ICS 35.240
L70/84

团　　体　　标　　准

T/ZSA 67.2-2019

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

2019-12-31 发布　　2020-03-01 实施

中关村标准化协会　发布

目 次

前　言

T/ZSA 67-2019《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/ZSA 67-2019《移动智能终端密码模块技术框架》的第2部分。

本部分按照GB/T 1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。中关村标准化协会不承担识别这些专利的责任。

本部分由中关村标准化协会技术委员会提出并归口。

本部分主要起草单位：中关村网络安全与信息化产业联盟、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/ZSA 67-2019《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/ZSA 67-2019《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/ZSA 67-2019《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

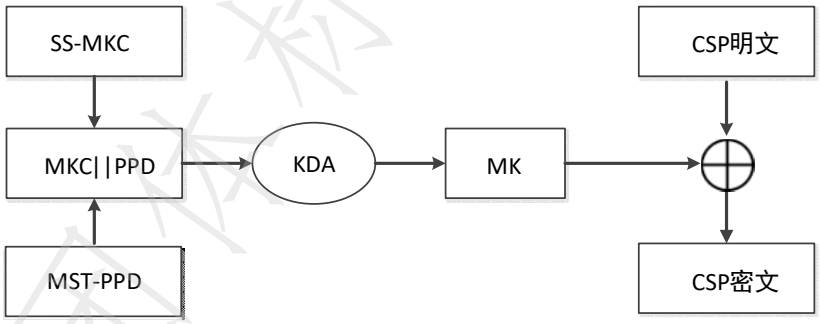

图1 CMMST-KELP密钥加密保护原理

5.2 安全风险

CMMST-KELP方案主要为防范以下风险设计：

a) 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。

b) 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。

c) 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。

d) 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。

a)移动端和服务端联合保证主密钥安全。

b)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；

c)服务端 SS-CC 完成 SS-MKC 产生，MST-PPD 验证等。

d)MST-CC 和 SS-CC 软件代码保护。

e)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。

f)运行边界保护。

g)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。

h)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：

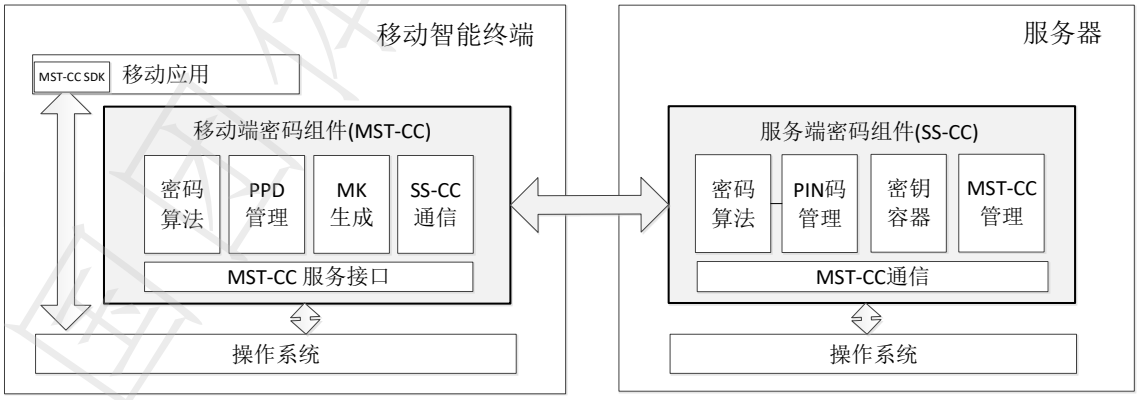

图2 CMMST-KELP技术架构

MST-CC至少包括完成以下功能的模块：

a） 密码算法。实现核准的密码算法，如 SM2,SM3,SM4.

b） PPD 管理。负责 MST-PPD 输入及验证。

c） 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。

d) 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。

e) 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。

f) SS-CC 至少包括完成以下功能的模块：

g) 密码算法。实现核准的密码算法，如 SM2,SM3,SM4。

h) PIN 码管理。负责密码主管 PIN 码验证，启动 SS-CC。

i) 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。

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

k) MST-CC 通信。提供与 MST-CC 的通信连接接口。

l) 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 工作流程

7.1 概述

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”

