ICS 35.040
L 80
备案号：49738—2015

GM

中华人民共和国密码行业标准

GM/T 0039—2015

密码模块安全检测要求

Security test requirements for cryptographic modules

2015-04-01 发布　　2015-04-01 实施

国家密码管理局　　发布

中华人民共和国密码
行业标准
密码模块安全检测要求
GM/T 0039—2015
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 7 字数 198 千字
2015年6月第一版 2015年6月第一次印刷
*
书号:155066·2-28769 定价 90.00 元

GM/T 0039-2015

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用重新起草法参考 ISO/IEC 24759:2014《信息技术　安全技术　密码模块检测要求》编制，与 ISO/IEC 24759:2014 的一致性程度为非等效。

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。

本标准的主要起草单位：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。

本标准的主要起草人：汪雪林、李大为、邓开勇、陈国、陈保儒、张一飞、胡伯良、朱鹏飞、罗鹏、张众、雷银花、莫凡、林春、蒋红宇、谭武征、张万涛、高能。

密码模块安全检测要求

1 范围

本标准依据 GM/T 0028—2014 的要求，规定了密码模块的一系列检测规程、检测方法和对应的送检文档要求。

本标准适用于密码模块的检测。

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 0028—2014 密码模块安全技术要求

GM/Z 4001 密码术语

3 术语和定义

GM/T 0028—2014 和 GM/Z 4001 所界定的术语和定义适用于本文件。

4 缩略语

下列缩略语适用于本文件。

API 应用程序接口(Application Program Interface)

CBC 密码分组链接(Cipher Block Chaining)

CSP 关键安全参数(Critical Security Parameter)

EDC 错误检测码(Error Detection Code)

EFP 环境失效保护(Environmental Failure Protection)

EFT 环境失效测试(Environmental Failure Testing)

FSM 有限状态模型(Finite State Model)

HDL 硬件描述语言(Hardware Description Language)

IC 集成电路(Integrated Circuit)

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

PROM 可编程只读存储器(Programmable Read-Only Memory)

PSP 公开安全参数(Public Security Parameter)

RAM 随机存取存储器(Random Access Memory)

RBG 随机比特生成器(Random Bit Generator)

ROM 只读存储器(Read-Only Memory)

SSP 敏感安全参数(Sensitive Security Parameter)

5 文档结构

5.1 概述

本标准第6章详细说明了一系列供检测机构使用的规程、方法以及对送检单位提交给检测机构文档的要求。第6章包括18条，其中6.1为通用要求，6.2～6.18对应于GM/T 0028—2014中的11个安全域和附录A～附录F。

5.2 条款和安全要求

在第6章的每条中，GM/T 0028—2014中的相应安全要求被分成了一系列条款集，全部内容直接引用GM/T 0028—2014，用宋体加粗字体表示。

各条款的格式为：

AY＜要求编号＞.＜条款序列编号＞

其中，“AY”表示安全要求，“要求编号”是指GM/T 0028—2014中指定的相应域的编号（即，对应1～12和A～F），“条款序列编号”是条内的序列标示符。在条款的编号后面，该条款所对应的安全等级列在圆括号内。

每个条款之后是对所需的送检文档的要求。这些要求描述了送检单位的文档类型或详细材料，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：

CY＜要求编号＞.＜条款序列编号＞.＜序列编号＞

其中，“CY”表示对送检单位提交文档的要求，这里的“要求编号”和“条款序列编号”与对应安全要求中的“要求编号”和“条款序列编号”相同，“序列编号”是对送检单位要求条款内的序列标识符。

所需的送检文档之后是对所需的检测规程的要求。这些要求指导检测人员在检测密码模块的某个给定条款时，他/她应该如何执行检测。

这些要求的格式如下：

JY＜要求编号＞.＜条款序列编号＞.＜序列编号＞

其中，“JY”表示对检测规程和方法的要求，这里的“要求编号”和“条款序列编号”与对应安全要求中的“要求编号”和“条款序列编号”相同，“序列编号”是对检测人员要求条款内的序列标识符。

5.3 引用条款说明

为了语句的连贯，本标准对直接引用GM/T 0028—2014的某些条款，增加了补充语句，这些语句用大括号“{”和“}”括起来，并且用斜体字宋体加粗表示。

此外，本标准所需的送检文档的要求和所需的检测规程的要求中采用的“应”与直接引用GM/T 0028—2014的条款中的“应当”含义相同。

6 安全检测要求

6.1 通用要求

注：本条声明了以满足第6章其他条的条款的通用要求。

AY01.01：（安全级别1,2,3,4）

本条规定了符合本标准的密码模块应当满足的安全要求。

注：本条款不单独进行检测。

AY01.02:(安全级别 1,2,3,4)

密码模块应当按照各个域的要求进行测试。

注 1:检测机构可以以下面一个或多个方式对密码模块的安全性进行测试:

a) 检测人员使用检测机构的设备进行测试。

b) 检测人员使用送检单位的设备进行测试。

c) 检测人员监督送检单位使用送检单位的设备进行测试。在此种情况下,检测机构需:

1) 解释己方不能进行测试的理由;

2) 制定所需的测试计划和测试任务;

3) 直接观察测试的执行情况。

如果任一条款的测试不成功,则此条款不通过。

注 2:本条款不单独进行检测。

AY01.03:(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。

AY01.04:(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。

注:本条款不单独进行检测。

6.2 密码模块规格

6.2.1 密码模块规格通用要求

AY02.01:(安全级别 1,2,3,4)

密码模块应当是硬件、软件、固件,或其中组合的集合,该集合至少使用一个核准的密码算法、安全功能或过程实现一项密码服务,并且包含在明确的密码边界内。

注 1:本条款不单独进行检测。

注 2:GM/T 0028—2014 的附录 C 列出了核准的安全功能。

AY02.02:(安全级别 1,2,3,4)

***{密码模块规格}*文档应当按照*{GM/T 0028—2014 附录}*A.2.2 中规定的要求编写。**

注:本条款作为 AYA.01 的一部分进行检测。

6.2.2 密码模块类型

AY02.03:(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。

所需的送检文档

CY02.03.01:送检单位的文档中应描述密码模块类型,并解释选择这一类型的依据。

CY02.03.02:送检单位应提供密码模块的规格,以标识所有密码模块的硬件、软件和/或固件部件。

所需的检测规程

JY02.03.01:检测人员应核实送检单位的文档中标识了 AY02.03 中定义的一种模块类型。

JY02.03.02:检测人员应通过审查送检单位提供的规格文档,并识别所有硬件、软件和/或固件部件,核实该密码模块与 AY02.03 中定义的密码模块类型一致。

AY02.04:(安全级别 1,2,3,4)

对于硬件和固件模块,{*GM/T 0028—2014*}7.7 中规定的物理安全和{*GM/T 0028—2014*}7.8 中规定的非入侵式安全要求应当适用。

注:本条款不单独进行检测。

AY02.05:(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—2014*}7.5 中规定的软件/固件安全和{*GM/T 0028—2014*}7.6 中规定的运行环境中的所有适用要求。

注:本条款不单独进行检测。

AY02.06:(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—2014*}7.7 中规定的物理安全和{*GM/T 0028—2014*}7.8 中规定的非入侵式安全中的所有适用要求。**

注:本条款不单独进行检测。

6.2.3 密码边界

6.2.3.1 密码边界通用要求

AY02.07:(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。

所需的送检文档

CY02.07.01:送检单位的文档中应详细说明密码边界内的所有部件。

所需的检测规程

JY02.07.01:检测人员应通过文档审查和模块检查核实所有部件在密码边界内。

JY02.07.02:检测人员应通过文档审查和模块检查核实没有未标识的部件在密码边界内。

AY02.08:(安全级别 1,2,3,4)

标准{*GM/T 0028—2014*}的要求应当适用于模块密码边界内的所有算法、安全功能、过程和部件。

注:本条款不单独进行检测。

AY02.09:(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、过程和部件(即标准{*GM/T 0028—2014*}范围内与安全相关的)。

所需的送检文档

CY02.09.01:送检单位应提供密码边界内所有与安全相关的算法、安全功能、过程和部件的清单,安全功能包括但不限于:

——分组密码;

——流密码;

——非对称密码算法和技术;

——消息鉴别码;

——杂凑函数;

——实体鉴别;

——密钥管理;

——随机比特生成器。

所需的检测规程

JY02.09.01:检测人员应核实送检单位的文档中明确标识和列出密码边界内所有与安全相关的算法、安全功能、过程和部件。

AY02.10:(安全级别 1,2,3,4)

用于核准的工作模式的非安全相关的算法、安全功能、过程和部件的实现应当不干扰或破坏密码模块核准的工作模式的运行。

所需的送检文档

CY02.10.01:送检单位的文档中应列出用于核准的工作模式的非安全相关的算法、安全功能、过程和部件,并且证明它们不干扰或破坏密码模块核准的工作模式的运行。

所需的检测规程

JY02.10.01:检测人员应通过文档审查和模块检查核实非安全相关的算法、安全功能、过程和部件的实现不干扰或破坏密码模块核准的工作模式的运行。

JY02.10.02:检测人员应核实送检单位提供的不干扰或破坏的任何理由的正确性。举证责任在送检单位,如果有任何不确定性或模糊性,检测人员应要求送检单位出示所需的进一步信息。

AY02.11:(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。

所需的送检文档

CY02.11.01:送检单位的文档中应提供密码模块的名称。

所需的检测规程

JY02.11.01:检测人员应核实送检单位提供的密码模块的名称与密码边界内的部件构成一致。

JY02.11.02:检测人员应核实密码模块的名称并未代表与密码边界内的部件构成不一致的部件或功能构成。

AY02.12:(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。

所需的送检文档

CY02.12.01:送检单位应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。

所需的检测规程

JY02.12.01:检测人员应核实送检单位为密码模块的每个互不相同的硬件、软件和/或固件部件提供了特定版本信息。

AY02.13:(安全级别 1,2,3,4)

***{密码边界内的某些硬件、软件和/或固件部件可以从标准{GM/T 0028—2014}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功能的运行。**

注:本条款作为 AY02.14 的一部分进行检测。

AY02.14:(安全级别 1,2,3,4)

***{密码模块规格的文档中}*应当阐明被排除的硬件、软件或固件部件。**

所需的送检文档

CY02.14.01:所有被排除在 GM/T 0028—2014 安全要求之外的硬件、软件和/或固件部件都应在送检单位的文档中明确列出。

CY02.14.02:送检单位的文档中应提供每个部件被排除的理由。送检单位应表明即使发生故障或误用,每个部件也不会干扰或破坏密码模块核准的安全功能的运行。

所需的检测规程

JY02.14.01:检测人员应核实送检单位是否表明模块的某些部件排除在 GM/T 0028—2014 的安全要求之外。

JY02.14.02:如果送检单位已经表明模块的某些组件从 GM/T 0028—2014 中排除,检测人员应核实每个排除的理由均被提供。这些理由必须表明即使部件出现故障,也不会造成 CSP、明文数据或其他一旦误用就可能导致危险的信息的泄露。如有以下证据的支持,这些理由将被视为可接受的:

——该组件不处理 CSP、明文数据或其他一旦被误用就可能导致危险的信息；

——该部件不与模块中允许以不恰当方式传递 CSP、明文数据或其他一旦被误用就可能导致危险的信息的安全相关部件连接；

——所有由部件处理的信息必须严格供模块内部使用，并不能以任何方式影响到与模块连接的设备。

JY02.14.03：检测人员应核实送检单位提供的所有排除理由的正确性。举证责任在送检单位；如存在任何不确定性或模糊性，检测人员应要求送检单位出示所需的进一步信息。

6.2.3.2 密码边界的定义

AY02.15：(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、基板或其他表面贴装；

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

——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；

——上面未列出的其他部件类型。

所需的送检文档

CY02.15.01：送检单位的文档中应标识硬件密码模块的所有硬件部件，并提供部件清单。

CY02.15.02：送检单位的文档中应标明模块的内部布局和安装方式(例如固定件和安装件)，包括近似比例的图纸。

CY02.15.03：送检单位的文档中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。

CY02.15.04：送检单位的文档应包括表示模块边界和其硬件部件相互关系的框图。

所需的检测规程

JY02.15.01：检测人员应核实送检单位的文档中包括部件清单，该部件清单包括密码模块的所有硬件部件。

JY02.15.02：检测人员应识别密码模块的所有硬件部件，并核实部件清单包括以下所有出现类型的部件，但不包括未在模块中使用的部件类型：

——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)；

——电源部件，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；

——电路板或其他表面贴装；

——外壳，包括任何门或封盖；

——加密模块外部设备或任何主要的独立子模块之间的物理连接器；

——软件和/或固件部件；

——其他上面未列出的部件类型。

JY02.15.03：检测人员应核实部件清单和其他条款提供的资料一致，其定义如下：

——AY02.07 中要求的密码模块的边界规格。核实所有在密码边界内的部件已包含在部件清单内，所有密码模块边界外的部件没有被列为密码模块部件；

——GM/T 0028—2014 附录 AYA.01 要求的框图规格。核实框图中的所有个体部件（如微处理器，存储器）也在部件清单中都有列出；

——AY02.14 条款规定被从 GM/T 0028—2014 安全要求排除的部件。核实这些部件仍然在部件清单中列出。

JY02.15.04：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。（物理和拆卸保护的要求在 GM/T 0028—2014 中的 7.7 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，这些接口可能泄露 CSP、明文数据或其他一旦被误用就可能导致破坏的信息。

JY02.15.05：检测人员应核实密码边界包括了在 AYA.01 要求的框图中标识的所有输入、输出或 CSP 处理、明文或其他一旦被误用就可能导致破坏的信息部件。

JY02.15.06：作为上述要求的一个部分特例，送检单位可在满足 AY02.13 的要求后被允许从 GM/T 0028—2014 的要求中排除某些特定部件。送检单位可以与处理排除在密码边界之外的部件一样有效的处理上述部件。这种情况下，检测人员应核实被排除部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破坏的信息。

JY02.15.07：检测人员应核实送检单位的文档中包含近似比例的图纸，其中展示了模块的内部布局，包括主要可识别部件的位置和大致尺寸。

JY02.15.08：检测人员应核实送检单位的文档中显示了模块的主要物理部件以及它们是如何安装或插入到模块中的。

JY02.15.09：检测人员应核实送检单位的文档中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；

——其他上面未列出的部件类型。

JY02.15.10：检测人员应核实送检单位提供的框图能够表示模块边界和其硬件部件相互关系。

AY02.16：（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。

所需的送检文档

CY02.16.01：送检单位的文档中应标识软件密码模块的所有软件部件，并提供部件清单。

CY02.16.02：送检单位的文档中应表明内部软件架构，包括软件部件是如何交互的。

CY02.16.03：送检单位的文档中应说明密码模块所运行的软件环境（例如操作系统，运行时库等）。

所需的检测规程

JY02.16.01：检测人员应核实送检单位的文档中包括部件清单，该部件清单包括密码模块的所有软件部件。

JY02.16.02：检测人员应核实部件清单包括以下所有出现类型的部件，但不包括未在模块中使用的

部件类型：

——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。

JY02.16.03：检测人员应核实送检单位的文档描绘的软件部件交互的内部软件架构准确。还应核实模块内的重要信息流和在密码模块内执行的过程，以及所有输入或输出到密码模块边界外的信息的清单。

JY02.16.04：检测人员应核实送检单位的文档中说明的密码模块所运行的软件环境（例如，操作系统，运行时库等）。

AY02.17：（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。

所需的送检文档

CY02.17.01：送检单位的文档中应标识固件密码模块的所有固件部件，并提供部件清单。

CY02.17.02：送检单位的文档中应表明内部固件架构，包括固件部件是如何交互的。

CY02.17.03：送检单位的文档中应说明密码模块所运行的固件环境（例如，操作系统，运行时库等）。

所需的检测规程

JY02.17.01：检测人员应核实送检单位的文档中包括部件清单，该部件清单包括密码模块的所有固件部件。

JY02.17.02：检测人员应核实部件清单包括以下所有出现类型的部件，但不包括未在模块中使用的部件类型：

——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。

JY02.17.03：检测人员应核实送检单位的文档描绘的固件部件交互的内部软件架构准确。还应核实模块内的重要信息流和在密码模块内执行的过程，以及所有输入或输出到密码模块边界外的信息的清单。

JY02.17.04：检测人员应核实送检单位的文档说明的密码模块所运行的固件环境。

AY02.18：（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分离的软件或固件部件的边界构成；

——包含每个部件所有端口和接口的集合。

所需的送检文档

CY02.18.01：送检单位的文档中应标识密码模块的类型是混合软件模块还是混合固件模块。

——混合软件模块应符合 CY02.15.01～CY02.15.04 和 CY02.16.01～CY02.16.03 的要求；

——混合固件模块应符合 CY02.15.01～CY02.15.04 和 CY02.17.01～CY02.17.03 的要求。

所需的检测规程

JY02.18.01：检测人员应核实送检单位的文档中标识了密码模块的类型是混合软件模块还是混合固件模块。

——混合软件模块应符合 JY02.15.01～JY02.15.10 和 JY02.16.01～JY02.16.04 的要求；

——混合固件模块应符合 JY02.15.01～JY02.15.10 和 JY02.17.01～JY02.17.04 的要求。

6.2.4 工作模式

6.2.4.1 工作模式通用要求

AY02.19：（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。

所需的送检文档

CY02.19.01:送检单位的文档中应说明密码模块核准的工作模式。

CY02.19.02:送检单位的文档中应描述如何启用核准的工作模式及方法。

所需的检测规程

JY02.19.01:检测人员应核实送检单位的文档包含了对核准的工作模式的描述。

JY02.19.02:检测人员应核实可以按照送检单位的文档中描述的方法启用核准的工作模式。

JY02.19.03: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。

AY02.20:(安全级别 1,2,3,4)

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、安全功能或过程。

所需的送检文档

CY02.20.01:送检单位的文档中应说明密码模块核准的工作模式所使用的核准的密码算法、安全功能或过程以及那些规定于 GM/T 0028—2014 的 7.4.3 中的服务。

CY02.20.02:送检单位应提供一份所有核准的密码算法、安全功能或过程的验证证书。

所需的检测规程

JY02.20.01: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、安全功能或过程以及那些规定于 GM/T 0028—2014 的 7.4.3 中的服务或过程。

JY02.20.02:检测人员应核实送检单位提供的核准的密码算法、安全功能或过程的验证证书。

JY02.20.03: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—2014 附录 C 的规定。

AY02.21:(安全级别 1,2,3,4)

除非非核准的密码算法或安全功能是核准的过程的一部分,而且与核准的过程的安全无关,否则非核准的密码算法、安全功能和过程或其他未在《*GM/T 0028—2014*》7.4.3 中规定的服务不应当被操作员用于核准的工作模式中(例如,非核准的密码算法或非核准的密钥生成方式可能被用来混淆数据或 CSP,但是结果被视为未受保护的明文,且只能提供非安全相关功能)。

所需的送检文档

CY02.21.01:送检单位应提供一份所有非核准的密码算法、安全功能和过程的清单。

CY02.21.02:送检单位的文档中应说明核准的工作模式中未使用非核准的密码算法、安全功能和过程或其他未规定于 GM/T 0028—2014 的 7.4.3 中的服务。

CY02.21.03: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中应说明非核准的密码算法或安全功能是核准的过程的一部分,而且与核准的过程的安全无关,并且不干扰或破坏密码模块核准的工作模式的运行。

CY02.21.04:送检单位的文档应解释为什么使用的非核准的密码算法、安全功能和过程与核准的过程操作非安全相关。

所需的检测规程

JY02.21.01:检测人员应核实送检单位提供的所有非核准的密码算法、安全功能和过程的清单。

JY02.21.02: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、安全功能和过程或其他未规定于 GM/T 0028—2014 的 7.4.3 中的服务。

JY02.21.03: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过程的安全无关、并且不干扰或破坏密码模块核准的工作模式的运行。

JY02.21.04:检测人员应核实送检单位文档中上述解释的有效性。举证责任在送检单位;如存在任何不确定性或模糊性,检测人员应要求送检单位出示所需的进一步信息。

6.2.4.2 正常工作

AY02.22:(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。

所需的送检文档

CY02.22.01:送检单位的文档应提供完整的模块 CSP 清单,并说明它们在核准的和非核准的服务及工作模式中的作用。

CY02.22.02:送检单位的文档中应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。

所需的检测规程

JY02.22.01:检测人员应核实送检单位的文档说明了各个 CSP 在核准的和非核准的工作模式中的作用。

JY02.22.02:检测人员应核实核准的和非核准的服务和工作模式的 CSP 相互分离。

AY02.23:(安全级别 1,2,3,4)

模块的安全策略应当为模块所包括的每个工作模式(核准的和非核准的)定义完整的服务集合。

所需的送检文档

CY02.23.01:送检单位的安全策略文档中应为模块所包括的每个工作模式(核准的和非核准的)定义完整的服务集合。

所需的检测规程

JY02.23.01:检测人员应核实安全策略文档为每个工作模式(核准的和非核准的)定义了服务集合,并核实服务集合完整和准确。

AY02.24:(安全级别 1,2,3,4)

当服务正在以核准的方式使用核准的密码算法、安全功能或过程以及其他规定于*{GM/T 0028—2014}*7.4.3 中的服务或过程的时候,该服务应当给出相应的状态指示。

所需的送检文档

CY02.24.01:送检单位应给出当服务以核准的方式使用核准的密码算法、安全功能或过程以及其他规定于 GM/T 0028—2014 的 7.4.3 中的服务或过程时的状态指示方式。

所需的检测规程

JY02.24.01:检测人员应核实状态指示方式的合理性和有效性。

6.3 密码模块接口

6.3.1 密码模块接口通用要求

AY03.01:(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,这些端口和接口是出入模块的密码边界的入口和出口。

所需的送检文档

CY03.01.01:送检单位的文档中应说明密码模块的每个物理端口和逻辑接口,包括:

——物理端口和引脚分配;

——物理封盖,门或开口;

——逻辑接口(如,API 和所有其他的数据/控制/状态信号)、信号名称和功能;

——用于物理控制输入的手动控制(如,按钮或开关);

——用于物理状态输出的物理状态指示仪(如,指示灯或显示器);

——逻辑接口到物理端口、手动控制和模块物理状态显示之间的映射；

——上述端口和接口的物理的，逻辑的和电气的特性。

CY03.01.02：送检单位文档中应通过 GM/T 0028—2014 附录 A.2.2 和附录 B.2.2 要求提供的框图、设计规格、源代码以及原理图，说明密码模块的信息流和物理接入点。同时还需提供其他有助于明确说明信息流、物理接入点和物理端口、逻辑接口的关系的文档。

CY03.01.03：对于密码模块的每一个物理或逻辑的输入，以及物理或逻辑的输出，送检单位的文档中应明确逻辑接口所对应的物理输入或输出。

所需的检测规程

JY03.01.01：检测人员应核实送检单位的文档说明了密码模块的每个物理端口和逻辑接口。所需的说明应包括：

——所有的物理输入和输出端口，包括它们引脚排列，模块内的物理位置，经过每个端口的逻辑信号的总览，以及两个或多个信号共享同一个物理引脚时的信号流的时序；

——所有的物理封盖，门或开口，包括它们在模块内的物理位置，以及通过每个封盖/门/开口可访问和/或修改的部件或功能；

——所有的逻辑输入和输出接口（例如，API 和所有其他的数据/控制/状态信号），包括列写或注释的所有逻辑数据和控制输入以及数据和状态输入的框图，以及信号名称和功能的清单和描述；

——所有用于物理输入控制信号的手动控制，如开关或按钮，包括它们在密码模块内的位置，以及可手动输入的控制信号的描述和清单；

——所有的物理状态指示，包括它们在模块内的物理位置和物理输出状态指示信号的清单和描述；

——逻辑输入输出接口到物理输入输出端口、手动控制以及密码模块物理状态指示之间的映射；

——上述物理端口和接口的物理，逻辑和电气特性，包括引脚分配总览，加载到每个端口的逻辑信号，电压幅值及它们的逻辑含义（如，高或低电平代表逻辑“0”，“1”或其他意思）和信号的时序。

JY03.01.02：检测人员应通过检查 GM/T 0028—2014 附录 A.2.2 和附录 B.2.2 要求提供的框图、设计规格、源代码以及原理图，以核实送检单位的文档说明了密码模块的所有信息流和物理接入点信息。文档还应说明密码模块信息流和物理访问点与密码模块逻辑接口和物理端口之间的关系。

JY03.01.03：检测人员应核实对于每个密码模块的物理或逻辑输入，以及物理或逻辑输出，送检单位的文档明确逻辑接口所对应的物理输入或输出。

JY03.01.04：检测人员应通过检查密码模块，核实送检单位文档中的说明与密码模块的实际设计一致。

AY03.02：（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（例如：输入数据和输出数据可以使用同一个端口），或者逻辑接口也可以分布在一个或多个物理端口上（例如：输入数据可以通过串口也可以通过并口）。

所需的送检文档

CY03.02.01：送检单位的设计应根据 AY03.04 所列的类别将模块的接口分成逻辑上不同和相互分离的类别，并且如果适用，AY03.12 亦可作为依据。这些信息应符合 AY03.01 描述的逻辑接口和物理端口的规格。

CY03.02.02：送检单位的文档中应提供每类逻辑接口到密码模块的物理端口的之间的映射。逻辑接口可以在物理上分布在多个物理端口上，或两个或多个逻辑接口可以共享一个物理端口。如果两个或多个逻辑接口共享同一物理端口，送检单位的文档中应说明这些不同类别接口的信息流是如何在逻辑上相互分离的。

所需的检测规程

JY03.02.01：检测人员应通过分析送检单位的文档和检查密码模块来核实，模块的接口从逻辑上可

分成不同的和相互独立的类别(如 AY03.04 和 AY03.12 所述)。所有这些信息应符合 AY03.01 规定的逻辑接口和物理端口设计规范和规格。

JY03.02.02:检测人员应核实送检单位的文档中提供了每个类别的密码模块的逻辑接口到物理端口的映射。逻辑接口可以在物理上分布在一个或多个物理端口,或者两个或更多的逻辑接口可以共享一个物理端口。如果两个或多个接口共享相同的物理端口,检测人员应核查送检单位的文档中说明了输入、输出、控制和状态接口上的信息流在逻辑上是如何相互分离的。

AY03.03:(安全级别 1,2,3,4)

{*密码模块接口*}文档应当按照{*GM/T 0028—2014*}A.2.3 的要求编写。

所需的送检文档

CY03.03.01:送检单位的文档中密码模块接口部分应按照 GM/T 0028—2014 附录 A.2.3 的要求编写。

所需的检测规程

JY03.03.01:检测人员应核实文档中密码模块接口部分符合 GM/T 0028—2014 附录 A.2.3 的要求。

6.3.2 接口类型

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

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

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

注:本条没有应检测的条款。

6.3.3 接口定义

AY03.04:(安全级别 1,2,3,4)

