ICS 35.040
L 80

中华人民共和国国家标准

GB/T 37092—2018

信息安全技术　密码模块安全要求

Information security technology—Security requirements for cryptographic modules

2018-12-28 发布　　2019-07-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国科学院数据与通信保护研究教育中心、国家密码管理局商用密码检测中心、北京握奇智能科技有限公司、北京数字认证股份有限公司、飞天诚信科技股份有限公司、北京海泰方圆科技有限公司、北京华大智宝电子系统有限公司、北京创原天地科技有限公司。

本标准主要起草人:荆继武、高能、屠晨阳、郑昉昱、江伟玉、周国良、马原、刘宗斌、刘泽艺、汪婧、罗鹏、汪雪林、陈国、詹榜华、朱鹏飞、蒋红宇、陈跃、张万涛、刘丽敏、向继。

引　言

在信息技术中，密码技术的使用需求日益增强，比如数据需要密码机制的保护以防止非授权的泄露或操控。密码机制可以用于支持实体鉴别和不可抵赖等安全服务，密码机制的安全性与可靠性直接取决于实现它们的密码模块。

本标准对密码模块提出了四个递增的、定性的安全要求等级，但不对密码模块的正确应用和安全部署进行规范。密码模块的操作员在使用或部署密码模块时，有责任确保密码模块提供的安全保护是充分的，且对信息所有者而言是可接受的，同时任何残余风险要告知信息所有者。密码模块的操作员有责任选取合适的安全等级的密码模块，使得密码模块能够满足应用的安全需求并适应所处环境的安全现状。

信息安全技术　密码模块安全要求

1　范围

本标准针对密码模块规定了安全要求，为密码模块定义了四个安全等级，并分别给出了四个安全等级的对应要求。

本标准适用于保护计算机与电信系统内敏感信息的安全系统所使用的密码模块。本标准也为密码模块的设计、开发提供指导，为密码模块安全要求的检测提供参考。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 15852(所有部分)　信息技术　安全技术　消息鉴别码

GB/T 17964　信息安全技术　分组密码算法的工作模式

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 33133.1　信息安全技术　祖冲之序列密码算法　第 1 部分：算法描述

GM/T 0001.2　祖冲之序列密码算法　第 2 部分：基于祖冲之算法的机密性算法

GM/T 0001.3　祖冲之序列密码算法　第 3 部分：基于祖冲之算法的完整性算法

GM/T 0044(所有部分)　SM9 标识密码算法

3　术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

证书　certificate

关于实体的一种数据，该数据由认证机构的私钥或秘密密钥签发，并无法伪造。

3.2

条件自测试　conditional self-test

当规定的测试条件出现时，由密码模块执行的测试。

3.3

关键安全参数　critical security parameter

与安全相关的秘密信息，这些信息被泄露或被修改后会危及密码模块的安全性。

注：关键安全参数可以是明文形式的也可以是经过加密的。

3.4

密码边界　cryptographic boundary

明确定义的边线，该边线建立了密码模块的物理和/或逻辑边界，并包括了密码模块的所有硬件、软件和/或固件部件。

3.5

密码模块　cryptographic module

实现了安全功能的硬件、软件和/或固件的集合，并且被包含在密码边界内。

注：密码模块根据其组成，可分为硬件密码模块、固件密码模块、软件密码模块以及混合密码模块。

3.6

密码模块接口　cryptographic module interface

密码模块的逻辑入口或出口，为逻辑信息流提供进出模块的通道。

3.7

密码模块安全策略　cryptographic module security policy

密码模块运行应遵从的安全规则的明确说明，其中包含了从本标准的要求导出的规则以及厂商要求的规则。

3.8

差分功耗分析　differential power analysis

对密码模块的功耗变化进行分析，并用以获取密码操作相关的信息。

3.9

故障注入　fault induction

通过应用短暂的电压、辐射、激光或时钟偏移技术，导致硬件中的操作行为发生变化的技术。

3.10

多因素鉴别　multi-factor authentication

至少具有两个独立鉴别因素的鉴别。

注：独立的鉴别因素类别包括：已知某物，拥有某物，以及具有某属性。

3.11

非入侵式攻击　non-invasive attack

一种针对密码模块的攻击，该攻击对密码边界内的部件不进行直接的物理接触，且这类攻击不会更改密码模块所处的状态。

3.12

运行环境　operational environment

密码模块安全运行所需要的所有软件、固件和硬件的集合，其中包括操作系统和硬件平台。

注：运行环境分为可修改的运行环境、受限制的运行环境以及不可修改的运行环境。

3.13

运行前自测试　pre-operational self-test

密码模块在上电或实例化（在关闭电源、重置、重启、冷启动、供电中断等之后）至转换到运行状态之间执行的测试。

3.14

公开安全参数　public security parameter

与安全性相关的公开信息，一旦被修改，会威胁到密码模块安全。

注：例如，公钥、公钥证书、自签名证书、信任锚、与计数器和内部保持的日期和时间相关联的一次性口令。公开安全参数如果不能被修改或者修改后能够被密码模块发现，此时可以认为该公开安全参数是受保护的。

3.15

运行时环境　runtime environment

一种虚拟机状态，在计算机运行时，为进程和程序提供软件服务。

注：运行时环境可能与操作系统本身，也可能与其下运行的软件有关，其主要目的在于实现“平台无关”的编程目标。

3.16

安全功能　security function

密码算法及其工作模式，包括：分组密码、序列密码、非对称密码、消息鉴别码、杂凑函数、随机数生成、实体鉴别和敏感安全参数生成和建立等。

3.17

敏感安全参数　sensitive security parameters

包括**关键安全参数**(3.3)和**公开安全参数**(3.14)。

3.18

简单功耗分析　simple power analysis

对指令执行(或单个指令的执行)模式的直接(主要是可视化的)分析，它与密码模块的功耗有关，并用以获取密码操作相关的信息。

3.19

知识拆分　split knowledge

密钥被拆分成多个密钥分量，从密码模块输出给多个实体的过程。单个分量不能提供原始密钥的知识。密钥分量被各个实体输入密码模块能够重新组合成原始密钥，合成密钥可以需要所有分量或一部分分量来完成。

3.20

敏感安全参数建立　sensitive security parameter establishment

将共享的敏感安全参数提供给一个或多个实体的过程。

注：敏感安全参数建立包括敏感安全参数协商、传输以及输入或输出。

4　缩略语

下列缩略语适用于本文件。

API：应用程序接口(Application Program Interface)

CBC：密码分组链接(Cipher Block Chaining)

ECB：电子译码本(Electronic Codebook)

EDC：错误检测码(Error Detection Code)

EFP：环境失效保护(Environmental Failure Protection)

EFT：环境失效测试(Environmental Failure Testing)

FSM：有限状态模型(Finite State Model)

HDL：硬件描述语言(Hardware Description Language)

HMAC：基于杂凑的消息鉴别码(Hash-Based Message Authentication Code)

IC：集成电路(Integrated Circuit)

PIN：个人身份识别码(Personal Identification Number)

5　密码模块安全等级

5.1　概述

密码模块是指实现密码运算、密钥管理等功能的硬件、软件、固件或者其组合。本标准适用于保护计算机与电信系统内敏感信息的安全系统所使用的密码模块。为了保护密码模块和密码模块中包含和控制的敏感安全参数，以及满足众多应用领域的、不同程度的安全需求，本标准规定了4个要求递增的安全等级，高安全等级在低安全等级的基础上进一步提高了安全性。本标准中给出的一些常见的例子，

是用于阐明如何满足本标准的安全要求，而不是为了约束或列举所有的情况。下文分别概述了4个安全等级。4个安全等级所涉及的密码技术是相同的。

本标准采用了“应[xx.yy]”方式对标准中的所有安全要求进行标识和顺序编号，其中，xx表示条款，yy是该条款中的数字索引。如果本标准中的某句话中出现“应[xx.yy]”，即表示该句是本标准的一项安全要求，编号为[xx.yy]。本标准总共有12个条款，与密码模块的安全通用要求以及11个安全域相对应，1～12分别代表：通用要求；密码模块规格；密码模块接口；角色、服务和鉴别；软件/固件安全；运行环境；物理安全；非入侵式安全；敏感安全参数管理；自测试；生命周期保障；以及对其他攻击的缓解。每个条款中又包含具体的安全要求，每个安全要求从[xx.01]开始按顺序编号。

本标准下文中凡是包含“应[xx.yy]”的句子都被视为密码模块的一项安全要求，这种标识方式可以被本标准对应的后续检测标准直接引用，也可被密码模块厂商提交的文档引用。

5.2 安全一级

安全一级提供了最低等级的安全要求。安全一级阐明了密码模块的基本安全要求，例如，密码模块应使用至少一个核准的安全功能或核准的敏感安全参数建立方法。软件或固件密码模块可以运行在不可修改的、受限的或可修改的运行环境中。硬件密码模块除了需要达到产品级部件的基本要求之外，没有其他特殊的物理安全机制要求。密码模块实现的针对非入侵式攻击或其他攻击的缓解方法需要有文档记录。安全一级密码模块的例子有：个人计算机中的硬件加密板卡、运行在手持设备或通用计算机上的密码工具包。

当密码模块外部的应用系统已经配置了物理安全、网络安全以及管理过程等控制措施时，安全一级的密码模块就非常适用。这使得密码模块的使用者可以选择多种密码解决方案来满足安全需求。

5.3 安全二级

安全二级在安全一级的基础上增加了拆卸证据的要求，例如使用拆卸存迹的涂层或封条，或者在封盖或门上加防撬锁等手段以提供拆卸证据。

拆卸存迹的封条或防撬锁应安装在封盖或门上，以防止非授权的物理访问。当物理访问密码模块内的安全参数时，密码模块上拆卸存迹的涂层或封条就应破碎。

安全二级要求基于角色的鉴别。密码模块需要鉴别并验证操作员的角色，以确定其是否有权执行对应的服务。

安全二级的软件密码模块可以运行在可修改的环境中，该环境应实现基于角色的访问控制或自主访问控制，但自主访问控制应能定义新的组，通过访问控制列表(ACL)分配权限，以及将一个用户分配给多个组。访问控制措施应防止非授权地执行、修改以及读取实现密码功能的软件。

5.4 安全三级

除了安全二级中要求的拆卸存迹物理安全机制外，安全三级还要求更强的物理安全机制，以进一步防止对密码模块内敏感安全参数的非授权访问。这些物理安全机制应能够以很高的概率检测到以下行为并作出响应，这些行为包括：直接物理访问、密码模块的使用或修改，以及通过通风孔或缝隙对密码模块的探测。上述物理安全机制可以包括坚固的外壳、拆卸检测装置以及响应电路。当密码模块的封盖/门被打开时，响应电路应将所有的关键安全参数置零。

安全三级要求基于身份的鉴别机制，以提高安全二级中基于角色的鉴别机制的安全性。密码模块需要鉴别操作员的身份，并验证经鉴别的操作员是否被授权担任特定的角色以及是否能够执行相应的服务。

安全三级要求手动建立的明文关键安全参数是经过加密的、使用可信信道或使用知识拆分来输入或输出。

安全三级的密码模块应有效防止电压、温度超出密码模块正常运行范围对密码模块安全性的破坏。攻击者可以故意让密码模块的环境参数偏离正常运行范围，从而绕过密码模块的防护措施。密码模块应设计有环境保护特性，用以检测环境异常并置零关键安全参数，或者能够通过环境失效测试从而提供一个合理的保障，确保不会因环境异常破坏密码模块的安全性。

安全三级的密码模块应提供非入侵式攻击缓解技术的有效性证据和检测方法。

对于软件密码模块，并没有在本标准的所有条款中给出安全三级的要求。因此，软件密码模块能够达到的最大整体安全等级限定为安全二级。

安全三级的密码模块增加了生命周期保障的要求，比如自动配置管理、详细设计、底层测试以及基于厂商所提供的鉴别信息的操作员鉴别。

5.5 安全四级

安全四级是本标准中的最高安全等级。该等级包括较低等级中所有的安全特性，以及一些扩展特性。

安全四级的物理安全机制应在密码模块周围提供完整的封套保护，其目的是无论外部电源是否供电，当密码模块包含敏感安全参数时，检测并响应所有非授权的物理访问。从任何方向穿透密码模块的外壳都会以很高的概率被检测到，并将导致所有未受保护的敏感安全参数立刻被置零。由于安全四级的密码模块自身具有较高的安全机制，所以它特别适用于无物理保护的环境。

安全四级要求对操作员进行多因素鉴别。最低限度下，要求使用下列因素中的两个：

——已知某物，如秘密口令；

——拥有某物，如物理钥匙或令牌；

——具有某属性，如生物特征。

安全四级的密码模块应有效防止电压、温度超出密码模块正常运行范围对密码模块安全性的破坏。密码模块应设计有环境保护特性，专门用以检测环境异常并置零关键安全参数，从而提供一个合理的保障，确保不会因环境异常破坏密码模块的安全性。

按照国家相关部门规定的、安全四级的非入侵式攻击缓解检测指标，检测密码模块中实现的、7.8中规定的针对非入侵式攻击的缓解方法。

安全四级要求密码模块的设计应通过一致性验证，即验证前置和后置条件与功能规格之间的一致性。

6 功能安全目标

本标准中规定的安全要求涉及密码模块的安全设计和实现。安全要求从安全目标的最低等级开始，随着安全目标等级的递增而增加。这些要求源于密码模块的下列功能性安全目标：

——使用并正确实现核准的安全功能，以保护敏感信息；

——防止非授权地操作或使用密码模块；

——防止非授权地泄露密码模块的内容，其中包括关键安全参数；

——防止对密码模块和密码算法进行非授权或检测不到的修改，包括非授权地修改、替换、插入和删除敏感安全参数；

——提供密码模块运行状态的指示；

——保证密码模块在核准的工作模式下能够正确运行；

——检测出密码模块运行中的错误，防止这些错误非授权地公开、修改、替换或使用关键安全参数，或者非授权地修改或替换公开安全参数；

——保证正确地设计、分配和实现密码模块。

7 安全要求

7.1 通用要求

符合本标准的密码模块应[01.01]满足的安全要求。这些安全要求涵盖了密码模块的设计、实现、操作以及废弃相关的域，具体包括：密码模块规格；密码模块接口；角色、服务和鉴别；软件/固件安全；运行环境；物理安全；非入侵式安全；敏感安全参数管理；自测试；生命周期保障；以及对其他攻击的缓解。

表1总结了每个域的安全要求。

密码模块应[01.02]针对各个域的要求进行检测。密码模块应[01.03]在每个域中独立地进行评级。上述11个安全域中，有些域随着安全等级的递增，安全要求也相应增加。密码模块在这些域中获得的评级反映了密码模块在该域中所能达到的最高安全等级，即密码模块应满足该域针对该等级的所有安全要求。另外一些域的安全要求不分安全等级，那么密码模块在这些域中将获得与整体评级相当的评级。

除了在每个安全域中获得独立的评级之外，密码模块还将获得一个整体评级。整体评级设定为11个域所获得的最低评级。

本标准要求密码模块提供相关的文档，具体要求见附录A和附录B。待确认或评估的密码模块应[01.04]提供所有相关文档，包括用户和安装手册、设计说明、生命周期文档等。

