ICS 35.040
L 80

中华人民共和国国家标准

GB/T 39786—2021

信息安全技术
信息系统密码应用基本要求

Information security technology—
Baseline for information system cryptography application

2021-03-09 发布　　2021-10-01 实施

国家市场监督管理总局
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。

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: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、中国科学院数据与通信保护研究教育中心、公安部第三研究所、上海交通大学、北京信息安全测评中心、成都卫士通信息产业股份有限公司、中国金融电子化公司、飞天诚信科技股份有限公司、安徽科测信息技术有限公司、深圳市网安计算机安全检测技术有限公司、山东省计算中心(国家超级计算济南中心)、中国电子科技集团公司第十五研究所(信息产业信息安全测评中心)、北京电子科技学院、北京三未信安科技发展有限公司、兴唐通信科技有限公司。

本标准主要起草人:詹榜华、宋玲娓、罗鹏、邓开勇、夏鲁宁、霍炜、刘健、许长伟、田敏求、傅大鹏、马原、郑昉昱、陈广勇、黎水林、银鹰、刘芳、肖秋林、张众、李晨旸、张晓溪、杨宏志、朱鹏飞、倪又明、程苏秦、刘健、阎亚龙、高志权、钟博、张文科、刘尚焱。

信息安全技术
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第一级到第四级的密码应用的基本要求，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技术层面提出了第一级到第四级的密码应用技术要求，并从管理制度、人员管理、建设运行和应急处置四个方面提出了第一级到第四级的密码应用管理要求。

注：第五级密码应用仅在本标准中描述通用要求，第五级密码应用技术要求和管理要求不在本标准中描述。

本标准适用于指导、规范信息系统密码应用的规划、建设、运行及测评。在本标准的基础之上，各领域与行业可结合本领域与行业的密码应用需求来指导、规范信息系统密码应用。

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。

GB/T 37092 信息安全技术 密码模块安全要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

机密性 confidentiality

保证信息不被泄露给非授权实体的性质。

3.2

数据完整性 data integrity

数据没有遭受以非授权方式所作的改变的性质。

3.3

真实性 authenticity

一个实体是其所声称实体的这种特性。真实性适用于用户、进程、系统和信息之类的实体。

3.4

不可否认性 non-repudiation

证明一个已经发生的操作行为无法否认的性质。

3.5

加密 encipherment；encryption

对数据进行密码变换以产生密文的过程。

3.6

密钥 key

控制密码算法运算的关键信息或参数。