ICS 35.240
L70/84

团　　体　　标　　准

T/ EMCG 004.3-2021

移动智能终端密码模块安全检测要求 第3部分：密钥多端协同计算保护密码模块检测

Security test requirements for cryptographic modules in mobile smart terminal
Part 3: Key protection based on multi-party computation

2021－08－12 发布　　2021－08－12 实施

中关村网络安全与信息化产业联盟　发布

目　　次

前　言

T/EMCG 004-2021《移动智能终端密码模块检测要求》分为4个部分：

第1部分：密钥加密本地保护密码模块检测

第2部分：密钥加密服务端保护密码模块检测

第3部分：密钥多端协同计算保护密码模块检测

第4部分：基于安全芯片的密码模块检测

本文件为T/EMCG 004-2021《移动智能终端密码模块检测要求》的第3部分。

本文件按照GB/T 1.1-2020给出的规则起草。

本文件由中关村网络安全与信息化产业联盟企业移动计算工作组（EMCG）提出。

本文件由参与T/EMCG 004-2021《移动智能终端密码模块检测要求》标准制定的全体单位投票表决通过。

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。

本文件主要起草单位：中关村网络安全与信息化产业联盟、北京三博安科技有限公司、北京江南天安科技有限公司、江苏通付盾科技有限公司、奇安信科技集团股份有限公司、中国科学院信息工程研究所等。

本文件主要起草人：王冬冬、贾世杰、王克、张凡、汪德嘉、朱旭光、傅文斌等。

移动智能终端密码模块安全检测要求
第3部分：密钥多端协同计算保护密码模块检测

1 范围

本文件依据T/EMCG 001.4-2019技术架构，规定了密钥多端协同计算密码模块的一系列检测规程、方法和对应的送检文档要求。移动智能终端密码模块产品生产、检测机构可参考本文件开展相关密码产品检测。

2 规范性引用文件

下列文件中的条款通过T/EMCG 004-2021《移动智能终端密码模块检测要求》的本文件的引用而成为本文件的条款。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GM/T 0005 随机性检测规范

GM/T 0019 通用密码服务接口规范

GM/T 0028 密码模块安全技术要求

GM/T 0039 密码模块安全检测要求

GM/T 0059 服务器密码机检测规范

T/ EMCG 001-2019（所有部分） 移动智能终端密码模块技术框架

3 术语和定义

T/EMCG 001-2019所界定的术语和定义适用于本文件。

4 符号和缩略语

下列符号和缩略语适用于本文件。

API	应用程序接口（application program interface）
APP	移动智能终端应用软件（application）
CC	密码组件（cryptographic components）
CMMST	移动智能终端密码模块（cryptographic module of mobile smart terminal）
CMMST-KPBMC	密钥多端协同计算保护移动智能终端密码模块（CMMST of key protection based on multi-party computation）
CSP	关键安全参数（critical security parameter）
KPBMC	密钥多端协同计算保护（key protection based on multi-party computation）
MST	移动智能终端（mobile smart terminal）

MST-CC	移动智能终端密码组件（mobile smart terminal cryptographic components）
PIN	个人身份识别码（personal identification number）
PPD	个人特征数据（personal profile data）
SDK	软件开发套件（software development kit）
SS-CC	服务端密码组件（server side cryptographic components）
SSP	敏感安全参数（sensitive security parameter）
TPSS-CC	第三方服务端密码组件（third party server side cryptographic components）

5 文档结构

5.1 概述

本文件第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6.1～6.11对应T/EMCG 001.4-2019中第6～16章的11个安全域。

