ICS 35.240
L70/84

团　　体　　标　　准

T/ EMCG 004.1-2021

移动智能终端密码模块安全检测要求 第1部分：密钥加密本地保护密码模块检测

Security test requirements for cryptographic modules in mobile smart terminal
Part 1: Key-encrypted local protection

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 II
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 符号和缩略语 1
5 文档结构 2
5.1 概述 2
5.2 条款 2
6 安全检测要求 2
6.1 密码模块规格 2
6.2 密码模块接口 4
6.3 角色、服务和鉴别 5
6.4 软件/固件安全 7
6.5 运行环境 8
6.6 密码模块物理安全 8
6.7 非入侵式安全 8
6.8 敏感安全参数管理 9
6.9 自测试 15
6.10 生命周期保障 15
6.11 对其他攻击的缓解 19

前　言

T/EMCG 004-2021《移动智能终端密码模块安全检测要求》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安全检测要求》的第1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安全检测要求》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：张凡、王克、王冬冬、贾世杰、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1部分：密钥加密本地保护密码模块检测

1 范围

本文件依据T/EMCG 001.2-2019技术架构，规定了密钥加密本地保护密码模块的一系列检测规范、检测方法和送检文档要求。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安全检测要求》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 0003.3 SM2椭圆曲线公钥密码算法第3部分：密钥交换协议

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

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合于本文件。

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）
CC	密码组件（cryptography components）
CMMST	移动智能终端密码模块（mobile smart terminal cryptography components）
CMMST-KELP	密钥加密本地保护移动智能终端密码模块（CMMST of key-encrypted local protection）
CSP	关键安全参数（critical security parameter）
P_M	用户公钥（user public key）
d_M	用户私钥（user private key）
MK	主密钥（master key）

MKC	主密钥分量（master key component）
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 cryptography components ）
MST-PPD	移动智能终端个人特征数据（mobile smart terminal personal profile data）
PIN	个人身份标识码（personal identification number）
PPD	个人特征数据（personal profile data）
PSP	公开安全参数（public security paramete）
SDK	软件开发套件（software development kit）
SS	服务端（server side）
SSP	敏感安全参数（sensitive security parameter）
SS-CC	服务端密码组件（server side Cryptography components）
SS-MKC	服务端主密钥分量（server side master key component）

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 001.2-2019中第8~18章的11个安全域。

5.2 条款

在第6章的每条中，T/EMCG 001.2-2019中的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 001.2-2019。

各条款格式为：

安全要求

AY<T/EMCG 001.2-2019对应内容章节号>.<条款序列号>

送检文档

CY<T/EMCG 001.2-2019对应内容章节号>.<条款序列号>

检测规程及方法

JY<T/EMCG 001.2-2019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 001.2-2019中11个安全域第8~18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

AY8.1.01：

CMMST-KELP为软件模块类型，须满足GM/T 0028-2014 7.2.2节关于软件模块的要求。

送检文档

CY8.1.01：送检单位的文档中应解释CMMST-KELP软件密码模块类型选择的依据。

CY8.1.02：送检单位应提供CMMST-KELP密码模块的规格，以标识所有CMMST-KELP密码模块的软件部件。

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标识了AY8.1.01中模块类型。

JY8.1.02：检测人员应通过审查送检单位提供的规格文档，并识别所有软件部件，核实该CMMST-KELP密码模块与AY8.1.01定义的密码模块类型一致。

6.1.2 密码边界

AY8.2.01：

CMMST-KELP边界为MST-CC、SS-CC的可执行文件和文件集。

送检文档

CY8.2.01：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。

检测规程及方法

JY8.2.01：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。

AY8.2.02：

MST-CC包括完成以下功能的模块：密码算法，PPD管理，MK生成，SS-CC通信，MST-CC服务接口。

送检文档

CY8.2.02：送检单位的文档中应表明MST-CC内部软件架构，包括软件部件是怎样交互的。

检测规程及方法

JY8.2.02：检测人员应核实MST-CC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。

AY8.2.03：

SS-CC包括完成以下功能的模块：密码算法，密码主管PIN码管理，密钥容器，MST-CC管理，MST-CC通信。

送检文档

CY8.2.03：送检单位的文档中应表明SS-CC内部软件架构，包括软件部件是怎样交互的。

检测规程及方法

JY8.2.03：检测人员应核实SS-CC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。

AY8.2.04：

MST-CC、SS-CC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。MST-CC与SS-CC通过通信模块完成数据交换。

