ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 43206—2023

信息安全技术
信息系统密码应用测评要求

Information security technology—Testing and evaluation requirements 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：国家密码管理局商用密码检测中心、中国科学院信息工程研究所、公安部第三研究所、国家信息技术安全研究中心、中国电子科技集团公司第十五研究所、中国电子技术标准化研究院、国家信息中心、工业和信息化部电子第五研究所、中国科学院软件研究所、北京市政务信息安全保障中心(北京信息安全测评中心)、北京国家数字金融技术检测中心有限公司、深圳市网安计算机安全检测技术有限公司、道普信息技术有限公司、国电南京自动化股份有限公司、浙江东安检测技术有限公司、北京银联金卡科技有限公司、智巡密码(上海)检测技术有限公司、哈尔滨工业大学(深圳)、安徽科测信息技术有限公司、新疆量子通信技术有限公司。

本文件主要起草人：罗鹏、肖秋林、马原、张立花、许长伟、陈天宇、黄晶晶、郑昉昱、田敏求、王兵、刘健、杨宏志、吴冬宇、陆臻、张宇翔、李升、任金强、黎水林、李大为、李宏卓、张五一、张晓溪、杨辰、蔡一鸣、孙鑫、高锐、吕娜、宋玲娓、郭守坤、何双羽、杨龙、李霞、王国朝、胡盖、胡燕雄、沈汀、张绍博、韩玮。

信息安全技术
信息系统密码应用测评要求

1 范围

本文件规定了信息系统第一级到第四级密码应用的通用测评要求、技术测评要求、管理测评要求，并给出了整体测评要求、风险分析和评价、测评结论的要求。

注：本文件描述的信息系统密码应用等级与GB/T 39786—2021规定的密码应用等级一致，其中第五级密码应用的测评要求不在本文件中描述。

本文件适用于指导、规范信息系统密码应用安全性评估工作中的测评活动。

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 25069—2022 信息安全技术 术语

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

GM/Z 4001 密码术语

3 术语和定义

GB/T 25069—2022、GB/T 39786—2021和GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

密码应用安全性评估人员 commercial cryptography application security evaluation staff

通过国家密码管理部门认可的考核或具有密码技术应用员、密码工程技术人员职业技能等级证书，从事密码应用安全性评估的人员。

注：简称“密评人员”。

3.2

核查 examine

密评人员对测评对象进行访谈、文档审查、实地查验和分析，以帮助密评人员理解、澄清或取得证据的过程。

注：核查时可选用的测评方式以及方式的选用说明参考GM/T 0116—2021。

[来源：GB/T 25069—2022，3.237，有修改]

3.3

测评单元 unit of testing and evaluation

一组相对独立和完整的测评内容，由测评指标、测评对象、测评实施和结果判定组成。