团　　体　　标　　准

T/EMCG 001.2-2019

移动智能终端密码模块技术框架
第 2 部分：密钥加密本地保护技术架构

Technical framework of cryptographic module for mobile smart terminal

Part 2: Key-encrypted local protection

2019-07-05 发布　　2019-07-05 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 001-2019《移动智能终端密码模块技术框架》分为5个部分：

第1部分：总则

第2部分：密钥加密本地保护技术架构

第3部分：密钥加密服务端保护技术架构

第4部分：密钥多端协同计算保护技术架构

第5部分：基于安全芯片的技术架构

本部分为T/EMCG 001-2019《移动智能终端密码模块技术框架》的第2部分。

本部分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。

本部分由参与T/EMCG 001-2019《移动智能终端密码模块技术框架》标准制定的单位投票表决通过。

本部分主要起草单位：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）、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、北京江南天安科技有限公司、江苏通付盾科技有限公司、北京握奇数据股份有限公司、卫士通信息产业股份有限公司、鼎桥通信技术有限公司等。

本部分主要起草人：张凡、王克、傅文斌、刘宗斌、李勃、张晶、李向荣、鲁洪成、张令臣等。

引 言

在开放移动网络和便携移动终端系统环境中，如何保护敏感安全参数成为移动智能终端密码软件模块设计和实现的核心问题。在移动智能终端中对敏感安全参数进行加密存储是解决软件密码模块安全性的主要方法。但如果加密密钥容易被非法获得，或密钥质量达不到要求则对敏感安全参数安全构成威胁。因此，本标准通过控制主密钥安全生成与使用以保证敏感安全参数加密密钥的安全。

移动智能终端密码模块技术框架
第2部分：密钥加密本地保护技术架构

1 范围

T/EMCG 001-2019《移动智能终端密码模块技术框架》的本部分规范了移动智能终端（mobile smart terminal MST）使用的密钥加密本地保护的移动智能终端密码模块（CMMST-KELP）技术架构，给出了方案的安全原理和保障措施，描述了技术架构组成、主要工作流程示例，以及对GM/T 0028-2014中规定的11个安全域描述，最后给出应用示例。

本标准是GM/T 0028-2014在移动智能终端中实现密码模块中的具体展开和补充，适用于指导密码模块制造厂家设计、实现移动智能终端密码模块。也可作为移动智能终端使用密码模块的参考。

2 规范性引用文件

下列文件中的条款通过T/EMCG 001-2019《移动智能终端密码模块技术框架》的本部分的引用而成为本部分的条款。

GM/T 0003.3-2012 SM2椭圆曲线公钥密码算法第3部分：密钥交换协议

GM/T 0005- 2012 随机性检测规范

GM/T 0008-2012 安全芯片密码检测准则

GM/T 0019-2012通用密码服务接口规范

GM/T 0028-2014 密码模块安全技术要求

T/ EMCG 001.1-2019《移动智能终端密码模块技术框架 第1部分：总则》

3 术语和定义

3.1

非对称密钥对 asymmetric key pair

一对相关的密钥，其中私有密钥规定私有变换，公开密钥规定公开变换。

3.2

关键安全参数 critical security parameter；CSP

与安全相关的秘密信息，这些信息被泄露或被修改后会危及密码模块的安全性。如，移动应用用户私钥。

[GM/T 0028-2014，定义3.15]