5.2 条款

在本文件第6章的每条中，T/EMCG 001.4-2019相应安全要求被分成了一系列条款集，宋体加粗字体表示全部内容直接引用T/EMCG 001.4-2019。

各条款格式为：

安全要求

AY<T/EMCG 001.4-2019对应内容章节号>.<条款序列号>

送检文档

CY<T/EMCG 001.4-2019对应内容章节号>.<条款序列号>

检测规程及方法

JY<T/EMCG 001.4-2019对应内容章节号>.<条款序列号>

其中“AY”表示安全要求，“CY”表示文档要求，“JY”表示检测规程和方法要求。“章节号”是T/EMCG 001.4-2019中11个安全域第6～16章节号，“条款序列号”是条内的序列标识符。

6 安全检测要求

6.1 密码模块规格

6.1.1 密码模块类型

AY6.1.01：

CMMST-KPBMC是混合软件密码模块，包括MST-CC、SS-CC及TPSS-CC软件模块及服务器密码机。

送检文件

CY6.1.01送检单位的文档中应解释CMMST-KPBMC混合软件密码模块选择的依据。

CY6.1.02送检单位应提供CMMST-KPBMC混合软件密码模块的规格，以标识所有CMMST-KPBMC混合软件密码模块的软件、硬件部件。

检测规程及方法

JY6.1.01检测人员应核实送检单位的文档中是否标识了AY6.1.01中模块类型。

JY6.1.02检测人员应通过审查送检单位提供的规格文档，识别所有软件、硬件部件，核实该CMMST-KPBMC混合软件密码模块与AY6.1.01定义的密码模块类型一致。

6.1.2 密码边界

AY6.2.01：

密钥双端协同计算保护CMMST-KPBMC边界为MST-CC、SS-CC的可执行文件或文件集以及服务器密码机。

（1） MST-CC至少包括完成以下功能的模块：密码服务接口，密码算法，PPD输入，随机数生成，SS-CC通信。

（2） SS-CC至少包括完成以下功能的模块：用户密钥管理，服务器密码机，MST-CC通信。

（3） MST-CC、SS-CC软件模块运行在独立的进程空间中，使用操作系统进程间通信接口与密码边界外进行数据交换。

AY6.2.02：（安全一、二级）

密钥三端协同计算保护CMMST-KPBMC边界为MST-CC、SS-CC、TPSS-CC的可执行文件或文件集以及服务器密码机。

（1） MST-CC至少包括完成以下功能的模块：密码服务接口，密码算法，PPD输入，随机数生成，SS-CC通信。

（2） SS-CC至少包括完成以下功能的模块：用户密钥管理，服务器密码机，MST-CC、TPSS-CC通信。

（3） TPSS-CC至少包括完成以下功能的模块：用户密钥管理，服务器密码机，SS-CC通信；

（4） MST-CC、SS-CC、TPSS-CC软件模块运行在独立的进程空间中，使用操作系统进程间通信接口与密码边界外进行数据交换。

送检文档

CY6.2.01：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。

CY6.2.02：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。

CY6.2.03：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）。

CY6.2.04：送检单位的文档中应标识SS-CC、TPSS-CC中的服务器密码机等硬件部件。

检测规程及方法

JY6.2.01：检测人员应核实送检单位的文档中是否包括硬件部件清单，该部件清单包括服务器密码机等硬件部件。

JY6.2.02：检测人员应识别密码模块的硬件部件，即服务器密码机。

JY6.2.03：检测人员应核实部件清单和其它小节条款提供的资料是否一致，其定义如下：

——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；

——核实框图中的所有个体部件也在部件清单中都有列出；

——核实这些被从GM/T 0028安全要求排除的部件仍然在部件清单中列出。

JY6.2.04：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。模块设计还必须确保密码模块没有不受控的输入输出接口，这些接口可能泄漏CSP、明文数据或其他一旦被误用就可能导致系统被破坏的信息。

JY6.2.05：检测人员应核实密码边界包括了所有输入、输出或CSP处理、明文或其他一旦被误用就可能导致系统被破坏的信息部件。

JY6.2.11：检测人员应核实送检单位的文档中的部件清单，该部件清单包括密码模块的所有软件部件。

JY6.2.12：检测人员应核实部件清单包括以下所有出现的部件类型，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；