附录C、附录D、附录E和附录F提供了核准的安全功能、核准的敏感安全参数生成和建立方法、核准的鉴别机制以及非入侵式攻击及常用的缓解方法等相关内容。

表1 安全要求总表

安全域	安全一级	安全二级	安全三级	安全四级
1 密码模块规格	密码模块、密码边界、核准的密码功能以及正常的工作模式的说明； 密码模块的描述，包括所有硬件、软件和固件部件； 所有服务提供状态信息以指示服务何时按照核准的方式使用核准的密码算法、安全功能或过程			
2 密码模块接口	要求的和可选的接口； 所有接口和所有输入输出数据路径的说明		可信信道	
3 角色、服务和鉴别	要求的角色、服务与可选的角色、服务逻辑上相隔离	基于角色或基于身份的操作员鉴别	基于身份的鉴别	多因素鉴别
4 软件/固件安全	核准的完整性技术，以及定义的软件或固件密码模块接口、混合固件密码模块接口	基于核准的数字签名或带密钥信息消息鉴别码的完整性测试	基于核准的数字签名的完整性测试	
	以及混合软件固件密码模块接口；可执行代码			

表 1（续）

安全域		安全一级	安全二级	安全三级	安全四级
5 运行环境		不可修改的、受限的；对敏感安全参数的控制			
		可修改的； 对敏感安全参数的控制	可修改的； 基于角色或自主访问控制；审计机制		
6 物理安全		产品级部件	拆卸证据； 不透明的遮盖物或外壳	封盖和门上的拆卸检测与响应电路； 牢固的外壳或涂层； 防止直接探测的保护； EFP 或 EFT	拆卸检测和响应封壳； EFP； 故障注入的缓解
7 非入侵安全		能够缓解附录 F 中规定的非入侵式攻击			
		文档阐明附录 F 中规定的缓解技术和有效性		提供缓解检测方法	缓解检测
8 敏感安全参数管理		随机数生成器、敏感安全参数生成、建立、输入和输出、存储以及置零			
		自动的敏感安全参数传输或敏感安全参数协商使用核准方法			
		手动建立的敏感安全参数可以以明文的形式输入或输出		手动建立的敏感安全参数，可以以加密的形式、通过可信信道或使用知识拆分过程输入或输出	
9 自测试		运行前：软件/固件完整性测试、旁路测试以及关键功能测试			
		条件：密码算法、配对一致性、软件/固件加载、手动输入、条件旁路以及关键功能测试			
10 生命周期保障	1） 配置管理	密码模块、部件和文档的配置管理系统。每一项在整个生命周期中都有唯一标识并可追踪		自动配置管理系统	
	2） 设计	密码模块设计成允许对所有提供的安全相关服务进行测试			
	3） FSM	有限状态模型			
	4） 开发	有注释的源代码、版图或 HDL	软件高级语言； 硬件高级描述语言		文档注明密码模块部件执行的前置条件，以及当部件执行完毕时预期为真的后置条件
	5） 测试	功能测试		底层测试	
	6） 配送与操作	初始化流程	配送流程		使用厂商提供的鉴别信息的操作员鉴别
	7） 生命终止	安全清理密码模块的流程		安全销毁密码模块的流程	
	8） 指南文档	管理员和非管理员指南			
11 其他攻击的缓解		缓解其他攻击的说明，目前对这些攻击还没有可检测要求			验证缓解技术的有效性

7.2 密码模块规格

7.2.1 密码模块规格通用要求

密码模块应[02.01]是硬件、软件、固件，或它们之间组合的集合，该集合至少使用一个核准的密码算法、安全功能或过程实现一项密码服务，并且包含在定义的密码边界内。

密码模块文档应[02.02]按照 A.2.2 中规定的要求编写。

7.2.2 密码模块类型

密码模块应[02.03]定义为下列一种密码模块类型：

——硬件密码模块：密码边界规定为硬件边线。固件和/或软件，其中还可以包括操作系统，可以被包含在硬件密码边界内。

——软件密码模块：密码边界为执行在可修改的运行环境中的纯软件部件（可以是一个或多个软件部件）划定界线。软件密码模块的运行环境所包含的计算平台和操作系统，在定义的密码边界之外。

——固件密码模块：密码边界为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界线。固件密码模块的运行环境所包含的计算平台和操作系统，在定义的密码边界之外，但是与固件密码模块明确绑定。

——混合软件密码模块：密码边界为软件部件和分离的硬件部件（即软件部件不在硬件密码模块边界中）的集合划定界线。软件运行的环境所包含的计算平台和操作系统，在定义的混合软件密码模块边界之外。

——混合固件密码模块：密码边界为固件部件和分离的硬件部件（即固件部件不在硬件密码模块边界中）的合成划定界线。固件运行的环境所包含的计算平台和操作系统，在定义的混合固件密码模块边界之外，但是与混合固件密码模块明确绑定。

对于硬件和固件密码模块，应[02.04]满足 7.7 中规定的物理安全和 7.8 中规定的非入侵式安全的所有适用要求。

对于运行于可修改环境中的软件密码模块，应[02.05]满足 7.8 中规定的非入侵式安全中的所有适用要求；7.7 中规定的物理安全要求是可选的。

对于混合密码模块，应[02.06]满足 7.5 中规定的软件/固件安全、7.6 中规定的运行环境、7.7 中规定的物理安全和 7.8 中规定的非入侵式安全中的所有适用要求。

7.2.3 密码边界

7.2.3.1 密码边界通用要求

密码边界应[02.07]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。本标准的要求应[02.08]适用于密码边界内的所有算法、安全功能、过程和部件。密码边界应[02.09]至少包含密码模块内所有安全相关的算法、安全功能、过程和部件（即本标准范围内与安全相关的）。非安全相关的算法、安全功能、过程和部件也可以包含在密码边界内。用于核准工作模式的非安全相关的算法、安全功能、过程和部件的实现应[02.10]不干扰或破坏密码模块核准的运行。

密码模块的名称应[02.11]代表密码边界内的部件构成，不应代表大于实际范围的构成或产品。密码模块应[02.12]至少具有代表每个互不相同的硬件、软件和/或固件部件的特定版本信息。

密码边界内的某些硬件、软件和/或固件部件可以从本标准的要求中排除。被排除的硬件、软件或固件部件的实现应[02.13]不干扰或破坏密码模块核准的安全运行。应[02.14]阐明被排除的硬件、软

件或固件(见附录 A)。

7.2.3.2 密码边界的定义

不同类型的密码模块,其密码边界有所差异,具体内容如下:

a) **硬件密码模块**的密码边界应[02.15]划界并确定:

硬件部件集合,可包括:

——在部件之间提供互联的物理配线的物理结构,包括电路板、基板或其他表面贴装;

——有效电器元件,如半集成、定制集成或通用集成的电路、处理器、内存、电源、转换器等;

——外壳、灌封或封装材料、连接器和接口之类的物理结构;

——固件,可以包含操作系统;

——上面未列出的其他部件类型。

b) **软件密码模块**的密码边界应[02.16]划界并确定:

——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。

c) **固件密码模块**的密码边界应[02.17]划界并确定:

——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。

d) **混合密码模块**的密码边界应[02.18]:

——由密码模块硬件部件的边界以及分离的软件或固件部件的边界构成;

——包含每个部件所有端口和接口的集合。

混合密码模块除了分离的软件或固件部件,密码模块的硬件部件还可以包含嵌入式的软件或固件。

7.2.4 工作模式

7.2.4.1 工作模式通用要求

密码模块可以有核准的工作模式和非核准的工作模式。核准的工作模式是指密码模块在该工作模式下只能使用核准的安全功能提供安全相关服务。

操作员应[02.19]能够在核准的工作模式下操作密码模块。核准的工作模式应[02.20]定义为一组服务的集合,其中至少有一个服务使用了核准的密码算法、安全功能或过程。

非核准的密码算法、安全功能和过程或其他未规定于 7.4.3 中的服务不应[02.21]被操作员用于核准的工作模式中,除非非核准的密码算法或安全功能是核准的过程的一部分,而且与核准的过程的安全无关。例如,使用非核准的密码算法或非核准的方式生成的密钥,混淆数据或关键安全参数,结果也被视为未受保护的明文,且不能提供安全相关功能。

7.2.4.2 正常工作

正常工作是指算法、安全功能、服务或过程的完整集合都是可用的和/或可配置的。

核准的和非核准的服务和工作模式的关键安全参数应[02.22]相互分离,例如,不共享或不相互访问。核准的随机数生成器的输出可以提供给非核准的算法、安全功能或过程,只要随机数生成器种子无法在非核准的模式中访问就无需置零种子。

密码模块的安全策略应[02.23]为密码模块所包括的每个工作模式(核准的和非核准的)定义完整的服务集合。

当服务正在以核准的方式使用核准的密码算法、安全功能或过程,以及其他规定于 7.4.3 中的服务或过程的时候,该服务应[02.24]给出相应的状态指示。

7.2.4.3 降级工作

降级工作是指当密码模块进入错误状态后，某些算法、安全功能、服务或过程的操作集合仍然是可用的和/或可配置的。本标准要求当密码模块出现任何错误，都应[02.25]进入错误状态并停止工作，不能降级工作。

7.3 密码模块接口

7.3.1 密码模块接口通用要求

所有进出密码模块的逻辑信息流，都应[03.01]只能通过已定义的物理端口和逻辑接口，这些端口和接口是出入密码边界的入口和出口。密码模块逻辑接口应[03.02]是相互分离的，这些逻辑接口可以共享一个物理端口，例如，输入数据和输出数据可以使用同一个端口，或者逻辑接口也可以分布在一个或多个物理端口上，例如，输入数据可以通过串口也可以通过并口。密码模块软件部件的应用程序接口(API)可以定义为一个或多个逻辑接口。

密码模块文档应[03.03]按照 A.2.3 的要求编写。

7.3.2 接口类型

密码模块的接口类型包括：

——硬件密码模块接口定义为用于请求硬件密码模块服务的命令全集，请求服务的命令中包括输入到密码模块或者由密码模块输出的参数。

——软件或固件密码模块接口定义为用于请求软件或固件密码模块服务的命令全集，请求服务的命令中包括输入到密码模块或者由密码模块输出的参数。

——混合固件或混合软件密码模块接口定义为用于请求混合固件或混合软件密码模块服务的命令全集，请求服务的命令中包括输入到密码模块或者由密码模块输出的参数。

7.3.3 接口定义

密码模块应[03.04]具备下列五种接口(“输入”和“输出”是相对于密码模块而言的)：

——数据输入接口：由密码模块处理的所有输入数据(通过“控制输入”接口输入的控制数据除外)，包括明文、密文、敏感安全参数和另一个密码模块的状态信息，应[03.05]通过“数据输入”接口输入。当密码模块执行 7.10 中自测试时，密码模块可以通过数据输入接口接收数据。

——数据输出接口：除“状态输出”接口输出的状态数据以及通过“控制输出”接口输出的控制数据之外，所有从密码模块输出的输出数据，包括明文、密文和敏感安全参数等，应[03.06]通过“数据输出”接口输出。在执行手动输入、运行前自测试、软件/固件加载和置零的过程中，或者当密码模块处在错误状态时，应[03.07]禁止通过“数据输出”接口输出数据。

——控制输入接口：所有用于控制密码模块运行的输入命令、信号(例如，时钟输入)及控制数据(包括手动控制如开关、按钮和键盘，以及功能调用)应[03.08]通过“控制输入”接口输入。

——控制输出接口：所有用于控制密码模块运行的输出命令、信号及控制数据(例如，对另一个密码模块的控制命令)应[03.09]通过“控制输出”接口输出。当密码模块处于错误状态时，应[03.10]禁止通过“控制输出”接口的控制输出，除非在安全策略中规定了一些例外情况。

——状态输出接口：所有用于指示密码模块状态的输出信号、指示器(例如，错误指示器)和状态数据[包括返回码和物理指示器，比如视觉的(显示器，指示灯)，声音的(蜂鸣器提示音，响铃)，以及机械的(振动器)]，应[03.11]通过“状态输出”接口输出。状态输出可以是显式的或隐式的。

除软件密码模块以外，所有密码模块还应[03.12]具备下列接口：

——电源接口：输入密码模块的所有外部电能应[03.13]通过电源端口输入。电源端口不是必需的，当所有能量由密码模块的密码边界内部提供或维持时（例如，通过内部电池），电源接口可以不存在。

密码模块应[03.14]区分数据、控制信息和电源的输入，以及数据、控制信息、状态信息和电源的输出。密码模块规格应[03.15]明确规定输入数据以及控制信息的格式，包括对所有可变长度输入的长度限制。

7.3.4 可信信道

可信信道是在密码模块和发送者或接收者之间建立的链路，用于安全传输未受保护的明文密钥分量、鉴别数据以及其他关键安全参数。明文密钥指的是未经加密的密钥，或由非核准的方法混淆的密钥。可信信道在密码模块定义的输入或输出端口以及预期的发送者或接收者终端的通信链路上，可以防止窃听以及来自恶意的操作员/实体、进程或其他设备的物理或逻辑篡改。

密码模块的可信信道要求包括：

a） 安全一级和安全二级：

对于安全一级和安全二级，没有可信信道要求。

b） 安全三级：

对于安全三级：

——密码模块应[03.16]实现可信信道，用于在密码模块与发送者或接收者终端之间传输未受保护的明文密钥分量、鉴别数据以及其他关键安全参数；

——可信信道应[03.17]防止在通信链路上的非授权修改、替换和泄露；

——可信信道使用的物理端口应[03.18]与其他物理端口实现物理隔离；或可信信道使用的逻辑接口应[03.19]与其他逻辑接口实现逻辑隔离；

——基于身份的鉴别应[03.20]用于所有使用可信信道的服务；

——当可信信道在使用时，应[03.21]提供状态指示器。

c） 安全四级：

对于安全四级，除了安全三级的要求以外，基于身份的多因素鉴别应[03.22]用于所有使用可信信道的服务。

7.4 角色、服务和鉴别

7.4.1 角色、服务和鉴别通用要求

密码模块应[04.01]支持操作员的授权角色以及与每个角色相对应的服务。一个操作员可以担任多种角色。如果密码模块支持多个操作员同时操作，那么密码模块内部应[04.02]确保各个操作员担任的角色相隔离及相应的服务相隔离。当服务执行不会修改、泄露或替换关键安全参数和公开安全参数时，例如显示状态、自测试或者其他不影响密码模块安全的服务，操作员无需担任一个授权角色。

密码模块可能需要鉴别机制，以鉴别操作员对密码模块的访问，以及验证操作员是否被授权担任请求的角色和执行该角色下的服务。

密码模块文档应[04.03]按照 A.2.4 中规定的要求编写。

7.4.2 角色

密码模块应[04.04]至少支持密码主管角色。密码主管角色应[04.05]负责执行密码初始化或管理功能，以及常用的安全服务，例如，密码模块初始化、关键安全参数和公开安全参数的管理以及审计功能。

密码模块可以支持用户角色。如果密码模块支持用户角色，那么用户角色应[04.06]负责执行一般的安全服务，包括密码操作和其他核准的安全功能。

密码模块可以支持维护员角色。维护员角色是指在物理维护服务(例如，打开密码模块封盖)和/或逻辑维护服务(例如，运行某种诊断如内置的自测试)时担任的角色。当进入或退出维护员角色时，所有不受保护的敏感安全参数应[04.07]被置零。

除了上述角色以外，密码模块还可支持其他角色。

7.4.3 服务

7.4.3.1 服务通用要求

服务应[04.08]指的是密码模块所能执行的所有服务、操作或功能。服务输入应[04.09]包括密码模块在启动或获取特定服务、操作或功能时，所使用的所有数据或控制输入。服务输出应[04.10]包括由服务输入启动或获取的服务、操作或功能，所产生的所有数据和状态输出。每个服务输入应[04.11]产生一个服务输出。

