ICS 35.040
L 80
备案号：

中华人民共和国密码行业标准

GM/T XXXX—XXXX

金融数据密码机技术规范

Specifications of Financial Cryptographic Server

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

××××-××-××发布　　××××-××-××实施

国家密码管理局 发布

目　次

前　言

本规范规定了金融数据密码机相关的技术规范，包括金融数据密码机的功能要求、硬件要求、软件要求、安全性要求和检测要求等内容，规范金融数据密码机的研制、使用和维护。金融及其相关机构的设备选型和横向评测提供指导和依据。

本规范由密码行业标准化技术委员会提出并归口。

本规范主要起草单位：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、济南得安计算机技术有限公司。

本规范主要起草人：李元正、张世雄、黄锦、张所成、徐明翼、王妮娜、郑海森

金融数据密码机技术规范

1　范围

本规范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。

本规范适用于金融数据密码机的研制，适用于金融安全业务使用金融数据密码机，也可用于指导金融数据密码机的检测。

2　规范性引用文件

下列文件中的条款通过本规范的引用而成为本规范的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本规范，然而，鼓励根据本规范达成协议的各方研究是否可使用这些的最新版本。凡是不注日期的引用文件，其最新版本适用于本规范。

GB/T 17964－2008信息技术 安全技术 分组密码算法的工作模式；

GB/T 4943-1995　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；

GM/T 0002-2012　SM4分组密码算法；

GM/T 0003-2012　SM2椭圆曲线公钥密码算法；

GM/T 0004-2012　SM3密码杂凑算法；

GM/T 0005-2012　随机性检测规范；

GM/T 0006-2012　密码应用标识规范；

GM/T AAAAA　　密码设备管理技术规范；

3　术语和定义

下列术语和定义适用于本规范。

3.1

金融数据密码机　Financial cryptographic server

用于金融领域，针对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。

3.2

对称密码算法 symmetric cryptographic algorithm

又称秘密密钥算法或单密钥算法，是加密和解密均采用同一秘密密钥进行变换的密码算法。

3.3

公钥密码算法 puclic-key cryptographic algorithm

又称非对称密码算法或双钥密码算法，是指加密密钥和解密密钥为两个不同密钥的密码算法。

3.4

杂凑算法 hash algorithm

杂凑算法是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

SM2

国家密码管理部门发布的商用非对称密钥密码算法，基于椭圆曲线非对称密钥密码算法理论，密钥长度为256位。

3.6

SM3

国家密码管理部门发布的商用消息杂凑算法，该算法产生的杂凑值长度为256位。

3.7

SM4

国家密码管理部门发布的商用对称密钥密码算法，SM4是一个分组密码算法，分组长度为128位，密钥长度为128位。

3.8

加密/解密 encrypt/ encryption /decrypt /decryption

加密是通过加密算法对明文进行变换产生密文的过程。解密是与加密过程相逆的过程，通过解密算法将密文转换成明文。

3.9

物理安全环境 Physically Secure Environment（PSE）

具有访问控制机制或其它安全机制的环境，设计上防止密钥部分或全部泄露、或环境中存储的其它秘密数据泄露等任何非授权访问。例如，具有不间断的访问控制、物理安全保护和监控的房间或安全实体。

3.10

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，例如：采用防撬手段防止密码机被非法开箱。

3.11

主密钥 Master Key（MK）

在密钥加密密钥和传输密钥的层次关系中，最高级的密钥加密密钥称为主密钥。也可称为主文件密钥（Master File Key）或本地主密钥（Local Master Key）。

3.12

密钥分隔 Key separation（KS）

保证每个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。

3.13

数据密钥 Data Key（DK）

指保护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。

3.14

校验值 Check Value（CV）

通过不可逆转算法计算的结果值，校验值通常在密钥下采用密码变换一个任意串的结果。没有密钥的情况下，计算正确的校验值是不可行的，不能通过校验值来测定一个密钥。

3.15

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，PIN只包含十进制数字。

3.16

密钥装载 Key Loading（KL）

手工或电子手段传送密钥到金融数据密码机中的过程。

3.17

手工密钥分发 Manual Key Distribution（MKD）

密钥通常以明文形态（采用物理保护措施），用密码信封等非电子手段分发的一种密钥分发方式。

3.18

手工密钥注入 Manual Key Entry（MKE）

用键盘等注入密钥到金融数据密码机。

3.19

衍生密钥 Derived Key（DK）

衍生密钥基码通过密码技术计算出的结果密钥。

3.20

衍生密钥基码 Base Derivation Key（BDK）

一个用来通过密码技术计算出其它密钥的密钥。

3.21

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

下列符号和缩略语适用于本规范。

ECB	（分组密码的）电子密本（工作方式）	(Electronic Codebook)
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)
OFB	（分组密码的）输出反馈（工作方式）	(Output Feedback)
Hash	散列函数运算，又称杂凑运算	(Hash Algorithm)
API	应用程序接口简称应用接口	(Application Program Interface)
PAN	主账号	（Primary Account Number）
PIN	个人识别码	（Personal Identification Number）
MAC	消息认证码	（Message Authentication Code）
CMAC	基于加密算法的消息认证码	（cipher-Based Message Authentication Code）
MK	主密钥	（Master Key）
DK	数据密钥	（Data Key）
MAK	MAC 计算密钥，属于数据密钥	（MAC Key）
PIK	PIN 加密密钥，属于数据密钥	（PIN Key）
LMK	本地主密钥	（Local Master Key）
ZMK	区域主密钥	（Zone Mastter 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）
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）

