ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0134—2024

密码模块安全设计指南

Security design guidance for cryptographic modules

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：北京握奇智能科技有限公司、中国科学院大学、商用密码检测认证中心、飞天诚信科技股份有限公司、深圳市文鼎创数据科技有限公司、山东大学、北京海泰方圆科技股份有限公司、工业信息安全（四川）创新中心有限公司、北京江南天安科技有限公司、北京天威诚信电子商务服务有限公司、西安得安信息技术有限公司、智巡密码（上海）检测技术有限公司、鼎铉商用密码测评技术（深圳）有限公司、豪符密码检测技术（成都）有限责任公司、长春吉大正元信息技术股份有限公司、浙江蚂蚁密算科技有限公司。

本文件主要起草人：张渊、郑昉昱、李国友、李勃、王慧、李小雨、朱鹏飞、崔永娜、刘伟丰、陈妍、孔凡玉、罗影、胡伯良、马晓艳、王超、马洪富、韩玮、胡之斐、饶金涛、孙浩、张宇韬、李超。

引　言

GM/T 0028—2024《密码模块安全技术要求》针对密码模块的11个安全域分别规定了四个安全等级的对应要求，本文件从密码模块安全设计的角度阐述了落实这些要求的通用设计方法和建议，旨在为GM/T 0028—2024中的安全要求条款提供解释和指导，以促进对GM/T 0028—2024理解的一致性和应用标准的符合性。

密码模块安全设计指南

1 范围

本文件提供了密码模块安全设计过程的指导和建议，给出了针对 GM/T 0028—2024 对应的安全要求章节中，有代表性安全要求条款疑问的具体解读、解释和设计指导。

本文件适用于密码模块的设计、开发和检测。本文件不适用于密码安全芯片设计的指导。

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 信息安全技术 术语

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 35276 信息安全技术 SM2 密码算法使用规范

GM/T 0005 随机性检测规范

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0028—2024 密码模块安全技术要求

GM/T 0083 密码模块非入侵式攻击缓解技术指南

GM/T 0084 密码模块物理攻击缓解技术指南

GM/T 0103 随机数发生器总体框架

3 术语和定义

GB/T 25069 和 GM/T 0028—2024 界定的术语和定义适用于本文件。

4 缩略语

下列缩略语适用于本文件。

CA：认证中心（Certificate Authority）

DEP：默认入口点（Default Entry Point）

EEPROM：带电可擦可编程只读存储器（Electrically Erasable Programmable Read Only Memory）

5 设计原则

5.1 符合性

GM/T 0028—2024 规定了密码模块的四个安全等级及对应的安全要求，这对密码模块的安全设计

是至关重要的。GM/T 0028—2024 的 11 个安全域中规定的具体安全条款是密码模块安全设计时的重要因素。

5.2 系统性

密码模块安全设计宜按系统性原则考虑其技术框架、需求分析、安全域选取和详细设计。

6 密码模块安全设计过程

6.1 密码模块设计技术框架

6.1.1 密码模块的一般性质

密码模块本身是承担具体安全功能的产品，它一般具备以下性质：

a) 有明确的边界，边界上有可靠的隔离机制；
b) 外部只能通过边界上已定义的接口访问和操作密码模块，而且只有授权用户才能访问和操作密码模块；
c) 密码模块按照设计运行、提供安全功能服务，且敏感安全参数在安全功能服务过程中不会被非授权的访问、使用、泄露、修改和替换；
d) 可以防范攻击者从正常接口或者在边界之外收集可利用信息，以缓解非入侵式攻击或其他攻击。

6.1.2 密码模块设计技术框架

密码模块的安全性由其自身保证以满足 GM/T 0028 的安全要求，密码模块设计技术框架见图 1。此外，还需考虑调用密码模块的实体以及密码模块所处的外部环境。

a) 密码模块所处的外部环境：密码模块的整体安全性除了依赖于密码模块自身，还依赖于其所处的外部环境，特别是安全等级较低的密码模块。
b) 调用密码模块的实体：调用密码模块的实体可能是人、应用或进程，密码模块的安全功能由具体密码应用需求所决定，同时密码模块的安全性可能部分依赖于密码模块的调用者，特别是安全等级较低的密码模块。

图 1 中(1)～(11)分别代表 GM/T 0028—2024 中 7.1 中规定的 11 个安全域。图 1 展示了这 11 个安全域与密码模块设计技术框架的关联关系。图 1 中对于不同类型的密码模块，其边界划定和内部的组件可能不同。比如软件密码模块的边界不包括操作系统和物理边线。

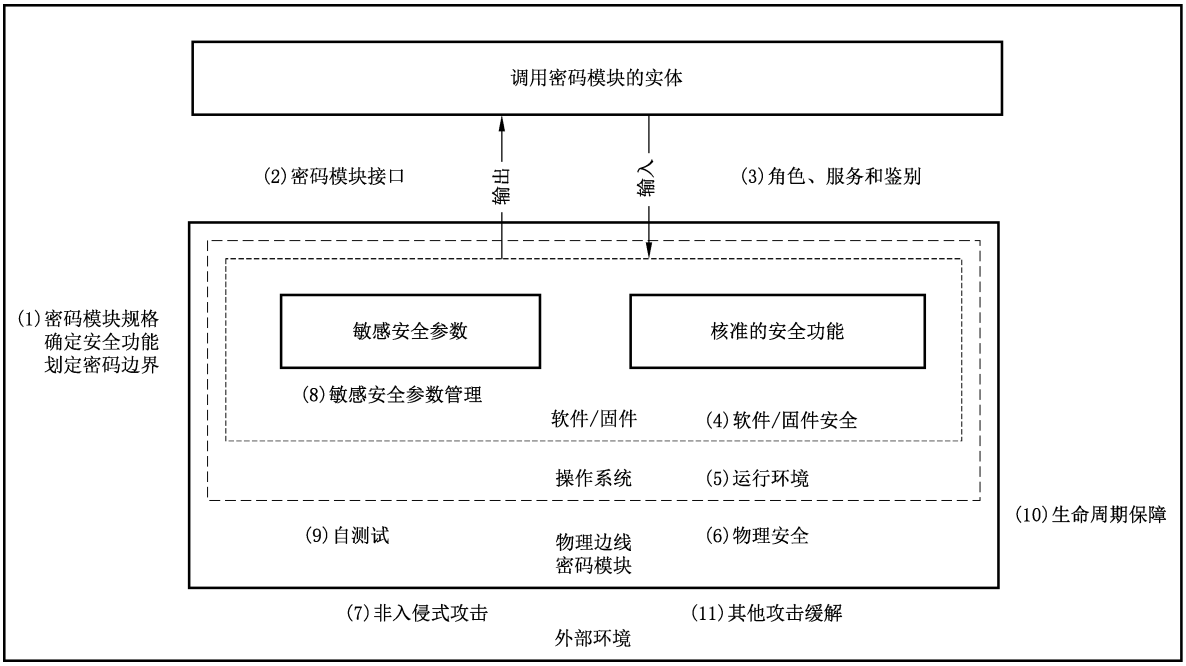

图 1　密码模块设计技术框架

6.2　密码模块需求分析

6.2.1　功能需求分析

密码模块的设计者需要根据密码模块调用者的需求，根据 GM/T 0028—2024 的附录 C 选取相应的安全功能。为了降低密码模块自身由于安全漏洞所导致的安全风险，密码模块的安全功能宜尽量精简，只包括必要的安全功能。

6.2.2　安全需求分析和安全等级选取

在选取密码模块所达到的安全等级时，需要考虑 2 个部分内容。

a）　调用密码模块实体的应用需求：包括调用密码模块实体所需要的安全功能以及所保护信息资产的重要程度。它直接影响了密码模块的安全等级要求，以及对于密码模块的功能设计。

b）　密码模块所处的外部环境：主要指外部环境提供的防护能力。外部环境的防护能力越低，环境中存在的安全风险就越高；而防护能力越高，则安全风险也会随之降低。它直接影响了密码模块的安全等级要求，以及对于密码模块的功能设计。

6.3　安全域选取

按照 GM/T 0028—2024 中[02.04]、[02.05]和[02.06]的要求，不同密码模块类型的安全域选取见表 1。

表 1　不同密码模块类型的安全域选取

安全域	(1)密码模块规格	(2)密码模块接口	(3)角色、服务和鉴别	(4)软件/固件安全	(5)运行环境	(6)物理安全	(7)非入侵式安全	(8)敏感安全参数管理	(9)自测试	(10)生命周期保障	(11)对其他攻击的缓解
硬件密码模块	√	√	√	√[–]	√[#]	√	√	√	√	√	可选

表 1　不同密码模块类型的安全域选取（续）

安全域	(1)密码模块规格	(2)密码模块接口	(3)角色、服务和鉴别	(4)软件/固件安全	(5)运行环境	(6)物理安全	(7)非入侵式安全	(8)敏感安全参数管理	(9)自测试	(10)生命周期保障	(11)对其他攻击的缓解
软件密码模块	√	√	√	√	√	可选	√*	√	√	√	可选
固件密码模块	√	√	√	√	√#	√	√	√	√	√	可选
混合软件密码模块	√	√	√	√	√#	√	√	√	√	√	可选
混合固件密码模块	√	√	√	√	√#	√	√	√	√	√	可选

