ICS 35.040
L 80
备案号：61709—2018

GM

中华人民共和国密码行业标准

GM/T 0054—2018

信息系统密码应用基本要求

General requirements for information system cryptography application

2018-02-08 发布　　2018-02-08 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。

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。

本标准凡涉及密码算法相关内容，按照国家有关法规实施。

本标准起草单位：北京数字认证股份有限公司、国家密码管理局商用密码检测中心、成都卫士通信息产业股份有限公司、长春吉大正元信息技术股份有限公司、中国金融电子化公司、上海交通大学、长沙银河网络有限公司。

本标准起草人：詹榜华、邓开勇、傅大鹏、钟博、阎世杰、傅勇、阎夏强、高振鹏、胡建勋、黄一飞、张众、银鹰、周志洪、李继红、董桂斋。

引　言

密码技术作为网络安全的基础性核心技术，是信息保护和网络信任体系建设的基础，是保障网络空间安全的关键技术。

本标准主要从信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面提出了等级保护不同级别的密码技术应用要求，明确了等级保护不同级别的密钥管理和安全管理要求。

本标准中，“密码”是指“商用密码”。

本标准文本中，“可”表示可以、允许，是陈述型描述，表示在标准的界限内所允许的条款；“宜”表示推荐、建议，是推荐型描述，表示该条款是首选但不是必须要求；“应”表示应该、要求，是要求型描述，表明符合标准需要满足的要求。

信息系统密码应用基本要求

1 范围

本标准规定了信息系统商用密码应用的基本要求。

本标准适用于指导、规范和评估信息系统中的商用密码应用。

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/T 0005 随机性检测规范

GM/T 0028 密码模块安全技术要求

GM/T 0036 采用非接触卡的门禁系统密码应用技术指南

GM/Z 4001—2013 密码术语

3 术语和定义

GM/Z 4001—2013 界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GM/Z 4001—2013 中的一些术语和定义。

3.1

动态口令 one-time-password；OTP；dynamic password

基于时间、事件等方式动态生成的一次性口令。

3.2

访问控制 access control

按照特定策略，允许或拒绝用户对资源访问的一种机制。

3.3

机密性 confidentiality

保证信息不被泄露给非授权的个人、进程等实体的性质。

3.4

加密 encipherment；encryption

对数据进行密码变换以产生密文的过程。

3.5

解密 decipherment；decryption

加密过程对应的逆过程。

3.6

密码算法 cryptographic algorithm

描述密码处理过程的运算规则。

3.7

密钥 key

控制密码算法运算的关键信息或参数。