ICS 35.240
L70/84

团　　体　　标　　准

T/ EMCG 004.2-2021

移动智能终端密码模块安全检测要求 第 2 部分：密钥加密服务端保护密码模块检测

Security test requirements for cryptographic modules in mobile smart terminal
Part 2: Key-encrypted protection on server side

EMCG

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

EMCG

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2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：汪德嘉、朱旭光、王克、张昀球、王冬冬、贾世杰、张凡、傅文斌等。

EMCG

移动智能终端密码模块安全检测要求
第2部分：密钥加密服务端保护密码模块检测

1 范围

本文件依据T/EMCG 001.3-2019技术架构，规定了密钥加密服务端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 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术语和定义

T/ZISIA-EMCG 001.3-2019所界定的术语和定义适用于本文件。

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）
CSP	关键安全参数（critical security parameter）
CMMST	移动智能终端密码模块（cryptographic module of mobile smart terminal）
CMMST-KEPOSS	密钥加密服务端保护移动智能终端密码模块（CMMST of key-encrypted protection on server side）
P_M	用户公钥（user public key）
d_M	用户私钥（user private key）

MK	主密钥（master key）
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 PPD）
PSP	公开安全参数（public security parameter）
SDK	软件开发工具包（software development kit）
SSP	敏感安全参数（sensitive security parameter）
SS-CC	服务端密码组件（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 001.3-2019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 001.3-2019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 001.3-2019。

各条款格式为：

AY<T/EMCG 001.3-2019对应内容章节号>.<条款序列号>

送检文档

CY<T/EMCG 001.3-2019对应内容章节号>.<条款序列号>

检测规程及方法

JY<T/EMCG 001.3-2019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 001.3-2019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-KEPOSS为软件密码模块，完成核准的SM2，SM3，SM4算法。

送检文档

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

CY8.1.02：送检单位应提供CMMST-KEPOSS密码模块的规格，以标识所有CMMST-KEPOSS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-KEPOSS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-KEPOSS边界为MST-CC及SS-CC的可执行文件或文件集。

送检文档

CY8.2.01：送检单位的文档中应详细说明密码边界内MST-CC、SS-CC的所有部件。

检测规程及方法

JY8.2.01：检测人员应通过文档审查和模块检查核实MST-CC、SS-CC所有部件在密码边界内。

JY8.2.02：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。

AY8.2.02：

MST-CC至少包括完成以下功能的模块：SSP加解密、MK生成、密码算法、SS-CC通信、环境安全检测、PPD输入、CMMST-KEPOSS-API。

送检文档

CY8.2.02：送检单位的文档中描述的MST-CC的所有部件应包括SSP加解密、MK生成、密码算法、SS-CC通信、环境安全检测、PPD输入、CMMST-KEPOSS-API。

检测规程及方法

JY8.2.03：检测人员应通过文档审查和模块检查核实MST-CC只有SSP加解密、MK生成、密码算法、SS-CC通信、环境安全检测、PPD输入、CMMST-KEPOSS-API模块。

AY8.2.03：

SS-CC至少包括完成以下功能的模块：密码算法、SSP存储管理、MST-CC通信。

送检文档

CY8.2.03：送检单位的文档中描述的SS-CC的所有部件应包括密码算法、SSP存储管理、MST-CC通信。

检测规程及方法

JY8.2.04：检测人员应通过文档审查和模块检查核实SS-CC只有密码算法、SSP存储管理、MST-CC通信模块。

6.1.3 工作模式

AY8.3.01：

须满足GM/T 0028 7.2.4中对安全一级，安全二级软件模块的要求。

送检文档

CY8.3.01：送检单位的文档按照GM/T 0039 6.2.4 所要求的送检材料。

检测规程及方法

JY8.3.01：检测人员按照GM/T 0039 6.2.4 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

AY9.1.01：

CMMST-KEPOSS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密码模块MST-CC、SS-CC及TPSS-CC的每个逻辑接口，包括：