密码模块应当具备下列 5 种接口("输入"和"输出"是相对于模块而言的):

——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。

AY03.05:(安全级别 1,2,3,4)

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。

所需的送检文档

CY03.05.01: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);

——来自外部的状态信息；

——其他输入数据。

CY03.05.02：若适用，送检单位的文档中应说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。

所需的检测规程

JY03.05.01：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—2014 的 7.9 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 AY03.08 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 AY03.16～AY03.22 中）。

JY03.05.02：检测人员应核实送检单位的文档中是否说明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。检测人员应使用外部输入设备输入数据到数据输入接口，并使用该外部输入设备核实该输入数据。

AY03.06：（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。

所需的送检文档

CY03.06.01：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；

——经过处理或存储后从密码模块输出的其他信息。

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 AY03.16～AY03.22 中）。

CY03.06.02：若适用，送检单位的文档中应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、显示器、和/或其他存储设备。

所需的检测规程

JY03.06.01：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。检测人员应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—2014 的 7.9 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,AY03.11 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 AY03.18 和 AY03.19 小节中的相应要求。

JY03.06.02:检测人员应核实送检文档是否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、显示器和/或其他存储设备。检测人员应使用外部输出设备从外部输出接口输出数据,并使用该外部输出设备核实该输出数据。

AY03.07:(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。

所需的送检文档

CY03.07.01:送检单位的文档中应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—2014 的 7.11.4 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。

CY03.07.02:送检单位的文档中应说明密码模块的设计如何能确保模块在自测试时,数据输出接口禁止输出所有数据(自测试在 GM/T 0028—2014 的 7.10 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,显示自测试的状态信息可从状态输出接口输出以确定错误类型。

所需的检测规程

JY03.07.01:检测人员应核实送检单位的文档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。

JY03.07.02: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,送检单位应对检测人员提供该检测不能进行的合理解释。

JY03.07.03:检测人员应核实送检单位的文档说明了密码模块处于自测试模式时,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测试,数据输出接口禁止输出所有数据,直至自测试结束。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,用来显示自测试结果的状态信息可允许从状态输出接口输出。

JY03.07.04:检测人员应使模块执行自测试并核实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测试结果,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,送检单位应对检测人员提供该检测不能进行的合理解释。

JY03.07.05:检测人员应核实送检单位的文档说明了密码模块如何确保在自测试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。

AY03.08:(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。

所需的送检文档

CY03.08.01: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,密码模块的硬件部件);

——手动控制输入(如,使用开关、按钮或键盘);

——其他输入控制数据。

CY03.08.02:若适用,送检单位的文档中应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。

所需的检测规程

JY03.08.01: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。

JY03.08.02:检测人员应核实送检单位的文档中是否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。检测人员应使用外部输入设备输入命令到控制输入接口,并使用该外部输入设备核实该输入命令。

AY03.09:(安全级别 1,2,3,4)

所有用于控制密码模块运行的输出命令、信号及控制数据(例如,对另一个模块的控制命令)应当通过"控制输出"接口输出。

所需的送检文档

CY03.09.01: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。

CY03.09.02:若适用,送检单位的文档中应说明所有和密码模块同时使用并用于从控制输出接口输出控制数据的外部设备,如智能卡、令牌、显示器和/或其他存储设备。

所需的检测规程

JY03.09.01:检测人员应核实用于控制密码模块操作的输出命令,信号和控制数据经控制输出接口输出。

JY03.09.02:检测人员应核实送检单位的文档中是否说明了任何与密码模块同时使用并用于从控制输出接口输出控制数据的外部设备,如智能卡,令牌,显示器和/或其他存储设备。

AY03.10:(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,除非在安全策略中规定了一些例外情况。

所需的送检文档

CY03.10.01:送检单位的文档中应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。

CY03.10.02:送检单位文档应详细描述当密码模块处于自检状态时,密码模块的设计是如何保证控制输出接口禁止控制输出。

所需的检测规程

JY03.10.01:检测人员应核实当密码模块处于错误状态时,禁止通过"控制输出"接口输出。

JY03.10.02:检测人员应核实当密码模块处于自检状态时,禁止通过"控制输出"接口输出。

AY03.11:(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。

所需的送检文档

CY03.11.01: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,使用灯、蜂鸣器、音调、铃声、指示器或显示器);

——其他输出状态信息。

CY03.11.02:若适用,送检单位的文档中应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。

所需的检测规程

JY03.11.01: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。

JY03.11.02:检测人员应核实送检单位的文档中说明了所有的外部输出设备(若适用),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。

AY03.12:(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。

注:本条款不单独进行检测。

AY03.13:(安全级别 1,2,3,4)

电源接口:输入密码模块的所有外部电能应当通过电源接口输入。

注:当所有电能由密码模块内部提供或维持时,则电源接口是不需要的,内部电池的替换被认为是物理维护行为,应符合 GM/T 0028—2014 中的 7.7 中指定的要求。

所需的送检文档

CY03.13.01:如果密码模块需要向密码边界外的其他元件提供电能,或从密码边界外的其他元件获取电能(例如,电源或外部电池),送检文档中应指定电源接口及相关的物理端口。

CY03.13.02:所有从密码边界外的其他元件输入到密码模块或从密码模块输出到密码边界外的其他元件的电能应通过指定电源接口。

所需的检测规程

JY03.13.01:检测人员应核实送检单位的文档中说明密码模块是否需要从密码边界外的其他元件获取电能,或者是否向密码边界外的其他元件提供电能(例如,电源、电源线、电源插口/插座,或外部电池)。检测人员还应核实送检单位的文档中指定的电源接口和相应的物理端口。

JY03.13.02:通过检查密码模块,检测人员应核实从密码模块输入或输出到密码边界外的其他元件

的电能通过指定的电源接口。

AY03.14:(安全级别 1,2,3,4)

密码模块应当区分数据、控制信息和电源输入,以及数据、控制信息和状态信息输出。

所需的送检文档

CY03.14.01:送检单位的文档中应说明密码模块是如何区分数据、控制信息和电源输入,以及数据、控制信息和状态信息输出。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、控制信息和状态信息的物理和逻辑路径区分开来的。

CY03.14.02:送检单位的文档中应说明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、控制信息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、控制信息和状态信息的物理逻辑路径是物理共享的,送检单位的文档中应说明密码模块是如何强制实现逻辑分离。

CY03.14.03:送检单位文档应具有一致性,应说明密码模块区分数据、输入控制和数据控制、输出控制和输出状态,应说明通过密码模块可用的输入接口输入数据和状态信息的物理和逻辑路径,在物理上和逻辑上与通过密码模块可用的输出接口输出数据和状态信息的物理和逻辑路径是相分离的。

所需的检测规程

JY03.14.01:检测人员应核实送检单位的文档中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。

JY03.14.02:检测人员应核实送检单位的文档中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,检测人员应核实送检单位的文档说明了密码模块是如何强制实现逻辑分离的。

JY03.14.03:检测人员应核实送检单位文档的一致性,核实密码模块区分数据、输入控制和数据控制、输出控制和输出状态,以及通过可用的输入接口输入数据和状态信息的物理和逻辑路径,与通过可用的输出接口输出数据和状态信息的物理和逻辑路径在物理上和逻辑上是相分离的。

AY03.15:(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。

所需的送检文档

CY03.15.01:送检单位的文档中密码模块规格部分应明确规定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。

所需的检测规程

JY03.15.01:检测人员应核实文档中密码模块规格部分明确规定了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长度限制。

6.3.4 可信信道

AY03.16:(安全级别 3,4)

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受保护的明文CSP、密钥分量以及鉴别数据。

所需的送检文档

CY03.16.01:送检单位的文档中应说明实现了可信信道,并描述可信信道的实现方式。

所需的检测规程

JY03.16.01:检测人员应核实密码模块实现了可信信道,并核实该可信信道可以保证在密码模块与

发送者或接收者终端之间传输未受保护的明文 CSP、密钥分量以及鉴别数据的安全性。

AY03.17:(安全级别 3,4)

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。

所需的送检文档

CY03.17.01:送检单位的文档中应说明可信信道可以防止在通信链路上的非授权修改、替换和泄露。

所需的检测规程

JY03.17.01: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。

JY03.17.02:检测人员替换可信信道上传输的数据,应该不被接受。

JY03.17.03:检测人员应无法侦听获取到可信信道上传输的数据。

AY03.18:(安全级别 3,4)

可信信道使用的物理端口应当与其他物理端口实现物理隔离。

所需的送检文档

CY03.18.01:送检单位的文档中应说明可信信道所使用的物理端口,并描述其如何与其他物理端口实现物理隔离。

所需的检测规程

JY03.18.01:检测人员应核实文档中说明了可信信道所使用的物理端口,并描述了如何与其他物理端口实现物理隔离。

JY03.18.02: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。

AY03.19:(安全级别 3,4)

可信信道使用的逻辑接口应当与其他逻辑接口实现逻辑隔离。

所需的送检文档

CY03.19.01:送检单位的文档中应说明可信信道所使用的逻辑接口,并描述其如何与其他逻辑接口隔离。

所需的检测规程

JY03.19.01:送检单位的文档中应说明可信信道所使用的逻辑端口,并描述其如何与其他逻辑端口实现逻辑隔离。

JY03.19.02: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。

AY03.20:(安全级别 3,4)

基于身份的鉴别应当用于所有使用可信信道的服务。

所需的送检文档

CY03.20.01:送检单位的文档中应列举所有使用可信信道的服务。

CY03.20.02:送检单位的文档中应说明所有使用可信信道的服务采用了基于身份的鉴别,并描述实现方式。

所需的检测规程

JY03.20.01:检测人员应核实送检单位的文档中列举了所有使用可信信道的服务。

JY03.20.02:检测人员应核实所有使用可信信道的服务采用了基于身份的鉴别,并核实实现方式的安全性。

AY03.21:(安全级别 3,4)

当可信信道在使用时,应当提供状态指示器。

所需的送检文档

CY03.21.01:送检单位的文档中应说明使用可信信道的状态指示器和状态信息。

所需的检测规程

JY03.21.01：检测人员应核实密码模块具有可信信道使用状态指示器。

JY03.21.02：检测人员应核实可信信道在使用时，状态指示器正确指示状态。

AY03.22：（安全级别 4）

基于身份的多因素鉴别应当用于所有使用可信信道的服务。

所需的送检文档

CY03.22.01：送检单位的文档中应说明所有使用可信信道的服务采用了基于身份的多因素鉴别，并描述实现方式。

所需的检测规程

JY03.22.01：检测人员应核实所有使用可信信道的服务采用了基于身份的多因素鉴别，并核实实现方式的安全性。

6.4 角色、服务和鉴别

6.4.1 角色、服务和鉴别通用要求

AY04.01：（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。

AY04.02：（安全级别 1,2,3,4）

如果密码模块支持多个操作员同时操作，那么模块内部应当确保各个操作员担任的角色相隔离及相应的服务相隔离。

所需的送检文档

CY04.02.01：送检单位的文档中应说明是否支持多个操作员同时操作。

CY04.02.02：如果密码模块支持多个操作员同时操作，送检单位应描述怎样实现每一个操作员担任角色相隔离及相应服务相隔离的方法。

CY04.02.03：送检单位的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员角色又是用户角色）。

所需的检测规程

JY04.02.01：检测人员应核实送检单位的文档中如实描述密码模块实现的多个操作员角色与服务强制相隔离的方法。

JY04.02.02：检测人员应担任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。检测人员应核实，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担任角色的服务，以此来核实不同操作员角色与服务的分离。

JY04.02.03：如果送检单位的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担任受限角色，尝试违反限制条件，以此核实模块通过阻止第二操作员担任角色，强制执行这些约束。

AY04.03：（安全级别 1,2,3,4）

***{角色、服务和鉴别}*文档应当按照*{GM/T 0028—2014}*附录 A.2.4 中规定的要求编写。**

所需的送检文档

CY04.03.01：送检单位的文档中角色、服务和鉴别部分应按照 GM/T 0028—2014 附录 A.2.4 中规定的要求编写。

所需的检测规程

JY04.03.01：检测人员应核实文档中角色、服务和鉴别部分按照 GM/T 0028—2014 附录 A.2.4 中

规定的要求编写。

6.4.2 角色

AY04.04:(安全级别 1,2,3,4)

密码模块应当至少支持密码主管角色。

所需的送检文档

CY04.04.01:送检单位的密码模块产品应包括至少一个密码主管角色。

所需的检测规程

JY04.04.01:检测人员应核实送检单位的文档中定义了至少一个密码主管角色。

AY04.05:(安全级别 1,2,3,4)

密码主管角色应当负责执行密码初始化或管理功能,以及常用的安全服务,例如,模块初始化、CSP 和 PSP 的管理以及审计功能。

所需的送检文档

CY04.05.01:送检单位的文档中应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。

所需的检测规程

JY04.05.01:检测人员应核实送检单位的文档中描述了密码主管角色的功能。

JY04.05.02:检测人员应核实给出的密码主管角色名和许可服务与 AY04.05 说明相符。

注:担任角色应按 JY04.02.02 进行检测。

AY04.06:(安全级别 1,2,3,4)

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

所需的送检文档

CY04.06.01:如果密码模块支持用户角色,送检单位的文档中应说明用户角色负责执行的安全服务。

所需的检测规程

JY04.06.01:检测人员应核实送检单位的文档中描述了用户角色的功能。

JY04.06.02:检测人员应核实给出的用户角色名和许可服务与 AY04.06 说明相符。

注:担任角色应按 JY04.02.02 进行检测。

AY04.07:(安全级别 1,2,3,4)

当进入或退出维护员角色时,所有不受保护的 SSP 应当被置零。

所需的送检文档

CY04.07.01:送检单位的文档中应说明当维护员角色登录或退出时,模块的 SSP 是怎样动态清零的。

所需的检测规程

JY04.07.01:如果送检单位的文档说明密码模块实现了维护员角色,检测人员应核实送检单位的文档说明当进入或退出维护员角色时,清零所有未经加密的 SSP 的方法。

JY04.07.02:在非维护员角色状态下,检测人员应为所有未经加密的 SSP 加载非零值。进入维护员角色后,检测人员应核实清零已被执行。

JY04.07.03:在维护员角色状态下,检测人员应为所有未经加密的 SSP 加载非零值,从维护员角色退出后,检测人员应核实清零已被执行。

6.4.3 服务

6.4.3.1 服务通用要求

AY04.08:(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。

AY04.09:(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。

AY04.10:(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。

AY04.11:(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。

AY04.12:(安全级别 1,2,3,4)

密码模块应当为操作员提供下列服务:

——显示模块版本号;

——显示状态;

——执行自测试;

——执行核准的安全功能;

——执行置零。

注:本条款在 AY04.13～AY04.17 中进行检测。

AY04.13:(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。

所需的送检文档

CY04.13.01:送检单位的文档中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服务,并描述具体操作步骤和方法。

CY04.13.02:送检单位的文档中应说明密码模块输出的名称或模块标识符以及版本信息的定义规则,并说明这些信息是否与模块的审验记录相关联。

所需的检测规程

JY04.13.01:检测人员应核实送检单位的文档中说明了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服务,并描述了具体操作步骤和方法。

JY04.13.02:检测人员应核实密码模块输出的名称或模块标识符以及版本信息的定义规则与文档中定义的规则符合。

JY04.13.03:如果密码模块输出的名称或模块标识符以及版本信息与模块的审验记录相关联,检测人员应核实。

AY04.14:(安全级别 1,2,3,4)

密码模块应当输出当前的状态。

所需的送检文档

CY04.14.01:送检单位的文档中应说明密码模块具有输出当前状态的服务。

所需的检测规程

JY04.14.01:检测人员应核实送检单位的文档中说明了密码模块具有输出当前状态的服务。

JY04.14.02:检测人员应核实密码模块具有输出当前状态的服务。

AY04.15:(安全级别 1,2,3,4)

密码模块应当执行初始化和规定于*{GM/T 0028—2014}*7.10.2 中的运行前自测试。

所需的送检文档

CY04.15.01:送检单位的文档中应说明密码模块具有初始化和运行前自测试服务。

所需的检测规程

JY04.15.01:检测人员应核实送检单位的文档中说明了密码模块具有初始化和运行前自测试服务。

JY04.15.02:检测人员应核实密码模块的初始化和运行前自测试服务。

AY04.16:(安全级别 1,2,3,4)

密码模块应当至少执行一个在*{GM/T 0028—2014}*7.2.4 中规定的核准的工作模式中使用的核准的安全功能。

所需的送检文档

CY04.16.01:送检单位的文档中应说明密码模块核准的工作模式中使用的核准的安全功能。

所需的检测规程

JY04.16.01:检测人员应核实送检单位的文档中说明的密码模块核准的工作模式中使用的核准的安全功能。

AY04.17:(安全级别 1,2,3,4)

密码应当按照*{GM/T 0028—2014}*7.9.7 中的规定执行参数置零。

所需的送检文档

CY04.17.01:送检单位的文档中应说明密码模块支持密码参数置零的服务。

所需的检测规程

JY04.17.01:检测人员应核实送检单位的文档中说明了密码模块支持密码参数置零的服务。

6.4.3.2 旁路能力

AY04.18:(安全级别 1,2,3,4)

如果密码模块输出的数据是受到密码技术保护的(例如,经过加密),但是通过更改密码模块的配置或者由于操作员的干预,密码模块能够将数据直接输出(例如,不再经过加密),此时,应当定义该模块具有旁路能力。

注:本条款不单独进行检测。

AY04.19:(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。

所需的送检文档

CY04.19.01:如果模块实现旁路能力,送检单位的文档中应描述这个旁路服务。

CY04.19.02:送检单位的文档应说明在开启密码模块的旁路功能之前,操作员应担任相应的授权角色。

所需的检测规程

JY04.19.01:如果模块实现旁路能力,检测人员应核实送检单位的文档中描述了这个旁路服务。

JY04.19.02:检测人员应核实送检单位的文档中说明了在开启密码模块的旁路功能之前,操作员应担任相应的授权角色。

JY04.19.03:检测人员应核实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。

AY04.20:(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。

注:本条款作为 AY04.21 的一部分进行检测。

AY04.21:(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用于控制旁路能力的软件和/或硬件配置(例如,设置两个不同的软件或硬件标志位,其中一个可以由用户发起)。**

所需的送检文档

CY04.21.01:送检单位的文档应说明使用两个独立的内部操作来激活旁路能力。

CY04.21.02:送检单位的文档中应说明两个独立的内部操作能够改变用于控制旁路能力的软件和/或硬件配置,并描述这两个独立的内部操作。

所需的检测规程

JY04.21.01:检测人员应核实送检单位的文档说明了需要使用两个独立的内部操作来激活旁路能力。

JY04.21.02:检测人员应核实密码模块需要两个独立的内部操作才能激活旁路功能。

JY04.21.03:检测人员应核实送检单位的文档说明了两个独立的内部操作能够改变用于控制旁路能力的软件和/或硬件配置。

JY04.21.04:检测人员应核实两个独立的内部操作能够改变用于控制旁路能力的软件和/或硬件配置。

AY04.22:(安全级别 4)

***{接 AY04.20}*对于安全四级模块,上述两个独立的内部操作应当由两个不同的操作员完成。**

所需的送检文档

CY04.22.01:送检单位的文档中应描述如何由两个不同的操作员共同完成两个独立的内部操作才能激活旁路能力。

所需的检测规程

JY04.22.02:检测人员应核实激活旁路能力的内部操作和步骤。

JY04.22.03:检测人员应担任两个独立操作员的身份:操作员 1 和操作员 2。操作员 1 和操作员 2 分别完成两个独立的内部操作,来核实可以激活旁路能力。然后由操作员 1 完成两个独立的内部操作,来核实不能激活旁路能力。

AY04.23:(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:

——未被激活,表明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);

——被激活,表明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);

——同时存在被激活和未被激活,表明模块此时提供的某些服务是使用了密码功能,而某些服务没有使用密码功能(例如,对于拥有多个通信信道的模块,明文数据是否被加密取决于每个信道的配置)。

所需的送检文档

CY04.23.01:送检单位的文档中应描述如何指示旁路能力是否被激活的状态。

所需的检测规程

JY04.23.01:检测人员应核实密码模块具备状态指示,可以明确表示旁路功能是否被激活的状态。

6.4.3.3 自启动密码服务能力

AY04.24:(安全级别 1,2,3,4)

自启动密码服务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。

所需的送检文档

CY04.24.01:如果密码模块支持自启动密码服务能力,送检单位的文档中应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可以保留下来。

所需的检测规程

JY04.24.01:检测人员应核实密码模块自启动能力必须由密码主管配置。

JY04.24.02:检测人员应核实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,可以保留下来。

AY04.25:(安全级别 1,2,3,4)

***{如果密码模块实现了自启动密码服务能力,那么}*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。**

所需的送检文档

CY04.25.01:送检单位应定义两个独立的内部操作来激活自启动密码服务能力。

CY04.25.02:送检单位应提供文档详细说明两个独立的内部操作是如何改变控制自启动输出密码能力的软件和/或硬件的行为。

CY04.25.03:送检单位应提供文档详细说明两个独立的内部操作是如何防止单个错误造成不经意的输出。

所需的检测规程

JY04.25.01:检测人员应确定密码模块是否实现了自启动密码服务能力。检测人员应核实送检单位文档详细说明了在执行自启动密码服务能力前,密码模块执行了两个独立的内部操作。同时检测人员应核实送检单位文档详细说明了这两个独立的内部操作是如何防止单个错误造成的不经意的输出。

JY04.25.02:检测人员应激活自启动密码服务能力,确认两个独立的内部操作如上所述。如果在激活过程中执行了任何一个软件或固件的组件,检测人员应审查源代码,以确保在激活自启动密码服务能力前,该软件或固件组件支持两个独立内部操作的要求。

JY04.25.03:检测人员应核实当自启动密码模块能力被激活时,有一个状态指示器来显示该事件。

AY04.26:(安全级别 1,2,3,4)

***{接 AY04.25}*这两个独立的内部操作应当能够改变用于控制该能力的软件和/或硬件配置(例如,设置两个不同的软件或硬件标志位,其中一个可以由用户发起)。**

所需的送检文档

CY04.26.01:送检单位的文档中应描述内部操作如何改变用于控制旁路能力的软件和/或硬件配置。

所需的检测规程

JY04.26.01:检测人员应核实如果改变用于控制自启动密码服务能力的软件和/或硬件的配置需要两个独立的内部操作。

AY04.27:(安全级别 4)

***{接 AY04.25}*对于安全四级模块,上述两个独立的内部操作应当由两个不同的操作员完成。**

所需的送检文档

CY04.27.01:送检单位的文档中应描述如何由两个不同的操作员共同完成两个独立的内部操作才能激活自启动密码服务能力。

所需的检测规程

JY04.27.01:检测人员应核实激活自启动密码服务能力的内部操作和步骤。

JY04.27.02:检测人员应担任两个独立操作员的身份:操作员 1 和操作员 2。操作员 1 和操作员 2 分别完成两个独立的内部操作,来核实可以激活自启动密码服务能力。然后由操作员 1 完成两个独立的内部操作,来核实不能激活自启动密码服务能力。

AY04.28:(安全级别 1,2,3,4)

***{如果密码模块实现了自启动密码服务能力,那么}*模块应当显示其状态以指示自启动密码服务能力是否被激活。**

所需的送检文档

CY04.28.01:送检单位的文档应描述如何指示自启动密码服务能力是否被激活的状态。

所需的检测规程

JY04.28.01:检测人员应核实密码模块具备状态指示,可以明确表示自启动密码服务能力是否被激活的状态。

6.4.3.4 软件/固件加载

AY04.29:(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*{AY04.30～AY04.34}*。

注:本条款不单独进行检测。

AY04.30:(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。

所需的送检文档

CY04.30.01:送检单位提供加载的软件或固件的文件清单和说明。

CY04.30.02:送检单位应提供审验机构提供的审验报告或证明。

所需的检测规程

JY04.30.01:检测人员应核实清单中所包含的软件和固件,具有审验机构的审验报告。

AY04.31:(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/固件加载完成以及加载测试成功通过。

所需的送检文档

CY04.31.01:送检单位的文档中应描述在加载及加载测试过程中禁止数据输出的过程。

所需的检测规程

JY04.31.01:检测人员应核实在软件/固件加载以及加载测试成功通过前,密码模块的数据输出接口禁止输出数据。

AY04.32:(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—2014}*7.10.3.4 中规定的软件/固件加载条件自测试。

所需的送检文档

CY04.32.01:送检单位的文档中应描述运行加载的软件/固件的操作步骤和方法。

CY04.32.02:送检单位的文档中应说明在运行加载的代码之前执行了 GM/T 0028—2014 的 7.10.3.4 中规定的软件/固件加载条件自测试,并描述操作步骤和方法。

所需的检测规程

JY04.32.01:检测人员应核实在软件/固件加载条件自测试成功通过前,加载的代码应不能运行;条件自测试成功通过后,加载的代码应可以运行。

AY04.33:(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的**安全功能,直到成功执行*{GM/T 0028—2014}*7.10.2 中规定的运行前自测试。**

所需的送检文档

CY04.33.01: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的安全功能在运行之前,应该成功执行 GM/T 0028—2014 的 7.10.2 中规定的运行前自测试。

CY04.33.02:送检单位的文档中应描述运行前自测试的方法和步骤。

所需的检测规程

JY04.33.01:检测人员应核实在软件/固件运行前自测试成功通过前,任何已经加载的或已被修改的核准的安全功能应不能运行。

AY04.34:(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—2014*}7.4.3 中的软件或固件。

所需的送检文档

CY04.34.01:送检单位的文档中应描述运行加载的软件/固件的版本信息。

CY04.34.02:送检单位的文档中应描述获取模块版本信息的方法和步骤。

所需的检测规程

JY04.34.01: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,核实密码模块的版本信息按照 GM/T 0028—2014 的 7.4.3 中规定进行了增加和/或更新。

AY04.35:(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替换,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。

所需的送检文档

CY04.35.01: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。

所需的检测规程

JY04.35.01:检测人员应核实审验报告或证明与新软件或固件相符合。

AY04.36:(安全级别 1,2,3,4)

新加载的软件或固件镜像应当在模块上电重置之后才能运行。

所需的送检文档

CY04.36.01:如果支持镜像的完全替换,送检单位的文档中应详细说明新加载的软件或固件镜像在模块上电重置之后是如何运行的。

所需的检测规程

JY04.36.01:检测人员应核实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。

JY04.36.02:检测人员应核实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。

AY04.37:(安全级别 1,2,3,4)