送检文档

CY8.2.04：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）。

检测规程及方法

JY8.2.04：检测人员应核实送检单位的文档描述中软件部件交互的内部软件组成。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清单。

JY8.2.04：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）。

6.1.3 工作模式

AY8.3.01：

须满足GM/T 0028-2014 7.2.4中对安全一级,安全二级软件模块的要求。

送检文档

参见GM/T 0039 6.2.4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

参见GM/T 0039 6.2.4章节关于安全一、二级软件密码模块检测规程要求。

6.2 密码模块接口

6.2.1 物理和逻辑接口

AY9.1.01：

CMMST-KELP逻辑接口分布在MST-CC和SS-CC上，两方逻辑接口类型相同。

送检文档

CY9.1.01：送检单位的文档中应说明MST-CC、SS-CC、密码算法，密码主管PIN码管理，密钥容器，MST-CC管理，MST-CC通信逻辑接口，包括：

——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；

——逻辑接口的特征。

检测规程及方法

JY9.1.01：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、密码算法，密码主管PIN码管理，密钥容器，MST-CC管理，MST-CC通信的逻辑端口。所需的说明包括：

——所有的逻辑输入输出接口（例如，API和所有其他数据、控制、状态信号）；

——所有逻辑接口的特征。

JY9.1.02：检测人员应通过检查送检单位提供的的框图、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。

JY9.1.03：检测人员应核实对于每个密码模块的逻辑输入以及逻辑输出，送检单位的文档明确逻辑接口的特征。

JY9.1.04：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。

JY9.1.05：检测人员可通过使用已知的 SS-CC 公钥，MST-CC 的公私钥还原 MST-CC 与 SS-CC 之间通信明文的方式核实 MST-CC 与 SS-CC 之间加密通信方式。

JY9.1.06：检测人员可通过使用送检单位说明的 MST-CC 模块 API 编制相应的测试程序，通过测试程序运行结果判断 MST-CC 的 API 是否与设计说明一致。

6.2.2 接口类型

AY9.2.01：

CMMST-KELP接口类型为软件或固件模块接口(SFMI)类型。

注：本条款不单独进行检测。

6.2.3 接口定义

AY9.3.01：

CMMST-KELP接口定义参照GM/T 0019-2012通用密码服务接口规范。

送检文档

CY9.3.01：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

JY9.3.01：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。

6.2.4 可信通道

AY9.4.01:

对于CMMST-KELP此项无要求。

注：本条款不单独进行检测。

6.3 角色、服务和鉴别

6.3.1 角色

AY10.1.01：

CMMST-KELP设有两种角色：移动应用用户，密码主管。

移动应用用户：MST使用者，使用MST-CC实现密钥生成、数据签名/验签及加解密等；

密码主管：负责操作SS-CC， 以及CMMST-KELP系统管理。

送检文档

CY10.1.01：送检单位的文档中应说明是否支持多个角色同时操作。

CY10.1.02：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。

CY10.1.03：送检单位还应描述多个角色的限制。

CY10.1.04：送检单位的密码模块产品应包括至少一个密码主管角色。

CY10.1.05：送检单位的文档应描述密码主管角色的功能。

CY10.1.06：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

JY10.1.01：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角色与服务强制隔离的方法。

JY10.1.02：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与服务的分离。

JY10.1.03：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。

JY10.1.04：检测人员应核实送检单位的文档中描述了密码主管角色的功能。

JY10.1.05：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

AY10.2.01：

CMMST-KELP除按GM/T 0028-2014 7.4.3.1中对安全一级、安全二级软件模块的要求提供必需的服务外，SS-CC还须提供面向密码主管角色的操作服务，包括用户管理及安全策略管理（如MST-PPD验证次数设置）等。

