ICS 35.040
L 80
备案号：

中华人民共和国密码行业标准

GM/T XXXX—2014

密码模块安全检测规范

Test requirements for cryptographic modules

（征求意见稿）

（本稿完成时间：2014-5-13）

（在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上）

××××-××-××发布　　××××-××-××实施

国家密码管理局 发布

目 次

前　言

本标准依据 GB/T 1.1-2009 给出的规则起草。

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这些专利的责任。

本标准由密码行业标准化技术委员会提出并归口。

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

本规范主要起草人：汪雪林、李大为、邓开勇、陈国、陈宝儒、张一飞、胡伯良、朱鹏飞、蒋红宇、罗鹏、高能、雷银华、莫凡、林春、谭武征、张万涛。

密码模块安全检测规范

1 范围

本标准旨在描述可供检测机构检测密码模块是否符合 GM/T 0028 密码模块安全要求的一系列方法。这些方法是为了保证在检测过程中高度的客观性，并确保各检测机构测试结果的一致性。

本标准同时给出了送检单位提供给检测机构材料的要求，该材料通常作为补充证据用于证明其密码模块对 GM/T 0028 密码模块安全要求的符合性。

在密码模块提交给检测机构之前，送检单位可将本标准作为指导来判断该密码模块是否符合 GM/T 0028 所提出的安全要求。

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。

GM/T 0005　　随机性检测规范

GM/T 0028　　密码模块安全要求

3 术语和定义

为了解释本文档，以下术语和定义已经在 GM/T 0028 密码模块安全要求中给出，并在本文档中继续应用。

注：后面带有方括号的注释的定义是原文摘录自 GM/T 0028 密码模块安全要求。其他的名词和术语对 GM/T 0028 密码模块安全要求做了适当的修改。

3.1

非对称密码技术 asymmetric cryptographic technique

使用两个相关变换的密码技术——一个公开变换（由公钥定义）和一个秘密变换（由私钥定义）。非对称密码技术的特点是，给定公钥变换结果，在给定的有限时间、有限计算资源条件下，计算得出私钥变换结果是不可行的。

3.2

威胁 compromise

对关键安全参数（GM/T 0028 密码模块安全要求，3.16）的未经授权的泄露、修改、替换或使用，或是对公开安全参数（GM/T 0028 密码模块安全要求，3.91）的未经授权的修改或替换。

3.3

密码模块安全策略/安全策略 cryptographic module security policy/security policy

密码模块操作应遵循的明确安全规则，包括为满足本标准要求而提出的规则以及模块采用的其他额外规则。见GM/T 0028附录B。

[GM/T 0028 密码模块安全要求，3.24]

3.4

密码主管 crypto officer

由个体或进程（如主体）所承担的角色，代表个体允许密码模块执行密码初始化或管理职能。

[GM/T 0028 密码模块安全要求，3.17]

3.5

固件 firmware

存储于密码边界内的硬件中、执行期间不能被动态写入或修改的程序与数据组成部分。如存储硬件，包括但不限于ROM、PROM、EEPROM与FLASH。

[GM/T 0028 密码模块安全要求，3.40]

3.6

输入数据 input data

输入密码模块的信息，用于数据变换或认可的安全功能运算。

[GM/T 0028 密码模块安全要求，3.51]

3.7

维护角色 maintenance role

承担物理维护及/或逻辑维护服务的角色。维护服务可包括但不仅限于硬件及/或软件诊断。

[GM/T 0028 密码模块安全要求，3.61]

3.8

钝化 passivation

在半导体结，表面或元器件以及集成电路中构建检测和保护功能的反应过程所产生的效应。如二氧化硅和磷玻璃可用于此用途，但钝化材料由工艺决定。

3.9

公钥 public key

实体的非对称密钥对中可以公开的密钥。在非对称签名机制中，公钥用于签名验证计算。在非对称加密机制中，公钥用于加密变换。密钥“公开”并不意味着所有人都能获取。公钥可能仅被某特定群体的成员获取。

[GM/T 0028 密码模块安全要求，3.88]

3.10

角色 role

用户关联的安全属性，定义了用户对密码模块的访问权限或使用限制。一个角色可能关联一个或多个服务；一个角色可能关联一个或多个用户；一个用户也可能承担一个或多个角色。

3.11

安全功能 security function

国家密码管理机构认可的随机数发生器，实体鉴别，密钥建立，密码算法及其操作模式。如分组算法、流密码、非对称算法、消息认证码、杂凑函数，或其他安全功能等。详见GM/T 0028附录C。

[GM/T 0028 密码模块安全要求，3.98]

3.12

种子密钥 seed key

用于初始化随机数发生器的秘密值。

3.13

简单能量分析 simple power analysis，SPA

为了从密码操作中提取出有用信息，对指令集（或单一指令）执行模式进行的直接（通常是视觉的）分析，通常与密码模块的电源能量消耗有关。

3.14

软件 software

密码边界内的程序及数据组成，通常保存在可擦写媒介中，可在执行过程中动态地写入或修改。如可擦除媒介，包括但不限于硬盘。

[GM/T 0028 密码模块安全要求，3.108]

3.15

知识拆分 split knowledge

将密钥拆分为多个密钥组件的过程，其中单个密钥组件不享有任何原始密钥信息。随后这些密钥组件可以由各实体导入或导出密码模块，组合后重新生成原始密钥。全部或部分组件可能需要执行组合操作。

3.16

系统软件 system software

密码边界内的通用软件，其目的在于方便进行密码模块操作。如操作系统、编译器及通用程序。

3.17

拆卸证据 tamper evidence

用于指示企图侵害密码模块安全的易观察到的迹象。

4 缩略语

下列缩略语适用于本文件：

API	Application Program Interface	应用程序接口
CBC	Cipher Block Chaining	密码分组链接
CSP	Critical Security Parameter	关键安全参数
EDC	Error Detection Code	错误检测码
EFP	Environmental Failure Protection	环境失效保护
EFT	Environmental Failure Testing	环境失效测试
FSM	Finite State Model	有限状态模型
HDL	Hardware Description Language	硬件描述语言
IC	Integrated Circuit	集成电路
PIN	Personal Identification Number	个人身份识别码
PROM	Programmable Read-Only Memory	可编程只读存储器
PSP	Public Security Parameter	公开安全参数
RAM	Random Access Memory	随机存取存储器
RBG	Random Bit Generator	随机比特生成器
ROM	Read-Only Memory	只读存储器

5 文档结构

5.1 概述

本文档第 6 章阐述了一系列供检测机构使用的方法以及对送检单位提交给检测机构材料的要求。第 6 章包括 12 个小节，相当于 GM/T 0028 密码安全要求的 12 个方面加上 GM/T

0028 密码模块安全要求的附录 A 到 F。

5.2 条款和安全要求

在第 6 章的每个小节里，GM/T 0028 的安全要求相应的分成了一系列条款集（即对一个符合给定领域和给定等级安全要求模块而言，结论才能为真）。全部内容直接引自 GM/T 0028 密码模块安全要求。

各条款的格式为：

AS<要求编号>.<条款序列编号>

其中，“要求编号”是指 GM/T 0028 中指定的相应区域的编号（即，对应 1 到 12）。“条款序列编号”是小节内的序列标示符。在条款的结论后面，该条款所应用的安全等级列在圆括号内。

下面的每个条款是对送检单位提交材料的要求集。这些要求描述了送检单位提交的文档或详细材料的类型，以便于检测人员核实（文档或材料）与给定条款的符合性。

这些要求的格式如下：

VE<要求编号>.<条款序列编号>.<序列编号>

这里的“要求编号”和“条款序列编号”与各条款的“要求编号”和“条款序列编号”完全相同。序列编号是上述对送检单位要求条款内的序列标识符。

同样的，下面的每个条款和要求是对检测密码模块的人员的要求集。这些要求指导检测人员在以检测某个给定条款下的密码模块为目的时，他/她如何执行检测。

这些要求的格式如下：

TE<要求编号>.<条款序列编号>.<序列编号>

“要求编号”和“条款序列编号”与相应的条款要求编号和条款序列编号相同。“序列编号”是上述对检测人员要求条款内的序列标识符。

5.3 互引用的条款

为了明确说明与 GM/T 0028 或其他标准中的互引用的条款，这些条款编号用大括号“{”和“}”括起来，互引用的部分用斜体字表示。

6 安全要求

6.1 检测要求总述

检测方应根据本章节在各个领域描述的安全要求对密码模块进行检测，并对密码模块在各个领域的安全等级独立进行评估。

检测方可以以下面一个或多个方式对密码模块的安全性进行检测：

a） 检测人员使用检测方的设备进行检测。

b） 检测人员使用送检方的设备进行检测。

c） 检测人员监督送检方使用送检方的设备进行检测。在此种情况下，检测方需：

1） 阐述己方不能进行检测的理由；

2） 制定所需的检测计划和检测任务；

3） 直接观察检测的执行情况。

如果任一条款的检测不成功，则此条款不通过。

本小节阐述了满足第 6 章其他小节的要求总和。它本身没有检测条款，且不应单独进行检测。

6.2 通用要求

AS01.01：（安全级别 1，2，3，4）

该条款规定了符合本标准的密码模块应当满足的安全要求。这些安全要求涵盖了有关密码模块的设计、实现、操作以及处置的域，具体包括：密码模块规格；模块接口，角色、服务和鉴别；软件和固件安全；运行环境；物理安全；非入侵式攻击安全；敏感安全参数管理；自测试；生命周期保障；以及对其它攻击的缓解。

注：本条款不单独进行检测。

AS01.02：（安全级别 1，2，3，4）
密码模块应当针对各个域的要求进行测试。

注：本条款不单独进行检测。

AS01.03：（安全级别 1，2，3，4）
密码模块应当在每个域中独立地进行评级。

注：本条款不单独进行检测。

AS01.04：（安全级别 1，2，3，4）
待审验或评估的密码模块应当提供所有相关文档，包括用户和安装手册、设计说明、生命周期文档等。

送检单位需要提交的材料

VE01.04.01：送检单位需提供密码模块相关文档，至少包含：
——密码模块安全策略；
——用户手册；
——安装手册；
——设计说明；
——生命周期文档。

所需的检测程序

TE01.04.01：检测人员应核实送检单位提供的文档，至少包含：
——密码模块安全策略；
——用户手册；
——安装手册；
——设计说明；
——生命周期文档。

6.3 密码模块的规格

6.3.1 密码模块规格说明通用要求

AS02.01：（安全级别 1，2，3，4）
密码模块应当是硬件、软件、固件、或它们之间的组合的集合，该集合至少使用一个核准的密码算法、安全功能或进程实现一项已定义的密码服务，并且被包含在定义的密码边界内。

注 1：本条款不单独进行检测。
注 2：GM/T 0028 的附录 C 列出了已认可的安全功能。

AS02.02：（安全级别 1，2，3，4）
密码模块规格说明应当按照 GM/T 0028 A.2.2 和 B.2.2 中规定的要求编写。

送检单位需要提交的材料

VE02.02.01 送检单位提供的密码模块安全策略文档中需包含密码模块的规格说明，并且需按照 GM/T 0028 A.2.2 和 B.2.2 的要求编写。

所需的检测程序

TE02.02.01 检测人员应核实送检单位提供的密码模块安全策略文档中包含密码模块的规格说明，并且符合 GM/T 0028 A.2.2 和 B.2.2 的要求。

6.3.2 密码模块类型

AS02.03：（安全级别 1，2，3，4）
密码模块应当定义为下列一种模块类型：
——硬件模块
——软件模块
——固件模块
——混合软件模块
——混合固件模块

送检单位需要提交的材料

VE02.03.01：送检单位需提供密码模块类型的描述，明确定义送检产品的模块类型。

所需的检测程序

TE02.03.01：检测人员应核实送检单位提供的模块类型的描述准确，是否符合 GM/T 0028 7.2.2 中对密码模块类型的定义。

AS02.04：（安全级别 1，2，3，4）
对于硬件和固件模块，GM/T 0028 7.7 节中规定的物理安全和 GM/T 0028 7.8 节中规定的非入侵式安全要求应当适用。

送检单位需要提交的材料

VE02.04.01：对于硬件和固件模块，送检单位应在文档中说明应对物理和非入侵攻击的安全策略。

所需的检测程序

TE02.04.01：检测人员应执行并核准密码模块产品是否通过 GM/T 0028 7.7 节中规定的物理安全和 GM/T 0028 7.8 节中规定的非入侵式安全要求相关测试。

AS02.05：（安全级别 1，2，3，4）
{对于混合模块}软件和固件部件应当满足 GM/T 0028 7.5 节中规定的软件/固件安全和 GM/T 0028 7.6 节中规定的运行环境中的所有适用要求。

送检单位需要提交的材料

VE02.05.01：对于混合模块，送检单位应在文档中说明软件和固件部件针对软件/固件安全

和运行环境所采用的安全策略。

所需的检测程序

TE02.05.01：检测人员应执行并核准密码模块产品是否通过 GM/T 0028 7.5 节中规定的软件/固件安全和 GM/T 0028 7.6 节中规定的运行环境相关测试。

AS02.06：（安全级别 1，2，3，4）
{对于混合模块}硬件部件应当满足 GM/T 0028 7.7 节中规定的物理安全和 GM/T 0028 7.8 节中规定的非入侵式安全中的所有适用要求。

送检单位需要提交的材料

VE02.06.01：对于混合模块，，送检单位应在文档中说明硬件部件应对物理和非入侵攻击的安全策略。

所需的检测程序

TE02.06.01：检测人员应执行并核准密码模块产品是否通过 GM/T 0028 7.7 节中规定的物理安全和 GM/T 0028 7.8 节中规定的非入侵式安全要求相关测试。

6.3.3　密码边界

6.3.3.1　密码边界通用要求

AS02.07：（安全级别 1，2，3，4）
密码边界应当由定义明确的边线（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。

注：本条款不单独进行检测。

AS02.08：（安全级别 1，2，3，4）
GM/T 0028 中的安全要求适用于模块密码边界内的所有算法、安全功能、进程和部件。

注：本条款不单独进行检测。

AS02.09：（安全级别 1，2，3，4）
密码边界应当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（即本标准范围内与安全相关的）。

送检单位需要提交的材料

VE02.09.01:，送检单位应明确标识密码模块内所有安全相关的安全功能，包括：

——分组密码；
——流密码；
——非对称密钥；
——消息鉴别码；
——杂凑函数；
——实体鉴别；
——密钥建立；
——随机数生成器。

VE02.09.02：送检单位应明确标识与安全功能对应的密码算法。

所需的检测程序

TE02.09.01：检测人员应确认本条款下所有已明确标识的安全功能都包括在条款 AS02.07 的密码边界内。

TE02.09.02：检测人员应核实，与安全功能的对应的密码算法能否满足安全功能的要求。

AS02.10：（安全级别 1，2，3，4）
用于核准工作模式的非安全相关的算法、安全功能、进程和部件的实现应当不干扰或破坏密码模块核准的操作。

送检单位需要提交的材料

VE02.10.01：如果密码模块边界内包含非安全相关的算法、安全功能、进程和部件，则需要在送检单位的文档中一一列举并描述其使用范围和场景。

VE02.10.02：送检单位应明确说明用于核准工作模式的非安全相关的算法、安全功能、进程和部件的实现应当不干扰或破坏密码模块核准的操作。

所需的检测程序

TE02.10.01：检测人员应核实送检单位提供的密码模块边界内包含的非安全相关的算法、安全功能、进程和部件。

TE02.10.02：检测人员应核实用于核准工作模式的非安全相关的算法、安全功能、进程和部件的实现应当不干扰或破坏密码模块核准的操作。

AS02.11：（安全级别 1，2，3，4）
密码模块的名称应当代表密码边界内的部件构成，不应代表大于原有范围的构成或产品。

送检单位需要提交的材料

VE02.11.01：送检单位需在文档中明确说明密码模块的名称。

所需的检测程序

TE02.11.01：检测人员应核实送检单位提供的密码模块名称是否代表密码边界内的部件构成，是否大于原有范围的构成或产品。

AS02.12：（安全级别 1，2，3，4）
密码模块应当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。

送检单位需要提交的材料

VE02.12.01：送检单位需提供密码模块每个互不相同的硬件、软件和/或固件部件的特定版本信息。

所需的检测程序

TE02.12.01：检测人员应核实送检单位提供的密码模块每个互不相同的硬件、软件和/或固件

部件的特定版本信息。

AS02.13：（安全级别 1，2，3，4）
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当不干扰或破坏密码模块核准的安全操作。

送检单位需要提交的材料

VE02.13.01：送检单位需在文档中明确指出被排除的硬件、软件或固件部件，并说明其实现不干扰或破坏密码模块核准的安全操作。

VE02.13.02：送检单位需在文档中阐明被排除的硬件、软件或固件的原因。

所需的检测程序

TE02.13.01：检测人员应核实被排除的硬件、软件或固件部件的实现不干扰或破坏密码模块核准的安全操作。

TE02.13.02：检测人员应核实阐明的被排除的硬件、软件或固件的原因是否充分。

AS02.14：（安全级别 1，2，3，4）
密码模块规格说明文档应当阐明被排除的硬件、软件或固件。

送检单位需要提交的材料

VE02.14.01：送检单位需提供密码模块规格说明文档，并按照 GM/T 0028 附录 A 中的要求阐述被排除的某些硬件、软件和/或固件部件。

所需的检测程序

TE02.14.01：检测人员应核实送检单位提供的密码模块规格说明文档中，是否按照 GM/T 0028 附录 A 中的要求，对被排除的硬件、软件或者固件进行了阐明。

6.3.3.2　密码边界的定义

AS02.15：（安全级别 1，2，3，4）
硬件密码模块的密码边界应当划界并确定：
——在部件之间提供互联的物理配线的物理结构，包括电路板、基底或其它表面贴装；
——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；
——封套、灌封或封装材料、连接器和接口之类的物理结构；
——固件，可能包含操作系统；
——上面未列出的其它部件类型。

送检单位需要提交的材料

VE02.15.01：送检单位需在文档中指明硬件密码模块边界内的所有硬件、软件和固件组件，并提供硬件清单。

VE02.15.02：送检单位的文档应指明模块的密码边界。此边界应是明确定义而且连续的外围以确立此模块的物理边界。边界定义应指明模块组件及其连接（端口），以及模块组件之间

的信息流，处理流程和输入/输出数据。

VE02.15.03：密码模块边界应包括所有的输入、处理或输出重要安全参数的硬件或软件。

VE02.15.04：送检单位文档应指明如 GM/T 0028 密码模块安全要求中所定义模块的物理实体——即，单芯片密码模块，多芯片嵌入式密码模块，或多芯片独立式密码模块。

VE02.15.05：送检单位的文档应标明模块的内部布局和安装方式（例如固定件和安装件），包括最接近尺寸的图纸。该图纸不需要显示集成电路的内部构成。

VE02.15.06：送检单位的文档应描述模块的主要物理参数，包括对外壳、接入点、电路板、电源位置、电路接线、冷却系统以及其他关键参数的说明。

所需的检测程序

TE02.15.01：检测人员应核实送检单位提供的文档中提供了密码模块的所有硬件，软件和固件组件的清单。

TE02.15.02：检测人员应核实密码模块组件清单中的以下类型组件，除了未使用的组件类型外：

——处理器，包括微处理器，数字信号处理器，定制处理器，微控制器，或任何其他类型的处理器；
——存储程序的可执行代码和数据的 ROM 集成电路，这可能包括掩膜编程 ROM，可编程 ROM（PROM）如紫外线可擦除 PROM（EPROM）、电可擦除 PROM（EEPROM）或 Flash 存储器；
——随机访问存储器(RAM)或其他用于临时数据存储的集成电路；
——半定制、专用集成电路，如门阵列、可编程逻辑阵列、现场可编程门阵列或其他可编程逻辑元件；
——全定制、专用集成电路，包括任何自定义的密码集成电路；
——其他的有源电子电路元件（如果无源电路元件作为密码模块的一部分但不提供相关安全功能，送检单位就不必将其列出，如上拉/下拉电阻或旁路电容这样的元件）；
——电源组件，包括电源、电压转换模块（例如，交流—直流或直流—直流模块）、变压器、输入电源连接器和输出电源连接器；
——电路板或其他安装在表面的组件；
——外壳，包括任何可移除封门或封盖；
——加密模块外部设备的或任何主要的独立子模块之间的物理连接器；
——可修改的软件/固件模块；
——不可修改的软件/固件模块；
——其他上面未列出的组件类型。

TE02.15.03：检测人员应核实组件清单与本小节的其他条款提供的信息一致，其定义如下：

——密码模块的边界说明。核实所有在密码边界内的组件已包含在组件清单内，所有密码模块边界外的组件没有被列为密码模块组件；
——处理器和软件/固件说明。核实组件清单中的处理器，软件模块和硬件模块符合要求；
——物理配置说明。核实组件清单中的物理结构列表（如电路板或其他安装表面，外壳和连接器）和 AS02.15 的说明一致；
——框图说明。核实框图中的所有个体组件（如处理器，专用集成电路）也在组件清单中都有列出；
——在 AS02.13 条款规定之下被 GM/T 0028 要求排除在外的组件。核实应排除在外的组件仍在组件清单中列出。

TE02.15.04：检测人员应核实文档明确界定了密码模块的物理边界。这可以通过提供一个密码模块内的所有主要元器件和用来连接密码模块外部设备端口的清单来说明。文档还应提供密码模块内的重要信息流和在密码模块内执行的进程，以及所有输入或输出到密码模块边界外的信息的清单。

TE02.15.05：检测人员应核实送检单位提供的文档包含密码边界处的组件足够多的细节描述来精确定义密码边界。

TE02.15.06：检测人员应核实密码边界是物理连续的，以保证没有任何漏洞可以让非受控的输入、输出或其他接口进入密码模块。（物理和侵害保护的要求在 GM/T 0028 的 7.7 节分别有说明。）模块设计还必须确保密码模块没有不受控的输入输出接口，这些接口可能泄漏关键安全参数（CSP）、明文数据或其他一旦被误用就可能导致危险的信息。

TE02.15.07：检测人员应核实密码边界包括了所有输入、输出或 CSP 处理、明文以及其他一旦被滥用就可能导致危险的组件，且这些组件与送检单位提供的系统框图相一致。

TE02.15.08：作为上述要求的一个部分特例，送检单位可在满足 AS02.13 节的要求后被允许从 GM/T 0028 的要求中排除某些特定组件。送检单位可以与处理排除在密码边界之外的组件一样有效的处理上述组件。这种情况下，检测人员应核实被排除组件和其他模块之间的所有接口或物理连接，不允许不受控的泄露 CSP、明文数据，或其他一旦被误用就可能导致危险的信息。

TE02.15.09：检测人员应核实送检单位明确了密码模块是一个如 GM/T 0028 的 7.7 节定义的单芯片模块，多芯片嵌入式模块或多芯片独立式模块。

TE02.15.10：检测人员应核实送检单位的文档中包含最接近实际尺寸的图纸，其中显示了模块的内部布局，包括主要可识别组件的位置和大致尺寸。

TE02.15.11：检测人员应核实送检单位的文档显示了模块的主要物理部件以及它们是以何种方式组装或插入到模块中的。

TE02.15.12：检测人员应核实送检单位的文档描述了模块的主要物理参数。这至少包括以下内容：

——外壳的形状和大致尺寸，包括所有的封门或封盖；
——电路板大致尺寸，布局和内部连接；
——电源，电源转换器和电源输入及输出的位置；
——电路接线：通路和端子；
——冷却系统，如导板、冷却气流、换热器、散热片、风扇或其他散热安排；
——其他上面未列出的组件类型。

AS02.16：（安全级别 1，2，3，4）
软件密码模块的密码边界应当划界并确定：
——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。

送检单位需要提交的材料

VE02.16.01：送检单位需提供软件密码模块边界内的所有可执行文件或文件集，并提供软件文件清单。

VE02.17.02：送检单位文档应给出包括软件部件如何交互的内部软件架构。

VE02.17.03：送检单位文档应给出密码模块所运行的软件环境（例如操作系统，运行时库等）。

所需的检测程序

TE02.16.01：检测人员应核实送检的构成密码模块的可执行文件或文件集是否与软件文件清单一致。

TE02.17.02：检测人员应核实送检单位文档给出的包括软件部件如何交互的内部软件架构。

TE02.17.03：检测人员应核实送检单位文档给出的密码模块所运行的软件环境。

AS02.17：（安全级别 1，2，3，4）
固件密码模块的密码边界应当划界并确定：
——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。

送检单位需要提交的材料

VE02.17.01：送检单位需提供固件密码模块边界内的所有可执行文件或文件集，并提供固件文件清单。

VE02.17.02：送检单位文档应给出包括固件部件如何交互的内部软件架构。

VE02.17.03：送检单位文档应给出密码模块所运行的固件环境（例如操作系统，运行时库等）。

所需的检测程序

TE02.17.01：检测人员应核实送检的构成密码模块的可执行文件或文件集是否与固件文件清单一致。

TE02.17.02：检测人员应核实送检单位文档给出的包括固件部件如何交互的内部软件架构。

TE02.17.03：检测人员应核实送检单位文档给出的密码模块所运行的固件环境。

AS02.18：（安全级别 1，2，3，4）
混合密码模块的密码边界应当：
——由模块硬件部件的边界以及不相交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。

送检单位需要提交的材料

VE02.18.01：送检单位需在文档中指明混合密码模块边界内的所有硬件、软件和固件组件，并提供文件清单。

VE02.18.02：送检单位需在文档中指明所有端口和接口的标识及功能。

所需的检测程序

TE02.18.01：检测人员应核实送检的硬件、软件和固件组建是否与清单一致。

TE02.18.02：检测人员应核实送检密码模块的端口和接口是否与文档描述一致。

6.3.4 工作模式

6.3.4.1 工作模式通用要求

AS02.19：（安全级别 1，2，3，4）
操作员应当能够在核准的工作模式下操作模块。

送检单位需要提交的材料

VE02.19.01：送检单位需提供文档，明确阐述密码模块核准的工作模式。

VE02.19.02：送检单位应在文档中说明如何启用核准的工作模式及指令。

所需的检测程序

TE02.19.01：检测人员应核实操作员可以在核准的工作模式下操作密码模块。

AS02.20：（安全级别 1，2，3，4）
一个核准的工作模式应当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、安全功能或进程、以及那些规定于 GM/T 0028 的第 7.4.3 节中的服务或进程。

送检单位需要提交的材料

VE02.20：送检单位需提供文档，说明密码模块核准的工作模式所使用的核准的密码算法、安全功能或进程、以及那些规定于 GM/T 0028 的第 7.4.3 节中的服务或进程。

所需的检测程序

TE02.20.01：检测人员应核实文档中所描述的核准的工作模式，至少有一个服务使用了核准的密码算法、安全功能或进程、以及那些规定于 GM/T 0028 的第 7.4.3 节中的服务或进程。

TE02.20.02：检测人员应核实文档中所描述的核准的工作模式，使用的安全功能符合 GM/T 0028 附录 C 的规定。

AS02.21：（安全级别 1，2，3，4）
非核准的密码算法、安全功能和进程或其它未规定于 GM/T 0028 第 7.4.3 节中的服务不应当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进程的一部分，而且与核准的进程操作非安全相关。

送检单位需要提交的材料

VE02.21.01：送检单位需提供文档说明核准的工作模式中未使用非核准的密码算法、安全功能和进程或其它未规定于 GM/T 0028 第 7.4.3 节中的服务。

VE02.21.02：如果核准的工作模式中使用了非核准的密码算法或安全功能，送检单位需提供文档应说明非核准的密码算法或安全功能是核准的进程的一部分，而且与核准的进程操作非安全相关。

所需的检测程序

TE02.21.01：检测人员应核实密码模块核准的工作模式中未使用非核准的密码算法、安全功能和进程或其它未规定于 GM/T 0028 第 7.4.3 节中的服务。

