ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0124—2022

安全隔离与信息交换产品密码检测规范

Cryptography test specification for secure separation and information exchange product

2022-11-20 发布　　2023-06-01 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：国家密码管理局商用密码检测中心、奇安信网神信息技术（北京）股份有限公司、南瑞集团有限公司、北京安盟信息技术股份有限公司。

本文件主要起草人：孙浩、燕爽、邓开勇、李冬、李国友、杨维永、朱孟江、唐磊、张璐、张大伟、韩斐、刘智飞。

安全隔离与信息交换产品
密码检测规范

1 范围

本文件规定了安全隔离与信息交换产品的密码检测内容、检测要求、检测方法及文档要求。

本文件适用于安全隔离与信息交换产品的检测，以及该类产品的研制。

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 15843(所有部分) 信息技术 安全技术 实体鉴别

GB/T 20279—2015 信息安全技术 网络和终端隔离产品安全技术要求

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 32915 信息安全技术 二元序列随机性检测方法

GB/T 32918(所有部分) 信息安全技术 SM2 椭圆曲线公钥密码算法

GM/T 0062 密码产品随机数检测要求

GM/Z 4001—2013 密码术语

3 术语和定义

GM/Z 4001 界定的及以下术语和定义适用于本文件。

3.1

安全隔离与信息交换产品 secure separation and information exchange product

能够保证不同网络之间在网络协议终止的基础上，通过安全通道在实现网络隔离的同时进行安全数据交换的软硬件组合。

3.2

安全域 security domain

具有相同的安全保护需求和相同的安全策略的计算机或网络区域。

3.3

安全等级 security level

网络隔离与信息交换产品的安全等级划分为基本级和增强级。

4 检测内容

4.1 概述

安全隔离与信息交换产品检测的主要内容包括 12 项：