所有 SSP 应当在运行新镜像之前被置零。

所需的送检文档

CY04.37.01:送检单位的文档中应列举所有 SSP,并说明所有 SSP 在运行镜像之前被置零。

CY04.37.02:送检单位的文档中应提供如何实施置零技术的原理性解释。

所需的检测规程

JY04.37.01:检测人员应核实在运行新的镜像之前,所有的 SSP 都被置零。

JY04.37.02:检测人员应核实送检单位提供的置零技术的原理性解释是否合理。

6.4.4 鉴别

AY04.38:(安全级别 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。作为 AY04.39 的一部分进行检测。

AY04.39:(安全级别 2,3,4)

***{接 AY04.38}*并且应当鉴别其能否担任所选定的角色(或角色的集合)。**

所需的送检文档

CY04.39.01: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式地或显示地选择一个或多个角色的机制,以及鉴别操作员担任的角色。

所需的检测规程

JY04.39.01:检测人员应核实送检单位的文档说明了一个或多个角色的选择机制,以及鉴别操作员担任的角色。

JY04.39.02:检测人员应担任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。

AY04.40:(安全级别 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鉴别,那么模块应当鉴别该操作员能否担任该新角色。

所需的送检文档

CY04.40.01:送检单位的文档中应描述操作员变换角色的能力,还必须说明怎样鉴别操作员担任的新角色。

所需的检测规程

JY04.40.01:检测人员应检查送检单位的文档以核实操作员改变角色的方法,包括怎样鉴别操作员担任的新角色。

JY04.40.02:检测人员应执行以下测试:

a) 担任一个角色,尝试将其改变为操作员已鉴别的其他角色,核实模块允许操作员可对分配的新角色请求服务。

b) 担任一个角色,尝试将其改变为操作员未鉴别的其他角色,核实模块不允许操作员可对分配的新角色请求服务。

AY04.41:(安全级别 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。作为 AY04.42 的一部分进行检测。

AY04.42:(安全级别 3,4)

***{接 AY04.41}*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。

AY04.43:(安全级别 1,2,3,4)

***{接 AY04.42}*并且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)。**

所需的送检文档

CY04.43.01: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员身份鉴别的机制、操作员的身份鉴别、一个或多个角色隐式地或显式地选择、操作员担任角色的鉴别。

所需的检测规程

JY04.43.01:检测人员应核实送检单位的文档说明怎样唯一标识操作员,怎样鉴别其身份,操作员怎样选择角色,怎样鉴别操作员基于身份鉴别担任的角色。

JY04.43.02:检测人员在鉴别过程中应初始化一个错误,且核实模块不允许检测人员继续进行鉴别程序。

JY04.43.03:检测人员应成功鉴别模块中他/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,并核实担任角色的鉴别是失败的。

AY04.44:(安全级别 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。

所需的送检文档

CY04.44.01:送检单位的文档中应描述操作员改变角色的能力,还应说明对操作员新角色的身份鉴别是必要的。

所需的检测规程

JY04.44.01:检测人员应核实送检单位的文档以证实操作员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鉴别的操作员角色。

JY04.44.02:检测人员应进行如下测试:

a) 担任一个角色,尝试将其改变为检测人员担任的已鉴别的其他角色,核实检测人员的身份不用被重新鉴别,再核实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担任的是另一个角色。

b) 担任一个角色,尝试将其改变为检测人员担任的未鉴别的其他角色,以核实模块拒绝基于操作员身份的角色访问。

AY04.45:(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,模块应当要求重新鉴别操作员。

所需的送检文档

CY04.45.01:送检单位的文档中应描述当模块被重置、重启、关闭时,如何将之前的鉴别结果清除。

所需的检测规程

JY04.45.01:检测人员应核实送检单位的文档描述模块被重置、重启、关闭时,之前的鉴别结果已经被清除。

JY04.45.02:检测人员应担任一个或多个角色,重置、重启、关闭再打开模块,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。

AY04.46:(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。

所需的送检文档

CY04.46.01:送检单位的文档中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。

所需的检测规程

JY04.46.01:检测人员应审查送检单位的文档,核实文档描述了鉴别数据的保护措施。检测人员应核实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。

JY04.46.02:检测人员应进行如下测试:

——尝试访问(绕开文件保护机制)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。

——使用送检单位的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。

AY04.47:(安全级别 2,3,4)

如果第一次访问密码模块时,模块不包含鉴别操作员所需的鉴别数据,那么应当使用其他被授权的方法(例如,过程控制,使用出厂设置或默认的鉴别数据)对模块进行访问控制和初始化鉴别。

所需的送检文档

CY04.47.01:送检单位的文档中应说明在初始化模块之前控制模块访问的方法。

所需的检测规程

JY04.47.01：检测人员应核实送检单位的文档描述了操作员在首次访问模块时的鉴别程序。

JY04.47.02：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，并应核实模块访问被拒绝。检测人员应担任一个授权角色并核实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担任其他角色并核实模块拒绝此角色的访问。

AY04.48：（安全级别 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。

所需的送检文档

CY04.48.01：送检单位提供的文档中应说明默认鉴别数据的内容和使用方式。

所需的检测规程

JY04.48.01：检测人员应核实使用默认鉴别数据可以第一次访问密码模块。

JY04.48.02：检测人员应核实使用默认鉴别数据在第一次鉴别后，鉴别数据必须要求被更换；如未更换，使用默认鉴别数据再次鉴别不通过。

AY04.49：（安全级别 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。

所需的送检文档

CY04.49.01：送检单位的文档中应说明采用何种核准的安全功能鉴别操作员。

所需的检测规程

JY04.49.01：检测人员应核实鉴别采用的安全功能符合 GM/T 0028—2014 附录 C 的要求。

AY04.50：（安全级别 2，3，4）

模块应当实现{*GM/T 0028—2014*}附录 E 中规定的一种核准的鉴别机制。

所需的送检文档

CY04.50.01：送检单位的文档中应说明采用何种核准的鉴别机制。

所需的检测规程

JY04.50.01：检测人员应核实密码模块采用的鉴别机制符合 GM/T 0028—2014 附录 E 的规定。

AY04.51：（安全级别 2，3，4）

在模块的安全策略文档（见{*GM/T 0028—2014*}附录 B）中应当描述鉴别机制的强度。

所需的送检文档

CY04.51.01：送检单位提供符合 GM/T 0028—2014 附录 B 要求的安全策略文档，描述鉴别机制的预期强度。

所需的检测规程

JY04.51.01：检测人员应核实送检单位提供的安全策略文档符合 GM/T 0028—2014 附录 B 的要求。

JY04.51.02：检测人员应核实送检单位提供的文档描述了鉴别机制的预期强度。

AY04.52：（安全级别 2，3，4）

对于每次核准的鉴别机制的尝试使用，模块应当满足鉴别强度要求。

所需的送检文档

CY04.52.01：送检单位的文档中应说明密码模块支持的每个核准的鉴别机制，及鉴别强度。

所需的检测规程

JY04.52.01：检测人员应核实送检单位文档描述了每个核准的鉴别机制的鉴别强度。

JY04.52.02：检测人员应核实送检单位文档中每个核准的鉴别机制都满足目标。

AY04.53：（安全级别 2，3，4）

对于在 1 min 内对核准的鉴别机制的多次尝试使用，模块应当满足鉴别强度要求。

所需的送检文档

CY04.53.01:送检单位文档中应说明,每个核准的鉴别机制在 1 min 内的多次随机尝试使用通过核准的鉴别机制的成功概率。

所需的检测规程

JY04.53.01:检测人员应核实送检单位文档描述了核准的鉴别机制,及在 1 min 内随机尝试使用成功的概率。

JY04.53.02:检测人员应核实送检单位文档描述了核准的鉴别机制在 1 min 内随机尝试使用成功率都满足目标。

AY04.54:(安全级别 2,3,4)

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)。

所需的送检文档

CY04.54.01:送检单位的文档中应说明密码模块鉴别机制的实现方法和原理。

所需的检测规程

JY04.54.01:检测人员应核实密码模块核准的鉴别机制不依赖于在文档中的过程控制或安全规则。

AY04.55:(安全级别 2)

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。

所需的送检文档

CY04.55.01:送检单位的文档中应说明软件密码模块所采用的操作系统。

CY04.55.02:送检单位的文档中应说明操作系统实现的鉴别机制。

所需的检测规程

JY04.55.01:检测人员应核实软件密码模块所使用的操作系统的鉴别机制符合要求。

AY04.56:(安全级别 2,3,4)

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)。

所需的送检文档

CY04.56.01:送检单位的文档中应说明,在输入鉴别数据时,隐藏鉴别数据给操作员的反馈信息的方法。

所需的检测规程

JY04.56.01:检测人员应检查送检单位文档并核实身份鉴别数据在数据输入过程中不可见。

JY04.56.02:检测人员应输入鉴别数据,并核实在输入鉴别数据过程中不可见。

AY04.57:(安全级别 2,3,4)

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。

所需的送检文档

CY04.57.01:送检单位文档中应说明,在操作员输入鉴别数据时使用的反馈机制。

所需的检测规程

JY04.57.01:检测人员应审查送检单位文档并核实反馈机制不提供可用于猜测或确定身份认证数据的信息。

JY04.57.02:检测人员应输入每个担任角色的鉴别数据,确保反馈机制不提供有用的信息。

AY04.58:(安全级别 1)

如果模块不支持鉴别机制,模块应当要求操作员隐式或显式地选择一个或多个角色。

所需的送检文档

CY04.58.01:送检单位应记录密码模块运行的鉴别类型。应记录操作员隐式或显示地选择一个或

一系列角色的机制，及操作员担任角色的鉴别方法。

CY04.58.02：送检单位的文档中应提供操作员隐式或显示地的担任角色的描述。

所需的检测规程

JY04.58.01：检测人员应核实送检单位的文档提供了操作员明确或不明确的担任角色的描述，及担任每个角色的方法。

JY04.58.02：检测人员应调用送检单位的文档中描述的方法，并核实每个角色都能被明确的或不明确的担任。

AY04.59：（安全级别 2）

密码模块应当至少采用基于角色的鉴别机制以控制对模块的访问。

注：本条款作为 AY04.38～AY04.40 的一部分进行检测。

AY04.60：（安全级别 3，4）

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。

注：本条款作为 AY04.41～AY04.44 的一部分进行检测。

AY04.61：（安全级别 4）

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。

所需的送检文档

CY04.61.01：送检单位的文档中应说明密码模块采用的基于身份的多因素鉴别机制。

所需的检测规程

JY04.61.01：检测人员核实密码模块采用基于身份的多因素鉴别机制以控制对模块的访问。

JY04.61.02：检测人员应核实密码模块采用的基于身份的多因素鉴别机制。

6.5 软件/固件安全

AY05.01：（安全级别 1，2，3，4）

本条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。

AY05.02：（安全级别 1，2，3，4）

***{软件/固件安全}*文档应当按照*{GM/T 0028—2014 附录}*A.2.5 中规定的要求编写。**

所需的送检文档

CY05.02.01：送检材料的软件/固件安全部分应按照 GM/T 0028—2014 附录 A.2.5 中规定的要求编写。

所需的检测规程

JY05.02.01：检测人员应核实送检单位完整的提供了 GM/T 0028—2014 附录 A.2.5 所要求的文档。

AY05.03：（安全级别 1，2，3，4）

对于安全一级，下列安全要求*{AY05.04～AY05.11}*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。

AY05.04：（安全级别 1，2，3，4）

所有的软件和固件应当符合*{GM/T 0028—2014}*7.11.7 中的规定，确保安装前未被修改。

所需的送检文档

CY05.04.01：送检单位应提供软件和固件的说明书。

CY05.04.02：送检文档应描述如何确保在安装前所有的软件与固件未被修改。

所需的检测规程

JY05.04.01：检测人员应通过检查密码模块核实送检文档中的说明书与密码模块的实际设计一致。

JY05.04.02:检测人员应核实送检单位使用的,确保在安装前所有的软件与固件未被修改的方法的安全性。

AY05.05:(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。

所需的送检文档

CY05.05.01:送检文档中应详细说明所有的软件和固件部件所使用的、已核准的完整性技术。这些完整性技术可由该密码模块提供,也可由另一个经审验的密码模块提供。

CY05.05.02:送检文档中应明确说明如何在所有的软件和固件部件中应用了完整性技术(使用单个的消息鉴别码或签名,或多个分离的鉴别码或签名)。

CY05.05.03:送检文档应明确说明完整性技术所使用密钥的位置。如果核准的数字签名被当作完整性技术使用,那么送检材料应明确说明签名私钥(用于生成参考签名)的位置。

所需的检测规程

JY05.05.01:检测人员应通过检查密码模块核实模块中的所有软件和固件部件都使用了核准的完整性技术。

AY05.06:(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。

所需的送检文档

CY05.06.01:送检单位应提供软件和固件完整性测试的说明书。这个机制应是核准的安全功能。

CY05.06.02:送检文档中应说明如果完整性测试失败,模块将进入错误状态。

CY05.06.03:送检文档中应说明在多个分离的消息鉴别码或签名中,任何一个消息鉴别码或签名验证失败都会导致模块进入错误状态。

所需的检测规程

JY05.06.01:检测人员应核实如果完整性测试失败,模块进入错误状态。

JY05.06.02:检测人员应核实在完整性测试完成后,此测试过程中生成的临时值被置零。

JY05.06.03:检测人员应核实在多个分离的消息鉴别码或签名中,任何一个消息鉴别码或签名的验证失败都导致模块进入错误状态。

AY05.07:(安全级别 1,2,3,4)

在多个分离的消息鉴别码或签名中,任何一个鉴别码或签名验证失败都应当导致模块进入错误状态。

注:本条款不单独进行检测。

AY05.08:(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。

注:本条款不单独进行检测。

AY05.09:(安全级别 1,2,3,4)

操作员应当能够通过*{GM/T 0028—2014}*7.3.2 中规定的 SFMI、HSMI 或 HFMI 服务按需执行核准的完整性技术。

所需的送检文档

CY05.09.01:送检文档应说明通过 SFMI、HSMI 或 HFMI 服务按需执行已核准的完整性技术的方法。

所需的检测规程

JY05.09.01:检测人员应核实可通过 SFMI、HSMI 或 HFMI 服务完成完整性测试。

JY05.09.02:检测人员应核实在完整性测试的执行过程中,(GM/T 0028—2014 的 7.3.2 中提到的)

密码模块的所有的数据和控制输入、数据和状态输出以及(GM/T 0028—2014 的 7.4.3 中提到的)相关服务可通过 HMI、SFMI、HFMI 或 HSMI 服务传输。

AY05.10:(安全级别 1,2,3,4)

***{GM/T 0028—2014}*7.3.3 中规定的密码模块的所有数据和控制输入,数据、控制和状态输出,以及*{GM/T 0028—2014}*7.4.3 中规定的服务,应当通过定义的 HMI、SFMI、HFMI 或 HSMI 完成。**

注:本条款不单独进行检测。

AY05.11:(安全级别 1,2,3,4)

如果新加载的软件或固件是密码模块运行所必须的,但不是完全替换或覆盖经审验的模块,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。

所需的送检文档

CY05.11.01:送检单位应提供通过已审验的模块实现软件/固件加载测试的说明。

所需的检测规程

JY05.11.01:检测人员应核实送检文档及其实现。

AY05.12:(安全级别 2,3,4)

对于安全二级,下列要求*{AY05.13～AY05.16}*应当适用于密码模块内的软件或固件部件。

注:本条款不单独进行检测。作为 AY05.13～AY05.16 的一部分进行检测。

AY05.13:(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。

所需的送检文档

CY05.13.01:送检单位应提供可执行形式的软件和固件的说明。

所需的检测规程

JY05.13.01:为避免存在可动态修改的代码,检测人员应核实送检单位的软件说明书和密码模块的相关实现。

AY05.14:(安全级别 2,3,4)

应当确保操作员无法通过 HMI、SFMI、HFMI 或 HSMI 接口的服务或控制设置,启动或执行调试技术。

所需的送检文档

CY05.14.01:送检文档应提供 HMI、SFMI、HFMI 或 HSMI 服务的说明。

所需的检测规程

JY05.14.01:检测人员应核实送检文档中的服务或控制设置的说明。

JY05.14.02:检测人员应核实送检文档,确认操作者无法通过这些服务或控制设置,启动或执行调试技术。

JY05.14.03:检测人员应测试这些服务或控制设置,以核实操作者不能启动或执行调试技术。

AY05.15:(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:本条款作为 AY05.16 的一部分进行检测。

AY05.16:(安全级别 2,3,4)

***{接 AY05.15}*如果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。**

所需的送检文档

CY05.16.01:送检文档应标识用于保持密码软件和固件部件完整性的技术。

所需的检测规程

JY05.16.01:检测人员应核实送检文档符合 CY05.16.01 的要求。

JY05.16.02:检测人员应尝试破坏密码软件和固件部件。如果完整性未被破坏,则检测不通过。

AY05.17:(安全级别 3,4)

对于安全三级和四级,下列要求{*AY05.18～AY05.21*}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。

AY05.18:(安全级别 3,4)

密码边界内的所有软件和固件应当使用核准的数字签名进行保护。

注:本条款作为 AY05.19 的一部分进行检测。

AY05.19:(安全级别 3,4)

***{接 AY05.18}*如果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。**

所需的送检文档

CY05.19.01:送检文档应说明核准的数字签名机制。

CY05.19.02:送检文档中应说明如果使用核准的数字签名机制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,模块应进入错误状态。

所需的检测规程

JY05.19.01:检测人员应通过检查密码模块核实密码边界内的所有软件和固件部件使用的加密机制包含了已核准的数字签名机制。

JY05.19.02:检测人员应使用已核准的数字签名计算的结果与之前生成的结果进行比较,如果不相等,则测试失败,模块进入错误状态。

AY05.20:(安全级别 3,4)

数字签名技术可以包含单个签名,或者多个分离的签名,分离的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 AY05.05 一起进行检测。

AY05.21:(安全级别 3,4)

签名私钥应当保存在模块外。

所需的送检文档

CY05.21.01:送检文档应满足 CY05.05.03 的要求。送检单位的设计应确保生成参考签名的签名私钥保存在密码模块的边界之外。

所需的检测规程

JY05.21.01:检测人员应通过检查和文档审查,核实签名私钥保存在密码边界外。

6.6 运行环境

6.6.1 运行环境通用要求

AY06.01:(安全级别 1,2)

如果运行环境是不可修改或受限制的,{*GM/T 0028—2014*}7.6.2 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。作为 AY06.04 的一部分进行检测。

AY06.02:(安全级别 1,2)

如果运行环境是可修改的,{*GM/T 0028—2014*}7.6.3 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。若适用,作为 AY06.05～AY06.29 的一部分进行检测。

AY06.03:(安全级别 1,2)

***{运行环境}*文档应当按照*{GM/T 0028—2014 附录}*A.2.6 中规定的要求编写。**

所需的送检文档

CY06.03.01:送检单位提供的文档应按照 GM/T 0028—2014 附录 A.2.6 中规定的要求编写。

所需的检测规程

JY06.03.01：检测人员应核实送检单位提供的文档按照 GM/T 0028—2014 附录 A.2.6 中规定的要求编写。

6.6.2 受限或不可修改运行环境的操作系统要求

AY06.04：（安全级别 1）

如果模块在{*GM/T 0028—2014*}7.7 中达到安全一级，则{*GM/T 0028—2014*}7.6.3 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。作为 AY06.05～AY06.08 的一部分进行检测。

6.6.3 可修改运行环境的操作系统要求

AY06.05：（安全级别 1，2）

每一个密码模块的实例应当能够控制和支配自己的 SSP。

注 1：密码模块的每一个实例控制和支配自己的 SSP，不由外部进程/操作员所有和控制。

注 2：这一要求不能由管理文件和程序来实现，必须由密码模块本身来实现。

所需的送检文档

CY06.05.01：送检单位的文档中应描述用来确保密码模块的加密进程运行时每一个实例能够控制和支配自己的 SSP 的操作系统机制。

所需的检测规程

JY06.05.01：检测人员应通过审查送检单位的文档和检查操作系统，核实当密码模块运行时每一个实例能够控制和支配自己的 SSP。

JY06.05.02：检测人员应通过审查送检单位的文档和检查操作系统，核实这一要求由密码模块本身来实现。

JY06.05.03：检测人员应运行管理员和用户指南文档中描述的密码功能，当密码功能执行时，该检测人员或另一检测人员应在密码模块受控的情况下尝试非授权访问密钥、私钥、临时密钥生成值和其他 SSP。

AY06.06：（安全级别 1，2）

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。

所需的送检文档

CY06.06.01：送检单位的文档中应描述运行环境机制用来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。

所需的检测规程

JY06.06.01：检测人员应通过审查送检单位的文档和检查运行环境机制，核实运行环境提供了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。

JY06.06.02：检测人员应运行管理员和用户指南文档中描述的密码功能，该检测人员或另一检测人员应尝试访问 CSP 和修改 SSP，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。

AY06.07：（安全级别 1，2）

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。

所需的送检文档

CY06.07.01：送检单位应提供文档描述对运行环境配置的所有规定。

所需的检测规程

JY06.07.01:检测人员应核实送检单位的文档中对运行环境配置的所有规定。

JY06.07.02:检测人员应核实运行环境配置的所有规定记录在安全策略中。

AY06.08:(安全级别 1,2)

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。

注:这一要求不能由管理文件和程序来实现,必须由密码模块本身来实现。

所需的送检文档

CY06.08.01:送检单位的文档中应描述用来确保密码模块产生的进程由模块自己所有,不由外部进程/操作员所有的操作系统机制。

所需的检测规程

JY06.08.01:检测人员应通过审查送检单位的文档和检查操作系统,核实密码模块产生的进程由模块自己所有,不由外部进程/操作员所有。

JY06.08.02:检测人员应通过审查送检单位的文档和检查操作系统,核实这一要求由密码模块本身来实现。

JY06.08.03:检测人员应运行管理员和用户指南文档中的描述的密码功能,当密码功能执行时,该检测人员或另一检测人员应尝试通过外部独立进程或操作员获取由密码模块产生的密码进程的所有权。

AY06.09:(安全级别 2)

对于安全二级,操作系统还应当满足下列*{AY06.10～AY06.29}*要求或者经审验机构许可。

注 1:如果运行环境要求未由审验机构指定,这个条款按照 AY06.10～AY06.29 进行检测。

注 2:如果运行环境要求由审验机构指定,这个条款按照以下进行检测。

所需的送检文档

CY06.09.01:送检单位应提供文档描述运行环境。

CY06.09.02:送检单位的文档中应比较密码模块的运行环境和审验机构许可的运行环境。

所需的检测规程

JY06.09.01:检测人员应核实送检单位的文档中对操作系统进行了描述。

JY06.09.02:检测人员应通过检查操作系统,核实和送检单位对操作系统的描述一致。

JY06.09.03:检测人员应通过审查送检单位对操作系统的描述和检查操作系统,核实该操作系统为审验机构所许可。

AY06.10:(安全级别 2)

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。操作系统实现了基于角色的访问控制,或者实现了自主访问控制,该自主访问控制可通过访问控制列表(ACL)来定义新的组和分配权限,并且能够给每个用户分配多个组。

所需的送检文档

CY06.10.01:送检单位应提供操作系统文档描述操作系统控制机制,该机制应实现了基于角色的访问控制,或者实现了自主访问控制,该自主访问控制可通过访问控制列表(ACL)来定义新的组和分配权限,并且能够给每个用户分配多个组。

所需的检测规程

JY06.10.01:检测人员应通过审查送检单位的文档和检查操作系统控制机制,核实该机制实现了基于角色的访问控制,或者实现了自主访问控制,该自主访问控制可通过访问控制列表(ACL)来定义新的组和分配权限,并且能够给每个用户分配多个组。

JY06.10.02:检测人员应配置操作系统的基于角色的访问控制或者自主访问控制,为特定的用户或组分配权限。检测人员担任一个允许的用户或组角色,应尝试执行、修改或读取授权访问的 SSP、控制

或状态数据。

JY06.10.03：检测人员应配置操作系统的基于角色的访问控制或者自主访问控制，为特定的用户或组分配权限。检测人员应担任一个不同的用户或组角色，应尝试执行、修改或读取非授权访问的 SSP、控制或状态数据。

AY06.11：（安全级别 2）

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。

所需的送检文档

CY06.11.01：送检单位应提供操作系统文档描述操作系统控制机制，该机制正确配置后可以防止非授权地执行、修改和读取 SSP、控制和状态数据。

所需的检测规程

JY06.11.01：检测人员应通过审查送检单位的文档和检查操作系统控制机制，核实操作系统正确配置后可以防止非授权地执行、修改和读取 SSP、控制和状态数据。

JY06.11.02：检测人员应正确配置操作系统，使之可防止非授权地执行、修改和读取 SSP、控制和状态数据。在密码进程执行期间，检测人员应尝试执行、修改和读取授权访问的 SSP、控制和状态数据。

JY06.11.03：检测人员应正确配置操作系统，使之可防止非授权地执行、修改和读取 SSP、控制和状态数据。在密码进程执行期间，检测人员应尝试执行、修改和读取非授权访问的 SSP、控制和状态数据。

AY06.12：（安全级别 2）

***{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或组以及与它们相关的权限。**

所需的送检文档

CY06.12.01：送检单位应提供操作系统文档描述操作系统的访问控制机制如何进行相关配置，以定义和实现有权运行模块中密码软件的角色或组以及与它们相关的权限。

所需的检测规程

JY06.12.01：检测人员应通过审查文档和检查操作系统控制机制，核实操作系统可进行相关配置，以定义和实现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。

JY06.12.02：检测人员应配置操作系统控制机制，定义和实现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。检测人员应确认这些角色和分组有权运行模块中密码软件。

JY06.12.03：检测人员应配置操作系统控制机制，定义和实现无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。检测人员应确认这些角色和分组无权运行模块中密码软件。

AY06.13：（安全级别 2）

***{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或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。**

所需的送检文档

CY06.13.01：送检单位应提供操作系统文档描述操作系统的访问控制机制如何进行相关配置，以定义和实现有权修改（写、替换和删除）存储在密码边界内软件的角色或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。

所需的检测规程

JY06.13.01：检测人员应通过审查文档和检查操作系统控制机制，核实操作系统可进行相关配置，以定义和实现有权修改（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。

JY06.13.02：检测人员应配置操作系统控制机制，定义和实现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。检测人员应确认这些角色和分组有权修改（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。

JY06.13.03：检测人员应配置操作系统控制机制，定义和实现无权修改（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。检测人员应确认这些角色和分组无权修改（写、替换和删除）上述存储在密码边界内的软件。

AY06.14：（安全级别 2）

***{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 和明文数据的角色或组以及与它们相关的权限。**

所需的送检文档

CY06.14.01：送检单位应提供操作系统文档描述操作系统的访问控制机制应如何进行相关配置，以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。