TE02.21.02：如果核准的工作模式中使用了非核准的密码算法或安全功能，检测人员应核实非核准的密码算法或安全功能与核准的进程操作非安全相关。

6.3.4.2 正常工作

AS02.22：（安全级别 1，2，3，4）
核准的和非核准的服务和工作模式的 CSP 应当相互分离。

送检单位需要提交的材料

VE02.22.01：送检单位需提供文档，详细描述核准的和非核准的服务和工作模式的操作方式，并说明 CSP 是如何分离的。

所需的检测程序

TE02.22.01：检测人员应核实核准的和非核准的服务和工作模式的 CSP 应当相互分离，相互之间不能共享和相互访问。

AS02.23：（安全级别 1，2，3，4）
模块的安全策略应当定义一组服务的完备集合，包括提供给每个定义的工作模式（核准的和非核准的）的服务。

送检单位需要提交的材料

VE02.23.01：送检单位需提供文档说明密码模块所包含的安全策略。

所需的检测程序

TE02.23.01：检测人员应核实每个工作模式所包含的安全策略是否完备。

AS02.24：（安全级别 1，2，3，4）
当服务以核准的方式使用核准的密码算法、安全功能或进程、以及其它规定于 GM/T 0028 第 7.4.3 节中的服务或进程时，上述服务应当给出相应的指示。

送检单位需要提交的材料

VE02.24.01：送检单位需提供文档说明当服务以核准的方式使用核准的密码算法、安全功能或进程、以及其它规定于 GM/T 0028 第 7.4.3 节中的服务或进程时，其状态的指示方式。

所需的检测程序

TE02.24.01：检测人员应核实状态指示方式的合理性和有效性。

6.3.4.3 降级工作

AS02.25：（安全级别 1，2，3，4）
对于密码模块在降级工作中运行，下列{AS02.26-AS2.30}要求应当适用：

注：本条款不单独进行检测。

AS02.26：（安全级别 1，2，3，4）
应当只能在退出错误状态之后，进入降级工作。

送检单位需要提交的材料

VE02.26.01：送检单位提供的密码模块支持降级功能。

VE02.26.02：送检单位提供密码模块进入错误状态的操作文档。

所需的检测程序

TE02.26.01：检测人员应核实密码模块是否支持降级功能。

TE02.26.02：检测人员应核实密码模块只能在退出错误状态之后，才进入降级工作。

AS02.27：（安全级别 1，2，3，4）
模块应当在进入重新配置的和降级的工作时，提供状态信息。

送检单位需要提交的材料

VE02.27.01：送检单位提供的密码模块支持降级功能。

VE02.27.02：送检单位提供密码模块进入重新配置的和降级的工作时的提示信息说明文档。

所需的检测程序

TE02.27.01：检测人员应核实密码模块重新配置的和降级的工作时，提示相关状态信息，并确认提示信息的合理性和有效性。

AS02.28：（安全级别 1，2，3，4）
应当隔离失效的机制或功能。

送检单位需要提交的材料

VE02.28.01：送检单位提供密码模块具有失效能力的说明文档，并阐述该机制或功能失效后的隔离方式。

所需的检测程序

TE02.28.01：检测人员应核实失效的机制或功能已被隔离。

AS02.29：（安全级别 1，2，3，4）
应当在进入降级工作后第一次运行使用之前，执行所有条件算法自测试。

送检单位需要提交的材料

VE02.29.01：送检单位提供文档说明密码模块所支持的条件算法。

VE02.29.02：送检单位提供文档中应声明密码模块在进入降级工作后第一次运行使用之前，执行了所有条件算法自测试。

所需的检测程序

TE02.29.01：检测人员应核实密码模块进入降级工作后第一次运行使用之前，是否执行了所有条件算法的自测试。

AS02.30：（安全级别 1，2，3，4）
如果尝试使用失效的算法、安全功能、或进程，服务应当给出指示。

送检单位需要提交的材料

VE02.30.01：送检单位提供文档说明使用失效的算法、安全功能、或进程，服务时，密码模块产品所给出的指示信息列表。

所需的检测程序

TE02.30.01：检测人员应核实使用失效的算法、安全功能、或进程，服务时，密码模块是否给出与文档一致的指示信息。

AS02.31：（安全级别 1，2，3，4）
密码模块应当停留在降级工作中，直到密码模块成功通过所有运行前以及条件自测试。

送检单位需要提交的材料

VE02.31.01：送检单位提供的密码模块支持降级功能，并在文档中说明从降级工作模式恢复到正常工作模式前，执行的运行前以及条件自测试。

所需的检测程序

TE02.31.01：检测人员应核实密码模块在未通过所有运行前以及条件自测试前，是否停留在降级工作中。

TE02.31.01：检测人员应核实密码模块在通过所有运行前以及条件自测试后，是否恢复到正常工作模式。

AS02.32：（安全级别 1，2，3，4）
如果密码模块没有通过运行前自测试，模块不应当进入降级工作。

注：本条款作为 AS02.31 的一部分进行检测。

6.4 密码模块接口

6.4.1 密码模块接口通用要求

AS03.01：（安全级别 1，2，3，4）
所有进出密码模块的逻辑信息流，都应当只能通过已定义的物理端口和逻辑接口，这些端口和接口应当是出入模块密码边界的入口点和出口点。

送检单位需要提交的材料

VE03.01：送检单位提供文档说明密码模块所支持的所有物理端口和逻辑接口。

所需的检测程序

TE03.01.01：检测人员应核实密码模块是否具备文档中所描述的物理端口和逻辑端口。

TE03.01.02：检测人员应核实密码模块只能通过这些端口作为模块密码边界的入口点和出口点。

AS03.02：（安全级别 1，2，3，4）
密码模块逻辑接口应当是相互分离的，这些逻辑接口可以共享一个物理端口。

送检单位需要提交的材料

VE03.02.01：送检单位提供文档说明密码模块所有逻辑接口是相互分离的。

VE03.02.02：送检单位文档中应列举共享一个物理端口的逻辑接口。

所需的检测程序

TE03.02.01：检测人员应核实密码模块的逻辑端口是相互分离的。

AS03.03：（安全级别 1，2，3，4）
文档应当按照 GM/T 0028 A.2.3 的要求编写。

送检单位需要提交的材料

VE03.03.01：送检单位应按照 GM/T 0028 附录 A.2.3 的要求提供密码模块接口说明文档。

所需的检测程序

TE03.03.01：检测人员应核准密码模块接口说明文档是否符合 GM/T 0028 附录 A.2.3 的要求。

6.4.2 接口类型

本小节没有需要单独进行检测的项目。

6.4.3 接口定义

AS03.04：（安全级别 1，2，3，4）
密码模块应当具备下列五种接口：
——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

注：本条款不单独进行检测。

AS03.05：（安全级别 1，2，3，4）
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、SSP 和另一个模块的状态信息，应当通过“数据输入”接口输入。当模块执行自测试时，模块可以通过数据输入接口接收数据。

送检单位需要提交的材料

VE03.05.01：密码模块应有数据输入接口。所有输入到模块和由模块处理的数据（除通过控制输入接口输入的控制数据）应通过数据输入接口进入，包括：

——明文数据；
——密文或签名数据；
——加密密钥和其他密钥管理数据（明文或密文）；
——认证数据（明文或加密的）；
——来自外部渠道的状态信息；
——其他输入数据。

VE03.05.02：如适用，送检单位的文档应明确指明所有与密码模块同时使用的外部输入设备，此设备用于输入数据到数据输入接口，如智能卡，令牌，键盘，密钥加载器，和/或生物识别设备。

所需的检测程序

TE03.05.01：检测人员应通过检查，核实密码模块包括数据输入接口，并且其功能如前所述。检测人员应核实所有输入到模块和由密码模块处理的（除控制数据通过控制输入接口进入外）数据经数据输入接口进入，包括：

——待加密或签名的明文数据；
——用于由模块解密或验证的密文及签名数据；
——输入到模块或由模块使用的明文或加密密钥以及其他密钥管理，包括数据和向量初始化，分片密钥信息，和/或密钥核算信息（其他密钥管理要求包含在 GM/T 0028 密码模块安全要求的 7.9 节中）；
——输入到密码模块的明文或加密认证数据，包括登录口令，PIN，和/或生物识别设备；
——自外部渠道的状态信息（如，其他密码模块或设备）；
——除 AS03.08 中涵盖的控制信息外，任何其他输入到密码模块中用于处理或存储的信息。

注：对于安全等级 1 和 2，物理端口或用于 CSP 明文输入的端口可能与密码模块的其他物理端口共享（安全等级 3 和 4 对应的要求分散在 AS03.16~AS03.22 中）。

TE03.05.02：检测人员应核实送检单位的文档是否详述了任何与密码模块一起使用并用于输入数据到数据输入接口的外部输入设备，如智能卡，令牌，键盘，密钥加载器，和或生物识别设备。检测人员应使用经认证的外部输入设备输入数据到数据接口，并核实使用外部输入设备输入数据功能如文档所述。

AS03.06：（安全级别 1，2，3，4）
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 SSP 等，应当通过“数据输出”接口输出。

送检单位需要提交的材料

VE03.06.01：密码模块应具有数据输出接口。所有已被处理以及由密码模块输出的数据（除通过状态输出接口输出的状态字外），包括：

——明文数据；
——密文数据和数字签名；
——加密密钥和其他密钥管理数据（明文或加密的）；
——对外部目标的控制信息；
——其他输出数据。

注：对于安全等级 1 和 2，物理端口和用于明文加密密钥和其他明文 CSP 输出的端口可能与密码模块的其他物理端口共享。（安全等级 3 和 4 对应的要求分散在 AS03.16~AS03.22 中）。

VE03.06.02：如适用，送检单位的文档应详细说明所有和密码模块同时使用并用于从数据输出接口输出数据的外部输出设备，如智能卡，令牌，显示，和/或其他存储设备。

所需的检测程序

TE03.06.01：检测人员应通过检查，核实密码模块具有如前所述的数据输出接口和数据输出接口功能。检测人员须核实所有被密码模块处理的和由模块输出的数据（除通过状态数据输出接口输出的状态数据外），包括：

——已由密码模块解密的明文数据；
——已加密的密文数据，和由密码模块生成的数字签名；
——在内部产生并由模块输出的明文或加密密钥以及其他密钥管理数据，包括初始化数据和向量，分片密钥信息，和/或密钥统计信息（其他的密钥管理要求在 GM/T 0028 密码模块安全要求中）；
——密码模块输出外部目标的控制信息（如，另一个密码模块或设备）；
——其他由密码模块处理或存储后输出的信息，AS03.11 中说明的状态信息例外。

注：对于安全等级 1 和 2，物理端口和用于输出明文 CSP 的端口可能与其他密码模块的物理端口共享对于安全等级 3 和 4，检测人员应分别检测 AS03.18 和 AS03.19 小节中的相应要求。

TE03.06.02：检测人员应核实送检文档是否具体说明了任何与密码模块同时使用并用于从数据输出接口输出数据的外部输出设备，如智能卡，令牌，显示，和/或其他存储设备。检测人员应使用经确认的外部输出设备，并核实使用外部输出设备输出的数据与文档所述一致。

AS03.07：（安全级别 1，2，3，4）
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，应当禁止通过“数据输出”接口输出数据。

送检单位需要提交的材料

VE03.07.01：送检单位文档应具体说明密码模块如何确保模块处在错误状态时，数据输出接口禁止输出所有数据（错误状态在 GM/T 0028 密码模块安全要求的 7.11.4 小节中说明）。只要不含 CSP，明文数据或其他滥用可能造成安全威胁的信息，状态信息可从状态输出接口输出以确定错误的类型。

VE03.07.02：送检单位的文档应具体说明密码模块的设计如何能确保模块在自检时，数据输出接口禁止输出所有数据（自检在 GM/T 0028 密码模块安全要求的 7.10 节说明）。只要不含 CSP，明文数据或其他滥用可能造成安全威胁的信息，显示自检的状态信息可从状态输出接口输出以确定错误类型。

所需的检测程序

TE03.07.01：检测人员应核实送检单位的文档具体说明了在错误状态时，数据输出接口禁止输出所有数据。检测人员应通过送检单位的文档核实一旦探测到错误条件并进入错误状态，数据输出接口应禁止输出所有数据，直到从错误中恢复过来。只要检测人员核实不含 CSP，明文数据或其他滥用可能造成安全威胁的信息，用来确定错误的类型的状态信息可允许从状态输出接口输出。

TE03.07.02：检测人员应使密码模块进入每个指定的错误状态，并验证此时数据输出接口禁止输出所有数据。如果状态信息是从状态输出接口输出以确定错误类型，检测人员应验证这些输出信息为非敏感信息。下面的操作可使密码模块进入错误状态，即：打开防篡改封盖或

封门，输入非正确格式的命令、密钥或参数，降低输入电压和/或其他任何引起错误的操作。如果检测人员不能使模块产生错误，送检单位须对检测人员提供该检测不能进行的合理解释。

TE03.07.03：检测人员应核实送检单位的文档具体说明了密码模块处于自检模式时，数据输出接口禁止输出所有数据。检测人员应通过送检单位的文档核实模块一旦执行自检，数据输出接口禁止输出所有数据，直至自检结束。只要检测人员核实不含 CSP，明文数据或其他滥用可能造成安全威胁的信息，用来显示自检结果的状态信息可允许从状态输出接口输出。

TE03.07.04：检测人员应使模块执行自检并确认数据输出接口禁止所有数据的输出。如果状态信息从状态输出接口输出用以显示自检结果，检测人员应核实其不含 CSP，明文数据或其他滥用可能造成安全威胁的信息。
如果检测人员不能使模块产生错误，送检单位须对检测人员提供该检测不能进行的合理解释。

TE03.07.05：检测人员应核实送检单位的文档具体说明了密码模块如何确保在自检或错误模式下数据输出接口禁止输出所有数据。检测人员还应通过检查，核实密码模块的设计，即数据输出接口无论是在逻辑上还是物理上在上述情况下是禁用的。

AS03.08：（安全级别 1，2，3，4）
所有用于控制密码模块操作的输入命令、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）应当通过“控制输入”接口输入。

送检单位需要提交的材料

VE03.08.01：密码模块应具有控制输入接口。用于控制密码模块操作的所有命令，信号和控制数据（除经数据输入接口输入的数据）须经控制输入接口进入，包括：

——命令输入，逻辑上通过 API 输入（如，软件和密码模块的固件）；
——信号输入，逻辑或物理上通过一个或多个的物理端口（如，密码模块的硬件组件）
——手动控制输入（如，使用开关，按钮或键盘）；
——其他输入控制数据。

VE03.08.02：如适用，送检单位的文档应具体说明所有与密码模块一起使用并用于向控制输入接口输入命令，信号和控制数据的外部输入设备，如智能卡，令牌，或键盘。

所需的检测程序

TE03.08.01：检测人员应通过检查，核实密码模块包括了控制输入接口，并且控制输入接口如前所述。检测人员应检查用于控制密码模块操作的所有命令，信号，和控制数据（除通过数据输入接口输入的数据）都应通过控制输入接口输入，包括：

——命令输入，逻辑上通过 API 输入，如调用软件库或智能卡的函数；
——信号输入，逻辑或物理上通过一个或多个物理端口输入的信号，如通过串行端口或 PC 卡下发的命令或信号；
——手动控制输入（如，使用开关，按钮，或键盘）；
——其他输入控制数据。

TE03.08.02：检测人员核实送检单位的文档是否具体说明了用于向控制输入接口输入命令，信号和控制数据的所有外部输入设备，如智能卡，令牌，或键盘。检测人员应通过控制输入接口使用可识别的外部输入设备输入命令，并确认使用外部设备输入命令与文档所述一致。

AS03.09：（安全级别 1，2，3，4）
所有用于控制密码模块操作的输出命令、信号及控制数据（例如，对另一个模块的控制命

令）应当通过“控制输出”接口输出。

送检单位需要提交的材料

VE03.09：密码模块应具有控制输出接口，用于控制密码模块操作的输出命令，信号和控制数据须经控制输出接口输出。

所需的检测程序

TE03.09：检测人员应核实用于控制密码模块操作的输出命令，信号和控制数据是否经控制输出接口输出。

AS03.10：（安全级别 1，2，3，4）
当密码模块处于错误状态时，应当禁止通过“控制输出”接口的控制输出，除非在安全策略中有规定和记载了一些例外情况。

送检单位需要提交的材料

VE03.10.01：送检单位提供的密码模块应具有控制输出接口。

VE03.10.02：送检单位提供文档说明密码模块处于错误状态时，采用什么策略来禁止密码模块通过“控制输出”接口来输出。

所需的检测程序

TE03.10：检测人员应核实当密码模块处于错误状态时，是否禁止通过“控制输出”接口输出。

AS03.11：（安全级别 1，2，3，4）
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））应当通过“状态输出”接口输出。

送检单位需要提交的材料

VE03.11.01：密码模块应具有状态输出接口。所有用于显示或指示模块状态的状态信息，信号，逻辑指示以及物理指示仪应通过状态输出接口输出，包括：

——状态信息输出，逻辑上通过 API 输出；
——信号输出，逻辑或物理上通过一个或多个物理端口输入的信号，如通过串行端口或 PC 卡下发的命令或信号；
——手动状态输出（如，使用 LED，蜂鸣器，或显示器）；
——其他输出状态信息。

VE03.11.02：如适用，送检单位文档应具体说明所有的外部输出设备，该类设备用于通过状态输出接口输出状态信息，信号，逻辑指示和物理指示，如智能卡，令牌，显示器和/或其他存储设备。

所需的检测程序

TE03.11.01：检测人员应通过检查，核实密码模块包括了状态输出接口，且状态输出接口功能如前所述。检测人员应检查所有用于指示或显示模块状态的状态信息，信号，逻辑指示，和物理指示仪应通过状态输出接口输出，包括：

——状态信息输出，逻辑上通过 API 输出，如调用软件库或智能卡的函数；
——信号输出，逻辑或物理上通过一个或多个物理端口输入的信号，如通过串行端口或 PC 卡下发的状态信息；
——手动状态输出（如，使用 LED，蜂鸣器，或显示器）；
——其他输出状态信息。

TE03.11.02：检测人员应核实送检单位的文档具体说明了所有的外部输出设备（如适用），该类设备用于通过状态输出接口输出状态信息，信号，逻辑指示和物理指示，如智能卡，令牌，显示器和/或其他存储设备。

AS03.12：（安全级别 1，2，3，4）
除软件密码模块以外，所有模块还应当具备下列接口：
——电源接口

送检单位需要提交的材料

VE03.12：送检单位提供的密码模块产品应具备电源接口（除非所有能量由密码模块的密码边界内部提供或维持时）。

所需的检测程序

TE03.12：检测人员应确认送检产品具备电源接口或内部电池。

AS03.13：（安全级别 1，2，3，4）
输入密码模块的所有外部电能应当通过电源接口输入。

送检单位需要提交的材料

VE03.13.01：如果密码模块需要向密码边界外的其他元件提供电源，或从密码边界外的其他元件获取供电（例如，电源或外接电池），送检文档应指定电源接口及相关的物理端口。

VE03.13.02：所有的从密码模块输入或输出到密码边界外的其他元件的电源应通过指定电源接口。

所需的检测程序

TE03.13.01：检测人员应确认送检单位文档是否详细说明，该密码模块是否需要从密码边界外的其他元件获取供电，或者是否向密码边界外的其他元件提供电源（例如，电源、电源线、电源插口/插座，或外部电池）。检测人员还应确认送检单位文档指定的电源接口和相应的物理端口。

TE03.13.02：通过检查密码模块，检测人员应确认从密码模块输入或输出到密码边界外的其他元件的电源通过指定的电源接口。

注：如果模块内部可提供或维持所需电源，则不需要电源接口，内嵌电池作为物理维持行为替换电源接口，在 GM/T 0028 密码模块安全要求的 7.11.4 小节中有详细说明。

AS03.14：（安全级别 1，2，3，4）
密码模块应当区分数据、控制信息和能量输入，以及数据、控制信息和状态信息输出。

送检单位需要提交的材料

VE03.14.01：送检单位文档应详细说明密码模块是如何识别输入数据和控制数据，及输出数

据和输出状态。通过密码模块输入接口输入数据和控制信息的物理和逻辑路径，在物理上和逻辑上是如何与通过密码模块输出接口输出数据和状态信息的物理和逻辑路径区分开来的。

VE03.14.02：送检单位文档应指出用于输入数据和控制信息的物理逻辑路径如何在物理上和逻辑上与用于输出数据和状态信息的物理逻辑路径区分开来。如果用于输入数据和控制信息的物理逻辑路径与用于输出数据和状态信息的物理逻辑路径是物理共享的，送检单位文档应详细说明密码模块是如何强制实现逻辑分离。

所需的检测程序

TE03.14.01：检测人员应确认送检单位文档详细说明了密码模块如何区分输入数据、控制数据以及输出数据、输出状态。数据输入接口输入数据，控制输入接口输入控制信息，这些数据应在逻辑上或物理上与输出数据接口的输出数据和状态输出接口的状态信息区分开。

TE03.14.02：检测人员应确认送检单位文档详细说明了输入数据和控制信息的物理逻辑路径如何与输出数据和状态信息的物理逻辑路径如何在物理上和逻辑上分开。如果用于输入数据和控制信息的物理逻辑路径与用于输出数据和状态信息的物理逻辑路径是物理共享的，检测人员应确认送检单位文档详细说明了密码模块是如何强制实现逻辑分离的。

AS03.15：（安全级别 1，2，3，4）
密码模块规格应当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。

送检单位需要提交的材料

VE03.15.01：送检单位文档应详细说明密码模块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限制。

所需的检测程序

TE03.15.01：检测人员应核准密码模块说明文档是否按照 GM/T 0028 附录 A 的要求，详细描述密码模块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限制。

6.4.4 可信信道

AS03.16：（安全级别 3）
密码模块应当实现可信信道，用于在密码模块与发送者或接收者终端之间传输未保护的明文 CSP、密钥分量以及鉴别数据。

送检单位需要提交的材料

VE03.16.01：送检单位应在文档中描述可信信道的实现方式。

所需的检测程序

TE03.16.01：检测人员应核准密码模块是否实现可信信道。

AS03.17：（安全级别 3）
可信信道应当防止在通信链路上的非授权修改、替换和泄露。

送检单位需要提交的材料

VE03.17.01：送检单位应提供文档详细描述可信信道的数据保护方式。

所需的检测程序

TE03.17.01：检测人员未授权修改可信信道上传输的数据，应该不被接受。

TE03.17.02：检测人员替换可信信道上传输的数据，应该不被接受。

TE03.17.03：检测人员应无法侦听获取到可信信道上传输的数据。

AS03.18：（安全级别 3）
可信信道使用的物理端口应当与其它物理端口实现物理隔离。

送检单位需要提交的材料

VE03.18.01：送检单位应提供文档指明可信信道所使用的物理端口，并详细描述其如何与其他物理端口实现物理隔离。

所需的检测程序

TE03.18.01：检测人员应核实可信信道所采用的物理端口与其他物理接口物理上隔离。

AS03.19：（安全级别 3）
可信信道使用的逻辑接口应当与其它逻辑接口实现逻辑隔离。

送检单位需要提交的材料

VE03.19.01：送检单位应提供文档指明可信信道所使用的逻辑接口，并详细描述其如何与其他逻辑接口隔离。

所需的检测程序

TE03.19.01：检测人员应核实可信信道所采用的逻辑接口与其他逻辑接口逻辑上隔离。

AS03.20：（安全级别 3）
基于身份的鉴别应当用于所有使用可信信道的服务。

送检单位需要提交的材料

VE03.20.01：送检单位应在提供的文档中指出使用可用信道的服务，并描述使用这些服务前使用的身份鉴别方式和流程。

所需的检测程序

TE03.20：检测人员应核实在使用密码模块的可信信道服务前，必须进行基于身份的鉴别。

AS03.21：（安全级别 3）
当可信信道在使用时，应当提供状态指示器。

送检单位需要提交的材料

VE03.21.01：送检单位应在提供的文档中指出使用可用信道的状态指示器和状态信息。

所需的检测程序

TE03.21.01：检测人员应核实密码模块是否具有文档描述的可用信道状态指示器。

TE03.21.02：检测人员应核实可用信道在使用时，状态指示器是否正确指示状态。

AS03.22：（安全级别 4）
对于安全四级，除了安全三级的要求以外，多因素基于身份的鉴别应当用于所有使用可信信道的服务。

送检单位需要提交的材料

VE03.22.01：送检单位文档应详细指出密码模块所有使用可信信道的服务。

VE03.22.02: 送检单位文档应详细描述使用可信信道服务前，采用的身份鉴别方式和流程。

所需的检测程序

TE03.22.01：检测人员应核实在使用所有的可信信道的服务前，使用了有效的多因素身份鉴别方法来鉴别用户的身份。

6.5 角色、服务和鉴别

6.5.1 角色、服务和鉴别通用要求

AS04.01：（安全级别 1，2，3，4）
密码模块应当支持操作员的授权角色以及与每个角色相对应的服务。

注：本条款不单独进行检测。

AS04.02：（安全级别 1，2，3，4）
如果密码模块同时支持多个操作员，那么模块内部应当确保每个操作员担任的角色及相应的服务相隔离。

送检单位需要提交的材料

VE04.02.01：送检单位文档应详细说明是否允许多个操作员。送检单位应描述怎样实现每一操作员授权角色和相应服务分离的方法。

VE04.02.02：送检单位文档还应描述对多个操作员的限制（例如，不允许一个操作员既是维护工程师角色又是用户角色）。

所需的检测程序

TE04.02.01：检测人员应确认送检单位文档如实描述密码模块实现的多个操作员角色与服务强制分离的方法。

TE04.02.02：检测人员应承担两个独立操作员的身份：操作员 1 和操作员 2。操作员应赋予不同的角色。检测人员应确认，每个角色只执行分配于其角色的服务。对于每一个操作员，

检测人员应测试其可否执行其他操作员承担角色的服务，以此来确认不同操作员角色与服务的分离。

TE04.02.03：如果送检单位文档给出关于多个操作员行为的限制条件，检测人员应尝试以独立操作员身份并行地承担受限角色，尝试违反限制条件，以此核实模块通过阻止第二操作员承担角色，强制执行这些约束。

AS04.03：（安全级别 1，2，3，4）
文档应当按照 A.2.4 中规定的要求编写。

送检单位需要提交的材料

VE04.03.01：送检单位应按照 GB/T 0028 附录 A.2.4 中规定的要求提供文档。

所需的检测程序

TE04.03.01：检测人员应确认送检单位提供的文档符合 GB/T 0028 附录 A.2.4 中规定的要求。

6.5.2 角色

AS04.04：（安全级别 1，2，3，4）
密码模块应当至少支持密码主管角色。

送检单位需要提交的材料

VE04.04.01：送检单位的密码模块产品应包括至少一个密码主管角色。

所需的检测程序

TE04.04.01：检测人员应确认送检单位文档定义了至少一个密码主管角色。

AS04.05：（安全级别 1，2，3，4）
密码主管角色应当设定为执行密码初始化或管理功能，以及常用的安全服务，例如，模块初始化、CSP 和 PSP 的管理以及审计功能。

送检单位需要提交的材料

VE04.05.01：送检单位提供文档描述密码主管角色的功能，包括：执行密码初始化或管理功能，以及常用的安全服务，例如，模块初始化、CSP 和 PSP 的管理以及审计功能。