3.3

密码主管 cryptographic administrator

服务端负责密码组件运行的管理者。

3.4

密码主管 PIN cryptographic administrator PIN

密码主管个人身份识别码，用来启动服务端密码组件。

3.5

密钥派生算法 key derivation algorithm；KDA

使用合规的密钥产生方法（如 GM/T 0003.3-2012 中 5.4.3 规范），通过作用于共享秘密和双方都知道的其它参数，产生一个或多个共享密钥的算法。

3.6

主密钥 master key；MK

为对称密钥，通过合规的密钥产生方法产生，用来对敏感安全参数进行加密。

3.7

移动智能终端密码组件 mobile smart terminal cryptographic components；MST-CC

部署在移动智能终端中的密码组件，或独立构成，或与服务端密码组件（SS-CC）一起构成移动智能终端密码模块。

3.8

移动智能终端 PPD mobile smart terminal cryptographic components PPD;MST-PPD

移动智能终端密码组件用户的个人特征数据。

3.9

个人特征数据 personal profile data；PPD

个人知道的因素，如PIN码，手势码，以及个人的生物特征，如指纹、脸部特征等。

3.10

公开安全参数 public security parameter;PSP

与安全相关的公开信息，一旦被修改会威胁到密码模块安全。如，本标准中服务端密码组件公钥。

[GM/T 0028-2014，定义3.73]

3.11

敏感安全参数 sensitive security parameter;SSP

包括关键安全参数和公开安全参数。
[GM/T 0028-2014，定义3.82]

3.12

服务端密码组件 server side cryptographic components；SS-CC

部署在服务端中的密码组件，与移动智能终端密码组件（MST-CC）一起构成移动智能终端密码模块。

3.13

主密钥分量 MK component；MKC

服务端密码组件针对移动智能终端密码组件生成的一定长度的随机数（一个MST-CC对应一个MKC），与移动智能终端PPD一起生成主密钥。

3.14

用户私钥 user private key

在移动应用用户非对称密钥对中，只应由该用户使用的密钥。

3.15

用户公钥 user public key

在移动应用用户非对称密钥对中，能够公开的密钥。

4 符号和缩略语

CC	密码组件（cryptographic components）
CMMST	移动智能终端密码模块（mobile smart terminal cryptographic 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）
KDA	密钥派生算法（key derivation algorithm）
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 cryptographic 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 cryptographic components）
SS-MKC	服务端主密钥分量（server side master key component）

5 概述

5.1 方案原理

基于密钥加密本地保护的移动智能终端密码模块（CMMST of key-encrypted local protection；CMMST-KELP）技术架构，是为移动智能终端（MST）使用软件密码模块而设计的。CMMST-KELP通过移动智能终端密码组件（MST-CC）向移动应用提供核准的密码服务。CMMST-KELP对密码模块关键安全参数（CSP），如用户私钥，使用主密钥（MK）进行加密，存储在MST中，并采取多项安全措施，以实现T/EMCG 001.1-2019《移动智能终端密码模块技术框架 第1部分：总则》的安全目标，满足GM/T 0028-2014中一级或二级密码模块安全要求。

CMMST-KELP使用以安全方式产生的主密钥对CSP进行加密，并保护在MST中。在MST-CC初始化时，移动智能终端密码组件（MST-CC）、服务端密码组件（SS-CC）分别产生移动端个人特征数据（MST-PPD）和服务端主密钥分量（SS-MKC），MST-CC在本地将PPD和MKC进行组合，通过密钥派生算法（KDA）生成MK，用MK对CSP进行加密保护。CMMST-KELP密钥加密保护原理如图1所示