——MST-CC的SSP加解密、MK生成、密码算法、SS-CC通信、环境安全检测、PPD输入、CMMST-KEPOSS-API的协议、控制信号；

——SS-CC的密码算法、SSP存储管理、MST-CC通信的协议、控制信号等。

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及TPSS-CC每个逻辑端接口。所需的说明包括：

——MST-CC的SSP加解密、MK生成、密码算法、SS-CC通信、环境安全检测、PPD输入、CMMST-KEPOSS-API的协议、控制信号；

——SS-CC的密码算法、SSP存储管理、MST-CC通信的协议、控制信号等。

6.2.2 接口类型

AY9.2.01：

须满足GM/T 0028 7.3.2中对安全一级,安全二级软件模块的要求，CMMST-KEPOSS为软件模块，向移动应用提供API调用。

送检文档

CY9.2.01：送检单位的文档按照GM/T 0039 6.3.2 所要求的送检材料。

检测规程及方法

JY9.2.01：检测人员按照GM/T 0039 6.3.2 所要求的检测规程。

6.2.3 接口定义

AY9.3.01：

CMMST-KEPOSS接口定义参照GM/T 0019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，包含MST-CC、SS-CC两个密码组件接口。

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，包含MST-CC、SS-CC两个密码组件接口。

6.3 角色、服务和鉴别

6.3.1 角色

AY10.1.01：

CMMST-KEPOSS设立两种角色：SS-CC管理员、移动应用用户。

送检文档

CY10.1.01：送检单位的密码模块产品应包括至少两种角色，SS-CC管理员、移动应用用户。

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定义了至少两种角色，SS-CC管理员、移动应用用户。

AY10.1.02：

SS-CC管理员：负责SS-CC初始化，密钥密文数据库管理。

送检文档

CY10.1.02：送检单位的文档中应描述SS-CC管理员角色的功能包括：SS-CC初始化，密钥密文数据库管理。

检测规程及方法

JY10.1.02：检测人员应核实送检单位的文档中描述了SS-CC管理员角色的功能。

AY10.1.03：

移动应用用户：执行密码功能，如数据签名、数据验签、数据加密、数据解密。

送检文档

CY10.1.03：送检单位的文档中应描述移动应用用户角色的功能包括：执行密码功能，如数据签名、数据验签、数据加密、数据解密。

检测规程及方法

JY10.1.03：检测人员应核实送检单位的文档中描述了移动应用用户角色的功能。

6.3.2 服务

6.3.2.1 服务通用要求

AY10.2.01：

为SS-CC管理员、移动应用用户角色所提供的服务如表1：

表1 CMMST-KEPOSS角色与服务

服　务	描　述	SS-CC 管理员	移动应用 用户
SS-CC初始化	初始化SS-CC，为MST-CC提供运行基础。	√	×
MST-CC的初始化	初始化MST-CC	×	√
数据签名	为移动应用提供数据签名	×	√
数据验签	为移动应用提供数据签名验签	×	√
数据加密	为移动应用提供数据加密	×	√
数据解密	为移动应用提供数据解密	×	√

