ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0132—2023

信息系统密码应用实施指南

Implementation guide for information system cryptography application

2023-12-04 发布　　2024-06-01 实施

国家密码管理局　　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。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：兴唐通信科技有限公司、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、中国科学院数据与通信保护研究教育中心、北京信安世纪科技有限公司、北京数盾信息科技有限公司、三未信安科技股份有限公司、阿里云计算有限公司、中电科网络安全科技股份有限公司、公安部第三研究所、蚂蚁科技集团股份有限公司、鼎铉商用密码测评技术(深圳)有限公司、北京天融信网络安全技术有限公司、中金金融认证中心有限公司、阿里巴巴(中国)网络技术有限公司、上海市数字证书认证中心有限公司、中互金认证有限公司、国家信息技术安全研究中心、深圳市腾讯计算机系统有限公司、中国电子科技集团公司第十五研究所、中国国家铁路集团有限公司、暨南大学、启明星辰信息安全技术有限公司。

本文件主要起草人：王彦力、刘尚焱、许长伟、王兵、马原、郑昉昱、肖秋林、吴星宇、贾世杰、田爱军、孙丽伟、姚长远、胡伟、何济尘、梅秋丽、汪宗斌、秦体红、吴冬宇、刘健、张立花、杨辰、陈天宇、吕娜、袁静、乐宏彦、陈萧宇、许涛、张大江、周君平、张宇翔、宋铮、陈磊、万志宇、马春旺、朱红儒、谭武征、李增局、姬生利、杨龙、田涛、于航、高志权、鹿淑煜、吴波、华珊、李升、方海峰、肖飞、安高峰、贺磊、司华峰、彭晋、黄天宁、李冰、谢灿、蒋增增、苏继海、孙欣、刘志刚、史汝辉、朱凌。

信息系统密码应用实施指南

1 范围

本文件给出了信息系统密码应用的流程指导和建议，描述了规划、建设、运行及终止阶段的实施过程及主要活动。

本文件适用于指导信息系统密码应用的实施。

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 20984 信息安全技术 信息安全风险评估方法

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GM/T 0115 信息系统密码应用测评要求

GM/T 0116 信息系统密码应用测评过程指南

GM/Z 4001 密码术语

3 术语和定义

GB/T 39786 和 GM/Z 4001 界定的术语和定义适用于本文件。

4 信息系统密码应用实施概述

4.1 角色和职责

信息系统密码应用中涉及的各类角色及其职责如下。

a） 密码管理部门

负责依法管理密码工作。

b） 信息系统责任单位

通常包括项目建设单位以及信息系统运营、使用单位，负责依照信息系统密码应用的管理规范和技术标准，进行密码应用方案的设计；使用符合国家规定、满足信息系统对应等级密码应用基本要求的密码算法、密码技术、密码产品和密码服务，开展信息系统密码应用建设或整改工作；制定、落实各项密码应用配套安全管理制度，定期对信息系统密码应用安全状况、密码应用配套安全管理制度及措施的落实情况进行自查；自行或委托商用密码应用安全性评估机构开展商用密码应用安全性评估（简称“密评”），包括密码应用方案密评（简称“方案密评”）和信息系统密评（简称“系统密评”）；对密码应用安全事件进行应急处置。

c） 密码应用集成服务单位

负责根据信息系统责任单位的委托，依照信息系统密码应用的管理规范和技术标准，协助信息系统责任单位完成信息系统密码应用的规划、建设、运行及终止阶段的工作（包括但不限于密码应用咨