密码模块应[04.12]为操作员提供下列服务：

a) 显示密码模块版本号。密码模块应[04.13]输出名称或密码模块标识符以及版本信息，这些信息可以与密码模块的确认记录相关联。

b) 显示状态。密码模块应[04.14]输出当前的状态。其中可以包括响应服务请求的状态指示器的输出。

c) 执行自测试：密码模块应[04.15]执行初始化和规定于 7.10.2 中的运行前自测试。

d) 执行核准的安全功能。密码模块应[04.16]至少执行一个在 7.2.4 中规定的核准的工作模式中使用的核准的安全功能。

e) 执行置零。密码应[04.17]按照 7.9.7 中的规定执行参数置零。

除了上述规定的服务以外，密码模块还可以提供其他的服务、操作或功能，包括核准的和非核准的。一些特定的服务可能不止一个角色使用它，例如，用户角色和密码主管角色都可使用密钥输入服务。

7.4.3.2 旁路能力

旁路能力是指某种服务所具备的部分或全部绕过密码功能的能力。如果密码模块输出的数据是受到密码技术保护的(例如，经过加密)，但是通过更改密码模块的配置或者由于操作员的干预，密码模块能够将数据直接输出(例如，不再经过加密)，此时，应[04.18]定义该密码模块具有旁路能力。

如果密码模块实现了旁路能力，那么：

——在开启密码模块的旁路功能之前，操作员应[04.19]担任相应的授权角色。

——应[04.20]使用两个独立的内部操作来激活旁路能力，以防止单个错误造成不经意地输出明文数据。这两个独立的内部操作应[04.21]能够改变用于控制旁路能力的软件和/或硬件配置(例如，设置两个不同的软件或硬件标志位，其中一个可以由用户发起)。

——对于安全四级密码模块，上述两个独立的内部操作应[04.22]由两个不同的操作员完成。

——密码模块应[04.23]显示其状态以指示旁路能力是否：

- 未被激活，表明密码模块此时只提供使用密码功能的服务(例如，明文数据经过加密之后输出密码模块)；
- 被激活，表明密码模块此时只提供没有使用密码功能的服务(例如，明文数据未经过加密就输出密码模块)；
- 同时存在激活和去活，表明密码模块此时提供的某些服务使用了密码功能，而某些服务没有使用密码功能(例如，对于拥有多个通信信道的密码模块，明文数据是否被加密取决于

每个信道的配置)。

7.4.3.3 自启动密码服务能力

自启动密码服务能力是指无需外界操作员请求,密码模块就能够执行密码操作和其他核准的安全功能或敏感安全参数管理技术。自启动密码服务能力应[04.24]由密码主管配置,而且该配置可以在密码模块经过重置、重启或开关电源之后保留下来。

如果密码模块实现了自启动密码服务能力,那么:

——应[04.25]需要两个独立的内部操作来激活该能力,以防止单个错误造成不经意的输出。这两个独立的内部操作应[04.26]能够改变用于控制该能力的软件和/或硬件配置(例如,设置两个不同的软件或硬件标志位,其中一个可以由用户发起)。

——对于安全四级密码模块,上述两个独立的内部操作应[04.27]由两个不同的操作员完成。

——密码模块应[04.28]显示其状态以指示自启动密码服务能力是否被激活。

7.4.3.4 软件/固件加载

如果密码模块具有加载外部软件或固件的能力,那么应[04.29]满足下列要求:

——加载的软件或固件应[04.30]在加载之前经过确认机构的确认,以维持确认效力。

——应[04.31]禁止通过数据输出接口输出数据,直到软件/固件加载完成以及加载测试成功通过。

——在运行加载的代码之前应[04.32]执行 7.10.3.4 中规定的软件/固件加载条件自测试。

——密码模块应[04.33]拒绝运行任何已经加载的或已被修改的核准安全功能,直到成功执行7.10.2中规定的运行前自测试。

——应[04.34]修改密码模块的版本信息,以表示增加和/或更新了最新加载的 7.4.3 中的软件或固件。

如果新软件或固件的加载是镜像的完全替换,它应[04.35]构成一个全新的密码模块,需要由确认机构重新确认,以维持确认效力。新加载的软件或固件镜像应[04.36]在密码模块上电重置之后才能运行。所有敏感安全参数应[04.37]在运行新镜像之前被置零。

7.4.4 鉴别

密码模块可能需要鉴别机制以鉴别访问密码模块的操作员,并验证该操作员能否担任其请求的角色,以及能否执行相应的服务。下列几类机制用于密码模块的访问控制:

基于角色的鉴别:如果密码模块支持基于角色的鉴别机制,那么密码模块应[04.38]要求操作员隐式地或显式地选择一个或多个角色,并且应[04.39]鉴别其能否担任所选定的角色(或角色的集合)。不要求密码模块鉴别操作员的个人身份。选择角色和鉴别能否担任所选定的角色可以结合起来进行。如果密码模块允许操作员变换角色,且如果请求的新角色之前未被鉴别,那么密码模块应[04.40]鉴别该操作员能否担任该新角色。

基于身份的鉴别:如果密码模块支持基于身份的鉴别机制,密码模块应[04.41]要求单独且唯一标识操作员,应[04.42]要求操作员隐式地或显式地选择一个或多个角色,并且应[04.43]鉴别操作员的身份,以及操作员是否被授权担任所选定的角色(或角色的集合)。鉴别操作员的身份、选择角色,以及鉴别能否授权担任所选定的角色可以结合起来进行。如果密码模块允许操作员变换角色,且如果请求的新角色之前未被授权,那么密码模块应[04.44]验证经标识的操作员是否被授权担任该新角色。

密码模块可以允许通过鉴别的操作员执行其授权角色所允许的所有服务,或者也可以针对每个服务或一组服务分别进行鉴别。当密码模块被重置、重启、关闭且随后又被打开时,密码模块应[04.45]要求重新鉴别操作员。

密码模块可能需要多种类型的鉴别数据以实现模块支持的鉴别机制,包括(但不限于)知道或拥有

口令、PIN、密钥等；拥有物理钥匙、令牌等；或具备个人特征（例如，生物特征）。应[04.46]保护密码模块内的鉴别数据以防止非授权的泄露、修改和替换。核准的安全功能可被用于鉴别机制。

鉴别机制的初始化允许特殊处理。如果第一次访问密码模块时，密码模块不包含鉴别操作员所需的鉴别数据，那么应[04.47]使用其他被授权的方法（例如，过程控制，使用出厂设置或默认的鉴别数据）对密码模块进行访问控制和初始化鉴别。如果使用了默认的鉴别数据来控制对密码模块的访问，那么默认的鉴别数据应[04.48]在第一次鉴别后被更换。该默认的鉴别数据不需要满足 7.9.7 中置零要求。

鉴别机制可以是一组具有不同鉴别属性的机制，这些机制结合起来可以满足本条款的要求。如果密码模块使用安全功能鉴别操作员，那么那些安全功能应[04.49]是核准的安全功能。此外，密码模块还应满足下列要求：

——密码模块应[04.50]实现附录 E 中规定的一种核准的鉴别机制。

——在密码模块的安全策略文档（见附录 B）中应[04.51]描述鉴别机制的强度。

——对于每次核准鉴别机制的尝试使用，密码模块应[04.52]满足鉴别强度要求。对于在一分钟之内对核准鉴别机制的多次尝试使用，密码模块应[04.53]满足鉴别强度要求。

——核准的鉴别机制应[04.54]依赖于密码模块的具体实现，而不依赖于在文档中的过程控制或安全规则（例如，口令长度限制）。

——对于安全二级的软件密码模块，操作系统可以实现鉴别机制。如果操作系统实现了鉴别机制，那么鉴别机制应[04.55]满足本条的要求。

——在鉴别过程中，应[04.56]隐藏鉴别数据给操作员的反馈信息（例如，在输入口令时没有可视的字符显示）。无意义的字符可以代替实际的鉴别数据显示。

——在尝试鉴别的过程中，提供给操作员的反馈信息应[04.57]防止削弱鉴别机制强度。

密码模块对鉴别机制的采用，应满足下列要求：

a） 安全一级：

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。如果密码模块不支持鉴别机制，密码模块应[04.58]要求操作员隐式或显式地选择一个或多个角色。

b） 安全二级：

对于安全二级，密码模块应[04.59]至少采用基于角色的鉴别以控制对密码模块的访问。

c） 安全三级：

对于安全三级，密码模块应[04.60]采用基于身份的鉴别机制以控制对密码模块的访问。

d） 安全四级：

对于安全四级，密码模块应[04.61]采用基于身份的多因素鉴别机制以控制对密码模块的访问。

7.5 软件/固件安全

密码模块定义为 7.2.2 中规定的硬件、软件、固件或混合密码模块。本条的要求应[05.01]适用于密码模块的软件和固件部件。

完全由硬件实现的密码模块无需满足本标准的软件/固件安全要求。

用于核准的完整性技术的签名验证公钥或 HMAC 的密钥可以存在于密码模块代码中，而且此时它们不被视为敏感安全参数。

密码模块文档应[05.02]按照 A.2.5 中规定的要求编写。

密码模块的软件和固件部件应满足下列要求：

a） 安全一级：

对于安全一级，下列安全要求应[05.03]适用于密码模块内的软件和固件部件：

——所有的软件和固件应[05.04]符合 7.11.7 中的规定，确保安装前未被修改。

——密码边界内的所有软件和固件部件应[05.05]使用核准的完整性技术进行保护，这些完整性技术可以由该密码模块提供，也可以由另一个经确认的密码模块提供。

——如果完整性测试失败，密码模块应[05.06]进入错误状态。核准的完整性技术可以包含单个鉴别码或签名，或者多个分离的消息鉴别码或签名。在多个分离的消息鉴别码或签名中，任何一个消息鉴别码或签名验证失败都应[05.07]导致密码模块进入错误状态。一旦完成了完整性测试，密码模块软件或固件的完整性测试的过程中生成的临时值应[05.08]被置零。

——操作员应[05.09]能够通过 7.3.2 中规定的硬件密码模块接口、软件或固件密码模块接口、混合固件密码模块接口或混合软件密码模块接口服务按需执行核准的完整性技术。

——7.3.3 中规定的密码模块的所有数据和控制输入，数据、控制和状态输出，以及 7.4.3 中规定的服务，应[05.10]通过定义的硬件密码模块接口、软件或固件密码模块接口、混合固件密码模块接口或混合软件密码模块接口完成。

——对于软件或固件密码模块，如果加载的软件或固件镜像完全替换或覆盖了已确认的密码模块镜像，则软件/固件加载测试是不适用的，因为替换或覆盖将形成一个新的密码模块。如果新加载的软件或固件是密码模块运行所必须的，但不是完全替换或覆盖经确认的密码模块，那么软件/固件加载测试是适用的，并且应[05.11]由经过确认的密码模块执行该测试。

b) 安全二级：

对于安全二级，除了安全一级的要求，还有下列要求应[05.12]适用于密码模块内的软件或固件部件：

——密码模块的软件和固件部件应[05.13]只包含可运行形式的代码，例如，不包括源代码、目标代码或实时编译的代码。

——应[05.14]确保操作员无法通过硬件密码模块接口、软件或固件密码模块接口、混合固件密码模块接口或混合软件密码模块接口的服务或控制设置，启动或执行调试技术。

——密码边界内的所有软件和固件应[05.15]使用核准的数字签名或带密钥的消息鉴别码进行保护。如果计算的结果未能成功通过验证，则测试失败，并且密码模块应[05.16]进入错误状态。

c) 安全三级和安全四级：

对于安全三级和安全四级，除了安全一级和安全二级的要求，下列要求应[05.17]适用于密码模块内的软件和固件部件：

——密码边界内的所有软件和固件应[05.18]使用核准的数字签名进行保护。如果计算的结果未能成功通过验证，则测试失败，并且密码模块应[05.19]进入错误状态。

——数字签名技术可以包含单个签名，或者多个分离的签名，分离的签名中任何一个签名的验证失败都应[05.20]导致密码模块进入错误状态。签名私钥应[05.21]保存在密码模块外。

7.6 运行环境

7.6.1 运行环境通用要求

密码模块运行环境涉及对密码模块运行所需的软件、固件和/或硬件的管理。软件、固件或混合密码模块的运行环境至少包括密码模块部件、计算平台、以及控制或支持软件或固件在计算平台上运行的操作系统。硬件密码模块内部可以包含一个运行环境，该环境可以包含支持密码模块内部软件或固件运行的操作系统。如果适用的话，虚拟机（系统和/或进程）和运行时环境（例如，Java 运行时环境——

JRE)也可以视为操作系统的一部分。

通用运行环境是指使用商用的通用操作系统(即资源管理器)来管理软件和固件部件,以及管理系统和操作员进程(线程),其中包括了通用的应用程序软件,如文字处理器等。

运行环境可以是不可修改的、受限制的或可修改的。以下条款阐明了三个特定的运行环境:

a) 不可修改的运行环境是设计成或配置成防止操作员或进程对密码模块部件、计算平台或操作系统进行修改的运行环境,即该环境中的密码模块部件、计算平台或操作系统是不允许被修改的。该环境可以包含运行在不可编程计算平台上的固件密码模块,或具有阻止加载任何其他软件或固件能力的硬件密码模块。

b) 受限制的运行环境是设计成或配置成允许操作员或进程受控地对密码模块部件、计算平台或操作系统进行修改的运行环境,即该环境中的密码模块部件、计算平台或操作系统的修改应满足相关的要求。该环境可以是运行于可编程硬件密码模块的固件,并且在该密码模块中加载其他固件需要满足 7.4.3.4 中规定的固件加载要求。

c) 可修改的运行环境是指通过重新配置可以增加/删除/修改某些功能的环境,和/或包含通用操作系统功能(例如,可以选择使用计算机操作系统、配置智能卡操作系统或者加载可编程的软件)的环境。如果操作员或进程可以修改软件部件,和/或加载和执行某些软件(例如,文字处理器),这些软件不是已有软件、固件或混合密码模块中的一部分,则该操作系统被视为可修改的运行环境。可修改的运行环境具有以下特点:

在运行环境内可以添加或修改功能。这些添加或者被修改的功能可能会干扰密码模块的运行,除非运行环境禁止这样的干扰。在这样的环境中,要求运行在同一个运行环境下且不属于运行环境可信部分的功能,除了通过密码模块已定义的接口以外,不能通过其他途径访问敏感安全参数。因此,要求运行环境在运行时,具备把密码模块的功能与该运行环境中的其他功能相互隔离的能力,使得那些被隔离的其他功能无法从密码模块中获取与关键安全参数相关的信息,而且除了密码模块自身提供的接口以外,无法通过其他途径修改密码模块的关键安全参数、公开安全参数或执行流。可能需要对运行环境进行特定的配置,以充分保护密码模块的代码和数据(例如,禁止密码模块进行特定类型的内部进程通信,或者为含有密码模块敏感安全参数或代码的文件分配限制性访问权限)。

表 2 提供了一些运行环境的示例。

表 2 运行环境示例

配置示例	运行环境
计算平台不允许加载代码,且不允许操作员修改操作系统或密码模块的配置	不可修改
计算平台包含允许加载额外代码的操作系统,该代码已通过鉴别且满足本标准中所有适用要求	受限制
计算平台允许加载代码,该代码不需满足本标准的软件或固件加载要求	可修改
计算平台上的操作系统可由操作员配置,允许移除安全保护	可修改