送检文档

CY10.2.01：送检单位的文档中应说明为SS-CC管理员提供的SS-CC初始化服务。

CY10.2.02：送检单位的文档中应说明为移动应用用户提供的服务，包括：MST-CC的初始化、数据签名、数据验签、数据加密、数据解密。

检测规程及方法

JY10.2.01：检测人员应核实送检单位文档中说明的SS-CC管理员提供的SS-CC初始化服务是否得到实现。

JY10.2.02：检测人员应核实送检单位文档中说明的移动应用用户提供的服务是否得到实现，包括：MST-CC的初始化、数据签名、数据验签、数据加密、数据解密。

6.3.2.2 旁路能力

AY10.2.1.01：

CMMST-KEPOSS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

AY10.2.2.01：

CMMST-KEPOSS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

AY10.2.3.01：

CMMST-KEPOSS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

AY10.3.01：

CMMST-KEPOSS应满足GM/T 0028 7.4.4中对安全一级,安全二级软件模块的要求。

注：本条款不单独进行检测。

AY10.3.02：

CMMST-KEPOSS的SS-CC管理员：输入口令SS-CC方可执行操作。

送检文档

CY10.3.02：送检单位的文档中应说明SS-CC管理员需要进行基于口令的身份鉴别。

检测规程及方法

JY10.3.02：检测人员应核实送检单位的文档中说明了SS-CC管理员的身份鉴别方式，并描述具体操作步骤和方法。

JY10.3.03：检测人员应核实按照送检单位的文档中描述的SS-CC管理员身份鉴别操作步骤和方法可以实际完成SS-CC管理员身份鉴别。

AY10.3.03：

CMMST-KEPOSS的移动应用用户：输入PPD后方可调用MST-CC完成密码服务。

送检文档

CY10.3.03：送检单位的文档中应说明移动应用用户需要使用PPD进行身份鉴别。

检测规程及方法

JY10.3.04：检测人员应核实送检单位的文档中说明了移动应用用户的身份鉴别方式，并描述具体操作步骤和方法。

JY10.3.05：检测人员应核实送检单位文档中采用了PPD作为移动应用用户的身份鉴别方式。

6.4 软件/固件安全

AY11.01：

MST-CC 自检时进行 MST-CC 完整性校验。

送检文档

CY11.01：送检单位的文档中应说明MST-CC完整性校验的方式，时机，范围。

检测规程及方法

JY11. 01：检测人员应核实送检单位的文档中说明了MST-CC完整性校验的方式，时机，范围，并描述具体操作步骤和方法。

JY11. 02：检测人员应核实按照送检单位的文档中描述的MST-CC完整性校验操作步骤和方法可以实际完成MST-CC完整性校验。

AY11. 02：

使用 MST-CC 加固措施防止软件被动态调试和静态逆向分析。

送检文档

CY11.02：送检单位的文档中应说明防止MST-CC被动态调试和静态逆向分析的措施。

检测规程及方法

JY11.03：检测人员应核实送检单位的文档中说明了防止MST-CC被动态调试和静态逆向分析的措施。

JY11.04：检测人员应核实MST-CC不能被动态调试，并可缓解静态逆向分析攻击。

6.5 运行环境

6.5.1 运行环境通用要求

AY12.1.01：

CMMST-KEPOSS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：

MST-CC须运行在独立的进程空间中；

送检文档

CY12.2.01：送检单位的文档中应描述用来确保MST-CC的进程运行在独立进程空间的操作系统机制。

检测规程及方法

JY12.2.01：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MST-CC的进程运行在独立进程空间。

AY12.2.02：

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；

送检文档

CY12.2.02：送检单位的文档中应说明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。

检测规程及方法

JY12.2.02：检测人员应核实送检单位的文档中说明了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。

JY12.2.03：检测人员应核实MST-CC不能运行在root、越狱的操作系统中。

AY12.2.03：

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

CY12.2.03：送检单位的文档中应说明SS-CC运行环境在工艺设计、硬件配置等方面采取了相应的保护措施。

检测规程及方法

JY12.2.04：检测人员应核实送检单位的文档中说明了SS-CC运行环境在工艺设计、硬件配置等方面采取了相应的保护措施。

6.6 物理安全

AY13.01：

CMMST-KEPOSS不涉及物理安全要求。

注：本条款不单独进行检测。

6.7 非入侵式安全

AY14.01：

CMMST-KEPOSS不涉及非入侵式安全要求。

注：本条款不单独进行检测。

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-KEPOSS敏感安全参数（SSP）包括：

d_M——用户私钥

P_M——用户公钥

MK——主密钥

PPD——用户个人特征数据

须满足 GM/T 0028 7.9.1 中对安全一级,安全二级软件模块的要求，

注：本条款不单独进行检测。

AY15.02：

关键安全参数（CSP）d_M、MK、PPD 在密码模块内保护以防止非授权的访问、使用、泄露、修改和替换。其中 d_M 通过核准的密码算法进行加密，保存在 SS-CC 中。