所需的检测程序

TE04.05.01：检测人员应确认给出的角色名和许可服务与上述文档说明相符。

注：承担角色应按 TE04.02.02 测试。

AS04.06：（安全级别 1，2，3，4）
如果密码模块支持用户角色，那么用户角色应当设定为执行常用的安全服务，包括加密操作和其它核准的安全功能。

送检单位需要提交的材料

VE04.06.01：如果密码模块有用户角色，送检单位文档应明确说明支持用户角色。文档应按名字和许可服务详细、完整的说明用户角色。

所需的检测程序

TE04.06.01：检测人员应确认送检单位文档的说明适合授权角色，并确认按名字、用途和许可服务说明用户角色。

注：承担角色应按 TE04.02.02 测试。

AS04.07：（安全级别 1，2，3，4）
当进入或退出维护角色时，所有不受保护的 SSP 应当被置零。

送检单位需要提交的材料

VE04.07.01：送检单位文档应详细说明当维护角色登录或退出时，模块的SSP是怎样动态清零的。

所需的检测程序

TE04.07.01：如果送检单位文档说明密码模块实现了维护角色，检测人员应确认送检单位文档详细说明当进入或退出维护角色时，清零所有未经加密的 SSP 的方法。

TE04.07.02：在非维护角色状态下，检测人员应为所有未经加密的 SSP 加载非零值。进入维护角色后，检测人员应确认清零已被执行。

TE04.07.03：在维护角色状态下，检测人员应为所有未经加密的 SSP 加载非零值，从维护角色退出后，检测人员应确认清零已被执行。

6.5.3 服务

6.5.3.1 服务通用要求

AS04.08：（安全级别 1，2，3，4）
服务应当指的是密码模块所能执行的所有服务、操作或功能。

注：本条款不单独进行检测。

AS04.09：（安全级别 1，2，3，4）
服务输入应当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。

注：本条款不单独进行检测。

AS04.10：（安全级别 1，2，3，4）
服务输出应当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。

注：本条款不单独进行检测。

AS04.11：（安全级别 1，2，3，4）

每个服务输入应当产生一个服务输出。

注：本条款不单独进行检测。

AS04.12：（安全级别 1，2，3，4）
密码模块应当为操作员提供下列服务：
a) 显示模块版本号；
b) 显示状态；
c) 执行自测试；
d) 执行核准的安全功能；
e) 执行置零。

注：本条款不单独进行检测。

AS04.13：（安全级别 1，2，3，4）
密码模块应当输出名称或模块标识符以及版本信息，这些信息可以与模块的审验记录相关联。

所需的送检单位文档
VE04.13.01：送检单位文档应说明密码模块具有输出名称或模块标识符以及版本信息的功能，并描述具体操作步骤和方法。

所需的检测程序

TE04.13.01：检测人员应确认“显示模块版本号”指标与送检单位文档符合。

AS04.14：（安全级别 1，2，3，4）
密码模块应当输出当前的状态。其中可能包括响应服务请求的状态指示器的输出。

所需的送检单位文档

VE04.14.01：送检单位文档应说明密码模块具有输出当前状态的功能，并描述具体操作步骤和方法。

所需的检测程序

TE04.14.01：检测人员应确认“显示状态”指标与送检单位文档符合。

AS04.15：（安全级别 1，2，3，4）
密码模块应当执行初始化和 GM/T 0028 7.10.2 中的运行前自测试。

所需的送检单位文档

VE04.15.01：送检单位文档应说明密码模块具有初始化和自测试功能，并描述具体操作步骤和方法。

所需的检测程序

TE04.15.01：检测人员应确认密码模块的初始化和自测试与送检单位文档符合。

AS04.16：（安全级别 1，2，3，4）
按照 GM/T 0028 7.2 中的规定，密码模块应当至少执行一个在核准的工作模式中使用的核准的安全功能。

所需的送检单位文档

VE04.16.01：送检单位文档应说明密码模块支持的核准的工作模式和使用的核准安全功能，并描述具体操作步骤和方法。

所需的检测程序

TE04.16.01：检测人员应确认密码模块至少可以执行一个在核准的工作模式中使用的核准的安全功能。

AS04.17：（安全级别 1，2，3，4）
按照 GM/T 0028 7.9.7 中的规定，密码应当执行参数置零。

所需的送检单位文档

VE04.17.01：送检单位文档应说明密码模块支持密码参数置零的功能，并描述具体操作步骤和方法。

所需的检测程序

TE04.17.01：检测人员应确认密码模块能够正确执行密码参数置零。

6.5.3.2　旁路能力

AS04.18：（安全级别 1，2，3，4）

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。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，应当定义该模块具有旁路能力。

注：本条款不单独进行检测。

AS04.19：（安全级别 1，2，3，4）

在开启密码模块的旁路功能之前，操作员应当担任相应的授权角色。

送检单位需要提交的材料

VE04.19.01：送检单位提供的密码模块支持旁路功能。

VE04.19.02：送检单位在提供的文档中详细描述旁路功能的使用步骤和方法。

所需的检测程序

TE04.19.01：检测人员应确认操作员被授权相应角色后才可以开启密码模块的旁路功能。

AS04.20：（安全级别 1，2，3，4）

应当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。

送检单位需要提交的材料

VE04.20.01：送检单位在提供的文档中详细描述激活旁路功能的内部操作和步骤。

所需的检测程序

TE04.20.01：检测人员应确认密码模块需要两个独立的内部操作才能激活旁路功能。

AS04.21：（安全级别 1，2，3，4）

（应当使用两个独立的内部操作来激活旁路能力）这两个独立的内部操作应当能够改变控制旁路能力的软件和/或硬件的行为（例如，设置两个不同的软件或硬件标志位，其中一个可能由用户控制）。

送检单位需要提交的材料

VE04.21.01：送检单位在提供的文档中详细描述内部操作如何改变控制旁路能力的软件和/或硬件行为。

所需的检测程序

TE04.21.01：检测人员应确认密码模块需要两个独立的内部操作能够改变控制旁路能力的软件和/或硬件的行为。

AS04.22：（安全级别 1，2，3，4）

模块应当显示其状态以指示旁路能力是否：

a) **未被激活，且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模块）；**

b) **被激活，且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模块）；**

c) **可选择地激活或去活，以及模块此时提供的某些服务是使用了密码功能，而某些服务是没有使用密码功能（例如，对于拥有多个通信信道的模块，明文数据是否被加密取决于每个信道的配置）。**

送检单位需要提交的材料

VE04.22.01：送检单位在提供的文档中描述如何指示旁路功能被激活的状态。

所需的检测程序

TE04.22.01：检测人员应确认密码模块具备标识，可以明确表示旁路功能是否被激活的状态。

6.5.3.3 自启动密码输出能力

AS04.23：（安全级别 1，2，3，4）

自启动密码输出能力应当由密码主管配置，而且该配置可能在模块经过重置、重启或开关电源之后可以保留下来。

送检单位需要提交的材料

VE04.23.01：如果密码模支持自启动密码输出能力，送检单位应在提供的文档中详细说明该功能只能由密码主管配置，在模块重置、重启或开关电源之后是否保留下来。

所需的检测程序

TE04.23.01：检测人员应确认密码模块自启动能力是否由密码主管配置。

TE04.23.02：检测人员应确认密码模块自启动配置成功后，在模块重置、重启或开关电源后，是否可以保留下来。

AS04.24：（安全级别 1，2，3，4）

应当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。

送检单位需要提交的材料

VE04.24.01：送检单位在提供的文档中详细描述激活旁路功能的内部操作和步骤。

所需的检测程序

TE04.24.01：检测人员应确认密码模块需要两个独立的内部操作才能激活自启动密码输出功能。

AS04.25：（安全级别 1，2，3，4）

（应当需要两个独立的内部操作来激活该能力）这两个独立的内部操作应当能够改变控制该能力的软件和/或硬件的行为（例如，设置两个不同的软件或硬件标志位，其中一个可能由用户控制）。

送检单位需要提交的材料

VE04.25.01：送检单位在提供的文档中详细描述内部操作如何改变控制旁路能力的软件和/或硬件行为。

所需的检测程序

TE04.25：检测人员应确认密码模块需要两个独立的内部操作能够改变控制自启动密码输出能力的软件和/或硬件的行为。

AS04.26：（安全级别 1，2，3，4）

模块应当显示其状态以指示自启动密码输出能力是否被激活。

送检单位需要提交的材料

VE04.26.01：送检单位在提供的文档中描述如何指示自启动密码输出功能被激活的状态。

所需的检测程序

TE04.26.01：检测人员应确认密码模块具备标识，可以明确表示自启动密码输出功能是否被激活的状态。

6.5.3.4　软件/固件加载

AS04.27：（安全级别 1，2，3，4）

如果密码模块具有加载外部软件或固件的能力，那么应当满足下列要求：

注：本条款不单独进行检测。

AS04.28：（安全级别 1，2，3，4）
加载的软件或固件应当在加载之前经过审验机构的审验，以维持审验效力。。

送检单位需要提交的材料

VE04.28.01：送检单位提供加载的软件或固件的文件清单和说明。

VE04.28.02：送检单位应提供审验机构提供的审验报告或证明。

所需的检测程序

TE04.28.01：检测人员应确认清单中所包含的软件和固件，具有审验机构的审验报告。

AS04.29：（安全级别 1，2，3，4）
应当禁止通过数据输出接口输出数据，直到软件/固件加载以及加载测试成功通过。

送检单位需要提交的材料

VE04.29.01：送检单位提供文档描述软件/固件加载以及加载测试的操作步骤。

所需的检测程序

TE04.29.01：检测人员应确认在软件/固件加载以及加载测试成功通过前，密码模块的数据输出端口应禁止数据输出。

AS04.30：（安全级别 1，2，3，4）
在运行加载的代码之前应当执行 GM/T 0028 7.10.3.4 中规定的软件/固件加载测试。

送检单位需要提交的材料

VE04.30.01：送检单位提供文档描述运行加载的软件/固件的操作步骤和方法。

VE04.30.02：送检单位应提供文档说明在运行加载的代码之前执行了 GM/T 0028 7.10.3.4 中

规定的软件/固件加载测试，并描述操作步骤和方法。

所需的检测程序

TE04.30.01：检测人员应确认在软件/固件加载测试成功通过前，加载的代码应不能运行。

TE04.30.02：检测人员应确认在软件/固件加载测试成功通过后，加载的代码应可以运行。

AS04.31：（安全级别 1，2，3，4）
密码模块应当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 GM/T 0028 7.10.2 中规定的运行前自测试。

送检单位需要提交的材料

VE04.31.01：送检单位提供的文档中应说明任何已经加载的或已被修改的核准安全功能在运行之前，应该成功执行 GM/T 0028 7.10.2 中规定的运行前自测试。

VE04.31.02：送检单位提供文档，描述运行前自测是的方法和步骤。

所需的检测程序

TE04.31.01：检测人员应确认在软件/固件加载测试成功通过前，任何已经加载的或已被修改的核准安全功能应不能运行。

AS04.32：（安全级别 1，2，3，4）
应当修改模块的版本信息，以表示增加和/或更新了最新加载的 GM/T 0028 7.4.3 中的软件或固件。

送检单位需要提交的材料

VE04.32.01：送检单位提供文档描述运行加载的软件/固件的版本信息。

VE04.32.02：送检单位提供文档描述检查模块版本信息的方法和步骤。

所需的检测程序

TE04.32.01：检测人员在软件或固件加载前后，分别获取模块的版本信息，核准密码模块的版本信息是否按照 GM/T 0028 7.4.3 的规定进行了增加和/或更新。

AS04.33：（安全级别 1，2，3，4）
如果新软件或固件的加载是镜像的完全更替，它应当构成一个全新的模块，需要由审验机构重新审验，以维持审验效力。

送检单位需要提交的材料

VE04.33.01：如果新软件或固件的加载是镜像的完全更替,送检单位应提供审验机构重新核发的审验报告或证明。

所需的检测程序

TE04.33.01：检测人员应核准审验报告或证明是否与新软件或固件相符合。

AS04.34：（安全级别 1，2，3，4）
新的软件或固件镜像应当在模块上电重置之后才能运行。

送检单位需要提交的材料

VE04.34.01：送检单位提供文档描述新的软件或固件镜像的运行步骤和方法。

所需的检测程序

TE04.34.01：检测人员应确认，新的软件或固件镜像更新后，密码模块未重新上电重置，应不能运行。
TE04.34.01：检测人员应确认，新的软件或固件镜像更新后，密码模块重新上电重置后，应可以运行。

AS04.35：（安全级别 1，2，3，4）
所有 SSP 应当在运行新镜像之前被置零。

送检单位需要提交的材料

VE04.35.01：送检单位提供文档列举所有 SSP，并说明所有 SSP 在运行镜像之前被置零。

所需的检测程序

TE04.35.01：检测人员应核准在运行新的镜像之前，所有的 SSP 都被置零。

6.5.4 鉴别

AS04.36：（安全级别 1，2，3，4）
如果密码模块支持基于角色的鉴别机制，那么模块应当要求操作员隐式地或显式地选择一个或多个角色。

注：本条款不单独进行检测。

AS04.37：（安全级别 1，2，3，4）
（如果密码模块支持基于角色的鉴别机制，那么模块）应当鉴别其能否担任所选定的角色（或角色的集合）。

送检单位需要提交的材料

VE04.37.01：送检单位应记录模块实现的鉴别类型。送检单位应记录用来实现隐含或明确地选择一个或多个角色的机制，以及鉴别操作者承担的角色。

所需的检测程序

TE04.37.01：检测人员应确认送检单位文档详细说明了一个或多个角色的选择机制，以及鉴别操作者承担的角色。

TE04.37.02：检测人员应承担每个角色并且在认证过程中初始化一个错误。检测人员应核实模块拒绝访问其角色。

AS04.38：（安全级别 1，2，3，4）

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，那么模块应当鉴别该操作员能否担任该新角色。

送检单位需要提交的材料

VE04.38.01：送检单位文档应描述操作者改变角色的能力，还必须说明怎样辨认操作者承担的新角色。

所需的检测程序

TE04.38.01：检测人员应检查送检单位文档以确认操作者改变角色的方法，包括怎样辨认操作者承担的新角色。

TE04.38.02：检测人员应执行以下测试：

a） 承担一个角色，尝试将其改变为操作者已鉴别的其他角色，确认模块允许操作者可对分配的新角色请求服务。

b） 承担一个角色，尝试将其改变为操作者未鉴别的其他角色，确认模块不允许操作者可对分配的新角色请求服务。

AS04.39：（安全级别 1，2，3，4）
如果密码模块支持基于身份的鉴别机制，模块应当要求单独且唯一标识操作员。

注：本条款不单独进行检测。

AS04.40：（安全级别 1，2，3，4）
（如果密码模块支持基于身份的鉴别机制）应当要求操作员隐式地或显式地选择一个或多个角色。

注：本条款不单独进行检测。

AS04.41：（安全级别 1，2，3，4）
（如果密码模块支持基于身份的鉴别机制）应当鉴别操作员的身份，以及操作员是否被授权担任所选定的角色（或角色的集合）。

送检单位需要提交的材料

VE04.41.01：送检单位应记录模块内实现的鉴别类型。送检单位应记录用于执行操作者身份鉴别的机制、操作者的身份认证、一个或多个角色明确或不明确的选择、操作者承担角色的鉴别。

所需的检测程序

TE04.41.01：检测人员应确认送检单位文档详细说明怎样唯一标识操作者，怎样认证其身份，操作者怎样选择角色，怎样鉴别操作者基于身份鉴别承担的角色。

TE04.41.02：检测人员在鉴别过程中应初始化一个错误，且确认模块不允许检测人员继续进行鉴别程序。

TE03.16.03：检测人员应成功认证模块中他/她的身份。当需要选择一个或多个角色时，检测人员应选择不与认证身份相符的角色，并确认承担角色的鉴别是失败的。

AS04.42：（安全级别 1，2，3，4）

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，那么模块应当验证经标识的操作员是否被授权担任该新角色。

送检单位需要提交的材料

VE04.42：送检单位文档应描述操作者改变角色的能力，还应说明对操作者新角色的身份鉴别是必要的。

所需的检测程序

TE04.42.01：检测人员应确认送检单位文档以证实操作者无需重新进行身份鉴别而改变角色的方法，包括核查对以前没有认证的操作者角色。

TE04.42.02：检测人员应进行如下测试：

a） 承担一个角色，尝试将其改变为检测人员承担的已鉴别的其他角色，确认检测人员的身份不用被重新鉴别，再确认检测人员能获得与新角色有关的服务。检测人员执行的新角色的服务不应与以前的角色相关，以此来验证检测人员承担的是另一个角色。

b） 承担一个角色，尝试将其改变为检测人员承担的未鉴别的其他角色，以确认模块拒绝基于操作者身份的角色访问。

AS04.43：（安全级别 1，2，3，4）
当密码模块被重置、重启、关闭且随后又被打开时，模块应当要求鉴别操作员。

送检单位需要提交的材料

VE04.43：送检单位文档应描述当模块断电时如何将之前的鉴别结果清除。

所需的检测程序

TE04.43.01：检测人员应确认送检单位文档描述模块断电后之前的鉴别结果已经被清除。

TE04.43.02：检测人员应承担一个或多个角色，关闭模块电源，再打开模块电源，并尝试执行这些角色相应的服务。为满足之前的说明，模块应拒绝服务的访问，并需要检测人员重新鉴别。

AS04.44：（安全级别 1，2，3，4）
应当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。

送检单位需要提交的材料

VE04.44.01：送检单位文档应描述模块所有鉴别数据的保护措施。保护措施应包括防止未经授权的泄露、修改和替换机制。

所需的检测程序

TE04.44.01：检测人员应审查送检单位文档，确认文档描述了鉴别数据的保护措施。检测人员应确认文档描述了如何保护数据，从而防止未经授权的泄露、修改和替换。

TE04.44.02：检测人员应进行如下测试：

a） 尝试访问（避免文件保护机制）未给检测人员授权访问的鉴别数据。如果模块拒绝访问或只不允许访问加密数据或其他保护形式的数据，符合规定。

b） 使用送检单位文档未说明的方法修改鉴别数据，并尝试输入修改后的数据。模块应

不允许检测人员使用修改后的数据进行鉴别。

AS04.45：（安全级别 1，2，3，4）
鉴别机制的初始化允许特殊处理。如果密码模块不包含第一次访问模块时鉴别操作员所需的鉴别数据，那么应当使用其它被授权的方法（例如，程序控制或使用出厂设置或默认的鉴别数据）对模块进行访问控制和初始化鉴别。

送检单位需要提交的材料

VE04.45.01：送检单位文档应详细说明在初始化模块之前控制模块访问的方法。

所需的检测程序

TE04.45.01：检测人员应确认送检单位文档描述了操作者在首次访问模块时的鉴别程序。

TE04.45.02：若在初始化之前访问模块是受限的，检测人员应在未初始化的模块上添加一个错误，并应确认模块访问被拒绝。检测人员应承担一个授权角色并确认所需的鉴别过程符合文档说明。检测人员应在初始化模块前尝试承担其他角色并确认模块拒绝此角色的访问。

AS04.46：（安全级别 1，2，3，4）
如果使用了默认的鉴别数据来控制对模块的访问，那么默认的鉴别数据应当在第一次鉴别后被更换。

送检单位需要提交的材料

VE04.46.01：送检单位提供的密码模块采用模式鉴别数据来控制对模块的访问。

VE04.46.02：送检单位提供文档详细说明默认鉴别数据的内容和使用方式。

所需的检测程序

TE04.46.01：检测人员应确认通过默认鉴别数据可以访问密码模块。

TE04.46.02：检测人员应确认，在第一次鉴别后，鉴别数据被更换。

AS04.47：（安全级别 1，2，3，4）
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当是核准的安全功能。

送检单位需要提交的材料

VE04.47.01：送检单位提供文档详细说明采用何种核准的安全功能鉴别操作员。

所需的检测程序

TE04.47.01：检测人员应确认密码模块采用的鉴别方式是否与文档描述一致。

TE04.47.02：检测人员应确认鉴别采用的安全功能符合 GM/T 0028 附录 C 的要求。

AS04.48：（安全级别 1）
模块应当实现 GM/T 0028 附录 E 中规定的一种核准的鉴别机制。

送检单位需要提交的材料

VE04.48.01：送检单位提供文档详细说明采用何种核准的鉴别机制。

所需的检测程序

TE04.48.01：检测人员应确认密码模块采用的鉴别机制是否与文档描述一致。

TE04.48.02：检测人员应确认密码模块采用的鉴别机制是否与与 GM/T 0028 附录 E 的规定一致。

AS04.49：（安全级别 1）
在模块的安全策略文档（附录 B）中应当描述鉴别机制的预期强度。

送检单位需要提交的材料

VE04.49.01：送检单位提供符合 GM/T 0028 附录 B 要求的安全策略文档，描述鉴别机制的预期强度。

所需的检测程序

TE04.49.01：检测人员应确认送检单位提供的文档是否符合 GM/T 0028 附录 B 的要求。

TE04.49.02：检测人员应确认送检单位提供的文档是否描述鉴别机制的预期强度。

AS04.50：（安全级别 1）
对于核准鉴别机制的每次尝试，模块应当满足预期的鉴别强度。

送检单位需要提交的材料

VE04.50.01：送检单位提供文档详细说明密码模块支持的核准的鉴别方式的鉴别强度。

所需的检测程序

TE04.50.01：检测人员多次尝试核准的鉴别机制，模块应满足预期鉴别强度。

AS04.51：（安全级别 1）
对于在一分钟之内对核准鉴别机制的多次尝试，模块应当满足预期的鉴别强度。

送检单位需要提交的材料

VE04.51.01：送检单位提供文档详细说明密码模块支持的核准的鉴别方式的鉴别强度。

所需的检测程序

TE04.51.01：检测人员在一分钟之内多次尝试核准的鉴别机制，模块应满足预期鉴别强度。

AS04.52：（安全级别 1）
核准的鉴别机制应当依赖于模块的具体实现，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）。

送检单位需要提交的材料

VE04.52：送检单位提供文档详细说明密码模块鉴别机制的实现方法和原理。

所需的检测程序

TE04.52：检测人员应核准密码模块核准的鉴别机制不依赖于过程控制和安全规则。

AS04.53：（安全级别 2）
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，那么鉴别机制应当满足本条款的要求。

送检单位需要提交的材料

VE04.53.01：送检单位提供文档明确说明软件密码模块所采用的操作系统。

VE04.53.02：送检单位提供文档详细说明操作系统实现的鉴别机制。

所需的检测程序

TE04.53.01：检测人员应核准软件密码模块所使用的操作系统的鉴别机制符合要求。

AS04.54：（安全级别 2）
在鉴别过程中，应当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）。

送检单位需要提交的材料

VE04.54.01：送检单位提供文档详细描述密码模块的鉴别过程。

所需的检测程序

TE04.54.01：检测人员应确认鉴别过程中，密码模块是否隐藏鉴别数据给操作员的反馈信息。

AS04.55：（安全级别 2）
在尝试鉴别的过程中，提供给操作员的反馈信息应当防止削弱鉴别机制强度。

送检单位需要提交的材料

VE04.55.01：送检单位提供文档详细描述密码模块的鉴别过程和强度。

所需的检测程序

TE04.55.01：检测人员尝试鉴别过程，记录给操作员的反馈信息，确保这些信息不会削弱鉴别机制强度。

AS04.56：（安全级别 1）
对于安全一级，不要求密码模块采用鉴别机制以控制对模块的访问。如果模块不支持鉴别机制，模块应当需要操作员隐式或显式地选择一个或多个角色。

送检单位需要提交的材料

VE04.56.01：送检单位提供文档说明采用的鉴别方式。

所需的检测程序

TE04.56.01：检测人员确认无果模块不支持鉴别机制，模块是否需要操作员隐式或显式地选择一个或多个角色。

AS04.57：（安全级别 2）
对于安全二级，密码模块应当至少采用基于角色的鉴别以控制对模块的访问。

送检单位需要提交的材料

VE04.57.01：送检单位提供文档说明采用的鉴别方式。

所需的检测程序

TE04.57.01：检测人员确认密码模块是否至少采用基于角色的鉴别以控制对模块的访问。

AS04.58：（安全级别 3）
对于安全三级，密码模块应当采用基于身份的鉴别机制以控制对模块的访问。

送检单位需要提交的材料

VE04.58.01：送检单位提供文档说明采用的鉴别方式。

所需的检测程序

TE04.58.01：检测人员确认密码模块是否采用基于身份的鉴别机制以控制对模块的访问。

AS04.59：（安全级别 4）
对于安全四级，密码模块应当采用基于身份的多因素鉴别机制以控制对模块的访问。

送检单位需要提交的材料

VE04.59.01：送检单位提供文档说明采用的鉴别方式。

所需的检测程序

TE04.59.01：检测人员确认密码模块是否采用基于身份的多因素鉴别机制以控制对模块的访问。

6.6 软件/固件安全

AS05.01：（安全级别 1，2，3，4）
本条款的要求应当适用于密码模块的软件和固件部件。

注：本条款不单独进行检测。

AS05.02：（安全级别 1，2，3，4）
描述软件/固件安全的文档(密码模块安全策略)应当按照 GM/T 0028 附录 A.2.5 中规定的要求编写。

送检单位需要提交的材料

VE05.02.01: 送检单位提供文档应描述实现软件/固件安全的策略。

所需的检测程序

TE05.02.01: 检测人员应核实送检单位提供文档应描述软件/固件安全，并且符合 GM/T 0028 A.2.2.5 的要求。

AS05.03：（安全级别 1，2，3，4）
安全要求 AS05.04- AS05.10 应当适用于密码模块内的软件和固件部件。

注：本条款不单独进行检测。

AS05.04：（安全级别 1，2，3，4）
所有的软件和固件应当符合 GM/T 0028 第 7.11.7 节中规定的本标准安全要求的格式，并确保安装前未被修改。

送检单位需要提交的材料

VE05.04.01:送检单位提供文档需包含软件和固件的安全要求说明。

所需的检测程序

TE05.04.01: 检测人员应核实送检单位文档包含软件和固件的安全要求说明，并且符合 GM/T 0028 7.11.7 中规定的安全要求格式。

AS05.05：（安全级别 1，2，3，4）
密码边界内的所有软件和固件部件应当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，也可以由另一个经审验的密码模块提供。

送检单位需要提交的材料

VE05.05.01: 送检单位文档中需描述核准的完整性技术。

VE05.05.02: 送检单位文档中需描述所有软件和固件部件使用核准的完整性技术。

所需的检测程序

TE05.05.01: 检测人员应核实送检单位文档描述了核准的完整性技术。

TE05.05.02: 检测人员应核实送检单位文档中包含所有软件和固件部件使用核准的完整性技术的描述。

AS05.06：（安全级别 1，2，3，4）
如果完整性测试失败，模块应当进入错误状态。

注：本条款与 AS05.08 一起进行测试。

AS05.07：（安全级别 1，2，3，4）
在多个不相交鉴别码或签名中，任何一个鉴别码或签名的验证失败都应当导致模块进入错误状态。

注：本条款与 AS05.08 一起进行测试。

AS05.08：（安全级别 1，2，3，4）
一旦完成了完整性测试，模块软件或固件的完整性测试的过程中生成的临时值应当被置零。

送检单位需要提交的材料

VE05.08.01: 送检单位文档中需描述模块错误状态指示信息。

VE05.08.02: 送检单位文档中需描述：如果完整性测试失败，模块将进入错误状态。

VE05.08.03:送检单位文档中应描述：在多个不相交鉴别码或签名中，任何一个鉴别码或签名的验证失败都会导致模块进入错误状态。

VE05.08.04:送检单位提供文档中应描述：一旦完成完整性测试，模块软件或固件的完整性测试过程中生成的临时值被置零。

所需的检测程序

TE05.08.01：检测人员应证实所有软件和固件部件使用核准的完整性技术。

TE05.08.02：检测人员应核实送检单位文档中包含模块错误状态指示信息的描述。

TE05.08.03：检测人员应核实送检单位文档中描述了如果完整性测试失败，模块进入错误状态。

TE05.08.04：检测人员应检测如果完整性测试失败，模块进入错误状态。

TE05.08.05：检测人员应核实送检单位文档中描述了在多个不相交鉴别码或签名中，任何一个鉴别码或签名的验证失败都导致模块进入错误状态。

TE05.08.06：检测人员应检测：在多个不相交鉴别码或签名中，任何一个鉴别码或签名的验证失败都导致模块进入错误状态。

TE05.08.07：检测人员应核实送检单位文档中包含描述了在完成了完整性测试之后，模块软件或固件的完整性测试的过程中生成的临时值被立即置零。

TE05.08.08：检测人员应检测：完成了完整性测试后，在模块软件或固件的完整性测试的过程中生成的临时值被立即置零。

AS05.09：（安全级别 1，2，3，4）
操作员应当能够通过 GM/T 0028 第 7.3.2 节中规定的 SFMI、HSMI 或 HFMI 服务按需执行核准的完整性技术。