所需的检测规程

JY06.14.01：检测人员应通过审查文档和检查操作系统控制机制，核实操作系统可进行相关配置，以定义和实现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。

JY06.14.02：检测人员应配置操作系统控制机制，定义和实现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。

JY06.14.03：检测人员应配置操作系统控制机制，定义和实现无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。检测人员应确认这些角色和分组无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。

AY06.15：（安全级别 2）

***{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 的角色或组以及与它们相关的权限。**

所需的送检文档

CY06.15.01：送检单位应提供操作系统文档描述操作系统的访问控制机制如何进行相关配置，以定义和实现有权输入 SSP 的角色、分组以及与它们相关的权限。

所需的检测规程

JY06.15.01：检测人员应通过审查文档和检查操作系统控制机制，核实操作系统可进行相关配置，以定义和实现有权输入 SSP 的角色、分组以及与它们相关的权限。

JY06.15.02：检测人员应配置操作系统控制机制，定义和实现有权输入 SSP 的角色、分组以及与它们相关的权限。

JY06.15.03：检测人员应配置操作系统控制机制，定义和实现无权输入 SSP 的角色、分组以及与它们相关的权限。检测人员应确认这些角色和分组无权输入 SSP。

AY06.16：（安全级别 2）

下列规定*{AY06.17～AY06.20}*应当与密码模块安全策略文档中已定义的角色和服务相一致。

注：本条款不单独进行检测。作为 AY06.17～AY06.20 的一部分进行检测。

AY06.17：（安全级别 2）

当密码模块不支持维护员角色时，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）。

所需的送检文档

CY06.17.01:送检单位应提供操作系统文档描述当密码模块不在维护模式时,操作系统如何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)。

CY06.17.02:送检单位提供的有关密码模块不在维护模式时,操作系统如何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)的说明书应与安全策略中已定义的角色、分组和服务相一致。

所需的检测规程

JY06.17.01:检测人员应通过文档审查和操作系统访问控制机制检查,核实操作系统可进行相应配置,使得密码模块不在维护模式时,所有操作员和运行的进程都不能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)。

JY06.17.02:检测人员应核实密码模块不在维护模式时,操作系统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)的相关措施与安全策略中已定义的角色、分组和服务相一致。

JY06.17.03:检测人员应配置操作系统控制机制,使得密码模块不在维护模式时,所有操作员和运行的进程都不能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)。检测人员应担任操作员的角色,确认当密码模块不在维护模式时,他不能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)。同时,检测人员应确认当密码模块不在维护模式时,运行的进程不能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)。

AY06.18:(安全级别 2)

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

所需的送检文档

CY06.18.01:送检单位应提供操作系统文档描述操纵系统如何防止用户进程对其他进程的 SSP 以及系统 SSP 进行读或写操作。

CY06.18.02:送检单位提供的有关操作系统如何防止用户进程对其他进程的 SSP 以及系统 SSP 进行读或写操作的说明书应与安全策略中已定义的角色、分组和服务相一致。

所需的检测规程

JY06.18.01:检测人员应通过审查文档和检查操作系统控制机制,核实操作系统可进行相关配置,以防止用户进程对其他进程的 SSP 以及系统 SSP 进行读或写操作。

JY06.18.02:检测人员应核实操作系统防止用户进程对其他进程的 SSP 以及系统 SSP 进行读或写操作的相关措施与安全策略中已定义的角色、分组和服务相一致。

JY06.18.03:检测人员应配置操作系统控制机制,防止用户进程对其他进程的 SSP 以及系统 SSP 进行读或写操作。检测人员应确认用户进程的确无法对其他进程的 SSP 以及系统 SSP 进行读或写操作。

AY06.19:(安全级别 2)

满足以上要求*{AY06.16～AY06.18}*的操作系统配置应当在管理员指南中阐明。

所需的送检文档

CY06.19.01:送检单位应提供管理员指南文档描述操作系统的配置如何满足了 AY06.16～AY06.18 的要求。

所需的检测规程

JY06.19.01:检测人员应核实送检单位提供的管理员指南描述了操作系统的配置如何满足了 AY06.16～AY06.18 的要求。

AY06.20:(安全级别 2)

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。

所需的送检文档

CY06.20.01:送检单位应提供管理员指南文档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。

所需的检测规程

JY06.20.01:检测人员应核实送检单位的管理员指南文档声明了操作系统应按照需要保护的模块内容所指定的要求进行配置。

AY06.21:(安全级别 2)

操作系统的身份标识和鉴别机制应当满足*{GM/T 0028—2014}*7.4.4 中规定的要求,并在模块安全策略文档中具体阐明。

注:本条款不单独进行检测。作为 AY06.24～AY06.28 的一部分进行检测。

AY06.22:(安全级别 2)

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。

注:本条款不单独进行检测。作为 AY06.24～AY06.28 的一部分进行检测。

AY06.23:(安全级别 2)

操作系统应当至少拥有以下属性*{AY06.24～AY06.28}*。

注:本条款不单独进行检测。作为 AY06.24～AY06.28 的一部分进行检测。

AY06.24:(安全级别 2)

操作系统应当提供具有审计事件日期和时间的审计机制。

注:本条款假定密码模块使用操作系统提供的审计机制来审计识别的事件。对于密码模块软件使用其他文件作为审计日志是不够的,无论如何很好的保护。

所需的送检文档

CY06.24.01:送检单位应提供操作系统文档描述操作系统提供的审计机制,以及审计事件日期和时间的标注方法。

所需的检测规程

JY06.24.01:检测人员应通过审查文档和检查操作系统,核实操作系统提供了具有审计事件日期和时间的审计机制。

AY06.25:(安全级别 2)

密码模块应当不把 SSP 写入任何审计记录中。

所需的送检文档

CY06.25.01:送检单位应提供操作系统文档描述密码模块为操作系统的审计机制提供审计记录的服务。

所需的检测规程

JY06.25.01:检测人员应通过审查文档和检查密码模块服务(为操作系统的审计机制提供审计记录),核实密码模块未把 SSP 写入任何审计记录中。

JY06.25.02:检测人员应运行密码模块提供审计记录的服务,检查操作系统的审计日志,核实其中未包括任何 SSP。

AY06.26:(安全级别 2)

***{密码模块的}*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。

所需的送检文档

CY06.26.01:送检单位应提供操作系统文档描述被操作系统审计机制记录的所有密码模块事件。

所需的检测规程

JY06.26.01:检测人员应通过审查文档和检查密码模块服务,核实操作系统的审计机制提供了密码模块的下列事件的审计事件记录:

——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;

——将操作员添加或删除密码主管角色(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。

JY06.26.02:检测人员应运行提供审计事件记录的密码模块服务,和检查操作系统的审计日志,核实记录了密码模块的下列事件:

——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;

——将操作员添加或删除密码主管角色(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:检测人员不用检测由操作系统提供和送检单位识别的审计机制。

AY06.27:(安全级别 2)

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标识。

所需的送检文档

CY06.27.01:送检单位应提供操作系统文档描述被操作系统审计机制记录的所有操作系统事件。

所需的检测规程

JY06.27.01:检测人员应通过操作系统文档审查,核实文档描述的操作系统审计机制所提供和记录的操作系统事件包括:

——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;

——将操作员添加或删除密码主管角色(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标识。

JY06.27.02:检测人员应运行密码模块服务,核实操作系统的审计机制能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;

——将操作员添加或删除密码主管角色(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。

AY06.28:(安全级别 2)

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。

所需的送检文档

CY06.28.01:送检单位应提供操作系统文档描述如何配置操作系统以防止操作员,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。

所需的检测规程

JY06.28.01:检测人员应通过检查操作系统配置管理文档,核实文档描述了如何配置操作系统以防止操作员,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。

JY06.28.02:检测人员应正确配置操作系统以防止操作员,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。

JY06.28.03:检测人员应担任安全策略中给出的、拥有特权的操作员的角色,确认其能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。

JY06.28.04:检测人员应担任安全策略未给出的、不拥有特权的操作员角色,确认其不能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。

AY06.29:(安全级别 2)

无论密码模块是否在核准的工作模式下运行,应当只有配置成满足以上安全要求{*AS06.05～AS06.28*}的操作系统才符合该安全等级。

注:本条款不单独进行检测。作为 AY06.05～AY06.28 的一部分进行检测。

6.7 物理安全

6.7.1 物理安全实体

AY07.01:(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)。

所需的送检文档

CY07.01.01:送检文档中应描述模块使用的、适用的物理安全机制,模块中所有的硬件、软件、固件及数据(包括未经加密的加密密钥和未经加密的 CSP)均应受到保护。

所需的检测规程

JY07.01.01:检测人员应核实送检文档描述了模块使用的、适用的物理安全机制。

JY07.01.02:检测人员应核实所述的物理安全机制被实现。

AY07.02:(安全级别 1,2,3,4)

密码边界内的所有硬件、软件、固件、数据分量以及 SSP 应当受到保护。

注：本条款不单独进行检测。

AY07.03：(安全级别 1,2,3,4)

本条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。

AY07.04：(安全级别 1,2,3,4)

本条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。

AY07.05：(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：

——在上述企图行为之后，通过其留下的可见标志(例如，拆卸证据)，和/或

——在上述企图行为过程中。

注：本条款不单独进行检测。

AY07.06：(安全级别 1,2,3,4)

***{接 AY07.05}*并且密码模块应当立即采取恰当的措施保护 SSP。**

注：本条款不单独进行检测。

AY07.07：(安全级别 1,2,3,4)

***{物理安全}*文档应当按照*{GM/T 0028—2014 附录}*A.2.7 中规定的要求编写。**

注：本条款不单独进行检测。

6.7.2 通用物理安全要求

AY07.08：(安全级别 1,2,3,4)

下列要求*{AY07.09～AY07.13}*应当适用于所有密码模块物理实体。

注：本条款 AY07.09～AY07.13 的一部分进行检测。

AY07.09：(安全级别 1,2,3,4)

模块文档中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。

所需的送检材料

CY07.09.01：送检文档应按照 GM/T 0028—2014 中 7.7.1 的要求明确说明密码模块的物理实体，包括单芯片密码模块、多芯片嵌入式模块，或多芯片独立式模块。

所需的检测规程

JY07.09.01：检测人员应核实送检单位标识了密码模块的类型，它应是 GM/T0028—2014 中 7.7.1 定义的三种类型之一，单芯片密码模块，多芯片嵌入式密码模块，或多芯片独立式模块。检测人员应独立确定物理实体满足下述 3 种类型之一。三个物理实体的基本特点和常见例子概括如下：

——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，或者可以嵌入可能没有物理保护的外壳或其他模块中。这个单芯片由片装和外部输入/输出连接器组成，其中片装使用统一的外部材料如塑料或陶瓷包装。例如：单 IC 芯片、单 IC 芯片智能卡或者包含实现密码功能的单 IC 芯片的其他系统。

——多芯片嵌入式密码模块。特点：模块由两个或两个以上互相连接的 IC 芯片构成，并物理嵌入到其他产品或未被物理保护的外壳中。例如：适配器和扩展板。

——多芯片独立密码模块。特点：两个或两个以上互相连接的 IC 芯片嵌入到完全受到物理保护的外壳中。例如：加密路由器、安全无线电话和 USB 令牌。

JY07.09.02：检测人员应核实送检文档标明了模块应达到的安全级别。检测人员应独立确定模块实际满足的安全级别。

AY07.10:(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。

所需的送检文档

CY07.10.01:送检材料应明确说明检测到拆卸行为后,置零操作的响应时间。

所需的检测规程

JY07.10.01:检测人员应核实送检文档标明了检测到拆卸行为后的置零操作的响应时间。

JY07.10.02:检测人员应核实置零响应机制属实。

AY07.11:(安全级别 1,2,3,4)

***{如果模块包含的维护员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:被模块厂商或其他被授权个体访问),那么}*应当定义维护访问接口。**

所需的送检文档

CY07.11.01:送检文档应描述模块使用的维护访问接口。

所需的检测规程

JY07.11.01:检测人员应核实送检文档描述了维护访问接口。

JY07.11.02:检测人员应核实送检文档与实现一致。

AY07.12:(安全级别 1,2,3,4)

***{如果模块包含的维护员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:被模块厂商或其他被授权个体访问),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。**

所需的送检文档

CY07.12.01:送检文档应说明维护访问接口,包括任何封盖或门。

所需的检测规程

JY07.12.01:检测人员应核实送检文档提供了维护访问接口,包括任何封盖或门。

AY07.13:(安全级别 1,2,3,4)

***{如果模块包含的维护员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:被模块厂商或其他被授权个体访问),那么}*维护访问接口内包含的任何封盖或门应当使用适当的物理安全机制来进行安全保护。**

所需的送检文档

CY07.13.01:送检文档应说明维护访问接口,包括任何封盖或门。

所需的检测规程

JY07.13.01 检测人员应核实使用了合适的物理安全机制保护维护访问接口中所有的可拆除封盖和门。

AY07.14:(安全级别 1,2,3,4)

下列要求*{AY07.15～AY07.16}*应当适用于安全一级的所有密码模块。

注:本条款 AY07.15～AY07.16 的一部分进行检测。

AY07.15:(安全级别 1,2,3,4)

密码模块应当由产品级部件组成,这些产品级部件采用了标准钝化技术,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他物理损害。

所需的送检文档

CY07.15.01:模块应是一个标准的、产品级质量的 IC 芯片,并应达到商业级规范中对电源、温度、可靠性、震动和振动等的要求。模块应对于整个芯片使用标准钝化技术。送检材料中应说明 IC 芯片的质量。如果使用的芯片不是标准的设备,也应说明其钝化设计。

所需的检测规程

JY07.15.01：通过审查送检文档和检查模块，检测人员应核实模块包含由统一外部材料和标准连接器组成的标准集成电路。通过送检文档，检测人员应核实模块内的芯片在供电和电压范围、温度、可靠性、冲击和震动方面达到商业级别。

JY07.15.02：通过审查送检文档，检测人员应核实模块中应用了标准钝化。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的物理破坏。如果未使用标准钝化，文档中应提供相关信息以证明其等价于使用了标准钝化方法。

AY07.16：（安全级别 1，2，3，4）

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

注：本条款作为 AY07.10 的一部分进行检测。

AY07.17：（安全级别 2，3，4）

安全二级的所有密码模块应当满足下列要求*｛AY07.18～AY07.20｝*。

注：本条款作为 AY07.18～AY07.20 的一部分进行检测。

AY07.18：（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的拆卸证据（例如，在封盖、外壳或封条上）。

注：本条款作为单芯片实体进行检测，参考 AY07.34 和 AY07.35 的部分内容；

本条款作为多芯片嵌入式实体进行检测，参考 AY07.44 和 AY07.45 的部分内容；

本条款作为多芯片独立式实体进行检测，参考 AY07.62 和 AY07.63 的部分内容。

AY07.19：（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 400 nm～750 nm）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。

所需的送检文档

CY07.19.01：送检材料应明确说明拆卸存迹的材料、涂层或外壳在可见光范围内应为不透明或半透明的。

所需的检测规程

JY07.19.01：检测人员应通过审查送检文档和检查模块，核实拆卸存迹材料、涂层或外壳在可见光范围内是不透明或半透明的。

AY07.20：（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。

所需的送检文档

CY07.20.01：如果被封盖或外壳包含的模块含有任何通风孔或缝，则这些通风孔或缝应具有特殊的构造，从而防止通过直接观察外壳内部的构造或部件进行信息收集。送检文档应描述通风的物理设计方法。

所需的检测规程

JY07.20.01：通过审查送检文档和检查模块，检测人员应核实模块的封盖或外壳是否含有通风孔、缝或其他开口，如果有，则应核实其构造为可防止通过直接观察封盖或外壳内部的构造或部件进行信息收集。

AY07.21：（安全级别 3，4）

安全三级的所有密码模块应当满足下列要求*｛AY07.22～AY07.28｝*。

注：本条款不单独进行检测，作为 AY07.22～AY07.28 的一部分进行检测。

AY07.22：（安全级别 3，4）

如果模块含有任何门或封盖，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 AY07.13 的一部分进行检测；
本条款对于单芯片实体而言作为 AY07.38 的一部分进行检测；
本条款对于多芯片嵌入式实体而言作为 AY07.50 的一部分进行检测；
本条款对于多芯片独立式实体而言作为 AY07.62 的一部分进行检测。

AY07.23：(安全级别 3,4)

在打开门、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 AY07.13 的一部分进行检测；
本条款对于单芯片实体而言作为 AY07.38 的一部分进行检测；
本条款对于多芯片嵌入式实体而言作为 AY07.50 的一部分进行检测；
本条款对于多芯片独立式实体而言作为 AY07.62 的一部分进行检测。

AY07.24：(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运行状态。

注：本条款对于单芯片实体而言作为 AY07.38 的一部分进行检测；
本条款对于多芯片嵌入式实体而言作为 AY07.50 的一部分进行检测；
本条款对于多芯片独立式实体而言作为 AY07.65 的一部分进行检测。

AY07.25：(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的构造，从而防止未被检测到的对模块内部的物理探测(例如，防止使用单铰链探头探测)。

所需的送检文档

CY07.25.01：如果被封盖或外壳包含的模块含有任何通风孔或缝，则这些通风孔或缝的构造应能防止未被检测到的对模块内部的物理探测。送检文档应描述通风结构的物理设计方法。

所需的检测规程

JY07.25.01：通过审查送检文档和检查模块，检测人员应核实模块的封盖或外壳是否含有通风孔、缝或其他开口，如果有，则应核实其构造为可防止未被检测到的对模块内部的物理探测。

AY07.26：(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，坚固或硬质的保形或非保形的外壳、涂层或灌封材料应当维持强度和硬度特征。

所需的送检文档

CY07.26.01：送检文档应明确说明外壳的硬度，以及该硬度适用于该模块设计的原因。

所需的检测规程

JY07.26.01：通过模块审查送检文档和检查模块，检测人员应核实外壳与文档中描述的设计一致。

AY07.27：(安全级别 3,4)

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

所需的送检文档

CY07.27.01：如果使用了拆卸封条，送检单位应提供拆卸存迹封条的明确说明。

所需的检测规程

JY07.27.01：如果使用了拆卸封条，检测人员应核实拆卸封条如文档描述地被唯一编号或者能被独立识别。

AY07.28：(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 AY07.68 的一部分进行检测。

AY07.29：(安全级别 4)

安全四级的所有模块应当满足下列要求{*AY07.30～AY07.33*}。

注：本条款作为 AY07.30～AY07.33 的一部分进行检测。

AY07.30:(安全级别 4)

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

注:本条款对于单芯片实体而言作为 AY07.40 的一部分进行检测;

本条款对于多芯片嵌入式实体而言作为 AY07.52 的一部分进行检测;

本条款对于多芯片独立式实体而言作为 AY07.64 的一部分进行检测。

AY07.31:(安全级别 4)

密码模块应当具有 EFP 特性。

注:本条款作为 AY07.72 的一部分进行检测。

AY07.32:(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。

所需的送检文档

CY07.32.01:送检文档应明确指出防止错误注入攻击的保护机制。

所需的检测规程

JY07.32.01:检测人员应通过审查送检文档和检查模块核实每项保护机制属实。

AY07.33:(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{*GM/T 0028—2014*}附录 B 规定的要求进行记录。

所需的送检文档

CY07.33.01:送检文档应明确指出模块使用的错误注入缓解技术和缓解指标,并按照 GM/T 0028 附录 B 的要求进行记录。

所需的检测规程

JY07.33.01:检测人员应核实模块使用了如文档所述的错误注入缓解技术和缓解指标。

6.7.3 物理安全实体的物理安全要求

6.7.3.1 单芯片密码模块

注 1:除了 GM/T 0028—2014 的 7.7.2 中规定的通用安全要求,还针对单芯片密码模块规定了下列要求。

注 2:对安全一级的单芯片密码模块没有其他额外要求。

AY07.34:(安全级别 2,3,4)

安全二级的单芯片密码模块应当满足下列要求{*AY07.35*}。

注:本条款作为 AY07.35 的一部分进行检测。

AY07.35:(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)把密码模块覆盖起来,或者将模块装在一个拆卸存迹的外壳中,以阻止直接观察、探测或操控模块,并在企图拆卸或移动模块后留下证据。

注:此要求与 AY07.18 相关。

所需的送检文档

CY07.35.01:送检文档应说明防拆卸涂层及其特点。

所需的检测规程

JY07.35.01:通过审查送检文档和检查模块,检测人员应核实模块被防篡改涂层覆盖;通过检查,检察人员应核实防拆卸涂层完全覆盖模块,并且该涂层可防止对单芯片的直接观察、探测或操作。

AY07.36:(安全级别 3,4)

安全三级的单芯片密码模块应当满足下列要求{*AY07.37～AY07.39*}。

注：本条款在 AY07.37 或 AY07.38 中进行检测。

所需的送检文档

CY07.36.01：送检文档应声明 AY07.37 和 AY07.38 中说明的两种方法中哪一种用来满足这一要求。

所需的检测规程

JY07.36.01：检测人员应核实送检文档料中指定了 AY07.37 和 AY07.38 中的哪一种方法用于满足这一要求。

JY07.36.02：如果满足 AY07.37 中指定的方法，检测人员应遵循 JY07.37 中的检测程序；如果发现 AY07.38 方法，检测人员应遵循 AY07.38 中的检测程序。

AY07.37：(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)把模块覆盖起来。*{或满足 AY07.38 的要求}*。

所需的送检文档

CY07.37.01：送检文档应清晰描述在 AY07.34 中指定的方法被用于满足此要求。

CY07.37.02：送检材料应提供详细的设计信息，特别是涂层材料的种类和特性。

所需的检测规程

JY07.37.01：通过检查检测人员核实送检文档中说明了模块由坚固的不透明防拆卸涂层覆盖。

JY07.37.02：检测人员应核实送检材料文档充分描述了详细设计信息，特别是所用涂层的种类和特性。

JY07.37.03：检测人员应核实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。通过检查核实涂层完全覆盖模块，该涂层明显不透明，且能够阻止直接的观察、探测或操作。

AY07.38：(安全级别 3，4)

***{如果不满足 AY07.37 的要求}*应当实现模块的外壳。**

注：本条款不单独进行检测。在 AY07.39 中进行检测。

AY07.39：(安全级别 4)

***{接 AY07.38}*以致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。**

所需的送检文档

CY07.39.01：送检材料应提供详细的设计信息，特别是当模块封装含有任何门或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。

CY07.39.02：如果模块封装含有任何门或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门，并且在移除封盖或打开门之前，所有未经加密的 CSP 应清零。当未经加密的 CSP 包含在模块中，则电路应是运行的。

所需的检测规程

JY07.39.01：检测人员应核实送检文档详细说明了模块无论含有门或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门或封盖或定义的维护访问接口，则检测人员应核实送检文档说明了该模块含有拆卸响应和清零电路。

JY07.39.02：如果模块封装含有任何门或封盖或指定的维护访问接口，检测人员应核实送检文档说明了当封盖或门被移除，或维护访问接口被访问时，模块清零电路对所有未经加密的 CSP 清零。

JY07.39.03：通过审查送检文档和检查模块，检测人员应核实当模块中含有未经加密的 CSP 时，拆卸响应和清零电路保持运行。

JY07.39.04：通过审查送检文档和检查模块，检测人员核实在极可能导致对模块的严重损害不存在时，封装不会被移除或渗透。

JY07.39.05：如果模块封装含有任何门或封盖或指定的维护访问接口，则当封盖或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对所有未经加密的 CSP 清零。

JY07.39.06：检测人员应检测在极可能导致对模块的严重损害不存在时，封装不会被移除或渗透。

AY07.40：（安全级别 4）

安全四级的单芯片密码模块应当满足下列要求*{AY07.41～AY07.42}*。

注：本条款在 AY07.41～AY07.42 中进行检测。

AY07.41：（安全级别 4）

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

所需的送检文档

CY07.41.01：送检文档中应清晰核实使用的涂层的种类，并提供涂层材料的详细特性，特别是它的硬度和抗移除性。

CY07.41.02：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撬开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。

所需的检测规程

JY07.41.01：检测人员通过检查送检单位文档，应核实模块由坚固不透明的抗移除的涂层覆盖。

JY07.41.02：检测人员应核实模块涂层的抗移除特性。检测人员应尝试从模块剥落或撬开涂层材料，并核实在合理应用力量的情况下，模块停止工作或模块电路明显被物理破坏是不可能的。

AY07.42：（安全级别 4）

抗移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，即模块将不能工作。

所需的送检文档

CY07.42.01：送检文档应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。

所需的检测规程

JY07.42.01：检测人员应核实送检文档以确定模块抗移除涂层的溶解特性。

JY07.42.02：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 CY07.32.01 中提供的文档，确定什么类型的溶剂可威胁抗移除涂层。

6.7.3.2 多芯片嵌入式密码模块

注：除了 GM/T 0028—2014 中的 7.7.2 中规定的通用安全要求，还针对多芯片嵌入式密码模块规定了下列要求。

AY07.43：（安全级别 1，2，3，4）

如果密码模块被装在一个外壳或封盖中，那么应当使用产品级的外壳或封盖。

所需的送检文档

CY07.43.01：模块应整个包含在一个产品级的外壳或封盖中。送检文档应对外壳或封盖进行描述。

所需的检测规程

JY07.43.01：检测人员应核实送检文档中说明了模块包含在产品级的外壳或封盖中。

AY07.44：（安全级别 2，3，4）

安全二级的多芯片嵌入式密码模块应当满足下列要求*{AY07.45～AY07.48}*。

注：本条款不单独进行检测。

AY07.45：（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）把模块部件覆盖起来，以阻

止直接观察，并提供企图拆卸或移动模块部件的证据。*{或满足 AY07.46 的要求}*。

所需的送检文档

CY07.45.01：送检单位提供应提供坚固封装的设计文档。模块部件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）覆盖，以阻止直接观察并提供企图拆卸或移动模块部件的证据。