送检文档

CY15.01：送检单位的文档中应描述关键安全参数（CSP）d_M、MK、PPD在密码模块内为防止非授权的访问、使用、泄露、修改和替换的机制。

CY15.02：送检单位的文档中应描述d_M通过核准的密码算法进行加密，并保存在SS-CC中。

检测规程及方法

JY15.01：检测人员应验证送检单位的文档中所描述的关键安全参数（CSP）d_M、MK、PPD在密码模块内为防止非授权的访问、使用、泄露、修改和替换的机制的有效性。

JY15.02：检测人员可通过实际访问、使用、截取、修改和替换（CSP）d_M、MK、PPD方法，观测CMMST- KEPOSS启动自检情况，自检成功，则本测试要求通过。

JY15.03：检测人员应验证送检单位的文档中所描述的d_M通过核准的密码算法进行加密，并保存在SS-CC中的有效性。

JY15.04：检测人员可检测d_M 密文是否符合相关加密算法密文特征，检测人员可用同一公开标准算法，使用同一密钥对同一明文加密，检查密文是否与d_M一致。

AY15.03：

公开安全参数（PSP）P_M 在 MST-CC 内保存，防止非授权修改和替换。

送检文档

CY15.03：送检单位的文档中应描述公开安全参数（PSP）P_M在MST-CC内保存，防止非授权修改和替换的机制。

检测规程及方法

JY15.05：检测人员应验证送检单位的文档中所描述的公开安全参数（PSP）P_M在MST-CC内保存，防止非授权修改和替换的有效性。

JY15.06：检测人员可通过实际访问、修改和替换P_M方法，观测CMMST- KEPOSS启动自检情况，自检成功，则本测试要求通过。

AY15.04：

敏感安全参数（SSP）与移动应用用户 PPD 相关联。

送检文档

CY15.04：送检单位的文档中应描述敏感安全参数（SSP）与移动应用用户PPD相关联的机制。

检测规程及方法

JY15.07：检测人员应验证送检单位的文档中所描述的敏感安全参数（SSP）与移动应用用户PPD相关联的有效性。

JY15.08：检测人员可采用下面方法验证SSP与PPD相关联的有效性，使用同一用户PPD多次生成SSP，SPP应当一致，使用不同用户PPD生成的SPP应当不一致。

6.8.2 随机比特生成器

AY15.1.01：

须满足GM/T 0028 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：送检单位的文档按照GM/T 0039 6.9.2 所要求的送检材料。

检测规程及方法

JY15.1.01：检测人员按照GM/T 0039 6.9.2 所要求的检测规程。

6.8.3 敏感安全参数的生成

AY15.2.01：

d_M和 P_M由 MST-CC 内部的 SSP 加解密模块产生,生成符合 GM/T 0003.3 中相关规定。

送检文档

CY15.2.01：送检单位提交的文档应描述敏感安全参数用户私钥（d_M）、用户公钥（P_M）由MST-CC内部的SSP加解密模块产生的流程。

检测规程及方法

JY15.2.01：检测人员应核实送检单位的文档列出了敏感安全参数用户私钥（d_M）、用户公钥（P_M）由MST-CC内部的SSP加解密模块产生的流程。

AY15.2.02：

MK 由 PPD 通过合规的密钥产生方法（如 GM/T 0003.3 中 5.4.3 规范）产生，其过程在

MST-CC MK 生成模块中执行。

送检文档

CY15.2.02：送检单位提交的文档应描述主密钥（MK）由用户个人特征数据（PPD）通过合规的密钥产生方法。

检测规程及方法

JY15.2.02：检测人员应核实送检单位的文档列出了主密钥（MK）由用户个人特征数据（PPD）通过合规的密钥产生方法。检测人员可使用同一PPD多次调用合规的密钥产生算法应得到同一MK（此处忽略随机比特）的方法进行核实。

AY15.2.03：

PPD 由 MST-CC PPD 输入模块输入生成。

送检文档

CY15.2.03：送检单位提交的文档应描述用户个人特征数据（PPD）由MST-CC PPD输入模块输入生成的方法。

检测规程及方法

JY15.2.03：检测人员应核实送检单位的文档列出了用户个人特征数据（PPD）由MST-CC PPD输入模块输入生成的方法。检测人员可采用检测MST- CC PPD模块是否存在PIN码、指纹、人脸特征、巩膜、声纹等个人特征数据输入模块的方法进行核实。

