ICS 35.040
L 80

中华人民共和国国家标准

GB/T 38625—2020

信息安全技术
密码模块安全检测要求

Information security technology—
Security test requirements for cryptographic modules

(ISO/IEC 24759:2017,Information technology—Security techniques—
Test requirements for cryptographic modules,NEQ)

2020-04-28 发布　　2020-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　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 …… 1
5　概述 …… 1
6　安全检测要求 …… 2
6.1　通用要求 …… 2
6.2　密码模块规格 …… 3
6.3　密码模块接口 …… 13
6.4　角色、服务和鉴别 …… 24
6.5　软件/固件安全 …… 41
6.6　运行环境 …… 46
6.7　物理安全 …… 57
6.8　非入侵式安全 …… 81
6.9　敏感安全参数管理 …… 83
6.10　自测试 …… 95
6.11　生命周期保障 …… 114
6.12　对其他攻击的缓解 …… 127
6.13　文档要求 …… 128
6.14　密码模块安全策略 …… 128
6.15　核准的安全功能 …… 129
6.16　核准的敏感安全参数生成和建立方法 …… 129
6.17　核准的鉴别机制 …… 129
6.18　非入侵式攻击及常用的缓解方法 …… 129
附录A（规范性附录）　安全等级对应表 …… 130

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 24759:2017《信息技术　安全技术　密码模块检测要求》编制，与 ISO/IEC 24759:2017 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。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：北京握奇智能科技有限公司、国家密码管理局商用密码检测中心、飞天诚信科技股份有限公司、苏州中科全象智能科技有限公司、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。

本标准主要起草人：汪雪林、陈国、罗鹏、于华章、朱鹏飞、邓开勇、吕春梅、陈保儒、李静进、胡伯良、蒋红宇、田敏求、张众、雷银花、高能、肖青海、郑强。

信息安全技术
密码模块安全检测要求

1 范围

本标准依据 GB/T 37092—2018,规定了密码模块的检测要求和对应的送检材料要求。

本标准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自行测试。

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。

GB/T 25069—2010 信息安全技术 术语

GB/T 37092—2018 信息安全技术 密码模块安全要求

3 术语和定义

GB/T 37092—2018 和 GB/T 25069—2010 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:电子译码本(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)

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

RAM:随机存取存储器(Random Access Memory)

ROM:只读存储器(Read-Only Memory)

5 概述

第 6 章详细说明了对送检厂商提供给检测机构材料的要求以及检测机构检测所使用的程序要求。第 6 章共 18 条,包括 6.1 通用要求以及对应于 GB/T 37092—2018 中的 11 个安全域和附录 A～