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。

3.7

用户密钥对　user key pair

存储在设备内部的用于应用密码运算的非对称密钥对，包含签名密钥对和加密密钥对。

3.8

虚拟机　virtual machine

由共享真实数据处理系统的各种资源来实现其内部功能的一种虚拟数据处理系统，其中信息独属于某位特定用户来使用。

4　缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

CBC：密文分组链接工作模式（Cipher Block Chaining Operation Mode）

CFB：密文反馈工作模式（Cipher Feedback Operation Mode）

CPCI：紧凑型外设部件互连（Compact Peripheral Component Interconnect）

CTR：计数器工作模式（Counter Operation Mode）

DMA：直接存储器访问（Direct Memory Access）

ECB：电码本工作模式（Electronic Codebook Operation Mode）

GCM：Galois 计数器模式（Galois Counter Mode）

HMAC：带密钥的杂凑算法（Keyed-Hash Message Authentication Code）

IC：集成电路（Integrated Circuit）

I/O：输入/输出（Input/Output）

IPSec：IP 安全（Internet Protocol Security）

KVM：一个开源的系统虚拟化模块（Kernel-based Virtual Machine）

Mini PCI-E：微型高性能外设部件互连（Mini Peripheral Component Interconnection Express）

OFB：输出反馈工作模式（Output Feedback Operation Mode）

PCI：外设部件互连（Peripheral Component Interconnection）

PCI-E：高性能外设部件互连（Peripheral Component Interconnection Express）

SATA：串行 ATA（Serial Advanced Technology Attachment）

SoC：系统级芯片（System on Chip）

SSL：安全套接字层（Secure Sockets Layer）

USB：通用串行总线（Universal Serial Bus）

VPN：虚拟专用网络（Virtual Private Network）

5　概述

密码卡是一种硬件密码模块，具有以下特征：

a）　具备但不限于下列一个或多个硬件接口：PCI、PCI-E、Mini PCI-E、SATA 、USB、CPCI、M.2 等；

b）　由多芯片组成、嵌入式运行；

c）　具有密码运算功能、密钥管理功能、物理随机数产生功能和设备自身安全保护措施。

密码卡可作为关键密码部件内嵌于需要密码运算和密钥管理等安全功能的计算机上，例如：服务器密码机、SSL VPN 网关、IPSec VPN 网关、云服务器密码机、时间戳服务器、安全认证网关等，也可直接作为密码资源使用或直接为应用程序提供密码功能。

6 功能要求

6.1 功能分类

密码卡的功能包括基本功能和扩展功能。

a) 基本功能，主要包括：
   1) 初始化；
   2) 密码运算；
   3) 密钥管理；
   4) 访问控制；
   5) 设备自检；
   6) 设备信息存储。
b) 扩展功能是根据应用需要进行合理扩充的功能，主要包括：虚拟化。

6.2 初始化

应至少支持初始和就绪两个状态。在初始状态下，可获取设备信息、添加管理员及操作员（若支持操作员角色）、生成或恢复设备密钥对和保护密钥。就绪状态下，应能根据角色权限执行相关操作。

6.3 密码运算

6.3.1 非对称密码算法

应支持至少一种 GB/T 37092—2018 的附录 C 中核准的非对称密码算法，支持数字签名及验证、数据加解密和密钥协商等运算。

6.3.2 对称密码算法

应支持至少一种 GB/T 37092—2018 的附录 C 中核准的对称密码算法。

应支持 ECB 和 CBC 两种工作模式，可支持其他工作模式（如 CFB、OFB、CTR、GCM 等）作为扩展功能，工作模式应符合 GB/T 17964、GB/T 36624 描述的工作模式。

6.3.3 密码杂凑算法

应支持至少一种 GB/T 37092—2018 的附录 C 中核准的密码杂凑算法，宜支持带密钥的杂凑算法（HMAC）运算，HMAC 应遵循 GB/T 15852.2。