6.8.4 敏感安全参数的建立

AY15.3.01：

CMMST-KEPOSS 敏感安全参数须满足 GM/T 0028 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：送检单位的文档按照GM/T 0039 6.9.4 所要求的送检材料。

检测规程及方法

JY15.3.01：检测人员按照GM/T 0039 6.9.4 所要求的检测规程。

6.8.5 敏感安全参数的输入和输出

AY15.4.01：

d_M和P_M由MST-CC内部自动生成。

送检文档

CY15.4.01：送检单位提交的文档应明确描述用户私钥（d_M）、用户公钥（P_M）在MST-CC内部自动生成。

CY15.4.02：检测人员应核实送检单位的文档中描述用户私钥（d_M）、用户公钥（P_M）在MST-CC内部自动生成。

检测规程及方法

JY15.4.01：检测人员应核实送检单位的文档中描述用户私钥（d_M）、用户公钥（P_M）在MST-CC内部自动生成。

AY15.4.02：

PPD由MST-CC的PDD输入模块（UI）人工输入，PPD不输出到密码模块外。

送检文档

CY15.4.03：送检单位提交的文档应明确描述PPD人工输入流程，且详细说明防止PPD泄露的机制。

检测规程及方法

JY15.4.02：检测人员应核实送检单位的文档中描述了个人特征数据（PPD）由MST-CC的PDD输入模块（UI）人工输入，个人特征数据（PPD）不输出到密码模块外，且列出了详细的业务流程。

JY15.4.03：检测人员应核实个人特征数据（PPD）由MST-CC的PDD输入模块（UI）人工输入的业务流程。

JY15.4.04：检测人员应根据送检单位的文档中详细的业务流程核实个人特征数据（PPD）不能被输出到密码模块外。

JY15.4.05：检测人员应核实防止PPD泄露机制的有效性。检测人员检测MST-CC是否存在以网络、存储等形式向外输出PPD的行为。

AY15.4.03：

MK由MST-CC的MK生成模块生成，用后清除，不输出到密码模块外。

送检文档

CY15.4.04：送检单位提交的文档应明确描述主密钥（MK）由MST-CC的MK生成模块生成，用后清除，不输出到密码模块外，且列出详细的业务流程。

检测规程及方法

JY15.4.06：检测人员应核实送检单位的文档中描述了主密钥（MK）由MST-CC的MK生成模块生成，用后清除，不输出到密码模块外，且列出了详细的业务流程。

JY15.4.07：检测人员应根据送检单位的文档中详细的业务流程核实主密钥（MK）不能被输出到密码模块外。检测人员可采用检测MST-CC是否存在以网络、存储等形式向外输出MK的行为的方法检测MK使用完成是否还在内存、硬盘、网络等地方残留。

AY15.4.04：

d_M以加密的形式输入给通信模块。

送检文档

CY15.4.05：送检单位提交的文档应明确描述用户私钥（d_M）以加密的形式输入给通信模块，且列出详细的业务流程。

检测规程及方法

JY15.4.08：检测人员应核实送检单位的文档中描述了用户私钥（d_M）以加密的形式输入给通信模块，且列出了详细的业务流程。

JY15.4.09：检测人员应根据送检单位的文档中详细的业务流程核实用户私钥（d_M）将被加密后传输给通信模块。检测人员可采用检测输入至通信模块的d_M 是否符合相关密码算法密文特征的方法进行核实。

AY15.4.05：

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

CY15.4.06：送检单位提交的文档应明确描述个人特征数据（PPD）输入防护，至少包括采用输入试错锁定机制、设置试错次数；且列出详细的业务流程。

检测规程及方法

JY15.4.10：检测人员应核实送检单位的文档中描述了个人特征数据（PPD）输入防护，且输入防护措施至少包括采用输入试错锁定机制、设置试错次数，且列出了详细的业务流程。

