ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0039—2024
代替 GM/T 0039—2015

密码模块安全检测要求

Security test requirements for cryptographic modules

2024-12-27 发布　　2025-07-01 实施

国家密码管理局　　发布

目　　次

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 0039—2015《密码模块安全检测要求》，与GM/T 0039—2015相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了测评单元[02.05]软件密码模块非入侵式安全要求和物理安全要求（见6.2.2.3，2015年版的6.2.2）；
b) 更改了验证证书、数据和向量初始化、分片密钥信息、密钥核算信息、手动状态输出、产品级质量的IC芯片的表述（见6.2.4.1.2、6.3.3.2、6.3.3.3、6.3.3.8、6.7.2.8，2015年版的6.2.4.1、6.3.3、6.7.2）；
c) 增加了“降级工作”的要求（见6.2.4.3）；
d) 更改了测评单元[03.04]密码模块接口定义的安全要求，增加了密码模块接口定义的送检材料要求和检测程序要求（见6.3.3.1，2015年版的6.3.3）；
e) 更改了测评单元[03.06]密码模块数据输出接口关于输出内容的要求（见6.3.3.3，2015年版的6.3.3）；
f) 更改了测评单元[03.07]密码模块数据输出接口禁止通过数据输出接口输出数据的条件（见6.3.3.4，2015年版的6.3.3）；
g) 增加了测评单元[04.16]密码模块安全功能的检测程序要求（见6.4.3.1.9，2015年版的6.4.3.1）；
h) 增加了测评单元[04.17]密码模块参数置零服务的检测程序要求（见6.4.3.1.10，2015年版的6.4.3.1）；
i) 更改了测评单元[04.25]和测评单元[04.26]自启动密码服务能力的送检材料要求和检测程序要求（见6.4.3.3.2、6.4.3.3.3，2015年版的6.4.3.3）；
j) 增加了测评单元[05.09]密码模块执行完整性技术的硬件密码模块接口类型（见6.5.9，2015年版的6.5）；
k) 更改了测评单元[05.16]和测评单元[05.19]软固件完整性验证的要求（见6.5.16、6.5.19，2015年版的6.5）；
l) 增加了测评单元[06.10]密码模块进程的要求（见6.6.3.6）；
m) 更改了测评单元[07.41]密码模块涂层抗移除的检测程序要求（见6.7.3.1.8，2015年版的6.7.3）；
n) 更改了测评单元[09.08]密码模块随机比特生成器最小熵值的要求（见6.9.2.3，2015年版的6.9.2）；
o) 增加了测评单元[09.30]密码模块敏感安全参数存储的要求（见6.9.6.4）；
p) 更改了测评单元[10.14]密码模块运行前自测试的检测程序要求（见6.10.2.1.1，2015年版的6.10.2.1）；
q) 更改了测评单元[12.02]密码模块对其他攻击缓解机制验证的检测程序要求（见6.12.2，2015年版的6.12）；
r) 更改了密码模块非入侵式攻击及缓解方法检测指标（见6.18，2015年版的6.18）。

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、北京握奇智能科技有限公司、飞天诚信科技股份有限公

司、北京华大智宝电子系统有限公司、北京海泰方圆科技有限公司、中国科学院数据与通信保护研究教育中心、北京创原天地科技有限公司、格尔软件股份有限公司、中国科学院信息工程研究所。

本文件主要起草人：汪雪林、崔永娜、张渊、邓开勇、李红芳、牛路宏、谢亚丽、李勃、李大为、雷银花、陈国、陈保儒、张一飞、胡伯良、朱鹏飞、罗鹏、张众、莫凡、林春、蒋红宇、谭武征、张万涛、高能、郑强、屠晨阳。

本文件及其所代替文件的历次版本发布情况为：

——2015 年首次发布为 GM/T 0039—2015；

——本次为第一次修订。

密码模块安全检测要求

1 范围

本文件规定了密码模块的安全检测要求以及对应的送检材料要求。

本文件适用于检测机构对送检密码模块的检测，也可用于指导密码模块研制厂商的研制、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 25069 信息安全技术 术语

GM/T 0028—2024 密码模块安全技术要求

3 术语和定义

GB/T 25069 和 GM/T 0028—2024 界定的术语和定义适用于本文件。

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）

CBC：密码分组链接（Cipher Block Chaining）

ECB：电码本（Electronic Codebook）

EDC：错误检测码（Error Detection Code）

EFP：环境失效保护（Environmental Failure Protection）

EFT：环境失效测试（Environmental Failure Testing）

FSM：有限状态模型（Finite State Model）

HDL：硬件描述语言（Hardware Description Language）

IC：集成电路（Integrated Circuit）

PIN：个人身份识别码（Personal Identification Number）

VHDL：超高速集成电路硬件描述语言（Very High Speed Integrated Circuit Hardware Description Language）

5 概述

本文件详细说明了对送检厂商提供给检测机构材料的要求、检测机构检测所使用的程序要求以及附录 A 中每个测评单元对应的密码模块安全等级要求。