——保存在内存中由一个或多个处理器执行的密码模块的实例。

JY6.2.13：检测人员应核实送检单位的文档描述的软件部件交互的内部软件架构准确。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。

JY6.2.14：检测人员应核实送检单位的文档中说明密码模块所运行的软件环境（例如操作系统，运行时库）。

6.1.3 工作模式

AY6.3.01：

CMMST-KPBMC运行于密码模块核准的工作模式下。

送检文档

按照GM/T 0039第6.2.4章节关于所要求的送检文档。

检测规程及方法

按照GM/T 0039第6.2.4章节关于所要求的检测规程。

6.2 密码模块接口

6.2.1 物理和逻辑接口

AY7.1.01：

CMMST-KPBMC逻辑接口分布在MST-CC、SS-CC及TPSS-CC上，各方逻辑接口类型相同。

送检文档

CY7.1.01：送检单位的文档中应说明密码模块MST-CC、SS-CC及TPSS-CC的API接口，包括：

----应明确说明与移动智能终端APP对接的MST-CC的API调用方式；

----应明确说明与应用系统进行业务对接的SS-CC及TPSS-CC的API调用方式；

检测规程及方法

JY7.1.01：检测人员应核实送检单位的文档说明了密码模块的MST-CC、SS-CC及TPSS-CCAPI接口。所需的说明包括：

JY7.1.02：检测人员应通过检查送检单位提供的的源代码资料，以核实送检单位的MST-CC、SS-CC及TPSS-CC的所有API接口已实现。

JY7.1.03：检测人员应根据接口说明调用MST-CC、SS-CC及TPSS-CC的API接口，核实送检单位送检的MST-CC、SS-CC及TPSS-CC与实际设计一致。

6.2.2 接口类型

AY7.2.01：

CMMST-KPBMC接口类型为混合软件模块接口类型。

注：本条款不单独进行检测。

6.2.3 接口定义

AY7.3.01：

CMMST-KPBMC接口定义参照GM/T 0019通用密码服务接口规范。

送检文档

CY7.3.01：送检单位的文档中应说明密码模块所提供的所有密码服务接口。

检测规程及方法

JY7.3.01：检测单位应核实送检单位文档中说明的所有密码服务接口，并通过调用密码组件的API接口（双端：MST-CC和SS-CC的API接口，三端：MST-CC、SS-CC及TPSS-CC的API接口），实现协同签名操作，并通过对应公钥成功验证。

6.3 角色、服务和鉴别

6.3.1 角色

AY8.1.01：

CMMST-KPBMC支持密码主管角色、移动应用用户角色。

密码主管：负责对SS-CC、TPSS-CC进行操作，以及CMMST-KPBMC系统管理。（三端协同计算密码模块有两个密码主管，分别对SS-CC、TPSS-CC进行操作。）