JY15.4.11：检测人员应根据送检单位的文档中详细的业务流程通过实际测试核实个人特征数据（PPD）输入防护机制。检测人员可采用故意输入错误PPD多次，检测PPD是否具有锁定机制和试错次数的方法进行核实。

6.8.6 敏感安全参数的存储

AY15.5.01：

用MK加密存储d_M，可使用多种PPD（如PIN码、手势码、指纹等）作为MK生成因子。

送检文档

CY15.5.01：送检单位提交的文档应明确描述用MK加密存储d_M时，可使用多种PPD（如PIN码、手势码、指纹等）作为MK生成因子，且列出详细的业务流程。

检测规程及方法

JY15.5.01：检测人员应核实送检单位的文档中描述了用MK加密存储d_M时，可使用多种PPD（如PIN码、手势码、指纹等）作为MK生成因子，且列出了详细的业务流程。

JY15.5.02：检测人员应根据送检单位的文档中详细的业务流程核实可使用多种PPD（如PIN码、手势码、指纹等）作为MK生成因子。检测人员可使用约定的一个或者多个PPD检测是否可正确解密d_M的方法进行核实。

AY15.5.02：

P_M存储在移动应用中，只有验证用户PPD后才可使用。

送检文档

CY15.5.02：送检单位提交的文档应明确描述P_M存储在移动应用中，只有验证用户PPD后才可使用，且列出详细的业务流程。

检测规程及方法

JY15.5.03：检测人员应核实送检单位的文档中描述了P_M存储在移动应用中，只有验证用户PPD后才可使用，且列出了详细的业务流程。

JY15.5.04：检测人员应根据送检单位的文档中详细的业务流程核实只有验证用户PPD后才可使用P_M。检测人员可使用非正确用户PPD或者非正确PPD检测是否可正确解密P_M的方法进行核实。

AY15.5.03：

MST-CC的d_M不以明文形式出现在MST的非易失性存储中，d_M需上传SS-CC存储。

送检文档

CY15.5.03：送检单位提交的文档应明确描述MST-CC的d_M不以明文形式出现在MST的非易失性存储中，d_M需上传SS-CC存储，且列出详细的业务流程。

检测规程及方法

JY15.5.05：检测人员应核实送检单位的文档中描述了MST-CC的d_M不以明文形式出现在MST的非易失性存储中，d_M需上传SS-CC存储, 且列出了详细的业务流程。

JY15.5.06：检测人员应根据送检单位的文档中详细的业务流程核实d_M不以明文形式出现在MST的非易失性存储中。检测人员可使用检测SS- CC是否存在d_M 的备份，d_M 未出现在非易失性存储中的方法进行核实。

AY15.5.04：

SS-CC不以明文形式存储d_M。

送检文档

CY15.5.04：送检单位提交的文档应明确描述SS-CC不以明文形式存储d_M，且列出详细的业务流程。

检测规程及方法

JY15.5.07：检测人员应核实送检单位的文档中描述了SS-CC不以明文形式存储d_M, 且列出了详细的业务流程。

JY15.5.08：检测人员应根据送检单位的文档中详细的业务流程核实SS-CC不以明文形式存储d_M。检测人员可采用检测SS-CC存储的d_M 是否符合相关加密算法密文特征的方法进行核实。

AY15.5.05：

对d_M加密时，使用的对称加密算法的密钥长度至少为32位，分组长度最多256位。

送检文档

CY15.5.05：送检单位提交的文档应明确描述对d_M加密时，使用的对称加密算法的密钥长度至少为32位，分组长度最多256位。

CY15.5.06：送检单位提交的文档应提供对称加密算法相应代码、演示程序。

检测规程及方法

JY15.5.09：检测人员应核实送检单位的文档中描述了对d_M加密时，使用的对称加密算法的密钥长度至少为32位，分组长度最多256位。

JY15.5.10：检测人员应根据送检单位提供的代码和演示程序核实使用的对称加密算法的密钥长度至少为32位，分组长度最多256位。检测人员可采用检测d_M 的加密密钥长度是否符合本条款密钥长度的规定的方法进行核实。

