ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0115—2021

信息系统密码应用测评要求

Testing and evaluation requirements for information system cryptography application

2021-10-19 发布　　2022-05-01 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：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、公安部三所（公安部信息安全等级保护评估中心）、上海交通大学、中国电子科技集团第十五研究所（信息产业信息安全测评中心）、国家信息技术安全研究中心、深圳市网安计算机安全检测技术有限公司、北京信息安全测评中心、山东道普测评技术有限公司。

本文件主要起草人：肖秋林、罗鹏、马原、陈天宇、郑昉昱、银鹰、张立花、吕娜、黎水林、刘健、杨宏志、吴冬宇、李晨旸、张晓溪。

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不同等级密码应用的测评要求，从密码算法合规性、密码技术合规性、密码产品合规性、密码服务合规性以及密钥管理安全性等方面，提出了第一级到第五级的密码应用通用测评要求；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、应用和数据安全等四个技术层面提出了第一级到第四级的密码应用技术测评要求；从管理制度、人员管理、建设运行和应急处置等四个管理方面提出了第一级到第四级的密码应用管理测评要求，并给出了整体测评、风险分析和评价、测评结论等测评环节的要求。

本文件适用于指导、规范信息系统密码应用在规划、建设、运行环节的商用密码应用安全性评估工作。

注：第五级密码应用测评要求只在本文件中描述通用测评要求。

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 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 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

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

在商用密码应用安全性评估机构中从事商用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观察、查验和分析，以帮助密评人员理解、澄清或取得证据的过程。

4 概述

本文件根据 GB/T 39786—2021，将信息系统密码应用测评要求分为通用测评要求、密码应用技术和密码应用管理测评要求。第 5 章用于指导第 6 章的实施，不单独实施测评，也不单独体现在密码应用安全性评估报告的单元测评结果和整体测评结果中。附录 A 为 5.5 的测评实施参考。附录 B 和附录 C 分别给出了典型密码产品应用测评技术和典型密码功能测评技术，供密评人员在对信息系统中具体使用的密码产品或应用的密码功能进行测评实施时参考。