ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0046—2024
代替 GM/T 0046—2016

金融数据密码机检测规范

Test specification for financial cryptographic server

2024-12-27 发布　　2025-07-01 实施

国家密码管理局　　发布

目　　次

前言 …… Ⅲ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　检测环境 …… 2
6　检测内容及检测方法 …… 3
6.1　检测项目 …… 3
6.2　外观和结构检查 …… 3
6.3　功能检测 …… 3
6.4　性能检测 …… 7
6.5　其他检测 …… 8
7　送检技术文档要求 …… 8
8　判定规则 …… 8
附录 A（规范性）　检测项目列表 …… 9

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GM/T 0046—2016《金融数据密码机检测规范》，与GM/T 0046—2016相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 更改了外观和结构的检查中金融数据密码机部件和端口的检查要求（见6.2，2016年版的6.2）；

b) 更改了初始化检测中系统初始化配置、初始化管理员或操作员、初始化密钥生成（或恢复）与安装的检测方法（见6.3.1，2016年版的6.3.1）；

c) 更改了密码算法检测中对称密码算法、非对称密码算法和杂凑算法正确性的检测方法（见6.3.2，2016年版的6.3.2）；

d) 更改了密钥管理检测中密钥管理功能的检测要求和检测方法（见6.3.3，2016年版的6.3.3）；

e) 更改了随机数检测中随机数检测的依据标准以及所采用随机数发生器的检测要求和检测方法（见6.3.4，2016年版的6.3.4）；

f) 更改了访问控制检测中访问控制机制的检测要求和检测方法（见6.3.5，2016年版的6.3.5）；

g) 更改了设备远程管理检测的检测要求和检测方法，增加了设备远程管理的条件（见6.3.6，2016年版的6.3.6）；

h) 更改了日志审计检测的检测要求，增加了日志审计检测的日志类型和日志内容（见6.3.7，2016年版的6.3.7）；

i) 更改了业务功能检测的章节名称和业务功能的检测方法（见6.3.9，2016年版的6.3.9）；

j) 更改了性能检测中性能指标的计算方法以及性能单位（见6.4，2016年版的6.4）；

k) 更改了送检技术文档要求，删除了文档资料应包含的内容（见第7章，2016年版的第7章）；

l) 更改了判定规则的章节名称和要求（见第8章，2016年版的第8章）；

m) 更改了检测项目列表的格式和检测内容（见附录A，2016年版的附录A）。

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专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：商用密码检测认证中心、中电科网络安全科技股份有限公司、兴唐通信科技股份有限公司、山东得安信息技术有限公司、无锡江南信息安全工程技术中心。

本文件主要起草人：李红芳、邓开勇、罗鹏、崔永娜、谢亚丽、李国友、肖秋林、赵银春、安学刚、马洪富、张所成、齐传兵、刘常、丁余泉、刘先详、李元正、王妮娜、孔凡玉、李大为。

本文件及其所代替文件的历次版本发布情况为：

——2016年首次发布为GM/T 0046—2016；

——本次为第一次修订。

金融数据密码机检测规范

1 范围

本文件规定了金融数据密码机的检测环境、检测内容及检测方法、送检技术文档要求和判定规则。

本文件适用于金融数据密码机的检测，也可用于指导金融数据密码机的研制、生产和测试。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 32915 信息安全技术 二元序列随机性检测方法

GB/T 38625—2020 信息安全技术 密码模块安全检测要求

GM/T 0045—2016 金融数据密码机技术规范

GM/T 0050 密码设备管理 设备管理技术规范

GM/T 0062—2018 密码产品随机数检测要求

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

金融数据密码机 financial cryptographic device

用于金融领域，保护金融数据安全，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

物理防护 physical protection

用物理手段保护硬件密码设备及其密钥或敏感信息。

注：采用防撬手段防止密码机被非法开箱。

3.3

主密钥 master key

处于对称密码系统层次化密钥结构中的顶层，用于下层密钥的产生或保护。

3.4

校验值 check value

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。

注：在未知密钥的情况下，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。

3.5

个人识别码 personal identification number

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。

注：PIN 只包含十进制数字。

4 缩略语

下列缩略语适用于本文件：

API：应用程序接口(Application Program Interface)

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)