注 1：“√”指适用的安全域。

注 2：“—”指完全由硬件实现的密码模块不需选取“(4)软件/固件安全”。

注 3：“*”指提供对计时攻击的缓解措施对软件密码模块的安全设计是十分重要的。

注 4：“#”指如果密码模块物理安全域达到了安全二级及以上，且运行环境为受限或不可修改的，“(5)运行环境”无额外要求。

6.4　密码模块设计详细技术

6.4.1　设计流程

密码模块在进行设计时，宜遵循以下过程进行。

a) 边界划分和边界隔离机制设计：根据密码模块的需求分析，确定密码模块的密码边界，并根据不同的模块类型，设计和实现相应的物理/逻辑边界隔离机制。

b) 接口设计：根据密码模块的需求分析，确定在物理/逻辑边界隔离机制上建立对外服务的物理端口或逻辑接口。

c) 角色、服务、鉴别设计：根据密码模块的需求分析，确定密码模块对外提供的服务类型及其所使用的接口，同时确定哪些授权角色可以访问该服务，并确定每一个角色的鉴别方式。

d) 软件/固件设计：根据密码模块的功能，设计和实现密码模块的软件/固件，以确保其可以完成相应功能。

e) 敏感安全参数管理设计：根据密码模块安全功能所涉及的各类敏感安全参数，设计和实现全生命周期的保护措施。

f) 非入侵式安全/其他攻击缓解设计：分析攻击者从正常接口或从边界外收集信息，从而非授权获取密码模块敏感安全参数的风险，设计和实现非入侵式攻击的缓解措施；此外，可以设计和实现针对 GM/T 0028—2024 未考虑到、未来可能出现的新型攻击的缓解措施。

g) 自测试设计：在密码模块的运行前和运行时两个阶段进行自测试，保证密码模块持续运行在无故障的状态之下。

h) 过程和质量控制设计：部署必要的过程和质量控制手段，确保以上所有设计在生产过程中的正确实现。

6.4.2～6.4.8 中的每个设计过程均根据上述设计流程进行设计。

6.4.2 边界划分和边界隔离机制设计

需要在“(1)密码模块规格”中明确说明密码模块所实现的安全功能、划定密码边界。同时根据“(5)运行环境”和“(6)物理安全”的安全要求,设计出密码模块的密码边界隔离机制,有效地从物理或逻辑上将密码模块内部和外部进行区分,使得密码模块与外部的所有交互都通过密码模块接口,确保密码模块与外部的所有正常交互都通过已定义的、明确的接口来完成。

对于硬件模块,需要按照“(6)物理安全”的要求,在模块的物理边界上设计完善的物理隔离机制,硬件密码模块也可以包括软/固件组件,但由于软/固件组件完全包含在物理边界内部,因此一般不需要额外设计逻辑隔离机制。如果模块提供的物理隔离机制较弱,仅能满足“(6)物理安全”安全域的一级要求,那么则需要满足“(5)运行环境”中可修改运行环境的操作系统要求的安全一级要求,采用额外机制,例如还需配合模块内部的操作系统所提供的逻辑隔离机制,对模块的边界进行有效隔离。

对于软件模块,需要按照“(5)运行环境”中的可修改的运行环境要求,设计逻辑边界隔离机制。

对于固件模块,则需要按照“(6)物理安全”,在模块的物理边界上设计完善的物理隔离机制;若物理安全等级为一级,则还需要按照“(5)运行环境”中的可修改的运行环境要求,设计逻辑边界隔离机制。

对于混合软件模块,它的硬件组件和软件组件的边界是分离的,即软件组件不包含在硬件组件的物理边界内部;因此需要针对硬件组件和软件组件分别设计边界隔离机制。

对于混合固件模块,它的硬件组件和固件组件的边界是分离的,即固件组件不包含在硬件组件的物理边界内部;因此需要针对硬件组件和固件组件分别设计边界隔离机制。

6.4.3 接口设计

“(2)密码模块接口”规定了在边界上的、所有的各种不同类型的输入/输出接口,由此来实现密码模块核准的安全功能。接口设计的原则包括:

——密码模块与外部的所有正常交互都通过接口来完成;

——接口可以是物理端口和/或逻辑接口;

——接口是有限的,密码模块需要声明所有的物理端口和逻辑接口,并根据“(2)密码模块接口”的要求设计接口,同时关闭所有不必要的接口。

6.4.4 角色、服务和鉴别设计

“(3)角色、服务和鉴别”是对正常接口所提供的安全功能的使用控制,阻止外部对安全功能的非授权访问。角色、服务和鉴别的安全要求,是对通过接口提供的密码服务的使用控制,只有当接口是有限且明确时,才能够保证鉴别机制不会被绕过。

在设计角色时,需要根据密码模块自身的安全需求,设计不同的权限分配不同的角色。密码主管是必须的。角色可以是个人、进程、应用的实体。

除了安全一级外,需要为所有角色设计鉴别方式。

在设计服务时,需要考虑以下内容:

——通过哪个接口对外提供服务;

——哪个授权角色能够使用该服务;

——该服务与哪些敏感安全参数相关,以及该服务对敏感安全参数有哪些影响(敏感安全参数会通过该服务进行增加、删除或者修改)。

6.4.5 软件/固件设计

“(4)软件/固件安全”主要是为了实现密码模块内部的软件/固件的完整性保护,保证在安装前和运行前,密码模块自身功能没有被恶意修改或替换。

“(9)自测试”主要是确保密码模块自身功能没有发生故障，是一项运行前和运行时的安全措施。

“(4)软件/固件安全”和“(9)自测试”分别从安装部署、运行前、运行时的角度，确保密码模块实现的安全功能源自于密码模块的设计者，且不会失效或被修改。

6.4.6 敏感安全参数管理设计

“(8)敏感安全参数管理”主要是保护用于安全功能的密钥、随机数以及其他敏感安全参数在生成、建立、存储、置零和输入/输出过程中的安全，避免非授权的访问、使用、泄露、修改和替换。

在设计时，需要逐个列出所有的敏感安全参数，并从生成开始、直到置零，详细梳理敏感安全参数的状态和保护措施，并与“(8)敏感安全参数管理”进行对照，确保满足相关的要求。

6.4.7 非入侵式安全/其他攻击缓解设计

“(7)非入侵式安全”考虑了攻击者从正常接口或者在边界之外收集可利用信息、分析获得密钥、随机数，以及其他关键安全参数的侧信道攻击。

“(11)对其他攻击的缓解”，是对 GM/T 0028—2024 未考虑到、未来可能出现的新型攻击的缓解手段。

6.4.8 过程和质量控制设计

“(10)生命周期保障”规定了密码模块全生命周期保障的相关内容，涉及过程控制和质量控制，保证密码模块在设计、开发、测试、配送、操作的全生命周期内与目标方案的一致性，以满足预期的安全要求。

7 密码模块规格

7.1 用作接口的部件与密码边界的关系

7.1.1 相关安全条款

当对硬件密码模块的密码边界划界时，根据 GM/T 0028—2024 中 7.2.3.2 的[02.15]进行安全设计。

7.1.2 设计指导

硬件密码模块的密码边界规定为硬件边线，至少包含密码模块内所有安全相关的硬件部件。“用作接口的部件”是密码模块的物理端口，这些端口是出入密码边界的入口和出口。密码模块的物理端口形式多样，从简单的引脚或接插件，到具有 IC、实现复杂计算功能的装置或设备(如密码键盘、指纹传感器、摄像头)，其物理结构和功能原理各不相同。在确定用作接口的部件是否划入密码边界时，考虑以下因素：

——排除该部件时，密码模块是否仍具有连续的硬件边线；

——排除该部件时，新密码边界上是否具有密码模块提供的服务所必需的出入口；

——该部件是否与密码功能相关，其实现是否会干扰或破坏密码模块的安全运行；

——排除或包含该部件时，是否与其他现行标准存在兼容性问题。

当一个部件被排除在密码边界之外时，密码模块仍具有连续的硬件边线、新密码边界上仍具有服务所需的出入口、不会影响到密码模块的安全运行，那么这个部件划在密码边界外部；否则，这个部件划入密码边界内部。

示例 1：

考虑 USB 智能密码钥匙的 USB 接口：当从密码模块中排除 USB 接口时，密码模块缺少出入密码边界的主要物理端

口；且排除 USB 接口后，向“外”暴露出的电路或引脚与智能密码钥匙外壳不构成连续的硬件边线。因此 USB 智能密码钥匙的 USB 接口划入密码边界内部。

示例 2：

考虑蓝牙 IC 卡中的蓝牙模组：当从密码模块中排除蓝牙模组时，新密码边界上缺少通过蓝牙访问密码服务所需的出入口（即蓝牙通信接口）。因此，如果蓝牙 IC 卡密码模块提供了通过蓝牙访问密码功能的服务，则蓝牙模组划入密码边界内部。

示例 3：

考虑密码设备机箱外部连接的 IC 卡读卡器：当从密码模块中排除 IC 卡读卡器时，机箱外壳仍具有连续的硬件边线；新的密码边界上，仍具有访问密码服务所需的出入口；IC 卡读卡器的实现也不会影响密码设备的安全运行时，IC 卡读卡器划到密码边界外部。

7.2 密码模块的密码边界

7.2.1 相关安全条款

不同类型的密码模块，其密码边界有所差异，依据 GM/T 0028—2024 中 7.2.3.2 的[02.15]、[02.16]、[02.17]、[02.18]进行安全设计。

7.2.2 设计指导

对于密码边界的问题，按照如下进行设计：

硬件密码模块的密码边界：硬件模块包含物理硬件及必要的固件、操作系统和软件。硬件密码模块的密码边界如为产品机箱，则机箱内为密码边界内，所以设备内的主板、CPU、内存条、电源、密码卡、网卡、风扇、网口、串口、VGA 接口、USB 接口和其他外设接口均在密码边界内。硬件模块密码边界为硬件边线。

软件密码模块的密码边界：软件密码模块运行在可修改的运行环境中（硬件平台和操作系统），密码边界就是密码模块的软件实现本身，由一个或若干个软件部件组成。软件密码模块运行在具体的硬件平台和操作系统上，但具体的硬件平台和操作系统都不包括在软件密码模块的密码边界之内。

固件密码模块的密码边界：固件密码模块运行在不可修改或受限的运行环境中（硬件平台和操作系统），密码边界就是固件本身。固件密码模块与具体的硬件平台和操作系统绑定，但具体的硬件平台和操作系统都不包括在固件密码模块的密码边界之内。

混合密码模块包含硬件以及与硬件分离的软件或固件，当实现形式为分离的硬件和软件组件时，定义为混合软件密码模块；当实现形式为分离的硬件和固件组件时，定义为混合固件密码模块。

一种典型的混合密码模块是软件部件及为软件部件提供密码运算的密码卡所构成的密码模块，其中密码卡执行核心的密码计算，而配套软件调用密码卡，两者共同完成安全功能，且硬件和软件的边界是分离的。密码卡和其内部运行的固件不是混合密码模块，因为密码卡的边界内包括了内部固件，两者的边界不是分离的。

