ICS 35.040
L 80

中华人民共和国国家标准

GB/T 37092—2018

信息安全技术　密码模块安全要求

Information security technology—Security requirements for cryptographic modules

2018-12-28 发布　　2019-07-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　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:中国科学院数据与通信保护研究教育中心、国家密码管理局商用密码检测中心、北京握奇智能科技有限公司、北京数字认证股份有限公司、飞天诚信科技股份有限公司、北京海泰方圆科技有限公司、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。

本标准主要起草人:荆继武、高能、屠晨阳、郑昉昱、江伟玉、周国良、马原、刘宗斌、刘泽艺、汪婧、罗鹏、汪雪林、陈国、詹榜华、朱鹏飞、蒋红宇、陈跃、张万涛、刘丽敏、向继。

引　言

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

本标准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。

信息安全技术　密码模块安全要求

1　范围

本标准针对密码模块规定了安全要求，为密码模块定义了四个安全等级，并分别给出了四个安全等级的对应要求。

本标准适用于保护计算机与电信系统内敏感信息的安全系统所使用的密码模块。本标准也为密码模块的设计、开发提供指导，为密码模块安全要求的检测提供参考。

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 15843(所有部分)　信息技术　安全技术　实体鉴别

GB/T 15852(所有部分)　信息技术　安全技术　消息鉴别码

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 33133.1　信息安全技术　祖冲之序列密码算法　第 1 部分：算法描述

GM/T 0001.2　祖冲之序列密码算法　第 2 部分：基于祖冲之算法的机密性算法

GM/T 0001.3　祖冲之序列密码算法　第 3 部分：基于祖冲之算法的完整性算法

GM/T 0044(所有部分)　SM9 标识密码算法

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。

3.2

条件自测试　conditional self-test

当规定的测试条件出现时，由密码模块执行的测试。

3.3

关键安全参数　critical security parameter

与安全相关的秘密信息，这些信息被泄露或被修改后会危及密码模块的安全性。

注：关键安全参数可以是明文形式的也可以是经过加密的。

3.4

密码边界　cryptographic boundary

明确定义的边线，该边线建立了密码模块的物理和/或逻辑边界，并包括了密码模块的所有硬件、软件和/或固件部件。