ECB：(分组密码的)电子密本(工作方式)(Electronic Codebook)

LMK：本地主密钥(Local Master Key)

MAC：消息鉴别码(Message Authentication Code)

PIN：个人识别码(Personal Identification Number)

RSA：非对称密码算法(Rivest-Shamir-Adleman Algorithm)

TAK：终端 MAC 计算密钥(Terminal MAC Key)

TMK：终端主密钥(Terminal Master Key)

TPK：终端 PIN 加密密钥(Terminal PIN Key)

ZMK：区域主密钥(Zone Master Key)

ZPK：区域 PIN 加密密钥(Zone PIN Key)

5 检测环境

金融数据密码机检测环境用于测试金融数据密码机的功能、性能。检测环境拓扑见图 1。

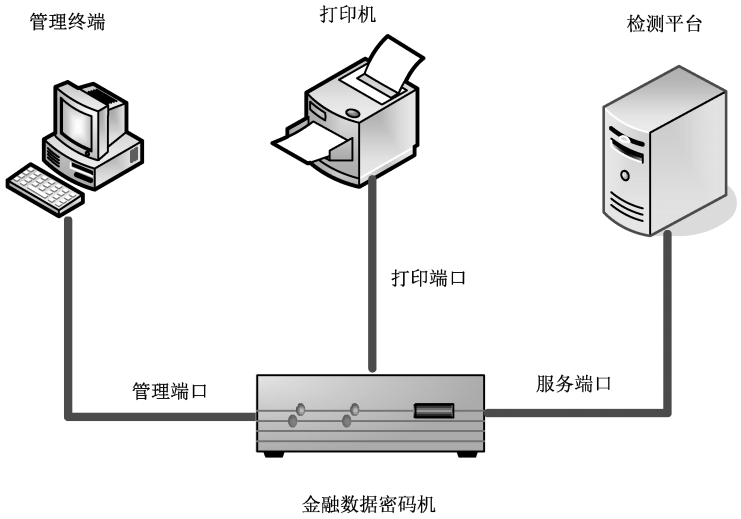

图 1 金融数据密码机检测环境拓扑图

检测环境主要由金融数据密码机、管理终端、打印机、检测平台以及相关通信链路组成。管理终端用于对金融数据密码机进行初始化检测、密钥管理检测、访问控制检测、日志审计检测、设备自检检测；检测平台用于密码算法检测、业务功能检测、随机数检测、设备远程管理检测以及性能检测；打印机用于应用编程接口检测时打印密码信封的功能检测。

6 检测内容及检测方法

6.1 检测项目

检测内容包括外观和结构检查、功能检测、性能检测和其他检测等，应符合附录 A 规定的检测项目。

6.2 外观和结构检查

检测要求：

金融数据密码机应具备以下部件或端口：

a) 上电、工作故障状态的视觉和声音提示；

b) 至少 1 个服务端口；

c) 至少 1 个管理端口；

d) 如果密钥存储采用微电保护存储方式，应具备密钥自毁装置。

金融数据密码机宜具备以下部件或端口：

a) 1 个打印端口；

b) 冗余电源；

c) IC 卡插座；

d) USB 端口；

e) 人机交互部件，如显示屏、按键等。

检测方法：

检测人员根据产品的物理参数，通过观察外观、内部部件及附件，核查金融数据密码机具备上述部件或端口。

6.3 功能检测

6.3.1 初始化检测

检测要求：

金融数据密码机应具备初始化功能，实现设备的初始状态到工作状态的转换。金融数据密码机的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。金融数据密码机只有在初始化操作完成之后才能提供密码服务。初始化检测应符合 GM/T 0045—2016 中 5.6 的要求。