任何一种类型的模块都有物理边界、逻辑边界的概念，具体为：

——对于硬件密码模块，物理边界、逻辑边界和密码边界一般是重合的；

——对于固件密码模块，逻辑边界和密码边界一般是重合的；固件密码模块的物理边界是所绑定的硬件平台所构成的边线，对于固件密码模块，“物理安全”安全域是适用的，主要检查的是对应物理边界的物理安全机制；

——对于软件密码模块，逻辑边界和密码边界一般是重合的；软件密码模块的物理边界是所在的硬件平台所构成的边线，对于软件密码模块，“物理安全”安全域是可选的，主要检查的是对应物理边界的物理安全机制；

——对于混合密码模块，其硬件组件的物理边界、逻辑边界和密码边界一般是重合的；其软/固件组

件的逻辑边界和密码边界一般是重合的，其软/固件组件的物理边界是所在的硬件平台所构成的边线。

密码模块边界信息的梳理见附录 A。

7.3 密码模块名称和版本标识

7.3.1 相关安全条款

密码模块的名称和版本标识依据 GM/T 0028—2024 中 7.2.3.1 的[02.11]、[02.12]进行安全设计。

7.3.2 设计指导

密码模块的名称和密码边界相匹配。

商用密码产品认证目录中规定了若干产品种类及其适用的标准，宜在能够匹配的情况下尽可能让产品名称包含对应的产品类别，尽可能根据产品的特性增加关键性的描述，例如：密码机的名称宜明确为“服务器密码机”，可在密码模块名称中增加公司标识性名称，例如“* *公司（公司名简称）服务器密码机”，若命名为“可信服务器密码机”，“可信”一词与可信计算产生关联，其超出了服务器密码机界定的范围，则不适用。

密码模块的版本标识为每个密码模块元素的特定版本控制信息。版本数字宜包含足够级别，更新/升级/更改宜反映在新版本中。例如，如果发布版本是 1.0、1.1 和 1.2，版本 1 则包含不够充足的内容信息。版本号也可以包含字母，例如，1.0a、1.0b 和 1.0c。版本号宜分段，并明确每个分段的含义。

7.4 “核准的过程”的确定和梳理

7.4.1 相关安全条款

密码模块核准的过程依据 GM/T 0028—2024 中 7.2.1 的[02.01]、7.2.4.1 的[02.20]进行安全设计。

7.4.2 设计指导

核准的密码算法、安全功能或过程是视为密码模块的基本组成单元。GM/T 0028—2024 的附录 C 规定了核准的密码算法和安全功能；设计者宜按照以下原则梳理密码模块所涉及的“过程”，确保其是“核准的”。

核准的过程指的是，二个或以上的核准的安全功能按照一定的规则组合执行所形成的序列，该序列中的安全功能之间可以穿插非安全功能的执行序列或操作员的操作序列。

核准的过程可能包括以下三种情况。

——核准的过程完全由密码模块的核准安全功能组合形成。例如，在执行对数据同时进行机密性和完整性保护时，首先调用安全功能“分组密码”进行数据加密，然后调用安全功能“消息鉴别码”进行数据完整性保护，连续调用这两个安全功能所完成的序列被视为“数据保护”过程。

——核准的过程包括了非安全功能的执行序列，例如动态口令过程中需要对时间因子、事件因子、挑战因子进行操作和计算，还需要进行截位和取模计算，这些执行序列不属于安全功能，但是作为核准的过程的一部分。

——核准的过程包括了操作员的操作序列，例如进行密钥协商过程时，其中需要操作员（可能是人或进程）对密码模块进行多次调用；又例如，在使用按键型智能密码钥匙进行签名操作前，需要操作员通过物理实体按键进行确认。以上操作员的这些执行序列可以作为核准的过程的一部分。

对于包括非安全功能的执行序列和操作员的操作序列的过程，密码模块厂商通过给出相应的证据说明这些序列不会影响该过程中其他核准安全功能的安全性。核准的过程不包括非核准的安全功能。

7.5 工作模式

7.5.1 相关安全条款

密码模块的工作模式依据 GM/T 0028—2024 中 7.2.4.1 的[02.19]、[02.20]和 7.2.4.2 的[02.23]进行安全设计。

7.5.2 设计指导

密码模块支持的工作模式宜按照下面的设计指导进行设计。

密码模块工作时所能执行的服务、操作或功能，对外都称作服务；每个服务输入产生一个服务输出。“工作模式”则定义为这样一组服务的集合。

首先，安全策略中宜描述密码模块支持的所有服务。依据具体的归类方法，从密码模块支持的所有服务的集合中，构造不同的子集作为不同的工作模式。特殊的，如果某个子集中不包含任何安全相关的服务、或安全相关的服务使用了非核准的安全功能，这一类子集统称为“非核准的工作模式”。

当一个子集中至少有一个安全相关的服务且所有安全相关的服务只使用核准的安全功能时，这个子集就定义为一个“核准的工作模式”。从密码模块支持的所有服务的合集中构造子集的方法，由密码模块的设计者定义。通常根据密码模块的生命周期、可配置的工作模式、可适用的业务场景这些维度进行归纳，为密码模块定义一个或多个核准的工作模式。密码模块至少具有一个核准的工作模式。

密码模块通过给出相应的状态指示来区分核准的和非核准的工作模式；且核准的和非核准的工作模式下，关键安全参数相互分离。密码模块不宜具有非核准的工作模式。

7.6 密码模块状态指示方式的建议

7.6.1 相关安全条款

密码模块状态指示依据 GM/T 0028—2024 中 7.2.4.2 的[02.24]进行安全设计。

7.6.2 设计指导

密码模块在核准的工作模式下的服务过程可能涉及多种状态指示，常见的状态指示方式列举如下。

通过不同的状态指示方式区分核准的工作模式和非核准的工作模式，状态指示方式可通过状态指示灯或报文状态字呈现。

示例 1：

硬件密码模块通过物理指示灯反应不同的状态。当密码模块工作在核准的工作模式时，亮绿灯；当密码模块工作在非核准的工作模式时，亮蓝灯；当密码模块工作在错误状态时，亮红灯。

示例 2：

软件密码模块所提供的安全功能以 API 函数方式对外服务，每个 API 函数返回结果都能指示调用服务是否成功，以状态字或输出参数的方式反馈具体的状态信息。

7.7 混合密码模块的密码边界和物理边线

7.7.1 相关安全条款

混合密码模块的密码边界依据 GM/T 0028—2024 中 7.2.3.2 的[02.18]进行安全设计。

7.7.2 设计指导

混合密码模块的密码边界和物理边线具有其特殊性，宜按照下面的设计指导进行设计。

混合密码模块依赖专用密码硬件（例如密码卡、密码芯片）实现密码功能，专用密码硬件是其组成的

一部分。

混合密码模块的密码边界内，至少包含硬件部件和位于硬件部件物理边线之外的软件或固件部件。混合密码模块中分离的两部分处于同一个运行环境中，或分别处于不同的运行环境中。

通常，混合密码模块对外提供的密码服务主要通过软件或固件的逻辑接口实现，硬件部件只与密码模块的软件或固件交换敏感安全参数和控制信息。

示例：

计算机中运行的密码软件配合计算机主板上连接的密码卡，构成混合软件密码模块。密码模块中的硬件部件是密码卡，软件部件是运行在操作系统中的密码软件，它们同处于以计算机机箱为物理边线的运行环境中。

7.8 混合密码模块内部部件之间的通信

7.8.1 相关安全条款

混合密码模块内部部件之间的通信依据 GM/T 0028—2024 中 7.2.3.2 的[02.18]、7.9.5 的[09.15]、[09.21]进行安全设计。

7.8.2 设计指导

在混合密码模块内部，分离的部件之间进行通信时，宜按照下面的设计指导进行设计。

混合密码模块的密码边界由软件或固件部件与分离的硬件部件这两个不相交的部分构成，其中每个部件的端口和接口都是密码边界上的出入口。混合密码模块中的这两部分之间互相通信时，信息要经历从密码模块物理边界内部到外部，再进入密码模块物理边界内部的过程。

在混合密码模块内部，软件或固件部件与分离的硬件部件之间若涉及交换敏感安全参数时，需要同时满足密码模块内部对敏感安全参数的保护要求，以及对敏感安全参数的输入和输出的安全要求。

例如，混合软件密码模块的软件部件如果向其硬件部件传输敏感安全参数，敏感安全参数从软件部件的密码模块物理边界内部到外部的过程，视作敏感安全参数的输出；敏感安全参数从硬件部件的密码模块物理边界外部进入内部的过程，视作敏感安全参数的输入。

8 密码模块接口

8.1 可信信道

8.1.1 相关安全条款

密码模块的可信信道依据 GM/T 0028—2024 中 7.3.4 的[03.16]、[03.17]、[03.18]、[03.19]进行安全设计。

8.1.2 设计指导

当三级及以上的密码模块输入或输出明文密钥分量、鉴别数据以及其他关键安全参数时，采用可信信道传输。如果密码模块的输入输出不包括未受保护的敏感信息，不必使用可信信道。可信信道一般用于无法使用密码技术进行安全保护的情况。

可信信道使用密码模块定义的输入或输出端口，通过物理隔离或逻辑隔离的方式，防止在通信链路上的非授权修改、替换和泄露。

物理隔离即可信信道使用的接口是独占的，在这种情况下，需要说明如何保证该信道的物理独占性。比如，密码机专门使用了一个 IC 卡读卡器接口用于密钥分量的导入，该物理端口不用于其他用途。

逻辑隔离即可信信道使用的物理端口可以不是独占的。在这种情况下，需要说明该逻辑接口如何保证在执行可信信道功能时的物理独占性。比如，密码机为某个物理端口配备了专门的可信信道开关，

开关开启时，该物理端口专门用于密钥明文分量的导入，开关关闭时，该物理端口可用于其他用途，但不再用于密钥分量的导入。

8.2 常用的物理端口与逻辑接口的关系

8.2.1 相关安全条款

密码模块的接口依据 GM/T 0028—2024 中 7.3.3 的[03.04]、[03.05]、[03.06]、[03.07]、[03.08]、[03.09]、[03.10]、[03.11]进行安全设计。

