	主账号去掉校验位的最后 12 位
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“JD”
状态代码	2	N	正常为“00”，其他为错误
PIN	7	N	LMK(02,03)加密
消息尾	Nt	A	与输入相同

7.3.1.12 PIN 块从 LMK 到 ZPK

将 PIN 块由 LMK 保护转化为 ZPK 保护。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“JG”
算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留，用于扩展其他算法类型
ZPK	1A+32H	H	LMK(06,07)加密
PIN 格式	2	N	PIN 块格式
PAN	12	N	主账号去掉校验位的最后 12 位
PIN	7	N	LMK(02,03)加密
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“JH”
状态代码	2	N	正常为“00”，其他为错误
PIN 块	32	H	ZPK 加密
消息尾	Nt	A	与输入相同

7.3.1.13 PIN 块从 ZPK1 到 ZPK2

将 PIN 块 由 ZPK1 保护转化为 ZPK2 保护。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“CC”
算法类型 1	1	A	‘1’—SM4 ‘2’—SM1 其他保留,用于扩展其他算法类型
算法类型 2	1	A	‘1’—SM4 ‘2’—SM1 其他保留,用于扩展其他算法类型
ZPK1	1A+32H	H	LMK(06,07)加密
ZPK2	1A+32H	H	LMK(06,07)加密
MaxPINLength	2	N	最大 PIN 长度,值为 12
PINBlock	32	H	转换前 PINBlock,ZPK1 加密
PIN 格式 1	2	N	转换前 PIN 块格式
PIN 格式 2	2	N	转换后 PIN 块格式
PAN	12	N	主账号去掉校验位的最后 12 位
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“CD”
状态代码	2	N	正常为“00”,其他为错误
PIN 块	32	H	ZPK2 加密
消息尾	Nt	A	与输入相同

7.3.1.14 产生 MAC

利用 MAK 计算 MAC 值。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“MS”
数据块标识	1	A	‘0’—:唯一块; ‘1’ 第一块; ‘2’—中间块; ‘3’—最后块;
KeyType	1	A	‘0’—TAK ‘1’—ZAK
MacAlog	1	A	‘1’—9.19 ‘2’—XOR ‘3’—POSMAC 其他保留

算法类型	1	A	'1'—SM4 '2'—SM1 其他保留,用于扩展其他算法类型
MAK	1A+32H	H	LMK 加密
IV	32	H	仅当为中间块或最后块时此域才存在
MAC 数据长度	4	N	N 在 1～2 048 之间
MAC 数据	N	A	N 在 1～2 048 之间
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	"MT"
状态代码	2	N	正常为"00",其他为错误
MAC	32	H	
消息尾	Nt	A	与输入相同

7.3.1.15 验证 MAC

利用 MAK 计算 MAC 值,并与命令中的 MAC 值比较。

输入域	**长度**	**类型**	**备注**
消息头	Nh	A	
命令码	2	A	"MC"
KeyType	1	A	'0'—TAK '1'—ZAK
MacAlog	1	A	'1'—9.19 '2'—XOR '3'—POSMAC 其他保留
算法类型	1	A	'1'—SM4 '2'—SM1 其他保留,用于扩展其他算法类型
MAK	1A+32H	H	LMK 加密
MAC	8	H	用于验证的 MAC 码
MAC 数据长度	4	N	在 1～2 048 之间
MAC 数据	N	A	N 在 1～2 048 之间
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	"MD"
状态代码	2	N	正常为"00",其他为错误
消息尾	Nt	A	与输入相同

7.3.1.16 产生 CVN

产生卡校验码 CVN。

输入域	A	类型	备注
消息头	Nh	A	
命令码	2	A	“CW”
算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留，用于扩展其他算法类型
CVK_A/B	1A＋32	H	用LMK(14,15)加密
主账号	n	N	12～19 位
Delimiter	1	A	“;”，PAN 结束符
卡有效期	4	N	“YYDD”格式
卡服务代码	3	N	
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“CX”
状态代码	2	N	正常为“00”，其他为错误
CVV	3	N	卡校验码
消息尾	Nt	A	与输入相同