移动应用用户：使用MST-CC实现私钥分量生成、数据签名/验签及加解密等。

送检文档

CY8.1.01：送检单位的文档中应说明是否支持多个角色同时操作。

CY8.1.02：如果密码模块支持多个角色同时操作，送检单位应描述怎样实现每个角色相隔离及相应服务隔离的方法。

CY8.1.03：送检单位应描述多个操作员的限制（例如，不允许一个操作员既是密码主管角色又是用户角色）。

CY8.1.04：送检单位的密码模块产品应包括至少一个密码主管角色和用户角色。

CY8.1.05：送检单位的文档应描述密码主管角色的功能。

CY8.1.06：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。

检测规程及方法

JY8.1.01：检测人员应核实送检单位的文档中是否描述密码模块实现多个角色与服务强制隔离的方法。

JY8.1.02：检测人员应担当不同角色，对于每个角色，检测人员应测试其是否可执行其他角色的服务，以此来核实不同角色间服务的分离。

JY8.1.03：如果送检单位的文档给出关于对每个角色行为的限制条件，检测人员应尝试以对应角色执行被限制行为，以此核实模块是否执行这些约束。

JY8.1.04：检测人员应核实送检单位的文档中描述了密码主管角色和用户角色的功能。

JY8.1.05：检测人员应给出密码主管角色和许可服务与送检单位文档描述一致。

6.3.2 服务

6.3.2.1 服务通用要求

AY8.2.1.01：

CMMST-KPBMC满足GM/T 0028 7.4.3要求。

送检文档

CY8.2.1.01：参见GM/T 0039第6.4.3.1章节关于密码模块送检文档要求。

检测规程及方法

JY8.2.1.01：参见GM/T 0039第6.4.3.1章节关于密码模块检测规程要求。

6.3.2.2 旁路能力

AY8.2.2.01：

CMMST-KPBMC不具备旁路能力或功能。

注：本条款不单独进行检测。

6.3.2.3 自启动密码服务能力

AY8.2.3.01：

CMMST-KPBMC不具备自启动密码服务能力或功能。

注：本条款不单独进行检测。

6.3.2.4 软件/固件加载

AY8.2.4.01：

CMMST-KPBMC不具备加载外部软件/固件功能。

注：本条款不单独进行检测。

6.3.3 鉴别

AY8.3.01：

CMMST-KPBMC除满足GM/T 0028 7.4.4对安全二级的要求外，还具备以下功能：

（1） MST-CC采用PPD对移动应用用户身份进行鉴别。

（2） SS-CC及TPSS-CC采用硬件Token（令牌）对密码主管进行身份认证。

送检文档

CY8.3.01：参见GM/T 0039第6.4.4章节关于安全一、二级密码模块送检文档要求。

CY8.3.02：送检单位文档应说明MST-CC对移动应用用户身份进行鉴别的方式。

CY8.3.03：送检单位文档应说明SS-CC及TPSS-CC对密码主管身份进行鉴别的方式。

检测规程及方法

JY8.3.01：参见GM/T 0039第6.4.4章节关于安全一、二级软件密码模块检测规程要求。

JY8.3.02：检测单位应核实送检单位的文档中描述的MST-CC对移动应用用户身份鉴别的方式。

JY8.3.03：检测单位应核实送检单位的文档中描述的SS-CC及TPSS-CC对密码主管身份鉴别的方式。

6.4 软件/固件安全

AY9.01：

CMMST-KPBMC满足GM/T 0028 7.5对安全一、二级的技术要求。

送检文档

CY9.01：参见GM/T 0039第6.5章节关于安全一、二级软件密码模块送检文档要求。

检测规程及方法

JY9.01：参见GM/T 0039第6.5章节关于安全一、二级软件密码模块检测规程要求。

6.5 运行环境

AY10.01：

CMMST-KPBMC运行于可修改的运行环境，需满足GM/T 0028 7.6对安全二级的技术要求。

MST-CC、SS-CC以及TPSS-CC的软件模块须运行在独立的进程空间中，依托操作系统的访问控制机制。

送检文档

CY10.01：参见 GM/T 0039 第 6.6.3 章节关于安全一、二级软件密码模块送检文档要求。