对于不可修改或受限制的运行环境,用于保证该环境不可修改或受限制的控制部件可以包括计算平台的、操作系统的或密码模块本身的属性,或者包括上述全部的属性。

在不可修改或受限制的环境下执行的代码在本标准中被视为固件。在可修改的环境下执行的代码在本标准中被视为软件。

如果运行环境是不可修改或受限制的,7.6.2 中规定的操作系统要求应[06.01]适用。

如果运行环境是可修改的,7.6.3 中规定的操作系统要求应[06.02]适用。

密码模块文档应[06.03]按照 A.2.6 中规定的要求编写。

7.6.2 受限或不可修改运行环境的操作系统要求

除了 7.6.1 中规定的通用安全要求，针对受限或不可修改运行环境的操作系统还规定了下列要求：

a) 安全一级：

如果密码模块在 7.7 中达到安全一级，则 7.6.3 中规定的安全一级的要求应[06.04]适用。

b) 安全二级、安全三级、安全四级：

没有额外的要求。

7.6.3 可修改运行环境的操作系统要求

除了 7.6.1 中规定的通用安全要求，针对可修改运行环境的操作系统还规定了下列要求：

a) 安全一级：

下列要求适用于安全一级密码模块的操作系统：

——每一个密码模块的实例应[06.05]能够控制和支配自己的敏感安全参数。

——运行环境应[06.06]提供应用进程间相互隔离的能力，以阻止进程间对关键安全参数不受控的访问以及对敏感安全参数不受控的修改，无论关键安全参数和敏感安全参数是在进程内存中还是存储在运行环境内的永久性存储体中。这保证了只有密码模块和运行环境的可信部分可以直接访问敏感安全参数。对运行环境配置的规定应[06.07]记录在密码模块的安全策略中。

——如果密码模块产生进程，其产生的进程应[06.08]由密码模块自己所有，并且不由除密码模块所在进程外的其他进程/操作员所有。

不能通过管理文档和流程来实施这些要求，而是应由密码模块本身来实施。

b) 安全二级：

对于安全二级，除了安全一级的要求以外，操作系统还应[06.09]满足下列要求或者经确认机构许可：

——密码模块所在的进程应[06.10]由密码模块自己所有，并且与包括调用者进程在内的其他进程逻辑隔离。

——所有密码软件、敏感安全参数、控制和状态信息应[06.11]在操作系统的控制之下。操作系统实现了基于角色的访问控制，或者实现了自主访问控制，该自主访问控制可通过访问控制列表(ACL)来定义新的组和分配权限，并且能够给每个用户分配多个组。操作系统应[06.12]正确配置，以防止非授权地执行、修改和读取敏感安全参数、控制和状态数据。

——为了保护明文数据、密码软件、敏感安全参数和鉴别数据，操作系统具备以下访问控制机制或能支持以下访问控制机制的实现：

- 应[06.13]能够通过配置，对角色或组赋予仅能执行密码模块中密码软件的权限。
- 应[06.14]能够通过配置，对角色或组赋予仅能修改(写、替换和删除)存储在密码边界内软件和数据的权限，这些软件和数据包括执行密码功能的程序、密码操作相关数据(例如，密码操作的审计数据)、敏感安全参数和明文数据。
- 应[06.15]能够通过配置，对角色或组赋予仅能读取密码操作相关数据(例如，密码操作的审计数据)、关键安全参数和明文数据的权限。
- 应[06.16]能够通过配置，对角色或组赋予仅能导入敏感安全参数的权限。

——下列规定应[06.17]与密码模块安全策略文档中已定义的角色和服务相一致：

- 当密码模块不支持维护员角色时，操作系统应[06.18]防止所有操作员和运行的进程访问、使用、泄露、修改和替换正在运行的密码进程(例如，已加载的和正执行的密码

程序镜像)。在这种情况下,运行的进程是指所有不由操作系统所拥有或启动的进程(例如,由操作员启动的进程),无论该进程是密码相关的还是非密码相关的。

- 操作系统应[06.19]防止用户进程对其他进程的敏感安全参数以及系统敏感安全参数进行读或写操作。
- 满足以上要求的操作系统配置应[06.20]在管理员指南中阐明。管理员指南指的是密码主管和/或其他管理角色使用的书面资料,用于正确地配置、维护和管理密码模块。管理员指南应[06.21]声明:操作系统应按照需要保护的密码模块内容所指定的要求进行配置。

操作系统的身份标识和鉴别机制应[06.22]满足 7.4.4 中规定的要求,并在密码模块安全策略文档中具体阐明。

所有密码软件、敏感安全参数、控制和状态信息应[06.23]在操作系统的控制之下,操作系统应[06.24]至少拥有以下属性:

——操作系统应[06.25]提供具有审计事件日期和时间的审计机制。密码模块应[06.26]不把敏感安全参数写入任何审计记录中。

——下列事件应[06.27]被操作系统的审计机制记录下来:

- 修改、访问、删除以及添加密码操作相关数据和敏感安全参数;
- 尝试对密码主管功能提供无效输入;
- 将操作员添加至密码主管角色或将其删除(如果那些角色是由密码模块管理的);
- 使用安全相关的密码主管功能;
- 请求访问与密码模块相关的鉴别数据;
- 使用与密码模块相关的鉴别机制(例如,登录);
- 显式的请求担任密码主管角色。

——操作系统的审计机制应[06.28]能够审计下列操作系统相关事件:

- 操作员对审计数据的所有读写访问;
- 访问密码模块用于存储密码操作相关数据或敏感安全参数的文件;
- 将操作员添加至密码主管角色或将其删除(如果那些角色是由密码模块管理的);
- 对鉴别数据管理机制的使用请求;
- 当该安全等级支持可信信道时,对可信信道功能的使用请求,无论请求是否被批准;
- 当该安全等级支持可信信道时,可信信道的启动方和接收方的身份标识。

——操作系统应[06.29]正确配置以防止操作员,除安全策略中给出的、拥有特权的操作员以外,修改存储在密码模块运行环境中的密码模块软件和审计数据。

无论密码模块是否在核准的工作模式下运行,应[06.30]只有配置成满足以上安全要求的操作系统才符合该安全等级。操作系统宜使用核准的安全功能对审计记录进行保护,以防止非授权的修改。

c) 安全三级和安全四级

本标准对可修改运行环境的操作系统不提供安全三级和安全四级的要求。因此,可修改运行环境的操作系统无法达到安全三级和安全四级。

7.7 物理安全

7.7.1 物理安全实体

密码模块应[07.01]采用物理安全机制以限制对密码模块内容的非授权物理访问,并阻止对已安装密码模块的非授权使用或修改(包括整个密码模块的替换)。密码边界内的所有硬件、软件、固件、数据

分量以及敏感安全参数应[07.02]受到保护。

若密码模块完全由软件实现，使得物理安全仅由计算平台提供，那么该密码模块将不受本标准物理安全要求的限制。

本条中的要求应[07.03]适用于硬件和固件密码模块，以及混合密码模块中的硬件和固件部件。

本条的要求应[07.04]适用于已定义的密码模块物理边界。

物理安全要求是针对下列三类密码模块物理实体做出规定的：

——单芯片密码模块是指由单个集成电路(IC)芯片构成的密码模块，该芯片可以作为独立密码模块使用，或者可以嵌入到一个可能没有物理保护的外壳或产品内。单芯片密码模块的例子有单 IC 芯片和单 IC 芯片智能卡。

——多芯片嵌入式密码模块是指由两个或多个互相连接的 IC 芯片构成的密码模块，这些芯片嵌入到一个可能没有物理保护的外壳或产品内。多芯片嵌入式密码模块的例子有适配器和扩展板。

——多芯片独立式密码模块是指由多个互相连接的 IC 芯片构成的密码模块，该密码模块的整个外壳受到物理保护。多芯片独立密码模块的例子有加密路由器、安全无线电话和 USB 令牌。

依据密码模块的物理安全机制，企图进行非授权物理访问、使用或修改的行为应[07.05]在以下时间点以很高的概率被检测到：

——在上述企图行为之后，通过其留下的可见标志(例如，拆卸证据)，和/或

——在上述企图行为过程中。

并且密码模块应[07.06]立即采取恰当的措施保护敏感安全参数。

表 3 总结了物理安全的要求，分别针对 4 个安全等级列出了通用的要求以及针对三类特定实体的要求。对于特定实体，每一安全等级在同一等级的通用要求以及前一等级的特定实体的要求之上，进一步增强了安全要求。

表 3　物理安全要求总结

安全等级	所有实体的通用要求	单芯片密码模块	多芯片嵌入式密码模块	多芯片独立密码模块
安全一级	产品级部件； 标准钝化处理； 当访问维护访问接口时，按照规定的程序置零或自动置零	无额外要求	产品级的外壳或封盖	产品级的外壳或封盖
安全二级	显示拆卸的证据； 在可见光谱下不透明或半透明； 防止通过孔或缝直接观察	芯片或外壳上拆卸存迹的涂层	拆卸存迹的封装材料或外壳，其门上、封盖上带有拆卸存迹的封条或防撬锁	拆卸存迹的封装材料或外壳，其门上、封盖上带有拆卸存迹的封条或防撬锁
安全三级	拆卸响应与置零电路； 当访问维护访问接口时，自动置零； 防止通过孔和缝进行探测； 针对温度和电压的 EFP 或 EFT	芯片上拆卸存迹的硬质涂层，或者抗擦除、抗穿透的坚固外壳	拆卸存迹的硬质封装材料或坚固外壳	拆卸存迹的硬质封装材料或坚固外壳
安全四级	拆卸检测和响应封套； 针对温度与电压的 EFP； 针对故障注入的保护	芯片上抗移除的硬质涂层	拆卸检测和具有置零能力的响应封套	拆卸检测和具有置零能力的响应封套

总体而言，安全一级提出了最基本的安全要求。安全二级增加了拆卸存迹机制的要求，以及确保无法对密码模块关键区域的内部操作收集信息的要求。安全三级增加了使用坚固或硬质的保形或非保形外壳的要求，要求外壳的封盖和门具有拆卸检测和响应机制，并且要求抵抗通过开口或入口的直接探测。安全三级还要求具备环境失效保护(EFP)或环境失效测试(EFT)。安全四级进一步增加了使用坚固或硬质的保形或非保形外壳的要求，要求整个外壳具有拆卸检测和响应机制。安全四级还要求具备环境失效保护，以及防止故障注入攻击。

当密码模块被设计成允许物理访问(例如，被密码模块厂商或其他授权个体访问)时，需要为维护访问接口规定安全要求。拆卸检测和拆卸响应并不能代替显式的拆卸证据。

密码模块文档应[07.07]按照 A.2.7 中规定的要求编写。

7.7.2 通用物理安全要求

下列要求应[07.08]适用于所有密码模块物理实体：

——密码模块文档应[07.09]阐述密码模块的物理实体以及所实现的物理安全机制达到的安全等级。

——每当为物理安全进行置零操作时，应[07.10]在极短的时间内执行置零，以防止敏感数据在检测到拆卸行为与密码模块置零之间泄露出去。

——如果密码模块包含的维护角色需要对密码模块内容进行物理访问，或者密码模块被设计成允许物理访问(例如，被密码模块厂商或其他授权个体访问)，那么：

- 应[07.11]定义维护访问接口。
- 维护访问接口应[07.12]包括所有通向密码模块内容的物理访问路径，包括任何封盖或门。
- 维护访问接口内包含的任何封盖或门应[07.13]使用适当的物理安全机制来进行安全保护。

密码模块的通用物理安全要求包括：

a) 安全一级

下列要求应[07.14]适用于安全一级的所有密码模块：

——密码模块应[07.15]由产品级部件组成，这些产品级部件采用了标准钝化技术，例如，对整个密码模块电路使用保形涂料或封闭底漆，以防止环境损害或其他物理损害。

——当维护密码模块时，应[07.16]由操作员按照规定的程序执行置零，或由密码模块自动执行。

b) 安全二级

除了安全一级的通用要求，安全二级的所有密码模块还应[07.17]满足下列要求：

——在尝试物理访问密码模块时，密码模块应[07.18]提供显式的拆卸证据(例如，在封盖、外壳或封条上)。

——拆卸存迹的材料、涂层或外壳应[07.19]在可见光谱内(即波长范围为 400 nm～750 nm)是不透明或者半透明的，从而防止对密码模块关键区域的内部操作进行信息收集。

——如果密码模块包含通风孔或缝，那么孔或缝应[07.20]具有特殊的构造，从而防止通过直接观察密码模块内部的构造或部件进行信息收集。上述直接观察利用了密码模块内部结构或部件发出的可见光。

c) 安全三级

除了对安全一级和安全二级的通用要求，安全三级的所有密码模块还应[07.21]满足下列要求：

——如果密码模块含有任何门或封盖，或者定义了维护访问接口，那么密码模块应[07.22]包含拆卸响应与置零电路。在打开门、封盖或维护访问接口时，拆卸响应与置零电路应[07.

23]立即置零所有未受保护的敏感安全参数。当密码模块内包含未受保护的敏感安全参数时，拆卸响应与置零电路应[07.24]保持运行状态。

——如果密码模块含有通风孔或缝，那么孔或缝应[07.25]具有特殊的构造，从而防止未被检测到的对密码模块内部的物理探测(例如，防止使用单铰链探头探测)。

——当密码模块温度超出运行、存放和分发的预期温度范围时，坚固或硬质的保形或非保形的外壳、涂层或灌封材料应[07.26]维持强度和硬度特征。

——如果使用了拆卸封条，那么应[07.27]使用被唯一编号或者能够独立识别的封条(例如，唯一编号的存迹胶带或可唯一识别的手写封条)。

——密码模块应[07.28]具有 EFP 特性或经过 EFT。

d) 安全四级

除了安全一级、安全二级和安全三级的通用要求，安全四级的所有密码模块还应[07.29]满足下列要求：

——密码模块应[07.30]使用抗移除的硬质不透明涂层或具有拆卸响应和置零能力的拆卸检测封套保护起来。

——密码模块应[07.31]具有 EFP 特性。

——密码模块应[07.32]提供保护措施，以防止故障注入攻击。故障注入攻击的缓解技术以及采用的缓解指标应[07.33]在文档中按照附录 B 规定的要求进行记录。

7.7.3 物理安全实体的物理安全要求

7.7.3.1 单芯片密码模块

除了 7.7.2 中规定的通用安全要求，还针对单芯片密码模块规定了下列要求：

a) 安全一级：

对安全一级的单芯片密码模块没有其他额外要求。

b) 安全二级：

除了安全一级的要求，安全二级的单芯片密码模块还应[07.34]满足下列要求：

——应[07.35]使用拆卸存迹涂层(例如，拆卸存迹的钝化材料或覆盖在钝化层上的拆卸存迹材料)把密码模块覆盖起来，或者将密码模块装在一个拆卸存迹的外壳中，以阻止直接观察、探测或操控密码模块，并在企图拆卸或移动密码模块后留下证据。

c) 安全三级：

除了安全一级和安全二级的要求，安全三级的单芯片密码模块还应[07.36]满足下列要求：

——应[07.37]使用拆卸存迹的硬质不透明涂层(例如，涂在钝化层上的硬质不透明环氧树脂)把密码模块覆盖起来。或

——应[07.38]实现密码模块的外壳，以致企图或穿透外壳的行为应[07.39]极有可能对密码模块造成严重损害，即密码模块将不能工作。

d) 安全四级：

除了安全一级、安全二级和安全三级要求，安全四级的单芯片密码模块还应[07.40]满足下列要求：

——应[07.41]使用抗移除的硬质不透明涂层将密码模块覆盖起来，该涂层具有硬度与黏力特性，以致企图剥落或撬开涂层的行为将极有可能对密码模块造成严重损害，即密码模块将不能工作。

——抗移除的涂层应[07.42]具有溶解特性，以致企图溶解涂层的行为将极有可能溶解或严重损害密码模块，即密码模块将不能工作。

7.7.3.2 多芯片嵌入式密码模块

除了 7.7.2 中规定的通用安全要求，还针对多芯片嵌入式密码模块规定了下列要求：

a) 安全一级：

如果密码模块被装在一个外壳或封盖中，那么应[07.43]使用产品级的外壳或封盖。

b) 安全二级：

除了安全一级的要求，安全二级的多芯片嵌入式密码模块还应[07.44]满足下列要求：

——应[07.45]使用拆卸存迹的涂层或灌封材料(例如，耐腐蚀涂层或防渗透涂料)把密码模块部件覆盖起来，以阻止直接观察，并提供企图拆卸或移动密码模块部件的证据。或