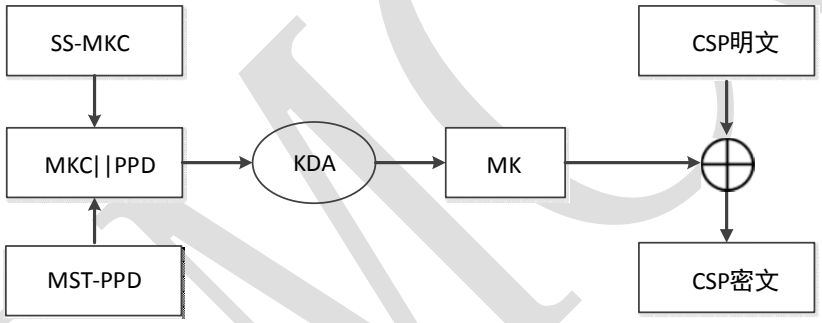

图1 CMMST-KELP密钥加密保护原理

5.2 安全风险

CMMST-KELP方案主要为防范以下风险设计：

（1） 非法产生MK：移动用户MST-PPD和服务端SS-MKC同时泄露可非法产生MK。

（2） MK强度：MST-CC在可修改的运行环境中运行，MK生成易受干扰，影响密钥质量，造成加密强度不够。

（3） 运行环境：MST-CC在可修改的运行环境中运行，MST-CC敏感安全参数可能被非法读取。

（4） 通信：MST-CC与SS-CC通信使用公开信道，传递SS-MKC信息可被窃听、重放攻击，造成SS-MKC泄露。

5.3 安全措施

CMMST-KELP采取以下安全措施防范密码模块面临的安全风险，满足GM/T 0028-2014标准中一级或二级密码模块要求。

（1）移动端和服务端联合保证主密钥安全。

移动端 MST-CC 完成 PPD 输入，MK 生成，敏感安全参数加密存储，与 SS-CC 安全通信等；

服务端 SS-CC 完成 SS-MKC 产生，MST-PPD 验证等。

（2）MST-CC 和 SS-CC 软件代码保护。

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

（3）运行边界保护。

MST-CC 运行在操作系统独立的进程空间，移动应用通过操作系统进程间通信机制与 MST-CC 信息交换。

（4）通信保护。采用预置 SS-CC 公钥方式建立 MST-CC 和 SS-CC 安全通道。

6 技术架构

CMMST-KELP由移动端密码组件MST-CC和服务端密码组件SS-CC组成，移动应用调用MST-CC SDK接口完成核准的密码服务。MST-CC内置SS-CC的公钥，用此公钥建立MST-CC与SS-CC加密信道、MST-CC初始化、MST-PPD验证、数据加载等功能。

SS-CC完成MST-PPD验证，密码主管PIN码输出等功能。SS-CC密码主管通过下发管理控制指令给MST-CC完成相应的管理功能。

CMMST-KELP技术架构如图2所示：

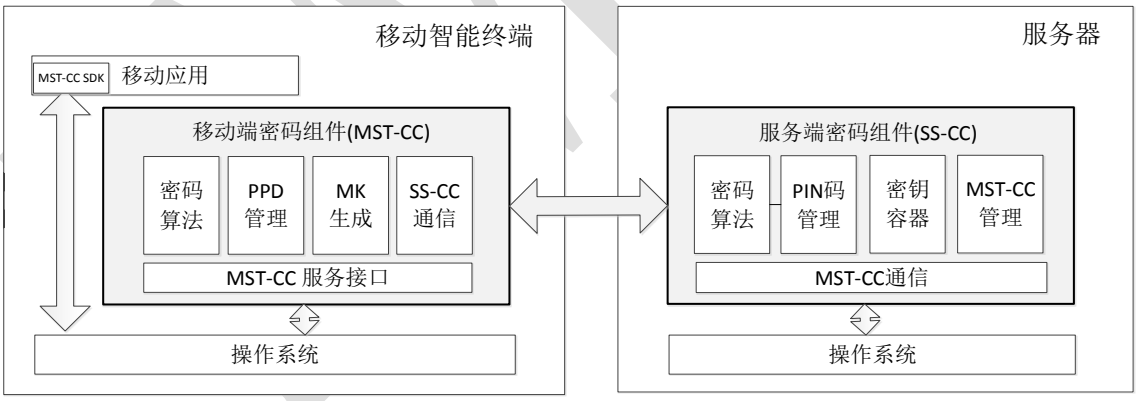

图2 CMMST-KELP技术架构

MST-CC至少包括完成以下功能的模块：

（1）密码算法。实现核准的密码算法，如 SM2,SM3,SM4.