送检单位需要提交的材料

VE05.09.01:送检单位文档中应描述操作员能够通过 GM/T 0028 第 7.3.2 节中规定的 SFMI、HSMI 或 HFMI 服务按需执行核准的完整性技术。

所需的检测程序

TE05.09.01:检测人员应核实送检单位文档中描述了操作员能够通过 SFMI、HSMI 或 HFMI 服务按需执行核准的完整性技术，GM/T 0028 第 7.3.2 节中描述了 SFMI、HSMI 和 HFMI 服务。

AS05.10：（安全级别 1，2，3，4）
GM/T 0028 第 7.3.3 节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，以及第 7.4.3 节中规定的服务，应当通过定义的 HMI、SFMI、HFMI 或 HSMI 完成。

送检单位需要提交的材料

VE05.10.01：送检单位文档应描述：GM/T 0028 第 7.3.3 节中规定的密码模块的所有数据和控制输入，及数据、控制和状态输出，以及 GM/T 0028 第 7.4.3 节中规定的服务是通过定义的 HMI、SFMI、HFMI 或 HSMI 完成的

所需的检测程序

TE05.10.01：检测人员应核实送检单位文档中说明了在 GM/T 0028 第 7.3.3 节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 GM/T 0028 第 6.4.3 节中规定的服务都是通过定义的 HMI、SFMI、HFMI 或 HSMI 完成的。

AS05.11：（安全级别 1，2，3，4）
如果加载的软件或固件关联到、修改了或者就是经过审验的模块可以运行起来的必备部分，但没有完全更替或覆盖经过审验的模块，那么软件/固件加载测试是适用的，并且应当由经过审验的模块执行该测试。

送检单位需要提交的材料

VE05.11.01：送检单位文档中描述了如果加载的软件或固件关联到、修改了或者就是经过审验的模块可以运行起来的必备部分，却未完全更替或覆盖经过验证的模块，则软件/固件加载测试是适用的，并且由经过审验的模块执行该测试。

所需的检测程序

TE05.11.01：检测人员应核实送检单文档描述了如果加载的软件或固件关联到、修改了或者就是经过审验的模块可以运行起来的必备部分，却没有完全更替或覆盖经过验证的模块，那么软件/固件加载测试是适用的，并且该测试由经过审验的模块执行。

AS05.12：（安全级别 2，3，4）
{对于安全二级而言，除了安全一级的要求，还有}AS05.13-AS05.16 适用于模块中的软件或固件部件。

注：本条款不单独进行检测。

AS05.13：（安全级别 2，3，4）
模块的软件或固件部件应当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）。

送检单位需要提交的材料

VE05.13.01：送检单位文档应说明模块的软件或固件部件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）。

所需的检测程序

TE05.13.01：检测人员应核实送检单位文档说明了模块的软件或固件部件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）。

AS05.14：（安全级别 2，3，4）
应当确保操作者无法通过 HMI、SFMI、HFMI 或 HSMI 接口的服务或控制设置，启动或执行调试技术。

送检单位需要提交的材料

VE05.14.01：送检单位提供的文档应描述操作者无法通过 HMI、SFMI、HFMI 或 HSMI 接口的服务或控制设置，启动或执行调试技术。

所需的检测程序

TE05.14.01：检测人员应核实送检单位文档中说明了操作者无法通过 HMI、SFMI、HFMI 或 HSMI 接口的服务或控制设置，启动或执行调试技术。

TE05.14.02：检测人员应检测：操作者不能通过 HMI、SFMI、HFMI 或 HSMI 接口的服务或控制设置，启动或执行调试技术。

AS05.15：（安全级别 2，3，4）
密码边界内的所有软件或固件应当使用核准的数字签名或带密钥的消息鉴别码进行保护。

注：本条款与 AS05.16 一起进行测试。

AS05.16：（安全级别 2，3，4）
在使用核准的数字签名或带密钥的消息鉴别码保护密码边界内的所有软件和固件时，如果使用核准的数字签名或带密钥的消息鉴别码计算的结果不等于之前生成的结果，则测试失败，并且模块应当进入错误状态。

送检单位需要提交的材料

VE05.16.01：送检单位文档中应描述密码边界内的所有软件或固件使用核准的数字签名或带密钥的消息鉴别码进行保护。

VE05.16.02：送检单位文档应描述：如果使用核准的数字签名或带密钥的消息鉴别码计算的结果与之前生成的结果不相同，则测试失败，并且模块进入错误状态。

所需的检测程序

TE05.16.01：检测人员应核实送检单位文档说明了密码边界内的所有软件或固件都使用核准的数字签名或带密钥的消息鉴别码进行保护。

TE05.16.02：检测人员应核实送检单位文档说明了:如果使用核准的数字签名或带密钥的消息鉴别码计算的结果不等于之前生成的结果，则测试失败，并且模块进入错误状态。

TE05.16.03：检测人员应进行如下检测：使用核准的数字签名或带密钥的消息鉴别码计算的结果不等于之前生成的结果时，测试失败，并且模块进入错误状态。

AS05.17：（安全级别 3，4）
{对于安全三级和四级，除了安全一级和二级的要求之外，还}应满足 AS05.18- AS05.21 的要

求。

注：本条款不单独进行检测。

AS05.18：（安全级别 3，4）
密码边界内的所有软件或固件应当使用核准的数字签名进行保护。

注：本条款与 AS05.19 一起进行测试。

AS05.19：（安全级别 3，4）
在使用核准的数字签名保护密码边界内的所有软件和固件时，如果使用核准的数字签名对密码边界内的软件或固件进行计算的结果不等于之前生成的结果，则测试失败，并且模块应当进入错误状态。

送检单位需要提交的材料

VE05.19.01：送检单位文档应描述核准的数字签名。

VE05.19.02：送检单位文档应说明密码边界内的所有软件或固件使用核准的数字签名进行保护。

VE05.19.03：送检单位文档应描述：如果使用核准的数字签名对密码边界内的软件或固件进行计算的结果不等于之前生成的结果，则测试失败，并且模块进入错误状态。

所需的检测程序

TE05.19.01：检测人员应核实送检单位文档说明了核准的数字签名。

TE05.19.02：检测人员应核实送检单位文档中说明了密码边界内的所有软件或固件都使用核准的数字签名进行保护。

TE05.19.03：检测人员应核实送检单位提供的文档中描述如下内容：如果使用核准的数字签名对密码边界内的软件或固件进行计算的结果不等于之前生成的结果，则测试失败，并且模块进入错误状态。

TE05.19.04：检测人员应进行如下检测：如果使用核准的数字签名对密码边界内的软件或固件进行计算的结果不等于之前生成的结果，则测试失败，并且模块进入错误状态。

AS05.20：（安全级别 3，4）
数字签名技术可以包含单个签名，或者多个部分签名，部分签名中的任何一个签名的验证失败都应当导致模块进入错误状态。

注：本条款与 AS05.21 一起进行测试。

AS05.21：（安全级别 3，4）
对于数字签名技术而言，签名私钥应当保存在模块外

送检单位需要提交的材料
VE05.21.01：送检单位文档应描述了数字签名技术可以包含单个签名，或者多个部分签名，部分签名中的任何一个签名的验证失败都导致模块进入错误状态。

VE05.21.02：送检单位文档应描述如下内容：数字签名技术的签名私钥保存在模块外。

所需的检测程序

TE05.21.01：检测人员应核实送检单位文档中描述了：数字签名技术可以包含单个签名，或者多个部分签名，部分签名中的任何一个签名的验证失败都导致模块进入错误状态。

TE05.21.02：检测人员应检测：部分签名中的任何一个签名的验证失败都导致模块进入错误状态。

TE05.21.03：检测人员应核实送检单位提供文档中描述如下内容：数字签名技术的签名私钥保存在模块外。

6.7 运行环境

6.7.1 运行环境通用要求

AS06.01：（安全级别 1，2，3，4）
如果运行环境是不可修改或受限制的，GM/T 0028 第 7.6.2 节中规定的操作系统要求应当适用。

注：本条款不单独进行检测。

AS06.02：（安全级别 1，2，3，4）
如果运行环境是可修改的，GM/T 0028 第 7.6.3 节中规定的操作系统要求应当适用。

注：本条款不单独进行检测。

AS06.03：（安全级别 1，2，3，4）
文档应当按照 GM/T 0028 A.2.6 中规定的要求编写。

送检单位需要提交的材料

VE06.03.01：送检单位需在文档中描述密码模块的运行环境，配置运行环境的安全规则、设置和限制条件。

VE06.03.02：如果密码模块使用了操作系统，送检单位应提供配置操作系统符合相应要求的管理员指南文档。

所需的检测程序

TE06.03.01：检测人员应核实送检单位提供的文档中描述了密码模块的运行环境和配置。

TE06.03.01：如果密码模块使用了操作系统，检测人员应核实送检单位提供了 VE06.03.02 中要求的文档。

6.7.2 受限或不可修改运行环境的操作系统要求

AS06.04：（安全级别 1，2，3，4）
如果模块在 GM/T 0028 第 7.7 节中达到安全一级，则 GM/T 0028 第 7.6.3 节中规定的安全一级的要求应当适用。

注：本条款不单独进行检测。

6.7.3 可修改运行环境的操作系统要求

AS06.05：（安全级别 1，2，3，4）

每一个密码模块的实例应当能够控制和支配自己的 SSP。

送检单位需要提交的材料

VE06.05.01：送检单位需在文档中描述密码模块的每一个实例是如何控制和支配自己的 SSP 的。

所需的检测程序

TE06.05.01：检测人员应检查送检单位提供的文档中描述了密码模块的每个实例是如何控制和支配自己的 SSP 的。

TE06.05.02：检测人员应核实每一个密码模块的实例应当能够控制和支配自己的 SSP。

AS06.06：（安全级别 1，2，3，4）

运行环境应当提供应用进程间相互隔离的能力，以阻止进程间对 CSP 不受控的访问以及对 SSP 不受控的修改,无论 CSP 和 SSP 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。

送检单位需要提交的材料

VE06.06.01：送检单位需在文档中描述进程间 CSP 和 SSP 相互隔离的能力。

VE06.06.02：送检单位应提供测试程序验证进程间隔离策略的能力。

所需的检测程序

TE06.06.01：检测人员应核实送检单位提供的文档中描述了进程间 CSP 和 SSP 相互隔离的能力。

TE06.06.02：检测人员应运行多个进程，并尝试通过其中一个进程访问其它进程的 CSP 或修改 SSP。

AS06.07：（安全级别 1，2，3，4）

对运行环境配置的规定应当记录在密码模块的安全策略中。

送检单位需要提交的材料

VE06.07.01：送检单位应在安全策略文档中描述对运行环境配置的规定。

所需的检测程序

TE06.07.01：检测人员应核实安全策略文档中描述了对运行环境配置的规定。

AS06.08：（安全级别 1，2，3，4）

密码模块产生的进程应当由模块自己所有，不由外部进程/操作员所有。

送检单位需要提交的材料

VE06.08.01：送检单位文档中应描述机制，该机制使密码进程运行时其它程序不能访问 CSP 和/或 PSP。

所需的检测程序

TE06.08.01：通过检查检测人员确认送检单位文档中说明了密码模块运行时其它程序不能访问 CSPs 和/或 PSPs。

TE06.08.02：检测人员应按照管理员和用户指南文档中的描述实现密码功能。当密码功能执行时，同一或另外检测人员须尝试访问明文私钥及密钥、中间密钥生成值以及 CSP。

AS06.09：（安全级别 2，3，4）

对于安全二级，除了安全一级的要求以外，操作系统还应当满足下列要求或者经审验机构许可。

注：本条款不单独进行检测。

AS06.10：（安全级别 2，3，4）

所有密码软件、SSP、控制和状态信息应当在操作系统的控制之下。

送检单位需要提交的材料

VE06.10.01：送检单位应提供文件，该文件说明了控制密码模块的操作系统已成功经过相关检测机构的认可。

所需的检测程序

TE06.10.01：检测人员应确认操作系统已得到认证证书。

AS06.11：（安全级别 2，3，4）

操作系统应当正确配置，以防止非授权地执行、修改和读取 SSP、控制和状态数据。

送检单位需要提交的材料

VE06.11.01：送检单位应在安全策略文档中描述对操作系统安全配置的规定。

所需的检测程序

TE06.11.01：检测人员应审查安全策略文档中描述的操作系统安全配置是否存在漏洞或缺陷。

TE06.11.02：操作系统正确配置后，检测人员应尝试在未授权的情况下，执行、修改和读取SSP、控制和状态数据。

AS06.12：（安全级别 2，3，4）

（为了保护明文数据、密码软件、SSP 和鉴别数据，操作系统的访问控制机制}应当定义和实现了有权运行模块中密码软件的角色、分组以及与它们相关的权限。

送检单位需要提交的材料

VE06.12.01：送检单位文档要求在 VE06.15.01 中指定。

所需的检测程序

TE06.12.01：该 TE 作为 TE06.15.01 的一部分进行检测。

TE06.12.02：检测人员须承担一角色，该角色有权运行存储的密码模块软件和固件组件。检测人员须通过运行存储的密码模块软件和固件组件来确认操作系统访问控制机制的正确配置。

TE06.12.03：检测人员须承担一角色，该角色无权运行存储的密码模块软件或固件组件。检测人员须通过运行存储的密码模块软件和固件组件的尝试来确认操作系统访问控制机制的正确配置。如果检测人员可运行存储的密码模块软件和固件组件，则该检测失败。

AS06.13：（安全级别 2，3，4）

（为了保护明文数据、密码软件、SSP 和鉴别数据，操作系统的访问控制机制}应当定义和实现了有权修改（写、替换和删除）存储在密码边界内软件的角色、分组以及与它们相关的权限，这些软件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）、SSP 和明文数据。

送检单位需要提交的材料

VE06.13.01：送检单位文档要求在 VE06.15.01 中指定。

所需的检测程序

TE06.13.01：该 TE 作为 TE06.15.01 的一部分进行检测。

TE06.13.02：检测人员须承担一角色，该角色有权修改下列存储于密码边界内的密码模块软件或固件组件：

——密码程序；
——密码数据（例如：审计数据）；
——CSP；
——PSP；

——明文数据。
检测人员须修改存储于密码边界内的密码模块软件或固件组件。

TE06.14.03：检测人员须承担一角色，该角色无权修改存储的密码软件和固件组件。检测人员须尝试修改存储的密码软件和固件组件。

AS06.14：（安全级别 2，3，4）

（为了保护明文数据、密码软件、SSP 和鉴别数据，操作系统的访问控制机制}应当定义和实现了有权读取密码操作相关数据（例如，密码操作的审计数据）、CSP 和明文数据的角色、分组以及与它们相关的权限。

送检单位需要提交的材料

VE06.14.01：送检单位文档要求在 VE06.15.01 中指定。

所需的检测程序

TE06.14.01：该 TE 作为 TE06.15.01 的一部分进行检测。

TE06.14.02：检测人员须承担一角色，该角色有权读取下列存储于密码边界内的密码模块软件组件：
——密码数据（例如：审计数据）；
——CSP；
——明文数据。
检测人员须读取存储于密码边界内的密码模块软件组件。

TE06.14.03：检测人员须承担一角色，该角色无权读取存储的密码软件组件。检测人员须尝试读取存储的密码软件组件。

AS06.15：（安全级别 2，3，4）

（为了保护明文数据、密码软件、SSP 和鉴别数据，操作系统的访问控制机制}应当定义和实现了有权输入 SSP 的角色、分组以及与它们相关的权限。

送检单位需要提交的材料

VE06.15.01: 送检单位须提供文件，该文件说明了直接访问、自由访问控制机制为了达到 AS06.12，AS06.13，AS06.143，AS06.15 的要求是如何配置的。

所需的检测程序

TE06.15.01：检测人员须确认送检单位提供了 VE06.15.01 所需的信息。

TE06.15.02：检测人员须承担一角色，该角色有权访问 CSP 和/或 PSP。检测人员须访问 CSP 和/或 PSP。

TE06.15.03：检测人员须承担一角色，该角色无权够访问 CSP 和/或 PSP。检测人员须尝试访问 CSP 和/或 PSP。

AS06.16：（安全级别 2，3，4）

下列规定（AS06.17, AS06.18, AS06.18, AS06.19, AS06.20）应当与密码模块安全策略文档中已定义的角色、分组和服务相一致。

注：本条款不单独进行检测。

AS06.17：（安全级别 2，3，4）

当密码模块不在维护模式时，操作系统应当防止所有操作员和运行的进程修改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）。

送检单位需要提交的材料

VE06.17.01：送检单位须提供描述操作系统如何防止所有操作者及执行进程修改正在执行的密码处理的文档。

所需的检测程序

TE06.17.01：检测人员须确认送检单位提供了 VE06.17.01 中所需的信息。

TE06.17.02：密码模块不在维护模式时，检测人员须尝试修改执行的密码程序。如果一个操作者或执行进程能够修改正在执行的密码处理，则检测失败。

AS06.18：（安全级别 2，3，4）

操作系统应当防止用户进程对其它进程的 SSP 以及系统 SSP 进行读或写操作。

送检单位需要提交的材料

VE06.18.01：送检单位须提供操作系统如何防止用户进程对其它进程的 SSP 以及系统 SSP 进行读或写操作的说明文档。

所需的检测程序

TE06.18.01：检测人员须确认送检单位提供了 VE06.18.01 中所需的信息。

TE06.18.02：检测人员须尝试用户进程对其它进程的 SSP 以及系统 SSP 进行读或写操作。检测人员须确认没有读取或修改其它进程的 SSP 以及系统 SSP。

AS06.19：（安全级别 2，3，4）

满足以上要求（AS06.17、AS06.18）的操作系统配置应当在管理员指南中阐明。

送检单位需要提交的材料

VE06.19.01：送检单位须在密码模块管理员指南中阐明操作系统配置。

所需的检测程序

TE06.19.01：检测人员须确认送检单位的管理员指南中阐明了 VE06.19.01 中所需的信息。

AS06.20：（安全级别 2，3，4）

管理员指南应当声明：操作系统必须按照需要保护的模块内容所指定的要求进行配置。

送检单位需要提交的材料

VE06.20.01：送检单位须在密码模块管理员指南中声明操作系统是按照需要保护的模块内容所指定的要求进行的配置。

所需的检测程序

TE06.20.01：检测人员须确认送检单位的管理员指南中声明了 VE06.20.01 中所需的信息。

AS06.21：（安全级别 2，3，4）

对操作系统的标识和鉴别机制应当满足 GM/T 0028 第 7.4.3 节中规定的要求，并在模块安全策略文档中具体阐明。

送检单位需要提交的材料

VE06.21.01：送检单位须在密码模块管理员指南中声明操作系统是按照需要保护的模块内容所指定的要求进行的配置。

所需的检测程序

TE06.21.01：检测人员须确认送检单位的管理员指南中声明了 VE06.21.01 中所需的信息。

AS06.22：（安全级别 2，3，4）

所有密码软件、SSP、控制和状态信息应当在下列措施（AS06.23-AS06.29）的控制之下。

注：本条款不单独进行检测。

AS06.23：（安全级别 2，3，4）

操作系统应当至少拥有以下属性（AS06.24-AS06.28）。

注：本条款不单独进行检测。

AS06.24：（安全级别 2，3，4）

操作系统应当提供具有审计事件日期和时间的审计机制。

送检单位需要提交的材料

VE06.24.01：送检单位须在文档中声明操作系统具有审计事件日期和时间的审计机制。

所需的检测程序

TE06.24.01：检测人员须确认送检单位的文档中声明了 VE06.24.01 中所需的信息

TE06.24.01：检测人员须运行密码模块检查确认操作系统对事件的日期和事件进行了审计。

AS06.25：（安全级别 2，3，4）

密码模块应当不把 SSP 写入任何审计记录中。

送检单位需要提交的材料

VE06.25.01：送检单位须在文档中声明密码模块未把 SSP 写入任何审计记录中。

所需的检测程序

TE06.25.01：检测人员须确认送检单位的文档中声明了 VE06.25.01 中所需的信息

TE06.25.01：检测人员须运行密码模块检查确认审计记录中未含有 SSP。

AS06.26：（安全级别 2，3，4）

下列事件应当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 SSP；**
- **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。**

注：本条款假定：密码模块必须使用操作系统提供的审计机制来审计识别事件。密码模块使用其它文件作为审计日志是不够的，无论该文件保护的多么完善。

送检单位需要提交的材料

VE06.26.01：送检单位须识别所有由密码模块软件审计的事件。
该事件列表须包括在 AS06.27 中指定的事件。

所需的检测程序

TE06.26.01：检测人员须确认送检单位提供了 VE06.26.01 中所需的信息。

TE06.26.02：通过检查检测人员须确认送检单位文档中说明了密码模块使用由操作系统提供的审计机制来识别事件。

TE06.26.03：检测人员须在审计功能开启的情况下检测模块并执行能够产生审计事件的行

为。 如果所有事件均被审计，则检测人员须确认系统审计日志。

注：检测人员不须检测由操作系统提供和送检单位识别的审计机制。

AS06.27：（安全级别 2，3，4）

操作系统的审计机制应当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 SSP 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，对使用可信信道功能的尝试，并且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识别。**

注：本条款作为 AS06.26 的一部分进行检测。

AS06.28：（安全级别 2，3，4）

操作系统应当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。

送检单位需要提交的材料

VE06.28.01：送检单位应提供文档详细描述操作系统如何配置，以防止存储在密码模块运行环境中的密码模块软件和审计数据被修改。

所需的检测程序

TE06.28.01：检测人员应核查送检单位提供了 VE06.28.01 所需的信息。

TE06.28.02：检测人员应尝试修改存储在密码边界的审计数据。检测人员应核查没有授权的操作员不能访问存储在密码边界中的审计数据。

AS06.29：（安全级别 2，3，4）

无论密码模块是否在核准的工作模式下操作，应当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。应当通过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。

送检单位需要提交的材料

VE06.29.01：送检单位应详细描述操作系统的配置符合相应安全等级。

VE06.29.02：送检单位应声明使用了核准的安全功能对审计记录进行了保护。

所需的检测程序

TE06.29.01：检测人员应核查送检单位提供了 VE06.28.01 和 VE06.28.02 所需的信息。

TE06.29.02：检测人员应审查审计记录是否采用了核准的安全功能。

6.8 物理安全

6.8.1 物理安全实体

AS07.01：（安全级别 1，2，3，4）

密码模块应当采用物理安全机制以限制对模块内容的非授权物理访问，并阻止对已安装模块的非授权使用或修改（包括整个模块的替换）。

注：本条款不单独进行检测。

AS07.02：（安全级别 1，2，3，4）

密码边界内的所有硬件、软件、固件、数据组成部分以及 SSP 应当受到保护。

注：本条款不单独进行检测。

AS07.03：（安全级别 1，2，3，4）

本条款中的要求应当适用于硬件和固件模块、以及混合模块中的硬件和固件部件。

注：本条款不单独进行检测。

AS07.04：（安全级别 1，2，3，4）

本条款的要求应当适用于已定义的模块物理边界。

注：本条款不单独进行检测。

AS07.05：（安全级别 1，2，3，4）

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当在以下时间点以很高的概率被检测到：

——在企图行为之后，并且通过其留下的可见标志（例如，拆卸证据），和/或

——在企图行为过程中。

注：本条款不单独进行检测。

AS07.06：（安全级别 1，2，3，4）

在安全要求 AS07.05 描述的时间点，密码模块的物理安全机制检测到企图进行非授权物理访问、使用或修改的行为的同时，密码模块应当立即采取恰当的行动保护 SSP。

注：本条款不单独进行检测。

AS07.07：（安全级别 1，2，3，4）

文档应当按照 GM/T 0028 A.2.7 中规定的要求编写。

送检单位需要提交的材料

VE07.07.01：检测人员应核实送检单位提供的密码模块安全策略文档中描述物理安全的部分按照 GM/T 0028 A.2.7 中规定的要求编写。
.01
所需的检测程序

TE07.07.01：检测人员应核实送检单位提供的密码模块安全策略文档中描述物理安全的部分按照 GM/T 0028 A.2.7 中规定的要求编写。

6.8.2 通用物理安全要求

AS07.08：（安全级别 1，2，3，4）

安全要求 AS07.09- AS07.13 适用于所有密码模块物理实体。

注：本条款不单独进行检测。

AS07.09：（安全级别 1，2，3，4）

文档应当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。

所需的送检单位文档

VE07.09.01：送检单位文档应详细说明密码模块的物理实现形式。模块如在GM/T 0028第6.7小节中定义的那样，包括单芯片密码模块、多芯片嵌入模块、或多芯片独立模块。

说明的物理实现形式应与模块的物理设计一致。送检单位文档还应说明模块满足哪个安全等级（1 到 4）。

所需的检测程序

TE07.09.01：检测人员应确定送检单位定义了密码模块，参考 GM/T 第 6.7 小节，是单芯片模块、多芯片嵌入模块、或多芯片独立模块。

检测人员应独立确定物理实现形式满足以下说明的三个标准中的一个。三个物理实现形式的基本判断特性和一些常见例子概括如下。

——单芯片密码模块。特点：单个集成电路（IC）芯片构成的模块，该芯片可以作为独立模块使用，或者可以嵌入一个外壳或产品内（可能没有物理保护）。单芯片密码模块的例子有单 IC 芯片和单 IC 芯片智能卡。
——多芯片嵌入密码模块。特点：两个或多个互相连接的 IC 芯片构成的模块，这些芯

片嵌入在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。

——多芯片独立密码模块。特点：个互相连接的 IC 芯片构成的模块，该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和安全无线电话或USB令牌。

TE07.09.02：检测人员应确认送检单位文档声明了模块是为了满足哪个安全等级设计的。检测人员应独立确定模块事实上满足的安全等级。

AS07.10：（安全级别 1，2，3，4）

每当为保护物理安全进行置零操作时，应当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模块置零之间泄露出去,此安全要求适用于所有密码模块物理实体。

送检单位需要提交的材料

VE07.10.01：送检单位提供的密码模块安全策略文档中应描述， 为防止敏感数据在检测到拆卸行为与模块置零之间泄露出去，每当为保护物理安全是如何在极短的时间内执行操作的。

所需的检测程序

TE07.10.01：检测人员应核实送检单位提供的密码模块安全策略文档中描述物理安全的部分包含如下内容: 每当为保护物理安全进行置零操作时，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模块置零之间泄露出去。

TE07.10.02：检测人员应承担维护角色，并在单元上电时访问维护访问接口，确认所有操作密钥归零。

AS07.11：（安全级别 1，2，3，4）

如果模块包含的维护角色需要对模块内容进行物理访问，或者模块被设计成允许物理访问（例如：可被模块供应商或其它被授权的个人访问），那么应当定义维护访问接口。

送检单位需要提交的材料

VE07.11.01：送检单位文档应描述模块使用的维护访问接口。

所需的检测程序

TE07.10.01：检测人员应确认送检单位文档描述了维护访问接口。

TE07.10.02：检测人员应确认送检单位文档和实现是一致的。

AS07.12：（安全级别 1，2，3，4）

如果模块包含的维护角色需要对模块内容进行物理访问，或者模块被设计成允许物理访问

（例如：可被模块供应商或其它被授权的个人访问），那么维护访问接口应当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。

送检单位需要提交的材料

VE07.12.01：送检单位文档应详细说明维护访问接口，包括任何可移动的封盖或封门。

所需的检测程序

TE07.12.01：检测人员应确认送检单位文档，以核实提供的维护访问接口，包括任何可移动的封盖或封门。

AS07.13：（安全级别 1，2，3，4）

如果模块包含的维护角色需要对模块内容进行物理访问，或者模块被设计成允许物理访问（例如，被模块供应商或其它授权个体访问），那么维护访问接口内包含的任何封盖或门使用适当的物理安全机制来进行安全保护。

送检单位需要提交的材料

VE07.13.01：送检单位文档应详细说明维护访问接口，包括任何可移动的封盖或封封门。

所需的检测程序

TE07.13.01 检测人员应确认送检单位文档，以核实提供的维护访问接口，包括任何可移动的封盖或封门。

AS07.14：（安全级别 1，2，3，4）

下列要求（AS07.15-AS07.16）适用于安全一级的所有密码模块。

注：本条款不单独进行检测。

AS07.15：（安全级别 1，2，3，4）

密码模块应当由产品级部件组成，这些产品级部件包括标准钝化技术，例如对整个模块电路使用保型涂料或封闭底漆，以防止环境损害或其它物理损害。

送检单位需要提交的材料

VE07.15.01：模块应是一个标准的、高产品质量的 IC 芯片，被设计以满足电力、温度、可靠性、冲击和震动等商业级别。模块应对于整个芯片使用标准钝化技术。送检单位文档应说明 IC 芯片的质量。如果使用的芯片不是标准的设备，也应说明它的钝化设计

所需的检测程序

TE07.15.01：通过检查或从送检单位的文档中，检测人员应确认模块包含由外部统一材料和标准连接器组成的标准集成电路。通过送检单位文档，检测人员应核实模块内的芯片在电力

和电压范围、温度、可靠性、冲击和震动方面是商业等级的。

TE07.15.02：检测人员应确认送检单位文档中，模块有应用于它的标准钝化。钝化必须是应用于整个芯片电路，以保护其免受环境或其他物理破坏的密封涂层。如果没有使用标准钝化，那么文档应提供信息说明为什么它相当于标准的钝化方法。

AS07.16：（安全级别 1，2，3，4）

当维护密码模块时，应当由操作员按文档规定执行指令置零，或由密码模块自动执行。

注：本条款作为 AS07.12 的一部分进行检测。

AS07.17：（安全级别 2，3，4）

除了安全一级的通用要求，安全二级的所有密码模块还应当满足下列要求(AS07.18-AS07.20).