6.3.4 随机数生成

密码卡内部应包含至少两个独立的随机数发生器，提供随机数序列的生成。

6.3.5 扩展密码算法

密码卡可支持其他专用密码算法。

6.4 密钥管理

6.4.1 密钥体系

密码卡应支持至少三级密钥结构体制：第一级是保护密钥，第二级是用户密钥对、密钥加密密钥和设备密钥对，第三级是会话密钥、数据加密密钥。密钥结构见图 1。

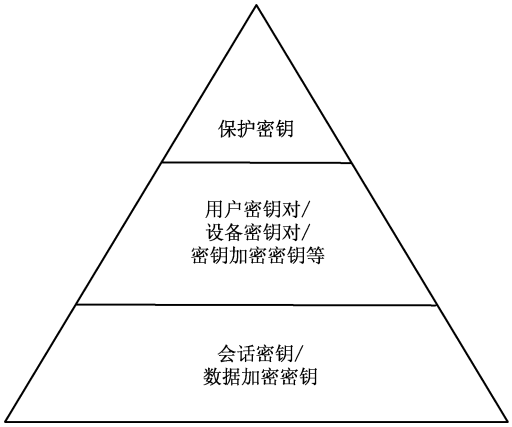

图 1　密钥结构

6.4.2　保护密钥

保护密钥用于用户密钥对或密钥加密密钥的安全存储保护。生成或安装、存储等功能满足以下要求：

a）　应在密码卡初始化时生成或通过可信信道安装，应使用随机数发生器生成；

b）　应以安全形式存储在密码卡硬件内部，如微电保护、密钥分量等；

c）　宜提供紧急销毁的安全保护措施，以确保密码卡自身的安全性。

6.4.3　设备密钥对

设备密钥对包括签名密钥对和加密密钥对，用于自身或所属设备的远程管理功能。生成或安装、导入、备份和恢复、销毁等功能满足以下要求：

a）　签名密钥对应在密码卡初始化时生成或安装，并以密文等安全形式存储在密码卡硬件内部；

b）　加密密钥对应由密钥管理中心生成，并在对应索引的签名公钥加密保护下导入，数据格式应遵循 GM/T 0018—2023 的 5.9；

c）　应提供设备密钥对的安全备份和恢复；

d）　宜提供紧急销毁的安全保护措施。

6.4.4　用户密钥对

用户密钥对包括签名密钥对和加密密钥对，用于实现数字签名、签名验证、加解密以及保护会话密钥等功能。生成或安装、导入、存储、运算、销毁等功能满足以下要求：

a）　签名密钥对应在密码卡内使用随机数发生器生成；

b）　加密密钥对应由密钥管理中心生成，并在对应索引的签名公钥加密保护下导入，数据格式应遵循 GM/T 0018—2023 的 5.9；

c）　应支持用户密钥对的存储；

d）　私钥应以密文等安全形式存储在密码卡硬件内部；

e）　私钥运算应受私钥访问控制码的安全访问控制保护；

f）　应提供用户密钥对的安全备份和恢复；

g）　应提供密钥销毁功能；

h）　宜提供紧急销毁的安全保护措施。

6.4.5 密钥加密密钥

密钥加密密钥用于会话密钥的安全保护功能。生成或安装、备份和恢复、销毁等功能满足以下要求：

a) 应支持由管理工具安装或调用密码卡生成；
b) 应提供密钥加密密钥的安全备份和恢复；
c) 应提供密钥销毁功能；
d) 宜提供紧急销毁的安全保护措施。

6.4.6 会话密钥和数据加密密钥

会话密钥和数据加密密钥用于数据加解密运算、MAC 计算等。生成、导入导出、存储、销毁等功能满足以下要求：

a) 应使用随机数发生器生成或密钥协商等安全方式生成；
b) 应支持基于用户密钥对或密钥加密密钥保护的安全导入导出；
c) 如需存储会话密钥或数据加密密钥，应支持用户密钥对或密钥加密密钥加密存储等安全保护措施；
d) 应提供密钥销毁功能；
e) 宜提供紧急销毁的安全保护措施。

6.5 访问控制

密码卡应支持权限分级的访问控制功能，并满足以下要求：

a) 应支持管理员权限，可支持操作员权限；
b) 应通过管理员权限认证后执行密钥管理操作；
c) 宜通过管理员权限或操作员权限认证后提供密码运算功能；
d) 无操作员时，可配置为上电启动后即提供密码运算功能。

6.6 设备自检

密码卡的自检功能要求如下：

a) 应具有上电自检功能并输出状态指示；
b) 设备自检功能应包括密码算法正确性检查、随机数自检、密钥等静态存储数据和固件完整性，及其他需要进行自检的功能部件；
c) 随机数自检应符合 GM/T 0062—2018 中 D 类产品的检测要求。