（2）PPD 管理。负责 MST-PPD 输入及验证。

（3）MK 生成。负责将 MST-PPD（如 PIN 码），通过符合国家相关要求的密钥生成机制（如《GMT 0003.4-2012 SM2 椭圆曲线公钥密码算法 》5.4.3）生成 MK。

（4）SS-CC 通信。负责与 SS-CC 建立安全通信连接，其中预置 SS-CC 公钥。

（5）MST-CC 服务接口。MST-CC 与移动应用接口，包括数据接口、控制接口及状态输出接口。

SS-CC 至少包括完成以下功能的模块：

（1）密码算法。实现核准的密码算法，如 SM2,SM3,SM4。

（2）PIN 码管理。负责密码主管 PIN 码验证，启动 SS-CC。

（3）密钥容器。存储管理敏感安全参数的文件。SS-CC 中的敏感安全参数均加密存储在密钥容器中。密钥容器只有在密码主管 PIN 码验证通过后方可使用。

（4）MST-CC 管理。完成 MST-PPD 验证和 SS-MKC 生成。

（5）MST-CC 通信。提供与 MST-CC 的通信连接接口。

CMMST-KELP 通过 MST-CC SDK 提供给移动应用调用 MST-CC 的软件接口。MST-CC 运行在操作系统独立的进程空间，移动应用通过操作系统进程间通信机制与 MST-CC 信息交换。

7 主要工作流程

本节只给出 MST-CC 初始化及 MST-PPD 验证流程，其他密码服务（如数据加解密、数据签名等）流程与一般密码模块相同。下面流程所描述的交换数据仅为确保流程安全而定义的必要数据，密码模块制造厂家可根据需要进行添加。

符号说明：

KDF()——密钥派生算法

A_ENC(KEY，DATA)——使用公钥加密数据 DATA

A_DEC(KEY，ENC_DATA)——使用私钥解密数据 DATA

Hash（DATA）——计算 DATA 杂凑值

S_ENC(KEY，DATA)——用对称密钥 KEY 加密 DATA

S_DEC(KEY，ENC_DATA)——用对称密钥 KEY 解密 DATA

||——表示“合并”

7.1 MST-CC初始化流程

MST-CC首次运行时须对MST-CC进行初始化。

MST-CC 软件发布时内置 SS-CC 公钥 P_S，用户已输入 PPD；SS-CC 已启动，已由密码主管 PIN 码生成生成 SS-CC 存储密钥 K_S

MST-CC初始化过程基本步骤：

1）MST-CC 自检；

2）MST-CC 向 SS-CC 请求初始化；

3）SS-CC 取得随机数 R 送 MST-CC；

4）MST-CC 生成 MST-CC 公私钥对（P_M、d_M），计算 PPD 杂凑值 H_{PPD}；

5）MST-CC 使用 P_S 加密$(R||H_{PPD}||P_M)$得到 C_M；

6）MST-CC 将数据 C_M发送给 SS-CC；

7）SS-CC 接收此数据，使用自身私钥 d_S解密 C_M，得到$(R||H_{PPD}||P_M)$。

8) SS-CC 生成用户 ID、SS-MKC，将(H$_{PPD}$||SS-MKC||P$_M$||PPD 尝试次数)使用 K$_S$加密，以用户 ID 为索引存储在密钥容器中；