送检文档

CY10.2.01：送检单位的文档需说明密码模块所提供的面向密码主管角色的操作服务。

检测规程及方法

JY10.2.01：检测单位应核实送检单位的文档中描述的为密码主管角色提供的操作服务。

6.3.2.2 旁路能力

AY10.2.1.01：

CMMST-KELP不提供旁路能力或功能。

注：本条款不单独进行检测。

6.3.2.3 自启动密码服务能力

AY10.2.2.01：

CMMST-KELP不提供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

AY10.2.3.01：

CMMST-KELP不提供加载外部软件/固件功能。

注：本条款不单独进行检测。

6.3.3 鉴别

AY10.3.01：

除满足GM/T 0028-2014 7.4.4中对安全一级、安全二级软件模块的要求外，还需支持以下基于角色的鉴别：

移动应用用户须输入MST-PPD经SS-CC验证，方可调MST-CC密码服务。

送检文档

CY10.3.01：参见GM/T 0039 6.4.4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

JY10.3.01：参见GM/T 0039 6.4.4章节关于安全一、二级软件密码模块检测规程要求。

AY10.3.02

除满足GM/T 0028-2014 7.4.4中对安全一级、安全二级软件模块的要求外，还需支持以下基于角色的鉴别：

SS-CC验证密码主管输入PIN码，方可执行操作。

送检文档

CY10.3.02：送检单位文档需说明SS-CC管理员和移动应用用户的鉴别方式。

检测规程及方法

JY10.3.02：检测单位应核实送检单位的文档中描述的SS-CC管理员和移动应用用户的鉴别方式。

6.4 软件/固件安全

AY11.01：

除满足GM/T 0028-2014 7.5中对安全一级、安全二级软件模块的要求外，CMMST-KELP软件安全措施还包括但不限于：

（1） 采用CMMST-KELP自身核准的完整性算法对MST-CC和SS-CC程序进行保护；

（2） 采取缓解动静态分析、攻击方法，对CMMST-KELP代码进行保护。如，代码、数据完整性检测，防动态调试，可执行代码混淆等。

送检文档

CY11.01：参见GM/T 0039 6.5章节关于安全一、二级软件密码模块送检文档要求。

CY11.02：送检单位文档需说明软件密码模块对自身完整性保护的方法。

CY11.03：送检单位文档需说明软件密码模块缓解动静态分析、攻击的方法。

检测规程及方法

JY11.01：参见GM/T 0039 6.5章节关于安全一、二级软件密码模块检测规程要求。

JY11.02：检测单位应核实送检单位文档说明的软件密码模块对自身完整性保护的方法。

JY11.03：检测单位应核实送检单位文档说明软件密码模块缓解动静态分析、攻击的方法。

6.5 运行环境

6.5.1 运行环境通用要求

AY12.1.01：

CMMST-KELP运作在可修改的运行环境中。

注：本条款不单独进行检测。

6.5.2 可修改运行环境的操作系统要求

AY12.2.01：（安全一级）

遵照GM/T 0028-2014 7.6.3中对应的安全1级要求。

送检文档

CY12.2.01：参见 GM/T 0039 6.6.3 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

JY12.2.01：参见 GM/T 0039 6.6.3 章节关于安全一、二级软件密码模块检测规程要求。

AY12.2.02：（安全二级）

在安全一级基础上，增加以下措施：

a) MST-CC须运行在独立的进程空间中；

b) MST-CC 须运行在合法的操作系统中，如未 root、未越狱的操作系统；

c) SS-CC 须运行在工艺设计、硬件配置等方面采取了相应的保护措施，具备基本物理安全防护的主机上。

送检文档

CY12.2.02：送检单位需说明密码模块 MST-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

检测规程及方法

JY12.2.02：检测单位需核实送检单温文档中描述的 MST-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 密码模块物理安全

