ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0121—2022

密 码 卡 检 测 规 范

Test specification for cryptographic board

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、山东渔翁信息技术股份有限公司、三未信安科技发展有限公司、北京江南天安科技有限公司、兴唐通信科技有限公司、成都卫士通信息产业股份有限公司、鼎铉商用密码测评技术（深圳）有限公司、智巡密码（上海）检测技术有限公司。

本文件主要起草人：陈妍、李国友、李冬、邓开勇、顾伟平、齐晶晶、宋志华、吴震、高志权、张玉国、桑洪波、马晓艳、姚长远、何济尘、高伟、孟琦、秦放、凌杭、包斯刚、韩玮。

密码卡检测规范

1 范围

本文件规定了密码卡的检测内容、检测方法、检测要求及文档要求。

本文件适用于密码卡的检测，以及该类密码设备的研制，也可用于指导基于该类密码设备的应用开发。

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 15852.2 信息技术 安全技术 消息鉴别码 第2部分：采用专用杂凑函数的机制

GB/T 17964 信息安全技术 分组密码算法的工作模式

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 32918(所有部分) 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 33133(所有部分) 信息安全技术 祖冲之序列密码算法

GB/T 33560 信息安全技术 密码应用标识规范

GB/T 35275 信息安全技术 SM2密码算法加密签名消息语法规范

GB/T 35276 信息安全技术 SM2密码算法使用规范

GB/T 38635(所有部分) 信息安全技术 SM9标识密码算法

GB/T 36624 信息技术 安全技术 可鉴别的加密机制

GM/T 0005 随机性检测规范

GM/T 0018 密码设备应用接口规范

GM/T 0039 密码模块安全检测要求

GM/T 0050 密码设备管理 设备管理技术规范

GM/T 0062 密码产品随机数检测要求

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

密码卡 cryptographic board card

具有密码运算功能、密钥管理和自身安全防护等功能的硬件板卡设备。

3.2

保护密钥 protection key

用于加密保护设备中其他密钥和敏感信息安全的密钥。