9) SS-CC 使用 P$_M$加密(R||SS-MKC||用户 ID)得到 C$_S$；

10) SS-CC 将 C$_S$发送给 MST-CC；

11) MST-CC 使用私钥 d$_M$解密 C$_S$，得到(R||SS-MKC||用户 ID)；

12) MST-CC 保存用户 ID 作为 MST-CC 的标识；

13) MST-CC 以(PPD||SS-MKC)为参数，使用 KDF()计算得到 MK；

14) MST-CC 使用 MK 加密 CSP（如 d$_M$），保存在密钥容器中；

15) 初始化完成。

MST-CC 初始化流程图见图 3。

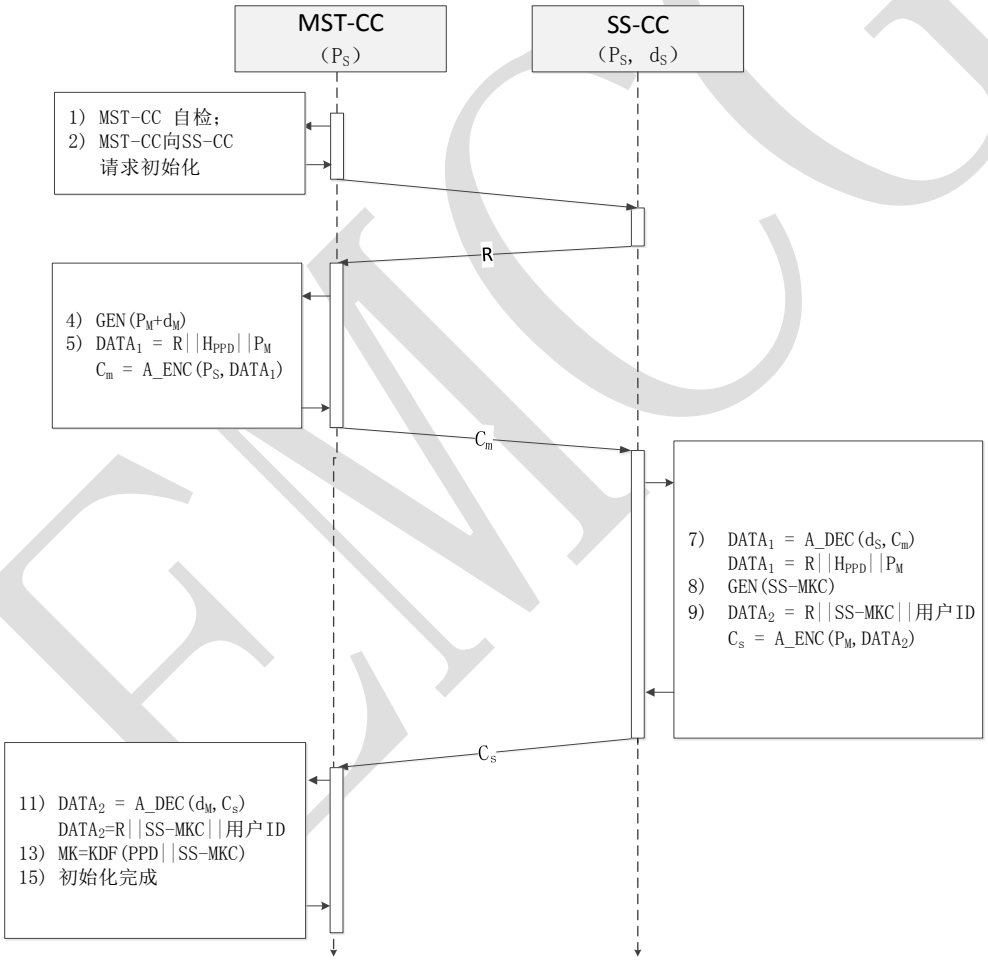

图3 MST-CC初始化流程图

7.2 MST-PPD验证流程

在得到SS-MKC前，MST-CC无法打开密钥容器中用户私钥，MST-CC不能提供密码服务，必须在接收移动应用用户输入MST-PPD，并验证其正确性后，解密密钥容器中用户私钥，MST-CC才能提供密码服务。

在MST-PPD验证前，MST-CC拥有：

P_S——SS-CC公钥

用户ID——移动应用用户标识

H_{PPD}' ——待验证MST-PPD杂凑值

MST-PPD 验证流程如图4所示：

1) MST-CC 向 SS-CC 请求 MST-PPD 验证；

2) SS-CC 发送随机数 R 给 MST-CC；

3) MST-CC 使用 P_S 加密(R||用户 ID|| H_{PPD}' || r_M)得到 C_M，其中 r_M 为随机数；

4) MST-CC 将数据 C_M 发送给 SS-CC；

5) SS-CC 使用自身私钥 d_S 解密 C_M，得到(R||用户 ID|| H_{PPD}' ||r_M)；

6) SS-CC 根据用户 ID 从密钥容器中得到 MST-CC 的对应数据(H_{PPD}||SS-MKC||P_M||PPD 尝试次数)，并用 K_S 解密，验证 H_{PPD}' 与 H_{PPD} 一致性、PPD 尝试次数，以上条件有一不满足，则置 MKC 为零（标识 MST-PPD 验证失败），修改 PPD 尝试次数；