检测方法：

a) 检测人员对金融数据密码机初次上电，核查金融数据密码机应能通过状态指示和声音进行报警，提示用户进行初始化；

b) 检测人员通过对未初始化的金融数据密码机执行密码服务，操作应失败；

c) 检测人员通过金融数据密码机管理工具进行初始化操作，初始化内容应至少包括系统初始配置(如：服务端口配置、管理端口配置)、添加管理员或操作员、生成(或恢复)初始密钥并安装；

d) 检测人员通过对已初始化的金融数据密码机执行密码服务，操作应成功。

6.3.2 密码算法检测

检测要求：

金融数据密码机应使用符合国家密码管理要求的密码算法，至少应支持 SM4 对称密码算法、SM2

非对称密码算法、SM3 杂凑算法。对称密码算法至少应包括 ECB 和 CBC 两种模式。密码算法检测应符合 GM/T 0045—2016 中 5.1 的要求。

检测方法：

a） 对称密码算法：

1） 加密：调用金融数据密码机加密功能对给定的密钥和明文经指定的算法和工作模式加密，结果和给定密文一致，则加密正确；

2） 解密：调用金融数据密码机解密功能对给定的密钥和密文经指定的算法和工作模式解密，结果和给定明文一致，则解密正确。

b） 非对称密码算法：

1） 密钥生成：调用金融数据密码机生成一对密钥，使用私钥对给定的数据签名，其结果由对应公钥验证通过，则密钥生成正确；

2） 签名：调用金融数据密码机签名功能，使用内部私钥对给定的数据签名，其结果由对应公钥验证通过，则签名正确；

3） 验签：调用金融数据密码机验签功能，使用给定的公钥对给定的签名值验签，验证通过，则验签正确；

4） 加密：调用金融数据密码机加密功能，使用给定的公钥对给定的明文加密，其结果由对应私钥解密成功，则加密正确；

5） 解密：调用金融数据密码机解密功能，使用内部私钥对给定的密文解密，其结果与对应明文一致，则解密正确。

c） 杂凑算法：

调用金融数据密码机杂凑运算功能，对给定的消息计算杂凑值，结果和给定杂凑值一致，则杂凑运算正确。

6.3.3 密钥管理检测

检测要求：

金融数据密码机应具备完善的密钥管理功能，密钥管理包括密钥的生成、注入、导入/导出、备份/恢复、查询和销毁，金融数据密码机必须保证密钥在生存周期各个环节的安全性。密钥管理检测应符合 GM/T 0045—2016 中 5.2 的要求。

检测方法：

金融数据密码机密钥管理功能的检测由金融数据密码机自身的密钥管理工具实现，应进行以下检测：

a） 产生主密钥：检测人员通过密钥管理工具使用指定的参数生成主密钥，应成功产生并显示主密钥校验值；

b） 导出主密钥：检测人员通过密钥管理工具的备份功能导出主密钥，核查主密钥安全存储到安全介质中；

c） 导入主密钥：检测人员通过密钥管理工具从外部安全介质导入主密钥，应成功导入并显示主密钥校验值；

d） 查询主密钥：检测人员通过密钥管理工具按照指定的查询参数查询主密钥，应成功显示主密钥校验值；

e） 备份密钥：检测人员通过密钥管理工具备份内部存储密钥，核查密钥以安全的方式备份到安全介质中；

f） 恢复密钥：检测人员通过密钥管理工具将备份的密钥恢复到金融数据密码机中，应正确显示密钥状态；

g) 销毁密钥：检测人员通过密钥管理工具使用指定的密钥销毁方式销毁密钥，如金融数据密码机提供硬件销毁方式，则通过销毁开关销毁密钥，密钥销毁后通过密钥管理工具查询，应显示密钥不存在；

h) 密钥自毁机制：如果密钥存储采用微电保护存储方式，检测人员应核查金融数据密码机密钥自毁装置，在加电与不加电两种情况下打开机箱，密钥都应被自动销毁，密钥销毁后通过密钥管理工具查询，应显示密钥不存在。

6.3.4 随机数检测

检测要求：

金融数据密码机应具备随机数生成功能，随机数应至少采用经密码检测认证的两个独立的基于物理熵源的随机数发生器产生的随机数异或生成。随机数质量应按照 GB/T 32915 的要求进行检测。随机数检测应符合 GM/T 0045—2016 中 5.3 的要求。

检测方法：

检测人员核查金融数据密码机随机数生成原理合理有效，通过调用随机数生成接口生成随机数，随机数质量检测结果应符合 GB/T 32915 的要求。

6.3.5 访问控制检测

检测要求：

金融数据密码机应提供措施防止非授权打开设备，打开金融数据密码机应有物理上的访问控制措施限制。金融数据密码机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身份认证机制，应拒绝任何非授权的访问或操作。访问控制检测应符合 GM/T 0045—2016 中 5.4 的要求。