5 功能要求

5.1 密码算法

金融数据密码机必须配用国家密码管理部门认可的用于金融领域的密码算法。

5.1.1 对称密码算法

金融数据密码机须配用 SM4 对称密码算法，SM4 密码算法的实现遵循 GM/T 0002-2012。

为满足与遗留系统兼容要求以及其它系统（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 DES/3DES/AES 密码算法及国家密码管理部门认可的其它算法。

对称密码算法的工作模式至少应包括 ECB 和 CBC 两种模式。

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

5.1.2 公钥密码算法

金融数据密码机须配用 SM2 非对称密码算法， SM2 密码算法的实现遵循 GM/T 0003-2012。

为满足与遗留系统兼容要求以及其它系统（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部门认可的其它算法。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 密码杂凑算法

金融数据密码机须配用 SM3 杂凑算法，SM3 杂凑算法的实现遵循 GM/T 0004-2012。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 0003-2012。

为满足与遗留系统兼容要求以及其它系统（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/MD5 密码算法及国家密码管理部门认可的其它算法。

杂凑算法用于数字签名和验证、消息认证码生成与验证以及随机数生成。

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模块，金融数据密码机应该配备完整的密钥管理措施，密钥保护涵盖密钥的整个生命周期。密钥安全风险是指业务系统中的各种主控密钥和应用主密钥在分发、保存、使用中的泄露、篡改、非法替换的风险。

金融数据密码机必须提供密钥安全性的设计保障。安全性设计必须有明确的密钥保护措施、方法消除密钥安全风险，安全性设计必须通过设计评审。密码机有明确的安全性设计验证测试用例。

金融数据密码机必须在设计上保证不同类型密钥在逻辑上是分隔的，并且提供防止密钥类型混用的防护措施，具有检测密钥类型混用等错误的机制，例如：计算消息认证码时，如果参与 MAC 计算的密钥是 PIK，设备必须立即错误返回。

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。

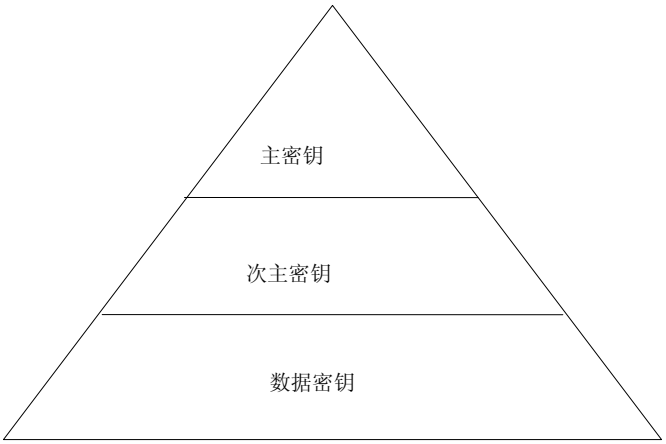

图 1 密钥结构图

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。主密钥的存储必须采用强安全措施，例如：主密钥存储存储在微电保护存储器中。主密钥不能以明文方式出现在密码机外，主密钥备份恢复须遵循多段方式、每段分人、多人分开保存的原则。

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。次主密钥必须加密存储，次主密钥必须加密保护后才能出现在密码机外。例如：采用主密钥保护分发。

数据密钥是实际保护金融业务数据安全的密钥，数据密钥必须加密存储，数据密钥必须加密保护后才能出现在密码机外。例如：采用次主密钥保护分发。

金融数据密码机中的密钥必须分层保护，保护原则为“使用少的保护使用多的“。顶层密钥（主密钥）只保护密钥加密密钥（次主密钥），会话密钥（数据密钥）由密钥加密密钥保护，不允许其它的密钥保护次序。

金融数据密码机必须提供安全机制防止密钥层次的混用，不同层次密钥在逻辑上应分开保存；在使用过程中，设备应能校验安全服务请求消息中使用的密钥层次是否正确，例如：不能用数据密钥保护区域主密钥，而是只能用主密钥保护区域主密钥。

5.2.3 密钥存储

金融数据密码机中主密钥必须安全存储，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必须遵循多段方式、每段分人、多人分开保存的原则。

次主密钥只能在系统备份时才能存储在密码机外，次主密码必须在主密钥的保护下才能存储在密码机外；数据密钥可以加密存储在密码机外，数据密钥必须在次主密钥的保护下才能存储在密码机外。

微电保护存储方案中应设计销毁密钥的触发装置。当触发装置被触发时，销毁微电保护所存储的所有密钥。采用微电保护的密钥可以采用明文方式存储。

5.2.4 密钥注入

密钥注入是一种安全的密钥分发方式，如果主密钥和次主密钥由外部设备产生，必须采用密钥注入的方式导入到密码机中，不能通过程序方式自动导入到密码机中。

密钥不允许以明文形态出现在金融数据密码机之外。明文形态的密钥部件在通过密码信封、码单、IC卡、USB KEY等形式输出时，必须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（KEK）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必须采用密钥分隔机制，分段传输、保存和注入，不同的密钥部件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

对长期保存的密钥，长期保存的密钥包括主密钥、次主密钥和数据密钥。金融数据密码机应具备备份/恢复功能。备份操作产生的备份文件必须以密文形式存储到到存储介质中，加密备份文件的密钥应有安全机制保证其安全。主密钥的备份须遵循多段方式、每段分人多人保存的原则。