所需的检测规程

JY07.45.01：检测人员应核实送检文档说明了模块被不透明的、拆卸存迹的材料封装。

JY07.45.02：检测人员应通过测试，核实模块提供了拆卸或移除模块组件的尝试的迹象。

JY07.45.03：检测人员应尝试进入电路的内部核实封装的强度，以核实封装不能被轻易破坏。

JY07.45.04：检测人员应通过检测，以核实极大可能不会对模块造成严重损害的情况下封装是不能移除或渗透的。

AY07.46：（安全级别 2，3，4）

***{如果不满足 AY07.45 的要求}*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。**

所需的送检文档

CY07.46.01：送检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。

所需的检测规程

JY07.46.01：检测人员通过审查送检文档和检查模块，应核实模块包含于外壳中，该外壳满足如下要求：

a) 外壳完全包含整个模块。

b) 外壳材料必须在送检文档中定义。

c) 外壳必须是产品级的。送检文档必须展示相同材料的外壳在商业上已被应用或提供数据以展示它与商用产品是等价的。

AY07.47：（安全级别 2，3，4）

如果外壳包含任何门或封盖，则门或封盖应当使用带有物理或逻辑钥匙的防撬锁。*{或满足 AY07.48 的要求}*。

所需的送检文档

CY07.47.01：如果外壳包含任何门或封盖，则门或封盖应使用防撬锁锁住，送检文档应描述防撬机械锁及其物理的或逻辑的钥匙。

所需的检测规程

JY07.47.01：检测人员应核实送检文档描述了门或封盖由防撬机械锁锁定，该机械锁使用物理或逻辑钥匙。

JY07.47.02：检测人员应尝试在不用密钥的情况下打开锁定的门或封盖，并确定在没留下损坏痕迹的情况下不能打开门或封盖。

AY07.48：（安全级别 2，3，4）

***{如果不满足 AY07.47 的要求，则门或封盖}*应当被拆卸存迹的封条保护起来（例如，存迹胶带或全息封条）。**

所需的送检文档

CY07.48.01：送检文档应描述拆卸存迹的封印。

所需的检测规程

JY07.48.01：检测人员应通过审查送检文档和检查模块，核实门或封盖带有防拆卸封条保护（如证据胶带或全息封条）。

JY07.48.02：检测人员应核实在不破坏或不移除封条时门或封盖不能打开，且封条被移开后不能被

替代。

AY07.49:(安全级别 3,4)

下列要求{*AY07.50～AY07.51*}应当适用于安全三级的多芯片嵌入式密码模块。

注:本条款在 AY07.50～AY07.51 中进行检测。

AY07.50:(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)把密码模块内的多芯片实体电路覆盖起来。{*或满足 AY07.51 的要求*}。

所需的送检文档

CY07.50.01:送检材料应提供硬质涂料或灌封材料的设计文档。

CY07.50.02:送检材料应提供硬质涂料或灌封材料的不透明特性的相关文档。

所需的检测规程

JY 07.50.01:检测人员应核实送检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。

JY 07.50.02:通过审查送检文档和检查模块,检测人员应核实硬质涂料或灌封材料的不透明特性。

JY 07.50.03:通过审查送检文档和检查模块,检测人员应核实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)。

AY07.51:(安全级别 3,4)

***{如果不满足 AY07.51 的要求}*模块应当被封装在坚固的外壳内。**

所需的送检文档

CY07.51.01:送检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(即模块将不可运行)。

CY 07.51.02:如果外壳含有门或封盖,则密码模块应含有拆卸响应和置零电路。该电路应能持续检测这些封盖和门,并且在封盖移除和门被打开之前,所有的未经加密的 CSP 应置零。只要未经加密的 CSP 包含在模块中,则电路应运行。

所需的检测规程

JY07.51.01:检测人员需核实送检文档详细说明了外壳包含门或封盖,以及维护访问接口,并且模块须包含拆卸响应和置零电路。

JY07.51.02:如果外壳含有门或封盖,或指定的维护访问接口,则检测人员应核实送检文档详细说明了当门或封盖移除或维护访问接口被访问时模块对所有未经加密的 CSP 置零。

JY07.51.03:检测人员应核实送检文档详细说明了使用了上述两条中的哪一条,并提供设计文档。

JY07.51.04:通过审查送检文档和检查模块,检测人员应核实当模块中包含未经加密的 CSP 时,拆卸响应和置零电路保持运行。

JY07.51.05:通过审查送检文档和检查模块,检测人员应核实在极大可能不会对模块造成严重损害时,外壳是不能移除或渗透的。

JY07.51.06:通过尝试进入电路的内部确认外壳的强度,检测人员应核实外壳是不能被轻易破坏的。通过审查送检文档和检查模块,检测人员应核实外壳是不可移除的。

JY07.51.07:如果坚固外壳含有门或封盖,或维护访问接口被指定,检测人员应根据送检材料核实当移除门或封盖时,模块对所有未经加密的 CSP 进行置零。

JY07.51.08:如果外壳含有门或封盖,或维护访问接口被指定,检测人员应检测当移除门或封盖或维护访问接口被访问时,模块对所有未经加密的 CSP 进行置零。

JY07.51.09:检测人员应检测在极大可能不会对模块造成严重损害的情况下,外壳是不能被移除或渗透的。

AY07.52:(安全级别 4)

下列要求{*AY07.53～AY07.59*}应当适用于安全四级的多芯片嵌入式密码模块。

注：本条款在 AY07.53～AY07.59 中进行检测。

AY07.53:(安全级别 4)

密码模块部件应当封装在坚固或硬质的保形或非保形的外壳中。

所需的送检文档

CY07.53.01:模块须包含在一个拆卸探测外壳中,该防拆卸外壳监测对模块灌封材料或外壳的攻击。送检文档须描述该外壳的设计。

所需的检测规程

JY07.53.01:通过检查送检材料,检测人员应核实模块含有拆卸探测外壳且模块完全封装在该外壳内。此屏障的设计使得任何通过例如切割、钻孔、铣、磨碾或溶解的方式对模块组件的访问都能被模块中的监测组件检测到。

AY07.54:(安全级别 4)

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

注：本条款不单独进行检测。在 AY07.55 中进行检测。

AY07.55:(安全级别 4)

***{接 AY07.54}*该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。**

所需的送检文档

CY07.55.01:模块须包含在一个拆卸探测外壳中,该防拆卸外壳监测对模块灌封材料或外壳的攻击。送检文档须描述拆卸探测外壳的设计。

所需的检测规程

JY07.55.01:通过审查送检文档和检查模块,检测人员应核实送检模块拆卸探测外壳,且模块完全封装在该外壳内。此屏障的设计使得任何通过例如切割、钻孔、铣、磨碾或溶解的方式访问模块组件都能被模块中的监测组件检测到。

AY07.56:(安全级别 4)

密码模块应当包含拆卸响应和置零电路。

注：本条款不单独进行检测。在 AY07.57 和 AY07.58 中进行检测。

AY07.57:(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。

所需的送检文档

CY07.57.01:密码模块应包含拆卸响应和置零电路,该电路应持续地监测拆卸探测外壳,一旦检测到拆卸行为,须对所有未经加密的 CSP 进行置零。当模块内含有未经加密的 CSP 时,置零电路应持续运行。送检文档应描述拆卸响应和置零电路的设计。

所需的检测规程

JY07.57.01:通过审查送检文档和检查模块,检测人员应核实模块含有拆卸响应和置零电路,且该电路不断地监测拆卸探测外壳;抵御通过各种方式的攻击,例如切割、钻孔、铣、磨或溶解外壳任一部分;并且置零所有未经加密的 CSP。

AY07.58:(安全级别 4)

***{接 AY07.57}*并且一旦检测到拆卸行为就应当立即置零所有未受保护的 SSP。**

所需的送检文档

CY07.58.01:模块须包含拆卸响应和置零电路,该电路应不断监测拆卸探测外壳,并且一旦检测到

拆卸行为，须对所有未经加密的 CSP 进行置零。送检文档应描述拆卸响应和置零电路的设计。

所需的检测规程

JY07.58.01：检测人员应破坏拆卸探测外壳屏障，并核实模块对所有未受保护的 CSP 进行清零。

AY07.59：（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运行状态。

所需的送检文档

注： 本条款不单独进行检测。

6.7.3.3 多芯片独立式密码模块

注： 除了 GM/T 0028—2014 的 7.7.2 中规定的通用安全要求，针对多芯片独立式密码模块还规定了下列要求。

AY07.60：（安全级别 1，2，3，4）

密码模块应当整个被封装在金属或硬质塑料的产品级外壳内，外壳可以包括门或封盖。

所需的送检文档

CY07.60.01：密码模块应完全包含于金属的或坚硬塑胶的产品级封装内，该封装可能包含门或封盖。送检文档应描述封装及其硬度特性。

所需的检测规程

JY07.60.01：通过审查送检文档和检查模块，检测人员应核实模块包含在外壳中，该外壳满足如下要求：

a) 模块应完全包含于外壳中。

b) 外壳材料必须是在送检文档中定义的成分。

c) 外壳必须是产品级的。送检文档必须说明相同材料的外壳在商业上已被应用，或提供数据以表明它与商用产品等价。

AY07.61：（安全级别 2，3，4）

安全二级的多芯片独立式密码模块应当满足下列要求*｛AY07.62～AY07.63｝*。

注： 本条款在 AY07.62 或 AY07.63 中进行检测。

AY07.62：（安全级别 2，3，4）

如果密码模块的外壳含有任何门或封盖，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。*｛或满足 AY07.63 的要求｝*。

所需的送检文档

CY07.62.01：如果外壳包含门或封盖，则它们须被由物理的或逻辑钥匙可打开的防撬机械锁锁定。送检文档应描述由物理的或逻辑的钥匙可打开的防撬机械锁机制。

所需的检测规程

JY07.62.01：检测人员应核实外壳是否含有门或封盖。检测人员应核实每个门或封盖被由物理的或逻辑密钥可打开的防撬机械锁锁定。检测人员应尝试在没有密钥的情况下打开锁定的门或封盖，以核实在没有损害痕迹的情况下门或封盖是不能打开的。

AY07.63：（安全级别 2，3，4）

***｛如果不满足 AY07.62 的要求，则门或封盖｝*应当使用拆卸存迹的封条（例如，存迹胶带或全息封条）进行保护。**

所需的送检文档

CY07.63.01：如果外壳通过例如证据胶带或全息封条的防篡改封条保护，送检文档应描述防篡改封条。

所需的检测规程

JY07.63.01：门或封盖通过例如证据胶带或全息封条的防篡改封条保护。检测人员应核实在没有

破坏或移除封条的情况下门或封盖不能打开，且封条不能移除后被替代。

AY07.64：（安全级别 3，4）

安全三级的多芯片独立密码模块应当满足下列要求{*AY07.65*}。

注：本条款在 AY07.65 中进行检测。

AY07.65：（安全级别 3，4）

模块应当被封装在坚固的外壳内，以致企图移除或穿透外壳的行为将极有可能对模块造成严重损害，即模块将不能工作。

所需的送检文档

CY07.65.01：送检文档应提供坚固外壳的设计文档。模块须完全包含在坚固外壳中。外壳设计须满足如下要求：移除外壳极可能对模块的内部电路造成严重的损害（例如：模块将不能工作）。

CY07.65.02：如果外壳含有门或封盖，则密码模块须含有拆卸响应和置零电路。该电路应持续地检测这些封盖和门，并且在封盖移除和门被打开之前，应置零所有的未经加密的 CSP。只要模块中包含未经加密的 CSP，电路就应该运行。

所需的检测规程

JY07.65.01：检测人员应核实：送检文档详细说明了无论封装包含门或封盖还是维护访问接口，模块须包含拆卸响应和置零电路。

JY07.65.02：如果外壳含有门或封盖，或指定的维护访问接口，则检测人员应核实送检单位文档详细说明了当门或封盖移除或维护访问接口被访问时模块对所有未经加密的 CSP 进行置零。

JY07.65.03：检测人员应核实送检文档详细说明了在 CY05.43.01 和 CY05.43.02 中实现哪个安全选项并提供设计文档。

JY07.65.04：检测人员应通过审查送检文档和检查模块，核实当未经加密的 CSP 包含在模块中时，拆卸响应和置零电路保持运行。

JY07.65.05：检测人员应通过审查送检文档和检查模块，核实在极大可能不会对模块造成严重损害时外壳是不能移除或渗透的。

JY07.65.06：通过尝试进入电路的内部，检测人员应核实外壳的强度，以证明外壳不能被轻易破坏。通过检查送检材料，检测人员应核实封装是不可移除的。

JY07.65.07：如果坚固外壳含有门或封盖，或者维护访问接口被指定时，检测人员应通过审查送检文档和检查模块，核实当移除门或封盖时，模块对所有未经加密的 CSP 置零。

JY07.65.08：如果封装含有门或封盖，或者维护访问接口被指定时，检测人员应检测当移除门或封盖或维护访问接口被访问时，模块对所有未经加密的 CSP 置零。

JY07.65.09：检测人员应检测在极大可能不会对模块造成严重损害时，外壳不能移除或渗透。

AY07.66：（安全级别 4）

安全四级的多芯片独立式密码模块应当满足下列要求{*AY07.67～AY07.72*}。

注：本条款在 AY07.67～AY07.72 中进行检测。

AY07.67：（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，拆卸检测机制包括：封盖开关（如微型开关、磁霍尔效应开关、永磁驱动器等）、动作探测器（如超声波、红外线或微波）或者{*GM/T 0028—2004*}7.7.3.2 中规定的安全四级描述的其他拆卸检测机制。

所需的送检文档

CY07.67.01：封装或灌封材料须使用拆卸探测机制的拆卸探测外壳进行封装。送检文档应描述拆卸探测外壳的设计机制。

所需的检测规程

JY07.67.01：通过检查送检材料，检测人员应核实模块封装或灌封材料包含拆卸探测机制，并通过

该机制保护模块组件。该机制的设计可以监测到任何通过破坏封装或灌封材料对模块组件的访问。

AY07.68:(安全级别 4)

拆卸检测机制应当能够对企图访问 SSP 的攻击做出响应,诸如切、钻、铣、磨、烧、熔、溶解等。

注:本条款作为 AY07.71 的一部分进行检测。

AY07.69:(安全级别 4)

密码模块应当包含拆卸响应和置零电路。

注:本条款作为 AY07.71 的一部分进行检测。

AY07.70:(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。

注:本条款作为 AY07.71 的一部分进行检测。

AY07.71:(安全级别 4)

***{接 AY07.70}*并且一旦检测到拆卸行为就应当立即置零所有未受保护的 SSP。**

所需的送检文档

JY07.71.01:密码模块应包含拆卸响应和置零电路,该电路应持续监测拆卸检测外壳,并且一旦检测到拆卸行为须立即置零所有未经加密的 CSP。当模块中包含未经加密的 CSP 时,拆卸响应及置零电路应持续运行。送检文档应描述拆卸响应和置零电路的设计。

所需的检测规程

JY07.71.01:检测人员确认送检文档说明了密码模块包含拆卸响应和置零电路,该电路应持续监测拆卸检测外壳;探测通过各种方式的攻击,例如:切割、钻孔、铣、磨或溶解外壳的任一部分;并且置零所有未经加密的 CSP。

JY07.71.02:检测人员应破坏拆卸检测外壳屏障,并确认模块对未经加密的 CSP 置零。

AY07.72:(安全级别 4)

当密码模块内包含未受保护的 SSP 时,拆卸响应和置零电路应当保持运行状态。

注:本条款作为 AY07.71 的一部分进行检测。

6.7.4 环境失效保护/测试

6.7.4.1 环境失效保护/测试通用要求

AY07.73:(安全级别 3,4)

安全三级的模块应当具有 EFP 特性或经过 EFT。

所需的送检文档

CY07.73.01:送检单位使用下述中的一种:

——EFP 特征;或

——EFT。

正如在 GM/T 0028—2014 的 7.7.4 中指出,确保如下四种异常环境状况或超出了模块常规运行范围的波动(意外的或有意的)将不会危及模块的安全:

——低温;

——高温;

——大负电压;

——大正电压。

送检单位应选择为每种条件使用 EFP 或 EFT,但是每个选择相对于其他条件的选择是独立的。送检单位应为每个条件提供相应的配套文档,指出选择的方法是如何使用的。

所需的检测规程

JY07.73.01:检测人员应核实送检文档声明了每个条件的 EFP/EFT 选择,以及指定方法如何

使用。

AY07.74:(安全级别 4)

安全四级的模块应当有 EFP 特性。

注：本条款在 AY07.75～AY07.77 中进行检测。

6.7.4.2 环境失效保护特性

AY07.75:(安全级别 3,4)

EFP 特性应当保护密码模块,防止由于故意或超出模块正常运行范围,对模块的安全性造成破坏。

注：本条款作为 AY07.77 的一部分检测。

AY07.76:(安全级别 3,4)

密码模块应当对超出阐明的正常运行的温度和电压范围进行监控并做出正确响应。

注：本条款作为 AY07.77 的一部分检测。

AY07.77:(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

——立即置零所有未受保护的 SSP。

所需的送检文档

CY07.77.01: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

——清零所有明文的 SSP。

文件应声明哪种方法被选择,并且提供在模块内执行 EFP 功能的详细说明。

所需的检测规程

JY07.77.01:检测人员应设置环境条件(周围的温度和电压)接近于模块正常运行时指定取值范围内的极值,并且核实模块在正常的运行参数中持续运行。

JY07.77.02:检测人员应扩大温度和电压范围至指定的正常范围之外,并核实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。

JY07.77.03: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,则检测人员应执行需要密钥的任务以核实模块自身不能完成那些任务。

6.7.4.3 环境失效测试程序

AY07.78:(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(故意的或意外的)而遭到破坏。

注：本条款作为 AY07.81 的一部分检测。

AY07.79、AY07.80:(安全级别 4)

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

注：本条款作为 AY07.81 的一部分检测。

AY07.81:(安全级别 4)

温度范围应当按照下列方式测试:从正常运行温度范围内下降到最低温度,此时要么模块关闭防止继续运行,要么立即置零所有未受保护的 SSP;并且应从正常运行温度范围内上升到最高温度,此时要

么模块关闭防止继续运行，要么立即置零所有未受保护的 SSP。

所需的送检文档

CY07.81.01：如果 EFP 在特定条件下使用，模块应在 AY07.82 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

——置零所有未经加密的 SSP。

文档应描述选择的方法，并且提供对 EFT 的详细描述。

所需的检测规程

JY07.81.01：检测人员应按照 AY07.82 的要求说明配置环境条件（周围的温度和电压），并核实模块要么继续正常运行，要么停止以阻止进一步操作，要么置零所有未经加密的 CSP。

JY07.81.02：如果模块的设计可置零所有未经加密的 SSP，并且在恢复正常环境条件后模块仍然运行，则检测人员应完成需要密钥的任务以核实模块自身不能完成这些任务。

AY07.82：（安全级别 4）

温度的测试范围应当为－100 ℃～＋200 ℃。

注：本条款作为 AY07.81 的一部分检测。

AY07.83：（安全级别 4）

***{接 AY07.82}*而且，一旦模块被关闭以防止继续运行，或所有未受保护的 SSP 被立即置零，或模块进入故障模式，则测试应当立即中断。**

注：本条款作为 AY07.81 的一部分检测。

AY07.84：（安全级别 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。

注：本条款作为 AY07.81 的一部分检测。

AY07.85：（安全级别 4）

电压范围应当按照下列方式测试：逐渐从正常运行电压范围内下降到最低电压，此时要么模块关闭防止继续运行，要么立即置零所有未受保护的 SSP。

注：本条款作为 AY07.81 的一部分检测。

AY07.86：（安全级别 4）

***{接 AY07.85}*并且应当逐渐从正常运行电压范围内上升到最高电压，此时要么模块关闭防止继续运行，要么立即置零所有未受保护的 SSP。**

注：本条款作为 AY07.81 的一部分检测。

6.8 非入侵式安全

AY08.01：（安全级别 1，2，3，4）

如果由密码模块实现、用于保护模块 CSP 的非入侵式攻击的缓解技术不在*{GM/T 0028—2014}*附录 F 中，则这些技术应当满足*{GM/T 0028—2014}*7.12 中规定的要求。

所需的送检文档

注：本条款不单独进行检测。作为 AY12.01～AY12.04 的一部分进行检测。

AY08.02：（安全级别 1，2，3，4）

如果由密码模块实现、用于保护模块 CSP 的非入侵式攻击的缓解技术在*{GM/T 0028—2014}*附录 F 中，则这些技术应当满足下列要求*{AY08.03～AY08.08}*。

注：本条款不单独进行检测。

AY08.03:(安全级别 1,2,3,4)

***{非入侵式安全}*文档应按照*{GM/T 0028—2014 附录}*A.2.8 中规定的要求编写。**

所需的送检文档

CY08.03.01:送检单位提供的文档应按照 GM/T 0028—2014 附录 A.2.8 中规定的要求编写。

所需的检测规程

JY08.03.01:检测人员应核实送检单位提供的文档按照 GM/T 0028—2014 附录 A.2.8 中规定的要求编写。

AY08.04:(安全级别 1,2,3,4)

文档中应当阐明用于保护模块 CSP 免受*{GM/T 0028—2014}*附录 F 中的所有非入侵式攻击的缓解技术。

所需的送检文档

CY08.04.01:送检单位应提供文档详细说明用于保护模块 CSP 免受所有非入侵式攻击的缓解技术。

所需的检测规程

JY08.04.01:检测人员应核实文档说明了用于保护模块 CSP 免受 GM/T 0028—2014 附录 F 中指定的所有非入侵式攻击的缓解技术。

AY08.05:(安全级别 1,2,3,4)

如果有相应措施,文档应当包括可以证明每个缓解技术有效性的证据。

所需的送检文档

CY08.05.01:送检单位应在文档中详细说明每个缓解技术的有效性。

所需的检测规程

JY08.05.01:检测人员应核实送检单位的文档中详细说明了每个缓解技术的有效性。

AY08.06:(安全级别 3)

密码模块应当实现用于保护 CSP 免受*{GM/T 0028—2014}*附录 F 中的所有非入侵式攻击的缓解技术。

所需的送检文档

CY08.06.01:送检单位的文档中应说明密码模块实现了用于保护 CSP 免受 GM/T 0028—2014 附录 F 中的所有非入侵式攻击的缓解技术。

所需的检测规程

JY08.06.01:检测人员应核实送检单位的文档中说明密码模块实现了用于保护 CSP 免受 GM/T 0028—2014 附录 F 中的所有非入侵式攻击的缓解技术。

AY08.07:(安全级别 3)

文档应当包括可以证明每个缓解技术有效性的证据,并提供测试方法。

所需的送检文档

CY08.07.01:送检单位应在文档中详细说明每个缓解技术的有效性。

CY08.07.02:送检单位应在文档中描述缓解技术有效性的测试方法。

所需的检测规程

JY08.07.01:检测人员核实送检单位的文档中详细说明了每个缓解技术的有效性。

JY08.07.02:检测人员应根据文档中描述的测试方法对每个缓解技术的有效性进行验证。

AY08.08:(安全级别 4)

密码模块应当接受测试以满足核准的非入侵式攻击缓解测试指标的要求。

所需的送检文档

CY08.08.01:送检单位应提交文档以说明密码模块使用的非入侵式攻击缓解方法。

所需的检测规程

JY08.08.01：检测人员应核实密码模块使用的非入侵式攻击缓解方法满足核准的非入侵式攻击缓解测试指标的要求。

6.9 敏感安全参数管理

6.9.1 敏感安全参数管理通用要求

AY09.01：（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。

所需的送检文档

CY09.01.01：送检单位的文档应描述模块内所有 CSP 的保护措施，包括防止非授权的访问、使用、泄露、修改和替换的实现机制。

所需的检测规程

JY09.01.01：检测人员应检查送检单位的文档描述了对 CSP 的保护。检测人员应核实文档如何使 CSP 免遭未经授权的访问、使用、泄露、修改和替换。

JY09.01.02：检测人员应（绕开文档描述的保护机制）尝试非授权访问 CSP，以查看模块拒绝访问。

JY09.01.03：检测人员应尝试使用送检材料中任何未说明的方法修改 CSP。

AY09.02：（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。

所需的送检文档

CY09.02.01：送检单位的文档中应描述防止所有 PSP 被未经授权的修改和替换的保护措施。

所需的检测规程

JY09.02.01：检测人员应核实送检单位的文档中描述的 PSP 是如何被保护以免受到未经授权的修改和替换。

JY09.02.02：检测人员应使用送检文档中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。

AY09.03：（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 相应的实体（即人、组、角色或进程）关联起来。

所需的送检文档

CY09.03.01：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。

所需的检测规程

JY09.03.01：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）的关联关系与文档描述的一致。

JY09.03.02：对于输入模块，检测人员先以正确的实体输入 SSP，模块应能正确输入；然后以错误的实体输入 SSP，模块应拒绝输入。

JY09.03.03：对于输出模块，检测人员先以正确的实体输出 SSP，模块应能正确输出；然后以错误的实体输出 SSP，模块应拒绝输出。

AY09.04：（安全级别 1,2,3,4）

口令的杂凑值、随机比特生成器状态信息和密钥生成的中间值应当被视为受保护的 CSP。

所需的送检文档

CY09.04.01：送检单位提交的文档中应描述如何保护口令的杂凑值、随机比特生成器状态信息和

密钥生成的中间值。

所需的检测规程

JY09.04.01:检测人员应核实文档中描述的保护方法有效。

JY09.04.02:检测人员应尝试获取口令的杂凑值、随机比特生成器状态信息和密钥生成的中间值。

AY09.05:(安全级别 1,2,3,4)

***{敏感安全参数管理}*文档应当按照*{GM/T 0028—2014 附录}*A.2.9 中规定的要求编写。**

所需的送检文档

CY09.05.01:送检单位提交的有关 SSP 管理的文档。

所需的检测规程

JY09.05.01:检测人员应核实文档按照 GM/T 0028—2014 的 A.2.9 中规定的要求编写。

6.9.2 随机比特生成器

AY09.06:(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,则核准的随机比特生成器应当用于提供这些值。

所需的送检文档

CY09.06.01:送检单位应提供用于核准的安全功能的所有 RBG 的清单,密码模块内 SSP 生成或 SSP 建立方法和它们的用途。

CY09.06.02:送检材料应描述核准的安全功能、SSP 生成或 SSP 建立所使用的随机数均由核准的随机比特生成器产生。

所需的检测规程

JY09.06.01:检测人员应核实文档描述了所有用于核准的安全功能、SSP 生成、SSP 建立所需的随机数,以及它们的使用方法。

JY09.06.02:检测人员应核实用于核准的安全功能、SSP 生成或 SSP 建立所使用的随机数均由核准的随机比特生成器产生。

AY09.07:(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视为 CSP。

所需的送检文档

CY09.07.01:如果熵是从模块密码边界外部收集的,送检单位提交的文档中应说明使用该熵作为输入所生成的数据流被视为 CSP。

所需的检测规程

JY09.07.01:如果熵是从模块密码边界外部收集的,检测人员应核实使用该熵作为输入所生成的数据流被视为 CSP。

AY09.08:(安全级别 1,2,3,4)

无论熵从密码边界内部还是外部收集,对于任何一个 CSP,其最小熵值应当不小于 256 比特。

所需的送检文档

CY09.08.01:无论熵从密码边界内部还是外部收集,送检单位的文档中应说明对于任何一个 CSP,其最小熵值不小于 256 比特。

所需的检测规程

JY09.08.01:无论熵从密码边界内部还是外部收集,检测人员应核实对于任何一个 CSP,其最小熵值不小于 256 比特。

AY09.09:(安全级别 1,2,3,4)