检测方法：

a) 检测人员通过物理方式访问金融数据密码机，核查其具备防止非授权打开设备的物理防护措施；

b) 检测人员通过金融数据密码机自身的管理工具进行访问控制检测：

   1) 登录不同管理角色，核查金融数据密码机应采用多因素登录方式；

   2) 通过配置金融数据密码机管理角色及权限，核查至少具备管理员、审计员、操作员角色及权限的划分；

   3) 经管理员授权后执行金融数据密码机关键安全操作（如密钥注入、密钥备份/恢复等密钥管理功能）应成功；

   4) 设置金融数据密码机服务端口授权访问机制，核查至少具备验证合法主机 IP 地址的功能。

6.3.6 设备远程管理检测

检测要求：

在有远程集中管理需求时，金融数据密码机宜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 0050 的要求。设备远程管理检测应符合 GM/T 0045—2016 中 5.5.2 的要求。

检测方法：

检测人员通过密码设备管理中心，按照 GM/T 0050 中管理指令要求向金融数据密码机下发指令，金融数据密码机应能正确响应。

6.3.7 日志审计检测

检测要求：

金融数据密码机应提供日志记录、查看和导出功能。每条日志内容应包括日志的主体和日志产生时间等元素。金融数据密码机日志类型应包括操作日志、管理日志和运行日志。日志审计检测应符合GM/T 0045—2016 中 5.5.1 的要求。

检测方法：

检测人员采用金融数据密码机自身的日志管理工具进行日志审计检测。

a) 核查金融数据密码机日志类型，应至少包括操作日志、管理日志和运行日志。

b) 核查金融数据密码机的日志内容，应至少包括：

   1) 操作日志：记录管理员的操作行为，包括登录认证、系统配置、密钥管理等，如果与设备管理中心连接，则应对相应操作进行记录；

   2) 管理日志：记录需审计的安全事件，包括自检失败、认证失败、非法访问等；

   3) 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。

c) 对金融数据密码机日志内容进行查看并执行日志导出功能，应成功导出。

6.3.8 设备自检检测

检测要求：

金融数据密码机应支持上电/复位自检、手动自检和周期性自检功能，自检项主要包括密码算法正确性检测、存储的密钥等敏感信息的完整性检测，以及密码运算部件等关键部件的正确性检测等。随机数检测应按照 GM/T 0062—2018 中 E 类产品的要求进行检测。任一自检项不通过时应报警并停止对外提供密码功能。设备自检检测应符合 GM/T 0045—2016 中 5.7 的要求。

检测方法：

a) 检测人员对金融数据密码机执行上电/复位，上电/复位自检应在每次加电/复位启动后自动执行。根据上电/复位自检结果核查自检项的完整性和自检机制的有效性，自检成功，金融数据密码机自动进入管理状态或工作状态。自检失败，金融数据密码机应报告结果并且停止对外提供密码服务。

b) 检测人员通过管理界面执行手动自检，自检结束后应报告检测结果，根据检测结果核查自检项的完整性和自检机制的有效性。

c) 检测人员通过管理工具配置自检周期，金融数据密码机按设定的周期自动执行，根据执行结果核查自检项的完整性和自检机制的有效性。自检失败，金融数据密码机应报告结果并且停止对外提供密码服务。

d) 检测人员对金融数据密码机设定自检异常情况，金融数据密码机应报告异常结果，进一步调用密码功能，操作应失败。

6.3.9 业务功能检测

检测要求：

金融数据密码机业务功能应符合 GM/T 0045—2016 中第 7 章的要求。

检测方法：

按照 GM/T 0045—2016 规定的业务功能应用编程接口逐条进行测试，所有接口测试正确，检测通过。

a) 向金融数据密码机发送正确的数据报文并解析响应报文，应返回正确结果并完成相应功能。

b) 向金融数据密码机发送涵盖 GM/T 0045—2016 表 3 中通用错误码类型的数据报文并解析响应报文，应返回相应的错误码，厂商自定义错误码不应与通用错误码冲突。

