ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0134—2024

密码模块安全设计指南

Security design guidance 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 …… Ⅴ
引言 …… Ⅵ
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　设计原则 …… 1
5.1　符合性 …… 1
5.2　系统性 …… 2
6　密码模块安全设计过程 …… 2
6.1　密码模块设计技术框架 …… 2
6.2　密码模块需求分析 …… 3
6.3　安全域选取 …… 3
6.4　密码模块设计详细技术 …… 4
7　密码模块规格 …… 6
7.1　用作接口的部件与密码边界的关系 …… 6
7.2　密码模块的密码边界 …… 7
7.3　密码模块名称和版本标识 …… 8
7.4　“核准的过程”的确定和梳理 …… 8
7.5　工作模式 …… 9
7.6　密码模块状态指示方式的建议 …… 9
7.7　混合密码模块的密码边界和物理边线 …… 9
7.8　混合密码模块内部部件之间的通信 …… 10
8　密码模块接口 …… 10
8.1　可信信道 …… 10
8.2　常用的物理端口与逻辑接口的关系 …… 11
8.3　逻辑接口相互隔离的建议 …… 11
8.4　输入设备作为物理端口时的接口描述方式 …… 11
8.5　软件密码模块的物理端口 …… 12
9　角色、服务和鉴别 …… 12
9.1　对新角色的验证 …… 12
9.2　无默认鉴别数据时的第一次访问鉴别 …… 13
9.3　鉴别数据的隐藏方法 …… 13

9.4 无需担任授权角色的情况 …… 13
9.5 多重操作者鉴别 …… 14
9.6 旁路能力 …… 14
9.7 激活旁路能力 …… 15
9.8 鉴别机制的强度 …… 15
9.9 密码主管角色确定 …… 15
9.10 软件密码模块的鉴别机制 …… 16
10 软件/固件安全 …… 16
10.1 确保软件/固件在安装前未被修改 …… 16
10.2 软件密码模块的完整性校验 …… 16
11 运行环境 …… 17
11.1 对运行环境配置的规定 …… 17
11.2 硬件密码模块的运行环境 …… 18
12 物理安全 …… 18
12.1 密码模块物理实体的分类 …… 18
12.2 物理安全置零时间 …… 18
12.3 对维护访问接口的安全要求 …… 19
13 非入侵式安全 …… 20
13.1 非入侵式攻击的主要类型以及缓解技术 …… 20
13.2 证明缓解技术有效性的方法和测试方法 …… 20
14 敏感安全参数管理 …… 21
14.1 敏感安全参数置零的例外 …… 21
14.2 置零的安全要求 …… 21
14.3 关于梳理敏感安全参数的建议 …… 21
14.4 随机数生成器状态信息 …… 22
14.5 置零的状态输出问题 …… 22
14.6 关于公开安全参数保护措施的建议 …… 23
14.7 关于评估敏感安全参数生成方法安全性的建议 …… 23
15 自测试 …… 24
15.1 周期自测试的需求和内容 …… 24
15.2 运行前自测试 …… 24
15.3 运行前软件/固件完整性测试 …… 25
15.4 运行前旁路以及旁路测试 …… 25
15.5 运行前关键功能测试 …… 25
15.6 密码算法条件测试 …… 26
15.7 手动输入条件自测试 …… 26
15.8 密码算法已知答案自测试 …… 26

15.9 密码算法自测试的方法 …… 27
15.10 运行前模块初始化过程 …… 27
15.11 软件/固件加载测试 …… 28
附录 A（资料性） 密码模块边界信息梳理 …… 29

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。

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：北京握奇智能科技有限公司、中国科学院大学、商用密码检测认证中心、飞天诚信科技股份有限公司、深圳市文鼎创数据科技有限公司、山东大学、北京海泰方圆科技股份有限公司、工业信息安全（四川）创新中心有限公司、北京江南天安科技有限公司、北京天威诚信电子商务服务有限公司、西安得安信息技术有限公司、智巡密码（上海）检测技术有限公司、鼎铉商用密码测评技术（深圳）有限公司、豪符密码检测技术（成都）有限责任公司、长春吉大正元信息技术股份有限公司、浙江蚂蚁密算科技有限公司。

本文件主要起草人：张渊、郑昉昱、李国友、李勃、王慧、李小雨、朱鹏飞、崔永娜、刘伟丰、陈妍、孔凡玉、罗影、胡伯良、马晓艳、王超、马洪富、韩玮、胡之斐、饶金涛、孙浩、张宇韬、李超。

引　言

GM/T 0028—2024《密码模块安全技术要求》针对密码模块的11个安全域分别规定了四个安全等级的对应要求，本文件从密码模块安全设计的角度阐述了落实这些要求的通用设计方法和建议，旨在为GM/T 0028—2024中的安全要求条款提供解释和指导，以促进对GM/T 0028—2024理解的一致性和应用标准的符合性。

密码模块安全设计指南

1 范围

本文件提供了密码模块安全设计过程的指导和建议，给出了针对 GM/T 0028—2024 对应的安全要求章节中，有代表性安全要求条款疑问的具体解读、解释和设计指导。

本文件适用于密码模块的设计、开发和检测。本文件不适用于密码安全芯片设计的指导。

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

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 32918（所有部分） 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GM/T 0005 随机性检测规范

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0028—2024 密码模块安全技术要求

GM/T 0083 密码模块非入侵式攻击缓解技术指南

GM/T 0084 密码模块物理攻击缓解技术指南

GM/T 0103 随机数发生器总体框架

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。

CA：认证中心（Certificate Authority）

DEP：默认入口点（Default Entry Point）

EEPROM：带电可擦可编程只读存储器（Electrically Erasable Programmable Read Only Memory）

5 设计原则

5.1 符合性

GM/T 0028—2024 规定了密码模块的四个安全等级及对应的安全要求，这对密码模块的安全设计