8.2.2 设计指导

常用的逻辑接口总共分为五大类，包括数据输入接口、数据输出接口、控制输入接口、控制输出接口、状态输出接口。

常用的物理端口有网口、USB 接口、开关、按钮、键盘、VGA 接口、状态显示灯、蜂鸣器和其他外设接口。

物理端口承载逻辑接口，多个逻辑接口可以复用一个物理端口，例如网口作为物理端口可承载数据输入、数据输出、控制输入、控制输出、状态输出逻辑接口功能。

8.3 逻辑接口相互隔离的建议

8.3.1 相关安全条款

密码模块的逻辑接口依据 GM/T 0028—2024 中 7.3.1 的[03.02]、7.3.3 的[03.14]进行安全设计。

8.3.2 设计指导

当数据、控制和状态信息的输入输出共享一个物理端口时，应用程序接口可以设计为通过不同的接口函数传输数据、控制和状态信息。当需要在同一个接口函数中传输数据、控制和状态信息时，使用不同的参数字段以及返回值来对数据、控制和状态信息进行区分。

示例 1：

GM/T 0016 中，获取智能密码钥匙设备状态接口定义如下：

ULONG DEVAPI SKF_GetDevState(LPSTR szDevName,ULONG * pulDevState)

其中，函数名 SKF_GetDevState 为控制输入信息；参数 szDevName 是设备名称，是数据输入信息；参数 pulDevState 返回设备状态，是数据输出信息；函数的返回值是成功或失败，属于状态输出信息。

示例 2：

GM/T 0016 中，智能密码钥匙生成 ECC 签名密钥对接口定义如下：

ULONG DEVAPI SKF_GenECCKeyPair (HCONTAINER hContainer,ULONG ulAlgId,ECCPUBLICKEYBLOB * pBlob)

其中，函数名 SKF_GenECCKeyPair 是控制输入信息；参数 hContainer 是密钥容器句柄，参数 ulAlgId 是算法标识，都属于数据输入信息；参数 pBlob 返回 ECC 公钥数据结构，是数据输出信息；函数的返回值是成功或失败，是状态输出信息。

8.4 输入设备作为物理端口时的接口描述方式

8.4.1 相关安全条款

密码模块的输入设备作为物理端口时接口依据 GM/T 0028—2024 中 7.2.2 的[02.03]进行安全设计。

8.4.2 设计指导

所有进出密码模块的逻辑信息流，都通过已定义的物理端口和逻辑接口传输，这些端口和接口是出入模块密码边界的入口和出口。密码模块逻辑接口是相互分离的，这些逻辑接口可以共享一个物理端口，或者逻辑接口也可以分布在一个或多个物理端口上。输入装置（例如 POS 密码应用系统的键盘）可以作为物理端口。如果该输入装置在密码边界内部，在描述密码产品的密码模块规格时，至少将一种逻辑接口映射到该输入装置。如果支持数据输入，则映射为数据输入接口；如果还支持控制信息触发，还可以映射为控制输入接口。

除此之外，如果使用可插拔的外设作为输入设备（例如 USB 接口的读卡器），在描述密码产品的密码模块规格时，可将与之相连的接口（例如 USB 接口）描述为密码模块的物理端口，将可插拔的输入设备排除在硬件边线范围之外。相应地，根据产品的实际情况和 GM/T 0028—2024 的要求设计物理端口与逻辑接口的映射关系。

8.5 软件密码模块的物理端口

8.5.1 相关安全条款

软件密码模块的物理端口依据 GM/T 0028—2024 中 7.3.1 的[03.01]进行安全设计。

8.5.2 设计指导

软件密码模块的物理端口可不予说明。

9 角色、服务和鉴别

9.1 对新角色的验证

9.1.1 相关安全条款

对新角色的验证依据 GM/T 0028—2024 中 7.4.1 的[04.01]、7.4.4 的[04.40]、[04.44]、[04.58]进行安全设计。

9.1.2 设计指导

安全一级密码模块可不支持鉴别；安全二级及以上的密码模块如果允许操作员变换角色，针对请求的新角色，根据密码模块支持的鉴别机制不同，宜按照下面的设计指导进行设计。

如果允许操作员担任多个角色，那么操作员不在同一时间担任多个角色，且担任新角色时不再担任原角色。

如果安全一级密码模块不支持鉴别机制，操作员隐式或显式地选择一个或多个角色；密码模块可不执行对角色的鉴别，但需要验证操作员能否担任该角色。例如，当密码模块未执行密码初始化时，操作员能请求担任密码主管角色，但不能担任用户角色。

密码模块执行基于角色的鉴别，如果请求的新角色之前未被鉴别则每个请求的新角色都需要被鉴别，且密码模块需要验证操作员能否担任该角色。

密码模块执行基于身份的鉴别，在操作员通过身份鉴别后，如果请求的新角色之前未被授权则对每个请求的新角色，密码模块需要验证经标识的操作员是否被授权担任该新角色，还需验证该操作员能否担任该新角色。

9.2 无默认鉴别数据时的第一次访问鉴别

9.2.1 相关安全条款

无默认鉴别数据时的第一次访问鉴别依据 GM/T 0028—2024 中 7.4.4 的[04.47]进行安全设计。

9.2.2 设计指导

第一次访问密码模块，是指密码模块每种角色的第一次访问。例如：密码模块出厂时只有管理员，管理员第一次访问密码模块时称为第一次访问；管理员创建了操作员和审计员，操作员和审计员第一次访问密码模块时也称为第一次访问。

第一次访问密码模块时，如果密码模块不包含鉴别数据，则需要操作员对密码模块进行初始化，初始化时产生鉴别数据，并通过鉴别数据对角色进行鉴别。例如：密码模块配送给操作员后，由操作员执行初始化操作并赋予第一次访问的操作员权限；或，密码模块出厂时未设置任何角色，操作员对密码模块初始化时创建管理员角色并设置其初始鉴别数据；或，密码模块出厂时预置了角色和默认鉴别数据。

9.3 鉴别数据的隐藏方法

9.3.1 相关安全条款

鉴别数据的隐藏依据 GM/T 0028—2024 中 7.4.4 的[04.56]进行安全设计。

9.3.2 设计指导

隐藏鉴别数据反馈信息，例如在操作员输入用户口令时，在终端屏幕上不显示所输入的敏感字符。常用的隐藏方式为以回码的形式进行隐藏，例如所有的输入数据以“*”的形式进行显示。

9.4 无需担任授权角色的情况

9.4.1 相关安全条款

无需担任授权角色的情况依据 GM/T 0028—2024 中 7.4.1 的描述进行安全设计。

9.4.2 设计指导

根据密码模块的安全级别不同，某些安全服务不需要操作员担任授权角色，具体按照下面的设计指导进行设计。

对于安全一级，不要求密码模块采用鉴别机制以控制对密码模块的访问，因此安全服务并不需要操作员担任任何授权角色。对于密码模块的访问，操作员隐式或显式地选择一个或多个角色即可。

对于安全等级为二级或以上，在核准的工作模式中，操作员为了获取核准的安全功能组成的所有服务，需要通过鉴别机制担任一个授权角色，除了以下安全服务的情形：

——在 GM/T 0028—2024 的 C.2.5 中指定的杂凑函数服务；

——随机数生成服务；

——数字签名验证服务，例如在 GM/T 0028—2024 附录 C 中指定的“SM2 椭圆曲线公钥密码算法”中的验签服务；

——对操作员的鉴别过程和/或设置操作员的鉴别数据的初始化过程；

——显示状态、自测试或其他符合下面 a)中例外情况的不影响模块声明的安全性的服务。

针对无需担任授权角色的情况。

a) 所述情形例外的原因是：

所涉及的算法和服务不会访问、创建、修改、泄露或替换该模块的关键安全参数；
所涉及的算法和服务不影响模块的安全性或受模块保护的信息的安全性。

b) GM/T 0028—2024 中 7.4 讨论了授权角色。授权角色是指任何已定义的角色。操作员被授权担任该角色之前，一些已定义的角色可能需要操作员根据鉴别机制进行鉴别。

c) 执行任何服务都需要操作员担任一个角色，GM/T 0028—2024 中 7.4.1 声明了一些角色没有经过鉴别的情形。GM/T 0028—2024 中 7.4.1 声明操作员不需要担任授权角色来完成某些服务，这意味着虽然模块可能被认证为安全等级为二级或以上，但是定义的角色仍然可能不需要操作员对角色进行鉴别来执行这些服务。

d) 请注意将随机数生成服务例外的原因是：一个核准的随机数生成服务能够被未授权的角色调用，甚至能够被非核准的服务中的角色调用。随机数生成服务的每一次调用都可能导致对该随机数生成器的秘密状态参数这一关键安全参数的修改。这种对关键安全参数的间接修改是允许的，因为它不会导致关键安全参数的弱化或者泄露。

e) 按照 GM/T 0028—2024 中 7.9.7 的要求执行所有未受保护的密钥和关键安全参数的置零，不被视为对这些参数的修改，因此相应的置零服务能够被未经授权的角色调用。

f) 对于可以更新模块代码并且仅使用上述例外的加密算法的服务，仍然需要对操作员进行鉴别（安全二级以上）。在模块中加载和运行新的或附加的代码，即使代码已经通过了所需的加载测试，也会带来安全隐患。提供此类能力的服务不是例外的情况。

g) 在鉴别操作员为授权角色之前，模块可以建立用于保护与操作员数据交换的安全连接（例如，使用核准的安全功能的 TLS）。在这种情况下，当身份验证数据发送到模块时，它将受到安全连接的保护。为保护身份验证数据和其他传输中的数据而建立安全连接可被视为“对操作员的鉴别过程”。在执行此类程序之前，不需要对操作员角色进行鉴别。当模块未对操作员角色进行鉴别的情况下建立安全连接，并声明为安全二级以上时，在执行任何需要身份鉴别的服务之前，模块应使用在同一安全连接下接收的身份验证数据对操作员进行鉴别。

