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。