注：本条款不单独进行检测。

AS07.18：（安全级别 2，3，4）

在尝试物理访问模块时，密码模块应当提供显示拆卸的证据（例如，在封盖、外壳或封条上）；

注：本条款作为单芯片具体化进行检测，参考 AS07.12 和 AS05.26 的部分内容；
本条款作为多芯片嵌入具体化进行检测，参考 AS05.35 和 AS05.36 的部分内容；
本条款作为多芯片独立具体化进行检测，参考 AS05.51 的部分内容。

AS07.19：（安全级别 2，3，4）

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

送检单位需要提交的材料

VE07.19.01：送检单位提供的文档应描述，在可见光内，指定涂层材料是不透明的。

所需的检测程序

TE07.19.01：检测人员应核实送检单位提供的文档描述了单芯片模块被在可见光内不透明的涂层所覆盖。

AS07.20：（安全级别 2，3，4）

如果密码模块包含通风孔或缝，那么孔或缝应当具有特殊的构造，从而防止通过直接观察

模块内部的构造或部件进行信息收集。上述直接观察可能会利用模块内部结构或部件发出的可见光。

注：本条款作为 AS07.25 的一部分进行检测。

AS07.21：（安全级别 3，4）

除了对安全一级和二级的通用要求，安全三级的所有密码模块还应当满足下列要求：(AS07.22-AS07.28)。

注：本条款不单独进行检测。

AS07.22：（安全级别 3，4）

如果模块含有任何门或可移动的封盖，或者定义了维护访问接口，那么模块应当包含拆卸响应与置零电路。

注：本条款对于通用要求而言作为 AS07.12 的一部分进行检测；
本条款对于单芯片实体而言作为 AS05.29 的一部分进行检测；
本条款对于多芯片实体而言作为 AS05.41 的一部分进行检测；
本条款对于多芯片独立实体而言作为 AS05.55 的一部分进行检测。

AS07.23：（安全级别 3，4）

在打开门、可移动封盖或维护访问接口时，拆卸响应与置零电路应当立即置零所有未受保护的 SSP。

注：本条款对于通用要求而言作为 AS05.11 的一部分进行检测；
本条款对于单芯片实体而言作为 AS05.29 的一部分进行检测；
本条款对于多芯片实体而言作为 AS05.41 的一部分进行检测；
本条款对于多芯片独立实体而言作为 AS05.55 的一部分进行检测。

AS07.24：（安全级别 3，4）

当密码模块内包含未受保护的 SSP 时，拆卸响应与置零电路应当保持可用状态。

注：本条款对于单芯片实体而言作为 AS05.29 的一部分进行检测；
本条款对于多芯片实体而言作为 AS05.41 的一部分进行检测；
本条款对于多芯片独立实体而言作为 AS05.55 的一部分进行检测。

AS07.25：（安全级别 3，4）

如果密码模块含有通风孔或缝，那么孔或缝应当具有特殊构造，从而防止对外壳内部进行物理探测时不被发现（例如，防止使用单铰链探头探测）。

送检单位需要提交的材料

VE07.25.01：如果被封盖或封装包含的模块含有通风孔或通风口，则这些通风孔或通风口的构建方式应能阻止封装内部的未被发现的物理探测。送检单位文档应描述物理通风结构的设计方法。

所需的检测程序

TE07.25.01：通过检查检测人员确认送检单位文档中说明了模块是否含有通风孔、通风口或其他开口的封盖或封装，如果是这样，那么它们的构建方式是否可以防止在封盖或封装内未被发现的探测。

AS07.26：（安全级别 3，4）

当模块温度超出运行、存放和分发的预期温度范围时，坚固或硬质、保型或非保型的外壳、涂层或灌封材料应当维持强度和硬度特征。

送检单位需要提交的材料

VE07.26.01：送检单位提供的文档应描述如下内容：当模块温度超出运行、存放和分发的预期温度范围时，坚固或硬质、保型或非保型的外壳、涂层或灌封材料应当维持强度和硬度特征。

所需的检测程序

TE07.26.01：检测人员应核实送检单位提供的文档包含如下内容：当模块温度超出运行、存放和分发的预期温度范围时，坚固或硬质、保型或非保型的外壳、涂层或灌封材料应当维持强度和硬度特征。

AS07.27：（安全级别 3，4）

如果使用了显示拆卸的封条，那么封条应当被唯一编号或者能够独立识别（例如，唯一编号的存迹胶布或可唯一识别的手写封条）。

送检单位需要提交的材料

VE07.27.01：送检单位提供的文档应描述如下内容：如果使用了显示拆卸的封条，那么封条应当被唯一编号或者能够独立识别（例如，唯一编号的存迹胶布或可唯一识别的手写封条）。

所需的检测程序

TE07.27.01：检测人员应核实送检单位提供的文档描述如下内容：如果使用了显示拆卸的封条，那么封条应当被唯一编号或者能够独立识别（例如，唯一编号的存迹胶布或可唯一识别的手写封条）。

AS07.28：（安全级别 3，4）

模块应当具有 EFP 特性或经过 EFT。

注：本条款作为 AS05.60-AS05.69 的一部分进行检测。

AS07.29：（安全级别 4）

除了安全一级、二级和三级的通用要求，安全四级的所有模块还应当满足下列要求: AS07.30-AS07.33。

注：本条款不单独进行检测。

AS07.30：（安全级别 4）

密码模块应当使用抗擦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。

送检单位需要提交的材料

VE07.30.01：送检单位文档须清晰描述 AS07.30 中指定的用于满足要求的方法。

VE05.28.02：送检单位文档须提供详图设计信息，特别是涂层材料的种类和特性。

所需的检测程序

TE07.30.01：通过检查检测人员确认送检单位文档中说明了模块由坚固的不透明防篡改涂层覆盖。

TE07.30.02：检测人员须确认送检单位文档材料充分描述了详图设计信息，特别是所用涂层的种类和特性。

TE07.30.03：检测人员须确认涂层所不容易渗透到内部电路的深度，并且该渗透会留下篡改标记。通过检查确认涂层完全覆盖模块，该涂层明显不透明，且能够阻止直接的观察、探测或操作。

AS07.31：（安全级别 4）

密码模块应当具有 EFP 特性。

送检单位需要提交的材料

所需的检测程序

AS07.32：（安全级别 4）

密码模块应当提供保护措施，以防止错误注入攻击。

送检单位需要提交的材料

VE07.32.01：送检单位提供的文档应描述如下内容：密码模块提供保护措施，以防止错误注入攻击。

所需的检测程序

TE07.32.01：检测人员应核实送检单位提供的文档描述如下内容：密码模块提供保护措施，以防止错误注入攻击。

AS07.33：（安全级别 4）

错误注入攻击的缓解技术以及采用的缓解指标应当在文档中按照 GB/T 0028 附录 B 规定的要求进行记录。

送检单位需要提交的材料

VE07.33.01：送检单位提供的文档应描述如下内容：错误注入攻击的缓解技术以及采用的缓解指标在文档中按照 GB/T 0028 附录 B 规定的要求进行记录。

所需的检测程序

TE07.33.01：检测人员应核实送检单位提供的文档描述如下内容：错误注入攻击的缓解技术以及采用的缓解指标在文档中按照 GB/T 0028 附录 B 规定的要求进行记录。

6.8.3 物理安全实体的物理安全要求

6.8.3.1 单芯片密码模块

注 1：除了 GM/T0028 第 6.7.2 节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。

注 2：对安全一级的单芯片密码模块没有其它额外要求。

AS07.34：（安全级别 2，3，4）

除了安全一级的要求，安全二级的单芯片密码模块还应当满足要求 AS07.35。

注：本条款不单独进行检测。

AS07.35：（安全级别 2，3，4）

应当使用拆卸存迹涂层（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）将密码模块覆盖起来，或者将模块装在一个拆卸存迹的外壳中，以阻止直接观察或探测、操控模块，并在企图拆卸或移动模块后留下证据。

注：此要求与 AS07.18 相关。

送检单位需要提交的材料

VE07.35.01：送检单位提交的文档应描述防拆卸存迹涂层及其特点。

所需的检测程序

TE07.35.01：检测人员应核实送检单位提供的文档描述防拆卸存迹涂层及其特点。

AS07.36：（安全级别 3，4）

除了安全一级和二级的要求，安全三级的单芯片密码模块还应当满足下列要求（AS07.37-AS07.39）。

送检单位需要提交的材料

VE07.36.01：送检单位提交的文档应当描述指定了 AS07.37 和 AS07.39 中的哪一种方法用于满足要求。

所需的检测程序

TE07.36.01：检测人员应核实送检单位提供的文档指定了 AS07.37 和 AS07.39 中的哪一种方法用于满足要求。

TE07.36.02：如果满足 AS07.37 中指定的方法，检测人员应遵循 TE07.37 中的检测程序；如果发现 AS07.38 方法，检测人员应遵循 AS07.38 中的检测程序。

AS07.37：（安全级别 3，4）

应当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）将模块覆盖起来，或满足 AS07.39 所描述的要求。

送检单位需要提交的材料

VE07.37.01：送检单位文档须清晰描述 AS07.34 中指定的用于满足要求的方法。

VE07.37.02：送检单位文档须提供详图设计信息，特别是涂层材料的种类和特性。

所需的检测程序

TE07.37.01：通过检查检测人员确认送检单位文档中说明了模块由坚固的不透明防拆卸涂层覆盖。

TE07.37.02：检测人员须确认送检单位文档材料充分描述了详图设计信息，特别是所用涂层的种类和特性。

TE07.37.03：检测人员须确认涂层所不容易渗透到内部电路的深度，并且该渗透会留下拆卸标记。通过检查确认涂层完全覆盖模块，该涂层明显不透明，且能够阻止直接的观察、探测或操作。

AS07.38：（安全级别 3，4）

如果不满足 AS07.37，其外壳应当合理实现，并满足 AS.07.39。

送检单位需要提交的材料

VE07.38.01：送检单位文档须提供详图设计信息，特别是当模块封装含有任何封门或可移动封盖或指定的维护访问接口时。封装的设计使移除或入侵封装的尝试极有可能对密码模块内部的电路造成严重损坏。

VE07.38.02：如果模块封装含有任何封门或可移动封盖或指定的维护访问接口，则该模块须含有拆卸响应和清零电路。该电路应持续监测这些封盖和封门，并且在移除封盖或打开封门之前，应清零所有未经加密的 CSPs。当未经加密的 CSPs 包含在模块中，则电路应是运行的。

所需的检测程序

TE07.38.01：检测人员确认送检单位文档详细说明了模块无论含有封门或可移动封盖或维护访问接口，模块封装是不能轻易打开的。如果模块封装含有任何封门或可移动封盖或定义的维护访问接口，则检测人员须确认送检单位文档详细说明了该模块含有拆卸响应和清零电路。

TE07.38.02：如果模块封装含有任何封门或可移动封盖或指定的维护访问接口，检测人员须确认送检单位文档说明了当封盖或封门被移除，或维护访问接口被访问时，模块清零电路清零所有未经加密的 CSPs。

TE07.38.03：通过检查检测人员确认送检单位文档中说明了：当模块中含有未经加密的 CSPs 时，拆卸响应和清零电路保持运行。

TE07.38.04：通过检查检测人员确认送检单位文档中说明了：在没有极可能导致对模块的严重损害时，封装不会被移除或渗透。

TE07.38.05：如果模块封装含有任何封门或可移动封盖或指定的维护访问接口，则当封盖或封门被移除或者维护访问接口被访问时，检测人员应检测模块会清零所有未经加密的 CSPs。

TE07.38.06：检测人员应检测在没有极可能导致对模块的严重损害时，封装不会被移除或渗透。

AS07.39：（安全级别 4）

企图移除或穿透外壳的行为应当极有可能对密码模块造成严重损害，即模块将不能工作。

注：本条款不单独进行检测。

AS07.40：（安全级别 4）

除了安全一级、二级和三级要求，安全四级的单芯片密码模块还应当满足下列要求（AS07.41-AS07.42）。

注：本条款不单独进行检测。

AS07.41：（安全级别 4）

应当使用抗擦除的硬质不透明涂层将密码模块覆盖起来，该涂层具有硬度与粘力特性，以致企图剥落或撬开涂层的行为将极有可能对模块造成严重损害（即模块将不起作用）。

送检单位需要提交的材料

VE07.41.01：送检单位文档应清晰确认使用的涂层的种类，并提供涂层材料的详细特性，特别是它的硬度和抗移除性。

VE07.41.02： 模块应由坚固不透明的，抗移除的涂层所覆盖。材料的硬度和粘性使得将材料从模块上剥离或查探的尝试极可能导致模块的严重损坏（例如，模块将不可运转）。涂层材料在可见光范围内是不透明的。

所需的检测程序

TE07.41.01：检测人员需核实送检单位文档中说明了模块由坚固不透明的抗移除的涂层覆盖。

TE07.41.02：检测人员应确认模块涂层的抗移除特性。检测人员应尝试剥除或探查模块的材料，并确认在能量的合理应用下，模块停止工作或模块电路明显被物理破坏是不可能的。

AS07.42：（安全级别 4）

抗擦除的涂层应当具有溶解特性，以致企图溶解涂层的行为将极有可能溶解或严重损害模块，即模块将不起作用。

送检单位需要提交的材料

VE07.42.01：送检单位文档须描述抗移除材料的溶解特性。涂层的溶解特性使通过溶解材料移除抗移除材料极可能会溶解或严重损害模块。

所需的检测程序

TE07.42.01：检测人员应确认送检单位文档以确定模块抗移除涂层的溶解特性。

TE07.42.02：检测人员应检测模块抗移除涂层的溶解特性。检测人员应根据在 VE07.38.01 中提供的文件，确定哪种类型的溶剂可威胁抗移除涂层。

6.8.3.2 多芯片嵌入式密码模块

注：除了 GM/T 0028 第 6.7.2 节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。

AS07.43：（安全级别 1，2，3，4）

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

送检单位需要提交的材料

VE07.43.01：模块应整个包含在一个产品级的封装或可移动封盖中。送检单位文档应对封盖或封装进行描述。

所需的检测程序

TE07.43.01：检测人员应核查送检单位文档中说明了模块包含在产品级的封装或可移动封盖中。

AS07.44：（安全级别 2，3，4）

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当满足下列要求(AS07.45-AS07.48)。

注：本条款不单独进行检测。

AS07.45：（安全级别 2，3，4）

应当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）将模块部件覆盖起来，以阻止直接观察以及提供企图拆卸或移动模块部件的证据。或

送检单位需要提交的材料

VE07.45.01：送检单位提供应提供坚固封装的设计文档。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）将模块部件覆盖起来，以阻止直接观察以及提供企图拆卸或移动模块部件的证据。

所需的检测程序

TE07.45.01 检测人员须确认：送检单位文档详细说明了无论封装包含封门或可移动封盖还是维护访问接口，模块须包含篡改响应和清零电路。

TE07.45.02：检测人员应核实送检单位提供的文档说明了：在没有极大可能对模块造成严重损害的情况下封装是不能移除或渗透的。

TE07.45.03：检测人员须通过尝试进入电路的内部确认封装的强度，以证明封装是不能轻易破坏的。通过检查检测人员确认送检单位文档中说明了封装是不可移除的。

TE07.45.04:：检测人员须检测在没有极大可能对模块造成严重损害的情况下封装是不能移

除或渗透的。

AS07.46：（安全级别 2，3，4）

模块应当被整个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。和

送检单位需要提交的材料

VE07.46.01：送检单位提供的文档应描述如下内容：模块被整个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。

所需的检测程序

TE07.46.01：检测人员应核实送检单位提供的文档应描述如下内容：模块被整个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。

AS07.47：（安全级别 2，3，4）

外壳包含任何门或封盖，则门或封盖应当使用防撬锁锁住，该防撬锁可以采用物理或逻辑钥匙，或者

送检单位需要提交的材料

VE07.47.01：如果外壳包含任何门或封盖，则门或封盖应当使用防撬锁锁住，送检单位文档应描述防撬机械锁及其物理的或逻辑的密钥。

所需的检测程序

TE07.47.01：检测人员应核实送检单位提供的文档描述了封门或封盖由防撬机械锁锁定，该机械锁使用物理或逻辑密钥。

TE07.47.02：检测人员须尝试在不用密钥的情况下打开锁定的封盖或封门，并确定在没留下损坏痕迹的情况下封盖或封门是不能打开的。

AS07.48：（安全级别 2，3，4）

应当被拆卸存迹的封印保护起来（例如，证据胶带或全息封印）。

送检单位需要提交的材料

VE07.48.01：送检单位提供的文档须描述拆卸存迹的封印。

所需的检测程序

TE07.48.01：检查检测人员需核实送检单位提供的文档TE07.48.02：检测人员须确认不破坏或不移除封印的情况下封盖或封门不能打开，且封印不能移开后被替代。

AS07.49：（安全级别 3，4）

除了安全一级和二级的要求，要求 AS07.50-AS07.51 应当适用于安全三级的多芯片嵌入式密码模块。

注：本条款不单独进行检测。

AS07.50：（安全级别 3，4）

应当使用硬质涂料或灌封材料（例如硬质环氧树脂材料）将密码模块内的多芯片实体电路覆盖起来，以致企图移动或穿透外壳的行为将极有可能对模块造成严重损害（即模块将不起作用）。或

送检单位需要提交的材料

VE07.50.01：送检单位提供的文档须提供硬质涂料或灌封材料（例如硬质环氧树脂材料）的设计文档。封装设计须满足如下要求：移除封装极可能对模块造成严重的损害（即模块将不起作用）。

所需的检测程序

TE07.50.01：检测人员须核实送检单位提供的文档对硬质涂料或灌封材料（例如硬质环氧树脂材料）进行了详细说明。

TE07.50.02：检测人员须核实送检单位提供的文档中说明了在不对模块造成严重损坏的情况下不能移除或渗透硬质涂料或灌封材料（例如硬质环氧树脂材料）。

AS07.51：（安全级别 3，4）

模块应当被包装在坚固的外壳内，以致企图移动或穿透外壳的行为将极有可能对模块造成严重损害（即模块将不起作用）。

送检单位需要提交的材料

VE07.51.01：送检单位提供的文档需提供坚固封装的设计文档。模块须完全包含在坚固封装中。封装设计须满足如下要求：移除封装极可能对模块造成严重的损害（**即模块将不起作用**）。

所需的检测程序

TE07.51.01： 检测人员需核实送检单位提供的文档中描述了坚固封装的设计。

TE07.51.02：检测人员需核实送检单位提供的文档中说明了在不对模块造成严重损坏的情况下不能一处或渗透坚固封装。

AS07.52：（安全级别 4）

除了安全一级、二级和三级的要求，要求 AS07.53-AS07.59 应当适用于安全四级的多芯片嵌入式密码模块。

注：本条款不单独进行检测。

AS07.53：（安全级别 4）

密码模块部件应当包装在坚固或硬质、保型或非保型的外壳中。

送检单位需要提交的材料

VE07.53.01： 送检单位提供的文档需描述如下内容：密码模块部件当包装在坚固或硬质、保型或非保型的外壳中。

所需的检测程序

TE07.53.01：检测人员需核实送检单位提供的文档描述如下内容：密码模块部件当包装在坚固或硬质、保型或非保型的外壳中。

AS07.54：（安全级别 4）

外壳应当用拆卸检测封套（例如，柔性的聚酯薄膜印制电路，带有蛇形的导线、或绕线的包装、或无弹性易碎电路、或坚固的外壳）封装起来。

送检单位需要提交的材料

VE07.54.01：送检单位提供的文档需描述如下内容：外壳用拆卸检测封套（例如，柔性的聚酯薄膜印制电路，带有蛇形的导线、或绕线的包装、或无弹性易碎电路、或坚固的外壳）封装起来。

所需的检测程序

TE07.54.01：检测人员需核实送检单位提供的文档描述如下内容：外壳用拆卸检测封套（例如，柔性的聚酯薄膜印制电路，带有蛇形的导线、或绕线的包装、或无弹性易碎电路、或坚固的外壳）封装起来。

AS07.55：（安全级别 4）

封套应当能够检测到企图访问 SSP 的拆卸行为，包括切、钻、磨、碾、烧、熔、溶解灌封材料或外壳等。

送检单位需要提交的材料

VE07.55.01：送检单位提供的文档需描述如下内容：封套能够检测到企图访问 SSP 的拆卸行为，包括切、钻、磨、碾、烧、熔、溶解灌封材料或外壳等。

所需的检测程序

TE07.55.01：检测人员需核实送检单位提供的文档描述如下内容：封套能够检测到企图访问 SSP 的拆卸行为，包括切、钻、磨、碾、烧、熔、溶解灌封材料或外壳等。

AS07.56：（安全级别 4）

密码模块应当包含拆卸响应和置零电路。

送检单位需要提交的材料

VE07.56.01：送检单位提供的文档需描述如下内容：密码模块包含拆卸响应和置零电路，篡改响应和清零电路的设计。

所需的检测程序

TE07.56.01：检测人员需核实送检单位提供的文档需描述如下内容：密码模块包含拆卸响应和置零电路，篡改响应和清零电路的设计。

AS07.57：（安全级别 4）

拆卸响应和置零电路应当能够持续地监控拆卸检测封套。

送检单位需要提交的材料

VE07.57.01：送检单位提供的文档需描述如下内容：拆卸响应和置零电路能够持续地监控拆卸检测封套。

所需的检测程序

TE07.57.01：检测人员需核实送检单位提供的文档需描述如下内容：拆卸响应和置零电路能够持续地监控拆卸检测封套。

AS07.58：（安全级别 4）

一旦检测到拆卸行为就应当立即置零所有未受保护的 SSP。

送检单位需要提交的材料

VE07.58.01：送检单位提供的文档需描述如下内容：一旦检测到拆卸行为就应当立即置零所有未受保护的 SSP。

所需的检测程序

TE07.58.01：检测人员须破坏篡改检测外壳屏障，并确认模块对所有未受保护的 SSP 进行清零。

AS07.59：（安全级别 4）

当密码模块内包含未受保护的 SSP 时，拆卸响应电路应当保持可用状态。

送检单位需要提交的材料

VE07.59.01：送检单位提供的文档需描述如下内容：当密码模块内包含未受保护的 SSP 时，拆卸响应电路应当保持可用状态。

所需的检测程序

TE07.59.01：检测人员需核实送检单位提供的文档需描述如下内容：当密码模块内包含未受保护的 SSP 时，拆卸响应电路应当保持可用状态。

6.8.3.3 多芯片独立式密码模块

注：除了 GM/T 0028 第 6.7.2 节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。

AS07.60：（安全级别 1,2,3,4）

密码模块应当整个被包装在金属或硬质塑料的产品级外壳内，外壳可以包括门或可移动封盖。

送检单位需要提交的材料

VE07.60.01：密码模块应完全包含于金属的或坚硬塑胶德产品级封装内，该封装可能包含封门或可移动封盖。送检单位文档须描述封装及其硬度特性。

所需的检测程序

TE07.60.01：通过检查检测人员确认送检单位文档中说明了模块包含在封装中，该封装满足如下要求：

a) 模块应完全包含于封装中。
b) 封装材料必须是在送检单位文档中定义的成分。
c) 封装必须是产品级的。送检单位文档必须显示相同材料的封装在商业上已被应用或提供数据以表明它与商用产品是等价的。

AS07.61：（安全级别 2,3,4）

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当满足要求 AS07.62-AS07.63。

注：本条款不单独进行检测。

AS07.62：（安全级别 2,3,4）

如果密码模块的外壳含有任何门或可移动封盖，那么门或封盖应当安装带有物理或逻辑钥匙的防撬机械锁，或者

送检单位需要提交的材料

VE05.62.01：如果封装包含可移动封盖或封门，则它们须被由物理的或逻辑密钥可打开的防撬机械锁锁定。送检单位文档须描述由物理的或逻辑的密钥可打开的防撬机械锁机制。

所需的检测程序

TE05.62.01：检测人员须确认封装是否含有可移动封盖或封门。检测人员须确认每个封盖或封门被由物理的或逻辑密钥可打开的防撬机械锁锁定。检测人员须尝试在没有密钥的情况下打开锁定的封盖或封门，以确认在没有损害痕迹的情况下封盖或封门是不能打开的。

AS07.63：（安全级别 2,3,4）

{如果不满足 AS07.62 时}应当使用拆卸存迹的封条（例如，证据胶带或全息封条）进行保护。

送检单位需要提交的材料

VE07.63.01：如果封装通过例如证据胶带或全息封条的防篡改封条保护，送检单位文档须描述防篡改封条。

所需的检测程序

TE07.63.01：封盖或封门通过例如证据胶带或全息封条的防篡改封条保护。检测人员须确认在没有破坏或移除封条的情况下封盖或封门不能打开，且封条不能移除后被替代。

AS07.64：（安全级别 3,4）

除了安全一级和二级的要求，安全三级的多芯片独立密码模块还应当满足要求 AS07.65。

注：本条款不单独进行检测。

AS07.65：（安全级别 3,4）

模块应当被包装在坚固的外壳内，以致企图移除或穿透外壳的行为将极有可能对模块造成严重损害（即模块将不起作用）。

注：本条款在 AS07.45 中检测。

AS07.66：（安全级别 4）

除了安全一级、二级和三级的要求，安全四级的多芯片独立式密码模块还应当满足要求 AS07.67-AS07.72。

注：本条款不单独进行检测。

AS07.67：（安全级别 4）

密码模块的外壳应当封装在使用下列一种拆卸检测机制的拆卸检测封套内：例如封盖开关（如微型开关、磁霍尔效应开关、永磁驱动器等）、动作探测器（如超声波的、红外线的或微波探测器）或者第 7.7.3.2 节中规定的安全四级描述的其它拆卸检测机制。

送检单位需要提交的材料

VE07.67.01：封装或陶瓷材料须被使用篡改探测机制的篡改探测外壳封装。送检单位文档须描述篡改探测外壳的设计机制。

所需的检测程序

TE07.67.01：通过检查检测人员确认送检单位文档中说明了模块封装或陶瓷材料包含篡改探测机制，通过该机制保护模块组件。该机制的设计使任何对封装或陶瓷材料的破坏以访问模块组件都能监测到。

AS07.68：（安全级别 4）

拆卸检测机制应当能够对诸如切、钻、铣、磨、烧、熔或溶解之类的攻击做出响应，这些攻击在一定程度上足以访问 SSP。

注：本条款不单独进行检测。

AS07.69：（安全级别 4）

密码模块应当包含拆卸响应和置零电路。

送检单位需要提交的材料

VE07.69.01：密码模块应包含篡改响应和清零电路，该电路应持续监测篡改检测外壳，且在探测到入侵时须立即清零所有未经加密的 CSPs。当模块中包含未经加密的 SSPs 时，篡改响应及清零电路应持续运行。送检单位文档须描述篡改响应和清零电路的设计。

所需的检测程序

TE07.69.01：检测人员确认送检单位文档中说明了密码模块包含篡改响应和清零电路，该电路应持续监测篡改检测外壳；探测通过各种方式的攻击，例如如切割、钻孔、铣、磨或溶解外壳任一部分；并且清零所有未经加密的 CSPs。

TE07.69.02：检测人员须破坏篡改检测外壳屏障，并确认模块对未经加密的 SSPs 进行清零。

AS07.70：（安全级别 4）

拆卸响应和置零电路应当能够持续地监控拆卸检测封套，并且

注：本条款不单独进行检测。

AS07.71：（安全级别 4）

一旦检测到拆卸行为就应当立即置零所有未受保护的 SSP。

注：本条款不单独进行检测。

AS07.72：（安全级别 4）

当密码模块内包含未受保护的 SSP 时，拆卸响应和置零能力应当保持可用状态。

注：本条款不单独进行检测。

6.8.4 环境失效保护/测试

6.8.4.1 环境失效保护/测试通用要求

AS07.73：（安全级别 3，4）

安全三级的模块应当具有 EFP 特性或经过 EFT。

AS07.74：（安全级别 4）

安全四级的模块应当有 EFP 特性。

6.8.4.2 环境失效保护特性

AS07.75：（安全级别 3，4）

EFP 特性应当保护密码模块，防止由不正常的环境条件或电压和温度超出模块正常运行范围的波动（意外的或引发的），对模块的安全性造成破坏。

注：本条款作为 AS07.77 的一部分检测。

AS07.76：（安全级别 3，4）

密码模块应当对超出规定的正常运行温度和电压范围的波动实施监控并做出正确响应。

注：本条款作为 AS07.77 的一部分检测。

AS07.77：（安全级别 3，4）

如果温度或电压超出密码模块的正常运行范围，则保护电路应当：

——关闭模块，防止继续运行，

或

——立即置零所有 CSP。

VE07.77.01：如果 EFP 在特定条件下使用，则模块应监测并且正确的响应在该条件下超出了正常工作范围的温度及电压波动。保护功能应持续地测量这些环境条件。如果一种条件确定超过模块正常的运行范围，保护电路应做出如下反应之一：

——关闭模块；或者

——清零所有未经加密的 CSP

文件应阐述哪种方法被选择，并且提供在模块内执行 EFP 功能的说明。

所需的检测程序

TE07.77.01：检测人员应设置环境条件（周围的温度和电压）接近于模块被指出的正常的运行范围的合适的极值，并且确认模块在正常的运行参数中持续运行。

TE07.77.02：检测人员应扩大温度和电压范围至指定的正常范围之外，并确认模块要么关闭以阻止进一步的操作，要么清零所有未经加密的 CSP。

TE07.77.03：如果模块的设计可清零所有未经加密的 CSP，并且在恢复正常环境条件后模块仍是运行的，则检测人员须完成需要密钥的任务以确认模块自身不能完成那些任务。

6.8.4.3 环境失效测试程序

AS07.78：（安全级别 3，4）

EFT 应当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模块温度和电压超出正常运行范围的波动（意外的或引发的）而遭到破坏。

注：本条款作为 AS07.84 的一部分检测。

AS07.79：（安全级别 3，4）

EFT 应当证明要求 AS07.80.