CY10.02：送检单位需说明密码模块 MST-CC、SS-CC 以及 TPSS-CC 的软件模块运行在独立进程空间的方法，检测合法操作系统的方法。

检测规程及方法

JY10.01：参见 GM/T 0039 第 6.6.3 章节关于安全一、二级软件密码模块检测规程要求。

JY10.02：检测单位需核实送检单位文档中描述的 MST-CC、SS-CC 以及 TPSS-CC 部分运行在独立进程空间的方法，检测合法操作系统的方法。

6.6 物理安全

AY11.01：

MST-CC不涉及物理安全。

注：本条款不单独进行检测。

AY11.02：

SS-CC、TPSS-CC中的服务器密码机需满足GM/T 0028 7.7安全二级技术要求。

送检文档

CY11.01：参见 GM/T 0039 第 6.7.2 章节和 6.7.3 章节关于安全一、二级密码模块送检文档要求。

CY11.02：送检文档应满足 GM/T 0059 第 7 章送检文档技术要求。

检测规程及方法

JY11.01：参见 GM/T 0039 第 6.7.2 章节和 6.7.3 章节关于安全一、二级密码模块检测规程要求。

JY11.02:检测单位应核实送检单位的文档中是否满足 GM/T 0059 第 7 章送检文档技术要求。

JY11.03：检测单位应按照 GM/T 0059 的检测环境和检测内容对服务器密码机进行检测。

6.7 非入侵式安全

AY12.01：

MST-CC不涉及非侵入式安全。

注：本条款不单独进行检测。

AY12.02：

SS-CC、TPSS-CC中的服务器密码机满足GM/T 0028 7.8安全二级技术要求。

送检文档

CY12.01：参见 GM/T 0039 第 6.8 章节关于安全一、二级密码模块送检文档要求。

检测规程及方法

JY12.01：参见 GM/T 0039 第 6.8 章节关于安全一、二级密码模块检测规程要求。

6.8 敏感安全参数管理

6.8.1 敏感安全参数管理通用要求

AY13.01：

CMMST-KPBMC敏感安全参数（SSP）包括：

d_{A1}——用户MST-CC私钥分量

d_{A2}——用户SS-CC私钥分量

d_{A3}——用户TPSS-CC私钥分量

P_A——用户公钥

PPD——用户个人特征数据

遵照GM/T 0028 7.9.1要求，CMMST-KPBMC对以上敏感安全参数进行管理。

（1） 关键安全参数（CSP）d_{A1}、PPD 在 MST-CC 内保护，防止非授权的访问、使用、泄露、修改和替换。

（2） 关键安全参数（CSP）d_{A2}、d_{A3} 在服务器密码机中生成，防止非授权的访问、使用、泄露、修改和替换。

（3） 公开安全参数（PSP）P_A 保存在 MST-CC 内，防止非授权修改和替换。

（4） 使用移动应用用户 PPD 与 d_A 相关联。

（5） 使用服务器密码机硬件 Token（令牌）将密码主管角色与 d_{A2}、d_{A3} 相关联。

送检文档

CY13.01：参见 GM/T 0039 第 6.9.1 章节关于密码模块送检文档的要求。

CY13.02：送检单位的文档应描述 MST-CC 内 CSP 和 PSP 的保护措施，包括防止非授权修改和替换的实现机制。

CY13.03：送检单位的文档应描述移动用户 PPD 与 d_{A1} 相关联的方式。

CY13.04：送检单位的文档应描述服务器密码机硬件 Token（令牌）将密码主管角色与 d_{A2}、d_{A3} 相关联的实现方式。

检测规程及方法

JY13.01：参见 GM/T 0039 第 6.9.1 章节关于密码模块检测规程要求。

JY13.02：检测人员应核实文档如何使 CSP 和 PSP 免遭非授权修改和替换。

JY13.03：检测人员可（绕开文档描述的保护机制）尝试非授权修改和替换 CSP 和 PSP，以查看模块拒绝访问。

JY13.04：检测人员可使用送检材料中任何未说明的方法修改 CSP 和 PSP。

6.8.2 随机比特生成器

AY13.1.01：

满足GM/T 0005-2012随机性检测要求。

送检文档

CY13.1.01：参见 GM/T 0039 第 6.9.2 章节关于软件密码模块送检文档的要求。