AY13.01：

CMMST-KELP无物理安全要求。

注：本条款不进行检测。

6.7 非入侵式安全

AY14.01：

CMMST-KELP对此无要求。

注：本条款不进行检测。

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

AY15.01：

CMMST-KELP敏感安全参数包括：

MST-CC关键安全参数：

r_M——MST-CC 与 SS-CC 通信加密使用的随机产生的对称密钥；

d_M——MST-CC 用户私钥；

MST-PPD——MST 用户个人特征数据；

MK——MST-CC 主密钥 ；

MST-CC公开安全参数：

P_M——MST-CC 公钥；

P_S——SS-CC 公钥；

SS-CC 关键安全参数：

d_S——SS-CC 私钥；

r_{MS}——SS-CC 与 MST-CC 通信加密使用的随机产生的对称密钥；

SS-MKC——SS-CC 产生的 MK 密钥分量，每个 MST-CC 对应一个 SS-MKC；

K_S——对称密钥，用于 SS-CC 加密存储敏感安全参数，由密码主管 PIN 码生成；

密码主管员 PIN——由密码主管员人工产生，用于产生 K_S启动 SS-CC 工作；

SS-CC 公开安全参数：

P_S——SS-CC 公钥；

P_M——MST-CC 公钥。

遵照 GM/T 0028-2014 7.9 中对安全一级、安全二级软件模块的要求，CMMST-KELP 对以上敏感安全参数进行管理。

注：本条款不单独进行检测。

AY15.02：

（1） MST-CC关键安全参数保护，防止非授权的访问、使用、泄露、修改和替换。

——d_M由MK加密存储在密钥容器文件中；

——MK由MST-PPD和SS-MKC组合生成；

——MST-PPD由用户保管；

——r_M在模块内临时生成、使用，不保存。

送检文档

CY15.01：送检单位的文档需描述 MST-CC 关键安全参数防止非授权的访问、使用、泄露、修改和替换的方法。

检测规程及方法

JY15.01：检测人员应核实送检单位的文档所描述的 MST-CC 关键安全参数防止非授权的访问、使用、泄露、修改和替换的方法。

JY15.02:检测人员可通过使用已知的 MK 打开密钥容器文件，提取 d_M 明文的方式核实 d_M 的存储方式。

JY15.03:检测人员可通过使用已知的 MST-PPD 及 SS-MKC 合成 MK 并可以正确加载密钥容器的方式核实 MK 的生成方式。

JY15.04:检测人员可通过确认测试环境中无文件保存 MST-PPD 的方式确认密码模块未保存 MST-PPD。

JY15.05:检测人员可通过确认测试环境中无文件保存 r_M 的方式确认 r_M 为临时生成，使用，不保存。

AY15.03：

（2） SS-CC关键安全参数保护，防止非授权的访问、使用、泄露、修改和替换。

——SS-MKC及SS-CC私钥d_S加密存放在密钥容器中；

——K_S由密码主管PIN生成，不永久保存；

——r_{MS}临时生成、使用，不保存。

送检文档

CY15.02：送检单位的文档需描述 SS-CC 关键安全参数防止非授权的访问、使用、泄露、修改和替换的方法。

检测规程及方法

JY15.06：检测人员应核实送检单位的文档所描述的 SS-CC 关键安全参数防止非授权的访问、使用、泄露、修改和替换的方法。

JY15.07:检测人员可通过使用已知密钥容器加密密钥可以解密出 SS-MKC 及 SS-CC 私钥 d_S 的方式核实 SS-MKC 及 SS-CC 私钥 d_S 的存储方式。

JY15.08:检测人员可通过已知 PIN 码生成的 K_S 与已知 K_S 比对验证 K_S 的生成方式。

JY15.09:检测人员可通过确认测试环境中无文件保存 r_{MS} 的方式确认 r_{MS} 为临时生成，使用，不保存。

AY15.04：

（3） MST-CC公开安全参数保护，防止非授权的修改和替换。

——P_S内置在MST-CC代码段，在MST-CC启动时对代码段做完整性校验；

——P_M 由移动应用保存。

送检文档

CY15.03：送检单位的文档需描述 MST-CC 公开安全参数保护，防止非授权的修改和替换的方法。

检测规程及方法

JY15.10：检测人员应核实送检单位的文档所描述的 MST-CC 公开安全参数保护，防止非授权的修改和替换的方法。

JY15.11:检测人员可通过修改 P_S，测试加密模块是否可正常加载的方式核实 P_S 完整性校验的有效性。

JY15.12:检测人员可通过确认测试环境中无文件保存 P_M 的方式确认 P_M 没有保存在密码模块

中。

AY15.05：

（4） SS-CC公开安全参数保护，防止非授权的修改和替换。

——P_S、P_M用 SS-CC 私钥签名保护。

送检文档

CY15.04：送检单位的文档需描述 SS-CC 公开安全参数保护，防止非授权的修改和替换的方法。

检测规程及方法

JY15.13：检测人员应核实送检单位的文档所描述的 SS-CC 公开安全参数保护，防止非授权的修改和替换的方法。

JY15.14:检测人员可通过已知 SS-CC 私钥对 P_S、P_M进行签名，并与密码模块保存的签名对比的方式核实 P_S、P_M用 SS-CC 私钥签名保护。

