ICS 35.040
L 80
备案号:44629—2014

中华人民共和国密码行业标准

GM/T 0028—2014

密码模块安全技术要求

Security requirements for cryptographic modules

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用重新起草法参考 ISO 19790:2012《密码模块安全要求》编制，与 ISO 19790:2012 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。

本标准由密码行业标准化技术委员会提出并归口。

本标准的主要起草单位：中国科学院数据与通信保护研究教育中心、北京握奇智能科技有限公司、北京数字认证股份有限公司、赞嘉电子科技(北京)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、国家密码管理局商用密码检测中心、上海格尔软件股份有限公司、北京创元天地科技有限公司。

本标准的主要起草人：高能、荆继武、汪婧、屠晨阳、汪雪林、陈国、詹榜华、张嘉纯、朱鹏飞、蒋红宇、陈跃、罗鹏、谭武征、张万涛、刘丽敏、王跃武、向继、王琼霄、林璟锵、夏鲁宁。

引　言

在信息技术中，密码的应用需求日益增强，比如数据需要密码的保护以防止非授权的访问。密码可以用于支持实体鉴别和不可抵赖等安全服务，密码的安全性与可靠性直接取决于实现它们的密码模块。

本标准规定了四个递增的、定性的安全要求等级，以满足密码模块在不同应用和工作环境中的要求。本标准规定的安全要求涵盖了有关密码模块的安全设计、实现、运行与废弃的安全元素(域)。这些域包括：密码模块规格，密码模块接口，角色、鉴别和服务，软件/固件安全，运行环境，物理安全，非入侵式安全，敏感安全参数管理，自测试，生命周期保障，以及对其他攻击的缓解。

本标准对密码模块提出了安全要求，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应用或部署模块时，有责任确保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。必须选取合适的安全等级的密码模块，使得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。

密码模块安全技术要求

1 范围

本标准针对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，规定了安全要求。本标准为密码模块定义了4个安全等级，以满足敏感数据以及众多应用领域的、不同程度的安全需求。针对密码模块的11个安全域，本标准分别给出了四个安全等级的对应要求，高安全等级在低安全等级的基础上进一步提高了安全性。

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。

GM/Z 0001 密码术语

本标准的附录C、附录D和附录E所列出的文件。

3 术语和定义

GM/Z 0001界定的以及下列术语和定义适用于本文件。

3.1

访问控制列表 access control list

允许访问一个对象的权限列表。

3.2

管理员指南 administrator guidance

密码主管和/或其他管理角色使用的书面资料，用于正确地配置、维护和管理密码模块。

3.3

核准机构 approval authority

授权核准和/或评估安全功能的机构。核准机构的职能是评估和核准安全功能，并不是测试密码模块是否符合本标准。

3.4

核准的数据鉴别技术 approved data authentication technique

经核准的，基于数字签名、消息鉴别码或带密钥的杂凑(如HMAC)等方法的数据鉴别技术。

3.5

核准的完整性技术 approved integrity technique

经核准的，基于杂凑、消息鉴别码或数字签名算法的完整性技术。

3.6

核准的工作模式 approved mode of operation

密码模块的一种工作模式，在该模式下只能使用核准的安全功能，该术语不要与密码算法工作模式混淆，如CBC模式。