检测规程及方法

JY13.1.01：参见 GM/T 0039 第 6.9.2 章节关于软件密码模检测规程要求。

6.8.3 敏感安全参数的生成

AY13.2.01：

CMMST-KPBMC 敏感安全参数遵照 GM/T 0028 7.9.3 要求生成。

（1） d_{A1}、d_{A2}、d_{A3} 分别在 MST-CC、SS-CC、TPSS-CC 中生成。

（2） 密钥双端协同计算架构公钥 P_A 在移动端生成。

（3） 密钥三端协同计算保护架构公钥 P_A 在服务端生成。

（4） PPD 由 MST-CC 接收用户输入生成。

送检文档

CY13.2.01：参见 GM/T 0039 第 6.9.3 章节关于密码模块送检文档的要求。

CY13.2.02：送检单位的文档需描述本节上文（1）～（4）条描述的敏感安全参数产生方法。

检测规程及方法

JY13.2.01：参见 GM/T 0039 第 6.9.3 章节关于密码模检测规程要求。

JY13.2.02：检测人员应核实送检单位的文档所描述本节上文（1）～（4）条描述的敏感安全参数产生方法的准确性，举证责任在送检单位，如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。

JY13.2.03：送检人员可使用 d_{A1}、d_{A2}、d_{A3}三个分量生成公私钥，再使用经检测认证的公钥算法检查该公私钥的准确性。

6.8.4 敏感安全参数的建立

AY13.3.01：

CMMST-KPBMC 敏感安全参数遵照 GM/T 0028 7.9.4 要求建立。

送检文档

CY13.3.01：参见 GM/T 0039 第 6.9.4 章节关于密码模块送检文档的要求。

检测规程

JY13.4.01：参见 GM/T 0039 第 6.9.4 章节关于密码模块检测规程要求。

6.8.5 敏感安全参数的输入和输出

AY13.4.01：

CMMST-KPBMC 敏感安全参数遵照 GM/T 0028 7.9.5 要求输入输出。

（1） d_{A1}、d_{A2}、d_{A3}不输出到密码模块外。

（2） PPD 输入防护须采用输入试错锁定机制，设置试错次数。

送检文档

CY13.4.01：参见 GM/T 0039 第 6.9.5 章节关于安全一、二级密码模块送检文档的要求。

CY13.4.02：送检单位提交的文档中需描述不允许 d_{A1}、d_{A2}、d_{A3}出现在密码模块外的机制。

CY13.4.03：送检单位提交的文档中需描述不同类型 PPD 的输入方式以及对应该类型输入方式的试错锁定机制和方法，针对试错次数的确定进行描述。

检测规程及方法

JY13.4.01：参见 GM/T 0039 第 6.9.5 章节关于安全一、二级软件密码模块检测规程要求。

JY13.4.02：检测人员需核实送检单位提交的文档中所描述本节上文（1）～（2）描述要求的实现方法。

JY13.4.03：检测人员需核实送检单位提交的文档中是否有对 d_{A1}、d_{A2}、d_{A3}不允许出现在密码模块外的描述。

JY13.4.04：检测人员需核实 d_{A1}、d_{A2}、d_{A3}不允许出现在密码模块外的实现方法。

JY13.4.05：检测人员需核实 PPD 输入防护是否采用了输入试错锁定机制，核实超过试错次

数是否进行锁定。

6.8.6 敏感安全参数的存储

AY13.5.01：

CMMST-KPBMC敏感安全参数遵照GM/T 0028 7.9.6要求存储。

（1） d_{A1}、d_{A2}、d_{A3}分别在MST-CC、SS-CC、TPSS-CC中存储。

（2） 至少使用PPD对d_{A1}进行（加密）保护。

（3） 使用服务端密钥对d_{A2}、d_{A3}进行（加密）保护。

（4） d_{A2}、d_{A3}应实现禁用或者销毁。

送检文档

CY13.5.01：参见 GM/T 0039 第 6.9.6 章节关于密码模块送检文档的要求。

CY13.5.02：送检单位提交的文档中需描述如何保证 d_{A1}、d_{A2}、d_{A3} 分别在 MST-CC、SS-CC、TPSS-CC 中的安全存储机制。