6.8.2 随机比特生成器

AY15.1.01：

须满足GM/T 0028-2014 7.9.2中对安全一级,安全二级软件模块的要求。

送检文档

CY15.1.01：参见 GM/T 0039 6.9.2 章节关于安全一、二级软件密码模块送检文档的要求。

检测规程及方法

JY15.1.01：参见 GM/T 0039-2015 6.9.2 章节关于安全一、二级软件密码模检测规程要求。

6.8.3 敏感安全参数的生成

AY15.2.01：

CMMST-KELP 敏感安全参数遵照 GM/T 0028—2014 7.9.3 要求生成。

送检文档

CY15.2.01：参见 GM/T 0039 6.9.3 章节关于安全一、二级软件密码模块送检文档的要求。

检测规程及方法

JY15.2.01：参见 GM/T 0039 6.9.3 章节关于安全一、二级软件密码模检测规程要求。

AY15.2.02：

CMMST-KELP 所有敏感安全参数均在 MST-CC 和 SS-CC 内产生；

送检文档

CY15.2.02：送检单位的文档需描述 MST-CC 和 SS-CC 敏感安全参数产生方法。

检测规程及方法

JY15.2.02：检测人员应核实送检单位的文档所描述的 MST-CC 和 SS-CC 敏感安全参数产生方法。

AY15.2.03：

r_M、r_{MS}使用核准的随机比特生成器生成，如 GM/T 0005-2012 随机性检测规范；

送检文档

CY15.2.03：送检单位的文档需描述随机比特生成器生成方法。

检测规程及方法

JY15.3.03：检测人员应核实送检单位的文档所描述的随机比特生成器生成方法。

AY15.2.04：

P_M、d_M、P_S、d_S生成满足 GM/T 0003.3-2012 中相关要求；

送检文档

CY15.2.04：送检单位的文档需描述 P_M、d_M、P_S、d_S生成方法。

检测规程及方法

JY15.2.04：检测人员应核实送检单位的文档所描述的 P_M、d_M、P_S、d_S生成方法。

AY15.2.05：

MK 使用 KDA 衍生，KDA 满足 GM/T 0003.3-2012 中 5.4.3 相关要求；

送检文档

CY15.2.05：送检单位的文档需描述 MK 生成方法。

检测规程及方法

JY15.2.05：检测人员应核实送检单位的文档所描述的 MK 生成方法。

AY15.2.06：

K_S由密码主管 PIN 衍生，且符合核准的密钥生成要求；

送检文档

CY15.2.06：送检单位的文档需描述 K_S生成方法。

检测规程及方法

JY15.2.06：检测人员应核实送检单位的文档所描述的 MK 生成方法。

AY15.2.07：

PPD 由密码主管 PIN 衍生，且符合核准的密钥生成要求；

送检文档

CY15.2.07：送检单位的文档需描述 PPD 生成方法。

检测规程及方法

JY15.2.07：检测人员应核实送检单位的文档所描述的 PPD 生成方法。

AY15.2.08：

SS-MKC 由密码主管 PIN 衍生，且符合核准的密钥生成要求；

送检文档

CY15.2.08：送检单位的文档需描述 SS-MKC 生成方法。

检测规程及方法

JY15.2.08：检测人员应核实送检单位的文档所描述的 SS-MKC 生成方法。

AY15.2.09：

密码主管员 PIN 由密码主管员人工产生；

送检文档

CY15.2.09：送检单位的文档需描述密码主管员 PIN 码生成方法。

检测规程及方法

JY15.2.09：检测人员应核实送检单位的文档所描述的密码主管员 PIN 码生成方法。

6.8.4 敏感安全参数的建立

AY15.3.01：

CMMST-KELP 敏感安全参数须满足 GM/T 0028-2014 7.9.4 中对安全一级,安全二级软件模块的要求建立。

送检文档

CY15.3.01：参见 GM/T 0039 6.9.4 章节关于安全一、二级软件密码模块送检文档的要求。

检测规程及方法

JY15.3.01：参见 GM/T 0039 6.9.4 章节关于安全一、二级软件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