7.3.1.17 验证 CVN

验证卡校验码 CVN。

输入域	A	类型	备注
消息头	Nh	A	
命令码	2	A	“CY”
算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留，用于扩展其他算法类型
CVK_A/B	1A＋32	H	用LMK(14,15)加密
CVV	3	N	验证的 CVV
主账号 r	n	N	主账号，12～19 位
分隔符	1	A	“;”，PAN 结束符
卡有效期	4	N	卡有效期，“YYDD”格式
卡服务代码	3	N	卡服务代码
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“CZ”
状态代码	2	N	正常为“00”，其他为错误
消息尾	Nt	A	与输入相同

7.3.1.18 定义打印格式

在打印密码信封前，先定义打印格式。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“PA”
格式数据	N	A	打印格式控制符
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“PB”
状态代码	2	N	正常为“00”,其他为错误
消息尾	Nt	A	与输入相同

7.3.1.19 打印密码信封

将 PIN 和相关数据输出到与加密机连接的串口或并口打印机上。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“PE”
类型	1	A	值为‘C’;
算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留,用于扩展其他算法类型
PAN	12	N	主账号去掉校验位的最后 12 位
PIN	L	N	用 LMK(02～03)加密,L=用户设定的 PIN 长度+1
打印域 0	n	A	打印字段 0,不包含“;”
分隔符	1	A	值为‘;’,打印字段结束符
打印域 1	n	A	打印字段 1,不包含“;”
…	…	…	…
打印域 n	n	A	最后一个打印字段,不包含“;”
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“PF”
状态代码	2	N	正常为“00”,其他为错误
保留	L+12	N	
消息尾	Nt	A	与输入相同

7.3.2 IC 卡应用

7.3.2.1 分散子密钥

使用指定的应用主密钥进行指定次数离散得到卡片应用子密钥,并用主控密钥加密后输出密钥密文和校验值。

输入域	长度	类型	备注
消息头	Nh	A	

命令类型	2	A	VC
算法类型	1	A	'1'—SM4 '2'—SM1 其他保留,用于扩展其他算法类型
密钥类型	3	A	'00A' 默认为 WWK(006)
主控密钥	1A+32H	H	LMK 加密
主控密钥分散次数	1	A	'0'、'1'、'2'、'3'
主控密钥分散算法	1	A	'1':银联标准、 分散次数为 0 该域不存在
主控密钥分散数据	N * 16	H	分散次数为 0 该域不存在
应用主密钥类型	3	A	发卡行应用主密钥类型 默认为 WWK(006)
应用主密钥	1A+32H	H	LMK 加密
应用密钥分散次数	1	H	'0'、'1'、'2'、'3'
应用密钥分散算法	1	H	1:银联标准、 分散次数为 0 该域不存在
应用密钥分散数据	N * 16	H	分散次数为 0 该域不存在
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	"VD"
状态代码	2	N	正常为"00",其他为错误
密文长度	2	N	密钥密文的长度
密文	N	H	密钥密文
密钥校验值	16	H	密钥校验值
消息尾	Nt	A	与输入相同

7.3.2.2 ARQC/ARPC 产生或验证

支持 JR/T 0025 规范,ARQC/TC/ACC 的验证、ARPC 的产生或同时验证 ARQC 并产生 ARPC。

输入域	**长度**	**类型**	**备注**
消息头	Nh	A	
命令码	2	A	"VM"
算法类型	1	A	'1'—SM4 '2'—SM1 其他保留,用于扩展其他算法类型