CY13.5.03：送检单位提交的文档中需描述 d_{A1} 使用 PPD 进行保护的方式，以及如何获取使用 d_{A1} 的实现机制。

CY13.5.04：送检单位提交的文档中需描述 d_{A2}、d_{A3} 如何使用服务端密钥进行机密性保护的方式。

CY13.5.05：送检单位提交的文档中需描述 d_{A2}、d_{A3} 禁用或者销毁的实现方式以及在何种情况下触发禁用或者销毁的机制。

检测规程及方法

JY13.5.01：参见 GM/T 0039 第 6.9.6 章节关于密码模块检测规程要求。

JY13.5.02：检测人员需核实送检单位提交的文档中是否描述 d_{A1}、d_{A2}、d_{A3} 分别在 MST-CC、SS-CC、TPSS-CC 中的安全存储机制，并对存储结果进行验证。

JY13.5.03：检测人员需核实送检单位提交的文档中是否描述 PPD 保护 d_{A1} 的实现方式，并验证在未通过 PPD 验证的情况下，不能使用 d_{A1}。

JY13.5.04：检测人员需核实送检单位提交的文档中是否描述 d_{A2}、d_{A3} 被服务端密钥进行加密保护的方式，并验证未通过解密的情况下不能正常使用 d_{A2}、d_{A3}，即 d_{A2}、d_{A3} 不解密的情况下，结合 d_{A1} 进行协同签名计算，计算出的签名值使用公钥 P_A 验证失败。

JY13.5.05：检测人员需核实送检单位提交的文档中是否描述 d_{A2}、d_{A3} 禁用或者销毁的实现方式，并验证在特殊情况下是否会出发 d_{A2}、d_{A3} 禁用或者销毁机制，即检测员按照送检单位描述的特殊情况触发 d_{A2}、d_{A3} 禁用或者销毁流程，然后再次使用 d_{A2}、d_{A3} 进行协同计算，验证是否还能正常计算出签名值并成功验签。

6.8.7 敏感安全参数的置零

AY13.6.01：

遵照GM/T 0028 7.9.7要求，CMMST-KPBMC没有未受保护的敏感安全参数，不需置零操作。

注：本条款不单独进行检测。

6.9 自测试

AY14.01：

CMMST-KPBMC除满足GM/T 0028 7.10对安全二级的技术要求外，还符合以下要求：

（1） 在协同生成用户私钥的同时，应生成自测试密钥。

（2） 软件每次启用、测试网络连通性后，应当对随机数进行自测试。

（3） 软件每次启用、测试网络连通性后，应当使用自测试密钥进行功能自测试。

送检文档

CY14.01：参见 GM/T 0039 第 6.10 章节关于安全一、二级密码模块送检文档的要求。

CY14.02：送检单位提交的文档中需描述本节上文（1）～（3）描述要求的实现方法。

CY14.03：送检单位提交的文档中需描述自测试过程中错误码描述。

CY14.04：送检单位提交的文档中需描述自测试报告的内容。

检测规程及方法

JY14.01：参见 GM/T 0039 第 6.10 章节关于安全一、二级密码模块检测规程要求。

JY14.02：检测单位需核实送检单位提交的文档中所描述本节上文（1）～（3）描述要求的实现方法。

6.10 生命周期保障

AY15.01：

符合密钥多端协同计算技术架构的密码模块需满足GM/T 0028 7.11对安全二级的技术要求。

送检文档

CY15.01：参见 GM/T 0039 第 6.11.1 章节关于密码模块送检文档的要求。

检测规程及方法

JY15.01：参见 GM/T 0039 第 6.11.1 章节关于密码模块检测规程要求。

6.11 对其他攻击的缓解

AY16.01：

符合密钥多端协同计算技术架构的密码模块需满足GM/T 0028 7.11对安全二级的技术要求。

送检文档

CY16.01：参见 GM/T 0039 第 6.12 章节关于安全一、二级密码模块送检文档的要求。

检测规程及方法

JY16.01：参见 GM/T 0039 第 6.12 章节关于安全一、二级密码模块检测规程要求。