9.5 多重操作者鉴别

9.5.1 相关安全条款

多重操作者鉴别依据 GM/T 0028—2024 中 7.4.2 的[04.04]、[04.05]、[04.06]、7.4.4 的[04.38]、[04.39]、[04.40]、[04.41]、[04.42]、[04.43]、[04.44]进行安全设计。

9.5.2 设计指导

如果既支持基于角色的鉴别机制又支持基于身份的鉴别机制（例如密码主管使用基于角色的鉴别机制，用户使用基于身份的鉴别机制），不满足安全三级的要求。原因在于 GM/T 0028—2024 中 7.4.4 明确要求安全三级的密码模块需要采用基于身份的鉴别机制，而未明确规定可使用其他的鉴别机制。这种设计满足安全二级的要求。

9.6 旁路能力

9.6.1 相关安全条款

旁路能力依据 GM/T 0028—2024 中 7.4.3.2 的[04.18]进行安全设计。

9.6.2 设计指导

旁路能力是可选的。旁路能力通常是为了业务需求而设置的独特功能：当使用密码模块的部分业务的通信对端不需要密码功能时，例如通信报文的目标地址是互联网或是尚未部署密码模块的局域网，

为保障业务系统的正常运行而激活启用密码模块的旁路功能，即原本会被加密/解密或签名/验证的数据，在符合特定条件时不再经过密码运算而被直接输出。GM/T 0028—2024 中 7.9.5 对敏感安全参数的输入和输出的要求仍适用。

旁路能力多见于通信安全的密码模块，例如 VPN，配置加密传输的隧道为密通，配置访问互联网的通道为明通。

密码模块内为每个通信通道设置单独的旁路开启/关闭的标记。激活指定通道的旁路能力后，对于经过本通道的数据或报文，直接透传转发。

9.7 激活旁路能力

9.7.1 相关安全条款

旁路能力的激活依据 GM/T 0028—2024 中 7.4.3.2 的[04.20]、[04.21]、[04.22]进行安全设计。

9.7.2 设计指导

两个独立的内部操作，指密码模块的操作员需要执行的两个不同的管理动作，例如管理终端上执行的管理命令、管理界面上的操作点击、密码模块实体上拨动某个开关/按钮。

通过执行一个管理动作，触发密码模块内的一个控制标记。当两个不同的标记均被触发，密码模块激活旁路能力，对于业务数据/报文不再经过密码运算，直接输出原文。

9.8 鉴别机制的强度

9.8.1 相关安全条款

鉴别机制的强度依据 GM/T 0028—2024 中 7.4.4 的[04.51]、[04.52]进行安全设计。

9.8.2 设计指导

鉴别机制的强度，可视为破解鉴别数据的成功概率。

密码模块使用动态令牌等设备进行操作员鉴别时，鉴别机制的强度等同于动态令牌等设备提供的用于鉴别的密码算法的安全强度，如 SM4 算法、SM2 算法的鉴别强度为 128 位。SM4 算法遵守 GB/T 32905 的规定，SM2 算法遵守 GB/T 32918、GB/T 35276 的规定。

密码模块使用所拥有的信息或个人生物特征进行操作员鉴别时(包括但不限于：口令、PIN 码、安全问题、指纹、虹膜)，对于每次核准鉴别机制的尝试使用，单次尝试的成功概率不大于百万分之一($1/10^6$)；1 min 之内多次尝试的成功概率不大于十万分之一。例如，对于 8 个数字的口令，可能的口令个数为 10^8 个，则单次猜中口令的概率为 $1/10^8$，不大于百万分之一；若密码模块设定了连续认证失败 6 次锁定账号 1 min，则 1 min 之内的最大尝试次数为 6 次，则 1 min 之内多次尝试的成功概率为 $6\times(1/10^8)$，不大于十万分之一。

9.9 密码主管角色确定

9.9.1 相关安全条款

密码主管角色的确定依据 GM/T 0028—2024 中 7.4.2 的[04.04]、[04.05]、[04.06]、7.4.4 的描述进行安全设计。

9.9.2 设计指导

有的密码产品在使用时不进行身份鉴别，可将密码产品生命周期中初始化阶段执行密码初始化(例

如写入敏感安全参数初值)的角色声明为密码主管。

9.10 软件密码模块的鉴别机制

9.10.1 相关安全条款

软件密码模块的鉴别机制依据 GM/T 0028—2024 中 7.4.4 的[04.55]进行安全设计。

9.10.2 设计指导

二级软件密码模块可能依赖操作系统的鉴别机制来实现对模块的访问控制。

二级密码模块需要支持基于角色或基于身份的鉴别机制来鉴别访问模块的操作员,并验证操作员角色及执行权限。对于二级软件密码模块,可借助运行该模块的操作系统实现的鉴别机制来达成操作员的访问鉴别与访问控制。操作系统实现的鉴别机制可不在软件密码模块的边界内,但是在进行检测时,仍需要对鉴别机制进行检测以确保其符合 GM/T 0028—2024 中 7.4.4 的要求。

操作系统的鉴别机制需要满足以下原则:

a) 实现的鉴别机制,符合 GM/T 0028—2024 中 7.4.4 的要求;

b) 基于角色的权限管理和访问控制机制;

c) 正确的权限配置,以防止非授权执行、读取、修改软件部件和敏感安全参数。

10 软件/固件安全

10.1 确保软件/固件在安装前未被修改

10.1.1 相关安全条款

依据 GM/T 0028—2024 中 7.11.7 的[05.04],确保软件/固件在安装前未被修改。

10.1.2 设计指导

为确保软件/固件在安装前未被修改,宜按照下面的设计指导进行设计。

对于密码模块的软件/固件部件,在安装之前先验证软件/固件程序的完整性。密码模块的安全策略宜明确说明在安装软件/固件前,验证软件/固件程序的完整性所需的步骤。

例如,在密码模块生产过程中,向密码模块安装软件/固件程序前,可先用生产工具计算待安装的软件/固件程序的杂凑值、消息鉴别码或签名值,用软件/固件发行商提供的完整性校验数据进行验证,验证通过后执行安装。安装过程中,可向密码模块写入上述完整性校验数据,用于密码模块执行软件/固件的运行前完整性自测试。

10.2 软件密码模块的完整性校验

10.2.1 相关安全条款

软件密码模块的完整性校验依据 GM/T 0028—2024 中 7.5 的[05.04]、[05.05]进行安全设计。

10.2.2 设计指导

软件密码模块的边界包括:

——构成密码模块的可执行文件或文件集;

——保存在内存中并由一个或多个处理器执行的密码模块的实例。

软件密码模块的完整性校验包括如下两部分内容。

——安装前完整性校验：软件密码模块的厂商宜设计完善的技术手段或过程控制措施，以保护软件密码模块在安装过程不被恶意篡改，比如操作员在安装之前手动对代码签名值进行验证后再进行安装，该完整性校验的实施主体一般不是密码模块，而是其他实体。当运行环境未提供API接口供软件部件的运行实例读取系统存储中自身程序镜像的数据时，密码模块的软件部件不能验证自身的完整性，则能够选择采用过程控制的方式。

——运行前完整性测试：软件密码模块在运行前（即加载到内存），对存储在非易失性存储器中的所有可执行文件或文件集进行完整性校验，防止软件密码模块由于意外出现错误或故障（比如存储软件密码模块的存储器发生比特翻转）。与安装前完整性校验不同，运行前完整性测试不以抵抗恶意篡改为目标。密码模块的运行前和条件自测试用于确保模块没有出现故障，模块故障可能会妨碍模块正确运行。运行前完整性测试需要由密码模块自身控制并独立判定结果，即该完整性校验的实施主体是密码模块自身，而不是其他实体。

对于安装前完整性校验，除了依赖过程控制措施外，还能够通过其他核准的密码模块对软件完整性进行验证。

对于运行前完整性校验，能够通过自身进行完整性校验，或者由自身调用其他核准的密码模块提供的完整性技术（如杂凑函数、消息鉴别码或数字签名）进行完整性校验。无论哪种方式，都需要由密码模块自身决定是通过还是失败。对于当运行环境未提供API接口供软件密码模块的运行实例读取系统存储中自身程序镜像的数据时（例如：JavaCard Applet运行实例无法读取CAP文件内容，由JavaCard系统验证CAP文件完整性），软件密码模块不能直接验证自身的完整性，这时软件密码模块能够通过调用运行环境中的核准的完整性技术对软件完整性进行验证，或对加载到内存中的相应代码、数据和段进行运行时完整性验证；这种情况下，软件密码模块与运行环境的安全机制是绑定的，即，软件密码模块只有在该运行环境下才能完成完整性校验。

该设计指导不仅适用于软件密码模块，也适用于各类密码模块的软件部分。

11 运行环境

11.1 对运行环境配置的规定

11.1.1 相关安全条款

运行环境配置依据GM/T 0028—2024中7.6.3的[06.06]、[06.07]进行安全设计。

11.1.2 设计指导

密码模块运行环境的软件、固件、主控固件的加载、更新均需要通过相应的校验。

运行环境提供了密码模块（特别是软件密码模块）运行的基本条件，提供了进程隔离和访问控制的逻辑隔离机制和审计机制。运行环境往往不在密码模块的边界内（即密码模块厂商无法直接控制），但是由于其提供了密码模块非常底层的安全机制保障，因此需要在密码模块配套的安全策略文档中描述对运行环境的配置，并需要密码模块在安装后由相应人员（如密码主管）按照安全策略文档对运行环境进行配置。未按照安全策略文档对运行环境进行配置，则认为密码模块无法达到相应的安全等级。需要注意的是，对于运行环境进行配置的责任者是密码模块的使用者，而不是厂商；厂商的主要责任是给出合适的安全策略文档。

常见的运行环境配置包括：在操作系统上增加特定的用户或用户组，为操作系统用户设定足够长的口令，开启或关闭特定的系统服务。

11.2 硬件密码模块的运行环境

11.2.1 相关安全条款

硬件密码模块的运行环境依据 GM/T 0028—2024 中 7.6.2 的[06.04]进行安全设计。

11.2.2 设计指导

硬件密码模块中如果包含操作系统，宜按照下面的设计指导进行设计。

硬件密码模块的密码边界规定为硬件边线，其中可包含固件和/或软件。硬件密码模块受物理安全提供的物理隔离机制保护，即硬件密码边界内包含的操作系统是不可修改或受限制的运行环境。