——密码模块应[07.46]被整个地包在金属或硬质塑料的产品级外壳中，该外壳可以有门或封盖。如果外壳包含任何门或封盖，则门或封盖应[07.47]使用带有物理或逻辑钥匙的防撬锁，或者应[07.48]被拆卸存迹的封条保护起来(例如，存迹胶带或全息封条)。

c) 安全三级：

除了安全一级和安全二级的要求，下列要求应[07.49]适用于安全三级的多芯片嵌入式密码模块：

——应[07.50]使用硬质涂料或灌封材料(例如，硬质环氧树脂材料)把密码模块内的多芯片实体电路覆盖起来。或

——密码模块应[07.51]被封装在坚固的外壳内。以致企图移除或穿透外壳的行为将极有可能对密码模块造成严重损害，即密码模块将不能工作。

d) 安全四级：

除了安全一级、安全二级和安全三级的要求，下列要求应[07.52]适用于安全四级的多芯片嵌入式密码模块：

——密码模块部件应[07.53]封装在坚固或硬质的保形或非保形的外壳中。外壳应[07.54]用拆卸检测封套(例如，带有蛇形导线的柔性聚酯薄膜印制电路，或绕线式的包装，或无弹性易碎电路，或坚固的外壳)封装起来，该封套应[07.55]能够检测到企图访问敏感安全参数的拆卸行为，包括切、钻、磨、碾、烧、熔、溶解灌封材料或外壳等。

——密码模块应[07.56]包含拆卸响应和置零电路。拆卸响应和置零电路应[07.57]能够持续地监控拆卸检测封套，并且一旦检测到拆卸行为就应[07.58]立即置零所有未受保护的敏感安全参数。当密码模块内包含未受保护的敏感安全参数时，拆卸响应电路应[07.59]保持运行状态。

7.7.3.3 多芯片独立式密码模块

除了 7.7.2 中规定的通用安全要求，针对多芯片独立式密码模块还规定了下列要求：

a) 安全一级：

密码模块应[07.60]整个被封装在金属或硬质塑料的产品级外壳内，外壳可以有门或封盖。

b) 安全二级：

除了安全一级的要求，安全二级的多芯片独立式密码模块还应[07.61]满足下列要求：

——如果密码模块的外壳含有任何门或封盖，那么门或封盖应[07.62]安装带有物理或逻辑钥匙的防撬机械锁，或者应[07.63]使用拆卸存迹的封条(例如，存迹胶带或全息封条)进行保护。

c) 安全三级：

除了安全一级和安全二级的要求，安全三级的多芯片独立密码模块还应[07.64]满足下列要求：

——密码模块应[07.65]被封装在坚固的外壳内，以致企图移除或穿透外壳的行为将极有可能对密码模块造成严重损害，即密码模块将不能工作。

d) 安全四级：

除了安全一级、安全二级和安全三级的要求，安全四级的多芯片独立式密码模块还应[07.66]满足下列要求：

——密码模块的外壳应[07.67]封装在使用下列一种或多种拆卸检测机制的拆卸检测封套内，拆卸检测机制包括：封盖开关(如微型开关、磁霍尔效应开关、永磁驱动器等)、动作探测器(如超声波、红外线、微波探测器)或者 7.7.3.2 中规定的安全四级描述的其他拆卸检测机制。拆卸检测机制应[07.68]能够对企图访问敏感安全参数的攻击做出响应，诸如切、钻、铣、磨、烧、熔、溶解等。

——密码模块应[07.69]包含拆卸响应和置零电路。拆卸响应和置零电路应[07.70]能够持续地监控拆卸检测封套，并且一旦检测到拆卸行为就应[07.71]立即置零所有未受保护的敏感安全参数。当密码模块内包含未受保护的敏感安全参数时，拆卸响应和置零电路应[07.72]保持运行状态。

7.7.4 环境失效保护(测试)

7.7.4.1 环境失效保护(测试)通用要求

电子设备和电路都被设计成在特定的环境条件范围内运行。故意或意外超出密码模块正常运行电压和温度范围，会导致电子设备或电路运行不稳定，也可能会导致电子设备或电路失效，从而危及密码模块的安全。密码模块具有环境失效保护(EFP)特性或者经过环境失效测试(EFT)，都能够合理地保证密码模块的安全性不被极端的环境条件所破坏。

对于安全一级、安全二级，密码模块不要求具有 EFP 特性或经过 EFT。安全三级的密码模块应[07.73]具有 EFP 特性或经过 EFT。安全四级的密码模块应[07.74]具有 EFP 特性。

7.7.4.2 环境失效保护特性

EFP 特性应[07.75]保护密码模块，防止由于故意或意外超出密码模块正常运行范围，对密码模块的安全性造成破坏。

密码模块应[07.76]对超出阐明的正常运行的温度和电压范围进行监控并做出正确响应。

如果温度或电压超出密码模块的正常运行范围，则保护电路应[07.77]：

——关闭密码模块，防止继续运行。或

——立即置零所有未受保护的敏感安全参数。

7.7.4.3 环境失效测试程序

EFT 应[07.78]对密码模块进行分析、仿真和测试，从而提供合理的保障，确保密码模块的安全性不会因密码模块温度和电压超出正常运行范围(故意的或意外的)而遭到破坏。

EFT 应[07.79]表明：如果密码模块的运行温度或电压超出正常运行范围并引起故障，密码模块的安全性应[07.80]不会遭到破坏。

温度范围应[07.81]按照下列方式测试：从正常运行温度范围内下降到最低温度，此时要么密码模块关闭防止继续运行，要么立即置零所有未受保护的敏感安全参数；并且应从正常运行温度范围内上升到最高温度，此时要么密码模块关闭防止继续运行，要么立即置零所有未受保护的敏感安全参数。温度的测试范围应[07.82]为－100 ℃～＋200 ℃；而且，一旦密码模块被关闭以防止继续运行，或所有未受保护的敏感安全参数被立即置零，或密码模块进入故障模式，则测试应[07.83]立即中断。应[07.84]在

敏感部件和关键设备处，而不仅在物理边界上，对温度进行内部实时监测。

电压范围应[07.85]按照下列方式测试：逐渐从正常运行电压范围内下降到最低电压，此时要么密码模块关闭防止继续运行，要么立即置零所有未受保护的敏感安全参数；并且应[07.86]逐渐从正常运行电压范围内上升到最高电压，此时要么密码模块关闭防止继续运行，要么立即置零所有未受保护的敏感安全参数。

7.8 非入侵式安全

非入侵式攻击是指没有通过物理方式修改或入侵密码模块就可以获取密码模块关键安全参数相关信息，从而破坏密码模块安全性的一种攻击手段。密码模块可以实现各种技术来缓解这些类型的攻击。对于本标准提出的每一个安全功能，其对应的非入侵式攻击的缓解检测指标应符合国家相关部门的有关要求。

如果由密码模块实现、用于保护密码模块关键安全参数的非入侵式攻击的缓解技术不在附录 F 中，则这些技术应[08.01]满足 7.12 中规定的要求。

如果由密码模块实现、用于保护密码模块关键安全参数的非入侵式攻击的缓解技术在附录 F 中，则这些技术应[08.02]满足下列要求。

密码模块文档应[08.03]按照 A.2.8 中规定的要求编写。

针对非入侵式安全还规定了下列要求：

a) 安全一级和安全二级：

对于安全一级和安全二级，文档应[08.04]阐明用于保护密码模块关键安全参数免受附录 F 中的所有非入侵式攻击的缓解技术。如果有相应措施，文档应[08.05]包括可以证明每个缓解技术有效性的证据。

b) 安全三级：

对于安全三级，除了安全一级和安全二级的要求，密码模块应[08.06]实现用于保护密码模块关键安全参数免受附录 F 中的所有非入侵式攻击的缓解技术，文档应[08.07]包括可以证明每个缓解技术有效性的证据，并提供检测方法。

c) 安全四级：

对于安全四级，除了安全一级、安全二级和安全三级的要求，密码模块应[08.08]接受检测以满足附录 F 的要求。

7.9 敏感安全参数管理

7.9.1 敏感安全参数管理通用要求

敏感安全参数包括关键安全参数和公开安全参数。敏感安全参数管理的安全要求涵盖了密码模块中敏感安全参数的整个生命周期。敏感安全参数管理包括随机数生成器、敏感安全参数生成、敏感安全参数建立、敏感安全参数输入和输出、敏感安全参数存储以及未受保护的敏感安全参数置零。

加密的关键安全参数是指使用核准的安全功能加密的关键安全参数。在本标准范围内，采用非核准的安全功能加密的关键安全参数在本标准中被视为未受保护的明文。

关键安全参数应[09.01]在密码模块内受保护以防止非授权的访问、使用、泄露、修改和替换。

公开安全参数应[09.02]在密码模块内受保护以防止非授权的修改和替换。

密码模块应[09.03]将生成的、输入或输出密码模块的敏感安全参数，与该敏感安全参数相应的实体(即人、组、角色、或进程)关联起来。

口令的杂凑值、随机数生成器状态信息和密钥生成的中间值应[09.04]被视为需要受保护的关键安全参数。

密码模块文档应[09.05]按照 A.2.9 中规定的要求编写。

7.9.2 随机数生成器

密码模块可以包含随机数生成器、随机数生成器链，或者其自身就是一个随机数生成器。附录 C 中列出了国家密码管理主管部门对核准的随机数生成器的要求。

如果核准的安全功能、敏感安全参数生成或敏感安全参数建立方法需要随机值，则应[09.06]使用核准的随机数生成器提供这些值。

如果熵是从密码边界外部收集的，那么使用该熵作为输入所生成的数据流应[09.07]被视为关键安全参数。对任何一个关键安全参数，无论熵从密码边界内部还是外部收集，收集的最小熵值应[09.08]不小于 256 比特且不小于关键安全参数的比特长度。如果熵从内部收集，还应[09.09]描述随机数的产生原理。

7.9.3 敏感安全参数的生成

敏感安全参数可以由密码模块内部生成，也可以由输入到密码模块的敏感安全参数衍生。

如果敏感安全参数的生成使用了核准随机数生成器的输出，破坏该方法的安全性(例如，猜测用于初始化确定性随机数生成器的种子值)应[09.10]至少与猜测已生成的敏感安全参数值的代价相当。

密码模块应[09.11]使用附录 D 中的核准生成方法来生成敏感安全参数，即该敏感安全参数使用核准的随机数生成器输出生成，或者通过核准的安全功能或建立方法，利用导入密码模块的敏感安全参数衍生。

7.9.4 敏感安全参数的建立

敏感安全参数建立可以包括：

——自动的敏感安全参数传输或敏感安全参数协商方法。或

——通过直接或电子方法进行手动的敏感安全参数输入或输出。

自动的敏感安全参数建立应[09.12]使用附录 D 中的核准方法。手动的敏感安全参数建立应[09.13]满足 7.9.5 中规定的要求。

7.9.5 敏感安全参数的输入和输出

敏感安全参数可以手动输入到密码模块或从密码模块输出，手动输入输出可以是直接的(例如，通过键盘或数字键盘输入，或通过显示器输出)，也可以是电子的(例如，通过智能卡/令牌、PC 卡、其他电子密钥加载设备，或密码模块操作系统)。如果敏感安全参数是手动输入到密码模块或从密码模块输出，输入或输出应[09.14]通过 7.3.2 中规定的已定义的硬件密码模块接口、软件或固件密码模块接口、混合固件密码模块接口或混合软件密码模块接口。

所有受密码技术保护的敏感安全参数，无论是输入密码模块的或从密码模块输出的，都应[09.15]使用核准的安全功能进行加密。

对于直接输入的敏感安全参数，输入值可以在短暂时间内显示出来，以允许视觉验证以及提高准确度。如果加密的敏感安全参数直接输入到密码模块，则敏感安全参数的明文值不应[09.16]显示出来。直接输入(明文或加密)的敏感安全参数应[09.17]在输入密码模块的过程中，使用 7.10.3.5 中规定的手动输入条件自测试进行验证，以保证准确度。

为了防止不经意地输出敏感信息，应[09.18]需要两个独立的内部操作来执行任意明文关键安全参数的输出。这两个独立的内部操作应[09.19]专门用于共同控制关键安全参数的输出。

对于通过无线连接的电子输入或输出，密钥分量、鉴别数据以及其他关键安全参数应[09.20]经过加密。

手动输入公开安全参数无需采用密码技术进行鉴别。

针对敏感安全参数的输入和输出还规定了下列要求：

a) 安全一级和安全二级：

明文密钥分量、鉴别数据以及其他关键安全参数可以通过物理端口和逻辑接口输入和输出，这些端口和接口可以是与密码模块的其他端口和接口共享的。

对于软件密码模块或混合软件密码模块的软件部件，密钥分量、鉴别数据以及其他关键安全参数可以以加密或明文的形式输入或输出，前提是密钥分量、鉴别数据以及其他关键安全参数应[09.21]只保留在该运行环境中，并满足 7.6.3 中规定的要求，防止非授权的访问、使用、泄露、修改和替换。

b) 安全三级：

对于安全三级，除了安全一级和安全二级的要求，密钥分量、鉴别数据以及其他关键安全参数应[09.22]以加密的形式或通过可信信道输入或输出密码模块。

作为关键安全参数，明文形式的对称密钥和私钥应[09.23]使用知识拆分过程，并使用可信信道输入或输出密码模块。

如果密码模块使用了知识拆分过程，密码模块应[09.24]使用基于身份的操作员鉴别，分别鉴别每个密钥分量的输入或输出，而且应[09.25]至少需要两个密钥分量来重建原来的密钥。

c) 安全四级：

对于安全四级，除了安全三级的要求，密码模块应[09.26]使用基于身份的多因素操作员鉴别，分别鉴别每个密钥分量的输入或输出。

7.9.6 敏感安全参数的存储

密码模块中敏感安全参数可以以明文形式或加密形式存储。密码模块应[09.27]将敏感安全参数的存储与相应的实体(例如，操作员、角色或进程)关联起来。

密码模块应[09.28]禁止非授权操作员访问明文关键安全参数。应[09.29]禁止非授权操作员修改公开安全参数。

针对敏感安全参数的储存还规定了下列要求：

a) 安全一级：

密码模块可以利用运行环境的安全机制，保护存储的敏感安全参数。

b) 安全二级、安全三级和安全四级：

密码模块应[09.30]使用不依赖于运行环境的安全机制，保护存储的敏感安全参数。

7.9.7 敏感安全参数的置零

密码模块应[09.31]提供密码模块内所有未受保护的敏感安全参数和密钥分量的置零方法。临时存储的敏感安全参数在使用之后，若在合理的时间内不再使用，宜被置零。

敏感安全参数被置零之后应[09.32]无法从密码模块中恢复和重用。

受保护的公开安全参数、加密的关键安全参数、受其他经确认的嵌入式密码模块(满足本标准要求)在逻辑或物理上保护的关键安全参数，不要求被置零。

只用于 7.10 中规定的自测试目的的参数无须满足置零要求。

针对敏感安全参数的置零还规定了下列要求：

a) 安全一级：

未受保护的敏感安全参数的置零可以由密码模块管理员按照规定的程序执行，而且不依赖于密码模块控制(例如，硬盘格式化等)。

b) 安全二级和安全三级：

密码模块应[09.33]对未受保护的敏感安全参数执行置零(例如,使用全 0 或全 1 或随机数据覆盖)。置零不应[09.34]使用一个未受保护的敏感安全参数来覆盖另一个未受保护的敏感安全参数。临时敏感安全参数在使用完毕之后应[09.35]被置零。密码模块应[09.36]在置零完成时提供输出状态指示。

c) 安全四级:

除了安全二级和安全三级的要求之外,还应[09.37]满足下列要求:

——置零应[09.38]是及时的、不可中断的,而且应[09.39]发生在足够短的时间内,以防止在开始置零到置零实际完成之间的时间内恢复出敏感数据。

——所有敏感安全参数(无论是明文形式还是密文形式)应[09.40]被置零,使得密码模块恢复到出厂状态。

7.10 自测试

7.10.1 自测试通用要求

密码模块的运行前自测试和条件自测试用于确保密码模块没有故障。所有自测试都应[10.01]被执行,自测试的通过或失败应[10.02]取决于密码模块自身,无论密码模块运行于核准模式还是非核准模式,都不依赖外部控制、外部提供的输入文本向量、预期的输出结果和操作员的干预。

运行前自测试应[10.03]在密码模块提供任何数据输出(通过数据输出接口)之前被执行,并成功通过。

条件自测试应[10.04]在相应的安全功能或过程被调用时执行。

密码模块应[10.05]对其实现的附录 C、附录 D、附录 E 中的密码算法,执行对应的自测试。

除了该标准中规定的测试,密码模块也可以执行其他运行前或关键功能条件自测试。

如果密码模块自测试失败,密码模块应[10.06]进入错误状态,并且应[10.07]按照 7.3.3 中的规定,输出一个错误指示。在错误状态下,密码模块不应[10.08]执行任何密码操作,或通过控制、数据输出接口输出控制和数据。密码模块不应[10.09]使用自测试失败的功能和算法,直至它们重新通过测试。如果密码模块自测试失败时密码模块不输出错误状态,密码模块操作员应[10.10]能够根据在安全策略(附录 B)中阐明的过程,判断该密码模块是否已经进入了错误状态。

在安全三级和安全四级中,密码模块应[10.11]维护错误日志,密码模块的授权管理员可以访问该日志。该错误日志应[10.12]至少提供最近的错误事件(例如,自测试失败)。

密码模块文档应[10.13]按照 A.2.10 中规定的要求编写。

7.10.2 运行前自测试

7.10.2.1 运行前自测试通用要求

运行前自测试是指由密码模块执行的一种测试,在密码模块上电或实例化(关闭、复位、重启、冷启动、供电中断等)之后至密码模块转入到运行状态之前执行。运行前自测试应[10.14]被密码模块执行并成功通过。

密码模块应[10.15]执行下列运行前测试:

——运行前软件/固件完整性测试;

——运行前旁路测试;

——运行前关键功能测试。

7.10.2.2 运行前软件/固件完整性测试

密码边界内的所有软件和固件部件都应[10.16]使用核准的完整性技术进行验证,并满足 7.5 中定

义的要求。如果验证失败,运行前软件/固件完整性测试应[10.17]失败。对于任何不受本标准安全要求约束的软件/固件,或任何存储在不可重配置内存中的可执行代码,不要求执行运行前软件/固件完整性测试。

如果硬件密码模块不包含软件或固件,密码模块应[10.18]至少实现一个 7.10.3.2 中规定的密码算法条件自测试作为运行前自测试。

用于运行前软件/固件测试的核准的完整性技术所使用的密码算法应[10.19]先通过 7.10.3.2 中规定的密码算法条件自测试。

7.10.2.3 运行前旁路测试

如果密码模块实现了旁路能力,那么密码模块应[10.20]确保管理旁路能力的逻辑是正确的。密码模块应[10.21]通过以下方法验证数据路径:

——将旁路开关设置在加密位置,验证通过旁路机制传输的数据是经过加密的。

——将旁路开关设置在非加密位置,验证通过旁路机制传输的数据是没有经过加密的。

7.10.2.4 运行前关键功能测试

其他一些关系到密码模块安全运行的重要安全功能应[10.22]在运行前进行测试。密码模块文档应[10.23]阐明需要在运行前进行测试的关键功能。

7.10.3 条件自测试

7.10.3.1 条件自测试通用要求

在下列测试规定的条件出现时,密码模块应[10.24]执行对应的测试:密码算法自测试、配对一致性测试、软件/固件加载测试、手动输入测试、旁路测试、关键功能测试以及周期自测试。

7.10.3.2 密码算法条件自测试

密码算法条件自测试:应[10.25]针对密码模块实现的每个核准的密码算法的所有密码功能(例如,安全功能、敏感安全参数建立方法、鉴别)进行密码算法测试。在密码算法第一次运行使用之前,应[10.26]执行该条件测试。

密码算法自测试可以是已知答案测试、对比测试或错误检测测试。

已知答案测试包括一组已知的输入向量(例如,数据、密钥生成材料或替代随机数的常量)的集合。这些已知的输入向量通过密码算法运算之后生成结果。将该结果与已知的、预期的输出结果进行比对。如果计算输出不等于已知答案,密码算法已知答案自测试应[10.27]失败。

算法自测试应[10.28]至少针对密码模块支持的最小核准密钥长度、模数长度、素数或曲线等进行测试。

如果算法规定了多个模式(例如,ECB、CBC 等),自测试应[10.29]至少选择其中一个模式,而且这个模式是受密码模块支持的或确认机构规定的。

已知答案测试的例子:

——单向的功能:输入测试向量生成的输出应[10.30]与预期的输出(例如,杂凑、带密钥的杂凑、消息鉴别、随机数生成器(确定的熵向量)、敏感安全参数协商)相等。

——可逆的功能:正向和反向功能都应[10.31]通过自测试(例如,对称密钥的加解密、敏感安全参数传输的加解密、数字签名的产生和验证)。

对比测试将两个或多个独立的密码算法实现的输出进行对比,如果输出不相等,则密码算法对比自测试应[10.32]失败。

错误检测测试利用集成在密码算法实现中的错误检测机制进行算法自测试，如果检测到错误，则密码算法错误检测测试应[10.33]失败。

7.10.3.3 配对一致性条件测试

如果一个密码模块生成公私钥对，配对一致性条件测试应[10.34]对每对生成的公钥和私钥（由附录C、附录D、附录E规定的适用的密码算法生成）执行。

7.10.3.4 软件/固件加载条件测试

如果密码模块可以从外部加载软件或固件，那么除了7.4.3.4中规定的要求，还应[10.35]执行下列要求：

——密码模块应[10.36]实现核准的鉴别技术以验证加载软件或固件是经过确认的。

——核准的鉴别技术所需的鉴别密钥应[10.37]在软件或固件加载之前，独立地加载到密码模块中。

——软件/固件的有效性应[10.38]成功通过核准的鉴别技术的验证，否则软件/固件加载测试应[10.39]失败。如果软件/固件加载测试失败，则不应[10.40]使用加载的软件或固件。

7.10.3.5 手动输入条件测试

如果敏感安全参数或密钥分量手动输入至密码模块，或者由于手动操作失误会导致某些参数错误，则应[10.41]执行以下手动密钥输入测试：

——敏感安全参数或密钥分量应[10.42]使用错误检测码（EDC）或者应[10.43]输入两次。

如果使用了EDC，则EDC的长度应[10.44]至少为16比特。如果EDC验证不符，或者两次输入不相等，那么测试应[10.45]失败。

7.10.3.6 旁路条件测试

如果密码模块实现了旁路能力，即密码模块可以提供不使用加密功能的服务（例如，在密码模块内传输明文），那么应[10.46]执行下列旁路条件测试，以保证密码模块部件的单点失效不会导致不经意地输出明文。

如果密码模块具有旁路开关，当开关在旁路服务和密码服务之间进行切换时，应[10.47]测试其提供密码处理服务的正确性。

如果密码模块可以自动在旁路服务和密码服务之间切换，当管理切换程序的机制（比如源/目的IP地址表）被修改时，应[10.48]测试其提供密码处理服务的正确性。

如果密码模块保存了管理旁路能力的内部信息，那么每当修改管理信息之前，该密码模块应[10.49]采用核准的完整性检测技术来验证管理信息的完整性，并且当修改完毕后，也应[10.50]采用核准的完整性检测技术来产生新的完整性校验值。

7.10.3.7 关键功能条件测试

其他一些关系到密码模块的安全运行的关键安全功能应[10.51]进行条件自测试。

7.10.3.8 周期自测试

针对周期自测试还规定了下列要求：

a) 安全一级和安全二级：

对于安全一级和安全二级，密码模块应[10.52]允许操作员在有周期测试需求的情况下，启动运行前自测试和条件自测试。请求启动周期自测试的方法包括：利用已有自测试服务、复位、

重启、上电循环。

b) 安全三级和安全四级：

除了安全一级和安全二级的要求，密码模块应[10.53]在已定义的时间周期内，自动重复执行运行前或条件自测试，而无需外部的输入或控制。安全策略(附录 B)应[10.54]阐明时间周期以及在重复执行运行前自测试或条件自测试期间可能导致密码模块运行中断的任何条件。例如，如果密码模块正在执行关键任务服务，该服务不能被中断，而启动运行前自测试的时间周期已过；自测试可能要等到又一个时间周期过去之后才执行。

7.11 生命周期保障

7.11.1 生命周期保障通用要求

生命周期保障是指密码模块厂商在密码模块的设计、开发、操作和生命终止期间使用最佳方法，以保障密码模块被正确地设计、开发、测试、配置、配送、安装和废弃，并保障密码模块配有适当的操作员管理文档。安全要求分别针对配置管理、设计、有限状态模型(FSM)、开发、测试、配送和操作以及指南文档做出规定。

密码模块文档应[11.01]按照 A.2.11 中规定的要求编写。

7.11.2 配置管理

配置管理阐述了密码模块厂商所实现的配置管理系统的安全要求。配置管理系统指的是通过控制密码模块的硬件、软件和文档的修改，实现对密码模块安全特性与安全保障进行管理的系统。使用配置管理系统的目的是为了防止意外或非授权地修改密码模块及其相关文档，并为密码模块及其相关文档的更改提供可追溯性。配置管理系统应通过严格的管理控制措施来控制密码模块和相关文档的优化与修改，从而保证密码模块的完整性。

针对配置管理还规定了下列要求：

a) 安全一级和安全二级：

安全一级和安全二级的密码模块应[11.02]满足下列安全要求：

——密码模块及其部件的开发过程以及相关文档都应[11.03]使用配置管理系统管理。

——每个配置条目(例如，密码模块、密码模块硬件部分、密码模块软件部件、密码模块 HDL、用户指南、安全策略等)的每个版本，都应[11.04]被分配并标注一个唯一的身份标识码。

——在经确认的密码模块的整个生命周期中，配置管理系统应[11.05]追踪并维护标识和版本的更改或每个配置条目的修订。

b) 安全三级和安全四级：

除了安全一级和安全二级要求，还应[11.06]使用自动的配置管理系统对配置条目进行管理。

7.11.3 设计

设计是密码模块功能规格的工程解决方案。功能规格指的是对端口和接口的高层描述，以及对密码模块行为的高层描述。设计的目的是用于保障密码模块的功能与安全策略中描述的预期功能相一致。

密码模块应[11.07]设计成允许测试所提供的所有安全相关服务。

7.11.4 有限状态模型

密码模块的运行应[11.08]使用 FSM(或同等模型)来说明，该 FSM 是用状态转移图、状态转移表和状态描述来表示的。FSM 应[11.09]足够详细，以证明密码模块符合本标准的所有要求。

密码模块的 FSM 应[11.10]至少包括下列运行状态和错误状态：

电源开启/关闭状态：密码模块的一种状态，此时密码模块处于电源关闭状态，或者处于待机模式（维持易失性存储器中存储的数据），或处于某种保存在非易失性存储器的运行状态（例如，休眠模式）。在这种状态下，密码模块可使用主、副或备用电源。该状态可以通过密码模块所使用的电源来区分。对于软件密码模块而言，开启电源则是指产生密码模块的可执行映像。

初始化状态：在密码模块转换到核准的状态之前，密码模块执行初始化所处的状态。

密码主管状态：执行密码主管服务的状态（例如，密码初始化、安全管理和密钥管理）。

关键安全参数输入状态：将关键安全参数输入至密码模块时所处的状态。

用户状态（若实现了用户角色）：授权用户获得安全服务、执行密码操作或执行其他核准的功能所处的状态。

核准的状态：执行核准的安全功能时所处的状态。

自测试状态：密码模块正在执行自测试时所处的状态。

错误状态：当密码模块遇到错误状况（例如，自测试失败）时所处的状态。单个密码模块错误状态可以由一个错误状况引起，也可以由多个错误状况引起。错误状态可以包括：表明有设备故障的“硬”错误，这类错误出现时，密码模块可能需要进行维护、保养或修理；或者是可恢复的“软”错误，这类错误出现时，密码模块可能需要初始化或重启。除了那些需要维护、保养或修理密码模块的“硬”错误所导致的错误状态，从错误状态中恢复过来应[11.11]是可以做到的。

每个不同的密码模块服务、安全功能使用、错误状态、自测试或操作员鉴别应[11.12]作为一个独立的状态来描述。

除密码主管以外，任何其他角色应[11.13]被禁止转换成密码主管状态。

密码模块还可以包含其他状态，例如下列两种状态，但不限于此：

旁路状态：密码模块的一种状态，此时由于密码模块配置改变或操作员干预，导致服务将原本正常情况下应以加密形式输出的特定数据或状态项，以明文形式输出。

不活动状态：密码模块静止（例如，低功耗、待机或休眠）的状态。

7.11.5 开发

密码模块应具有严格合规的开发过程，以确保：密码模块的实现与密码模块功能定义和安全策略相一致；密码模块是可维护的；经确认的密码模块是可再生产的。本条规定了密码模块在各个抽象层次上的安全要求，包括从功能规格到具体实现：

a) 安全一级：

安全一级的密码模块应[11.14]满足下列安全要求：

——如果密码模块包含软件或固件，那么源代码、编程语言、编译器、编译器版本和编译器选项、链接器和链接器选项、运行时库和运行时库设置、配置设置、生成过程和方法、生成选项、环境变量以及所有用于编译和链接源代码使其成为可运行形式的其他资源，都应[11.15]使用配置管理系统进行追踪。

——如果密码模块包含软件或固件，那么源代码应[11.16]用注释进行标注，注释应描述出软件或固件与密码模块设计的对应关系。

——如果密码模块包含硬件，若适用的话，文档应[11.17]阐明电路图和/或硬件描述语言（HDL）。

——如果密码模块包含硬件，HDL 代码应[11.18]用注释进行标注，注释应描述出硬件与密码模块设计的对应关系。

——对于软件和固件密码模块以及混合密码模块中的软件或固件部件：

- 7.5 和 7.10 中规定的完整性和验证技术机制的结果，应[11.19]在密码模块开发过程

中，由厂商计算并集成到软件或固件密码模块内。

- 密码模块文档应[11.20]阐明将源代码编译为可运行形式代码所使用的编译器、配置设置以及方法。
- 密码模块应[11.21]使用产品级的开发工具(例如，编译器)进行开发。

b) 安全二级和安全三级：

除了安全一级的要求，安全二级和安全三级的密码模块还应[11.22]满足下列安全要求：

——密码模块内所有软件或固件应[11.23]采用高级非私有语言实现。如果低级语言对密码模块的性能有重要作用或在高级语言无法使用的情况下，应[11.24]在使用低级语言(例如，汇编语言或微指令)时给出根据。

——密码模块内的定制集成电路应[11.25]采用高级硬件描述语言(HDL)实现(例如，VHDL或 Verilog)。

——密码模块内所有软件和固件的设计和实现应[11.26]避免使用对密码模块功能和运行不必要的代码、参数或符号。

c) 安全四级：

除了安全一级、安全二级和安全三级的要求，安全四级的密码模块还应[11.27]满足下列安全要求：

——对于每个密码模块的硬件和软件部件，文档应[11.28]具有注释，以阐明：进入密码模块部件、功能和程序时，为确保执行正确所需要的前置条件；密码模块部件、功能和程序完成时，预期值为真的后置条件。前置条件和后置条件可以使用任何足够详细的表示方法进行阐述，以完整且清晰地解释密码模块部件、功能或程序的行为。