IC 卡类型	1	A	'0'—Visa '1'—Europay or MasterCard M/Chip 其他保留
模式	1	A	'0'—只验证 ARQC/TC/ACC '1'—验证 ARQC,验证成功后生成 ARPC '2'—只产生 ARPC
密钥类型	3	A	"00A"
密钥	1A+32H	H	LMK 加密
卡片密钥分散因子	16	A	
会话密钥分散因子	4	A	
待验证 ARQC 值	16	A	
数据长度	4	N	"0000"～"4096",(模式为 0、1 时存在)
数据	N	A	加密机内部填充方式:先补 0x80,再补 0x00 直到长度为 16 的整数倍。(模式为'0'、'1'时存在)
ARC	4	A	(模式为'1'、'2'时存在)
消息尾	Nt	A	

输出域	长度	类型	备注
消息头	Nh	A	与输入相同
响应代码	2	A	"VN"
状态代码	2	N	正常为"00",其他为错误
ARPC 值	32	H	
消息尾	Nt	A	与输入相同

7.3.2.3 脚本加解密

支持 JR/T 0025 规范,对明文数据使用卡片加密过程密钥进行加解密计算。应用于应用系统存放脚本信息明文的情况.

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	"VI"
算法类型	1	A	'1'—SM4 '2'—SM1 其他保留,用于扩展其他算法类型
操作类型	1	A	'1':加密 '0':解密
IC 卡类型	1	A	'0'—Visa '1'—Europay or MasterCard M/Chip 其他保留
算法应用模式	1	A	'0':ECB '1':CBC
主密钥类型	3	A	"00A"
加密主密钥	1A+32H	H	被 LMK 加密的密文

卡片密钥分散因子	16	A	
会话密钥分散因子	4	A	
数据长度	4	N	“0000”～“4096”
初始向量 IV	16	A	CBC 模式时存在
数据		A	
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“VJ”
状态代码	2	N	正常为“00”，其他为错误
数据长度	4	N	数据长度
数据		A	加密结果是 8 的整数倍。解密结果为除去填充字符后的数据。
消息尾	Nt	A	与输入相同

7.3.2.4 计算脚本 MAC

支持 JR/T 0025 规范，计算发卡行脚本的消息认证码。

输入域	**长度**	**类型**	**备注**
消息头	Nh		
命令码	2	A	“VK”
算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留，用于扩展其他算法类型
IC 卡类型	1	A	0’—Visa ‘1’—Europay or MasterCard M/Chip 其他保留
密钥类型	3	A	“00A”
安全报文认证主密钥	1A＋32H	H	LMK 加密
卡片密钥分散因子	16	H	
会话密钥分散因子	4	H	
数据长度	4	N	“0000”～“4096”
数据		A	加密机内部填充方式：先补 0x80，再补 0x00 直到长度为 8 的整数倍。
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“VL”

状态代码	2	N	正常为“00”,其他为错误
MAC	16	A	MAC
消息尾	Nt	A	与输入相同

7.3.2.5 数据转加密

对 IC 卡发行数据进行转加密保护,并由卡片个人化系统完成 IC 卡写卡操作。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“VS”
解密算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留,用于扩展其他算法类型
密钥类型	3	A	“00A”
解密计算密钥	1A+32H	H	LMK 加密
解密算法模式	1	A	‘0’:ECB ‘1’:CBC
解密 IV	16	H	CBC 模式时存在
加密算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留,用于扩展其他算法类型
密钥类型	3	A	“00A”
加密计算密钥	1A+32H	H	LMK 加密
加密算法模式	1	A	‘0’:ECB ‘1’:CBC
加密 IV	8	H	CBC 模式时存在
数据长度	4	N	“0000”～“4096”
数据密文	N	H	
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“VT”
状态代码	2	N	正常为”00”,其他为错误
数据长度	4	N	“0000”～“4096”
密钥数据	N	H	
消息尾	Nt	A	与输入相同

7.3.2.6 数据加解密

对指定密钥进行指定次数的离散得到子密钥或过程密钥,使用该密钥对输入数据进行加密或解密计算。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“V2”