注：本条款作为 AS07.84 的一部分检测。

AS07.80

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，密码模块的安全性绝不应当遭到破坏。

注：本条款作为 AS07.84 的一部分检测。

AS07.81：（安全级别 3，4）

被测试的温度范围应当从正常运行温度范围内的温度下降到范围内的最低温度，在这个温度以下将会：（1）关闭模块防止继续运行，或（2）立即置零所有未受保护的 SSP。

注：本条款作为 AS07.84 的一部分检测。

AS07.82：（安全级别 3，4）

温度的测试范围应当为-100℃～+200℃（-150℉～+400℉（华氏度））；而且，一旦（1）模块被关闭以防止继续运行，（2）所有未受保护的 SSP 被立即置零，或

注：本条款作为 AS07.84 的一部分检测。

AS07.83：（安全级别 3，4）

（3）模块进入故障模式，则测试应当立即中断。

注：本条款作为 AS07.84 的一部分检测。

AS07.84：（安全级别 3，4）

应当在敏感部件和关键设备处，而不仅在物理边界内，对温度进行内部实时监测。

送检单位需要提交的材料

VE07.84.01：如果 EFP 在特定条件下使用，模块应在 AS07.51 中提到的温度和电压范围内进行检测。模块应满足：

——继续正常运行；或者

——停止；或者

——清零所有未经加密的 CSPs。

文件应描述选择的方法，并且提供 EFT 的详细描述。

所需的检测程序

TE07.84.01：检测人员须按照 AS07.51 中说明配置环境条件（周围的温度和电压），并确认模块要么继续正常运行，要么停止以阻止进一步操作，要么清零所有未经加密的 CSP。

TE07.84.02：如果模块的设计可清零所有未经加密的 CSP，并且在恢复正常环境条件后模块仍是运行的，则检测人员须完成需要密钥的任务以确认模块自身不能完成那些任务。

AS07.85：（安全级别 3，4）

被测试的电压范围应当逐渐从正常运行电压范围内的电压下降到范围内的最低电压，在这

个电压下将会：（1）关闭模块防止继续运行，或（2）立即置零所有未受保护的 SSP；并且应当逐渐从正常运行电压范围内的电压上升到范围内的最高电压，在这个电压以上将会：（1）关闭模块防止继续运行，或（2）立即置零所有未受保护的 SSP。

注：本条款作为 AS07.84 的一部分检测。

6.9 非入侵式安全

AS08.01：（安全级别 1，2，3，4）
如果由密码模块实现、用于保护模块 SSP 的非入侵式攻击的缓解技术不在 GM/T 0028 附录 F 中，则这些技术应当满足 GM/T 0028 第 7.12 节中规定的要求。

送检单位需要提交的材料

VE08.01.01：送检单位提交非入侵式安全的文档。

所需的检测程序

TE08.01.01：检测人员应核实送检单位提交的文档是否满足 GM/T 0028 第 7.12 节中规定的要求。

AS08.02：（安全级别 1，2，3，4）
如果由密码模块实现、用于保护模块 SSP 的非入侵式攻击的缓解技术在 GM/T 0028 附录 F 中，则这些技术应当满足 AS08.03、AS08.04、AS08.05、AS08.06、AS08.07 中规定的要求。

注：本条款不单独进行检测。

AS08.03：（安全级别 1，2，3，4）

6.8 中所提供的文档应当按照 GM/T 0028 A.2.8 中规定的要求编写。

送检单位需要提交的材料

VE08.03.01：送检单位提交非入侵式安全的文档。

所需的检测程序

TE08.03.01：检测人员应核实文档是否按照 GM/T 0028 A.2.8 中规定的要求编写。

AS08.04：（安全级别 1，2）

对于安全一级和二级，文档应当阐明所有用于保护模块 CSP 不受非入侵式攻击且包含在 GM/T 0028 附录 F 中的缓解技术。

送检单位需要提交的材料

VE08.04.01：送检单位提交非入侵式安全的文档。

所需的检测程序

TE08.04.01：检测人员核实文档是否阐明了所有用于保护模块 CSP 不受非入侵式攻击且包含

在 GM/T 0028 附录 F 中的缓解技术。

AS08.05：（安全级别 1，2，3，4）

阐明所有用于保护模块 CSP 不受非入侵式攻击且包含在 GM/T 0028 附录 F 中的缓解技术的文档应当包括可以证明每个缓解技术有效性的证据。

送检单位需要提交的材料

VE08.05.01：送检单位提交非入侵式安全的文档。

所需的检测程序

TE08.05.01：检测人员核实文档是否阐明了可以证明每个缓解技术有效性的证据。

AS08.06：（安全级别 3）

对于安全三级，除了安全一级和二级的要求，密码模块应当接受测试以满足 GM/T 0028 附录 F 中针对安全三级的核准非入侵式攻击缓解测试的指标要求。

送检单位需要提交的材料

VE08.06.01：送检单位提交非入侵式安全的文档。

所需的检测程序

TE08.06.01：检测人员按照 GM/T 0028 附录 F 中针对安全三级的核准非入侵式攻击缓解测试的指标要求，对测试品进行测试。

AS08.07：（安全级别 4）

对于安全四级，除了安全一级和二级的要求，密码模块应当接受测试以满足 GM/T 0028 附录 F 中针对安全四级的核准非入侵式攻击缓解测试的指标要求。

送检单位需要提交的材料

VE08.07.01：送检单位提交非入侵式安全的文档。

所需的检测程序

TE08.07.01：检测人员按照 GM/T 0028 附录 F 中针对安全四级的核准非入侵式攻击缓解测试的指标要求，对测试品进行测试。

6.10　敏感安全参数管理

6.10.1　敏感安全参数管理通用要求

AS09.01：（安全级别 1，2，3，4）

CSP 应当在模块内受保护以防止非授权的访问、使用、泄露、修改和替换。

送检单位需要提交的材料

VE09.01.01：送检单位的文档应说明对模块内部所有 CSP 的保护。保护应包括防止未经授权的公开，修改和替代的实施机制。

所需的检测程序

TE09.01.01：检测人员应检查送检单位的文档是否详细描述了对 CSP 的保护。检测人员应当核实文档如何使 CSP 免遭未经授权的访问、使用、泄露、修改和替换。

TE09.01.02：检测人员应完成以下检测：

a） 尝试访问（使用描述的保护机制）检测人员未被授权访问的 CSP。为满足这个声明，模块应拒绝访问或只允许加密访问或以其他方式保护 CSP。

b） 使用送检单位文档未描述的任意方法修改所有的 CSP，并且试图将他们加载到模块中。模块应不允许任何 CSP 被成功加载。检测人员应尝试使用私钥和公钥完成密码操作。模块应不执行这些操作。检测人员应利用 CSP 尝试执行密码服务。模块应不执行这些操作。

AS09.02：（安全级别 1，2，3，4）

PSP 应当在模块内受保护以防止非授权的修改和替换。

送检单位需要提交的材料

VE09.02.01：送检单位提交的文档应描述防止所有 PSP 被未经授权的修改和替换的保护措施。

所需的检测程序

TE09.02.01：检测人员应核实送检单位文档中描述的 PSP 是如何被保护以免受到未经授权的修改和替换。

TE09.02.02：检测人员应使用送检单位文档未描述的任意方法修改所有的 PSP，并且试图将他们加载到模块中。模块应不允许任何 PSP 被成功加载。为满足这个声明，检测人员应尝试使用这些 PSP 完成密码操作；模块应不执行这些操作。

AS09.03：（安全级别 1，2，3，4）

模块应当将生成的、输入或输出模块的 SSP，与该 SSP 被分配的实体（即人、组、角色、或进程）关联起来。

送检单位需要提交的材料

VE09.03.01：送检单位提供的文档应描述生成的、输入或输出模块的 SSP 与被分配实体（即人、组、角色、或进程）的关联关系。

所需的检测程序

TE09.03.01：检测人员应核实生成的、输入或输出模块的 SSP 与被分配实体（即人、组、角色、或进程）的关联关系是否与文档描述的一致。

AS09.04：（安全级别 1，2，3，4）

口令的杂凑值、RBG 状态信息和密钥生成的中间值应当被看作是受保护的 CSP。

送检单位需要提交的材料

VE09.04.01：送检单位提交的文档应描述如何保护口令的杂凑值、RBG 状态信息和密钥生成的中间值。

所需的检测程序

TE09.04.01：检测人员应核实文档中描述的保护方法是否有效。

TE09.04.02：检测人员应尝试是否能获取口令的杂凑值。

TE09.04.03：检测人员应尝试是否能获取 RBG 状态信息。

TE09.04.04：检测人员应尝试是否能获取密钥生成的中间值。

AS09.05：（安全级别 1，2，3，4）

6.9 中所提供的文档应当按照 GM/T 0028 A.2.9 中规定的要求编写。

送检单位需要提交的材料

VE09.05.01：送检单位提交的有关敏感安全参数管理的文档。

所需的检测程序

TE09.05.01：检测人员应核实文档是否按照 GM/T 0028 A.2.9 中规定的要求编写。

6.10.2 随机比特生成器

AS09.06：（安全级别 **1，2，3，4**）

如果核准的安全功能、SSP 生成或 SSP 建立方法需要随机值，则核准的 RBG 应当用于提供这些值。

送检单位需要提交的材料

VE09.06.01：送检单位提交的有关敏感安全参数管理的文档。

所需的检测程序

TE09.06.01： 检测人员应核实是否利用核准的 RBG 的输出作为安全功能所需要的随机数。

TE09.06.02： 检测人员应核实是否利用核准的 RBG 的输出作为 SSP 生成所需要的随机数。

TE09.06.03： 检测人员应核实是否利用核准的 RBG 的输出作为 SSP 建立方法所需要的随机数。

AS09.07：（安全级别 1，2，3，4）

如果熵是从模块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当被看作为 CSP。

送检单位需要提交的材料

VE09.07.01：送检单位提交的有关敏感安全参数管理的文档。

所需的检测程序

TE09.07.01： 检测人员应核实是否存在对熵作为输入所生成的数据流进行攻击的方法。

6.10.3 敏感安全参数的生成

AS09.08：（安全级别 1，2，3，4）

如果 SSP 的生成使用了核准 RBG 的输出，破坏该方法的安全性（例如，猜测用于初始化确定性 RBG 的种子值）应当至少与猜测已生成的 SSP 值的代价相当。

送检单位需要提交的材料

VE09.08.01：送检单位应指明 SSP 生成所使用的的 RBG 输出方法。

VE09.08.02：送检单位应提供证明文件证实使用的 RBG 输出方法是经过核准的。

VE09.08.03：送检单位应描述破坏 RBG 输出方法安全性的难度。

所需的检测程序

TE09.08.01：检测人员应核实 SSP 生成所使用的的 RBG 输出方法是经过核准的。

TE09.08.02:检测人员应核实破坏 RBG 输出方法安全性的难度应当至少与猜测已生成的 SSP 值的代价相当

AS09.09：（安全级别 1，2，3，4）

密码模块应当使用GM/T 0028附录D中的核准生成方法来生成SSP，即该SSP使用核准的RBG输出生成或由输入模块的SSP衍生，且该SSP可以用于核准的安全功能或作为SSP建立方法的输入。

送检单位需要提交的材料

VE09.09.01：送检单位提交的有关敏感安全参数管理的文档。

所需的检测程序

TE09.09.01：检测人员应核实是否使用了 GM/T 0028 附录 D 中的核准生成方法来生成 SSP。

6.10.4 敏感安全参数的建立

AS09.10：（安全级别 1，2，3，4）

自动的 SSP 建立应当使用 GM/T 0028 附录 D 中的核准方法。

送检单位需要提交的材料

VE09.10.01：送检单位提交的文档应描述 SSP 建立的方法。

所需的检测程序

TE09.10.01：检测人员应核实文档中描述的自动 SSP 的建立方法是否属于 GM/T 0028 附录 D 中的核准方法。

AS09.11：（安全级别 1，2，3，4）

手动的 SSP 建立应当满足 GM/T 0028 第 7.9.5 节中规定的要求。

送检单位需要提交的材料

VE09.11.01：送检单位提交的文档应描述 SSP 建立的方法。

所需的检测程序

TE09.11.01：检测人员应核实文档中描述的手动 SSP 建立应当满足 GM/T 0028 第 7.9.5 节中规定的要求。

6.10.5 敏感安全参数的输入和输出

AS09.12：（安全级别 1，2，3，4）

如果 SSP 是手动输入到模块或从模块输出，输入或输出应当通过 GM/T 0028 第 7.3.2 节中规定的已定义的 HMI、SFMI、HFMI 或 HSMI 接口。

送检单位需要提交的材料

VE09.12.01：送检单位提交的文档应描述所有手动输入和输出 SSP 方法。

所需的检测程序

TE09.12.01：检测人员核实是否存在不通过 GM/T 0028 第 7.3.2 节中规定的已定义的 HMI、SFMI、HFMI 或 HSMI 接口进行输入或输出的 SSP。

AS09.13：（安全级别 1，2，3，4）

所有受密码技术保护的 SSP，无论是输入模块的或从模块输出的，都应当使用核准的安全功能进行加密。

送检单位需要提交的材料

VE09.13.01：送检单位提交的文档应描述所有受密码技术保护的 SSP 输入和输出的方法。

所需的检测程序

TE09.13.01：检测人员核实是否存在未使用核准的安全功能进行加密的 SSP 进行了输入或输出。

AS09.14：（安全级别 1，2，3，4）

加密的 SSP 直接输入到模块，则 SSP 的明文值不应当显示出来。

送检单位需要提交的材料

VE09.14.01：送检单位提交的文档应描述加密的 SSP 直接输入到模块方法。

所需的检测程序

TE09.14.01：检测人员核实 SSP 的明文值是否显示了出来。

AS09.15：（安全级别 1，2，3，4）

直接输入（明文或加密）的 SSP 应当在输入模块的过程中，使用 GM/T 0028 第 7.10.3.5 节中规定的条件手动输入测试进行验证，以保证准确度。

送检单位需要提交的材料

VE09.15.01：送检单位提交的文档应描述往模块直接输入（明文或加密）SSP 的方法。

所需的检测程序

TE09.15.01：检测人员核实输入 SSP 时是否使用了错误检测码（EDC）或者输入两次。

TE09.15.02：若采用错误检测码（EDC）的方式，EDC 的长度是否至少为 16 比特。

AS09.16：（安全级别 1，2，3，4）

为了防止不经意地输出敏感信息，应当需要两个独立的内部操作来执行任意明文 CSP 的输出。

送检单位需要提交的材料

VE09.16.01：送检单位提交的文档应描述所有明文 CSP 输出的方法。

所需的检测程序

TE09.16.01：检测人员核实任意明文 CSP 的输出是否由两个独立的内部操作来完成。

AS09.17：（安全级别 1，2，3，4）

控制任意明文 CSP 输出的两个独立的内部操作应当专门用于共同控制 CSP 的输出。

送检单位需要提交的材料

VE09.17.01：送检单位提交的文档应描述所有明文 CSP 输出的方法。

所需的检测程序

TE09.17.01：检测人员核实控制任意明文 CSP 输出的两个独立的内部操作是否专门用于共同控制 CSP 的输出。

AS09.18：（安全级别 1，2，3，4）

对于通过无线连接的电子输入或输出，CSP、密钥分量和鉴别数据应当经过加密。

送检单位需要提交的材料

VE09.18.01：送检单位提交的文档应描述通过无线连接的电子输入或输出，CSP、密钥分量和鉴别数据的加密方法。

所需的检测程序

TE09.18.01：检测人员核实通过无线连接的电子输入或输出，CSP、密钥分量和鉴别数据是否经过了加密。

AS09.19：（安全级别 1，2）

对于软件模块或混合软件模块的软件部件，CSP、密钥分量和鉴别数据可以以加密或明文的形式输入或输出，前提是 CSP、密钥分量和鉴别数据应当只保留在该运行环境中，并满足 GM/T 0028 第 7.6.3 节中规定的要求。

送检单位需要提交的材料

VE09.19.01：送检单位提交的文档应描述软件部件中 CSP、密钥分量和鉴别数据输入或输出的方法。

VE09.19.01：送检单位提交的文档应描述 CSP、密钥分量和鉴别数据的输入或输出应当只保留在该运行环境中。

VE09.19.01：送检单位应在文档中说明 VE09.19.01 提到的运行环境满足 GM/T 0028 第 7.6.3 节中规定的要求。

所需的检测程序

TE09.19.01：检测人员核实 CSP、密钥分量和鉴别数据的输入和输出是否只保留在运行环境中。

TE09.19.02：检测人员核实运行环境是否满足 GM/T 0028 第 7.6.3 节中规定的要求。

AS09.20：（安全级别 3）

除了安全一级和二级的要求，CSP、密钥分量和鉴别数据应当以加密的形式或通过可信信道输入或输出模块。

送检单位需要提交的材料

VE09.20.01：送检单位提交的文档应描述 CSP、密钥分量和鉴别数据输入或输出的方法。

所需的检测程序

TE09.20.01：检测人员核实 CSP、密钥分量和鉴别数据是否以加密的形式或通过可信信道输入或输出模块。

AS09.21：（安全级别 3）

明文的对称密钥和私钥 CSP 应当使用知识拆分过程与可信信道输入或输出模块。

送检单位需要提交的材料

VE09.21.01：送检单位提交的文档应描述明文的对称密钥和私钥 CSP 输入或输出的方法。

所需的检测程序

TE09.21.01：检测人员核实明文的对称密钥和私钥 CSP 是否使用知识了拆分过程与可信信道输入或输出模块。

AS09.22：（安全级别 3）

如果模块使用了知识拆分过程输入或输出明文的对称密钥和私钥 CSP，模块应当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。

送检单位需要提交的材料

VE09.22.01：送检单位提交的文档应描述明文的对称密钥和私钥 CSP 输入或输出的方法。

所需的检测程序

TE09.22.01：检测人员核实模块是否使用了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。

AS09.23：（安全级别 3）

如果模块使用了知识拆分过程输入或输出明文的对称密钥和私钥 CSP，至少需要两个密钥分量来重建原来的密钥。

送检单位需要提交的材料

VE09.23.01：送检单位提交的文档应描述明文的对称密钥和私钥 CSP 输入或输出的方法。

所需的检测程序

TE09.23.01：检测人员核实使用知识拆分过程输入或输出明文的对称密钥和私钥 CSP 时，是否至少需要两个密钥分量来重建原来的密钥。

AS09.24：（安全级别 4）

如果模块使用了知识拆分过程输入或输出明文的对称密钥和私钥 CSP，除了安全三级的要求，模块应当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。

送检单位需要提交的材料

VE09.24.01：送检单位提交的文档应描述明文的对称密钥和私钥 CSP 输入或输出的方法。

所需的检测程序

TE09.24.01：检测人员核实使用知识拆分过程输入或输出明文的对称密钥和私钥 CSP 时，是否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。

6.10.6 敏感安全参数的存储

AS09.25：（安全级别 1，2，3，4）

模块应当将 SSP 的存储与相应的实体（例如，操作员、角色或进程）关联起来。

送检单位需要提交的材料'

VE09.25.01：送检单位提交的文档应描述 SSP 的存储方法。

所需的检测程序

TE09.25.01：检测人员核实 SSP 的存储是否与相应的实体（例如，操作员、角色或进程）关联起来。

AS09.26：（安全级别 1，2，3，4）

应当禁止非授权操作员访问明文 CSP。

送检单位需要提交的材料

VE09.26.01：送检单位提交的文档应描述 CSP 的访问方法。

所需的检测程序

TE09.26.01：检测人员核实是否存在非授权操作员可以访问明文 CSP。

AS09.27：（安全级别 1，2，3，4）

应当禁止非授权操作员修改 PSP。

送检单位需要提交的材料

VE09.27.01：送检单位提交的文档应描述 PSP 的修改方法。

所需的检测程序

TE09.27.01：检测人员核实是否存在非授权操作员可以可以修改 CSP。

6.10.7 敏感安全参数的置零

AS09.28：（安全级别 1，2，3，4）

密码模块应当提供模块内所有未受保护的 SSP 和密钥分量的置零方法。

送检单位需要提交的材料

VE09.28.01：送检单位提交的文档应描述所有未受保护的 SSP 和密钥分量的置零方法。

所需的检测程序

TE09.28.01：检测人员核实文档描述的置零方法是否有效。

AS09.29：（安全级别 1，2，3，4）

SSP 被置零之后应当无法从模块中恢复。

送检单位需要提交的材料

VE09.29.01：送检单位提交的文档应描述 SSP 置零的方法。

所需的检测程序

TE09.29.01：检测人员核实能否将置零之后的 SSP 恢复。

AS09.30：（安全级别 2, 3）

密码模块应当对未受保护的 SSP 执行置零。

送检单位需要提交的材料

VE09.30.01：送检单位提交的文档应描述对未受保护的 SSP 执行置零的方法。

所需的检测程序

TE09.30.01：检测人员核实文档描述的置零方法是否有效。

AS09.31：（安全级别 2，3）

置零不应当使用一个未受保护的 SSP 来覆盖另一个未受保护的 SSP。

送检单位需要提交的材料

VE09.31.01：送检单位提交的文档应描述对未受保护的 SSP 置零的方法。

所需的检测程序

TE09.31.01：检测人员核实是否存在使用一个未受保护的 SSP 来覆盖另一个未受保护的 SSP 的情况。

AS09.32：（安全级别 2，3）

临时 SSP 在使用完毕之后应当被置零。

送检单位需要提交的材料

VE09.32.01：送检单位提交的文档应描述对临时 SSP 的使用方法。

所需的检测程序

TE09.32.01：检测人员核实临时 SSP 在使用完毕之后是否被置零。

AS09.33：（安全级别 2，3）

模块应当在置零完成时提供输出状态指示。

送检单位需要提交的材料

VE09.33.01：送检单位提交的文档应描述对 SSP 置零的方法。

所需的检测程序

TE09.33.01：检测人员核实对 SSP 置零后，是否提供了输出状态指示。

AS09.34：（安全级别 4）

除了安全二级和三级的要求之外，还应当满足下列要求。

注：本条款不单独进行检测。

AS09.35：（安全级别 4）

{除了安全二级和三级的要求之外}安全级别 4 要求置零应当是及时的、不可中断的。

送检单位需要提交的材料

VE09.35.01：送检单位提交的文档应描述对 SSP 置零的方法。

所需的检测程序

TE09.35.01：检测人员核实对 SSP 置零是否是及时的、不可中断的。

AS09.36：（安全级别 4）

{除了安全二级和三级的要求之外}安全级别 4 要求置零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。

