ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0116—2021

信息系统密码应用测评过程指南

Testing and evaluation process guide 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。

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）、深圳市网安计算机安全检测技术有限公司、国家信息技术安全研究中心、山东道普测评技术有限公司、北京信息安全测评中心。

本文件主要起草人：肖秋林、罗鹏、马原、贾世杰、银鹰、郑昉昱、张立花、黎水林、牛莹姣、刘健、杨宏志、吴冬宇、张晓溪、陈亚男。

信息系统密码应用测评过程指南

1 范围

本文件规定了信息系统密码应用的测评过程，规范了测评活动及其工作任务。

本文件适用于商用密码应用安全性评估机构、信息系统责任单位开展密码应用安全性评估工作。

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—2010 信息安全技术 术语

GM/T 0115 信息系统密码应用测评要求

GM/Z 4001 密码术语

3 术语和定义

GB/T 25069—2010 和 GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

测评方 testing and evaluation agency

对信息系统开展密码应用安全性评估(简称“密评”)的主体。

注：具体可以是商用密码应用安全性评估机构或信息系统责任单位。

3.2

被测单位 agency under testing and evaluation

信息系统责任单位。

3.3

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

测评方中从事测评活动的人员。

注：简称“密评人员”。

4 概述

4.1 基本原则

测评方对信息系统开展密码应用安全性评估时，应遵循以下原则。

a) 客观公正性原则

测评实施过程中，测评方应保证在符合国家密码管理部门要求及最小主观判断情形下，按照与被测单位共同认可的密评方案，基于明确定义的测评方式和解释，实施测评活动。

b) 可重用性原则

测评工作可重用已有测评结果，包括商用密码检测认证结果和密码应用安全性评估的测评结果等。