算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留，用于扩展其他算法类型
密钥类型	3	A	默认为工作密钥(006)
加/解密计算密钥	1A+32H	H	LMK 加密
密钥分散次数	1	A	‘0’、‘1’、‘2’
密钥分散数据 1	16	H	分散次数为‘0’时，该域不存在
密钥分散数据 2	16	H	分散次数为‘0’或‘1’时，该域不存在
加密/解密标识	1	A	‘1’:加密、‘0’:解密
算法应用模式	1	A	‘0’:ECB、‘1’:CBC
初始向量 IV	32	H	当算法模式为:‘1’时存在
填充模式	1	A	‘1’:0x80+0x00(长度为 8 的整数倍时不填充) ‘2’:0x80+0x00(不管长度是否 8 的整数倍，都要填充) ‘3’:0x00(长度是 8 的整数倍时不填充) ‘4’:0x00(不管长度是否 8 的整数倍，都要填充)
计算数据长度	4	N	“0000”～“4096”
计算数据		H	
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“V3”
状态代码	2	A	正常为“00”，其他为错误
输出数据长度	4	N	
输出数据	N	H	
消息尾	Nt	A	与输入相同

7.3.2.7 计算 MAC

对指定密钥进行指定次数的离散得到子密钥或过程密钥，使用该密钥对输入数据进行 MAC 计算。

输入域	**长度**	**类型**	**备注**
消息头	Nh		
命令码	2	A	“V4”
算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留，用于扩展其他算法类型
密钥类型	3	A	“008”
安全报文认证主密钥	1A+32H	H	LMK 加密
MAC 算法标识	1	A	‘1’—9.19 ‘2’—XOR ‘3’—POSMAC 其他保留
分散次数	1	A	‘0’/‘1’/‘2’/‘3’

密钥分散因子	16	H	
数据长度	4	N	“0000”～“4096”
数据		A	加密机内部填充方式：先补 0x80，再补 0x00 直到长度为 8 的整数倍。
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“V5”
状态代码	2	N	正常为“00”，其他为错误
MAC	16	A	MAC
消息尾	Nt	A	与输入相同

7.3.3 基础密码运算服务

7.3.3.1 产生 SM2 密钥对

随机产生基于 SM2 密码算法的密钥对，密钥对包括 SM2 密码算法的公钥和私钥。私钥采用本地主密钥加密，公钥明文输出。

密钥可以保存在密码机中，保存在密码机中的密钥访问采用索引方式。

输入域	**长度**	**类型**	**备注**
消息头	Nh	A	
命令码	2	A	“UO”
密钥长度	4	N	比特长度：应为 256
密钥用途	1	A	‘1’：签名； ‘2’：加密； ‘3’：签名和加密
密钥索引	2	N	“00”～“19”：密码机内保存新生成的密钥。 “99”：不保存新生成的密钥。
密钥口令	8	A	密钥索引不等于“99”时存在
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
应答码	2	A	“UP”
状态代码	2	N	正常为”00”，其他为错误
密钥长度	4	N	密钥长度
密钥密文	N	B	密钥密文，LMK(36，37)加密的密钥，应包含长度、公钥、私钥、校验值。
公钥明文 X	32	B	
公钥明文 Y	32	B	
私钥密文	32	B	LMK(36，37)加密后的密文
消息尾	Nt	A	与输入相同

7.3.3.2 转加密 SM2 私钥

将一个 LMK(36，37)加密的 SM2 私钥转换为另一个密钥加密。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“UY”
算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留，用于扩展其他算法类型
SM2 私钥密文	32	B	LMK(36,37)加密的 SM2 私钥
加密密钥类型	3	A	“00A”
加密计算密钥	1A+32H	H	LMK 加密
加密算法模式	1	N	‘0’:ECB ‘1’:CBC
加密 IV	32	H	
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
响应代码	2	A	“UZ”
状态代码	2	N	正常为“00”，其他为错误
SM2 私钥密文	64	H	加密密钥加密
消息尾	Nt	A	与输入相同

