ICS 35.040
L 80
备案号：49738—2015

GM

中华人民共和国密码行业标准

GM/T 0039—2015

密码模块安全检测要求

Security test requirements for cryptographic modules

2015-04-01 发布　　2015-04-01 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。

本标准使用重新起草法参考 ISO/IEC 24759:2014《信息技术　安全技术　密码模块检测要求》编制,与 ISO/IEC 24759:2014 的一致性程度为非等效。

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。

本标准的主要起草单位: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、国家密码管理局商用密码检测中心、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、上海格尔软件股份有限公司。

本标准的主要起草人:汪雪林、李大为、邓开勇、陈国、陈保儒、张一飞、胡伯良、朱鹏飞、罗鹏、张众、雷银花、莫凡、林春、蒋红宇、谭武征、张万涛、高能。

密码模块安全检测要求

1 范围

本标准依据 GM/T 0028—2014 的要求，规定了密码模块的一系列检测规程、检测方法和对应的送检文档要求。

本标准适用于密码模块的检测。

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。

GM/T 0028—2014 密码模块安全技术要求

GM/Z 4001 密码术语

3 术语和定义

GM/T 0028—2014 和 GM/Z 4001 所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)

CSP 关键安全参数(Critical Security Parameter)

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)

PROM 可编程只读存储器(Programmable Read-Only Memory)

PSP 公开安全参数(Public Security Parameter)

RAM 随机存取存储器(Random Access Memory)

RBG 随机比特生成器(Random Bit Generator)

ROM 只读存储器(Read-Only Memory)

SSP 敏感安全参数(Sensitive Security Parameter)