备份出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中进行。

5.3 随机数生成和检测

金融数据密码机必须采用多个硬件物理噪声源的真随机数产生器器件产生密钥。用于产生密钥的随机数必须满足 GM/T 0005-2012。

金融数据密码机配用的随机数发生器必须通过送样检测、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 0005-2012 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 0005-2012 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 0005-2012 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 20000 比特。
- 检测项目：依据 GM/T 0005-2012 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 小时。

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 0005-2012 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产生失效后，密码机不能对外提供任何安全服务。

5.4 访问控制

金融数据密码机必须提供访问控制功能，防止非授权访问密码机引起的安全风险。访问控制包括密码机的管理、使用和业务等方面要求的访问控制。

5.4.1 管理要求

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；密码机必须提供管理员身份鉴别

机制。

金融数据密码机的物理访问控制实体（如：机箱锁）必须由授权管理员安全保存。

融数据密码机必须提供网络访问控制机制，只有安全管理员才能配置明确允许的主机访问密码机的安全策略。网络访问控制至少具有验证合法主机的 IP 地址的功能。

5.4.2 使用要求

金融数据密码机必须提供措施防止非授权打开设备，打开金融数据密码机需由物理上的访问控制措施限制。

无论在任何情况下，设备被打开，设备必须立即、自动毁掉设备中以明文状态存储的密钥，例如：存储在微电保护存储器中的主密钥。密文形态存储的密钥可以不自动销毁。

金融数据密码必须放置在物理安全的环境中使用。

5.4.3 业务要求

金融数据密码机必须具有授权状态和非授权状态，从非授权状态进入授权状态必须通过完善的身份认证；从授权状态到非授权状态不需要身份认证。

金融数据密码机中的关键安全操作必须在授权状态下进行，下列操作是关键安全操作。

密钥注入

密钥备份/恢复

密钥产生

密钥分散

密钥导入/导出

密钥归档

密钥销毁

5.5 设备管理

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 GM/T AAAAA 《密码设备管理规范》的要求。

5.5.1 设备自检

金融数据密码机须提供设备自检功能，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：

1. 操作日志，记录管理员、用户的操作行为，包括系统配置参数的修改等。
2. 审计日志，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。
3. 运行日志，记录设备的运行工作状态。

6 硬件要求

6.1 物理接口

金融数据密码机应物理分隔服务接口和管理接口，服务接口和管理接口可采用以太网、USB、串口或者其它接口形式。

6.2 状态指示器

金融数据密码机必须提供的工作状态指示器。

6.3 随机数发生器

随机数产生器须采用国家密码管理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必须符合 GB/T 9813－2000 《微型计算机通用规范》中关于“气候环境适应性”的规定要求。

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 小时。

7 安全业务要求

7.1 基本要求

金融数据密码机的通过应用编程接口对用户提供安全服务，实现安全功能。

金融数据密码机的底层软件应采用模块化设计，防止不同功能模块相互影响。金融数据密码机应通过技术措施防止用户的非法调用。

7.2 应用编程接口（API）

金融数据密码机的应用编程接口必须遵循本规范规定。

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。磁条卡应用主要适应基于磁条的银行卡，IC 卡应用基于 IC 卡技术的银行卡，国密算法 IC 卡应用在 IC 卡应用的基础上，增加国家密码管理局发布的密码算法的支持。

7.2.1 数据缩写

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	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；其它数据按从前往后、从左往右的顺序传输。

7.3 业务功能要求

金融数据密码机的业务功能要求通过外层用户的应用编程接口方式体现和说明。金融业务要求的安全服务功能根据不同应用类型划分，即磁条卡应用、IC 卡应用和基础密码运算服务等 3 类。下面分别描述。

7.3.1 磁条卡应用

1) 产生密钥

通过随机产生或分散产生的方式生成传输密钥分量，并将密钥分量的值写入 IC 卡或打印到密钥信封。密钥指定分量个数打印密码信封。

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 ‘10’－打印密钥信封 ‘01’－写入 IC 卡 ‘11’－打印密钥信封和写入 IC 卡 ‘12’－RSA 密钥加密
密钥类型	1	A	此处密钥不涉及加密 ‘1’－LMK, ‘2’－ZMK, ‘3’－MAK ‘4’－PIK, ‘5’－TMK, ‘6’－CVK ‘7’－PVK ‘8’—WWK ‘9’－TGMK ‘A’—ZEK
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
分散数	1	A	‘1’-‘3’，仅当模式＝1 时存在
分散数据 1	N	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	N	H	分散因子 N，仅当 Mode＝1 时存在。
公钥长度	4	A	当介质类型＝’12’时存在
公钥	N	B	输入公钥数据，DER 编码。当介质类型＝‘12’时存在
打印份数	1	A	打印密码时存在
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”，其它为错误
密钥	1A+16/ 1A+32/ 1A+48	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 MediaType＝‘12’时存在）
Kcv	16	H	校验码
消息尾	Nt	A	与输入相同

2) 导入密钥

将导入密钥 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	查看密钥类型表
ZMK	16H/32H/ 1A+32H/ 1A+48H	H	用 LMK (04,05)加密
密钥	16H/ 1A+32H/ 1A+48H	H	用 ZMK 加密
LMK 密钥方案	1	A	用 LMK 加密方式标志
Atalla 变体	1/2	N	可选项，用在 Atalla 系统
分隔符	1	A	可选项，值为“;”，如果出现此域，则必须出现下面密钥校验值参数
校验值	6	H	可选项，取密钥校验值的前六个 ASCII
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”，其它为错误
LMK 密文	16H/ 1A+32H/ 1A+48H	H	LMK 加密的密钥密文
校验码	16	H	密钥对 0 加密结果，目前输出类型为 0
消息尾	Nt	A	与输入相同