7.3.3.3 SM2 公钥加密

用 SM2 的公钥对数据加密。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“UU”
密钥索引	2	N	“00”～“19”，等于“99”时采用外部输入密钥
公钥明文 X	32	B	仅当公钥索引为“99”时有该域
公钥明文 Y	32	B	仅当公钥索引为“99”时有该域
数据长度	4	N	数据的字节数
数据	N	B	用于运算的数据。
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
应答码	2	A	“UV”
状态代码	2	N	正常为“00”，其他为错误
密文长度	4	N	
密文	N	B	
消息尾	Nt	A	与输入相同

7.3.3.4 SM2 私钥解密

用 SM2 的私钥对数据解密。

输入域	长度	类型	备注
消息头	Nh	A	

命令码	2	A	“UW”
密钥索引	2	N	“00”～“19”，等于“99”时采用外部输入密钥
密钥口令	8	A	密钥索引不等于“99”时存在
外部输入密钥长度	4	N	仅当密钥索引为“99”时有此域，下一个域长度
外部输入密钥	N	B	仅当密钥索引为“99”时有此域，SM2 密钥密文
密文长度	4	N	需要解密的数据长度
密文	N	B	需要解密的数据
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
应答码	2	A	“UX”
状态代码	2	N	正常为“00”，其他为错误
数据长度	4	N	明文数据的字节数
数据	N	B	明文
消息尾	Nt	A	与输入相同

7.3.3.5 SM2 签名

采用 SM2 密码算法对输入数据签名。签名的摘要可以由应用完成，也可以由密码机完成。密码机内部的摘要算法采用 SM3 算法。

输入域	**长度**	**类型**	**备注**
消息头	Nh	A	
命令码	2	A	“UQ”
密钥索引	2	N	“00”～“19”，等于“99”时采用外部输入密钥
密钥口令	8	A	密钥索引不等于“99”时存在
外部输入密钥长度	4	N	仅当密钥索引为“99”时有此域，下一个域长度
外部输入密钥	N	B	仅当密钥索引为“99”时有此域，SM2 密钥密文
摘要算法	2	N	01：不做摘要，此时数据长度应是 32 字节 02：用 SM3 在内部做摘要
用户标识长度	4	N	仅当摘要算法为 02 时有此域
用户标识	N	B	仅当摘要算法为 02 时有此域
数据长度	4	N	签名数据的字节数
数据	N	B	签名运算数据。 如果摘要值是 01，该数据应该是签名消息的摘要，且长度 32 字节。
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
应答码	2	A	“UR”
状态代码	2	N	正常为“00”，其他为错误
签名结果 R 部分	32	B	

签名结果 S 部分	32	B	
消息尾	Nt	A	与输入相同

7.3.3.6 SM2 验签

采用 SM2 密码算法验证签名。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“US”
密钥索引	2	N	“00”～“19”，等于“99”时采用外部输入密钥
密钥口令	8	H	密钥索引不等于“99”时存在
公钥明文 X	32	B	仅当公钥索引为“99”时有该域
公钥明文 Y	32	B	仅当公钥索引为“99”时有该域
签名结果 R	32	B	
签名结果 S	32	B	
摘要算法	2	N	01:不做摘要，此时数据长度应是 32 字节 02:用 SM3 在内部做摘要
用户标识长度	4	N	仅当摘要算法为 02 时有此域
用户标识	N	B	仅当摘要算法为 02 时有此域
数据长度	4	N	数据的字节数
数据	N	B	验签数据。 如果摘要算法是 01，该数据应该是验签数据的摘要，且长度为 32 字节。
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	Nh	A	与输入相同
应答码	2	A	“UT”
状态代码	2	N	
消息尾	Nt	A	与输入相同