7) SS-CC 使用 r_M 加密(R||SS-MKC||PPD 尝试次数)得到 C_S,并将 C_S 发送给 MST-CC；

8) MST-CC 使用 r_M 解密 C_S 得到(R||SS-MKC||PPD 尝试次数)；如果 SS-MKC 为零，则返回 PPD 验证失败结果，并附带 PPD 尝试次数；否则继续；

9) MST-CC 以(PPD||SS-MKC)为参数，使用 KDF()计算得到 MK，使用 MK 解密密钥容器中的敏感安全参数（如 d_M）；

10) MST-PPD 验证结束。

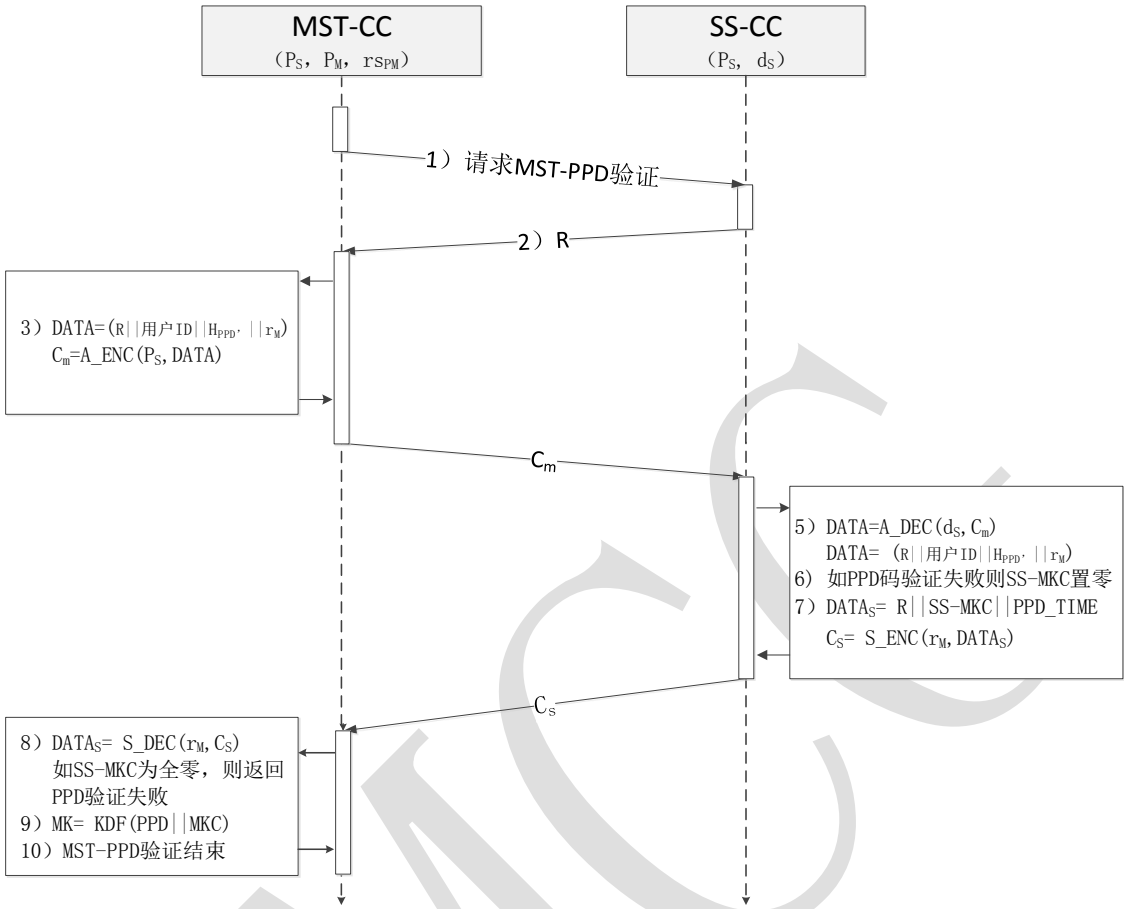

图 4 MST-PPD 验证流程

8 密码模块规格

CMMST-KELP在其密码边界内使用核准的密码算法SM2,SM3,SM4实现模块声明的功能,包括数据摘要计算，对称密钥加解密，非对称密钥加解密，签名/验签等。

8.1 密码模块类型

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。

8.2 密码边界

CMMST-KELP边界为MST-CC、SS-CC的可执行文件和文件集。如图2所示。

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。

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。

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。

MST-CC SDK不在密码安全边界内，如，为可集成到移动应用的动态链接库中。

8.3工作模式

CMMST-KELP的正常工作状态按GM/T 0028-2014 7.2.4.2要求实施。

9 密码模块接口

9.1 物理和逻辑接口

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。

9.2 接口类型

CMMST-KELP接口类型为软件或固件模块接口(SFMI)类型。

9.3 接口定义

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

9.4 可信信道

对于CMMST-KELP此项无要求。

10 角色、服务和鉴别

10.1 角色

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。

10.2 服务

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。

10.2.1 旁路能力

CMMST-KELP不提供旁路能力或功能。

10.2.2 自启动密码服务能力

CMMST-KELP不提供自启动密码服务能力或功能。

10.2.3 软件/固件加载

CMMST-KELP不提供加载外部软件/固件功能。

10.3 鉴别

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；
SS-CC验证密码主管输入PIN码，方可执行操作；

11 软件/固件安全

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。

12 运行环境

CMMST-KELP运行在可修改的运行环境中。

12.1 可修改运行环境的操作系统要求

采取以下措施满足GM/T 0028-2014 7.6.3安全一、二级模块要求：

（1） MST-CC、SS-CC 运行在独立的进程空间中，移动应用通过操作系统进程间通信机制与MST-CC 信息交换。

（2） MST-CC 须运行在合法的操作系统中，如未 root 操作系统。

（3） 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。