AY15.4.01：

CMMST-KELP敏感安全参数遵照GM/T 0028-2014 7.9.5要求输入输出。

送检文档

CY15.4.01：参见 GM/T 0039 6.9.5 章节关于安全一、二级软件密码模块送检文档的要求。

检测规程及方法

JY15.4.01：参见 GM/T 0039 6.9.5 章节关于安全一、二级软件密码模块检测规程要求。

AY15.4.02：

PPD由用户通过移动应用程序MST-CC SDK接口人工输入到密码模块中。

送检文档

CY15.4.02：送检单位提交的文档中需描述 PDP 的输入方式和过程。

检测规程及方法

JY15.4.02：检测单位需核实送检单位提交的文档中所描述的 PDP 的输入方式和过程。

AY15.4.03：

密码主管员PIN由密码主管员通过服务端软件SS-CC SDK接口人工输入到密码模块中。

送检文档

CY15.4.03：送检单位提交的文档中需描述密码主管员 PIN 码的输入方式和过程。

检测规程及方法

JY15.4.03：检测单位需核实送检单位提交的文档中所描述的密码主管员 PIN 码的输入方式和过程。

AY15.4.04：

PPD和密码主管员PIN输入须满足GM/T 0028-2014 7.9.5直接输入的敏感安全参数要求。

送检文档

CY15.4.04：送检单位提交的文档中需描述 PPD 和密码主管员 PIN 码的输入方式和过程。

检测规程及方法

JY15.4.04：检测单位需核实送检单位提交的文档中所描述的 PPD 和密码主管员 PIN 码的输入方式和过程。

AY15.4.05：

r_M、r_{MS}在MST-CC及SS-CC之间传递采用核准的密码算法加密保护。

送检文档

CY15.4.05：送检单位提交的文档中需描述 r_M、r_{MS} 在 MST-CC 及 SS-CC 之间传递采用核准的密码算法加密保护的方法。

检测规程及方法

JY15.4.05：检测单位需核实送检单位提交的文档中所描述的 r_M、r_{MS} 在 MST-CC 及 SS-CC 之间传递采用核准的密码算法加密保护的方法。

6.8.6 敏感安全参数的存储

AY15.5.01：

CMMST-KELP 敏感安全参数遵照 GM/T 0028－2014 7.9.6 要求存储。

送检文档

CY15.5.01：参见 GM/T 0039 6.9.6 章节关于安全一、二级软件密码模块送检文档的要求。

检测规程及方法

JY15.5.01：参见 GM/T 0039 6.9.6 章节关于安全一、二级软件密码模块检测规程要求。

AY15.5.02：

MST-CC 加密存储的 CSP 均与 PPD 绑定，验证不通过无法使用 CSP。

送检文档及方法

CY15.5.02：送检单位提交的文档中需描述 MST-CC CSP 的保护的方法。

检测规程及方法

JY15.5.02：检测单位需核实送检单位提交的文档中所描述的 MST-CC CSP 的保护方法。

AY15.5.03：

SS-CC 加密存储的 CSP 均与密码主管 PIN 绑定关联，绑定验证不通过无法使用 CSP。

送检文档

CY15.5.03：送检单位提交的文档中需描述 SS-CC CSP 的保护的方法。

检测规程及方法

JY15.5.03：检测单位需核实送检单位提交的文档中所描述的 SS-CC CSP 的保护方法。

AY15.5.04：

MST-CC、SS-CC 中 PSP 完整性由 MST-CC 代码数据完整性检测保证。

送检文档

CY15.5.04：送检单位提交的文档中需描述 MST-CC、SS-CC 中 PSP 完整性的保护的方法。

检测规程及方法

JY15.5.04：检测单位需核实送检单位提交的文档中所描述的 MST-CC、SS-CC 中 PSP 完整性

的保护方法。

6.8.7 敏感安全参数的置零

AY15.6.01：

遵照GM/T 0028－2014 7.9.7要求，CMMST-KELP没有未受保护的敏感安全参数，不需置零操作。

注：本条款不进行检测。

6.9 自测试

AY16.01：

CMMST-KELP须满足GM/T 0028-2014 7.10中对安全一级,安全二级软件模块的要求。MST-CC自测试须在MST-PPD初始化和MST-CC启动时进行。SS-CC在提供安全服务前须进行代码数据完整性自测试。