7.3.3.7 产生消息摘要

根据输入消息产生指定摘要类型的数据摘要。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“GM”
算法类型	2	A	“01”—SM3 “02”—SHA1 其他保留，用于扩展其他算法
数据长度	5	N	摘要数据长度
数据	n	B	
消息尾	Nt	A	
输出域	**长度**	**类型**	**备注**
消息头	8	A	与输入相同

响应代码	2	A	“GN”
状态代码	2	N	正常为“00”，其他为错误
摘要长度	2	N	摘要长度
摘要	N	B	摘要
消息尾	Nt	A	与输入相同

7.3.3.8 数据加解密

使用工作密钥对数据进行数据加/解密操作。加/解密时数据长度应满足相应算法要求；加密数据时，加密机不对数据进行填充。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“5E”
密钥类型	3	H	(006)
密钥	16H/1A +32H/ 1A+48H	H	密钥由 LMK 保护
算法类型	1	A	‘1’—SM4 ‘2’—SM1 其他保留，用于扩展其他算法类型
加密模式	1	A	0—解密 1—加密
算法模式	1	A	0—ECB 模式 1—CBC 模式
IV 长度	1	N	如果加密模式为 CBC，该域存在，否则此字段不存在。
IV	N	H	如果加密模式为 CBC，则该域为加解密初始向量，否则此域不存在。 SM1：16 字节 SM4：16 字节
数据长度	4	N	SM1：16 字节对齐 SM4：16 字节对齐
数据	N	H	加解密数据
消息尾	Nt	A	

输出域	长度	类型	备注
消息头	Nh	A	与输入相同
响应代码	2	A	“5F”
状态代码	2	N	正常为“00”，其他为错误
数据长度	4	N	加解密数据长度
数据	N	H	加解密数据
消息尾	Nt	A	与输入相同

7.3.4 错误码

表 3 是金融数据密码机返回的通用错误码，各厂商可以添加自定义错误码，但不能和下表冲突。

表 3 通用错误码

代码	具体描述
00	正确
01	密钥奇偶校验错误
02	密钥校验错
03	无效密钥长度标识
04	密钥长度错误(不符合算法要求)
05	不匹配的密钥长度
06	无效密钥类型错误
07	无效的密钥方案
08	用户存储区域的内容无效。重启、掉电或重写
09	无效的输入数据(无效的格式,无效的字符,或者没有提供足够的数据)
10	控制台或打印机没有准备好或者没有连接好
11	密码机不在授权状态
12	无效的 PIN 块格式代码
13	PIN 长度小于 4 或大于 12
14	无效的 PIN 格式
15	PIN 不匹配
16	MAC 值不匹配
17	无效的索引值
18	无效参数
19	无效的账号
20	密钥函数被禁止
21	私钥错误;报告给管理员
22	无效摘要信息语法(仅仅无哈希模式)
23	无效公钥/私钥对
24	公钥长度错误
25	私钥长度错误
26	哈希算法对象标识错误
27	证书偏移值与长度错
28	无效的固件校验和
29	内部的硬件/软件错:RAM 已坏,无效的错误代码,等等
30	设备未正确初始化
31～255	预留

8 安全性要求

金融数据密码机的安全性应符合 GM/T 0028 的要求。

9 检测要求

9.1 功能检测

功能检测目的是验证功能实现的正确性。功能检测包括下列的强制检测项目。

9.1.1 初始化检测

金融数据器密码机正常启动后，首先需要进行初始化操作后才能正常工作，初始化操作主要包括系统初始配置、初始化管理员或操作员、初始密钥生成(或恢复)与安装，使设备处于正常工作状态。检测结果符合 5.1 要求。

金融数据密码机在未完成初始化操作，不能对外提供安全服务。

9.1.2 密码运算检测

金融数据密码机的密码运算测试程序由国家密码管理主管部门认可的检测机构设计提供。检测方法是将金融数据密码机的密码运算结果与已知的正确结果进行比较，如果计算结果和正确结果相同，则测试通过；否则，测试失败。