在密码模块的物理安全强度较低的情况下(密码模块在物理安全中仅达到了安全一级)，仍需要硬件密码模块内部的操作系统提供必要的逻辑隔离机制，相关安全要求与 GM/T 0028—2024 中 7.6.3 规定的“可修改运行环境的操作系统要求”中安全一级的要求一致。

在密码模块的物理安全强度较高的情况下(密码模块在物理安全中达到了安全二级及以上)，物理安全机制已经提供了足够的物理隔离机制保护，不再需要依赖硬件密码模块内部的操作系统提供的逻辑隔离机制，即对操作系统没有额外的要求(也不需要遵守 GM/T 0028—2024 中 7.6.3 规定的安全一级的要求)。

12 物理安全

12.1 密码模块物理实体的分类

12.1.1 相关安全条款

密码模块物理实体的分类依据 GM/T 0028—2024 中 7.7.1 的[07.03]、[07.04]进行安全设计。

12.1.2 设计指导

由于物理安全要求是针对三类密码模块物理实体(单芯片/多芯片嵌入式/多芯片独立式)做出规定的，所以需要理清密码模块相应部分的情况。

——以智能 IC 卡产品为例，一般为单芯片密码模块。

——以 PCI-E/PCI 密码卡产品为例，一般为多芯片嵌入式密码模块。

——以安全网关、服务器密码机产品为例，一般为多芯片独立式密码模块。

12.2 物理安全置零时间

12.2.1 相关安全条款

物理安全置零时间依据 GM/T 0028—2024 中 7.7.2 的[07.10]进行安全设计。

12.2.2 设计指导

安全三级或安全四级的模块一般会部署拆卸响应与置零电路机制。当攻击者破坏密码模块的物理防护后，攻击者需要一段时间 t_A 才能访问到密码模块中存储着明文形态的敏感安全参数的存储器(无论是易失性存储器还是非易失性存储器)。当密码模块遭遇物理入侵时，密码模块检测到入侵的时间为 t_D；在检测到入侵后，密码模块执行置零的时间为 t_R。密码模块需要保证，其检测到入侵的时间 t_D 与完成置零的时间 t_R 之和应远远小于攻击者访问到存储器的时间 t_A，即 $t_D+t_R \ll t_A$。

例如，攻击者访问到密钥所在存储器的所需时间为 t_A=10 s，那么密码模块的物理安全检测时间和完成置零指令的时间之和 t_D+t_R 应远远小于 10 s，比如 1 s。假设密码模块的物理安全检测时间 t_D 为 0.3 s，那么条款中所规定的“极短时间”至多为 0.7 s。

以下以 GM/T 0084 中所定义的五种物理攻击方式为例，给出检测到拆卸行为到置零操作的最大完成时间：

——内部探针攻击：0.01 s；

——加工技术：0.5 s；

——聚能切割技术：0.01 s；

——能量攻击技术：0.01 s；

——环境改变技术：0.5 s。

对于未部署拆卸响应与置零电路机制的模块，一般采取手动置零的方式进行物理安全置零。以上最大完成时间同样适用于由操作员手动发起的置零操作。

12.3 对维护访问接口的安全要求

12.3.1 相关安全条款

维护访问接口的安全依据 GM/T 0028—2024 中 7.7.1，7.4.2 的[04.07]，7.7.2 的[07.11]、[07.12]、[07.13]、[07.16]、[07.18]、[07.22]、[07.23]进行安全设计。

12.3.2 设计指导

维护访问接口是一种非常规的物理形态的接口。通常不供密码主管或者其他用户使用，而是供密码模块厂商所定义的维护角色使用，主要用途是在不返厂的情况下对设备进行维护。维护角色访问维护访问接口时，一般需要越过密码模块的物理边界，对密码模块内部进行操作，因此维护访问接口需要特殊的安全要求。

维护访问接口的安全要求由厂商自行定义，除了需要满足相关安全条款的要求之外，还需要设计密码模块特定的安全机制，目标是：

——只能通过维护访问接口进行维护操作；维护接口一般是物理端口，可以单独设置，也可以是密码模块的门、封盖，但密码模块需要有能力区分是正常的维护还是异常的入侵；

——只有授权的维护角色才能访问维护访问接口，其他非授权的角色访问维护访问接口将被视为物理入侵；

——维护角色对密码模块的维护不会导致关键安全参数被非授权的访问、使用、泄露、修改和替换，也不会导致公开安全参数被非授权的修改和替换；

——维护完成后，验证密码模块的完整性不被破坏。

所有厂商定义的安全要求需要在安全策略文档中进行说明。

示例：

一个安全三级的服务器密码机在网卡损坏的情况下，需要访问密码模块的维护访问接口（打开机箱外壳的封盖），进行网卡的更换。为了保证这种场景下的安全性，一种可行的机制如下：

a) 密码主管登录密码模块，备份相关的敏感安全参数；

b) 维护角色登录密码模块，将密码模块切换至（密码模块生产者定义的）维护模式；

c) 维护角色登录之后，按照安全策略要求，对密码模块进行置零操作；

d) 维护角色访问密码模块的维护访问接口（打开机箱外壳的封盖）时，模块先通过拆卸响应与置零电路置零所有未受保护的敏感安全参数；

e) 维护角色进行维护操作；

f) 完成维护后，维护角色运行自测试服务，检查密码模块是否正常工作，然后退出；

g) 密码主管重新启动密码模块，运行自测试服务，并恢复备份的敏感安全参数。

13 非入侵式安全

13.1 非入侵式攻击的主要类型以及缓解技术

13.1.1 相关安全条款

非入侵式攻击的主要类型以及缓解技术依据 GM/T 0028—2024 中 7.8 的[08.04]、[08.05]、[08.06]、[08.07]进行安全设计。

13.1.2 设计指导

非入侵式攻击是指攻击者通过测量密码设备消耗的电量、密码运算时间、泄露的电磁信号以及其他侧信道信息，试图获取密钥或关键安全参数的攻击手段。常见的非入侵式攻击包括能量分析、计时分析和电磁泄露分析，见 GM/T 0028—2024 中[08.02]。除了以上这三种攻击手段之外，均列为其他攻击方式，见 GM/T 0028—2024 中[08.01]。

GM/T 0028—2024 附录 F 规定了对非入侵式攻击和相应的缓解技术的简要描述，GM/T 0083 中规定了详细的缓解技术。针对每一种非入侵式攻击方法，都存在多种缓解技术，可以采用多种缓解技术的组合方式，以得到更好的防护效果。软件密码模块宜具备计时分析攻击的缓解措施。

每一种缓解技术都是从提高计算复杂性、攻击代价的方面，加大非入侵式攻击者的攻击难度，使得攻击者不能在可接受的时间内获得秘密参数，通过理论分析和实际测试结果，来证明采用的缓解技术能够达到有效的防护效果。非入侵式攻击的种类以及相应的缓解技术都在不断发展演变，需要根据非入侵式攻击的更新变化，使用相应的新型缓解技术。

13.2 证明缓解技术有效性的方法和测试方法

13.2.1 相关安全条款

对于证明缓解技术有效性的方法和测试方法，依据 GM/T 0028—2024 中 7.8 的[08.04]、[08.05]、[08.06]、[08.07]进行安全设计。

13.2.2 设计指导

抵抗非入侵式攻击的主要方法，是通过各种缓解技术降低计算时间、电量消耗、电磁信号以及其他侧信道信息与秘密参数之间的关联性，提高非入侵式攻击者分析、获取秘密参数的攻击难度。

证明缓解技术的有效性，包括但不限于以下方法：

a) 理论分析：通过对缓解技术的理论分析和安全性证明，阐述缓解技术的有效性，包括与缓解技术相关的、已发表并被广泛认可的学术论文、标准；

b) 代码审查：提供非入侵缓解技术相关的软件或硬件代码，对其中的缓解技术进行代码分析，检查是否按照相应的原理正确实现；

c) 实际测试结果：通过搭建实际测试环境，对不采用/采用缓解技术的密码模块进行测试，根据测试结果表明缓解技术能够有效抵抗非入侵式攻击。

GM/T 0083 规定了缓解技术的测试方法、测试策略、测试框架和测试流程的详细内容。

14 敏感安全参数管理

14.1 敏感安全参数置零的例外

14.1.1 相关安全条款

敏感安全参数的置零依据 GM/T 0028—2024 中 7.9.7 的[09.31]进行安全设计。

14.1.2 设计指导

敏感安全参数置零存在以下例外的情况：

——如果使用了默认的鉴别数据来控制对密码模块的访问，该默认的鉴别数据不需要满足置零要求，但首次访问后需要修改；

——用于核准的完整性技术的签名验证公钥或消息鉴别码的密钥可以存在于密码模块代码中，此时它们不被视为敏感安全参数，不需要满足置零要求。

14.2 置零的安全要求

14.2.1 相关安全条款

置零方法依据 GM/T 0028—2024 中 7.9.7 的[09.31]进行安全设计。

14.2.2 设计指导

置零包括手动置零和自动置零两种方法，以下情况可以选择手动置零：

——当密码模块进入维护状态时，操作员能够手动执行置零操作；

——当密码模块在结束生命周期时，操作员能够手动执行置零操作。

以下情况执行自动置零：

——不再使用的敏感安全参数，如鉴别流程中的过程值，软算法下内存中计算的中间值，自动执行置零操作；

——对于三级和四级密码模块，当密码模块在检测到拆开封盖或外壳、进行探测相关操作时，自动执行置零操作。

14.3 关于梳理敏感安全参数的建议

14.3.1 相关安全条款

敏感安全参数的梳理依据 GM/T 0028—2024 中 7.9.1 的[09.01]、[09.02]进行安全设计。

14.3.2 设计指导

在提供密码模块完整的敏感安全参数清单时，常常出现忽略或遗漏某些敏感安全参数或者遗忘敏感安全参数在生命周期的某些阶段信息的情况。可采用表格的形式列举敏感安全参数及其在不同生命周期阶段的信息。例如，基于表 2 所述的形式辅助梳理密码模块的敏感安全参数信息。