3) 导出密钥

将导入密钥 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	查看密钥类型表
ZMK	16H/32H/ 1A+32H/ 1A+48H	H	用 LMK (04,05)加密
密钥	16H/ 1A+32H/ 1A+48H	H	用 LMK 加密
ZMK 密钥方案	1	A	用 ZMK 加密方式标志
Atalla 变体	1/2	N	可选项，用在 Atalla 系统
分隔符	1	A	可选项，值为“;”，如果出现此域，则必须出现下面密钥校验值参数
校验值	6	H	可选项，取密钥校验值的前六个 ASCII
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”，其它为错误
ZMK 密文	16H/ 1A+32H/	H	ZMK 加密的密钥密文

	1A+48H		
校验码	16	H	密钥对 0 加密结果，目前输出类型为 0
消息尾	Nt	A	与输入相同

4) 合成 ZMK

从三个 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”
ZMK 分量 1	16H/32H/ 1A+32H/ 1A+48H	H	ZMK 分量一，用 LMK（04,05）变种加密
ZMK 分量 2	16H/32H 1A+32H/ 1A+48H	H	ZMK 分量二，用 LMK（04,05）变种加密
ZMK 分量 3	16H/32H 1A+32H/ 1A+48H	H	ZMK 分量三，用 LMK（04,05）变种加密
Atalla 变体	1/2	N	可选项，用在 Atalla 系统
分隔符	1	A	可选项，值为“;”，如果出现此域，则必须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	“GH”
状态代码	2	N	正常为“00”，其它为错误
ZMK 密文	16H/32H 1A+32H/ 1A+48H	H	用 LMK（04,05）加密
校验码	16H/6H	H	ZMK 对 0 加密结果，根据 KCV 类型决定输出长度
消息尾	Nt	A	与输入相同

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”
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”，其它为错误
密钥密文	N	A	对应 LMK 加密的结果
消息尾	Nt	A	与输入相同

6) TAK 从 LMK 到 TMK

将 TAK 从 LMK 保护转为 TMK 保护。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“AG”
TMK	16H/ 1A+32H/ 1A+48H	H	用 LMK(14,15)加密
TAK	16H/ 1A+32H/ 1A+48H	H	用 LMK(16,17)加密
分隔符	1	A	可选项，值为“;”，如果出现此域，则必须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
TMK 密钥方案	1	A	可选项，用 TMK 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	“AH”
状态代码	2	N	正常为“00”，其它为错误
TAK 密文	16H/ 1A+32H/ 1A+48H	H	用 TMK 加密
消息尾	Nt	A	与输入相同

7） TAK 从 LMK 到 ZMK

将加密 TAK 从 LMK 保护转为 ZMK 保护，并计算 TAK 的校验值。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“MG”
ZMK	16H/32H 1A+32H/ 1A+48H	H	用 LMK(04,05)加密
TAK	16H/ 1A+32H/ 1A+48H	H	用 LMK(16,17)加密
Atalla 变体	1/2	N	可选项，用在 Atalla 系统

分隔符	1	A	可选项，值为“;”，如果出现此域，则必须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
状态代码	2	A	“MH”
出错代码	2	N	正常为“00”，其它为错误
TAK 密文	16H/ 1A+32H/ 1A+48H	H	用 ZMK 加密
校验码	16/6	H	TAK 对 0 加密结果，根据 KCV 类型决定输出长度
消息尾	Nt	A	与输入相同

8) TAK 从 ZMK 到 LMK

将加密 TAK 从 ZMK 保护转为 LMK 保护，并计算 TAK 的校验值。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“MI”
ZMK	16H/32H/ 1A+32H/ 1A+48H	H	用 LMK(04,05)加密
TAK	16H/ 1A+32H/ 1A+48H	H	用 ZMK 加密
Atalla 变体	1/2	N	可选项，用在 Atalla 系统
分隔符	1	A	可选项，值为“;”，如果出现此域，则必须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
状态代码	2	A	“MJ”
出错代码	2	N	正常为“00”，其它为错误
TAK 密文	16H/ 1A+32H/ 1A+48H	H	用 LMK(16,17)加密
校验码	16/6	H	TAK 对 0 加密结果，根据 KCV 类型决定输出长度
消息尾	Nt	A	与输入相同

9) 生成密钥校验值

计算送入加密机的 ZMK、ZPK、TMK/TPK/PVK、TAK 密钥的校验值（不支持双长度的 ZMK）。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“KA”
密钥	16H/ 1A+32H/ 1A+48H	H	LMK 加密加密的 ZMK 或 ZPK 或 TMK/TPK/PVK 或 TAK
密钥类型	2	N	“00”：ZMK “01”：ZPK “02”：TMK/TPK/PVK “03”：TAK
分隔符	1	A	可选项，值为“;”，如果出现此域，则必须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”，其它为错误
校验码	16/6	H	加密结果，根据 KCV 类型决定输出长度
消息尾	Nt	A	与输入相同

10) 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”
PIN	7	H	4-6 位数值数据，3-1 位“F”
PAN	12	N	主帐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”，其它为错误
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

11) 解密 PIN

解密密文 PIN。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“NG”

PAN	12	N	主帐号去掉校验位的最后 12 位
PIN 密文	7	N	用 LMK(02,03)加密，4-6 位数值数据，3-1 位“F”
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	“NH”
状态代码	2	N	正常为“00”，其它为错误
PIN	7	N	4-6 位明文 PIN，3-1 位“F”
引用数	12	N	利用 LMK(18,19)对主帐号加密后产生得到
消息尾	Nt	A	与输入相同