6.8.7 敏感安全参数的置零

AY15.6.01：

CMMST-KEPOSS中没有未受保护的SSP。满足GM/T 0028 7.9.7中对安全一级,安全二级软件模块的要求不需置零。

送检文档

CY15.6.01：送检单位的文档按照GM/T 0039 6.9.7 所要求的送检材料。

检测规程及方法

JY15.6.01：检测人员按照GM/T 0039 6.9.7 所要求的检测规程。

6.9 自测试

AY16. 01：

满足GM/T 0028 7.10中对安全一级,安全二级软件模块的要求。

MST-CC在初始化以及每次启动时进行MST-CC的自测试，包括MST-CC完整性、移动终端完整性（没有被root）等；

送检文档

CY16.01：送检单位的文档按照GM/T 0039 6.10 所要求的送检材料。

检测规程及方法

JY16.01：检测人员按照GM/T 0039 6.10 所要求的检测规程。

6.10 生命周期保障

6.10.1 配置管理

AY17.1.01：

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

CY17.1.01：送检单位的文档按照GM/T 0039 6.11所要求的送检材料。

检测规程及方法

JY17.1.01：检测人员按照GM/T 0039 6.11所要求的检测规程。

AY17.1.02：

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

CY17.1.02：送检单位的文档应明确描述配置管理权限分离的机制。

检测规程及方法

JY17.1.02：检测人员应核实送检单位的文档中描述了配置管理权限分离的机制。

JY17.1.03：检测人员应核实送检单位配置管理权限分离机制的有效性。

AY17.1.03：

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

CY17.1.03：送检单位的文档应明确描述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的机制。

检测规程及方法

JY17.1.04：检测人员应核实送检单位的文档中描述了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的机制。

JY17.1.05：检测人员应核实送检单位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机制的有效性。

AY17.1.04：

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

送检文档

CY17.1.04：送检单位的文档应明确描述配置管理系统维护CMMST-KEPOSS标识和版本的更改，或每个配置条目的修订。

检测规程及方法

JY17.1.06：检测人员应核实送检单位的文档中描述了配置管理系统维护CMMST-KEPOSS标识和版本的更改，或每个配置条目的修订。

AY17.1.05：

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

CY17.1.05：送检单位的文档应明确描述SS-CC支持建立生成移动应用标识和安全通信预置通信密钥以开启MST-CC生命周期的机制。

检测规程及方法

JY17.1.07：检测人员应核实送检单位的文档中描述了SS-CC支持建立生成移动应用标识和安全通信预置通信密钥以开启MST-CC生命周期的机制。

JY17.1.08：检测人员应核实送检单位SS-CC支持建立生成移动应用标识和安全通信预置通信密钥以开启MST-CC生命周期机制的有效性。

AY17.1.06：

MST-CC 须支持初始化密码模块以允许绑定用户。

送检文档

CY17.1.06：送检单位的文档应明确描述MST-CC支持初始化密码模块以允许绑定用户的机制。

检测规程及方法

JY17.1.09：检测人员应核实送检单位的文档中描述了MST-CC支持初始化密码模块以允许绑定用户的机制。

JY17.1.10：检测人员应核实送检单位MST-CC支持初始化密码模块以允许绑定用户机制的有效性。

AY17.1.07：

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

CY17.1.07：送检单位的文档应明确描述MST-CC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的机制。

检测规程及方法

JY17.1.11：检测人员应核实送检单位的文档中描述了MST-CC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的机制。

JY17.1.12：检测人员应核实送检单位MST-CC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机制的有效性。

AY17.1.08：

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

CY17.1.08：送检单位的文档应明确描述MST-CC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的机制。

检测规程及方法

JY17.1.13：检测人员应核实送检单位的文档中描述了MST-CC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的机制。

JY17.1.14：检测人员应核实送检单位MST-CC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机制的有效性。