表 2　敏感安全参数辅助梳理表

生命周期	敏感安全参数 1	敏感安全参数 2	敏感安全参数 3
关键安全参数/公开安全参数	本参数为关键安全参数还是公开安全参数	—	—
功能	参数功能的概要说明	—	—
生成	何时生成 生成方式 执行权限要求	—	—
存储	存储方式 执行权限要求	—	—
导入导出	能否导入导出 采取何种机制导入导出 执行权限要求,包括密码主管、用户、维护员、任意授权者,下同	—	—
使用	使用场景 使用目的 如何使用 执行权限要求	—	—
更新	参数有效期 更新方式 执行权限要求	—	—
备份恢复	何时备份/恢复 备份/恢复方式 执行权限要求	—	—
销毁	何时销毁 销毁方式 执行权限要求	—	—

14.4　随机数生成器状态信息

14.4.1　相关安全条款

随机数生成器状态信息的保护依据 GM/T 0028—2024 中 7.9.1 的[09.04]进行安全设计。

14.4.2　设计指导

随机数生成器状态信息具体所指的内容需要符合 GM/T 0103 的规定。

14.5　置零的状态输出问题

14.5.1　相关安全条款

置零的状态输出依据 GM/T 0028—2024 中 7.9.7 的[09.36]进行安全设计。

14.5.2 设计指导

针对某些密码模块在临时敏感安全参数置零完成时并不立即输出状态指示的问题，至少需要满足下述要求。

临时敏感安全参数置零作为完整流程的一部分，在整个流程中需要提供输出状态指示，通过返回相应的状态码或输出参数指示临时敏感安全参数置零是否成功。例如，智能密码钥匙在对过程密钥置零后并没有立即输出状态指示，而是在关闭密钥句柄命令执行完成后通过返回状态码来指示过程密钥置零是否成功。

软件密码模块在对过程密钥置零后可能没有立即输出状态指示，在关闭密钥句柄函数完成后通过状态码或输出参数来指示过程密钥置零是否成功。

14.6 关于公开安全参数保护措施的建议

14.6.1 相关安全条款

公开安全参数的保护依据 GM/T 0028—2024 中 7.9.1 的[09.02]进行安全设计。

14.6.2 设计指导

首先，密码模块涉及的公开安全参数众多，需要完整地梳理密码模块中包含的公开安全参数。常见的公开安全参数包括：

——对称密码算法：初始化向量；

——公钥密码算法：加密公钥、签名公钥、ECC 算法的域参数；实际使用中公钥多以证书形式存在，此时还需要包括 CA 的根公钥证书；

——密钥派生算法：涉及基于口令的密钥派生函数的盐值、迭代轮数，基于密钥的密钥派生函数的标签、上下文附加信息；

——标识密码算法：用户标识。

其次，针对这些公开安全参数，防止其被未经授权的修改和替换的常见保护措施包括：

——访问控制：限制非授权用户修改、替换公开安全参数；

——基于消息鉴别码或数字签名的密码机制：这种机制无法避免公开安全参数被修改和替换，但需要确保这些改动能被检测出来；

——在某些特殊的场景下，如果能确保杂凑值无法被修改，也可以单纯采用杂凑算法；这种机制和前一种相同，无法避免公开安全参数被修改和替换，但需要确保这些改动能被检测出来。

14.7 关于评估敏感安全参数生成方法安全性的建议

14.7.1 相关安全条款

敏感安全参数的生成方法依据 GM/T 0028—2024 中 7.9.3 的[09.10]、[09.11]进行安全设计。

14.7.2 设计指导

首先，需要理清敏感安全参数及其对应的生成方式，例如哪些敏感安全参数是由随机数生成器生成的，哪些敏感安全参数是协商建立的。这利于有针对性地描述不同生成方式的安全性和抵抗破坏的安全强度。

常见的敏感安全参数生成方式包括：

——通过随机数生成器产生；

——通过密钥派生算法产生。

常见的敏感安全参数建立方式包括：

——通过密钥传输(分发)建立；

——通过密钥协商建立。

然后，针对不同的敏感安全参数生成方式和建立方式，分别说明此敏感安全参数生成方式的安全性。

对于常见的敏感安全参数生成方式：

——如果采用随机数发生器产生敏感安全参数，说明随机数发生器产生此敏感安全参数的安全性；
如果采用随机数生成器产生密钥分量，说明密钥分量如何保证不降低密钥的安全性；

——如果采用密钥派生算法产生敏感安全参数，说明密钥派生算法的安全性和密钥材料的安全性。

对于常见的敏感安全参数建立方式：

——如果采用密钥传输建立敏感安全参数，说明密钥传输协议的安全性和加密密钥的安全性；

——如果采用密钥协商建立的敏感安全参数，说明密钥协商协议的安全性。

15 自测试

15.1 周期自测试的需求和内容

15.1.1 相关安全条款

周期自测试依据 GM/T 0028—2024 中 7.10.3.8 的[10.52]、[10.53]进行安全设计。

15.1.2 设计指导

自测试的目的是确保密码模块的密码安全功能没有故障，周期自测试是条件自测试的一种类型，周期自测试是条件自测试执行的一种时间策略，其目的是确保密码模块在运行一个周期时间后各项功能都是正常的，能够继续提供服务。

周期自测试需求、自测试时间周期及内容按照以下原则进行设计。

对于安全一级和安全二级的密码模块，是否需要执行周期自测试取决于其应用领域的其他规范要求或者设计者自定义的安全策略，在有周期自测试需求的情况下，由操作员来做启动周期自测试，周期自测试内容包括运行前自测试和条件自测试。

对于安全三级和安全四级的安全模块，设计者需要定义时间周期来执行周期自测试，且自测试的执行不依赖于外部控制，周期自测试需执行条件自测试，若期间密码模块有上电或实例化操作，需要执行运行前自测试以及条件自测试。

对于 GM/T 0062—2018 定义的 D 类和 E 类产品执行随机数周期自检。

15.2 运行前自测试

15.2.1 相关安全条款

运行前测试依据 GM/T 0028—2024 中 7.10.2.1 的[10.14]、[10.15]进行安全设计。

15.2.2 设计指导

运行前自测试的目的是确保密码模块在进入运行状态前各项功能是正常的，因此在密码模块在上电、实例化操作之后转入运行状态之前需要触发运行前自测试。

运行前自测试包括软件/固件完整性测试、旁路测试以及关键功能测试。

运行前自测试的触发条件按照以下原则进行设计：

——硬件模块：冷启动(上电)、复位、重启操作后，需要启动运行前自测试，例如 CPU 卡通过读卡

设备对卡片进行冷复位或者热复位后，卡内系统需要执行运行前自测试；

——软件/固件模块：启动执行、加载、实例化操作后，需要启动运行前自测试；

——混合模块：混合模块的硬件部分等同于硬件模块，混合模块的固件部分等同于固件模块，混合模块的软件部分等同于软件模块。

15.3 运行前软件/固件完整性测试

15.3.1 相关安全条款

运行前软件/固件完整性测试依据 GM/T 0028—2024 中 7.10.2.2 的[10.16]、[10.17]、[10.18]、[10.19]进行安全设计。

15.3.2 设计指导

完整性测试的目的是为了保证软件、固件在使用前是没有被修改的。

对于安全一级，需要使用核准的完整性技术进行保护，例如采用杂凑函数、消息鉴别码或数字签名对软件、固件代码做计算，通过与预存的对比值进行比较来确定完整性。

对于安全二级，需要使用核准的数字签名技术或者消息鉴别码进行保护，例如计算软件、固件代码的消息鉴别码，通过与预存的对比值进行比较来确定完整性。

对于安全三级和安全四级，需要使用数字签名技术进行保护，例如采用 SM2 算法验证软件、固件的签名值来确定完整性。

对于完整性测试中所使用到的密码运算功能，需要先执行条件自测试以确保完整性测试前所使用到的密码运算功能是正常的。

密码模块的软件/固件完整性测试的对象是模块的可重写的运行代码。可变应用数据不属于运行代码，例如配置文件数据或应用数据；不可重配置存储器中在写入后不可再次更新，因此也不属于完整性测试范围，例如一次性编程或者只读存储器中的数据，而 EEPROM、FLASH 存储器中的数据是可重写，因此此类存储器中保存的运行代码属于完整性测试的范围。

15.4 运行前旁路以及旁路测试

15.4.1 相关安全条款

运行前旁路以及旁路测试依据 GM/T 0028—2024 中 7.10.2.3 的[10.20]、[10.21]进行安全设计。

15.4.2 设计指导

“旁路”的定义是与“主路”相对应的。在密码模块中，“主路”是指提供密码服务功能的主路径，“旁路”是指除主路径之外的其他路径。如果存在旁路，密码模块可能在主路和旁路进行切换，旁路可以是物理存在的，也可以是逻辑存在的。

旁路测试的目的是为了确保旁路管理逻辑的正确性以及旁路主路切换是否影响密码功服务的正确性。

安全设计阶段需要定义密码模块是否存在旁路，如果不存在旁路，明确说明该密码模块无旁路，无需做旁路测试。如果密码模块存在旁路，则需要定义存在哪些旁路以及旁路切换机制，并按照运行前旁路测试要求做相关测试。

15.5 运行前关键功能测试

15.5.1 相关安全条款

运行前关键功能测试依据 GM/T 0028—2024 中 7.10.2.4 的[10.22]、[10.23]进行安全设计。

15.5.2 设计指导

运行前关键功能测试的目的是确保密码模块在进入运行状态前所涉及到关键功能是正确的。

密码模块的安全功能包括但不限于：SM2 签名验签、SM2 加解密、SM3 密码杂凑、SM4 加解密、生成随机数。其中，SM2 遵守 GB/T 32918、GB/T 35276 的规定，SM3 遵守 GB/T 32905 的规定，SM4 遵守 GB/T 32907 的规定，随机数质量符合 GM/T 0005。

密码模块的关键功能测试主要是测试所表述的关键功能的工作状态是否正常，关键功能的功能性是否正确。

15.6 密码算法条件测试

15.6.1 相关安全条款

密码算法条件测试依据 GM/T 0028—2024 中 7.10.3.2 的[10.25]、[10.26]、[10.27]、[10.28]、[10.29]、[10.32]、[10.33]进行安全设计。

