



# 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