12) 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”
ZPK	16H/ 1A+32H/ 1A+48H	H	LMK（06,07）加密
PIN 块	16	H	ZPK 加密
PIN 格式	2	N	PIN 块格式
PAN	12	N	主帐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”，其它为错误
消息尾	Nt	A	与输入相同

13) 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”
ZPK	16H/ 1A+32H/ 1A+48H	H	LMK (06,07)加密
PIN 块	16	H	ZPK 加密(Pin 块的密文)
PIN 格式	2	N	
主帐号	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”，其它为错误
PIN	7	N	LMK（02,03）加密
消息尾	Nt	A	与输入相同

14) 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”
TPK	16H/ 1A+32H/ 1A+48H	H	LMK（14,15）加密
PIN 块	16	H	TPK 加密
PIN 格式	2	N	PIN 块格式
PAN	12	N	主帐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”，其它为错误
PIN	7	N	LMK（02,03）加密
消息尾	Nt	A	与输入相同

15) 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”
ZPK	16H/ 1A+32H/ 1A+48H	H	LMK（06,07）加密
PIN 格式	2	N	PIN 块格式
PAN	12	N	主帐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”，其它为错误
PIN 块	16	H	ZPK 加密
消息尾	Nt	A	与输入相同

16) 产生终端 MAC

利用 TAK 计算 MAC 值。

输入域	长度	类型	备注

消息头	Nh	A	
命令码	2	A	“MA”
TAK	16H/ 1A+32H/ 1A+48H	H	LMK（16,17）加密
MAC 数据	N	A	N 在 1-2048 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	“MB”
状态代码	2	N	正常为“00”，其它为错误
MAC	8	H	
消息尾	Nt	A	与输入相同

17) 验证终端 MAC

利用 TAK 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”
TAK	16H/ 1A+32H/ 1A+48H	H	LMK（16,17）加密
MAC	8	H	用于验证的 MAC 码
MAC 数据	N	A	N 在 1－2048 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”，其它为错误
消息尾	Nt	A	与输入相同

18) 验证并转换终端 MAC

用 SourceTAK 验证输入的 MAC 值，然后再利用 DestTAK 重新计算 MAC 并返回计算结果。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“ME”
SourceTAK	16H/ 1A+32H/ 1A+48H	H	LMK(16,17)加密
DestTAK	16H/ 1A+32H/ 1A+48H	H	LMK(16,17)加密
MAC	8	H	用户验证的 MAC 码
MAC 数据	N	A	N 在 1 至 2048 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	“MF”

状态代码	2	N	正常为“00”，其它为错误
MAC	8	H	DestTAK 计算
消息尾	Nt	A	与输入相同

19) 产生 CVV

产生卡校验码 CVV。

输入域	A	类型	备注
消息头	Nh	A	
命令码	2	A	“CW”
CVK_A/B	32/1A+32	H	用 LMK（14,15）加密
主帐号	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”，其它为错误
CVV	3	N	卡校验码
消息尾	Nt	A	与输入相同

20) 验证 CVV

验证卡校验码 CVV。

输入域	A	类型	备注
消息头	Nh	A	
命令码	2	A	“CY”
CVK_A/B	32/1A+32	H	用 LMK（14,15）加密
CVV	3	N	验证的 CVV
主帐号 r	n	N	主帐号，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”，其它为错误
消息尾	Nt	A	与输入相同

21) 打印密码信封

将 PIN 和相关数据输出到与加密机串口连接的串口打印机上。

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’;
PAN	12	N	主帐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”，其它为错误
PIN 校验值	L+12	N	输入的密文 PIN(长度为用户设定的 PIN 长度+1) + 输入帐号号后 10 位（N） + 2 位校验数字（N）
消息尾	Nt	A	与输入相同

7.3.2 IC 卡应用

1) 分散密钥加密

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	N	A	
命令码	2	A	“V2”
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，‘X’+双倍长密钥密文
密钥分散次数	1	N	‘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	N	‘1’：加密、‘0’：解密
填充模式	1	N	‘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	
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	N	正常为“00”，其它为错误
输出数据长度	4	N	
输出数据		H	

2) 产生 RSA 密钥对

随机生成一对 RSA 密钥。

输入域	长度	类型	备注
消息头	8	A	
命令码	2	A	“EI”
模式	1	A	“0”－产生密钥并保存在 HSM 内，只输出公钥 “1”－产生密钥并保存在 HSM 内，输出公钥和 LMK 保护私钥 “2”－产生密钥，输出公钥和 LMK 保护的私钥 “3”－产生密钥并保存在 HSM 内，不输出公私钥 “4”-产生密钥并将密钥存入到 IC 卡备份
密钥长	4	A	模长位数，最小“0512”,最大“2048”（0512、1024、1152、1408、1984、2048）
公钥编码	2	N	输出公钥编码规则。如果 Mode=3 时，该域不存在。 01：DER 编码 02：PEM 编码
密钥索引	4	1A+3H	产生密钥存储在 HSM 内的索引号。模式!=0 时，该域不存在，如：G000
指数长度	4	N	可选参数，如果存在表示后续指数按十进制位的长度
指数	N	N	可选参数，必须为奇数，如果不存在，默认指数为 65537
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	“EJ”
状态代码	2	N	正常为“00”，其它为错误
公钥	n	B	编码公钥，模式=3，该域不存在。
私钥长度	4	N	私钥长度，模式=0 or 3，该域不存在。
私钥	n	B	私钥，被 LMK 加密。模式=0 or 3，该域不存在。