送检文档

CY16.01:送检单位提交的文档中需描述MST-CC自测试的流程与方法，SS-CC代码完整性自测试的方法。

检测规程及方法

JY16.01:检测单位需核实送检单位提交的文档中所描述的MST-CC自测试的流程与方法，SS-CC代码完整性自测试的方法。

6.10 生命周期保障

6.10.1 配置管理

AY17.1.01：

满足GM/T 0028-2014 7.11.2中对安全一级,安全二级软件模块的要求。

送检文档

CY17.1.01：参见 GM/T 0039 6.11.1 章节关于安全一、二级软件密码模块送检文档的要求。

检测规程及方法

JY17.1.01：参见 GM/T 0039 6.11.1 章节关于安全一、二级软件密码模块检测规程要求。

AY17.1.02：

MST-CC、SS-CC开发过程以及相关文档都需要使用配置管理系统。

送检文档

CY17.1.02：送检单位提交的文档中需描述 MST-CC、SS-CC 配置管理系统的使用方法。

检测规程及方法

JY17.1.02：检测单位需核实送检单位提交的文档中所描述的 MST-CC、SS-CC 配置管理系统的使用方法。

AY17.1.03：

MST-CC、SS-CC相关代码与相关文档在配置管理中需要进行权限分离。

送检文档

CY17.1.03：送检单位提交的文档中需描述 MST-CC、SS-CC 在配置管理系统中权限分离的管理方式。

检测规程及方法

JY17.1.03：检测单位需核实送检单位提交的文档中所描述的 MST-CC、SS-CC 在配置管理系统中权限分离的管理方式。

AY17.1.04：

MST-CC、SS-CC按不同模块的代码在配置管理中需要进行权限分离。

送检文档

CY17.1.04：送检单位提交的文档中需描述 MST-CC、SS-CC 不同模块在配置管理系统中权限分离的管理方式。

检测规程及方法

JY17.1.04：检测单位需核实送检单位提交的文档中所描述的 MST-CC、SS-CC 不同模块在配置管理系统中权限分离的管理方式。

AY17.1.05：

配置管理系统维护CMMST-KELP标识和版本的更改，或每个配置条目的修订。

送检文档

CY17.1.05：送检单位提交的文档中需描述 CMMST-KELP 标识和版本的更改或每个配置条目的修订的管理方式。

检测规程及方法

JY17.1.05：检测单位需核实送检单位提交的文档中所描述的 CMMST-KELP 标识和版本的更改或每个配置条目的修订的管理方式。

AY17.1.06：

SS-CC须支持建立生成移动应用标识、安全通信预置通信密钥以开启MST-CC生命周期。

送检文档

CY17.1.06：送检单位提交的文档中需描述 SS-CC 建立生成移动应用标识、安全通信预置通信密钥以开启 MST-CC 生命周期的方式。

检测规程及方法

JY17.1.06：检测单位需核实送检单位提交的文档中所描述的 SS-CC 建立生成移动应用标识、安全通信预置通信密钥以开启 MST-CC 生命周期的方式。

AY17.1.07：

MST-CC须支持初始化密码模块以允许绑定用户。

送检文档

CY17.1.07：送检单位提交的文档中需描述 MST-CC 初始化密码模块以允许绑定用户的方式。

检测规程及方法

JY17.1.07：检测单位需核实送检单位提交的文档中所描述的 MST-CC 初始化密码模块以允许绑定用户的方式。

AY17.1.08：

MST-CC须支持绑定用户以允许移动应用用户使用密码模块密码应用。

送检文档

CY17.1.08：送检单位提交的文档中需描述 MST-CC 绑定用户以允许移动应用用户使用密码模块密码应用的方式。

检测规程及方法

JY17.1.08：检测单位需核实送检单位提交的文档中所描述的 MST-CC 绑定用户以允许移动应用用户使用密码模块密码应用的方式。

AY17.1.09：

MST-CC须支持解绑、注销用户以禁止移动应用用户使用密码模块密码应用。

送检文档

CY17.1.09：送检单位提交的文档中需描述 MST-CC 解绑、注销用户以禁止移动应用用户使用密码模块密码应用的方式。

检测规程及方法

JY17.1.09：检测单位需核实送检单位提交的文档中所描述的 MST-CC 解绑、注销用户以禁止移动应用用户使用密码模块密码应用的方式。

AY17.1.10：

MST-CC须支持注销以销毁内存中的SSP。

送检文档

CY17.1.10：送检单位提交的文档中需描述 MST-CC 注销以销毁内存中的 SSP 的方式。

检测规程及方法

JY17.1.10：检测单位需核实送检单位提交的文档中所描述的 MST-CC 注销以销毁内存中的 SSP 的方式。

AY17.1.11：

SS-CC须支持注销移动应用标识以结束MST-CC生命周期。

送检文档

CY17.1.10：送检单位提交的文档中需描述 SS-CC 注销移动应用标识以结束 MST-CC 生命周期的方式。

检测规程及方法

JY17.1.10：检测单位需核实送检单位提交的文档中所描述的 SS-CC 注销移动应用标识以结束 MST-CC 生命周期的方式。

