ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 43207—2023

信息安全技术
信息系统密码应用设计指南

Information security technology—
Guidelines of design for information system cryptography application

2023-09-07 发布　　2024-04-01 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》的规定起草。

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专利的责任。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：鼎铉商用密码测评技术(深圳)有限公司、中国科学院信息工程研究所、哈尔滨工业大学(深圳)、中电科网络安全科技股份有限公司、北京海泰方圆科技股份有限公司、兴唐通信科技有限公司、北京数字认证股份有限公司、公安部第三研究所、国家信息技术安全研究中心、北京信安世纪科技股份有限公司、中科信息安全共性技术国家工程研究中心有限公司、北京市产品质量监督检验研究院、中国平安保险(集团)股份有限公司。

本文件主要起草人：李大为、陈磊、肖飞、马原、郑昉昱、周君平、王学进、蒋红宇、杨元原、傅大鹏、刘尚焱、王彦力、吴冬宇、汪宗斌、秦体红、徐根炜、胡建勋、李恒宇、李锐、贾世杰、陈天宇。

信息安全技术
信息系统密码应用设计指南

1 范围

本文件给出了信息系统密码应用设计指南，包括信息系统密码应用框架、密码应用方案设计原则、密码应用方案设计过程和密码应用方案设计指南。

本文件适用于指导信息系统密码应用方案的设计，也可作为信息系统密码保障建设、密码应用安全性评估和密码管理部门密码应用安全性评估备案工作的参考。

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 22240 信息安全技术 网络安全等级保护定级指南

GB/T 25069 信息安全技术 术语

GB/T 39786 信息安全技术 信息系统密码应用基本要求

3 术语和定义

GB/T 25069 和 GB/T 39786 界定的以及下列术语和定义适用于本文件。

3.1

密码应用方案 cryptography application scheme

用于指导信息系统责任主体合规、正确、有效地使用密码技术，部署密码保障系统的规划。

4 信息系统密码应用框架

使用密码保护的信息系统密码应用框架见图 1。