3) 分解 RSA 私钥分量

分解 RSA 私钥，并用保护密钥加密输出。

输入域	长度	类型	备注
消息头	8	A	
命令码	2	A	“UA”
保护密钥类型	3	A	密钥类型
保护密钥密文	1A+32H/	H	LMK 加密 ‘X’+双倍长 key 密文
保护密钥 分散次数	1	N	‘0’、 ‘1’、 ‘2’、 ‘3’
保护密钥 分散数据	N*16	H	分散次数为 0，该域不存在
私钥长度	4	A	
私钥	N	A	保护密钥加密保护
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	“V7”
状态代码	2	N	
nModeLen	4	N	模长度
Mode	N	A	模
eLen	4	N	指数长度
e	N	A	指数
dLen	4	N	指数长度
d	N	A	指数

Prime1Len	4	N	
Prime1	N	A	
Prime2Len	4	N	
Prime2	N	A	
Pexp1Len	4	N	
Pexp1	N	A	
Pexp2Len	4	N	
Pexp2	N	A	
coefLen	4	N	
coef	N	A	

4) 公钥运算

采用 RSA 公钥对输入的数据加密。

输入域	长度	类型	备注
消息头	8	A	
命令码	2	A	“UK”
加解密标志	1	N	‘0’－ 解密，‘1’－ 加密
填充模式	1	N	‘0’－ no pad ‘1’－ PKCS#1 v1.5 ‘2’－ OAEP
消息类型	1	N	‘1’－ Hex、‘0’ －二进制
公钥编码格式	1	N	‘1’－ DER
公钥长度	4	N	公钥长度 (长度为 0 时，用 HSM 内部密钥)
公钥	4	N	公钥长度为 0 时，表示加密机内 RSA 密钥索引。
	n	H/B	公钥长度不为 0 时，为外部传入的 RSA 公钥。
数据长度	4	N	数据长度
数据	n	H/B	数据
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	“UL”
状态代码	2	N	正常为”00”，其它为错误
数据长度	4	N	
数据	n	B	公钥加密的结果

5) 外部私钥运算

导入私钥对数据进行加解密运算。

输入域	长度	类型	备注
消息头	8	A	
命令码	2	A	“VA”
加解密标志	1	N	‘1’：加密 ‘0’：解密
填充模式	1	N	‘0’－ no pad ‘1’－ PKCS#1 v1.5 ‘2’－ OAEP
私钥长度	4	N	私钥长度
保护密钥类型	3	A	密钥类型
保护密钥密文	1A+32H/	H	LMK 加密 ‘X’+双倍长 key 密文

保护密钥分散次数	1	N	‘0’、‘1’、‘2’、‘3’
保护密钥分散数据	N*16	H	分散次数为 0，该域不存在
私钥	n	H	外部传入的 RSA 私钥（由保护密钥加密）。
数据长度	4	N	数据长度
数据	n	H	数据
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	“VB”
状态代码	2	N	正常为”00”，其它为错误
数据长度	4	N	
数据	n	H	私钥加解密的结果

6) 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	8	A	
命令码	2	A	“GM”
机制	2	A	“01”－SHA-1（默认） “02”－MD5 “04”－SHA-256 “05”－SM3
数据长	5	N	摘要数据长度
数据	n	B	
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”，其它为错误
摘要长度	2	N	摘要长度
摘要	N	B	摘要

7) RSA 签名

使用私钥对数据计算签名。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“EW”
HASH 标识	2	N	‘01’=SHA-1 ‘02’=MD5 ‘03’=ISO 10118-2，返回 16bytes ‘04’=No hash
签名标识	2	N	01
填充模式标识	2	N	“01”=PKCS#1 v1.5 “02”=OAEP
数据长度	4	N	签名数据长度，4 位 10 进制
数据	n	B	签名数据
分割符	1	A	‘;’
私钥索引	2	N	0~19 读加密机里的密钥 99 读外部传入的密钥的密钥

私钥长度	4	N	可选，当’私钥索引’大于 20 时有效。512～2048
私钥	n	B	可选，当’私钥索引’大于 20 时有效。用 LMK(34,35)解密
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	“EX”
出错代码	2	N	正常为”00”，其它为错误
签名长度	4	N	4 位 10 进制
签名	n	B	计算出的签名
消息尾	Nt	A	与输入相同

8) 安全报文计算

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	8	A	
命令类型	2	A	VC
密钥类型	3	A	主控密钥类型 默认为 WWK(006)
主控密钥	16H/ 1A+32H/ 1A+48H	H	LMK 加密
主控密钥分散次数	1	N	‘0’、‘1’、‘2’、‘3’
主控密钥分散算法	1	N	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	16H/ 1A+32H/ 1A+48H	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
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”，其它为错误
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

9) RSA 验签

使用公钥验证签名数据是否正确。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“EY”
摘要方法	2	N	“01”=SHA-1 “02”=MD5 “03”=ISO 10118-2, 返回 16bytes “04”=No hash
签名标识	2	N	01
填充模式	2	N	“01”=PKCS#1 v1.5 “02”=OAEP
签名长度	4	N	签名的字节长度
签名	n	B	待验证的签名
分隔符	1	A	‘;’
数据长度	4	N	用于签名的信息数据的字节长度
数据	n	B	要签名的信息
分割符	1	A	‘;’
MAC	4	B	对于公钥和证明数据的 MAC，用 LMK 对 36-37 计算。 0000：不需进行 MAC 校验。
公钥	n/1A+3H		公钥，用 ASN.1 格式编码的 DER（模、指数的序列）
验证数据	n	A	可选，（不能包含字符’;’）
消息尾	Nt	A	
输出域	长度	类型	备注
消息头	Nh	A	与输入相同
打印前状态			
响应代码	2	A	“EX”
出错代码	2	N	正常为”00”，其它为错误
消息尾	Nt	A	与输入相同