如果熵从内部收集,还应当描述随机比特的产生原理。

所需的送检文档

CY09.09.01：如果熵从内部收集，送检单位的文档中应描述随机比特的产生原理。

所需的检测规程

JY09.09.01：如果熵从内部收集，检测人员应核实送检单位的文档中描述了随机比特的产生原理。

6.9.3 敏感安全参数的生成

AY09.10：（安全级别 1，2，3，4）

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

所需的送检文档

CY09.10.01：送检单位的文档中应提供依据表明破坏 SSP 生成方法的安全性（例如，猜测用于初始化确定性随机比特生成器的种子值）应当至少与猜测已生成的 SSP 值的代价相当。

所需的检测规程

JY09.10.01：检测人员应核实送检单位的文档中提供了依据表明破坏 SSP 生成方法的安全性（例如，猜测用于初始化确定性随机比特生成器的种子值）至少与猜测已生成的 SSP 值的代价相当。

JY09.10.02：检测人员应核实送检单位提供的依据的准确性。举证责任在送检单位，如果有任何不确定性或模糊性，检测人员应要求送检单位出示所需的进一步信息。

AY09.11：（安全级别 1，2，3，4）

密码模块应当使用《*GM/T 0028—2014*》附录 D 中的核准的生成方法来生成 SSP，即该 SSP 使用核准的随机比特生成器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。

所需的送检文档

CY09.11.01：送检单位提交的文档应列出所有的 SSP 以及它们的用处，这些 SSP 或者是核准的 RBG 的输出、或者是用于核准的安全功能的输入到模块的 SSP 衍生、或者是用于密码模块的 SSP 建立方法。

所需的检测规程

JY09.11.01：检测人员应核实文档列出所有的 SSP 以及它们的用处，这些 SSP 或者是核准的 RBG 的输出、或者是用于核准的安全功能的输入到模块的 SSP 衍生、或者是用于密码模块的 SSP 建立方法。

6.9.4 敏感安全参数的建立

AY09.12：（安全级别 1，2，3，4）

自动的 SSP 建立应当使用《*GM/T 0028—2014*》附录 D 中的核准的方法。

所需的送检文档

CY09.12.01：送检单位提交的文档中应列出所有自动 SSP 的建立方法及其用途。

所需的检测规程

JY09.12.01：检测人员应核实文档列出了所有自动 SSP 的建立方法及其用途。

JY09.12.02：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—2014 附录 D 中的核实的方法。

AY09.13：（安全级别 1，2，3，4）

手动的 SSP 建立应当满足《*GM/T 0028—2014*》7.9.5 中规定的要求。

注：本条款作为 AY09.14～AY09.26 的一部分进行检测。

6.9.5 敏感安全参数的输入和输出

AY09.14:(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—2014*}7.3.2 中规定的已定义的 HMI、SFMI、HFMI 或 HSMI 接口。

注:本条款作为 AY03.04～AY03.14 的一部分进行检测。

AY09.15:(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。

所需的送检文档

CY09.15.01:送检单位提交的文档中应描述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)。

CY09.15.02:送检单位提交的文档中应描述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)的加密方法。

所需的检测规程

JY09.15.01:检测人员应核实文档中描述了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)。

JY09.15.02:检测人员应核实文档中描述了用于输入模块和从模块输出的受密码技术保护的 SSP 的加密方法。

JY09.15.03:检测人员应核实输入模块或从模块输出的用于受密码技术保护的 SSP 的加密方法是否使用了核准的安全功能。

AY09.16:(安全级别 1,2,3,4)

如果加密的 SSP 直接输入到模块,则 SSP 的明文值不应当显示出来。

所需的送检文档

CY09.16.01:对于加密的 SSP,文档中的 SSP 输入机制不应显示它们的明文值。

所需的检测规程

JY09.16.01:检测人员应核实文档中的 SSP 输入机制在加密的 SSP 输入过程中不显示它们的明文值。

JY09.16.02:检测人员应输入所有加密的 SSP,以核实没有 SSP 的明文显示。

AY09.17:(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—2014*}7.10.3.5 中规定的手动输入条件自测试进行验证,以保证准确度。

注:本条款作为 AY10.41～AY10.45 的一部分进行检测。

AY09.18:(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。

所需的送检文档

CY09.18.01:如果模块输出任何明文 CSP,送检单位的文档应描述这种输出服务。

CY09.18.02:对于明文 CSP 的输出,有限状态模型图以及其他的送检材料应说明该输出需要两个独立的内部操作。

所需的检测规程

JY09.18.01:检测人员应通过材料审核或有限状态模型核实模块允许明文 CSP 输出。

JY09.18.02:检测人员应通过有限状态模型和其他文档核实密码模块输出明文 CSP 是否需要两个独立的内部操作。

JY09.18.03：检测人员应在模块没有执行两个独立的内部操作的情况下尝试输出明文 CSP。如果模块允许如此行为，则模块未通过检测。

AY09.19：（安全级别 1，2，3，4）

***{接 AY09.18}*这两个独立的内部操作应当专门用于共同控制 CSP 的输出。**

注：本条款不单独进行检测，在 AY09.18 中进行检测。

AY09.20：（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。

所需的送检文档

CY09.20.01：如果模块通过无线接口输入或输出 CSP、密钥分量和鉴别数据，送检单位的文档应描述无线服务。

CY09.20.02：如果模块通过无线接口输入或输出 CSP、密钥分量和鉴别数据，送检文档应描述对 CSP、密钥分量和鉴别数据的加密方法。

所需的检测规程

JY09.20.01：检测人员应确认模块是否通过无线接口输入或输出 CSP、密钥分量和鉴别数据。

JY09.20.02：检测人员应核实使用了核准的加密方法加密 CSP、密钥分量和鉴别数据。

AY09.21：（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—2014}* 7.6.3 中规定的要求。

所需的送检文档

CY09.21.01：送检单位提交的文档中应描述软件部件中 CSP、密钥分量和鉴别数据输入或输出的方法。

CY09.21.02：送检单位提交的文档中应描述 CSP、密钥分量和鉴别数据的输入或输出应只保留在该运行环境中。

CY09.21.03：送检单位的文档中应说明 CY09.19.01 提到的运行环境满足 GM/T 0028—2014 7.6.3 中规定的要求。

所需的检测规程

JY09.21.01：检测人员应核实 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。

JY09.21.02：检测人员应核实运行环境是否满足 GM/T 0028—2014 7.6.3 中规定的要求。

AY09.22：（安全级别 3，4）

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。

注：本条款作为 AY09.15 或 AY03.16～AY03.22 的一部分进行检测。

AY09.23：（安全级别 3，4）

作为 CSP，明文形式的对称密钥和私钥应当使用知识拆分过程，并使用可信信道输入或输出模块。

所需的送检文档

CY09.23.01：送检单位提交的文档中应描述明文形式的对称密钥和私钥知识拆分过程，并使用可信信道输入或输出模块。

所需的检测规程

JY09.23.01：检测人员应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。

JY09.23.02：检测人员应核实知识拆分过程将密钥拆分成多个密钥分量，并且每个密钥分量未单独包含原密钥信息。

JY09.23.03：对于安全三级，检测人员应核实在 AY03.16～AY03.21 的可信信道，对于安全四级，检

测人员应核实在 AY03.22 的可信信道。

AY09.24:(安全级别 3)

如果模块使用了知识拆分过程,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。

所需的送检文档

CY09.24.01:送检单位提交的文档中应描述每个密钥分量使用了基于身份的鉴别。

所需的检测规程

JY09.24.01:检测人员应核实模块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。

AY09.25:(安全级别 3)

*{接 AY09.24}*而且应当至少需要两个密钥分量来重建原来的密钥。

所需的送检文档

CY09.25.01:送检单位提交的文档中应说明构建原来的 CSP 所需要的密钥分量。

所需的检测规程

JY09.25.01:检测人员应通过送检文档核实,在知识拆分过程时至少需要两个密钥分量来构建原来的 CSP。

JY09.25.02:检测人员应核实在知识拆分的情况下输出 CSP,不会导致可用于构建原来的 CSP 的单个分量的输出。

AY09.26:(安全级别 4)

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。

所需的送检文档

CY09.26.01:送检单位提交的文档中应说明每个密钥分量使用了基于身份的多因素操作员鉴别。

所需的检测规程

JY09.26.01:检测人员应核实多因素鉴别符合 AY04.59 的要求。

6.9.6 敏感安全参数的存储

AY09.27:(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。

所需的送检文档

CY09.27.01:送检单位提交的文档中应描述在密钥存储时,每个密钥与相应的实体正确关联的机制。

所需的检测规程

JY09.27.01:检测人员核实 SSP 的存储与相应的实体(例如,操作员、角色或进程)正确关联。

JY09.27.02:检测人员应修改密钥和实体的关联关系,并尝试运行密码功能,确定这些功能不能正常运行。

AY09.28:(安全级别 1,2,3,4)

应当禁止非授权操作员访问明文 CSP。

注:本条款在 AY09.01 中进行检测。

AY09.29:(安全级别 1,2,3,4)

应当禁止非授权操作员修改 PSP。

所需的送检文档

CY09.29.01:送检单位提交的文档中应说明禁止非授权操作员修改 PSP。

所需的检测规程

JY09.29.01：检测人员应核实送检单位的文档是否说明了禁止非授权操作员修改 PSP。

JY09.29.02：检测人员应以非授权角色，尝试修改密码模块中存储的 PSP，并确认该尝试失败。

6.9.7 敏感安全参数的置零

AY09.30：（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。

注：本条款在 AY09.01 中进行检测。

AY09.31：（安全级别 1，2，3，4）

SSP 被置零之后应当无法从模块中恢复和重用。

所需的送检文档

CY09.31.01：送检单位的文档应详细说明如何确保 SSP 被置零之后无法从模块中恢复。

所需的检测规程

JY09.31.01：检测人员应核实送检单位提供的原理的准确性。送检单位负责提供相关证明；如果有任何不确定或模糊之处，检测人员应要求送检单位提供需要的附加信息。

AY09.32：（安全级别 2，3，4）

密码模块应当对未受保护的 SSP 执行置零（例如，使用全 0 或全 1 或随机数据覆盖）。

所需的送检文档

CY09.32.01：送检单位文档应详细说明以下 SSP 置零信息：

——置零技术；

——约束（当明文 SSP 能被置零时）；

——置零的明文 SSP；

——未置零的明文 SSP 和原理；

——说明如何在危害明文 SSP 之前执行置零技术。

所需的检测规程

JY09.32.01：检测人员应核实送检单位的文档满足了 CY09.30.01 的要求。检测人员应核实送检单位提供的基本原理的准确性。送检单位负责提供相关证明；如果有任何不确定或模糊之处，检测人员应要求送检单位提供需要的附加信息。

JY09.32.02：检测人员应核实送检单位的文档满足了 CY09.30.01 的要求。检测人员应核实送检单位提供的基本原理的准确性。送检单位负责提供相关证明；如果有任何不确定或模糊之处，检测人员应要求送检单位提供需要的附加信息。

JY09.32.03：检测人员应核实模块中有哪些密钥可初始化置零指令。置零指令完成之后，检测人员应尝试用存储在模块中的每一个明文 SSP 执行密码操作。检测人员应核实所有明文 SSP 都不可访问。

JY09.32.04：检测人员应初始化置零指令，确认可在危害明文 SSP 之前执行密钥销毁。

JY09.32.05：检测人员应核实不能被置零指令置零的所有明文 SSP 是经过核准的算法加密的，或受其他经审验的嵌入式模块（满足 GM/T 0028—2014 要求）在逻辑或物理上保护的。

AY09.33：（安全级别 2，3，4）

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。

所需的送检文档

CY09.33.01：送检文档中应描述对未受保护的 SSP 置零的方法。

所需的检测规程

JY09.33.01：检测人员应核实不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。

AY09.34:(安全级别 2,3,4)

临时 SSP 在使用完毕之后应当被置零。

所需的送检文档

CY09.34.01:送检单位文档应明确说明临时 SSP 在使用完毕之后被置零。

所需的检测规程

JY09.34.01:检测人员应核实送检单位的文档是否说明了临时 SSP 在使用完毕之后被置零。

AY09.35:(安全级别 2,3,4)

模块应当在置零完成时提供输出状态指示。

所需的送检文档

CY09.35.01:送检单位文档应明确说明模块在置零完成时提供输出状态指示。

所需的检测规程

JY09.35.01:检测人员应核实送检单位提供的文档是否说明了模块在置零完成时提供输出状态指示。

JY09.35.02:检测人员应执行置零,确认输出状态指示。

AY09.36:(安全级别 4)

应当满足下列要求{*AY09.37～AY09.39*}。

注:本条款不单独进行检测。

AY09.37:(安全级别 4)

置零应当是及时的、不可中断的。

注:本条款在 AY09.38 中进行检测。

AY09.38:(安全级别 4)

{*接 AY09.37*}而且应当发生在足够短的时间内,以防止在开始置零到置零实际完成之间的时间内恢复出敏感数据。

所需的送检文档

CY09.38.01:送检单位的文档应说明模块置零是及时的、不可中断的,而且发生在足够短的时间内,以防止在开始置零到置零实际完成之间的时间内恢复出敏感数据。

所需的检测规程

JY09.38.01:检测人员应核实送检单位提供的文档说明了模块置零是及时的、不可中断的,而且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。

JY09.38.02:检测人员应执行模块置零,并尝试中断置零进程以防止它全部或部分完成。

AY09.39:(安全级别 4)

所有未受保护的 SSP(无论是明文形式还是密文形式)应当被置零,使得模块恢复到出厂状态。

所需的送检文档

CY09.39.01:送检单位的文档应说明所有未受保护的 SSP(无论是明文还是受密码技术保护的)被置零,使得模块返回到出厂状态。

所需的检测规程

JY09.39.01:检测人员应核实送检单位的文档说明了所有未受保护的 SSP(无论是明文还是受密码技术保护的)被置零,使得模块返回到出厂状态。

JY09.39.02:检测人员应执行模块置零,并核实模块返回到了出厂状态。

6.10 自测试

6.10.1 自测试通用要求

AY10.01:(安全级别 1,2,3,4)

所有自测试都应当被执行。

注：本条款不单独进行检测。

AY10.02：(安全级别 1,2,3,4)

***{接 AY10.01}*自测试的通过或失败应当取决于模块自身，无论模块运行于核准的工作模式还是非核准的工作模式，都不依赖外部控制、外部提供的输入文本向量、预期的输出结果和操作员的干预。**

注：本条款不单独进行检测。

AY10.03：(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。

注：本条款作为 AY10.14 的一部分进行检测。

AY10.04：(安全级别 1,2,3,4)

条件自测试应当在相应的安全功能或过程被调用时执行。

注：本条款作为 AY10.24 的一部分进行检测。

AY10.05：(安全级别 1,2,3,4)、AY10.06：(安全级别 1,2,3,4)

密码模块应当对其实现的*{GM/T 0028—2014}*附录 C、附录 D、附录 E 中定义的密码算法，执行对应的自测试。

注：本条款作为 AY10.25 的一部分进行检测。

AY10.06：(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。

所需的送检文档

CY10.06.01：针对每一项错误状态，送检文档应提供状态名称和状态描述，并列举状态的引发事件和可清除该状态并恢复正常运行的操作。

所需的检测规程

JY10.06.01：检测人员应确认送检文档的自测试列表中包括：

a) 运行前自测试：
   ——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。
b) 条件自测试；
   ——条件密码算法测试；
   ——条件成对一致性测试；
   ——条件软件/固件加载测试；
   ——条件手动输入测试；
   ——条件旁路测试；
   ——条件关键功能测试。

JY10.06.02：针对每一项错误状态，检测人员应检查送检文档详细说明了上述信息。

JY10.06.03：检测人员应引发每一个错误状态，并试图清除错误状态。检测人员应核实清除错误状态的必要操作与文档说明一致。如果检测人员不能引发所有的错误状态，则应检查代码列表和设计文档，判断清除错误状态的必要操作是否与送检文档描述的一致。

JY10.06.04：检测人员应核实无论运行于核准的工作模式还是非核准的工作模式，密码模块都完成了所有自测试。

JY10.06.05：检测人员应该通过检查和文档审查来确认自测试的通过或失败是由模块自身决定，没有外部控制、外部提供的输入文本向量、预期的输出结果或操作员的干预。

AY10.07：(安全级别 1,2,3,4)

***{接 AY10.06}*并且应当按照*{GM/T 0028—2014}*7.3.3 中的规定，输出一个错误指示。**

所需的送检文档

CY10.07.01：送检文档应记录每一项自测试对应的错误状态，并表明该错误状态对应的错误指示。

所需的检测规程

JY10.07.01：检测人员应核实送检文档列举了模块自测试失败后进入的所有错误状态，并明确各错误状态对应的错误指示。检测人员应将该错误状态列表与有限状态模型中定义的状态（参考 AY11.10）对比，确认它们是否一致。

JY10.07.02：检测人员应通过审核文档中对各自测试处理错误的方式说明，确认以下项目：

——自测试失败后模块进入错误状态；

——错误状态与文档及有限状态模型一致；

——模块输出一个错误指示；

——错误指示与文档所描述的一致。

JY10.07.03：检测人员应运行每一个自测试，使模块进入每一个错误状态。检测人员应比较观察到的错误指示是否与文档描述的一致，如果不一致，视为不通过检测。

AY10.08：（安全级别 1,2,3,4）

在错误状态下，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。

所需的送检文档

CY10.08.01：送检文档应满足 CY03.07.01、CY03.07.02、CY03.10.01 和 CY03.10.02 的要求。送检单位的设计应保证密码模块在错误状态下不能执行密码操作。

所需的检测规程

JY10.08.01：检测人员应核实当密码模块自测试失败时，模块是否按照 GM/T 0028—2014 7.3.3 中的规定，输出了一个错误指示。

JY10.08.02：检测人员应按 JY03.07.01、JY03.07.02、JY03.10.01 和 JY03.10.02 的要求进行检测，检测结果应表明：

a) 送检文档应表明在任何情况下，当处于错误状态时，密码模块都禁止通过控制和数据输出接口输出控制和数据；

b) 当处于错误状态时，密码模块禁止输出任何控制和数据。

AY10.09：（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，直至它们重新通过测试。

所需的送检文档

CY10.09.01：送检文档应说明密码模块不能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。

所需的检测规程

JY10.09.01：检测人员应对某一个自测试失败的功能或算法引入错误，并激活一项需要调用该功能或算法的操作，确认模块不能执行该操作。

JY10.09.02：检测人员应运行每一项自测试，并使模块进入错误状态或降级工作模式。检测人员应运行密码模块，确认模块不能够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。

AY10.10：（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根据在安全策略（*{GM/T 0028—2014}*附录 B）中的过程，判断该模块是否已经进入了错误状态。

所需的送检文档

CY10.10.01：如果模块自测试失败时模块不输出错误状态，送检单位应提供非私有的安全策略用以判断该模块是否已经进入了错误状态。

所需的检测规程

JY10.10.01：检测人员应运行每一项自测试，并使模块进入错误状态，确认模块可按照非私有的安全策略来判断是否进入了某一错误状态。

AY10.11：（安全级别 3，4）

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。

所需的送检文档

CY10.11.01：送检文档应具体说明模块的错误日志功能，包括日志中记录的信息类型（例如，失败的自测试和错误的发生时间）。

所需的检测规程

JY10.11.01：检测人员应通过文档审查核实非授权的管理员不能访问错误日志。

JY10.11.02：检测人员应通过文档审查确认错误日志至少提供了最近的错误事件。

JY10.11.03：检测人员应使密码模块进入一个错误状态，确认模块至少会产生最近错误事件的日志。

JY10.11.04：检测人员应以一个密码模块不支持的鉴别角色访问错误日志。如果访问成功，则该项检测失败。

JY10.11.05：检测人员应运行密码模块，并确认错误日志不能被非授权修改或替换。

AY10.12：（安全级别 3，4）

***{接 AY10.12}*该错误日志应当至少提供最近的错误事件（例如，自测试失败）。**

注：本条款在 AY10.11 中进行检测。

AY10.13：（安全级别 3，4）

***{自测试}*文档应当按照*{GM/T 0028—2014 附录}*A.2.10 中规定的要求编写。**

注：本条款作为 AYA.01 的一部分进行检测。

6.10.2 运行前自测试

6.10.2.1 运行前自测试通用要求

AY10.14：（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。

所需的送检文档

CY10.14.01：送检文档应提供每一项运行前自测试的信息。

CY10.14.02：送检文档应说明在密码模块上电或实例化之后至模块转入到操作状态之前的这段时间内执行运行前自测试的顺序。

所需的检测规程

JY10.14.01：检测人员应确认送检文档具体说明了每一项运行前自测试。检测人员应核实每一项运行前自测试是否与文档说明一致。

JY10.14.02：检测人员应确认送检文档具体说明了每一项运行前自测试。检测人员应核实每一项运行前自测试是否与文档说明一致。

AY10.15：（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。

注：本条款作为 AY10.17～AY10.24 的一部分进行检测。

6.10.2.2 运行前软件/固件完整性测试

AY10.16:(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—2014*}7.5 中定义的要求。

所需的送检文档

CY10.16.01:送检文档应描述密码边界内所有软件和固件部件的完整性验证所使用的核准的技术。

CY10.16.02:送检文档应说明核准的完整性技术是由密码模块本身实现的,还是由运行在核准的工作模式的另一个有效密码模块实现的。

CY10.16.03:送检文档应描述实现完整性技术的实施机制。

CY10.16.04:送检文档应按照 CY02.20.01 的要求提交该核准的完整性技术的有效性证明。

所需的检测规程

JY10.16.01:检测人员应确定送检单位按照 CY02.20.01 的要求提交了核准的完整性技术的有效性证明。

JY10.16.02:如果密码模块采用哈希或 MAC 进行软件/固件的完整性测试,检测人员应确认该测试文档详细地描述了哈希或 MAC 的计算和验证过程。

JY10.16.03:如果模块采用核准的数字签名进行软件/固件的完整性测试,检测人员应确认该测试文档包含以下内容:

a) 该核准的数字签名算法的详细说明;

b) 鉴定哪些受保护的软件和固件采用了核准的数字签名;

c) 确认软件/固件内置的核准的数字签名的预计算值;

d) 确认该核准的数字签名;

e) 如核准的数字签名认证失败,则这项自测试失败。

JY10.16.04:如果模块采用了核准的完整性验证技术,检测人员则应通过代码和/或设计文档审查,确认软件/固件的完整性验证与 JY10.16.01、JY10.16.02、JY10.16.03 相符。

JY10.16.05:如果该核准的完整性验证技术是由另一个有效模块提供的,检测人员应确认软件/固件完整性测试的通过与否是由 AY10.01 决定的。

JY10.16.06:检测人员应修改密码软件和固件部件,如果模块的完整性机制未检测到该修改,则此项检测未通过。

AY10.17:(安全级别 1,2,3,4)

***{接 AY10.16}*如果验证失败,运行前软件/固件完整性测试应当失败。**

注:本条款不单独进行检测。

AY10.18:(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—2014*}7.10.3.2 中规定的密码算法条件自测试作为运行前自测试。

注:本条款不单独进行检测。

AY10.19:(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—2014*}7.10.3.2 中规定的密码算法条件自测试。

所需的送检文档

CY10.19.01:送检文档应满足 CY10.15.02 的要求。

所需的检测规程

JY10.19.01:检测人员应通过代码和设计文档审查,确认用于运行前软件/固件测试的核准的完整

性技术所使用的密码算法已先通过自测试。

6.10.2.3 运行前旁路测试

AY10.20:(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。

所需的送检文档

CY10.20.01:送检文档应说明密码模块是如何确保管理旁路能力的逻辑是正确的。

所需的检测规程

JY10.20.01:检测人员应通过文档审查和模块检查,确认管理旁路能力的逻辑与文档描述一致。

JY10.20.02:检测人员应通过文档审查和检查,确认运行前旁路测试实现了管理旁路能力的逻辑。

JY10.20.03:检测人员应引入运行前旁路测试的各种错误状态,确认是按照 JY03.07.01～JY03.07.05 和 JY03.10.01～JY03.10.05 的要求实现了禁止输出。

JY10.20.04:检测人员应执行运行前旁路测试,确认按照 JY10.10.01 和 JY10.10.02 的要求,任何依赖于管理旁路逻辑的功能都无法被应用。

AY10.21:(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。

所需的送检文档

CY10.21.01:送检单位提交的文档中应描述运行前旁路测试的说明。

CY10.21.02:送检文档应说明如何将旁路开关设置在加密位置。

CY10.21.03:送检文档应描述旁路机制是如何通过将旁路开关设置在加密位置来实现加密数据通过数据路径传输的。

CY10.21.04:送检文档应说明如何将旁路开关设置在非加密位置。

CY10.21.05:送检文档应描述旁路机制是如何通过将旁路开关设置在非加密位置来实现非加密数据通过数据路径传输的。

所需的检测规程

JY10.21.01:检测人员应通过检查确认将旁路开关设置在加密位置时,模块将不实现旁路能力。

JY10.21.02:检测人员应通过代码和/或设计文档审查,确认旁路机制的实现与送检文档一致。

JY10.21.03:检测人员应通过代码和/或设计文档审查,确认模块在执行运行前旁路测试时,如果旁路开关设置在加密位置,经过旁路路径传输的数据是经过加密的。

JY10.21.04:检测人员应通过检查确认模块实现了旁路能力,能够将旁路开关设置在加密位置和非加密位置。

JY10.21.05:检测人员应通过代码和设计文档审查,确认模块在执行运行前旁路测试时,如果旁路开关设置在非加密位置,经过旁路路径传输的数据是没有经过加密的。

6.10.2.4 运行前关键功能测试

AY10.22:(安全级别 1,2,3,4)

其他一些关系到密码模块安全运行的重要安全功能应当在运行前进行测试。

注: 本条款作为 AY10.23 的一部分进行检测。

AY10.23:(安全级别 1,2,3,4)

模块文档应当阐明需要在运行前进行测试的关键功能。

所需的送检文档

CY10.23.01：送检文档应提供所有重要安全功能的说明材料。针对每一项重要安全功能，送检单位应指出：

a） 重要安全功能的目的；

b） 重要安全功能对应哪一项运行前重要安全功能测试；

c） 重要安全功能对应哪一项条件自测试。

所需的检测规程

JY10.23.01：检测人员应确认送检单位提交了所有重要安全功能以及检测这些重要安全功能的自测试文档。文档应包括如下信息：

a） 所有重要安全功能的描述和确认；

b） 对每一项重要安全功能，至少确认一项自测试。

JY10.23.02：通过代码和设计文档审查，检测人员应确认模块实现了每一项重要安全功能的指定自测试。

6.10.3 条件自测试

6.10.3.1 条件自测试通用要求

AY10.24：（安全级别 1，2，3，4）

在下列测试{*AY10.26～AY10.55*}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、手动输入测试、旁路测试以及关键功能测试。