7.11.6 厂商测试

本条对密码模块的厂商测试提出了要求，其中包括对密码模块中实现的安全功能的测试，从而确保了密码模块的实际行为与密码模块安全策略以及功能规格相一致：

a) 安全一级和安全二级：

对于安全一级和安全二级，文档应[11.29]阐明在密码模块上执行的功能测试。

对于软件或固件密码模块以及混合密码模块中的软件或固件部件，厂商应[11.30]使用通用的自动安全诊断工具(例如，检查缓冲区溢出等)。

b) 安全三级和安全四级：

除了安全一级和安全二级中的要求，文档还应[11.31]阐明在密码模块上执行的底层测试的过程与结果。

7.11.7 配送与操作

本条对密码模块的安全配送、安装以及启动提出了要求，确保将密码模块安全地配送给已授权的操作员，并以正确和安全的方式安装以及初始化：

a) 安全一级：

对于安全一级，文档应[11.32]阐明密码模块的安全安装、初始化与启动的流程。

b) 安全二级和安全三级：

除了安全一级的要求之外，文档还应[11.33]阐明在分发、安装和初始化密码模块的版本给已授权的操作员时，维持密码模块安全性所需的步骤。这些步骤应[11.34]详细指出在配送、安装和初始化密码模块给已授权操作员的过程中，如何检测密码模块是否被拆卸或篡改过。

c) 安全四级：

除了安全二级和安全三级中的要求之外，还应[11.35]要求密码模块使用厂商提供的操作员特

定鉴别数据对已授权的操作员进行鉴别。

7.11.8 生命终止

本条规定了当操作员不再使用密码模块时的安全要求：

a) 安全一级和安全二级：

对于安全一级和安全二级，文档应[11.36]阐明安全清理密码模块的流程。清理是指从密码模块中去除敏感信息(例如，敏感安全参数、用户数据等)的过程，使得清理后的密码模块可以分发给其他操作员或被废弃。

b) 安全三级和安全四级：

除了安全一级和安全二级的要求，文档应[11.37]阐明安全销毁密码模块所需的流程。

7.11.9 指南文档

本条中的要求旨在确保所有使用密码模块的实体能够得到详细的指导和步骤，从而能够以安全的方式管理与使用密码模块。

指南文档包括管理员指南和非管理员指南。

管理员指南应[11.38]阐明：

——密码主管和/或其他管理角色可用的密码模块的管理功能、安全事件、安全参数(以及适当的参数值)、物理端口以及逻辑接口。

——每种操作员鉴别数据及其对应鉴别机制的使用流程。

——在核准的工作模式下管理密码模块的措施。

——与密码模块安全操作相关的用户行为的假定。

非管理员指南应[11.39]阐明：

——密码模块用户可用的核准的和非核准的安全功能、物理端口以及逻辑接口。

——用户对密码模块的核准工作模式所承担的所有必要责任。

7.12 对其他攻击的缓解

密码模块可能还容易受到一些在本标准内其他条款未定义的攻击，密码模块对攻击的敏感性取决于密码模块的类型、实现以及实现环境。恶意环境(例如，攻击者可以是密码模块的授权操作员)中的密码模块可特别关注这些攻击。这些攻击通常依赖从密码模块物理外部获得的一些信息进行分析，以确定关于密码模块中关键安全参数的某些信息。

密码模块文档应[12.01]按照 A.2.12 中规定的要求编写。

针对其他攻击的缓解，还规定了下列要求：

a) 安全一级、安全二级和安全三级：

如果将密码模块设计为可缓解一种或多种在本标准中未定义的特定攻击，那么密码模块的相关文档应[12.02]列举出密码模块能够缓解的攻击。当制定出要求以及相关检测后，将对用于缓解攻击的安全机制进行验证，检测其是否存在且是否起作用。

b) 安全四级：

除了安全一级、安全二级和安全三级的安全要求，安全四级的密码模块还应[12.03]满足下列安全要求：

——如果声明了能够缓解本标准未定义的特定攻击，则文档应[12.04]详细说明缓解攻击的方法以及检测该缓解技术有效性的方法。

附 录 A
（规范性附录）
文档要求

A.1 用途

本附录规定了密码模块的最低文档要求，密码模块应[A.01]满足下列文档要求。

A.2 条款

A.2.1 通用

未对通用要求提出文档规定。

A.2.2 密码模块规格

密码模块规格的文档要求包括：

——密码模块类型的说明（硬件、软件、固件、混合软件和混合固件密码模块）。（安全一级、安全二级、安全三级和安全四级）

——密码边界的说明。（安全一级、安全二级、安全三级和安全四级）

——密码模块的硬件、软件和固件部件的说明，以及密码模块物理构造的描述。（安全一级、安全二级、安全三级和安全四级）

——密码模块中不受本标准安全要求约束的任何硬件、软件或固件的说明，并解释它们不受本标准安全要求约束的原因。（安全一级、安全二级、安全三级和安全四级）

——密码模块的物理端口和逻辑接口的说明（安全一级、安全二级、安全三级和安全四级）

——密码模块手动控制器件或逻辑控制位，物理或逻辑的状态指示器，以及对应的物理、逻辑与电气特性的说明。（安全一级、安全二级、安全三级和安全四级）

——密码模块采用的所有核准的和非核准的安全功能列表，以及所有核准的和非核准的工作模式的说明。（安全一级、安全二级、安全三级和安全四级）

——描述所有主要硬件部件及部件互联的密码模块图，包括所有微处理器、输入输出缓冲区、明文/密文缓冲区、控制缓冲区、密钥存储区、工作存储器以及程序存储器。（安全一级、安全二级、安全三级和安全四级）

——密码模块硬件和软件设计的说明。（安全一级、安全二级、安全三级和安全四级）

——所有安全相关信息的说明，包括密钥和私钥（未加密的和经加密的）、鉴别数据（例如，口令、PINs）、其他关键安全参数和泄露或修改后会危及密码模块安全的其他受保护信息（例如，审计事件、审计数据）。（安全一级、安全二级、安全三级和安全四级）

——密码模块安全策略说明，包括来源于本标准要求的规则和来源于厂商强制的任何附加要求的规则。（安全一级、安全二级、安全三级和安全四级）

A.2.3 密码模块接口

密码模块接口的文档要求包括：

——数据输入、数据输出、控制输入、控制输出、状态输出和电源接口的说明，接口包括物理的和逻

辑的。(安全一级、安全二级、安全三级和安全四级)

——可信信道接口的说明。(安全三级和安全四级)

——在错误状态下,如果不禁用控制输出接口,说明例外情况和理由。(安全一级、安全二级、安全三级和安全四级)

A.2.4 角色、鉴别和服务

角色、鉴别和服务的文档要求:

——密码模块支持的所有授权角色的说明。(安全一级、安全二级、安全三级和安全四级)

——密码模块提供的核准与非核准的服务、操作或功能的说明。每一个服务的服务输入、相应的服务输出以及经授权可以执行该服务的角色的说明。(安全一级、安全二级、安全三级和安全四级)

——密码模块提供的、不要求操作员担任授权角色即可执行的任何服务的说明,以及阐述这些服务为何不会对密钥和其他关键安全参数进行修改、泄露或替换,或者阐述它们为何不会对密码模块的安全性产生影响。(安全一级、安全二级、安全三级和安全四级)

——密码模块支持的鉴别机制,实现支持的鉴别机制所需的鉴别数据类型,用于控制第一次访问密码模块以及初始化鉴别机制的授权方法,以及密码模块支持的鉴别机制的强度等说明,包括支持使用多种鉴别机制的基本原理。(安全一级、安全二级、安全三级和安全四级)

——密码模块服务的说明,包括显示密码模块版本信息、显示状态、执行自测试、执行核准的安全功能、以及执行置零。(安全一级、安全二级、安全三级和安全四级)

——旁路机制的说明。(安全一级、安全二级、安全三级和安全四级)

——软件或固件加载机制的说明。(安全一级、安全二级、安全三级和安全四级)

——自启动密码服务能力控制逻辑和接口的说明。(安全一级、安全二级、安全三级和安全四级)

A.2.5 软件安全

软件安全的文档要求包括:

——所使用的核准的完整性技术的说明。(安全一级、安全二级、安全三级和安全四级)

——操作员按需执行核准的完整性技术的方法说明。(安全一级、安全二级、安全三级和安全四级)

——可执行代码格式的说明。(安全二级、安全三级和安全四级)

A.2.6 运行环境

运行环境的文档要求包括:

——密码模块运行环境的说明,包括(如果适用的话)密码模块所使用的操作系统。(安全一级和安全二级)

——配置运行环境的安全规则、设置和限制条件的说明。(安全一级和安全二级)

——配置操作系统符合相应要求的管理员指南文档。(安全二级)

A.2.7 物理安全

物理安全的文档要求包括:

——物理实体及其安全等级的说明。密码模块采用的物理安全机制的说明。(安全一级、安全二级、安全三级和安全四级)

——如果密码模块包含需要物理访问密码模块内容的维护角色,或者密码模块被设计为允许物理访问,那么应给出维护访问接口以及维护访问接口被访问时,如何置零关键安全参数的说明。(安全一级、安全二级、安全三级和安全四级)

——密码模块的正常运行范围的说明。密码模块采用的环境失效保护特性的说明或者执行的环境失效测试的说明。(安全三级和安全四级)

——采用的故障注入缓解技术的说明。(安全四级)

A.2.8 非入侵安全

非入侵式安全的文档要求包括:

——针对非入侵式攻击的缓解技术的说明。(安全一级、安全二级、安全三级和安全四级)

——每项采用的攻击缓解技术有效性的证据。(安全一级、安全二级、安全三级和安全四级)

A.2.9 敏感安全参数管理

敏感安全参数管理的文档要求包括:

——密码模块使用的所有密钥、密钥分量和其他敏感安全参数的说明。(安全一级、安全二级、安全三级和安全四级)

——密码模块使用的所有随机数生成器以及用法的说明。(安全一级、安全二级、安全三级和安全四级)

——密码模块对外部输入熵源的最小熵值说明。(安全一级、安全二级、安全三级和安全四级)

——密码模块使用的每个随机数生成器(核准的随机数生成器、非核准的随机数生成器和熵源)的说明。(安全一级、安全二级、安全三级和安全四级)

——如果熵是在密码模块的密码边界内收集的,最小熵及其生成方法的说明。(安全一级、安全二级、安全三级和安全四级)

——每个利用随机数生成器生成敏感安全参数方法的说明。(安全一级、安全二级、安全三级和安全四级)

——密码模块采用的所有敏感安全参数建立方法的说明。(安全一级、安全二级、安全三级和安全四级)

——密码模块采用的每个敏感安全参数生成方法的说明。(安全一级、安全二级、安全三级和安全四级)

——密码模块采用的每个核准的密钥生成方法的说明。(安全一级、安全二级、安全三级和安全四级)

——密码模块采用的敏感安全参数输入和输出方法的说明。(安全一级、安全二级、安全三级和安全四级)

——密码模块采用的密钥输入和输出方法的说明。(安全一级、安全二级、安全三级和安全四级)

——如果使用了知识拆分过程,证明如果需要 n 个密钥分量来重建原始关键安全参数,那么任何 $n-1$ 个分量不提供除长度之外的任何关于原始关键安全参数的信息。(安全三级和安全四级)

——密码模块采用的知识拆分过程的说明。(安全三级和安全四级)

——存储在密码模块的敏感安全参数的说明。(安全一级、安全二级、安全三级和安全四级)

——当关键安全参数存储在密码模块中,如何保护关键安全参数不被非授权的访问、使用、泄漏、修改和替换的说明。(安全一级、安全二级、安全三级和安全四级)

——当公开安全参数存储在密码模块中,如何保护公开安全参数不被非授权修改和替换的说明。(安全一级、安全二级、安全三级和安全四级)

——当密码模块内存储的公开安全参数已经被分配时,密码模块如何把该公开安全参数与实体(操作员、角色或进程)相关联的说明。(安全一级、安全二级、安全三级和安全四级)

——密码模块采用的置零方法,以及该方法防止被置零值的恢复和重用的原理。(安全一级、安全

二级、安全三级和安全四级）

A.2.10 自测试

自测试的文档要求包括：

——密码模块执行的自测试的说明，包括运行前测试和条件测试。（安全一级、安全二级、安全三级和安全四级）

——自测试成功和失败的状态指示器的说明。（安全一级、安全二级、安全三级和安全四级）

——当自测试失败时密码模块进入的错误状态的说明，以及退出错误状态，密码模块重新开始正常工作所必需的条件和操作的说明（例如，可能包括密码模块的维护、密码模块的重上电、自动密码模块恢复或把密码模块退回厂商）。（安全一级、安全二级、安全三级和安全四级）

——对密码模块安全操作起关键作用的所有安全功能的说明，并且定义了密码模块所执行的对应的运行前测试、条件测试。（安全一级、安全二级、安全三级和安全四级）

——如果密码模块实现了旁路能力，管理切换程序的机制或逻辑的说明。（安全一级、安全二级、安全三级和安全四级）

A.2.11 生命周期保障

生命周期保障的文档要求包括：

——密码模块配置管理系统的说明。（安全一级、安全二级、安全三级和安全四级）

——开发密码模块所需的支持文档以及由配置管理系统提供的相关文档的说明。（安全一级、安全二级、安全三级和安全四级）

——密码模块安全安装、初始化和启动过程的说明。（安全一级、安全二级、安全三级和安全四级）

——在分发和配送密码模块给授权操作员的过程中，维护密码模块安全性的过程说明。（安全二级、安全三级和安全四级）

——密码模块硬件、固件和软件设计与密码模块安全策略之间以及与 FSM 之间相一致的说明。（安全一级、安全二级、安全三级和安全四级）

——如果密码模块包含软件，带有注释的软件源代码的说明，注释应清楚地描述出软件与密码模块设计的对应关系。（安全一级、安全二级、安全三级和安全四级）

——如果密码模块包含硬件，硬件线路图和/或 HDL 列表的说明。（安全一级、安全二级、安全三级和安全四级）

——功能规格的说明，包括密码模块、密码模块功能、密码模块外部物理端口和逻辑接口、以及物理端口和逻辑接口用途的非形式化描述。（安全二级、安全三级和安全四级）

——描述密码模块内部主要部件功能、内部部件接口、部件接口用途以及内部信息流的详细设计的说明。（安全三级和安全四级）

——对密码模块设计与功能的一致性（包括前置条件和后置条件）进行非形式化证明的说明。（安全四级）

——FSM（或同等模型）所用的状态转移图和状态转移表的说明（安全一级、安全二级、安全三级和安全四级），包括：

- 密码模块的运行状态和错误状态；
- 从一个状态到另一个状态的状态转移；
- 导致从一个状态转移到另一个状态的输入事件，包括数据输入和控制输入；
- 从一个状态转移到另一个状态导致的输出事件，包括内部密码模块状态、数据输出以及状态输出。

——软件或固件的源代码的说明。（安全一级、安全二级、安全三级和安全四级）

——对于每个密码模块的硬件和软件部件，源代码所标注的注释，应说明：调用密码模块部件、功能或程序时，为确保执行正确所需要的前置条件；密码模块部件、功能或程序执行完成时，预期值为真的后置条件。（安全四级）

