ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0137—2024

密 码 卡 技 术 要 求

Technical requirements for cryptographic board

2024-12-27 发布　　2025-07-01 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：三未信安科技股份有限公司、中国科学技术大学、商用密码检测认证中心、山东大学、中电科网络安全科技股份有限公司、兴唐通信科技有限公司、渔翁信息技术股份有限公司、天津国芯科技有限公司、山东三未信安信息科技有限公司、北京格尔国信科技有限公司、豪符密码检测技术（成都）有限责任公司、山东多次方半导体有限公司。

本文件主要起草人：高志权、霍卫华、徐强、李玉峰、林璟锵、陈妍、李国友、李冬、邓开勇、雷银花、齐晶晶、桑洪波、张玉国、赵长松、杨国强、孔凡玉、郭刚、张斌、陈万钢、陈万瑶、曹丹、朱立通、张佳潇、张驰。

密码卡技术要求

1 范围

本文件规定了密码卡的功能要求、硬件要求、软件要求、安全性要求等有关内容。

本文件适用于密码卡的研制开发，也可用于指导密码卡的使用和检测。

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 网络安全技术 消息鉴别码 第2部分：采用专门设计的杂凑函数的机制

GB/T 17964 信息安全技术 分组密码算法的工作模式

GB/T 36624 信息技术 安全技术 可鉴别的加密机制

GB/T 37092—2018 信息安全技术 密码模块安全要求

GM/T 0018—2023 密码设备应用接口规范

GM/T 0062—2018 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

具有密码运算功能、密钥管理和自身安全保护功能的硬件板卡设备。

3.2

设备密钥对 device key pair

用于表明设备身份、对设备进行管理的非对称密钥对，包含签名密钥对和加密密钥对。

3.3

密钥加密密钥 key encrypting key；KEK

用于对密钥进行加密或解密的密钥。

3.4

私钥访问控制码 private key access password

用于获取私钥使用权限的口令字。

3.5

数据加密密钥 data encipherment/encryption key

用于数据加解密的密钥。

3.6

会话密钥 session key

在一次会话中使用的数据加密密钥。