所需的送检文档

CY10.24.01：送检文档应包括条件自测试的相关信息。

所需的检测规程

JY10.24.01：检测人员应核实送检文档包括了条件自测试的相关信息。

JY10.24.02：检测人员应核实模块实现的条件自测试与文档说明一致。

6.10.3.2 密码算法条件自测试

AY10.25：（安全级别 1，2，3，4）

密码算法条件自测试：应当针对模块实现的每个核准的密码算法的所有密码功能（例如，安全功能、SSP 建立方法、鉴别）进行密码算法测试。

注：本条款作为 AY10.26 的一部分进行检测。

AY10.26：（安全级别 1，2，3，4）

***{接 AY10.25}*在密码算法第一次运行使用之前，应当执行该条件测试。**

所需的送检文档

CY10.26.01：送检文档应包括条件密码算法自测试的详细说明。

CY10.26.02：送检文档应提供原理说明如何在密码算法第一次运行使用之前进行条件密码算法自测试的。

CY10.26.03：送检文档应具体说明是否针对模块的密码算法使用了已知答案测试或对比测试。如果采用了对比测试，送检文档应明确指出。

所需的检测规程

JY10.26.01：检测人员应通过模块检查或文档审查确认模块在密码算法第一次运行使用之前进行了条件密码算法自测试。

AY10.27:(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。

所需的送检文档

CY10.27.01:送检文档应详细说明用于比较计算输出与已知答案的方法。

CY10.27.02:送检文档应展示下列转变过程:当计算输出与已知答案不一致时,模块应进入错误状态并输出错误指示。

所需的检测规程

JY10.27.01:检测人员应核实送检文档与密码模块的实现一致。

JY10.27.02:该项检测应符合 JY10.06.02、JY10.07.01、JY10.07.02 和 JY10.07.03 的要求。

AY10.28:(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的密钥长度、模数长度、素数或曲线等进行测试。

所需的送检文档

CY10.28.01:送检文档应详细说明模块采用的每一个条件密码算法自测试。

所需的检测规程

JY10.28.01:检测人员应通过检查和文档审查,确认每一项算法自测试至少针对模块支持的最小核准的密钥长度、模数、素数或曲线等进行测试。

AY10.29:(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。

注:本条款作为 AY10.28 的一部分进行检测。

AY10.30:(安全级别 1,2,3,4)

***{已知答案测试的例子}*单向的功能:输入测试向量生成的输出应当与预期的输出[例如,杂凑、带密钥的杂凑、消息鉴别、随机比特生成器(确定的熵向量)、SSP 协商]相等。**

注:本条款作为 AY10.27 的一部分进行检测。

AY10.31:(安全级别 1,2,3,4)

***{已知答案测试的例子}*可逆的功能:正向和反向功能都应当通过自测试(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)。**

注:本条款作为 AY10.27 的一部分进行检测。

AY10.32:(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。

所需的送检文档

CY10.32.01:送检文档应描述密码算法对比自测试的实施方法。

CY10.32.02:送检文档应满足 CY10.27.03 的要求。

所需的检测规程

JY10.32.01:送检人员应确认对比测试的文档包含以下内容:

a) 采用了两种或以上独立的密码算法实现;

b) 持续不断地对比密码算法输出;

c) 当两者输出不相等时,模块能够进入错误状态并给出错误指示。

JY10.32.02:检测人员应通过代码和/或设计文档审核,确认模块是按照文档设计的步骤进行对比测试的。

AY10.33:(安全级别 1,2,3,4)

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

码算法错误检测测试应当失败。

所需的送检文档

CY10.33.01：送检文档应说明错误检测是对模块的密码算法采用已知答案测试还是比较测试。

所需的检测规程

JY10.33.01：检测人员应核实送检文档列出了以下内容：

a) 描述了密码算法的每个错误条件；

b) 详细描述了每个错误条件的指示器；

c) 所有可能的错误条件均进行了自测试。

6.10.3.3 配对一致性条件测试

AY10.34：(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对每对生成的公钥和私钥(由*{GM/T 0028—2014}*附录 C、附录 D、附录 E 规定的适用的密码算法生成)执行。

所需的送检文档

CY10.34.01：如果密钥传输或非对称算法使用公私钥对，则送检文档应描述公私钥对的一致性测试。该测试的步骤之一是用公钥对明文值或编码信息进行加密。所得的密文结果应与原明文值进行比较以验证二者的不同。

a) 如二者相等，则密码模块应进入错误状态并通过状态接口输出错误指示；

b) 如二者不等，则应使用私钥解密该密文，如果解密的结果与原明文不等，则公私钥对一致性测试不通过。

CY10.34.02：如果非对称密钥对仅用于数字签名的计算和/或验证，则送检文档应详细说明密码模块是通过数字签名的计算和验证来进行公私钥对一致性测试。如果该数字签名不能得以验证，则公私钥对一致性测试不通过。

CY10.34.03：如果公私钥对用于实现 SSP 协议，则送检文档应描述公私钥对一致性测试。文档应指明 SSP 协议的必要算法。此外，该测试的步骤之一是利用密钥对实现必要算法，核查其是否通过公私钥对一致性测试。

所需的检测规程

JY10.34.01：如果密钥传输或非对称算法使用公私钥对，则检测人员应通过代码和/或设计文档审查，并根据 CY10.34.01 的相关规定，确认公私钥对的一致性测试与送检文档是相符。

JY10.34.02：如果非对称密钥对仅用于数字签名的计算和验证，则检测人员应通过代码和/或设计文档审查，并根据 CY10.34.02 的相关规定，确认公私钥对的一致性测试与送检文档是相符的。

JY10.34.03：如果公私钥对用于实现 SSP 协议，则检测人员应通过代码和/或设计文档审查，并根据 CY10.34.03 的相关规定，确认公私钥对的一致性测试与送检文档是相符的。

6.10.3.4 软件/固件加载条件测试

AY10.35：(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—2014}*7.4.3.4 中规定的要求，还应当执行下列要求*{AY10.37～AY10.41}*。

注：本条款不单独进行检测。

AY10.36：(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是经过审验的。

所需的送检文档

CY10.36.01：送检文档应描述密码模块为验证加载软件或固件完整性而实现的核准的鉴别技术。

CY10.36.02：如果模块实现了核准的鉴别技术，送检单位应按照 CY02.20.01 的要求提交相关的有效证明。

CY10.36.03：送检文档应描述在软件/固件加载之前，如何将核准的鉴别技术所需的鉴别密钥独立地加载到模块中的。

CY10.36.04：如果软件/固件加载测试失败，则加载的软件/固件不可使用，送检文档应描述这一实现机制。

所需的检测规程

JY10.36.01：检测人员应通过文档审查确定软件/固件加载测试采用了哪些核准的鉴别技术。

JY10.36.02：检测人员应确认针对模块实现的核准的鉴别技术，送检单位提交了符合 CY02.20.01 要求的有效证明。

JY10.36.03：如果模块在软件/固件的加载测试中采用了核准的鉴别技术，那么检测人员应确认送检文档包含以下内容：

a) 所采用的核准的鉴别技术的具体说明；

b) 采用该核准的鉴别技术的软件和固件；

c) 当软件和固件加载完成后，所采用的核准的鉴别技术的计算；

d) 当加载测试启动后，所采用核准的鉴别技术的验证；

e) 如果核准的鉴别技术认证失败，则该项自测试失败。

JY10.36.04：检测人员应通过代码和/或设计文档审查，确认软件/固件的加载测试与 JY10.36.01、JY10.36.02 和 JY10.36.03 一致。

JY10.36.05：检测人员应通过修改加载的软件或固件或实施认证机制，启动自测试，并从状态输出接口观察输出指示来测试模块。如果未检测到软件/固件加载测试不通过的输出指示，则该项检测不通过。如果检测人员不能修改加载的软件或固件或实施认证机制，则送检单位应为检测人员提供合理的解释，以说明该测试不能通过的原因。

JY10.36.06：检测人员应运行密码模块，修改加载的软件、固件或参考的鉴别签名或实施认证机制，然后启动软件/固件加载测试。在自测试失败后，检测人员应确认加载的软件或固件不可使用，且模块的版本信息未改变。

JY10.36.07：检测人员应通过代码和/或设计文档审查，确认参考的鉴别签名的加载与软件/固件的加载是互相独立的。

JY10.36.08：检测人员应通过代码和/或设计文档审查，确认如果没有在软件/固件加载之前加载参考的鉴别签名，软件/固件加载测试将失败。

JY10.36.09：检测人员应运行密码模块，且在不加载参考的鉴别签名的情况下启动软件/固件加载测试。如果加载测试成功，则本项检测不通过。

AY10.37：（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。

注：本条款作为 AY10.36 的一部分进行检测。

AY10.38：（安全级别 1，2，3，4）

软件/固件的有效性应当成功通过核准的鉴别技术的验证。

注：本条款作为 AY10.36 的一部分进行检测。

AY10.39：（安全级别 1，2，3，4）

***{接 AY10.39}*否则软件/固件加载测试应当失败。**

注：本条款作为 AY10.36 的一部分进行检测。

AY10.40：（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。

注：本条款作为 AY10.36 的一部分进行检测。

6.10.3.5 手动输入条件测试

AY10.41：(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，或者由于手动操作失误会导致某些参数错误，则应当执行以下手动密钥输入测试{*AY10.43～AY10.46*}。

注：本条款不单独进行检测。

AY10.42：(安全级别 1,2,3,4)、AY10.44：(安全级别 1,2,3,4)

SSP 或密钥分量应当使用错误检测码(EDC)。{*或满足 AY10.43*}。

注：本条款不单独进行检测。

AY10.43：(安全级别 1,2,3,4)、AY10.44：(安全级别 1,2,3,4)

***{如果不满足 AY10.43，SSP 或密钥分量}*应当输入两次。**

注：本条款不单独进行检测。

AY10.44：(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。

注：本条款不单独进行检测。

AY10.45：(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。

所需的送检文档

JY10.45.01：送检单位应提供手动密钥输入测试文档。基于使用错误检测码或两次输入密钥的录入方式，手动密钥输入测试应包括：

a) 错误检测码(EDC)：
   ——EDC 算法的描述；
   ——校验过程的描述；
   ——测试成功或失败的预期输出。
b) 两次重复密钥录入：
   ——验证过程的描述；
   ——测试成功或失败的预期输出。

JY10.45.02：如果错误检测码(EDC)用于 SSP 或密钥分量，描述 SSP 或密钥分量格式(参见 AY09.03)的文档应包括对错误检测码域的说明。

所需的检测规程

JY10.45.01：检测人员应根据送检单位提供的文档确认手动密钥输入所使用的方法(错误检测码或两次密钥录入)。基于所使用的方法，检测人员应核实送检单位提供的文档、代码和/或对手动密钥输入测试的执行进行详细说明的设计文档，以确认其是否包含以下信息：

a) 错误检测码：
   ——所有手动输入 SSP 或密钥分量的格式，包括 EDC 域(参见 AY09.03)；
   ——EDC 算法的描述；
   ——EDC 校验过程的描述；
   ——测试成功或失败的所有预期输出。
b) 两次 SSP 或密钥分量输入：
   ——两次手动所有输入 SSP 或密钥分量；
   ——两次密钥输入验证过程的描述；
   ——测试成功或失败的所有预期输出。

JY10.45.02：对于使用 EDC 的手动密钥输入测试，检测人员应核实文档，确认所有手动输入 SSP 或密钥分量的格式包括 EDC 域，并且 EDC 的长度至少为 16 比特。

JY10.45.03：对于使用 EDC 的手动密钥输入测试，检测人员应进行如下测试：

a) 检测人员应手动输入所有 SSP，确认该过程，包括 SSP 的输入格式，与文档描述是否相符。

b) 检测人员应正确输入每种 SSP，并观察状态输出端口。如果未检测到输出指示，或输出指示与文档中描述的测试正确的指示不相符，则该项检测不通过。

c) 检测人员应使用每个输入的 SSP 进行密码操作，以此验证 SSP 输入的正确性。

d) 检测人员应修改每个手动输入 SSP 的 EDC 或 SSP 本身，并将其输入到密码模块中。检测人员应观察状态输出端口的输出指示；如果未检测到输出指示，或输出指示与文档中描述的测试正确的指示不相符，则该项检测不通过。

e) 检测人员应使用每个不能成功输入的 SSP 进行密码操作。这些操作应均告失败，以验证 SSP 未能成功输入。

JY10.45.04：对于使用两次 SSP 或密钥分量输入的手动输入测试，检测人员应进行如下测试：

a) 检测人员应正确输入各种手动输入型的 SSP，并观察状态输出端口。如果未检测到输出指示，或输出指示与文档中描述的测试正确的指示不相符，则该项检测不通过。

b) 检测人员应使用每个输入的 SSP 进行密码操作，以此验证 SSP 输入的正确性。

c) 检测人员应修改一个手动输入的 SSP，或第一个或第二个重复输入项，并将其输入到密码模块中。检测人员应观察状态输出端口的输出指示；如果未检测到输出指示，或输出指示与文档中描述的测试正确的指示不相符，则该项检测不通过。

d) 检测人员应使用每个不能成功输入的 SSP 进行密码操作。这些操作应均告失败，以验证 SSP 未能成功输入。

6.10.3.6 旁路条件测试

AY10.46：（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），那么应当执行下列旁路条件测试{*AY10.48～AY10.51*}，以保证模块部件的单点失效不会导致不经意地输出明文。

注：本条款作为 AY10.47～AY10.50 的一部分进行检测。

AY10.47：（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密码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。

所需的送检文档

CY10.47.01：如果密码模块实现了旁路功能，送检单位应进行旁路测试以确认当开关在旁路服务和加密服务之间进行切换时密码服务能够正确运行。

CY10.47.02：送检单位应提供旁路测试说明。旁路测试应说明当转换为加密服务时，模块不输出明文信息。

所需的检测规程

JY10.47.01：检测人员应核实模块执行了旁路测试以确认当关在旁路服务和加密服务之间进行切换时密码服务能够正确运行。

JY10.47.02：检测人员应通过对源代码和/或设计文档的检查确认送检单位提供的文档与旁路测试的执行相一致。

JY10.47.03：检测人员应将模块由旁路服务转换为加密服务并确认没有明文信息输出。

AY10.48:(安全级别 1,2,3,4)

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

所需的送检文档

CY10.48.01:如果密码模块能够自动在旁路服务与密码服务之间切换,那么送检单位应执行旁路测试以确认当管理切换程序的机制改变时,密码服务能够正确运行。

CY10.48.02:送检单位应提供旁路测试说明。旁路测试应确保当管理切换程序的机制改变时:

a) 确认该机制在最后一次修改后没有被更改。如果该机制被改变,密码模块应进入错误状态并由状态接口输出错误指示。

b) 通过证明模块没有输出明文信息来验证密码服务的正确运行。如果模块输出明文信息,则测试不通过。

所需的检测规程

JY10.48.01:检测人员应核实模块执行旁路测试以验证当管理切换程序的机制改变时,密码服务能够正确运行。

JY10.48.02:检测人员应通过检查源代码和/或设计文档核实送检测试说明与旁路测试执行相一致。

JY10.48.03:检测人员应核实旁路测试的正确运行通过:

a) 核实管理切换程序的机制,以确保机制在最后一次修改后没有改变。检测人员应记录使用的方法。如果设计允许,检测人员应改变该机制来测试所使用的方法。

b) 改变管理切换程序的机制以验证该机制的正确运行,并通过核实模块没有输出明文信息来验证密码服务的正确运行。

AY10.49:(安全级别 1,2,3,4)、AY10.51:(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。

注:本条款不单独进行检测。本条款作为 AY10.50 的一部分进行检测。

AY10.50:(安全级别 1,2,3,4)、AY10.51:(安全级别 1,2,3,4)

*{**接 AY10.49**}***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。**

所需的送检文档

CY10.50.01:送检文档应详细说明修改管理旁路能力的内部信息的方法。

CY10.50.02:送检单位应提供管理旁路能力的内部信息、更新信息的内部顺序以及用核准的完整技术来校验信息完整性的机制的详细说明。

所需的检测规程

JY10.50.01:检测人员应通过检查源代码和/或设计文档,确认模块内保存的管理信息与送检单位文档相符。

JY10.50.02:检测人员应通过检查源代码和/或设计文档,确认更新管理信息的内部顺序与送检单位文档相符。

JY10.50.03:检测人员应通过检查源代码和/或设计文档,确认保持管理信息的机制与送检单位文档相符。

6.10.3.7 关键功能条件测试

AY10.51:(安全级别 1,2,3,4)

其他一些关系到密码模块的安全运行的关键安全功能应当进行条件自测试。

注：本条款作为 AY10.24 的一部分进行检测。

6.10.3.8 周期自测试

AY10.52：(安全级别 1,2,3,4)

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：利用已有自测试服务、复位、重启、上电循环。

所需的送检文档

CY10.52.01：送检文档应描述操作员有周期测试需求的情况下启动运行前自测试的程序。所有的运行前自测试都应涵盖。

CY10.52.02：送检文档应描述操作员有周期测试需求的情况下启动条件自测试的程序。所有的条件自测试都应涵盖。

所需的检测规程

JY10.52.01：检测人员应审核送检文档，确认说明了所有运行前自测试的请求启动方法。

JY10.52.02：检测人员应启动请求的运行前自测试，确认请求的运行前自测试的启动过程与文档说明一致。

JY10.52.03：检测人员应启动请求的条件自测试，确认请求的条件自测试的启动过程与文档说明一致。

AY10.53：(安全级别 3,4)

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。

所需的送检文档

CY10.53.01：送检文档应说明模块如何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，且无需外部的输入或控制。

CY10.53.02：送检文档应详细说明用于指示密码模块运行被运行前或条件自测试中断的状态指示。

CY10.53.03：送检单位提供的非私有安全策略应提供在已定义的时间周期内，重复运行前自测试或条件自测试之间导致模块运行中断的信息和条件。

所需的检测规程

JY10.53.01：检测人员应通过观察密码模块，确认运行前自测试和条件自测试是按照 CY10.53.01 和 CY10.54.02 送检文档描述的进行自动重复执行的。

AY10.54：(安全级别 3,4)

安全策略(*{GM/T 0028—2014}*附录 B)应当阐明时间周期以及在重复执行运行前自测试或条件自测试期间可能导致模块运行中断的任何条件。

注：本条款作为 AY10.53 的一部分进行检测。

6.11 生命周期保障

6.11.1 生命周期保障通用要求

AY11.01：(安全级别 1,2,3,4)

***{生命周期保障}*文档应当按照*{GM/T 0028—2014 附录}*A.2.11 中规定的要求编写。**

所需的送检文档

CY11.01.01：送检单位提供的文档应按照 GM/T 0028—2014 附录 A.2.11 中规定的要求编写。

所需的检测规程

JY11.01.01：检测人员应核实送检单位提供的文档按照 GM/T 0028—2014 附录 A.2.11 中规定的要求编写。

6.11.2 配置管理

AY11.02:(安全级别 1,2,3,4)

密码模块应当满足下列安全要求{*AY11.03～AY11.05*}。

注:本条款作为 AY11.03～AY11.05 的一部分进行检测。

AY11.03:(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。

所需的送检文档

CY11.03.01:送检单位提供的文档中应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。

所需的检测规程

JY11.03.01:检测人员应审查送检单位提供的文档以核实配置管理系统得以实现。

AY11.04:(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。

所需的送检文档

CY11.04.01:送检单位提供的文档中应包括所有配置条目的配置清单,并应对唯一核实配置条目的方法进行说明。

CY11.04.02:送检单位提供的文档中应描述用以唯一标识每个经审验的配置条目版本的方法。

所需的检测规程

JY11.04.01:检测人员应核实送检单位提供的配置清单列入所有配置条目。

JY11.04.02:检测人员应核实送检单位的文档中详细说明了用以唯一标识所有配置条目的方法。

JY11.04.03:检测人员应核实送检单位的文档中对用以唯一标识每个经审验的配置条目版本的方法进行了描述。

JY11.04.04:检测人员应核实送检单位的文档中唯一标识了每个经审验的配置条目版本。

AY11.05:(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。

所需的送检文档

CY11.05.01:送检单位的文档应详细说明只有经过授权才能对配置条目进行更改的方法。

所需的检测规程

JY11.05.01:检测人员应核实送检单位的文档详细说明了只有经过授权才能对配置条目进行更改的方法。

AY11.06:(安全级别 3,4)

应当使用自动的配置管理系统对配置条目进行管理。

所需的送检文档

CY11.06.01:送检单位的文档中应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。

所需的检测规程

JY11.06.01:检测人员应核实送检的文档中详细说明了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。

6.11.3 设计

AY11.07:(安全级别 1,2,3,4)

密码模块应当设计成允许测试所提供的所有安全相关服务。

注:本条款在 6.4.3 中进行检测。

6.11.4 有限状态模型

AY11.08:(安全级别 1,2,3,4)

密码模块的运行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。

所需的送检文档

CY11.08.01: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标识和描述、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。

CY11.08.02:送检单位的文档中应建立以下完整描述:

——正常工作;
——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;
——可信信道;
——密码主管角色;
——用户角色;
——其他角色(若适用);
——安全服务;
——SSP 输入服务(若适用);
——显示状态服务;
——操作员鉴别;
——自测试;
——其他授权的服务、运行和功能(若适用);
——错误状态;
——旁路服务(若适用);
——维护访问接口(若适用);
——维护员角色(如果提供了维护访问接口);
——SSP 产生和建立服务(若适用);
——SSP 输出服务(若适用);
——空闲状态(若适用);
——非初始化状态(若适用)。

所需的检测规程

JY11.08.01:检测人员应核实送检单位提供了有限状态模块的描述。描述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。检测人员应核实状态转移描述包括内部模块条件、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。

JY11.08.02:检测人员应核实有限状态图和描述与送检单位的文档一致。送检单位的文档应描述下列项目:

——正常工作;
——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;
——可信信道;
——密码主管角色;
——用户角色;
——其他角色(若适用);
——安全服务;
——SSP 输入服务(若适用);
——显示状态服务;
——操作员鉴别;
——自测试;
——其他授权的服务、运行和功能(若适用);
——错误状态;
——旁路服务(若适用);
——维护访问接口(若适用);
——维护员角色(如果提供了维护访问接口);
——SSP 产生和建立服务(若适用);
——SSP 输出服务(若适用);
——空闲状态(若适用);
——非初始化状态(若适用)。

JY11.08.03:检测人员应核实在有限状态模型中每个不同的密码模块服务、安全功能用途、错误状态、自测试,或操作员鉴别被描绘成一个独立的状态。

JY11.08.04:检测人员应核实在有限状态图中标识的每一个状态也在有限状态模型的描述中进行了标识和描述。

JY11.08.05:检测人员应核实在有限状态模型的描述中标识和描述的每一个状态也在有限状态图中进行了标识。

JY11.08.06:检测人员应核实模块的运行与有限状态图和描述一致。

JY11.08.07:如果模块包括维护接口,那么检测人员应核实有限状态模型至少有一个维护状态定义。所有维护状态必须包含在有限状态图中,并在有限状态模型的描述中进行描述。

JY11.08.08:如果密码模块明确定义了不相交状态,检测人员应核实其状态描述。检测人员应核实数据和控制输入的所有可能的组合可以被划分为不相交的集合。

JY11.08.09:检测人员应执行密码模块,使其进入各个主状态。每个状态具有不同的标识,当模块处于此状态时,检测人员应尝试核实该标识。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),则检测失败。

JY11.08.10:检测人员应核实存在一个从初始上电状态到模型中每一个其他状态(非上电状态)的转移链。

JY11.08.11:检测人员应核实模型中存在一个从非断电状态到断电状态的转移链。

JY11.08.12：检测人员应核实定义了有限状态模型的行为，这些行为是所有可能数据和控制输入的结果。

AY11.09：（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。

注：本条款不单独进行检测。作为 AY11.10～AY11.13 的一部分进行检测。

AY11.10：（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）。

——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他核准的功能所处的状态。

——核准的状态：执行核准的安全功能时所处的状态。

——自测试状态：密码模块正在执行自测试时所处的状态。

——错误状态：当密码模块遇到错误状况（例如，自测试失败）时所处的状态。

注：本条款作为 AY11.08 的一部分进行检测。

AY11.11：（安全级别 1，2，3，4）

除了那些需要维护、保养或修理密码模块的“硬”错误所导致的错误状态，从错误状态中恢复过来应当是可以做到的。

所需的送检文档

CY11.11.01：对于不需要维护、服务或维修的密码模块错误状态，送检单位的文档中应描述其适用的恢复方法。

所需的检测规程

JY11.11.01：从不需要维护、服务或维修的错误状态中恢复，检测人员应核实密码模块能够被转移到一个可接受的运行或初始化状态。工作包括两部分：首先，检测人员应核实密码模块指示其进入错误状态；其次，核实模块在目标状态中运行正确。检测人员应报告是怎样核实这一要求的（例如，通过代码检测或通过模块测试）。

AY11.12：（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 AY11.08 的一部分进行检测。

AY11.13：（安全级别 1，2，3，4）

除密码主管以外，任何其他角色应当被禁止转换成密码主管状态。

所需的送检文档

CY11.13.01：送检单位的文档中应说明除密码主管以外，任何其他角色被禁止转换成密码主管状态。

所需的检测规程

JY11.13.01：检测人员应核实送检单位的文档中说明了除密码主管以外，任何其他角色被禁止转换成密码主管状态。

JY11.13.02：检测人员应尝试将用户角色转换成密码主管，如转换成功，则检测失败。

JY11.13.03：如有维护员角色，检测人员应尝试将维护员角色转换成密码主管，如转换成功，则检测失败。

6.11.5 开发

AY11.14：（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*{AY11.15～AY11.21}*。

注：本条款作为 AY11.15～AY11.21 的一部分进行检测。

AY11.15：（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他资源，都应当使用配置管理系统进行追踪。

所需的送检文档

CY11.15.01：对于包含软件和固件的密码模块，送检单位应提供源代码、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执行形式的其他资源。

CY11.15.02：对于 CY11.15.01 中记录的每一个条目，送检单位应提供文档说明这些条目采用了配置管理系统进行追踪。

所需的检测规程

JY11.15.01：对于包含软件和固件的密码模块，检测人员应核实送检单位提供了源代码、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执行形式的其他资源。