6.10.2 设计

AY17.2.01：

满足GM/T 0028-2014 7.11.3中对安全一级,安全二级软件模块的要求。

送检文档

CY17.2.01：参见 GM/T 0039 6.11.2 章节关于安全一、二级软件密码模块送检文档的要求。

检测规程及方法

JY17.2.01：参见 GM/T 0039 6.11.2 章节关于安全一、二级软件密码模块检测规程要求。

6.10.3 开发

AY17.3.01：

满足GM/T 0028-2014 7.11.5中对安全一级,安全二级软件模块的要求。

送检文档

CY17.3.01：参见 GM/T 0039 6.11.5 章节关于安全一、二级软件密码模块送检文档的要求。

检测规程及方法

JY17.3.01：参见 GM/T 0039 6.11.5 章节关于安全一、二级软件密码模块检测规程要求。

6.10.4 厂商测试

AY17.4.01：

满足GM/T 0028-2014 7.11.6中对安全一级,安全二级软件模块的要求。

送检文档

CY17.4.01：参见 GM/T 0039 6.11.6 章节关于安全一、二级软件密码模块送检文档的要求。

检测规程及方法

JY17.4.01：参见 GM/T 0039 6.11.6 章节关于安全一、二级软件密码模块检测规程要求。

6.10.5 有限状态模型

AY17.5.01：

满足GM/T 0028-2014 7.11.4中对安全一级,安全二级软件模块的要求。CMMST-KELP有限状态模型至少包括下列状态：

（1）..出厂状态：CMMST-KELP集成（安装）后尚未使用时所处状态。

（2）..自测试状态：CMMST-KELP正在执行自测试时所处的状态。

（3）..初始化状态：CMMST-KELP密码模块初始运行后进入“初始化状态”。

（4）..用户状态：当移动应用使用CMMST-KELP进行核准的密码服务时所处的状态。

（5）..核准的状态。CMMST-KELP正在执行核准的密码功能时所处的状态，当密码服务完成后退出此状态，转到用户状态。

（6）..关键安全参数输入状态。当MST-CC接收用户个人特征数据（PPD）时所处的状态。，而当用户输入正确PPD后将回到用户状态。

（7）..锁定状态：当用户输入PPD错误次数达到一定的阈值后CMMST-KELP将进入锁定状态。

（8） 错误状态。当密码模块遇到错误状况时转到此状态。

送检文档

CY17.5.01：参见 GM/T 0039 6.11.4 章节关于安全一、二级软件密码模块送检文档的要求。

CY17.5.02：送检单位提交的文档中需描述本节上文（1）～（8）描述要求的实现方法。

检测规程及方法

JY17.5.01：参见 GM/T 0039 6.11.4 章节关于安全一、二级软件密码模块检测规程要求。

JY17.5.02：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）～（8）描述要求的实现方法。

6.10.6 配送与操作

AY17.6.01：

CMMST-KELP采取以下措施进行配送：

（1）CMMST-KELP 安装、初始化和启动流程见 6.1.3.1 MST-CC 初始化流程；

（2）SS-CC 可在 MST-CC 模块初始化时对 MST-CC 代码进行完整性检测，确保 MST-CC 未被篡改。

送检文档

CY17.6.01：参见 GM/T 0039 6.11.7 章节关于安全一、二级软件密码模块送检文档的要求。

CY17.6.02：送检单位提交的文档中需描述本节上文（1）～（2）描述要求的实现方法。

检测规程及方法

JY17.6.01：参见 GM/T 0039 6.11.7 章节关于安全一、二级软件密码模块检测规程要求。

JY17.6.02：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）～（2）描述要求的实现方法。

6.10.7 生命终止

AY17.7.01：

MST-CC中加密存储的敏感安全参数可由密码主管角色通过SS-CC下指令清除。

送检文档

CY17.7.01：送检单位提交的文档中需描述 MST-CC 敏感安全参数被密码主管通过 SS-CC 指令清除的实现方法。

检测规程及方法

JY17.7.01：检测单位需核实送检单位提交的文档中所描述 MST-CC 敏感安全参数被密码主管通过 SS-CC 指令清除的实现方法。

6.10.8 指南文档

AY17.8.01：

满足GM/T 0028-2014 7.11.9中对安全一级,安全二级软件模块的要求。

送检文档

CY17.8.01：参见 GM/T 0039 6.11.9 章节关于安全一、二级软件密码模块送检文档的要求。

检测规程及方法

JY17.8.01：参见 GM/T 0039 6.11.9 章节关于安全一、二级软件密码模块检测规程要求。

6.11 对其他攻击的缓解

AY18.01：

CMMST-KELP对此无要求。

注：本条款不进行检测。