AY17.1.09：

MST-CC 须支持注销以销毁内存中的 SSP。

送检文档

CY17.1.09：送检单位的文档应明确描述MST-CC支持注销以销毁内存中的SSP的机制。

检测规程及方法

JY17.1.15：检测人员应核实送检单位的文档中描述了MST-CC支持注销以销毁内存中的SSP的机制。

JY17.1.16：检测人员应核实送检单位MST-CC支持注销以销毁内存中的SSP机制的有效性。

AY17.1.10：

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：送检单位的文档应明确描述SS-CC支持注销移动应用标识以结束MST-CC生命周期的机制。

检测规程及方法

JY17.1.17：检测人员应核实送检单位的文档中描述了SS-CC支持注销移动应用标识以结束MST-CC生命周期的机制。

JY17.1.18：检测人员应核实送检单位SS-CC支持注销移动应用标识以结束MST-CC生命周期机制的有效性。

6.10.2 设计

AY17.2.01：

满足GM/T 0028 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：送检单位的文档按照GM/T 0039 6.11.3所要求的送检材料。

检测规程及方法

JY17.2.01：检测人员按照GM/T 0039 6.11.3所要求的检测规程。

6.10.3 有限状态模型

AY17.3.01：

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

（1）..出厂状态：CMMST-KEPOSS集成（安装）后尚未使用时所处状态。

（2）..自测试状态：CMMST-KEPOSS正在执行自测试时所处的状态。

（3）..初始化状态：CMMST-KEPOSS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-KEPOSS进行核准的密码服务时所处的状态。

（5）..核准的状态。CMMST-KEPOSS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-KEPOSS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

CY17.3.01：送检单位的文档按照GM/T 0039 6.11.4所要求的送检材料。

检测规程及方法

JY17.3.01：检测人员按照GM/T 0039 6.11.4所要求的检测规程。

6.10.4 开发

AY17.4.01：

满足GM/T 0028 7.11.5中对安全一级,安全二级软件模块的要求。

送检文档

CY17.4.01：送检单位的文档按照GM/T 0039 6.11.5所要求的送检材料。

检测规程及方法

JY17.4.01：检测人员按照GM/T 0039 6.11.5所要求的检测规程。

6.10.5 厂商测试

AY17.5.01：

满足GM/T 0028 7.11.6中对安全一级,安全二级软件模块的要求。

送检文档

CY17.5.01：送检单位的文档按照GM/T 0039 6.11.6所要求的送检材料。

检测规程及方法

JY17.5.01：检测人员按照GM/T 0039 6.11.6所要求的检测规程。

6.10.6 配送与操作

AY17.6.01：

满足GM/T 0028 7.11.7中对安全一级,安全二级软件模块的要求。其中：

（1）安全一级

移动应用使用软件编译方式将MST-CC嵌入移动应用中，与移动应用软件一起安装到移动终端中。密码模块初始化流程见本文档7.1章节。

（2）安全二级

满足GM/T 0028 7.11.7中对应的安全二级要求。

送检文档

CY17.6.01：送检单位的文档按照GM/T 0039 6.11.7 所要求的送检材料。

检测规程及方法

JY17.6.01：检测人员按照GM/T 0039 6.11.7 所要求的检测规程。

6.10.7 生命终止

AY17.7.01：

满足GM/T 0028 7.11.8中对安全一级,安全二级软件模块的要求。

送检文档

CY17.7.01：送检单位的文档按照GM/T 0039 6.11.8 所要求的送检材料。

检测规程及方法

JY17.7.01：检测人员按照GM/T 0039 6.11.8 所要求的检测规程。

6.10.8 指南文档

AY17.8.01：

满足GM/T 0028 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：送检单位的文档按照GM/T 0039 6.11.9 所要求的送检材料。

检测规程及方法

JY17.8.01：检测人员按照GM/T 0039 6.11.9 所要求的检测规程。

6.11 对其他攻击的缓解

AY18.01：

满足GM/T 0028 7.12中对安全一级,安全二级软件模块的要求。

送检文档

CY18.01：送检单位的文档按照GM/T 0039 6.12 所要求的送检材料。

检测规程及方法

JY18.01：检测人员按照GM/T 0039 6.12 所要求的检测规程。

EMCG