密码运算检测的范围应包括金融数据密码机提供的每个对称密码算法、非对称密码算法和杂凑算法的每个功能函数，如：加密、解密、杂凑、数字签名、验证签名等，其中对称密码算法的检测应测试支持的密码算法工作模式，如：ECB、CBC 等。密码运算检测的检测结果应符合 5.1 要求。

9.1.3 密钥管理检测

密钥管理检测范围包括密钥产生、密钥注入、密钥导入/导出、密钥备份/恢复/归档等操作，通过配备的管理工具进行测试。密钥管理检测结果应符合 5.2 要求。

9.1.4 随机数检测

随机数检测程序由国家密码管理主管部门认可的检测机构设计提供。金融数据密码机生成的随机数比特流作为测试样本，输入到随机数检测程序中检测随机数的质量。随机数检测结果应符合 5.3 和 6.3 要求。

9.1.5 访问控制检测

采用金融数据密码机配用的管理工具或管理界面进行访问控制检测。不同的管理操作应设置不同的操作权限，登录金融数据密码机的管理工具应具备完善的身份认证机制；金融数据密码机应拒绝任何非授权的访问或操作。金融数据密码机访问控制检测结果应符合 5.4 要求。

9.1.6 设备管理检测

采用金融数据密码机配用的管理工具或管理界面进行设备管理测试，包括系统的配置、管理员或操作员的产生、密钥管理等等。设备管理功能的实现应符合密码设备相关管理规范的要求。设备管理检测结果应符合 5.5 要求。

9.1.7 日志审计检测

采用金融数据密码机配用的日志管理工具或界面进行日志审计检测。日志内容包括:管理员操作行为,包括登录认证、系统配置、密钥管理等操作。异常事件,包括认证失败、非法访问等异常事件的记录。日志审计检测结果应符合 5.5.2 要求。

9.1.8 设备自检检测

金融数据密码机的设备自检功能主要包括密码算法正确性检查、硬件物理噪声源产生随机数的随机性检查、存储密钥和数据完整性检查,以及关键部件的正确性检测等。设备自检检测结果应符合 5.7 要求。

9.1.9 业务功能检测

金融数据密码机业务功能检测结果应符合第 7 章要求。

9.2 性能检测

9.2.1 概述

性能检测的目的是测试各项密码运算的速度指标,便于各厂商设备的横向对比,以及作为用户选择金融数据密码机的依据。

下列各项速度性能测试中的测试量由数据报文长度和测试次数决定。可以根据各个测试项的具体耗时情况,依照等比序列来选取测试次数,例如:测试次数 N 可以选择 1 次、10 次、100 次、1 000 次、……,分别测试后得到不同测试次数时的性能序列。数据报文长度的选择在各个速度性能测试项中分别定义。

在 9.2.6、9.2.8 和 9.2.9 中的各个测试项的速度性能的计算如下式所示:

$$S = 8LN/(1\ 024 \times 1\ 024T)$$

其中,S 为速度,单位为兆比特每秒(Mbit/s);L 为数据报文的长度,单位为字节;N 为测试次数;T 为测量所耗费的时间,单位为秒(s)。

在除 9.2.6、9.2.8 和 9.2.9 外的各个测试项的速度性能的计算如下式所示:

$$S = N/T$$

其中,S 为速度,单位为次每秒(tps);N 为测试次数;T 为测量所耗费的时间,单位为秒(s)。

9.2.2 PIN 加密性能测试

将一个 PIN 进行加密操作,重复操作 N 次,测量其完成时间 T。用于测试的数据由检测机构设定。测试应进行多次,结果取平均值。

PIN 加密性能单位统一为次每秒(tps)。

9.2.3 PIN 转加密性能测试

将一个由 LMK 保护的 PIN 块转加密为 ZPK 保护的 PIN 块,重复操作 N 次,测量其完成时间 T。用于测试的数据由检测机构选取。测试应进行多次,结果取平均值。