6.7 设备信息存储

密码卡应具有唯一的设备标识信息，以区分不同厂家、不同型号的密码卡。设备标志信息应包括：生产厂商、设备类型、序列号、硬件版本、软件版本、支持算法等。用户通过这些信息来查验和辨识密码卡。设备标识信息通过 GM/T 0018—2023 中的函数 SDF_GetDeviceInfo 获取。

6.8 虚拟化

密码卡宜支持在虚拟化环境中使用，如支持 KVM、Docker 等虚拟化环境，可支持硬件虚拟化功能。

7 硬件要求

7.1 接口

密码卡硬件接口可具备但不限于：PCI、PCI-E、Mini PCI-E、SATA、USB、CPCI、M.2 等接口。

7.2 硬件组成

密码卡的基本硬件组成中包括但不限于以下一种或多种部件：

a) 密码算法模块；
b) 处理器；
c) 安全芯片；
d) 物理噪声源；
e) 非易失性存储器；
f) 接口芯片等。

7.3 密码算法模块

密码算法模块实现密码运算功能，宜采用经过检测认证的密码算法芯片或安全芯片以及通用可编程器件、固件等实现方式。

7.4 随机数发生器

随机数发生器实现随机数的生成/采集功能，应采用经过检测认证的物理噪声源或具备同等功能的安全芯片实现。

8 软件要求

8.1 软件构成

密码卡软件包括：固件、驱动程序、应用编程接口和管理工具。

8.2 固件

固件是运行于密码卡内部芯片的所有软件程序的总称。固件自检满足以下要求：

a) 应支持密码算法正确性自检；
b) 应支持固件完整性自检；
c) 应支持密钥与密钥管理记录的一致性及完整性自检；
d) 应支持随机数自检，符合 GM/T 0062—2018 中 D 类产品的检测要求；
e) 应支持数据完整性自检。

8.3 驱动程序

驱动程序是使计算机与密码卡进行相互通信的特殊程序。数据传输、安装/卸载、使用和操作满足以下要求：

a) 应透明传输应用系统和密码卡缓存区之间的数据，不截获且不解析应用系统的数据结构；
b) 应支持安装/卸载驱动程序；
c) 宜支持多个密码卡同时使用和操作的基本要求。

8.4 应用编程接口(API)

密码卡的 API 接口应遵循 GM/T 0018—2023。

8.5 管理工具

管理工具可通过管理界面实现对密码卡进行初始化、权限管理、密钥管理等管理功能。

管理工具可以是独立提供的软件,也可以集成在内嵌密码卡的密码整机管理工具。

9 安全性要求

9.1 通用安全

密码卡为硬件模块,安全性设计应遵循 GB/T 37092—2018 相应安全级别要求。访问控制安全、固件安全、虚拟化安全等方面不低于 9.2、9.3 和 9.4 的安全要求。

9.2 访问控制安全

管理员及操作员应采用智能密钥钥匙或智能 IC 卡作为安全管理载体。

9.3 固件安全

固件的安全要求如下:

a) 固件完整性校验应采用数字签名或 HMAC 机制;
b) 固件内不应包含源代码及解释执行的程序;
c) 固件无调试接口。

9.4 虚拟化安全

密码卡虚拟化是扩展功能。若密码卡支持虚拟化功能:

a) 应支持虚拟机与虚拟密码卡之间的绑定授权,虚拟机不能访问其他未绑定虚拟密码卡;
b) 应支持各虚拟密码卡间密钥及用户数据存储空间隔离相互独立;
c) 应支持各虚拟密码卡间管理隔离,各虚拟密码卡管理互不影响;
d) 应支持各虚拟密码卡间调用隔离,各虚拟密码卡的应用编程接口独立运行;
e) 宜支持创建多个虚拟密码卡,在各虚拟机中能够分别呈现独立的虚拟密码卡设备,且每个虚拟密码卡有独立的 I/O 资源、内存资源、DMA 资源、安全存储区等。

参 考 文 献

[1] 国家密码管理局.PCI 密码卡技术规范

中华人民共和国密码
行业标准
密码卡技术要求
GM/T 0137—2024
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
网址 www.spc.net.cn
总编室:(010)68533533　发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1　字数 19 千字
2025年6月第1版　2025年6月第1次印刷
*
书号:155066·2-39071　定价 31.00 元

GM/T 0137-2024