10) ARQC/ARPC 产生或验证

支持 EMV2000 规范和 PBOC2.0 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	8	A	
命令码	2	A	“VM”
IC 卡类型	1	A	‘1’ / ‘2’
模式	1	A	’0’-只验证 ARQC ’1’-验证 ARQC,验证成功后 ARPC ’2’-只产生 ARPC
密钥类型	3	A	”00A”
密钥	16H/ 1A+32H/ 1A+48H	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 8 的整数倍。(模式为’0’、’1’时存在)
ARC	4	A	(模式为’1’、’2’时存在)

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”，其它为错误
ARPC 值	16	A	

11) 脚本加解密

支持 EMV2000 规范和 PBOC2.0 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	8	A	
命令码	2	A	“VI”
操作类型	1	N	‘1’：加密　　‘0’：解密
IC 卡类型	1	N	‘1’ / ‘2’
算法应用模式	1	N	‘0’：ECB　　‘1’：CBC
主密钥类型	3	A	”00A”
加密主密钥	16H/ 1A+32H/ 1A+48H	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	
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”，其它为错误
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。

12) 计算脚本 MAC

支持 EMV2000 规范和 PBOC2.0 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			
命令码	2	A	“VK”
IC 卡类型	1	N	‘1’ / ‘2’
密钥类型	3	A	
安全报文认证主密钥	16H/ 1A+32H/ 1A+48H	H	LMK 加密
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”
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。

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”，其它为错误
MAC	16	A	MAC

13) 验证 TC

支持 EMV2000 规范和 PBOC2.0 规范，TC 的验证。

输入域	长度	类型	备注
消息头	8	A	
命令码	2	A	“VE”
IC 卡类型	1	N	‘1’ / ‘2’
密钥类型	3	A	”00A”
密钥	16H/ 1A+32H/ 1A+48H	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 TC 值	16	A	
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。
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	“VF”
状态代码	2	N	正常为”00”，其它为错误

14) PIN 转加密

用私钥解密出明文 PIN，再用 PIK 加密 PIN 并输出（RSA 转 3DES）。PIN 为登录密码或交易密码。注：登录密码支持数字、大小写字母、标点符号，交易密码支持数字。

输入域	长度	类型	备注
消息头	Nh	A	
命令码	2	A	“W0”
模式	2	A	“01”：只输出 PIK 加密的 PIN 块 “02”：.只输出 PIN 的 Hash 值 “03”：输出 PIK 加密的 PIN 块和 PIN 摘要值
算法标志	2	A	“01”－SHA-1 “02”－MD5
索引	4	N	“FFFF”：使用外部密钥；”0000”到”0019”：使用内部密钥
私钥长度	4	N	私钥长度(使用外部密钥时存在)
私钥		B	LMK(34-35)加密的私钥密文(使用外部密钥时存在)
输出 PIN 格式	2	A	PIN Block 的格式(’01’ ； ’08’) ’01’： ANSI 9.8 的 PIN 格式（8 字节 BCD 码）; ’08’： 银联互联网支付密码格式（24 字节 ASCII 码）。
PIN 块长度	4	N	公钥加密的 PIN 块长度
PIN 块	N	H	公钥加密的 PIN 块
PIK 密文	1A+32H/	H	LMK(06-07)加密，‘X’+双倍长密钥密文
输出帐号	N	N	加密 PIN 的帐号（需要时存在）

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	“W1”
状态代码	2	N	正常为”00”，其它为错误
密文 PIN	N	H	PIK 加密的 PIN 块，(模式=”01”、”03”时存在)
摘要长度	2	N	模式=”02”、”03”时存在
摘要		H	模式=”02”、”03”时存在
消息尾	Nt	A	与输入相同

7.3.3 基础密码运算服务

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	N	1：签名；2：加密；3：签名和加密
密钥索引	2	N	“00”－“20”：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	H	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”，其它为错误
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

2) 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”-“20”，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
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，此时数据长度必须是 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”，其它为错误
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

3) 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”~”20”，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，此时数据长度必须是 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

4) 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”~”20”，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
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”，其它为错误
密文长度	4	N	
密文	N	B	
消息尾	Nt	A	与输入相同

5) 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”~”20”，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
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”，其它为错误
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

6) 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	8	A	
命令码	2	A	“UY”
算法类型	1	A	1：3DES、7：SM4
SM2 私钥密文	32	B	LMK（36,37）加密的 SM2 私钥

加密密钥类型	3	A	密钥类型
加密计算密钥	16H/ 1A+32H/ 1A+48H	H	LMK 加密
加密算法模式	1	N	‘0’：ECB　　’1’：CBC
加密 IV	N	H	CBC 模式时存在 3DES ： 16 字节 SM4：　16 字节
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”，其它为错误
SM2 私钥密文	64	H	加密密钥加密（输出为 ASCII 码）

7) 数据加解密

使用工作密钥二进制流数据进行数据加解密操作。加解密时数据长度必须满足相应算法要求；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	“B8”
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	1：3DES、2：SM1、7：SM4
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	N	H	如果加密模式为 CBC，则该域为加解密初始向量，否则为空。 3DES：16 字节 SM1：　16 字节 SM4：　16 字节
数据长度	4	N	3DES：16 字节对齐 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	“B9”
状态代码	2	N	正常为”00”，其它为错误
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 API 错误码