6.4 性能检测

检测要求：

金融数据密码机的性能检测包括：对称密码算法性能、非对称密码算法性能、杂凑算法性能、常用计算方法性能(PIN、MAC、ARQC)、随机数发生器性能。

检测方法：

a) 对称密码算法的加/解密性能检测：

将一个长度为 L 字节的数据，发送给金融数据密码机进行加/解密操作，X 个线程并行，重复操作 N 次，测量其完成时间 T s。按照公式(1)计算。

$$S = 8 * L * N * X / (1\,024 * 1\,024 * T) \quad \cdots\cdots (1)$$

式中：

S ——速度，单位为兆比特每秒(Mbit/s)；

L ——数据报文的长度，单位为字节；

X ——线程数，单位为个；

N ——测试次数，单位为次；

T ——测试所耗费的时间，单位为秒(s)。

b) 非对称密钥生成性能检测：

金融数据密码机生成并输出密钥对，X 个线程并行，重复操作 N 次，测量其完成时间 T s。按照公式(2)计算。

$$S = X * N / T \quad \cdots\cdots (2)$$

式中：

S ——速度，单位为对每秒(对/s)；

X ——线程数，单位为个；

N ——测试次数，单位为次；

T ——测试所耗费的时间，单位为秒(s)。

c) 非对称密码算法加/解密性能检测：

将一个长度为 L 字节的数据，发送给金融数据密码机进行加/解密操作，X 个线程并行，重复操作 N 次，测量其完成时间 T s。按照公式(1)计算。

d) 非对称密码算法签名/验签性能检测：

将一个定长的数据，发送给金融数据密码机进行签名/验签操作，X 个线程并行，重复操作 N 次，测量其完成时间 T s。按照公式(3)计算：

$$S = X * N / T \quad \cdots\cdots (3)$$

式中：

S ——速度，单位为次每秒(次/s)；

X ——线程数，单位为个；

N ——测试次数，单位为次；

T ——测试所耗费的时间，单位为秒(s)。

e) 杂凑算法性能检测：

将一个长度为 L 字节的数据，发送给金融数据密码机进行杂凑运算，X 个线程并行，重复操作 N 次，测量其完成时间 T s。按照公式(1)计算。

f) PIN 加密性能检测：

将一个 PIN 发送给金融数据密码机进行加密操作，X 个线程并行，重复操作 N 次，测量其完成时间 T s。按照公式(3)计算。

g) PIN 转加密性能检测：
将一个由 LMK 保护的 PIN 块发送给金融数据密码机，转加密为 ZPK 保护的 PIN 块，X 个线程并行，重复操作 N 次，测量其完成时间 T s。按照公式(3)计算。

h) MAC 计算性能检测：
调用金融数据密码机，计算一个定长的 MAC 值，X 个线程并行，重复操作 N 次，测量其完成时间 T s。按照公式(3)计算。

i) ARQC 验证性能检测：
调用金融数据密码机，验证一个 ARQC 值，X 个线程并行，重复操作 N 次，测量其完成时间 T s。按照公式(3)计算。

j) 随机数发生器性能检测：
调用金融数据密码机生成并输出长度为 L 字节的符合随机特性的随机序列，X 个线程并行，连续执行 N 次，测量其完成时间 T s。按照公式(1)计算。