13 密码模块物理安全

CMMST-KELP无物理安全要求。

14 非入侵式安全

CMMST-KELP对此无要求。

15 敏感安全参数管理

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。

（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加密存储在密码容器文件中；

——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。

（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加密存放在密码容器中；

——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。

（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。

（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。

15.1 随机比特生成器

CMMST-KELP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。

15.2 敏感安全参数的生成

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

（1） CMMST-KELP 所有敏感安全参数均在 MST-CC 和 SS-CC 内产生。

（2） 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。

（3） P_M、d_M、P_S、d_S生成满足 GM/T 0003.3-2012 中相关要求。

（4） MK 使用 KDA 衍生，KDA 满足 GM/T 0003.3-2012 中 5.4.3 相关要求。

（5） K_S由密码主管 PIN 衍生，且符合核准的密钥生成要求。

（6） PPD 由 MST-CC 用户人工产生。

（7） SS-MKC 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。

（8） 密码主管员 PIN 由密码主管员人工产生。

15.3 敏感安全参数的建立

CMMST-KELP敏感安全参数遵照GM/T 0028—2014 7.9.4要求建立。

15.4 敏感安全参数的输入输出

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

（1） 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。

（2） 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。

（3） 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。

（4） 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。

15.5 敏感安全参数存储

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

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

（2） 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。

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

15.6 敏感安全参数置零

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。