——管理员指南应做出以下说明：（安全一级、安全二级、安全三级和安全四级）

- 密码主管可用的密码模块的管理功能、安全事件、安全参数（以及合适的参数值）、物理端口以及逻辑接口；
- 如何安全地管理密码模块的步骤；
- 与密码模块安全操作相关的用户行为的假设。

——非管理员指南应做出以下说明：（安全一级、安全二级、安全三级和安全四级）

- 密码模块用户可用的核准的安全功能、物理端口以及逻辑接口；
- 为确保密码模块安全操作，用户担当的必要责任。

A.2.12 对其他攻击的缓解

对其他攻击的缓解的文档要求包括：

——如果将密码模块设计为可缓解一种或多种本标准未定义的特定攻击，在密码模块的文档中列举出密码模块用以缓解攻击的安全机制。（安全一级、安全二级和安全三级）

——如果将密码模块设计为可缓解一种或多种本标准未定义的特定攻击，在文档中记载用于缓解攻击的方法以及检测缓解技术有效性的方法。（安全四级）

附 录 B
（规范性附录）
密码模块安全策略

B.1 用途

本附录总结了非私有安全策略中应[B.01]提供的要求。安全策略的格式应[B.02]按照本附录指示的顺序呈现。不应[B.03]在没有声明允许复制或分发的情况下，将安全策略标记为私有的或拥有版权的文档。

B.2 条款

B.2.1 通用

通用的安全策略要求包括：

——给出表格，说明密码模块在11个安全域中的等级以及所达到的整体安全等级。

B.2.2 密码模块规格

密码模块规格的安全策略要求包括：

——密码模块预定的用途和用法，包括预定的使用环境。

——密码模块的原理图、示意图或照片。如果是硬件密码模块，应包含密码模块的照片。如果安全策略包括密码模块的多个版本，每个版本应分别表述，或者注明该表述是针对所有版本的。对于软件或固件密码模块，安全策略应包含方框图，用以说明：

- 软件或固件密码模块中的逻辑对象相对操作系统、其他支持应用和密码边界的位置，使得逻辑对象和密码边界之间的所有逻辑层和物理层是定义明确的；
- 软件或固件密码模块中的逻辑对象与操作系统、其他物理边界内的支持应用等的交互。

——密码模块描述：

- 提供密码模块和所有部件（硬件、软件或固件）的详细版本/标识。

——硬件、软件、固件或混合密码模块检测：

- 对于软件密码模块、固件密码模块和混合密码模块，列出密码模块检测时所用的操作系统，并给出厂商确认适用于密码模块的操作系统的列表。

——密码模块的整体安全等级以及各个域的安全等级。

——密码模块物理边界和密码边界的准确定义：

- 在密码边界外部的硬件、软件或固件应在安全策略中阐明。
- 工作模式以及如何进入/退出每个模式。安全策略描述密码模块实现的每个核准的工作模式以及如何配置每个模式。
- 所有安全功能的列表，核准的和非核准的模式下采用的具体密钥强度，以及所实现的工作模式（例如，CBC）。
- 适用的框图。
- 整体安全设计和操作规则。
- 适用的初始化要求。

B.2.3 密码模块接口

密码模块接口的安全策略要求包括：

——所有端口与接口(物理和逻辑的)列表。

——定义通过五个逻辑接口的信息。

——阐述物理端口以及通过它们的数据。

——阐述可信信道。

——如果在错误状态时不禁用控制输出接口，给出相应的例外情况和理由。

B.2.4 角色、服务和鉴别

角色、服务和鉴别的安全策略要求包括：

——阐明所有角色。

——角色列表，以及相应的服务命令和输入输出。

——阐明每种鉴别方法，指明是基于身份还是基于角色的，以及该方法是否是必要的。

——如何满足鉴别要求的强度。

——如果具有旁路能力，启动旁路能力的两个独立的操作是什么以及如何检查旁路状态。

——如果具有自启动密码服务能力，启动自启动密码服务能力的两个独立的操作是什么以及如何表示自启动密码服务状态。

——如果从外部加载软件或固件，那么应阐明相应的加载控制措施，以及代码的隔离方法，从而防止对密码模块非授权的访问与使用。

——分别列出包括核准的和非核准的安全服务与非安全服务。

——对每个服务，给出：服务名称，服务用途和/或用法的描述(在一些情况下，服务名称自身就可以提供这些信息)，使用的或者实现的核准安全功能(算法、密钥管理技术或鉴别技术)列表。对于每个授权使用服务的角色，描述针对每个敏感安全参数的访问权限以及相应的角色鉴别方法。

——描述安装过程与密码鉴别机制。

B.2.5 软件/固件安全

软件/固件安全的安全策略要求包括：

——阐述所采用的核准的完整性技术。

——阐述操作员在需要的时候如何启动一个完整性测试。

——阐述每一个可执行代码的组成及其格式。

——如果密码模块是开源的，阐述把代码编译成可执行形式的编译器和必须的控制参数。

B.2.6 运行环境

运行环境的安全策略要求包括：

——确定运行环境(例如，不可修改的，受限的，或可修改的)。

——确定操作系统和经过检测的计算平台。

——对于适用的安全等级，解释如何满足安全要求。

——厂商可以声称密码模块能够移植到其他未经专门检测的操作系统，并且能够正确运行。

——阐述运行环境配置的安全规则、设置或限制。

B.2.7 物理安全

物理安全的安全策略要求包括：

——阐明具体实体(单芯片、多芯片嵌入式或多芯片独立式)。
——阐明密码模块实现的物理安全机制(例如,拆卸存迹封条、锁、拆卸响应和置零开关、报警器)。
——阐明为了确保维护好物理安全,操作员应执行的操作(例如,对拆卸存迹封条的定期检测以及拆卸响应和置零开关的测试):

- 如果密码模块要求操作员利用拆卸存迹封条或安全装置,这些装置在密码模块的整个生命周期中都可能被操作员利用或修改,阐明以下信息:B.2.2 中要求的相关照片或说明,以反映密码模块的配置或构造如规格所述;可以提供其他照片或说明,以反映其他配置。
- 如果为了满足不透明的要求,需要用填充面板覆盖未使用的插槽或开口,则贴着拆卸存迹封条的填充面板应包含在图片或说明中。填充面板应包含在零件列表中。
- 提供照片或说明,标识出满足物理安全要求的,密码模块中使用的所有拆卸存迹封条或安全装置的准确位置。
- 给出密码模块需要的拆卸存迹封条或安全装置的总数(例如,五个拆卸存迹封条和两个不透光屏幕)。提供标明了拆卸存迹封条或安全装置准确位置的照片或说明,要求对这些照片或说明进行逐条编号,并且照片或说明的数目与拆卸存迹封条或安全装置的总数相同(实际的拆卸存迹封条或安全装置不要求编号)。
- 如果拆卸存迹封条或安全装置是从密码模块厂商处可重新订购的零件,安全策略将标识从密码模块厂商处可以获得的封条、安全装置的零件号。重新配置后,密码模块操作员可能需要移除原有的并引入新的拆卸存迹封条或安全装置。
- 阐述操作员角色,该角色负责未使用封条的全程控制和安全,并直接控制和观察密码模块可能发生的改变。例如,当密码模块需要移除或者安装拆卸存迹封条或安全装置以进行重新配置时,为了确保密码模块的安全性以及确保密码模块修改后能够恢复到核准的工作模式,该角色应全程监控。
- 如果拆卸存迹封条或安全装置是可以被移除或重新安装的,应给出明确的说明,其中包含关于密码模块的设备或表面如何准备申请安装新的拆卸存迹封条或安全装置。

——阐述所实现的故障注入缓解方法。

B.2.8 非入侵式安全

非入侵式安全的安全策略要求包括:
——列出密码模块所采用的所有非入侵缓解技术,以保护密码模块关键安全参数免受非入侵攻击。
——描述上述缓解技术的有效性。

B.2.9 敏感安全参数管理

敏感安全参数管理的安全策略要求包括:
——提供一个密钥表格,用以阐明密钥类型、比特强度、安全功能、密钥生成的地点和方式、密钥是否被导入或导出、任何敏感安全参数生成与建立方法以及与其相关的其他密钥。
——列出一个其他敏感安全参数以及它们是如何生成的表格。
——阐明核准的和非核准的随机数生成器。
——描述随机数生成器输出的使用。
——阐明随机数生成器的熵源。
——阐明电子和手动密钥输入输出方法。
——阐明敏感安全参数存储技术。
——阐明不受保护的敏感安全参数的置零方法和原理,以及操作员的置零启动能力。
——如果采用了国家密码管理主管部门规定的、在过渡期内的算法或密钥长度,则应阐明。

B.2.10 自测试

自测试的安全策略要求包括：

——提供带有确定参数的运行前自测试和条件自测试的列表，并列出测试执行的条件。

——阐明自测试的时间周期，以及关于在两次自测试周期之间可能导致密码模块运行中断的任何条件的策略。

——描述所有错误状态和状态指示。

——描述运行初始化，如果适用的话。

B.2.11 生命周期保障

生命周期保障的安全策略要求包括：

——阐明安全安装、初始化、启动及运行密码模块的流程。

——阐明所有维护要求。

——提供管理员和非管理员指南(可以是单独的文档)。

B.2.12 对其他攻击的缓解

对其他攻击的缓解的安全策略要求包括：

——列出密码模块能够缓解的其他攻击。

——描述所列出缓解技术的有效性。

——列出安全性相关的指南和约束条件。

附 录 C
（规范性附录）
核准的安全功能

C.1 用途

本附录给出了适用于本标准的核准的安全功能列表，包括分组密码、序列密码、非对称密码、消息鉴别码、杂凑函数、实体鉴别、密钥管理和随机数生成。

C.2 条款

C.2.1 分组密码

本标准核准的分组密码包括：

a) GB/T 32907 信息安全技术 SM4 分组密码算法

b) GB/T 17964 信息安全技术 分组密码算法的工作模式

C.2.2 序列密码

本标准核准的序列密码包括：

a) GB/T 33133.1 信息安全技术 祖冲之序列密码算法 第1部分：算法描述

b) GM/T 0001.2 祖冲之序列密码算法 第2部分：基于祖冲之算法的机密性算法

c) GM/T 0001.3 祖冲之序列密码算法 第3部分：基于祖冲之算法的完整性算法

C.2.3 非对称密码

本标准核准的非对称密码包括：

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

b) GM/T 0044(所有部分) SM9 标识密码算法

C.2.4 消息鉴别码

GB/T 15852(所有部分) 信息技术 安全技术 消息鉴别码

C.2.5 杂凑函数

GB/T 32905(所有部分) 信息安全技术 SM3 密码杂凑算法

C.2.6 实体鉴别

GB/T 15843(所有部分) 信息技术 安全技术 实体鉴别

C.2.7 密钥管理

符合相关密码产品标准对密钥管理的要求。

C.2.8 随机数生成

随机数生成器应取得国家密码管理主管部门的认可。

附 录 D
（规范性附录）
核准的敏感安全参数生成和建立方法

D.1 用途

本附录给出了适用于本标准的敏感安全参数生成和建立方法列表。

D.2 条款

D.2.1 敏感安全参数生成

采用核准的随机数生成器的输出。

采用核准的安全功能，包括（但不限于）分组算法、杂凑算法等，利用进入密码模块的敏感安全参数衍生。

采用核准的敏感安全参数建立方法，利用进入密码模块的敏感安全参数衍生。

D.2.2 敏感安全参数建立方法

本标准核准的敏感安全参数建立方法包括：

a） GB/T 32918.3 信息安全技术 SM2 椭圆曲线公钥密码算法 第3部分：密钥交换协议

b） GM/T 0044.3 SM9 标识密码算法 第3部分：密钥交换协议

附 录 E
（规范性附录）
核准的鉴别机制

E.1 用途

本附录给出了适用于本标准的鉴别机制列表。

E.2 鉴别机制

本标准核准的鉴别机制包括：

a) 密码模块可以使用设备进行操作员鉴别，包括（但不限于）IC 卡，Token，USB Key 等，具体机制应符合 GB/T 15843。

b) 密码模块可以使用所拥有的信息或个人生物特征进行操作员鉴别，包括（但不限于）口令、PIN 码、安全问题、指纹、虹膜等，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；一分钟之内多次尝试的成功概率不大于十万分之一。

附 录 F
（规范性附录）
非入侵式攻击及缓解方法检测指标

F.1 用途

本附录给出了适用于本标准的非入侵式攻击及缓解方法检测指标。

F.2 非入侵式攻击

下面列出了常见的非入侵式攻击分析方法。

功耗分析：简单功耗分析（Simple Power Analysis，SPA）和差分功耗分析（Differential Power Analysis，DPA）。SPA 需要直接（例如，通过视觉）分析密码模块在执行密码过程中各指令的功耗模式。通过监视密码模块功耗的变化，可以发现所执行密码算法的模式和实现方法，从而获取密钥值。一阶 DPA 具有相同的目的，但是为了分析密码模块的功耗变化，使用了统计方法（例如，均值差、相关系数）对功耗变化进行统计分析，从而获取密钥值。二阶 DPA 针对采用防御技术的密码模块，通过分析密码模块两处功耗的变化，使用统计方法对功耗变化进行统计分析，从而获取密钥值。

电磁分析：由于密码模块电活动会导致密码模块发出的电磁信号发生变化，通过监视密码模块发出的电磁信号变化，可以采用简单电磁分析（Simple Electro-Magnetic Analysis，SEMA）和差分电磁分析（Differential Electro-Magnetic Analysis，DEMA）。SEMA 采用与 SPA 相同的方法对电磁信号变化进行分析，从而获取密钥值。DEMA 采用与 DPA 相同的方法对电磁信号变化进行分析，从而获取密钥值。

计时分析：计时分析攻击依赖于密码模块执行时间的精确测量与密码算法或过程有关的特殊数学操作之间的关系。对收集的耗时信息进行分析可以确定密码模块的输入和密钥之间的关系。通过对此关系的分析，从而推导密钥和其他关键安全参数。计时分析攻击假定攻击者具有有关密码模块的设计知识。

F.3 非入侵式攻击缓解方法检测指标

下面列出了常见的非入侵式攻击缓解方法检测指标。

密码模块可以采用平滑功耗或者改变导致功耗变化中间值的方法，包括（但不限于） 使用电容、使用内部电源、随机化密码算法或过程中的指令序列、采用双轨预充电电路、采用掩码等，降低功耗分析攻击的风险。对于 SPA，实施攻击所能获取的密钥量应小于 8 比特；对于一阶 DPA，实施攻击所能获取的密钥量应小于 8 比特；对于二阶 DPA，实施攻击所能获取的密钥量应小于 8 比特。

密码模块可以采用减少（在某些情况下可以阻止）电磁信号辐射的方法，包括（但不限于）对包括网线在内的全部组件添加屏蔽套、屏蔽层等，降低电磁泄漏攻击的风险。对于 SEMA，实施攻击所能获取的密钥量应小于 8 比特；对于一阶 DEMA，实施攻击所能获取的密钥量应小于 8 比特；对于二阶 DEMA，实施攻击所能获取的密钥量应小于 8 比特。

密码模块可以采用改变密码工作过程中时间波动的方法，包括（但不限于）控制算法或过程中各指令的运行、随机插入无关指令等，降低计时攻击的风险。对于计时分析，实施攻击所能获取的密钥量应小于 8 比特。

参 考 文 献

[1] ISO/IEC 19790:2012 Information technology—Security techniques—Security requirements for cryptographic modules

[2] National Institute of Standards and Technology, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, Federal Information Processing Standards Publication 140-2, May 25, 2001.

中 华 人 民 共 和 国
国 家 标 准
信息安全技术　密码模块安全要求
GB/T 37092—2018
*
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)
北京市西城区三里河北街 16 号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2018 年 12 月第一版
*
书号:155066·1-62069

GB/T 37092-2018