6.5 其他检测

6.5.1 安全性检测

金融数据密码机安全性检测应符合 GB/T 38625—2020 的要求。

6.5.2 环境适应性检测

金融数据密码机环境适应性检测应符合 GM/T 0045—2016 中 6.4 的要求。

6.5.3 可靠性检测

金融数据密码机可靠性检测应符合 GM/T 0045—2016 中 6.5 的要求。

7 送检技术文档要求

送检单位应按照商用密码检测认证机构的要求提交相关文档资料。

8 判定规则

本文件中，除 6.4、6.5.2 和 6.5.3 以外的各检测项目，其任意一项检测结果不通过，判定为产品检测不通过。

附 录 A
（规范性）
检测项目列表

检测项目列表见表 A.1。

表 A.1 检测项目表

测试项目	测试内容
外观和结构检查	金融数据密码机应具备以下主要部件或端口： a） 具备上电、工作故障状态的视觉和声音提示； b） 具备至少 1 个服务端口； c） 具备至少 1 个管理端口； d） 如果密钥存储采用微电保护存储方式，应具备密钥自毁机制
	金融数据密码机宜具备以下部件或端口： a） 宜具备 1 个打印端口； b） 宜具备冗余电源； c） 宜具备 IC 卡插座； d） 宜具备 USB 端口； e） 宜具备人机交互部件，如显示屏、按键等
初始化检测	如果没有初始化，是否提示报警
	执行初始化后，是否能进入工作状态
	管理员生成
	服务端口配置
	管理端口配置
密码算法检测	SM4 ECB 加密
	SM4 ECB 解密
	SM4 CBC 加密
	SM4 CBC 解密
	SM3 杂凑
	SM2 密钥生成
	SM2 签名
	SM2 验签
	SM2 加密
	SM2 解密
密钥管理检测	产生主密钥
	导出主密钥
	导入主密钥
	查询主密钥

表 A.1　检测项目表（续）

测试项目	测试内容	
密钥管理检测	备份密钥	
	恢复密钥	
	销毁密钥	
	密钥自毁机制	
随机数检测	随机数生成机制	
	随机数质量检测	
	产品随机数检测： a）　出厂检测； b）　上电检测； c）　周期检测； d）　单次检测	
访问控制检测	物理访问控制	
	管理权限角色划分	
	授权身份认证机制	
	关键安全操作必须由管理员授权	
	服务端口授权访问机制	
设备远程管理检测	按照 GM/T 0050 的要求进行检测	
日志审计检测	日志类型和内容： a）　操作日志； b）　管理日志； c）　运行日志	
	日志导出	
设备自检检测	上电/复位自检	
	手工自检	
	周期性自检	
业务功能检测	X0	产生密钥
	A6	导入密钥
	A8	导出密钥
	GG	合成 ZMK
	X2	LMK 加密密钥
	AG	TAK 从 LMK 到 TMK
	MG	TAK 从 LMK 到 ZMK
	MI	TAK 从 ZMK 到 LMK
	KA	生成密钥校验值

表 A.1　检测项目表（续）

测试项目	测试内容	
业务功能检测	BA	加密 PIN
	NG	解密 PIN
	BE	PIN 验证
	JE	PIN 块从 ZPK 到 LMK
	JC	PIN 块从 TPK 到 LMK
	JG	PIN 块从 LMK 到 ZPK
	MS	产生终端 MAC
	MC	验证终端 MAC
	ME	验证并转换终端 MAC
	CW	产生 CVV
	CY	验证卡校验码 CVV
	PE	打印密码信封
	V2	分散密钥加密
	El	产生 RSA 密钥对
	UA	分解 RSA 私钥分量
	UK	公钥运算
	VA	外部私钥运算
	GM	产生消息摘要
	EW	RSA 签名
	VC	安全报文计算
	EY	RSA 验签
	VM	ARQC/ARPC 产生或验证
	VI	脚本加解密
	VK	计算脚本 MAC
	VS	IC 卡发行数据转加密保护
	CC	PIN 转加密
	UO	产生 SM2 密钥对
	UQ	SM2 签名
	US	SM2 验签
	UU	SM2 公钥加密
	UW	SM2 私钥解密
	UY	转加密 SM2 私钥
	5E	数据加解密

表 A.1　检测项目表（续）

测试项目	测试内容
性能测试	PIN 加密
	PIN 转加密
	MAC 计算
	ARQC 验证
	SM4 ECB 加密
	SM4 ECB 解密
	SM4 CBC 加密
	SM4 CBC 解密
	SM2 加密
	SM2 解密
	SM3 杂凑
	随机数产生性能
	SM2 密钥生成
	SM2 签名
	SM2 验签
安全性检测	设备安全性检测应遵照 GB/T 38625—2020
环境适应性	金融数据密码机环境适应性检测应达到 GM/T 0045—2016 中 6.4 的要求
可靠性检测	金融数据密码机可靠性检测应达到 GM/T 0045—2016 中 6.5 的要求

中华人民共和国密码
行业标准
金融数据密码机检测规范
GM/T 0046—2024
*
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)
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 1.25　字数 27 千字
2025年6月第1版　2025年6月第1次印刷
*
书号:155066·2-39098　定价 38.00 元

GM/T 0046-2024