16 自测试

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。

17 生命周期保障

17.1 配置管理

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

17.2 设计

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

17.3 有限状态模型（FSM）

CMMST-KELP的状态是指MST-CC和SS-CC共同处于的状态，其有限状态模型如图5所示：

——出厂状态。密码模块集成（安装）后尚未使用所处的状态。

——初始化状态。密码模块初始运行后进入“初始化状态”。

——自测试状态。密码模块正在执行自测试时所处的状态。

——密码主管状态。SS-CC 密码主管进行模块管理、密钥管理（如更换 SS-CC 公私钥对）时处于的状态，此状态下 MST-CC 不能进行密码服务。

——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。

——锁定状态。关键安全参数输入错误进入此状态，此状态仅可有密码主管干预解锁，回到关键安全参数输入状态。

——用户状态。移动应用使用密码模块进行核准的密码服务时所处的状态。

——核准的状态。密码模块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。

——错误状态。当密码模块遇到错误状况时转到此状态。

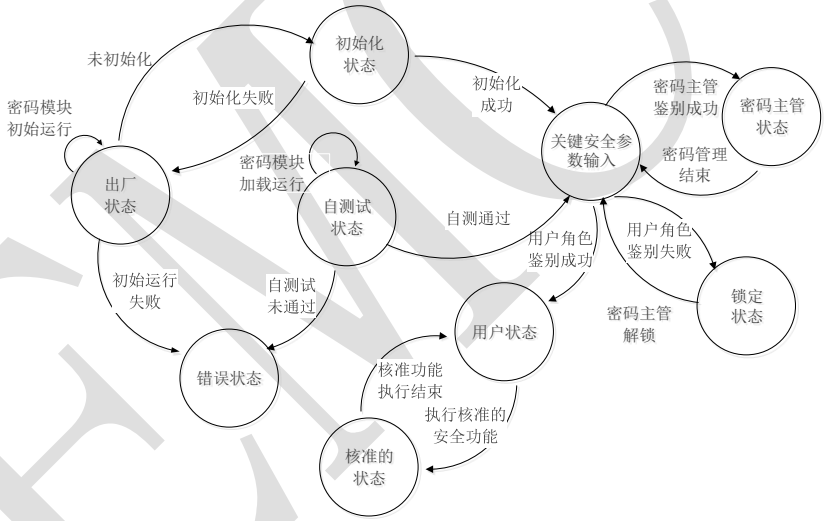

图5 CMMST-KELP有限状态图

17.4 开发

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

17.5 厂商测试

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

17.6 配送与操作

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。

17.7 生命终止

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。

17.8 指南文档

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

18 对其他攻击的缓解

CMMST-KELP对此无要求。

附　录A

（资料性附录）

应用示例

移动应用可按下列方法完成对CMMST-KELP密码模块集成。

（1）CMMST-KELP 开发者将 CMMST-KELP 系统提供给用户（CMMST-KELP 系统所有权属于该用户）。

（2）CMMST-KELP 用户首次运行 SS-CC，SS-CC 生成自己的公私钥对，及主密钥，并用主密钥加密存储自己的私钥。

（3）将 SS-CC 的公钥部署在 MST-CC SDK 中。

（4）MST-CC SDK 由 CMMST-KELP 移动应用开发者使用。

（5）移动应用开发者将 CMMST-KELP 集成到进移动应用中，为移动应用提供密码服务，如信息加解密、数据签名与验证等。

（6）集成 MST-CC 的移动应用安装到移动终端后第一次运行时，移动应用的用户输入 MST-PPD 进行初始化注册。

（7）注册完成后，SS-CC 将 SS-MKC 等信息发送到 MST-CC。

（8）MST-CC 根据下发的数据将本地 MST-PPD 及 SS-MKC 组合生成存储加密主密钥 MK，用 MK 加密存储移动应用密码模块敏感安全参数。MST-CC 初始化流程见本标准 7.1 节。

（9）当再次启动时，不需执行初始化操作，仅使用 MST-PPD 激活 MST-CC 即可调用 MST-CC 密码功能。