API 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。

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

8.1 密码算法

金融数据密码机应至少具备公钥密码算法、分组密码算法和密码杂凑算法。密码算法配用须符合本规范 5.1 节的规定。

8.2 密钥管理

金融数据密码机在密钥管理方面，应满足以下要求：

1) 管理密钥的使用不对应用系统开放；
2) 除公钥外，所有密钥均不能以明文形式出现在密码机外；
3) 内部存储的密钥应具备防止解剖、探测和非法读取有效的密钥保护机制；
4) 内部存储的密钥应具备防止非法使用和导出的权限控制机制；

5） 应具备防止不同类型密钥混用的措施；

8.3 系统要求

所使用的操作系统，除满足密码机的服务和管理功能要求之外，其余功能应全部关闭或裁减。

8.4 使用要求

金融数据密码机只接受合法的操作指令，非法指令应拒绝接受，而且不报错，防止非法用户利用非法指令返回错误码探测设备。

8.5 管理要求

8.5.1 管理员管理

金融数据密码机应设置管理员并分配权限，进行系统配置、密钥生成、密钥注入、密钥导入/导出、密钥备份/恢复/归档等操作。管理员应持有身份信息的硬件装置，与登录口令相结合登录系统，进行管理操作前应通过身份鉴别。

8.6 设备管理

8.6.1 设备初始化

金融数据密码机的初始化，除必须由厂商进行的操作外，系统配置、密钥管理、管理员管理员管理等关键安全操作均应由用户方设备管理人员完成。

8.7 设备自检

应对密码运算部件等关键部件进行正确性检查。

应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。

8.8 设备物理安全防护

符合本规范在工艺设计、密码设备设计、硬件配置等方面要采取相应的保护措施，保证设备基本的物理安全防护功能。

9 检测要求

检测要求规定了金融数据密码机的通用检测内容和方法。检测应包括外观和结构检查、提交文档的检查、功能检测、性能检验、敏感数据的保护与使用检测和物理检测等。

9.1 外观和结构的检查

根据产品的物理参数，对金融数据密码机的外观、尺寸、内部部件及附件进行检查。

9.2 提交文档的检查

金融数据密码机研制单位按照国家密码管理部门检测要求提交相关文档资料，作为检测依据。文档资料应包含但不限于以下内容：

1） 后台服务程序、应用编程接口和客户端管理软件的结构框图、流程图和基本功能的源代码；
2） 开机自检的工作原理说明；
3） 自测程序的工作原理说明；
4） 敏感数据信息的存储和使用说明；
5） 物理防护措施说明；
6） 技术工作总结报告；
7） 安全性设计报告；
8） 安装使用说明。

9.3 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。

9.3.1 初始化检测

金融数据器密码机正常启动后，需要首先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。检测结果符合本规范 5.1 和 8.5.2.1 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。

9.3.2 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得正确结果进行比较，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必须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必须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 和 8.1 要求。

9.3.3 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本规范 5.2 和 8.2 要求。

9.3.4 随机数检测

随机数检测程序由国家密码管理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本规范 5.3 和 6.3 要求。

9.3.5 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。不同的管理操作必须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本规范 5.5 要求。

9.3.6 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GM/T AAAAA 《密码设备管理规范》的要求。设备管理检测结果应符合本规范5.6和8.5.2要求。

9.3.7 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本规范 5.7 要求。

9.3.8 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、随机数产生器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本规范 5.8 和 8.5.2.2 要求。

9.3.9 应用编程接口（API）检测

金融数据密码机应用编程接口必须遵循本规范规定的应用编程接口，正确的调用环境和调用过程，API 函数应该返回正确的结果，并完成相应功能；对于设定的不正确的调用环境和调用过程，API 函数应返回相应的错误代码。

9.3.10 管理工具检测

采用金融数据密码机配用的管理工具或管理界面进行管理工具检测。管理工具检测结果应符合本规范 7.3 要求。

9.4 性能检测

9.4.1 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、1000 次…等，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 9.4.1、9.4.3 和 9.4.4 中包含的各个测试项的速度性能的计算如下式所示：

$$S = 8LN/(1024\times1024T)$$

其中，S为速度，单位为 Mbps(兆比特/秒)；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。

在 9.4.2 中包含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 tps（次/秒）；N为测试次数；T为测量所耗费的时间，单位为秒。

9.4.2 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选取。测试应进行多次，结果取平均值。

PIN 加密性能单位统一为 tps（次/秒）。

9.4.3 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 tps（次/秒）。

9.4.4 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 tps（次/秒）。

9.4.5 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 tps（次/秒）。

9.4.6 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进行测试。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 Mbps(兆比特/秒)。

9.4.7 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，必须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 tps（次/秒）。

9.4.8 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 Mbps(兆比特/秒)。

9.4.9 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 Mbps(兆比特/秒)。

9.4.10 非对称密钥生成性能测试

让金融数据密码机生成并输出指定数量的密钥对，测量其完成时间 *T*。测试应进行多次，结果取平均值。

非对称密钥生成性能单位统一为 tps（对/秒）。

9.5 环境适应性检测

环境适应性检测应按照 GB/T 9813－2000 规范中“5.8 环境试验”的要求进行，其结果应符合该规范中“4.8 环境要求”的要求。

9.6 其他检测

外观和结构检查、提交文档的检查按照相关标准进行。

10 合格判定

本规范中，除9.3.6、9.3.7、9.3.10、9.4以及9.5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。