ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0028—2024
代替 GM/T 0028—2014

密码模块安全要求

Security 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》给出的规定起草。

本文件替代GM/T 0028—2014《密码模块安全技术要求》，与GM/T 0028—2014相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 更改了本文件规范性引用的相关标准，用GB/T 32907、GB/T 33133、GB/T 32918、GB/T 35276、GB/T 35275、GB/T 32905分别代替了GM/T 0002、GM/T 0001、GM/T 0003、GM/T 0009、GM/T 0010、GM/T 0004（见C.2，2014年版的C.2）；

b) 删除了规范性引用的GM/T 0015（见2014年版的C.2.3）；

c) 增加了相关标准的规范性引用，新增了GB/T 36624（见C.2.1）、GB/T 38635（见C.2.3）、GB/T 41389（见C.2.3）、GM/T 0081（见C.2.3）、GB/T 15852.1（见C.2.4）、GB/T 15852.2（见C.2.4）、GM/T 0057（见C.2.6）、GM/T 0062（见C.2.8）、GM/T 0044.3（见D.2.2）、GB/T 25069（见第3章）、GM/T 0083（见F.3）；

d) 更改了术语证书、关键安全参数、密码边界、密码模块、错误注入、多因素鉴别、非入侵式攻击、运行环境、公开安全参数、安全功能、拆分知识及其定义（见3.1、3.3～3.5、3.9～3.12、3.14、3.16、3.18）；

e) 删除了术语访问控制列表、管理员指南、核准机构、核准的数据鉴别技术、核准的完整性技术、核准的工作模式、核准的安全功能、非对称密码技术、旁路能力、破坏、配置管理系统、控制信息、密码主管、数据路、电磁辐、电子密钥输入、经过加密的密、实体、熵、环境失效保护、环境失效测、错误检测码、可执行形式、有限状态模型、固件、固件模块、功能规格、功能测试、硬、硬件模块、硬件模块接口、混合模块、混合固件模块接、混合软件模块接口、输入数据、接口、密钥加载器、受限制的运行环、底层测试、维护员角色、微码、最小熵、可修改的运行环境、多芯片嵌入式密码模块、多芯片独立式密码模块、非管理员指南、不可修改的运行环境、非安全相关、正常工作、不透光、运行状态、操作员、输出数据、钝化、口令、个人身份识别码、物理保护、明文密钥、端口、产品级、公钥证书、封盖、角色、基于角色的访问控制、种子密钥、自测试、敏感数据、服务、服务输入、服务输出、简单能量分析、单芯片密码模块、软件、软件模块、软件/固件加载测试、软件/固件模块接口、状态信息、拆卸检测、拆卸证据、拆卸响应、信任锚、可信信道、用户、厂商、置零及其定义（见2014年版的3.1～3.9、3.11、3.13、3.14、3.16、3.20～3.50、3.52～3.54、3.56～3.59、3.61～3.91、3.94～3.100、3.103、3.104）；

f) 增加了术语密码模块接口、差分功耗分析及其定义（见3.6、3.8）；

g) 更改了缩略语ECB（见第4章，2014年版的第4章）；

h) 删除了2014版文件所列举的部分缩略语，删除了API、CCM、EDC、HDL、HFMI、HMI、HSMI、HMAC、PROM、SFMI（见2014年版的4）；

i) 更改了各类型密码模块的安全域适用性的表述形式（见7.2.2，2014年版的7.2.2）；

j) 增加了“降级工作”相关内容（见7.2.4.3）；

k) 更改了运行环境的安全二级要求的具体细节及表述形式（见7.6.3，2014年版的7.6.3）；

l) 更改了熵的要求的表述形式（见7.9.2，2014年版的7.9.2）；

m) 更改了敏感安全参数存储对不同安全等级的安全要求（见7.9.6节，2014年版的7.9.6）；

n) 增加了敏感安全参数生成和建立方法，更改了“条款”一节的表述形式，将GM/T 0003.3更新

为 GB/T 32918.3，新增了 GM/T 0044.3（见附录 D.2，2014 年版的附录 D.2）；

o） 更改了“鉴别机制”的表述形式，增加了密码模块对操作员所拥有的信息或个人生物特征的鉴别机制（见附录 E.2，2014 年版的附录 E.2）；

p） 更改了“非入侵式攻击”的表述形式（见附录 F，2014 年版的附录 F）；

q） 增加了“非入侵式攻击缓解方法检测指标”相关内容（见附录 F.3）。

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：中国科学院信息工程研究所、中国科学院大学、商用密码检测认证中心、北京数字认证股份有限公司、北京握奇智能科技有限公司、飞天诚信科技股份有限公司、北京海泰方圆科技股份有限公司、格尔软件股份有限公司、北京华大智宝电子系统有限公司、北京创原天地科技有限公司、华为技术有限公司、三未信安科技股份有限公司。

本文件主要起草人：高能、荆继武、屠晨阳、郑昉昱、夏鲁宁、张渊、郑强、朱鹏飞、雷银花、蒋红宇、马原、章庆隆、兰天、高志权、马存庆、刘丽敏、王跃武、向继、王琼霄、林璟锵、詹榜华、罗鹏、汪雪林、陈国、张嘉纯、陈跃、张万涛、谭武征、汪婧。

本文件及其所替代文件的历次版本发布情况为：

——2014 年首次发布为 GM/T 0028—2014；

——本次为第一次修订。

引　言

在信息技术中，密码技术的使用需求日益增强，比如数据需要密码技术的保护以防止非授权的泄露或操控。密码技术可以用于提供实体鉴别、加密保护和不可抵赖等安全服务，密码技术的安全性与可靠性直接取决于实现它们的密码模块。

本文件对密码模块提出了四个递增的、定性的安全要求等级，但不对密码模块的正确应用和安全部署进行规范。密码模块的操作员在使用或部署密码模块时，有责任确保密码模块提供的安全保护是充分的，且对信息所有者而言是可接受的，同时任何残余风险要告知信息所有者。密码模块的操作员有责任选取合适的安全等级的密码模块，使得密码模块能够满足应用的安全需求并适应所处环境的安全现状。

密码模块安全要求

1 范围

本文件确立了密码模块的四个安全等级，并分别规定了四个等级的安全要求。

本文件适用于保护计算机与电信系统内敏感信息的安全系统中密码模块的设计和开发及检测。

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 15843(所有部分) 信息技术 安全技术 实体鉴别

GB/T 15852.1 信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制

GB/T 15852.2 信息技术 安全技术 消息鉴别码 第2部分：采用专用杂凑函数的机制

GB/T 17964 信息安全技术 分组密码算法的工作模式

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 33133(所有部分) 信息安全技术 祖冲之序列密码算法

GB/T 35275 信息安全技术 SM2密码算法加密签名消息语法规范

GB/T 35276 信息安全技术 SM2密码算法使用规范

GB/T 36624 信息技术 安全技术 可鉴别的加密机制

GB/T 38635(所有部分) 信息安全技术 SM9标识密码算法

GB/T 41389 信息安全技术 SM9密码算法使用规范

GM/T 0005 随机性检测规范

GM/T 0057 基于IBC技术的身份鉴别规范

GM/T 0062 密码产品随机数检测要求

GM/T 0081 SM9密码算法加密签名消息语法规范

GM/T 0083 密码模块非入侵式攻击缓解技术指南

3 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

证书 certificate

关于实体的一种数据，该数据由认证机构的私钥或秘密密钥签发，并无法伪造。

注：例如，签名证书、加密证书。

[来源：GB/T 25069—2022，3.779，有修改]