15.6.2 设计指导

密码算法条件自测试的目的是为了确保密码算法的所有密码功能在使用前是正确的。

在密码算法第一次使用之前，执行密码算法条件自测试。

对密码算法所涉及到的所有密码功能，都需要执行密码算法条件自测试。

15.7 手动输入条件自测试

15.7.1 相关安全条款

手动输入条件自测试依据 GM/T 0028—2024 中 7.10.3.5 的[10.41]、[10.42]、[10.43]、[10.44]、[10.45]进行安全设计。

15.7.2 设计指导

手动输入条件自测试的目的，是确保手动输入的敏感安全参数在密码模块使用此参数前，是与输入者的期望一致的。

敏感安全参数的内容包括：关键安全参数和公开安全参数。例如输入的口令、密钥分量都属于敏感安全参数。

手动输入的敏感安全参数的校验方法有两种：

——使用错误检测码，且错误检测码长度至少为 16 位；

——输入两次并做输入一致性的比对。

15.8 密码算法已知答案自测试

15.8.1 相关安全条款

密码算法已知答案自测试依据 GM/T 0028—2024 中 7.10.3.2 的[10.27]进行安全设计。

15.8.2 设计指导

密码算法已知答案自测试是对密码算法实现执行健康检查。在核准的工作模式下，如果适用，可以对每一个核准的密码算法进行已知答案测试。

密码算法已知答案自测试常见情形举例如下：

——对称算法：如果模块实现了加密功能，那么模块需要预置加密值，使用已知数据和密钥执行加密，然后将结果值与预置加密值进行比较；如果模块实现了解密功能，那么模块需要预置解密值，使用已知数据和密钥执行解密，然后将结果与预置解密值进行比较；

——密码杂凑算法：如果模块实现了密码杂凑功能（例如 SM3），那么模块需要预置杂凑值，使用已知数据执行密码杂凑计算，然后将结果与预置杂凑值进行比较；

——消息鉴别码：如果模块实现了消息鉴别码功能，那么模块需要执行消息鉴别码已知答案自测试。

15.9 密码算法自测试的方法

15.9.1 相关安全条款

密码算法自测试的方法依据 GM/T 0028—2024 中 7.10.3.2 的[10.27]、[10.32]、[10.33]进行安全设计。

15.9.2 设计指导

密码算法自测试的方法按照如下示例进行设计：

——已知答案测试：例如 SM3 算法自测试，对预置的数据进行 SM3 运算得到杂凑值，比对杂凑值和预置 SM3 运算的结果，如果相等，SM3 运算自检通过；否则错误。SM3 算法遵守 GB/T 32905 的规定；

——对比测试：例如 SM4 算法自测试，用相同的输入，对比两个或多个独立的密码算法实现的输出结果，输出相同则自测试成功；

——错误检测测试：例如 SM2 算法自测试，预设 SM2 密钥对和预设原文以及预设签名值，使用预设公钥、预设原文、预设签名值进行验签，验签结果为成功，改变预设签名值中的一个或多个比特位，再次验签，验签结果为失败，检测结果符合预期则认为 SM2 签名验证自测试通过。使用预设 SM2 私钥对预设原文签名得到签名值，使用预设公钥、预设原文以及签名值验签，若验签成功，则认为 SM2 签名自测试通过。

15.10 运行前模块初始化过程

15.10.1 相关安全条款

运行前模块初始化过程依据 GM/T 0028—2024 中 7.10.2.1 的[10.14]、7.3.3 的[03.07]进行安全设计。

15.10.2 设计指导

运行前模块初始化过程是指发生在模块加电之后到模块完成运行前自测试并输出状态（成功或失败，指示模块已准备好执行或不能执行密码功能服务）这段时间内的过程。

在此期间，模块可能执行一些活动，但不被视为处于核准的工作模式下。

在初始化期间，模块：

——执行所有运行前自测试，测试完成后需要通过“状态输出”接口输出结果；

——执行正确初始化或实例化模块所需的所有必要内部服务，并联合执行运行前自测试；

——可能通过控制输入接口或数据输入接口接收控制输入和数据输入（例如，可为核准的服务接收控制请求和数据，一旦初始化完成，模块就可以遵照行事）；

——不通过数据输出接口输出数据，以下情况除外：

当被请求时，允许模块输出非安全相关的模块标识信息。模块需要防止输出内部的明文密钥、

私有密钥或关键安全参数。

安全策略需要描述在初始化期间输出的信息和执行的服务。

一旦初始化完成，模块将转换成运行状态，并开始提供核准的密码功能和服务（如果运行在核准的工作模式下）。

15.11 软件/固件加载测试

15.11.1 相关安全条款

软件/固件加载测试依据 GM/T 0028—2024 中 7.10.3.4 的[10.35]、[10.36]、[10.37]、[10.38]、[10.39]、[10.40]进行安全设计。

15.11.2 设计指导

针对硬件密码模块、软件密码模块和固件密码模块，上述要求的适用情况如下：

——对于硬件密码模块，如果可以在模块定义的物理边界内加载软件或固件，则适用 GM/T 0028—2024 中 7.10.3.4 的安全要求；

——对于软件密码模块，如果可以在模块定义的逻辑边界内加载软件，则适用 GM/T 0028—2024 中 7.10.3.4 的安全要求；

——对于固件密码模块，如果可以在模块已定义的逻辑边界或物理边界内加载固件，则适用 GM/T 0028—2024 中 7.10.3.4 的安全要求。

附 录 A
（资料性）
密码模块边界信息梳理

密码边界由定义明确的边线（例如，硬件、软件或固件部件的集合）组成，该边线建立了密码模块所有部件的边界。密码边界至少包含密码模块内所有安全相关的算法、安全功能、进程和部件。准确、清晰地梳理密码边界是充分理解密码模块信息的基础。

针对如何区分密码模块边界，如何梳理密码模块边界内部的部件、安全算法、安全功能，宜按如下步骤梳理密码模块的边界详情。

步骤 1：划定密码模块的边界，并理清边界内部的所有部件。基于已经明确的密码模块类型以及表 A.1 给出的辅助信息，确定密码模块的边界和边界内部的所有部件。

表 A.1 密码模块边界和部件辅助确认表

类型	密码边界	边界内部部件
硬件密码模块	密码模块的硬件边线	可能包括： ——电路板、基板在部件之间提供互联的物理配线； ——表面贴装件； ——半集成/定制集成或通用集成的电路； ——处理器； ——内存； ——电源； ——转换器； ——其他电器元件； ——外壳、灌封或封装材料； ——连接器和接口； ——固件和/或软件； ——操作系统； ——其他部件类型
软件密码模块	由执行在可修改运行环境中的一个或多个纯软件部件划定边界。运行环境所包含的计算平台和操作系统在密码边界之外	可能包括： ——构成了密码模块的可执行文件的集合； ——密码模块的实例，保存在内存中并由处理器执行
固件密码模块	由执行在受限的或不可修改的运行环境中的纯固件部件划定边界；运行环境所包含的计算平台和操作系统在密码边界之外，但是与密码模块明确绑定	可能包括： ——构成了密码模块的可执行文件的集合； ——密码模块的实例，保存在内存中并由处理器执行
混合软件密码模块	由软件部件和分离的硬件部件划定边界；软件运行环境所包含的计算平台和操作系统在密码边界之外	可能包括： ——硬件部件； ——分离的软件、嵌入式的软件部件； ——每个部件的所有端口和接口
混合固件密码模块	由固件部件和分离的硬件部件划定边界；固件运行环境所包含的计算平台和操作系统在密码边界之外，但是与密码模块明确绑定	可能包括： ——硬件部件； ——分离的固件、嵌入式的固件部件； ——每个部件的所有端口和接口

密码模块边界内部件不仅需要确定其类型，还需要确定每种部件的功能以及具体规格，比如主板型号、机箱规格尺寸、USB 接口为 USB2.0/USB3.0 或其他类型、Linux 操作系统的内核版本号以及硬盘型号。密码模块还需确定硬件/固件/软件的版本信息。

步骤 2：列举密码模块内所有安全相关的算法、服务、过程，以及非安全相关的算法、服务、过程，宜基于表 A.2 和表 A.3 给出的辅助信息确定密码模块的安全相关的算法、服务、过程。需要将使用的密码算法与产品实现的具体服务相结合。

表 A.2　密码模块安全相关的算法、安全功能、过程的辅助确认表

算法/功能/过程	规格	功能	实施部件
分组密码算法	算法规格、密钥强度、工作模式	实现的功能	由何种部件实现此算法/功能/过程
流密码算法	—	—	—
非对称密码算法	—	—	—
杂凑函数	—	—	—
消息鉴别码	—	—	—
实体鉴别	—	—	—
密钥管理	—	—	—
随机数发生器	—	—	—
其他	—	—	—

表 A.3　密码模块非安全相关的算法、安全功能、过程的辅助确认表

算法/功能/过程	规格	功能	实施部件	对密码模块核准运行的影响
非安全相关算法 1	—	—	—	是否干扰/破坏
非安全相关过程 1	—	—	—	—
非安全相关算法 2	—	—	—	—
非安全相关过程 2	—	—	—	—
其他	—	—	—	—

步骤 3：列举密码模块内所有排除在外的硬件、软件、固件，宜基于表 A.4 给出的辅助信息确定密码模块内所有排除在外的硬件、软件、固件，并说明排除在外的原因。

表 A.4　密码模块非安全相关的算法、安全功能、过程的辅助确认表

排除在外的部件	规格	功能	排除在外的原因	对密码模块核准运行的影响
软件 1	—	—	—	是否干扰/破坏
固件 1	—	—	—	—
硬件 1	—	—	—	—
其他	—	—	—	—

步骤 4：基于以上梳理信息，并结合对密码边界的要求，进一步准确、详尽地描述边界信息。

中华人民共和国密码
行业标准
密码模块安全设计指南
GM/T 0134—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 2.5　字数 63 千字
2025年6月第1版　2025年6月第1次印刷
*
书号:155066·2-39093　定价 65.00 元

GM/T 0134-2024