PIN 转加密性能单位统一为次每秒(tps)。

9.2.4 MAC 计算性能测试

计算一个随机的 256 字节数据的 MAC 值,重复操作 N 次,测量其完成时间 T。用于测试的数据

由检测机构选取。测试应进行多次，结果取平均值。

MAC 计算性能单位统一为次每秒(tps)。

9.2.5 ARQC 验证性能测试

验证一个 ARQC 值，重复操作 N 次，测量其完成时间 T。用于测试的数据由检测机构选取。测试应进行多次，结果取平均值。

ARQC 验证性能单位统一为次每秒(tps)。

9.2.6 对称密码算法的加解密性能测试

将一个定长数据报文进行加/解密操作，重复操作 N 次，测量其完成时间 T。用于测试的数据由检测机构选取，测试应进行多次，结果取平均值。

支持对称算法的多种工作模式，只需测试所支持的各种工作模式性能最高的模式的测试。应对所支持的所有使用方式(如加密、解密、数据摘要等)进行逐一测试。

对称密码算法的加解密性能单位统一为兆比特每秒(Mbit/s)。

9.2.7 非对称密码算法的加解密性能测试

将一个定长数据报文进行加/解密操作，重复操作 N 次，测量其完成时间 T。用于测试的数据由检测机构选取。测试应进行多次，结果取平均值。

支持多种非对称算法，应测试所支持的所有非对称密码算法及其各种应用模式。

非对称密码算法的加解密性能单位统一为次每秒(tps)。

9.2.8 数据杂凑算法性能测试

将一个定长数据报文进行摘要运算，重复操作 N 次，测量其完成时间 T。用于测试的数据由检测机构选取。测试应进行多次，结果取平均值。

数据杂凑算法性能单位统一为兆比特每秒(Mbit/s)。

9.2.9 随机数发生器性能测试

让金融数据密码机生成并输出长度为 L 的符合随机特性的随机序列 N 组，测量其完成时间 T。测试应进行多次，结果取平均值。

随机数发生器性能单位统一为兆比特每秒(Mbit/s)。

9.2.10 非对称密钥生成性能测试

让金融数据密码机按指定数量产生并输出密钥对，记录其完成时间 T。此项测试需进行多次，非对称密钥生成性能最终结果取多次的平均值。

非对称密钥生成性能单位统一为次每秒(tps)。

9.2.11 非对称密码算法签名性能测试

让金融数据密码机对 256 字节数据做非对称算法的签名计算，重复操作 N 次，测量其完成时间 T。用于测试的数据由检测机构选取。测试应进行多次，结果取平均值。

签名计算性能单位统一为次每秒(tps)。

9.2.12 非对称密码算法验签性能测试

让金融数据密码机对 256 字节数据做非对称算法的验证签名计算，重复操作 N 次，测量其完成时

间 T。用于测试的数据由检测机构选取。测试应进行多次，结果取平均值。

验证签名计算性能单位统一为次每秒(tps)。

9.3 环境适应性检测

环境适应性检测应按照 GB/T 9813—2000 中 5.8 的要求进行，其结果应符合该规范中“6.4 环境适应性”的要求。

9.4 安全检测

安全性检测应符合第 8 章的要求。

10 合格判定

除 9.2 以外的各项检测中，其任意一项检测结果不合格，判定为产品不合格。

GM/T 0045—2016

中华人民共和国密码
行业标准
金融数据密码机技术规范
GM/T 0045—2016
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2.5 字数 72 千字
2016年12月第一版 2016年12月第一次印刷
*
书号:155066·2-30309 定价 36.00 元

GM/T 0045-2016

打印日期:2019年4月11日 D088