送检单位需要提交的材料

VE09.36.01：送检单位提交的文档应描述对 SSP 置零的方法。

所需的检测程序

TE09.36.01：检测人员核实对 SSP 置零是否发生在足够短的时间内。

AS09.37：（安全级别 4）

除了安全二级和三级的要求之外，安全级别 4 要求无论是明文还是受密码技术保护的 SSP 应当被置零，使得模块返回出厂状态。

送检单位需要提交的材料

VE09.37.01：送检单位提交的文档应描述对 SSP 置零的方法。

所需的检测程序

TE09.37.01：检测人员核实对无论是明文还是受密码技术保护的 SSP 是否被置零。

6.11 自测试

6.11.1 自测试通用要求

AS10.01：（安全级别 1，2，3，4）

所有自测试都应当被执行。

送检单位需要提交的材料

VE10.01.01：送检单位提交的文档应描述模块自测试的说明。

所需的检测程序

TE10.01.01：检测人员核实模块是否进行了自测试。

AS10.02：（安全级别 1，2，3，4）

自测试的通过或失败应当由模块自身决定，无需外部的控制、外部提供输入文档向量、预期的输出接口、或操作员的干预，而且不管模块将运行于核准模式或非核准模式。

送检单位需要提交的材料

VE10.02.01：送检单位提交的文档应描述模块自测试的说明。

所需的检测程序

TE10.02.01：检测人员核实自测试结果是否只由模块本身决定，与外部的控制、外部提供输入文档向量、预期的输出接口、或操作员的干预都无关。

AS10.03：（安全级别 1，2，3，4）

运行前自测试应当在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。

送检单位需要提交的材料

VE10.03.01：送检单位提交的文档应描述模块自测试的说明。

所需的检测程序

TE10.03.01：检测人员核实在模块在提供任何数据输出（通过数据输出接口）之前是否执行了自测试，并成功通过。

AS10.04：（安全级别 1，2，3，4）

条件自测试应当在相应的安全功能或进程被调用时执行。

送检单位需要提交的材料

VE10.0.014：送检单位提交的文档应描述模块自测试的说明。

所需的检测程序

TE10.04.01：检测人员核实在相应的安全功能或进程被调用时，模块是否执行了条件自测试。

AS10.05：（安全级别 1，2，3，4）

密码模块应当对其实现的 GM/T 0028 附录 C 到 E 中定义的密码算法，执行对应的自测试。

送检单位需要提交的材料

VE10.05.01：送检单位提交的文档应描述模块自测试的说明。

所需的检测程序

TE10.05.01：检测人员核实在实现 GM/T 0028 附录 C 到 E 中定义的密码算法时，模块是否执行了自测试。

AS10.06：无

AS10.07：（安全级别 1，2，3，4）

如果密码模块自测试失败，模块应当进入错误状态。

送检单位需要提交的材料

VE10.07.01：送检单位提交的文档应描述模块自测试的说明。

所需的检测程序

TE10.07.01：检测人员核实当密码模块自测试失败时，模块是否进入了进入错误状态。

AS10.08：（安全级别 1，2，3，4）

如果密码模块自测试失败，模块应当按照 GM/T 0028 第 7.3.3 节中的规定，输出一个错误指示。

送检单位需要提交的材料

VE10.08.01：送检单位提交的文档应描述模块自测试的说明。

所需的检测程序

TE10.08.01：检测人员核实当密码模块自测试失败时，模块是否按照 GM/T 0028 第 7.3.3 节中的规定，输出了一个错误指示。

AS10.09：（安全级别 1，2，3，4）

在自测试失败进入错误状态下，密码模块不应当执行任何密码操作，或通过控制、数据输出接口输出控制和数据。

送检单位需要提交的材料

VE10.09.01：送检单位提交的文档应描述模块自测试的说明。

所需的检测程序

TE10.09.01：检测人员核实当密码模块自测试失败时，模块是否按照 GM/T 0028 第 7.3.3 节中的规定，输出了一个错误指示。

AS10.10：（安全级别 1，2，3，4）

模块不应当使用自测试失败的功能和算法，直至它们重新被测试并成功通过。

送检单位需要提交的材料

VE10.10.01：送检单位提交的文档应描述模块自测试的说明。

所需的检测程序

TE10.10.01：检测人员核实当密码模块自测试失败时，模块是否还在使用其功能和算法。

AS10.11：（安全级别 1，2，3，4）

如果模块自测试失败时模块不输出错误状态，模块操作员应当能够通过在安全策略（GM/T 0028 附录 B）中的方法和步骤，判断该模块是否已经进入了错误状态。

送检单位需要提交的材料

VE10.11.01：送检单位提交的文档应描述模块自测试的说明。

所需的检测程序

TE10.11.01：检测人员核实当密码模块自测试失败，如果不输出错误状态，是否提供给了操作员判断模块是否已经进入了错误状态的方法和步骤，并且此方法和步骤符合 GM/T 0028 附录 B 的安全策略。

AS10.12：（安全级别 3，4）

在安全三级和四级中，模块应当维护错误日志，密码模块的授权管理员可以访问该日志。

送检单位需要提交的材料

VE10.12.01：送检单位提交的文档应描述模块自测试的说明。

所需的检测程序

TE10.12.01：检测人员核实模块是否维护了错误日志。

TE10.12.02：检测人员核实授权管理员是否可以访问该日志。

AS10.13：（安全级别 3，4）

在安全三级和四级中，错误日志应当至少提供最近的错误事件（例如，自测试失败）。

送检单位需要提交的材料

VE10.13.01：送检单位提交的文档应描述模块自测试的说明。

所需的检测程序

TE10.13.01：检测人员核实错误日志是否记录了最近的错误事件。

AS10.14：（安全级别 1, 2，3，4）

6.10.1 中要求提交的所有文档应当按照 GM/T 0028 A.2.10 中规定的要求编写。

送检单位需要提交的材料

VE10.14.01：送检单位提交的自测试说明的文档。

所需的检测程序

TE10.14.01：检测人员核实文档是否按照 GM/T 0028 A.2.10 中规定的要求编写。

6.11.2 运行前自测试

6.11.2.1 运行前自测试通用要求

AS10.15：（安全级别 1, 2，3，4）

运行前自测试应当被密码模块执行并成功通过。

送检单位需要提交的材料

VE10.15.01：送检单位提交的自测试说明的文档。

所需的检测程序

TE10.15.01：检测人员核实自测试是否被密码模块执行并成功通过。

AS10.16：（安全级别 1, 2，3，4）

密码模块应当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。

送检单位需要提交的材料

VE10.16.01：送检单位提交的自测试说明的文档。

所需的检测程序

TE10.16.01：检测人员核实模块是否执行了运行前软件/固件完整性测试。

TE10.16.02：检测人员核实模块是否执行了运行前旁路测试。

TE10.16.03：检测人员核实模块是否执行了运行前关键功能测试。

6.11.2.2 运行前软件/固件完整性测试

AS10.17：（安全级别 1, 2，3，4）

密码边界内的所有软件和固件部件都应当使用核准的完整性技术进行验证，并满足 GM/T 0028 7.5 中定义的要求。

送检单位需要提交的材料

VE10.17.01：送检单位提交的文档应描述对软件和固件进行完整性验证的说明。

所需的检测程序

TE10.17.01：检测人员核实所有软件和固件是否都使用核准的完整性技术进行验证。

TE10.17.01：检测人员核实完整性验证是否满足 GM/T 0028 7.5 中定义的要求。

AS10.18：（安全级别 1, 2，3，4）

软件和固件部件的完整性验证失败，运行前软件/固件完整性测试应当失败。

送检单位需要提交的材料

VE10.18.01：送检单位提交的文档应描述对软件和固件部件进行完整性验证的说明。

所需的检测程序

TE10.18.01：检测人员核实当软件和固件部件的完整性验证失败时，运行前软件/固件完整性测试是否失败。

AS10.19：（安全级别 1, 2，3，4）

如果硬件模块不包含软件或固件，模块应当至少实现一个 GM/T 0028 第 7.10.3.2 节中规定的密码算法自测试作为运行前自测试。

送检单位需要提交的材料

VE10.19.01：送检单位提交的文档应描述模块运行前自测试的说明。

所需的检测程序

TE10.19.01：针对不包含软件或固件的硬件模块，检测人员核实模块是否至少实现了一个 GM/T 0028 第 7.10.3.2 节中规定的密码算法自测试作为运行前自测试。

AS10.20：（安全级别 1, 2，3，4）

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当先通过 GM/T 0028 第 7.10.3.2 节中规定的密码算法自测试。

送检单位需要提交的材料

VE10.20.01：送检单位提交的文档应描述对软件和固件进行完整性验证的说明。

所需的检测程序

TE10.20.01：检测人员核实用于运行前软件/固件完整性验证的算法是否先通过了 GM/T 0028 第 7.10.3.2 节中规定的密码算法自测试。

6.11.2.3 运行前旁路测试

AS10.21：（安全级别 1, 2，3，4）

如果密码模块实现了旁路能力，那么模块应当确保管理旁路能力的逻辑是正确的。

送检单位需要提交的材料

VE10.21.01：送检单位提交的文档应描述运行前旁路测试的说明。

所需的检测程序

TE10.21.01：检测人员核实模块管理旁路能力的逻辑是否是正确的。

AS10.22：（安全级别 1, 2，3，4）

模块应当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。

送检单位需要提交的材料

VE10.22.01：送检单位提交的文档应描述运行前旁路测试的说明。

所需的检测程序

TE10.22.01：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否经过加密。

TE10.22.02：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否没有经过加密的。

6.11.2.4 运行前关键功能测试

AS10.23：（安全级别 1, 2，3，4）

其它一些关系到密码模块安全操作的重要安全功能应当在运行前进行测试。

送检单位需要提交的材料

VE10.23.01：送检单位提交的文档应描述运行前进行自测试的说明。

所需的检测程序

TE10.23.01：检测人员核实其它一些关系到密码模块安全操作的重要安全功能是否在运行前进行测试。

AS10.24：（安全级别 1, 2，3，4）

文档应当阐明需要在运行前进行测试的关键功能。

送检单位需要提交的材料

VE10.24.01：送检单位提交的文档应描述运行前进行自测试的说明。

所需的检测程序

TE10.24.01：检测人员核实文档是否阐明了需要在运行前进行测试的关键功能。

6.11.3 条件自测试

6.11.3.1 条件自测试通用要求

AS10.25：（安全级别 1, 2，3，4）

在下列测试规定的条件出现时，密码模块应当执行对应的测试：密码算法自测试、配对一致性测试、软件/固件加载测试、手动密钥输入测试、条件旁路测试以及条件关键功能测试。

送检单位需要提交的材料

VE10.25.01：送检单位提交的文档应描述进行自测试的说明。

所需的检测程序

TE10.25.01：密码算法自测试的条件出现时，检测人员核实模块是否执行了此测试。

TE10.25.02：配对一致性测试的条件出现时，检测人员核实模块是否执行了此测试。

TE10.25.03：软件/固件加载测试的条件出现时，检测人员核实模块是否执行了此测试。

TE10.25.04：手动密钥输入测试的条件出现时，检测人员核实模块是否执行了此测试。

TE10.25.05：条件旁路测试的条件出现时，检测人员核实模块是否执行了此测试。

TE10.25.06：条件关键功能测试的条件出现时，检测人员核实模块是否执行了此测试。

6.11.3.2 密码算法条件自测试

AS10.26：（安全级别 1, 2，3，4）

应当针对每个核准的密码算法的所有密码功能（例如，安全功能、SSP 建立方法、鉴别）进行密码算法测试。

送检单位需要提交的材料

VE10.26.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.26.01：检测人员核实模块是否对每个核准的密码算法的所有密码功能（例如，安全功能、SSP 建立方法、鉴别）进行了密码算法测试。

AS10.27：（安全级别 1, 2，3，4）

在密码算法第一次运行使用之前，应当执行该条件测试。

送检单位需要提交的材料

VE10.27.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.27.01：检测人员核实在密码算法第一次运行使用之前，是否执行了该条件测试。

AS10.28：（安全级别 1, 2，3，4）

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当失败。

送检单位需要提交的材料

VE10.28.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.28.01：检测人员核实在密码在计算输出不等于已知答案时，密码算法已知答案自测试是否失败。

AS10.29：（安全级别 1, 2，3，4）

算法自测试应当至少针对模块支持的最小核准密钥长度、模数、素数或曲线等进行测试。

送检单位需要提交的材料

VE10.29.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.29.01：检测人员核实是否至少针对模块支持的最小核准密钥长度、模数、素数或曲线进行了测试。

AS10.30：（安全级别 1, 2，3，4）

如果算法规定了多个模式（例如，ECB、CBC 等），自测试应当至少选择其中一个模式，而且这个模式是受模块支持的或审验机构规定的。

送检单位需要提交的材料

VE10.30.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.30.01：检测人员核实是否对算法规定的多个模式（例如，ECB、CBC 等）中至少一个进行了自测试。

AS10.31：（安全级别 1, 2，3，4）

对于已知答案测试例子中单向的功能，输入测试向量生成的输出应当与预期的输出（例如，杂凑、带密钥的杂凑、消息鉴别、RBG（确定的熵向量）、SSP 协商）相等。

送检单位需要提交的材料

VE10.31.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.31.01：检测人员核实输入测试向量生成的输出应当与预期的输出（例如，杂凑、带密钥的杂凑、消息鉴别、RBG（确定的熵向量）、SSP 协商）是否相等。

AS10.32：（安全级别 1, 2，3，4）

对于已知答案测试例子中可逆的功能：正反功能都应当经过自测试（例如，对称密钥的加解密、SSP 传输的加解密、数字签名的产生和验证）。

送检单位需要提交的材料

VE10.32.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.32.01：检测人员核实正反功能是否都经过自测试。

AS10.33：（安全级别 1, 2，3，4）

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当失败。

送检单位需要提交的材料

VE10.33.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.33.01：检测人员核实当两个或多个独立的密码算法实现的输出对比不相等时，密码算法对比自测试是否失败。

6.11.3.3 配对一致性条件测试

AS10.34：（安全级别 1, 2，3，4）

如果一个密码模块生成公私钥对，配对一致性测试应当针对每对生成的公钥和私钥（由 GM/T 0028 附录 C 至 E 规定的适用的密码算法生成）执行。

送检单位需要提交的材料

VE10.34.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.34.01：检测人员核实配对一致性测试是否针对每对生成的公钥和私钥（由 GM/T 0028 附录 C 至 E 规定的适用的密码算法生成）执行。

6.11.3.4 软件/固件加载条件测试

AS10.35：（安全级别 1, 2，3，4）

如果密码模块可以从外部加载软件或固件，那么除了 GM/T 0028 第 7.4.3.4 节中规定的要求，还应当进行 AS10.36、AS10.37、AS10.38、AS10.39、AS10.40 的测试。

本条款不单独进行检测

AS10.36.01：**（安全级别 1, 2，3，4）**

密码模块应当实现核准的鉴别技术以验证加载软件或固件的完整性。

送检单位需要提交的材料

VE10.36.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.36.01：检测人员核实是否使用了核准的鉴别技术来验证加载软件或固件的完整性。

AS10.37：（安全级别 1, 2，3，4）

核准的鉴别技术所需的鉴别密钥应当在软件或固件加载之前，独立地加载到模块中。

送检单位需要提交的材料

VE10.37.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.37.01：检测人员核实核准的鉴别技术所需的鉴别密钥应当在软件或固件加载之前，是否独立地加载到模块中。

AS10.38：（安全级别 1, 2，3，4）

软件/固件的完整性应当成功通过核准的鉴别技术的验证。否则软件/固件加载测试应当失败。

送检单位需要提交的材料

VE10.38.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.38.01：检测人员核实软件/固件的完整性是否成功通过了核准的鉴别技术的验证。

AS10.39：（安全级别 1, 2，3，4）

在软件/固件的完整性没有通过核准的鉴别技术验证的情况下，软件/固件加载测试应当失败。

送检单位需要提交的材料

VE10.39.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.39.01：检测人员核实在软件/固件的完整性没有通过核准的鉴别技术验证的情况下，软件/固件加载测试是否失败。

AS10.40：（安全级别 1, 2，3，4）

如果软件/固件加载测试失败，则不应当使用加载的软件或固件。

送检单位需要提交的材料

VE10.40.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.40.01：检测人员核实在软件/固件加载测试失败的情况下，是否使用了加载的软件或固件。

6.11.3.5 手动输入条件测试

AS10.41：（安全级别 1, 2，3，4）

如果 SSP 或密钥分量手动输入至密码模块，由于手动操作失误会导致密钥输入错误，因此应当执行 AS10.42、AS10.43、AS10.44、AS10.45 手动密钥输入测试。

本条款不单独进行检测

AS10.42：（安全级别 1, 2，3，4）、AS10.43：（安全级别 1, 2，3，4）

SSP 或密钥分量应当使用错误检测码（EDC）或者应当输入两次。

送检单位需要提交的材料

VE10.42.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.42.01：检测人员核实 SSP 或密钥分量是否使用了错误检测码（EDC）或者输入了两次。

AS10.44：（安全级别 1, 2，3，4）

如果使用了 EDC，则 EDC 的长度应当至少为 16 比特。

送检单位需要提交的材料

VE10.44.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.44.01：检测人员核实 EDC 的长度是否至少为 16 比特。

AS10.45：（安全级别 1, 2，3，4）

如果 EDC 验证不符，或者两次输入不相等，那么测试应当失败。

送检单位需要提交的材料

VE10.45.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.45.01：检测人员核实如果 EDC 验证不符,测试是否失败。

TE10.45.02：检测人员核实如果两次输入不相等,测试是否失败。

6.11.3.6 旁路条件测试

AS10.46：（安全级别 1, 2，3，4）

如果密码模块实现了旁路能力，即模块可以提供不使用加密功能的服务（例如，在模块内传输明文），那么应当执行 AS10.47、AS10.48、AS10.49、AS10.50 旁路测试，以保证模块部件的单点失效不会导致不经意地输出明文。

本条款不单独进行检测

AS10.47：（安全级别 1, 2，3，4）

如果密码模块具有旁路开关，当开关在旁路服务和加密服务之间进行切换时，应当测试其提供密码处理服务的正确性。

送检单位需要提交的材料

VE10.47.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.47.01：检测人员核实当开关在旁路服务和加密服务之间进行切换时，其提供的密码处理服务是否正确。

AS10.48：（安全级别 1, 2，3，4）

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

送检单位需要提交的材料

VE10.48.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.48.01：检测人员核实当管理旁路服务和加密服务切换程序的机制（比如源/目的 IP 地址表）被修改时，其提供的密码处理服务是否正确。

AS10.49：（安全级别 1, 2，3，4）、 AS10.50：（安全级别 1, 2，3，4）

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，该模块应当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，也应当采用核准的完整性检测技术来产生新的完整性校验值。

送检单位需要提交的材料

VE10.49.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.49.01：检测人员核实每当修改管理信息之前，该模块是否采用了核准的完整性检测技术来验证管理信息的完整性。'

TE10.49.02：检测人员核实管理信息修改完毕后，该模块是否采用了核准的完整性检测技术来产生新的完整性校验值。

6.11.3.7 关键功能条件测试

AS10.51：（安全级别 1, 2，3，4）

其它一些关系到密码模块的安全操作的关键安全功能应当进行条件自测试。

送检单位需要提交的材料

VE10.51.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.51.01：检测人员核实其它关系到密码模块的安全操作的关键安全功能是否进行了条件自测试。

6.11.3.8 周期自测试

AS10.52：（安全级别 1, 2）

对于安全一级和二级，密码模块应当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：服务请求、复位、重启、上电循环。

送检单位需要提交的材料

VE10.52.01：送检单位提交的文档应描述密码模块周期自测试的说明。

所需的检测程序

TE10.52.01：检测人员核实操作员在有周期测试需求的情况下，是否能启动运行前自测试。

TE10.52.02：检测人员核实操作员在有周期测试需求的情况下，是否能启动条件自测试。

AS10.53：（安全级别 3, 4）

除了安全一级和二级的要求，模块应当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。

送检单位需要提交的材料

VE10.53.01：送检单位提交的文档应描述在已定义的时间周期内，如何自动重复执行运行前或条件自测试。

所需的检测程序

TE10.53.01：检测人员核实模块在已定义的时间周期内，是否自动重复执行运行前或条件自测试。

AS10.54：（安全级别 3, 4）

安全策略应当阐明时间周期以及在两次自测试周期之间可能导致模块运行中断的任何条件。例如，如果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。

送检单位需要提交的材料

VE10.54.01：送检单位提交的文档应描述密码算法自测试的说明。

所需的检测程序

TE10.54.01：检测人员核实文档中安全策略阐明的时间周期以及在两次自测试周期之间可能导致模块运行中断的任何条件，与实际是否相符。

6.12　生命周期保障

6.12.1　生命周期保障通用要求

AS11.01：（安全级别 1，2，3，4）

(生命周期保障)文档应当按照 GM/T 0028 A.2.11 中规定的要求编写。

送检单位需要提交的材料

VE11.01.01：送检单位应当提供生命周期保障文档。

所需的检测程序

TE11.01.01：检测人员应当检查送检单位提供的文档以确认是否符合GM/T 0028 A.2.11中规定的要求。

6.12.2　配置管理

AS11.02：（安全级别 1，2，3，4）

安全一级和二级的密码模块应当满足下列（AS11.2-AS11.4）安全要求。

注：本条款不单独进行检测。

AS11.03：（安全级别 1，2，3，4）

密码模块及其部件的开发过程以及相关文档都应当使用配置管理系统管理。

送检单位需要提交的材料

VE11.03.01：送检单位提供的文档应当对配置管理系统进行说明，该配置管理系统为密码模块及其部件的开发过程以及相关文档进行系统管理。

所需的检测程序

TE11.03.01：检测人员应当检查送检单位提供的文档以确认配置管理系统得以实现。

AS11.04：（安全级别 1，2，3，4）

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

送检单位需要提交的材料

VE11.04.01：送检单位提供的有关密码模块的文档应当包括所有配置项的配置列表。送检单位提供的文档应当对唯一确认配置项的方法进行说明。

VE11.04.02：送检单位提供的文档应当对用以唯一确认每个经验证的配置项版本的方法进行说明。

所需的检测程序

TE11.04.01：检测人员应当检查送检单位提供的包含配置项的配置列表。

TE11.04.02：检测人员应当检查送检单位提供的文档对用以唯一确认所有配置项的方法进行说明。

TE11.04.03：检测人员应当检查送检单位提供的文档对用以唯一确认每个经验证的配置项版本的方法进行说明。

TE11.04.04：检测人员应当检查送检单位提供的文档唯一地确认每个经验证的配置项版本。

AS11.05：（安全级别 1，2，3，4）

在经审验的密码模块的整个生命周期中，配置管理系统应当追踪并维护标识和版本的更改，或每个配置条目的修订。

送检单位需要提交的材料

VE11.05.01：送检单位应提供配置管理系统的说明文档，描述该系统是如何追踪并维护标识和版本的更改，或每个配置条目的更改。

所需的检测程序

TE11.05.01：检测人员应确认提交了VE11.05.01中要求的文档，并核实配置管理系统具有追踪并维护标识和版本的更改，或每个配置条目的更改的能力。

AS11.06：（安全级别 3，4）

(安全三级和四级)除了安全一级和二级要求，还应当使用自动的配置管理系统对配置条目进行管理。

送检单位需要提交的材料

VE11.06.01：送检单位应当详细说明配置管理系统如何提供一套自动化方法对配置条目进行管理。

所需的检测程序

TE11.06.01：检测人员应当检查送检单位提供的文档，该文档详细说明配置管理系统如何提供一套自动化方法，使用该方法时，只有经授权才能对密码模块的实现方法进行更改。

TE11.06.01：检测人员应当检查送检单位提供的文档，该文档详细说明配置管理系统如何提供一套自动化方法以支持密码模块的生成

6.12.3 设计

AS11.07：（安全级别 1，2，3，4）

密码模块应当设计成允许测试模块所提供的所有安全相关服务。

送检单位需要提交的材料

VE11.07.01：送检单位应在文档中设计密码模块所提供的所有安全相关服务允许被测试。

所需的检测程序

TE11.07.01：检测人员应当检查密码模块提供的所有安全相关服务已经设计成允许被测试。

6.12.4 有限状态模型

AS11.08：（安全级别 1，2，3，4）

密码模块的操作应当使用有限状态模型（或同等模型）来说明，该有限状态模型是用状态转移图、状态转移表和状态描述来表示的。

注：本条款作为 AS11.09 的一部分进行检测。

AS11.09：（安全级别 1，2，3，4）

有限状态模型应当足够详细，以证明密码模块符合本标准的所有要求。

所需的送检单位文档

VE11.09.01：送检单位应提供有限状态模型的描述。描述应包括对模块所有状态的定义和描述、以及对所有相关状态转移的描述。状态转移的描述应包括内部模块条件、引起状态转移的数据输入和控制输入，以及由状态转移导致的数据输出和状态输出。

TE11.09.02：送检单位文档应建立以下完整描述：

——数据输入接口；
——数据输出接口；
——控制输入接口；
——状态输出接口；
——密码管理员角色；
——用户角色；
——其他角色（如果可用）；
——密钥输入服务（如果可用）；
——显示状态服务；
——自测；
——其他认证的服务、运行、和功能（如果可用）；
——错误状态；
——旁路服务（如果可用）；
——维护接口（如果可用）；
——维护角色（如果提供维护接口）；
——密钥产生服务（如果可用）；
——密钥输出服务（如果可用）；
——空闲状态（如果可用）；
——非初始状态（如果可用）。

所需的检测程序

TE11.09.01：检测人员应确认送检单位提供了有限状态模块的说明。说明应包括对模块所有状态的识别和描述、以及对所有相关状态转移的描述。检测人员应确认状态转移说明包括内部模块条件、引起状态转移的数据输入和控制输入，以及由状态转移导致的数据输出和状态输出。

TE11.09.02：检测人员应确认有限状态图和说明与送检单位文档一致。送检单位文档说明下列项目：

——数据输入接口；
——数据输出接口；
——控制输入接口；
——状态输出接口；
——密码管理员角色；
——用户角色；
——其他角色（如果可用）；
——密钥输入服务（如果可用）；
——显示状态服务；
——自测；

——其他认证的服务、运行、和功能（如果可用）；
——错误状态；
——旁路服务（如果可用）；
——维护接口（如果可用）；
——维护角色（如果提供维护接口）；
——密钥产生服务（如果可用）；
——密钥输出服务（如果可用）；
——空闲状态（如果可用）；
——非初始状态（如果可用）；

TE11.09.03：检测人员应确认在有限状态表中定义的每个状态都在说明中定义和说明了。

TE11.09.04：检测人员应确认在说明中定义和声明的每个状态应在有限状态表中被定义。

TE11.09.05：检测人员应确认模块的运行与有限状态图和说明一致。

TE11.09.06：如果模块包括维护接口，那么检测人员应确认有限状态模型至少有一个维护状态说明。在有限状态模型说明中，所有的维护状态必须包括在有限状态转移表和描述中。

TE11.09.07：检测人员应检查密码模块的状态说明，以确定说明是否明确定义了不相关状态。检测人员应确认所有可能的数据和控制输入能够被区分为不相交的集合。

TE11.09.08：通过使模块进入各个主状态，检测人员可检查密码模块。对于每个有明显标识的状态，当模块处于此状态时，检测人员应观察确认标识。如果没有观察到期望的标识，或者同时观察到两个或更多这样的标识（表明模块同时处于多个状态），测试失败。

TE11.09.09：检测人员应确认存在从初始电源打开状态到每个非初始电源打开状态存在的一系列转移。

TE11.09.10：检测人员应确认存在从非电源关闭状态到模块电源关闭状态存在的一系列转移。

TE11.09.11：检测人员应确认定义了有限状态模型行为的所有可能数据和控制输入的结果。

AS11.10：（安全级别 1，2，3，4）

密码模块的 FSM 应当至少包括下列操作状态和错误状态：

- **电源开启/关闭状态：模块的一种状态，此时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）。**
- **普通初始化状态：在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）。**
- **CSP 输入状态：将 CSP 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**

它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。**

注：本条款作为 AS11.09 的一部分进行检测。

AS11.11：（安全级别 1，2，3，4）

从错误状态中恢复过来应当是可以做到的，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。

所需的送检单位文档

VE11.11.01：送检单位文档应描述对于不需要维护、服务、修理密码模块的错误状态是可恢复的。

所需的检测程序

TE11.11.01：从不需要维护、服务、修理的错误状态恢复，检测人员应确认密码模块能够被转移到一个可接受运行或初始化的状态。工作包括两部分：首先，检测人员应确认密码模块指示其进入错误状态；并且其次，确认模块在目标状态中运行正确。检测人员应报告是怎样核实其状态（例如，通过代码检测或通过测试模块）。

AS11.12：（安全级别 1，2，3，4）

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当作为一个独立的状态来描述。

注：本条款作为 AS11.09 的一部分进行检测。

AS11.13：（安全级别 1，2，3，4）

除密码主管以外，任何其它角色应当被禁止转换成密码主管状态。

所需的送检单位文档

VE11.13.01：送检单位文档应阐明除密码主管以外，任何其它角色被禁止转换成密码主管状态。

所需的检测程序

TE11.13.01：检测人员应尝试将用户转换成密码主管，如转换成功，则检测失败。

TE11.13.02：如有维护角色，检测人员应尝试将维护角色转换成密码主管，如转换成功，则检测失败。

6.12.5 开发

AS11.14：（安全级别 1，2，3，4）

安全一级的密码模块应当满足下列安全要求（AS11.15-AS11.21）。

注：本条款不单独进行检测。

AS11.15：（安全级别 1，2，3，4）

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它资源，都应当使用配置管理系统进行追踪。

所需的送检单位文档

VE11.15.01：送检单位应当提供包含在密码模块中的所有软件和固件组件名称的列表。

VE11.15.02：送检单位文档应提供配置项列表，标识了所有软件和固件的以下资源采用了配置管理系统进行追踪，包括：

——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；
——所有用于编译和链接源代码使其成为可运行形式的其它资源。