JY11.15.02：对于 CY11.15.01 中记录的每一个条目，检测人员应核实送检单位提供文档说明这些条目采用了配置管理系统进行追踪。

AY11.16：（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。

所需的送检文档

CY11.16.01：送检单位应提供包含在密码模块中的所有软件和固件部件名称的清单。

CY11.16.02：送检单位应提供包含在密码模块中的所有软件和固件部件的带有注释的源代码。

所需的检测规程

JY11.16.01：检测人员应使用送检单位提供的清单，来核实每一个软件或固件部件的源代码包含在密码模块中。

JY11.16.02：检测人员应核实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。

AY11.17：（安全级别 1,2,3,4）

如果密码模块包含硬件，若适用，文档应当阐明电路图和/或硬件描述语言（HDL）。

所需的送检文档

CY11.17.01：送检单位应提供包含在密码模块中的硬件部件清单。

所需的检测规程

JY11.17.01：检测人员应按照送检单位提供的清单，来核实文档中包括所有硬件部件的电路图和/或硬件描述语言（HDL）。

AY11.18：（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。

所需的送检文档

CY11.18.01:送检单位应提供包含在密码模块中的所有硬件部件的带有注释的 HDL 代码清单。

所需的检测规程

JY11.18.01:检测人员应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部件的 HDL 代码列表,并核实 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。

AY11.19:(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}{GM/T 0028—2014}*7.5 和 7.10 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,由厂商计算并集成到软件或固件模块内。**

所需的送检文档

CY11.19.01: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,送检单位应提供文档说明 GM/T 0028—2014 的 7.5 和 GM/T 0028—2014 的 7.10 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。

所需的检测规程

JY11.19.01: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,检测人员应核实送检单位提供文档说明了 GM/T 0028—2014 的 7.5 和 GM/T 0028—2014 的 7.10 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。

AY11.20:(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。**

注:本条款作为 AY11.15 的一部分进行检测。

AY11.21:(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。**

所需的送检文档

CY11.21.01:送检单位应提供文档说明密码模块应使用工业等级的开发工具(例如,编译器)进行开发。

所需的检测规程

JY11.21.01:检测人员应核实送检单位提供文档说明了密码模块应使用工业等级的开发工具(例如,编译器)进行开发。

AY11.22:(安全级别 2,3,4)

安全二级和三级的密码模块应当满足下列安全要求*{AY11.23～AY11.26}*。

注:本条款作为 AY11.23～AY11.26 的一部分进行检测。

AY11.23:(安全级别 2,3,4)

密码模块内所有软件或固件应当采用高级非私有语言实现。*{或满足 AY011.24 的要求}*。

所需的送检文档

CY11.23.01:送检单位应提供文档说明密码模块内所有软件或固件采用了高级非私有语言实现。

所需的检测规程

JY11.23.01:检测人员应核实送检单位提供文档说明了密码模块内所有软件或固件采用了高级非私有语言实现。

AY11.24:(安全级别 2,3,4)

***{如果不满足 AY011.23 的要求}*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。

所需的送检文档

CY11.24.01：送检单位应标识所有未使用高级语言的软件和固件部件，并对部件使用低级语言的根据。该根据应引证是由于高级语言不可用或提高软件或固件性能所需。

所需的检测规程

JY11.24.01：检测人员应检查所有软件和/或固件部件的源代码以核实哪些使用了低级语言。检测人员应核实除了 CY11.24.01 中标识的之外，没有软件和/或固件部件使用低级语言。

AY11.25：（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）。

所需的送检文档

CY11.25.01：送检单位应提供使用高级规范语言实现的硬件部件文档。

所需的检测规程

JY11.25.01：检测人员应核实送检单位的文档中包括 CY11.25.01 中指定的信息。

AY11.26：（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。

所需的送检文档

CY11.26.01：对于软件密码模块，送检单位应提供文档说明软件的设计和实现避免使用了对模块功能和运行不必要的代码、参数或符号。

所需的检测规程

JY11.26.01：对于软件密码模块，检测人员应核实送检单位提供文档说明软件的设计和实现避免使用了对模块功能和运行不必要的代码、参数或符号。

AY11.27：（安全级别 4）

安全四级的密码模块还应当满足下列安全要求*{AY11.28}*。

注：本条款作为 AY11.28 的一部分进行检测。

AY11.28：（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：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；模块部件、功能和程序完成时，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，该符号足够详细并完整和明确地解释密码模块部件、功能和程序的行为。

所需的送检文档

CY11.28.01：所有硬件、软件和固件部件的源代码应包括注释，如同 AY11.28 要求的前提条件及后续条件。

所需的检测规程

JY11.28.01：检测人员应核实所有源代码包括 CY11.28.01 中指定的信息。

6.11.6 厂商测试

AY11.29：（安全级别 1，2，3，4）

文档应当阐明在密码模块上执行的功能测试。

所需的送检文档

CY11.29.01：送检单位应提供文档详细说明在密码模块上执行的功能测试。

所需的检测规程

JY11.29.01：检测人员应核实送检单位提供的文档中详细说明了密码模块上执行的功能测试。

AY11.30:(安全级别 1,2,3,4)

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,厂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)。

所需的送检文档

CY11.30.01: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,送检单位应提供文档说明使用了通用的自动安全诊断工具(例如,检查缓冲区溢出等)。

所需的检测规程

JY11.30.01: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,检测人员应核实送检单位提供的文档中说明使用了通用的自动安全诊断工具(例如,检查缓冲区溢出等)。

AY11.31:(安全级别 3,4)

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。

所需的送检文档

CY11.31.01:送检单位的文档中应详细说明在密码模块上执行的底层测试的过程与结果。

所需的检测规程

JY11.31.01:检测人员应核实送检单位的文档中详细说明了在密码模块上执行的底层测试的过程与结果。

6.11.7 配送与操作

AY11.32:(安全级别 1,2,3,4)

文档中应当阐明密码模块的安全安装、初始化与启动的流程。

所需的送检文档

CY11.32.01:送检单位的文档中应描述对密码模块的安全安装、初始化以及启动所需的步骤。

所需的检测规程

JY11.32.01:检测人员应核实送检单位提供的文档说明包括安装、初始化以及启动的流程是在安全配置的环境中。

JY11.32.02:检测人员应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。

AY11.33:(安全级别 2,3,4)

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。

所需的送检文档

CY11.33.01:配送文档中应描述在将密码模块分发给已授权操作员的过程中用以维持安全性所需的流程。

所需的检测规程

JY11.33.01:检测人员应核实送检单位提供的文档中说明了在将密码模块的版本分发和配送给已授权操作员的过程中用以维持安全性所需流程的正确性。

AY11.34:(安全级别 2,3,4)

***{接 AY11.33}*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。**

所需的送检文档

CY11.34.01:送检单位的文档中应详细说明在将密码模块配送、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的流程。

所需的检测规程

JY11.34.01:检测人员应核实送检单位提供的文档中详细说明了在将密码模块配送、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的流程。

AY11.35:(安全级别 4)

应当要求已授权的操作员使用厂商提供的鉴别数据对模块进行鉴别。

所需的送检文档

CY11.35.01:送检单位的文档中应说明针对已授权的操作员使用厂商提供的鉴别数据对模块进行鉴别的流程。

所需的检测规程

JY11.35.01:检测人员应核实送检单位提供的文档中说明了针对已授权的操作员使用厂商提供的鉴别数据对模块进行鉴别的流程。

6.11.8 生命终止

AY11.36:(安全级别 1,2,3,4)

文档应当阐明安全清理密码模块的流程。

所需的送检文档

CY11.36.01:送检单位应提供文档详细说明安全清理密码模块的流程。

所需的检测规程

JY11.36.01:检测人员应核实送检单位提供的文档中详细说明了安全清理密码模块的流程。

AY11.37:(安全级别 3,4)

文档中应当阐明安全销毁模块所需的流程。

所需的送检文档

CY11.37.01:送检单位应提供文档详细说明安全销毁密码模块的流程。

所需的检测规程

JY11.37.01:检测人员应核实送检单位提供的文档中详细说明了安全销毁密码模块的流程。

6.11.9 指南文档

AY11.38:(安全级别 1,2,3,4)

管理员指南应当阐明:

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

——独立的操作员鉴别机制能够独立起作用所需的流程;

——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。

所需的送检文档

CY11.38.01:送检单位提供的文档中应包括 AY11.38 中列出的信息。

CY11.38.02:密码模块相应的管理员应可以得到非私有的指南。

所需的检测规程

JY11.38.01:检测人员应核实送检的文档中包括 AY11.38 中列出的信息。

AY11.39:(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的工作模式所担任的所有必要责任。

所需的送检文档

CY11.39.01:送检单位提供的文档中应包含 AY11.39 中列出的信息。

CY11.39.02:密码模块相应的非管理员可以得到非私有的指南。

所需的检测规程

JY11.39.01:检测人员应核实送检的文档中包括 AY11.39 中列出的信息。

6.12 对其他攻击的缓解

AY12.01:(安全级别 1,2,3,4)

***{对其他攻击的缓解}*文档应当按照*{GM/T 0028—2014 附录}*A.2.12 中规定的要求编写。**

所需的送检文档

CY12.01.01:送检单位提供的文档应按照 GM/T 0028—2014 附录 A.2.12 中规定的要求编写。

所需的检测规程

JY12.01.01:检测人员应核实送检单位提供的文档按照 GM/T 0028—2014 附录 A.2.11 中规定的要求编写。

AY12.02:(安全级别 1,2,3,4)

如果将密码模块设计为可缓解一种或多种在本标准中未定义的特定攻击,那么模块的相关文档应当列举出模块能够缓解的攻击。

所需的送检文档

CY12.02.01:送检单位应提供支持文档列举出模块能够缓解的攻击。

所需的检测规程

JY12.02.01:检测人员应核实送检单位提供支持文档列举出模块能够缓解的攻击。

AY12.03:(安全级别 4)

安全四级的密码模块应当满足下列安全要求*{AY12.04}*。

注:本条款作为 AY12.04 的一部分进行检测。

AY12.04:(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。

所需的送检文档

CY12.04.01:送检单位的文档中应详细说明用于缓解攻击的方法。

CY12.04.02:送检单位的文档中应详细说明测试缓解技术有效性的测试方法。

CY12.04.03:送检单位的文档中应详细说明缓解技术的有效性。

所需的检测规程

JY12.04.01:检测人员应核实送检单位的文档中详细说明了用于缓解攻击的方法。

JY12.04.02:检测人员应核实送检单位的文档中详细说明了测试缓解技术有效性的测试方法。

JY12.04.03:检测人员应核实送检单位的文档中详细说明了缓解技术的有效性。

6.13 A-文档要求

注:GM/T 0028—2014 附录 A 给出了密码模块文档的最低要求。

AYA.01:(安全级别 1,2,3,4)

本附录*{GM/T 0028—2014 附录 A}*规定了密码模块的最低文档要求,待测试的密码模块应当满足下列文档要求。

所需的送检文档

CYA.01.01:送检单位应按照但不局限于 GM/T 0028—2014 附录 A 中 A.2.1～A.2.12 的最低文档

要求提交密码模块文档。

所需的检测规程

JYA.01.01：检测人员应核实送检单位按照但不局限于 GM/T 0028—2014 附录 A 中 A.2.1～A.2.1 的最低文档要求提交了密码模块文档。

6.14 B-密码模块安全策略

注：GM/T 0028—2014 附录 B 给出了密码模块安全策略的最低要求。

AYB.01：(安全级别 1,2,3,4)

本附录{*GM/T 0028—2014 附录 B*}总结了非私有安全策略中应当提供的要求。

所需的送检文档

CYB.01.01：送检单位应按照但不局限于 GM/T 0028—2014 附录 B 中 B.2.1～B.2.12 的最低要求提交非私有安全策略。

所需的检测规程

JYB.01.01：检测人员应核实送检单位按照但不局限于 GM/T 0028—2014 附录 B 中 B.2.1～B.2.12 的最低要求提交了非私有安全策略。

AYB.02：(安全级别 1,2,3,4)

安全策略的格式应当按照本附录{*GM/T 0028—2014 附录 B*}指示的顺序呈现。

所需的送检文档

CYB.02.01：送检单位提供的非私有安全策略的格式应当按照 GM/T 0028—2014 附录 B 指示的顺序呈现。

所需的检测规程

JYB.02.01：检测人员应核实送检单位提供的非私有安全策略的格式按照 GM/T 0028—2014 附录 B 指示的顺序呈现。

AYB.03：(安全级别 1,2,3,4)

不应当在没有声明允许复制或分发的情况下，将安全策略标记为私有的或拥有版权的文档。

所需的送检文档

CYB.03.01：如果送检单位提供拥有版权的安全策略，则应提供声明允许复制或分发。

所需的检测规程

JYB.03.01：检测人员应核实送检单位提供的安全策略未标记为私有的或拥有版权的。

6.15 C-核准的安全功能

注：GM/T 0028—2014 附录 C 给出了密码模块核准的安全功能。

6.16 D-核准的敏感安全参数生成和建立方法

注：GM/T 0028—2014 附录 D 给出了密码模块核准的敏感安全参数生成和建立方法。

6.17 E-核准的鉴别机制

注：GM/T 0028—2014 附录 E 给出了密码模块核准的鉴别机制。

6.18 F-非入侵式攻击及常用的缓解方法

注：GM/T 0028—2014 附录 F 给出了密码模块非入侵式攻击及常用的缓解方法。

附 录 A
（资料性附录）
安全等级对应表

A.1 通用要求

表 A.1 通用要求安全等级对应表

条款	安全一级	安全二级	安全三级	安全四级
AY01.01	√	√	√	√
AY01.02	√	√	√	√
AY01.03	√	√	√	√
AY01.04	√	√	√	√

A.2 密码模块规格

表 A.2 密码模块规格安全等级对应表

条款	安全一级	安全二级	安全三级	安全四级
AY02.01	√	√	√	√
AY02.02	√	√	√	√
AY02.03	√	√	√	√
AY02.04	√	√	√	√
AY02.05	√	√	√	√
AY02.06	√	√	√	√
AY02.07	√	√	√	√
AY02.08	√	√	√	√
AY02.09	√	√	√	√
AY02.10	√	√	√	√
AY02.11	√	√	√	√
AY02.12	√	√	√	√
AY02.13	√	√	√	√
AY02.14	√	√	√	√
AY02.15	√	√	√	√
AY02.16	√	√	√	√
AY02.17	√	√	√	√

表 A.2（续）

条款	安全一级	安全二级	安全三级	安全四级
AY02.18	√	√	√	√
AY02.19	√	√	√	√
AY02.20	√	√	√	√
AY02.21	√	√	√	√
AY02.22	√	√	√	√
AY02.23	√	√	√	√
AY02.24	√	√	√	√

A.3 密码模块接口

表 A.3 密码模块接口安全等级对应表

条款	安全一级	安全二级	安全三级	安全四级
AY03.01	√	√	√	√
AY03.02	√	√	√	√
AY03.03	√	√	√	√
AY03.04	√	√	√	√
AY03.05	√	√	√	√
AY03.06	√	√	√	√
AY03.07	√	√	√	√
AY03.08	√	√	√	√
AY03.09	√	√	√	√
AY03.10	√	√	√	√
AY03.11	√	√	√	√
AY03.12	√	√	√	√
AY03.13	√	√	√	√
AY03.14	√	√	√	√
AY03.15	√	√	√	√
AY03.16			√	√
AY03.17			√	√
AY03.18			√	√
AY03.19			√	√
AY03.20			√	√
AY03.21			√	√
AY03.22				√

A.4 角色、服务和鉴别

表 A.4 角色、服务和鉴别安全等级对应表

条款	安全一级	安全二级	安全三级	安全四级
AY04.01	√	√	√	√
AY04.02	√	√	√	√
AY04.03	√	√	√	√
AY04.04	√	√	√	√
AY04.05	√	√	√	√
AY04.06	√	√	√	√
AY04.07	√	√	√	√
AY04.08	√	√	√	√
AY04.09	√	√	√	√
AY04.10	√	√	√	√
AY04.11	√	√	√	√
AY04.12	√	√	√	√
AY04.13	√	√	√	√
AY04.14	√	√	√	√
AY04.15	√	√	√	√
AY04.16	√	√	√	√
AY04.17	√	√	√	√
AY04.18	√	√	√	√
AY04.19	√	√	√	√
AY04.20	√	√	√	√
AY04.21	√	√	√	√
AY04.22				√
AY04.23	√	√	√	√
AY04.24	√	√	√	√
AY04.25	√	√	√	√
AY04.26	√	√	√	√
AY04.27				√
AY04.28	√	√	√	√
AY04.29	√	√	√	√

表 A.4（续）

条款	安全一级	安全二级	安全三级	安全四级
AY04.30	√	√	√	√
AY04.31	√	√	√	√
AY04.32	√	√	√	√
AY04.33	√	√	√	√
AY04.34	√	√	√	√
AY04.35	√	√	√	√
AY04.36	√	√	√	√
AY04.37	√	√	√	√
AY04.38		√	√	√
AY04.39		√	√	√
AY04.40		√	√	√
AY04.41			√	√
AY04.42			√	√
AY04.43			√	√
AY04.44			√	√
AY04.45	√	√	√	√
AY04.46	√	√	√	√
AY04.47		√	√	√
AY04.48		√	√	√
AY04.49		√	√	√
AY04.50		√	√	√
AY04.51		√	√	√
AY04.52		√	√	√
AY04.53		√	√	√
AY04.54		√	√	√
AY04.55		√		
AY04.56		√	√	√
AY04.57		√	√	√
AY04.58	√			
AY04.59		√		
AY04.60			√	√
AY04.61				√

A.5 软件/固件安全

表 A.5 软件/固件安全安全等级对应表

条款	安全一级	安全二级	安全三级	安全四级
AY05.01	√	√	√	√
AY05.02	√	√	√	√
AY05.03	√	√	√	√
AY05.04	√	√	√	√
AY05.05	√	√	√	√
AY05.06	√	√	√	√
AY05.07	√	√	√	√
AY05.08	√	√	√	√
AY05.09	√	√	√	√
AY05.10	√	√	√	√
AY05.11	√	√	√	√
AY05.12		√	√	√
AY05.13		√	√	√
AY05.14		√	√	√
AY05.15		√	√	√
AY05.16		√	√	√
AY05.17			√	√
AY05.18			√	√
AY05.19			√	√
AY05.20			√	√
AY05.21			√	√

A.6 运行环境

表 A.6 运行环境安全等级对应表

条款	安全一级	安全二级	安全三级	安全四级
AY06.01	√	√		
AY06.02	√	√		
AY06.03	√	√		
AY06.04	√			

表 A.6（续）

条款	安全一级	安全二级	安全三级	安全四级
AY06.05	√	√		
AY06.06	√	√		
AY06.07	√	√		
AY06.08	√	√		
AY06.09		√		
AY06.10		√		
AY06.11		√		
AY06.12		√		
AY06.13		√		
AY06.14		√		
AY06.15		√		
AY06.16		√		
AY06.17		√		
AY06.18		√		
AY06.19		√		
AY06.20		√		
AY06.21		√		
AY06.22		√		
AY06.23		√		
AY06.24		√		
AY06.25		√		
AY06.26		√		
AY06.27		√		
AY06.28		√		
AY06.29		√		

A.7 物理安全

表 A.7 物理安全安全等级对应表

条款	安全一级	安全二级	安全三级	安全四级
AY07.01	√	√	√	√
AY07.02	√	√	√	√
AY07.03	√	√	√	√

表 A.7（续）

条款	安全一级	安全二级	安全三级	安全四级
AY07.04	√	√	√	√
AY07.05	√	√	√	√
AY07.06	√	√	√	√
AY07.07	√	√	√	√
AY07.08	√	√	√	√
AY07.09	√	√	√	√
AY07.10	√	√	√	√
AY07.11	√	√	√	√
AY07.12	√	√	√	√
AY07.13	√	√	√	√
AY07.14	√	√	√	√
AY07.15	√	√	√	√
AY07.16	√	√	√	√
AY07.17		√	√	√
AY07.18		√	√	√
AY07.19		√	√	√
AY07.20		√	√	√
AY07.21			√	√
AY07.22			√	√
AY07.23			√	√
AY07.24			√	√
AY07.25			√	√
AY07.26			√	√
AY07.27			√	√
AY07.28			√	√
AY07.29				√
AY07.30				√
AY07.31				√
AY07.32				√
AY07.33				√
AY07.34		√	√	√
AY07.35		√	√	√
AY07.36			√	√
AY07.37			√	√

表 A.7（续）

条款	安全一级	安全二级	安全三级	安全四级
AY07.38			√	√
AY07.39				√
AY07.40				√
AY07.41				√
AY07.42				√
AY07.43	√	√	√	√
AY07.44		√	√	√
AY07.45		√	√	√
AY07.46		√	√	√
AY07.47		√	√	√
AY07.48		√	√	√
AY07.49			√	√
AY07.50			√	√
AY07.51			√	√
AY07.52				√
AY07.53				√
AY07.54				√
AY07.55				√
AY07.56				√
AY07.57				√
AY07.58				√
AY07.59				√
AY07.60	√	√	√	√
AY07.61		√	√	√
AY07.62		√	√	√
AY07.63		√	√	√
AY07.64			√	√
AY07.65			√	√
AY07.66				√
AY07.67				√
AY07.68				√
AY07.69				√

表 A.7（续）

条款	安全一级	安全二级	安全三级	安全四级
AY07.70				√
AY07.71				√
AY07.72				√
AY07.73			√	√
AY07.74				√
AY07.75			√	√
AY07.76			√	√
AY07.77			√	√
AY07.78			√	√
AY07.79				√
AY07.80				√
AY07.81				√
AY07.82				√
AY07.83				√
AY07.84				√
AY07.85				√
AY07.86				√

A.8 非入侵式安全

表 A.8 非入侵式安全安全等级对应表

条款	安全一级	安全二级	安全三级	安全四级
AY08.01	√	√	√	√
AY08.02	√	√	√	√
AY08.03	√	√	√	√
AY08.04	√	√	√	√
AY08.05	√	√	√	√
AY08.06			√	
AY08.07			√	
AY08.08				√

A.9 敏感安全参数管理

表 A.9 敏感安全参数管理安全等级对应表

条款	安全一级	安全二级	安全三级	安全四级
AY09.01	√	√	√	√
AY09.02	√	√	√	√
AY09.03	√	√	√	√
AY09.04	√	√	√	√
AY09.05	√	√	√	√
AY09.06	√	√	√	√
AY09.07	√	√	√	√
AY09.08	√	√	√	√
AY09.09	√	√	√	√
AY09.10	√	√	√	√
AY09.11	√	√	√	√
AY09.12	√	√	√	√
AY09.13	√	√	√	√
AY09.14	√	√	√	√
AY09.15	√	√	√	√
AY09.16	√	√	√	√
AY09.17	√	√	√	√
AY09.18	√	√	√	√
AY09.19	√	√	√	√
AY09.20	√	√	√	√
AY09.21	√	√		
AY09.22			√	√
AY09.23			√	√
AY09.24			√	
AY09.25			√	
AY09.26				√
AY09.27	√	√	√	√
AY09.28	√	√	√	√
AY09.29	√	√	√	√
AY09.30	√	√	√	√
AY09.31	√	√	√	√

表 A.9（续）

条款	安全一级	安全二级	安全三级	安全四级
AY09.32		√	√	√
AY09.33		√	√	√
AY09.34		√	√	√
AY09.35		√	√	√
AY09.36				√
AY09.37				√
AY09.38				√
AY09.39				√

A.10 自测试

表 A.10 自测试安全等级对应表

条款	安全一级	安全二级	安全三级	安全四级
AY10.01	√	√	√	√
AY10.02	√	√	√	√
AY10.03	√	√	√	√
AY10.04	√	√	√	√
AY10.05	√	√	√	√
AY10.06	√	√	√	√
AY10.07	√	√	√	√
AY10.08	√	√	√	√
AY10.09	√	√	√	√
AY10.10	√	√	√	√
AY10.11			√	√
AY10.12			√	√
AY10.13			√	√
AY10.14	√	√	√	√
AY10.15	√	√	√	√
AY10.16	√	√	√	√
AY10.17	√	√	√	√
AY10.18	√	√	√	√
AY10.19	√	√	√	√
AY10.20	√	√	√	√

表 A.10（续）

条款	安全一级	安全二级	安全三级	安全四级
AY10.21	√	√	√	√
AY10.22	√	√	√	√
AY10.23	√	√	√	√
AY10.24	√	√	√	√
AY10.25	√	√	√	√
AY10.26	√	√	√	√
AY10.27	√	√	√	√
AY10.28	√	√	√	√
AY10.29	√	√	√	√
AY10.30	√	√	√	√
AY10.31	√	√	√	√
AY10.32	√	√	√	√
AY10.33	√	√	√	√
AY10.34	√	√	√	√
AY10.35	√	√	√	√
AY10.36	√	√	√	√
AY10.37	√	√	√	√
AY10.38	√	√	√	√
AY10.39	√	√	√	√
AY10.40	√	√	√	√
AY10.41	√	√	√	√
AY10.42	√	√	√	√
AY10.43	√	√	√	√
AY10.44	√	√	√	√
AY10.45	√	√	√	√
AY10.46	√	√	√	√
AY10.47	√	√	√	√
AY10.48	√	√	√	√
AY10.49	√	√	√	√
AY10.50	√	√	√	√
AY10.51	√	√	√	√
AY10.52	√	√	√	√
AY10.53			√	√
AY10.54			√	√

A.11 生命周期保障

表 A.11 生命周期保障安全等级对应表

条款	安全一级	安全二级	安全三级	安全四级
AY11.01	√	√	√	√
AY11.02	√	√	√	√
AY11.03	√	√	√	√
AY11.04	√	√	√	√
AY11.05	√	√	√	√
AY11.06			√	√
AY11.07	√	√	√	√
AY11.08	√	√	√	√
AY11.09	√	√	√	√
AY11.10	√	√	√	√
AY11.11	√	√	√	√
AY11.12	√	√	√	√
AY11.13	√	√	√	√
AY11.14	√	√	√	√
AY11.15	√	√	√	√
AY11.16	√	√	√	√
AY11.17	√	√	√	√
AY11.18	√	√	√	√
AY11.19	√	√	√	√
AY11.20	√	√	√	√
AY11.21	√	√	√	√
AY11.22		√	√	√
AY11.23		√	√	√
AY11.24		√	√	√
AY11.25		√	√	√
AY11.26		√	√	√
AY11.27				√
AY11.28				√
AY11.29	√	√	√	√
AY11.30	√	√	√	√
AY11.31			√	√

表 A.11（续）

条款	安全一级	安全二级	安全三级	安全四级
AY11.32	√	√	√	√
AY11.33		√	√	√
AY11.34		√	√	√
AY11.35				√
AY11.36	√	√	√	√
AY11.37			√	√
AY11.38	√	√	√	√
AY11.39	√	√	√	√

A.12 对其他攻击的缓解

表 A.12 对其他攻击的缓解安全等级对应表

条款	安全一级	安全二级	安全三级	安全四级
AY12.01	√	√	√	√
AY12.02	√	√	√	√
AY12.03				√
AY12.04				√

中国标准出版社

密码模块安全检测要求