所需的检测程序

TE11.15.01：检测人员应核实配置项列表，确认 VE11.15.02 中列举到的资源采用了配置管理系统进行了追踪。

AS11.16：（安全级别 1，2，3，4）

如果密码模块包含软件或固件，那么源代码应当用注释进行标注，注释应该描述出软件或固件与模块设计的对应关系。

送检单位需要提交的材料

VE11.16.01：送检单位应当提供包含在密码模块中的所有软件和固件组件名称的列表。

VE11.16.02：送检单位应当提供包含在密码模块中的所有软件和固件组件的带有注释的源代码列表。

所需的检测程序

TE11.16.01：检测人员应当按照送检单位提供的目录来检查包含在密码模块中的所有软件和固件组件的源代码列表，并确认源代码用注释进行了标注，且注释描述出软件或固件与模块设计的对应关系。

AS11.17：（安全级别 1，2，3，4）

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

送检单位需要提交的材料

VE11.17.01：送检单位应当提供包含在密码模块中的硬件组件列表。

所需的检测程序

TE11.17.01：检测人员应当按照送检单位提供的目录来检查文档中包含硬件组件原理图和/或硬件描述语言（HDL）列表。

AS11.18：（安全级别 1，2，3，4）

如果密码模块包含硬件，HDL 代码应当用注释进行标注，注释应当描述出硬件与模块设计的对应关系。

送检单位需要提交的材料

VE11.18.01：送检单位应当提供包含在密码模块中的所有硬件组件的带有注释的HDL代码列表。

所需的检测程序

TE11.18.01：检测人员应当按照送检单位提供的目录来检查包含在密码模块中的所有硬件组件的HDL代码列表，并确认HDL代码用注释进行了标注，且注释描述出硬件与模块设计的对应关系。

AS11.19：（安全级别 1，2，3，4）

（对于软件和固件密码模块以及混合模块中的软件或固件部件）第 7.5 节和第 7.10 节中规定的完整性和验证技术机制的结果，应当在模块开发过程中，由供应商计算并集成到软件或固件模块内。

送检单位需要提交的材料

VE11.19.01：送检单位应当提供文档声明第7.5节和第7.10节中规定的完整性和验证技术机制的结果，在模块开发过程中，已计算并集成到软件或固件模块内。

VE11.19.02：送检单位应提供集成了完整性和验证技术机制的结果的软件或固件源代码。

所需的检测程序

TE11.19.01：检测人员应当审查软件或固件源代码，以确认进行了VE11.19.01提供文档中的声明。

AS11.20：（安全级别 1，2，3，4）

（对于软件和固件密码模块以及混合模块中的软件或固件部件）密码模块文档应当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。

送检单位需要提交的材料

VE11.20.01：送检单位应当提供文档描述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。

所需的检测程序

TE11.20.01：检测人员应当检查VE11.20.01中所需的信息。

AS11.21：（安全级别 1，2，3，4）

（对于软件和固件密码模块以及混合模块中的软件或固件部件）密码模块应当使用工业等级的开发工具（例如，编译器）进行开发。

送检单位需要提交的材料

VE11.21.01：送检单位应当提供所采用编译器的说明及版本。

所需的检测程序

TE11.21.01：检测人员应当检查编译器及版本是否为工业等级。

AS11.22：（安全级别 2，3，4）

除了安全一级的要求，安全二级和三级的密码模块还应当满足下列安全要求（AS11.23-AS11.26）。

注：本条款不单独进行检测。

AS11.23：（安全级别 2，3，4）

密码模块内所有软件或固件应当[11.23]采用高级非私有语言实现。

注：本条款和 AS11.24 一同进行测试。

AS11.24：（安全级别 2，3，4）

如果低级语言对模块的性能有重要作用或在高级语言无法使用的情况下，应当在使用低级语言（例如，汇编语言或微指令）时给出根据。

送检单位需要提交的材料

VE11.24.01：送检单位应当确认所有未使用高级语言的软件和固件组件，并对固件使用低级语言的原因提供合理的解释或说明。该说明应当指出此情况是由于高级语言不可用或提高软件及固件性能所需。

所需的检测程序

TE11.24.01：检测人员应当检查所有软件和/或固件组件的源代码以确认哪些使用低级语言。检测人员应当确认只有当 VE11.24.01 中的情况出现时，软件和/或固件组件才使用低级语言。

AS11.25：（安全级别 2，3，4）

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

送检单位需要提交的材料

VE11.25.01：送检单位应当提供使用高级规范语言实现的硬件组件文档。

所需的检测程序

TE11.25.01：检测人员应当检查送检单位提供的文档，该文档包括 VE11.25.01 中指定的信息

AS11.26：（安全级别 2，3，4）

软件密码模块的设计和实现应当避免使用对模块功能和运行不必要的代码、参数或符号。

送检单位需要提交的材料

VE11.26.01：送检单位如果在软件密码模块中使用了对模块功能和运行不必要的代码、参数或符号，应在文档中声明，并阐述原因。

VE11.26.02：送检单位应提供使用了对模块功能和运行不必要的代码、参数或符号的源代码列表和源代码。

所需的检测程序

TE11.26.01：检测人员应当检查送检单位提供的文档是否声明使用了对模块功能和运行不必

要的代码、参数或符号，如果有，审查其原因和必要性。

TE11.26.02：检测人员应审查源代码，核实对模块功能和运行不必要的代码、参数或符号的必要性，及对模块功能和运行的影响。

AS11.27：（安全级别 4）

除了安全一级、二级和三级的要求，安全四级的密码模块还应当满足下列安全要求（AS11.28）。

注：本条款不单独进行检测。

AS11.28：（安全级别 4）

对于每个密码模块的硬件和软件部件，文档应当具有注释，以阐明：(1)进入模块部件、功能或程序时，为确保执行正确所需要的前置条件；(2)模块部件、功能或程序完成时，预期值为真的后置条件。

注：该前提条件和后续条件可以用任意符号说明，该符号详细并明确解释了密码模块组件、功能或程序的行为。

送检单位需要提交的材料

VE11.28.01：所有硬件、软件和固件组件的源代码列表应当包含AS11.28要求的注释、前提条件及后续条件。

所需的检测程序

TE11.28.01：检测人员应当检查源代码列表，该列表包含 VE11.28.01 中指定的信息。

6.12.6 供应商测试

AS11.29：（安全级别 1，2，3，4）

对于安全一级和二级，文档应当阐明在密码模块上执行的功能测试。

送检单位需要提交的材料

VE11.29.01：送检单位应在文档中列举出密码模块所有的安全功能，包括但不限于以下安全功能：

——身份鉴别；
——访问控制；
——密码运算；
——密钥管理；

——文件管理；
——物理安全；
——生命周期管理；
——中间件安全。

VE11.29.02：送检单位应在测试文档中描述针对每个安全功能所进行的功能测试及测试深度。

VE11.29.03：送检单位应提供针对每个安全功能的功能测试程序。

所需的检测程序

TE11.29.01：检测人员应当检查测试文档中针对每个安全功能进行了覆盖测试，并检查测试深度是否充分。

TE11.29.02：检测人员应当采用送检单位提供的测试程序和自己开发的测试程序，验证每个安全功能是否存在缺陷和漏洞。

AS11.30：（安全级别 1，2，3，4）

（对于安全一级和二级）对于软件或固件密码模块以及混合模块中的软件或固件部件，供应商应当使用通用的自动安全诊断工具（例如，检查缓冲区溢出等）。

送检单位需要提交的材料

VE11.30.01：送检单位应在文档中列举出针对软件或固件密码模块以及混合模块中的软件或固件部件采用的自动安全诊断工具，包括静态和动态分析工具。

所需的检测程序

TE11.30.01：检测人员应当检查和确认采用的自动诊断工具是否可以满足要求，如满足要求，进行测试验证，检查是否存在缓冲区溢出等缺陷。

AS11.31：（安全级别 3，4）

（安全三级和四级）除了安全一级和二级中的要求，文档还应当阐明在密码模块上执行的底层测试的过程与结果。

送检单位需要提交的材料

VE11.31.01：送检单位应在文档中列举出针对底层设计所进行的测试过程与结果。

所需的检测程序

TE11.31.01：检测人员应当检查和验证底层测试的过程充分、结果准确。

6.12.7 配送与操作

AS11.32：（安全级别 1，2，3，4）

对于安全一级，文档应当阐明密码模块的安全安装、初始化与启动的流程。

送检单位需要提交的材料

VE11.32.01：送检单位提供的文档应当对密码模块的安全安装、初始化以及启动所需的步骤进行描述。

所需的检测程序

TE11.32.01：检测人员应当检查送检单位提供的文档，该文档包括安全配置的安装、初始化以及启动流程。

TE11.32.02：检测人员应当执行密码模块的安全安装、初始化以及启动流程并验证它们的正确性。

AS11.33：（安全级别 2，3，4）

（安全二级和三级）除了安全一级的要求之外，文档还应当阐明在分发、安装和初始化密码模块的版本给已授权的操作员时，维持模块安全性所需的步骤。

送检单位需要提交的材料

VE11.33.01：交付文档应当描述在将密码模块交付给授权操作员的过程中用以维持安全性所需的步骤。

所需的检测程序

TE11.33.01：检测人员应当检查送检单位提供的文档，该文档用以说明在将密码模块交付给授权操作员的过程中用以维持安全性所需步骤的正确性。

AS11.34：（安全级别 4）

（AS11.33 中提到的）这些步骤应当详细指出在配送、安装和初始化密码模块给已授权操作员的过程中，如何检测模块是否被拆卸过。

送检单位需要提交的材料

VE11.34.01：交付文档应当描述在将密码模块交付给授权操作员的过程中用以检测模块是否被拆卸过的方法。

所需的检测程序

TE11.34.01：检测人员应当检查送检单位提供的文档，该文档用以说明在将密码模块交付给授权操作员的过程中用以检测模块是否被拆卸过的方法的正确性。

TE11.34.02：检测人员应当尝试拆卸检测模块，然后采用送检单位文档中的检测方法检测是否被拆卸过，如可以检测出，则检测方法有效。

AS11.35：（安全级别 4）

（安全四级）除了安全二级和三级中的要求之外，还应当要求已授权的操作员使用供应商提供的鉴别数据对模块进行鉴别。

送检单位需要提交的材料

VE11.35.01：交付文档应当描述在将密码模块交付给授权操作员的过程中如何进行初始鉴别。

所需的检测程序

TE11.35.01：检测人员应当检查送检单位提供的文档中是否提供了初始鉴别方法。

TE11.35.02：检测人员应当尝试采用送检单位文档中提供的初始鉴别方法进行签名，检测是否可以通过鉴别。

6.12.8 生命终止

AS11.36：（安全级别 1，2，3，4）

对于安全一级和二级，文档应当阐明安全处理密码模块的流程。处理模块是指从模块中去除敏感信息（例如，SSP、用户数据等）的过程，使得模块可以分发给其它操作员或被处置。

送检单位需要提交的材料

VE11.36.01：送检单位应提供生命周期管理文档，描述安全处理密码模块的流程。

所需的检测程序

TE11.36.01：检测人员应当检查送检单位提供的文档中是否描述了安全处理密码模块的流程。

TE11.36.02：检测人员应采用VE11.36.01中描述的安全处理密码模块的流程，尝试从模块中去除敏感信息，并检查敏感信息是否去除完全。

AS11.37：（安全级别 3，4）

（安全三级和四级）除了安全一级和二级的要求，文档应当阐明安全销毁模块所需的流程。

送检单位需要提交的材料

VE11.37.01：送检单位应提供生命周期管理文档，描述安全销毁密码模块的流程。

所需的检测程序

TE11.37.01：检测人员应当检查送检单位提供的文档中是否描述了安全销毁密码模块的流程。

TE11.37.02：检测人员应采用VE11.37.01中描述的安全销毁密码模块的流程，尝试销毁密码模块，并检查是否还可用。

6.12.9 指南文档

AS11.38：（安全级别 1，2，3，4）

管理员指南应当阐明：

——密码主管和/或其它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。

——保持独立的操作员鉴别机制在功能上独立所需要的措施。

——如何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。

送检单位需要提交的材料

VE11.38.01：送检单位提供的管理员文档应当包括AS11.38中列出的信息。

VE11.38.02：对于密码管理员而言，未经过专有指导仅参照管理员指南，就可以使用密码模块。

所需的检测程序

TE11.38.01：检测人员应当检查该文档包含VE11.38.01和VE11.38.02中指定的信息。

AS11.39：（安全级别 1，2，3，4）

非管理员指南应当阐明：

——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。

送检单位需要提交的材料

VE11.39.01：送检单位提供的文档应当包含AS11.39中列出的信息。

VE11.39.02：对于密码管理员而言，未经过专有指导仅参照非管理员指南（用户指南），就可以使用密码模块。

所需的检测程序

TE11.39.01：检测人员应当检查该文档包含VE11.39和VE11.39.02中指定的信息。

6.13 对其它攻击的缓解

AS12.01：（安全级别 1，2，3，4）

文档应当按照 GM/T 0028 A.2.12 中规定的要求编写。

送检单位需要提交的材料

VE12.01.01：送检单位应当提供对其它攻击缓解的文档。

所需的检测程序

TE12.01.01：检测人员应当检查送检单位提供的文档以确认是否符合GM/T 0028 A.2.12中规定的要求。

AS12.02：（安全级别 1，2，3，4）

（安全一级、二级和三级）如果将密码模块设计为可缓解一种或多种在本标准未定义的特定攻击，那么模块的相关文档应当列举出模块能够缓解的攻击。

应对用于缓解攻击的安全机制进行验证，测试其是否存在且是否起作用。

送检单位需要提交的材料

VE12.02.01：送检单位应当列举出设计为可缓解一种或多种在本标准未定义的特定攻击。

所需的检测程序

TE12.02.01：检测人员应对用于缓解攻击的安全机制进行验证，测试其是否存在且是否起作用。

AS12.03：（安全级别 1，2，3，4）

（安全四级）除了安全一级、二级和三级的安全要求，安全四级的密码模块还应当满足下列安全要求（AS12.04）。

注：本条款不单独进行检测。

AS12.04：（安全级别 4）

如果声明了能够缓解本标准未定义的特定攻击，则文档应当详细说明缓解攻击的方法以及测试该缓解技术有效性的方法。

送检单位需要提交的材料

VE12.04.01：送检单位应当列举出能够缓解本标准未定义的特定攻击。

VE12.04.01：送检单位文档应当详细说明缓解攻击的方法以及测试该缓解技术有效性的方

法。

所需的检测程序

TE12.04.01：检测人员应对用于缓解攻击的安全机制进行验证，测试其是否存在且是否起作用。

附录 A

（资料性附录）

安全等级对应表

A.1 通用要求

表 A.1

	安全一级	安全二级	安全三级	安全四级
AS01.01	√	√	√	√
AS01.02	√	√	√	√
AS01.03	√	√	√	√
AS01.04	√	√	√	√

A.2 密码模块的规格

表 A.2

	安全一级	安全二级	安全三级	安全四级
AS02.01	√	√	√	√
AS02.02	√	√	√	√
AS02.03	√	√	√	√
AS02.04	√	√	√	√
AS02.05	√	√	√	√
AS02.06	√	√	√	√
AS02.07	√	√	√	√
AS02.08	√	√	√	√
AS02.09	√	√	√	√
AS02.10	√	√	√	√
AS02.11	√	√	√	√
AS02.12	√	√	√	√
AS02.13	√	√	√	√
AS02.14	√	√	√	√
AS02.15	√	√	√	√
AS02.16	√	√	√	√
AS02.17	√	√	√	√
AS02.18	√	√	√	√
AS02.19	√	√	√	√
AS02.20	√	√	√	√
AS02.21	√	√	√	√
AS02.22	√	√	√	√
AS02.23	√	√	√	√
AS02.24	√	√	√	√
AS02.25	√	√	√	√

表 A.2 （续）

AS02.26	√	√	√	√
AS02.27	√	√	√	√
AS02.28	√	√	√	√
AS02.29	√	√	√	√
AS02.30	√	√	√	√
AS02.31	√	√	√	√
AS02.32	√	√	√	√

A.3 密码模块接口

表 A.3

	安全一级	**安全二级**	**安全三级**	**安全四级**
AS03.01	√	√	√	√
AS03.02	√	√	√	√
AS03.03	√	√	√	√
AS03.04	√	√	√	√
AS03.05	√	√	√	√
AS03.06	√	√	√	√
AS03.07	√	√	√	√
AS03.08	√	√	√	√
AS03.09	√	√	√	√
AS03.10	√	√	√	√
AS03.11	√	√	√	√
AS03.12	√	√	√	√
AS03.13	√	√	√	√
AS03.14	√	√	√	√
AS03.15	√	√	√	√
AS03.16			√	
AS03.17			√	
AS03.18			√	
AS03.19			√	
AS03.20			√	
AS03.21			√	
AS03.22				√

A.4 角色、服务和鉴别

表 A.4

	安全一级	**安全二级**	**安全三级**	**安全四级**
AS04.01	√	√	√	√
AS04.02	√	√	√	√
AS04.03	√	√	√	√

AS04.04	√	√	√	√

表 A.4 （续）

AS04.05	√	√	√	√
AS04.06	√	√	√	√
AS04.07	√	√	√	√
AS04.08	√	√	√	√
AS04.09	√	√	√	√
AS04.10	√	√	√	√
AS04.11	√	√	√	√
AS04.12	√	√	√	√
AS04.13	√	√	√	√
AS04.14	√	√	√	√
AS04.15	√	√	√	√
AS04.16	√	√	√	√
AS04.17	√	√	√	√
AS04.18	√	√	√	√
AS04.19	√	√	√	√
AS04.20	√	√	√	√
AS04.21	√	√	√	√
AS04.22	√	√	√	√
AS04.23	√	√	√	√
AS04.24	√	√	√	√
AS04.25	√	√	√	√
AS04.26	√	√	√	√
AS04.27	√	√	√	√
AS04.28	√	√	√	√
AS04.29	√	√	√	√
AS04.30	√	√	√	√
AS04.31	√	√	√	√
AS04.32	√	√	√	√
AS04.33	√	√	√	√
AS04.34	√	√	√	√
AS04.35	√	√	√	√
AS04.36	√	√	√	√
AS04.37	√	√	√	√
AS04.38	√	√	√	√
AS04.39	√	√	√	√
AS04.40	√	√	√	√
AS04.41	√	√	√	√
AS04.42	√	√	√	√
AS04.43	√	√	√	√
AS04.44	√	√	√	√
AS04.45	√	√	√	√

AS04.46	√	√	√	√

表 A.4 （续）

AS04.47	√	√	√	√
AS04.48	√			
AS04.49	√			
AS04.50	√			
AS04.51	√			
AS04.52	√			
AS04.53		√		
AS04.54		√		
AS04.55		√		
AS04.56	√			
AS04.57		√		
AS04.58			√	
AS04.59				√

A.5 软件/固件安全

表 A.5

	安全一级	**安全二级**	**安全三级**	**安全四级**
AS05.01	√	√	√	√
AS05.02	√	√	√	√
AS05.03	√	√	√	√
AS05.04	√	√	√	√
AS05.05	√	√	√	√
AS05.06	√	√	√	√
AS05.07	√	√	√	√
AS05.08	√	√	√	√
AS05.09	√	√	√	√
AS05.10	√	√	√	√
AS05.11	√	√	√	√
AS05.12		√	√	√
AS05.13		√	√	√
AS05.14		√	√	√
AS05.15		√	√	√
AS05.16			√	√
AS05.17			√	√
AS05.18			√	√
AS05.19			√	√
AS05.20			√	√
AS05.21			√	√

A.6 运行环境

表 A.6

	安全一级	安全二级	安全三级	安全四级
AS06.01	√	√	√	√
AS06.02	√	√	√	√
AS06.03	√	√	√	√
AS06.04	√	√	√	√
AS06.05	√	√	√	√
AS06.06	√	√	√	√
AS06.07	√	√	√	√
AS06.08	√	√	√	√
AS06.09		√	√	√
AS06.10		√	√	√
AS06.11		√	√	√
AS06.12		√	√	√
AS06.13		√	√	√
AS06.14		√	√	√
AS06.15		√	√	√
AS06.16		√	√	√
AS06.17		√	√	√
AS06.18		√	√	√
AS06.19		√	√	√
AS06.20		√	√	√
AS06.21		√	√	√
AS06.22		√	√	√
AS06.23		√	√	√
AS06.24		√	√	√
AS06.25		√	√	√
AS06.26		√	√	√
AS06.27		√	√	√
AS06.28		√	√	√
AS06.29		√	√	√

A.7 物理安全

表 A.7

	安全一级	安全二级	安全三级	安全四级
AS07.01	√	√	√	√
AS07.02	√	√	√	√
AS07.03	√	√	√	√
AS07.04	√	√	√	√
AS07.05	√	√	√	√
AS07.06	√	√	√	√

表 A.7 （续）

AS07.07	√	√	√	√
AS07.08	√	√	√	√
AS07.09	√	√	√	√
AS07.10	√	√	√	√
AS07.11	√	√	√	√
AS07.12	√	√	√	√
AS07.13	√	√	√	√
AS07.14	√	√	√	√
AS07.15	√	√	√	√
AS07.16	√	√	√	√
AS07.17		√	√	√
AS07.18		√	√	√
AS07.19		√	√	√
AS07.20		√	√	√
AS07.21			√	√
AS07.22			√	√
AS07.23			√	√
AS07.24			√	√
AS07.25			√	√
AS07.26			√	√
AS07.27			√	√
AS07.28			√	√
AS07.29				√
AS07.30				√
AS07.31				√
AS07.32				√
AS07.33				√
AS07.34		√	√	√
AS07.35		√	√	√
AS07.36			√	√
AS07.37			√	√
AS07.38			√	√
AS07.39				√
AS07.40				√
AS07.41				√
AS07.42				√
AS07.43	√	√	√	√
AS07.44		√	√	√
AS07.45		√	√	√
AS07.46		√	√	√
AS07.47		√	√	√

AS07.48		√	√	√

表 A.7 （续）

AS07.49			√	√
AS07.50			√	√
AS07.51			√	√
AS07.52				√
AS07.53				√
AS07.54				√
AS07.55				√
AS07.56				√
AS07.57				√
AS07.58				√
AS07.59				√
AS07.60	√	√	√	√
AS07.61		√	√	√
AS07.62		√	√	√
AS07.63		√	√	√
AS07.64			√	√
AS07.65			√	√
AS07.66				√
AS07.67				√
AS07.68				√
AS07.69				√
AS07.70				√
AS07.71				√
AS07.72				√
AS07.73			√	√
AS07.74				√
AS07.75			√	√
AS07.76			√	√
AS07.77			√	√
AS07.78			√	√
AS07.79			√	√
AS07.80			√	√
AS07.81			√	√
AS07.82			√	√
AS07.83			√	√
AS07.84			√	√
AS07.85			√	√

A.8 非入侵安全

表 A.8

	安全一级	安全二级	安全三级	安全四级

AS08.01	√	√	√	√

表 A.8 （续）

AS08.02	√	√	√	√
AS08.03	√	√	√	√
AS08.04	√	√		
AS08.05	√	√	√	√
AS08.06			√	
AS08.07				√

A.9 敏感安全参数管理

表 A.9

	安全一级	安全二级	安全三级	安全四级
AS09.01	√	√	√	√
AS09.02	√	√	√	√
AS09.03	√	√	√	√
AS09.04	√	√	√	√
AS09.05	√	√	√	√
AS09.06	√	√	√	√
AS09.07	√	√	√	√
AS09.08	√	√	√	√
AS09.09	√	√	√	√
AS09.10	√	√	√	√
AS09.11	√	√	√	√
AS09.12	√	√	√	√
AS09.13	√	√	√	√
AS09.14	√	√	√	√
AS09.15	√	√	√	√
AS09.16	√	√	√	√
AS09.17	√	√	√	√
AS09.18	√	√	√	√
AS09.19	√	√		
AS09.20			√	
AS09.21			√	
AS09.22			√	
AS09.23			√	
AS09.24				√
AS09.25	√	√	√	√
AS09.26	√	√	√	√
AS09.27	√	√	√	√
AS09.28	√	√	√	√
AS09.29	√	√	√	√

AS09.30		√	√	
AS09.31		√	√	
AS09.32		√	√	

表 A.9 （续）

AS09.33		√	√	
AS09.34				√
AS09.35				√
AS09.36				√
AS09.37				√

A.10 自测试

表 A.10

	安全一级	安全二级	安全三级	安全四级
AS10.01	√	√	√	√
AS10.02	√	√	√	√
AS10.03	√	√	√	√
AS10.04	√	√	√	√
AS10.05	√	√	√	√
AS10.06	√	√	√	√
AS10.07	√	√	√	√
AS10.08	√	√	√	√
AS10.09	√	√	√	√
AS10.10	√	√	√	√
AS10.11	√	√	√	√
AS10.12			√	√
AS10.13			√	√
AS10.14	√	√	√	√
AS10.15	√	√	√	√
AS10.16	√	√	√	√
AS10.17	√	√	√	√
AS10.18	√	√	√	√
AS10.19	√	√	√	√
AS10.20	√	√	√	√
AS10.21	√	√	√	√
AS10.22	√	√	√	√
AS10.23	√	√	√	√
AS10.24	√	√	√	√
AS10.25	√	√	√	√
AS10.26	√	√	√	√
AS10.27	√	√	√	√
AS10.28	√	√	√	√
AS10.29	√	√	√	√
AS10.30	√	√	√	√

AS10.31	√	√	√	√
AS10.32	√	√	√	√
AS10.33	√	√	√	√

表 A.9 （续）

AS10.34	√	√	√	√
AS10.35	√	√	√	√
AS10.36	√	√	√	√
AS10.37	√	√	√	√
AS10.38	√	√	√	√
AS10.39	√	√	√	√
AS10.40	√	√	√	√
AS10.41	√	√	√	√
AS10.42	√	√	√	√
AS10.43	√	√	√	√
AS10.44	√	√	√	√
AS10.45	√	√	√	√
AS10.46	√	√	√	√
AS10.47	√	√	√	√
AS10.48	√	√	√	√
AS10.49	√	√	√	√
AS10.50	√	√	√	√
AS10.51	√	√	√	√
AS10.52	√	√		
AS10.53			√	√
AS10.54			√	√

A.11 生命周期保障

表 A.11

	安全一级	**安全二级**	**安全三级**	**安全四级**
AS11.01	√	√	√	√
AS11.02	√	√	√	√
AS11.03	√	√	√	√
AS11.04	√	√	√	√
AS11.05	√	√	√	√
AS11.06			√	√
AS11.07	√	√	√	√
AS11.08	√	√	√	√
AS11.09	√	√	√	√
AS11.10	√	√	√	√
AS11.11	√	√	√	√
AS11.12	√	√	√	√

AS11.13	√	√	√	√
AS11.14	√	√	√	√
AS11.15	√	√	√	√
AS11.16	√	√	√	√
AS11.17	√	√	√	√

表 A.11 （续）

AS11.18	√	√	√	√
AS11.19	√	√	√	√
AS11.20	√	√	√	√
AS11.21	√	√	√	√
AS11.22		√	√	√
AS11.23		√	√	√
AS11.24		√	√	√
AS11.25		√	√	√
AS11.26		√	√	√
AS11.27				√
AS11.28				√
AS11.29	√	√	√	√
AS11.30	√	√	√	√
AS11.31			√	√
AS11.32	√	√	√	√
AS11.33		√	√	√
AS11.34				√
AS11.35				√
AS11.36	√	√	√	√
AS11.37			√	√
AS11.38	√	√	√	√
AS11.39	√	√	√	√

A.12 对其它攻击的缓解

表 A.12

	安全一级	**安全二级**	**安全三级**	**安全四级**
AS12.01	√	√	√	√
AS12.02	√	√	√	√
AS12.03	√	√	√	√
AS12.04				√