7.2 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：

a) MST-CC 自检；

b) MST-CC 向 SS-CC 请求初始化；

c) SS-CC 取得随机数 R 送 MST-CC；

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

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

f) MST-CC 将数据 C_M发送给 SS-CC；

g) 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)。

h) 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；

i) SS-CC 使用 P_M加密(R||SS-MKC||用户 ID)得到 C_S；

j) SS-CC 将 C_S发送给 MST-CC；

k) MST-CC 使用私钥 d_M解密 C_S，得到(R||SS-MKC||用户 ID)；

l) MST-CC 保存用户 ID 作为 MST-CC 的标识；

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

n) MST-CC 使用 MK 加密 CSP（如 d_M），保存在密钥容器中；

o) 初始化完成。

MST-CC 初始化流程图见图 3。

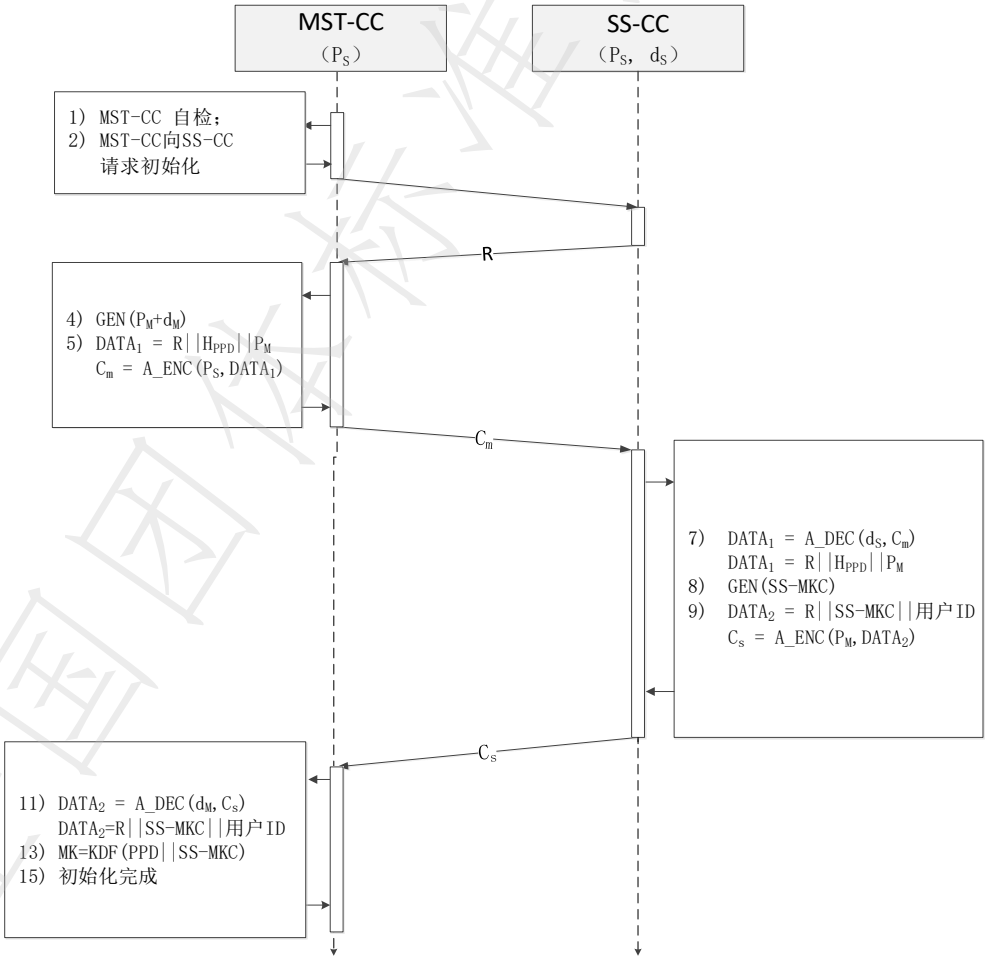

图3 MST-CC初始化流程图

7.3 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：

a） MST-CC 向 SS-CC 请求 MST-PPD 验证；

b） SS-CC 发送随机数 R 给 MST-CC；

c） 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；

d） MST-CC 将数据 C_M 发送给 SS-CC；

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

f） 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；

g） 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；

h） 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；

i） 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）；

j） MST-PPD 验证结束。

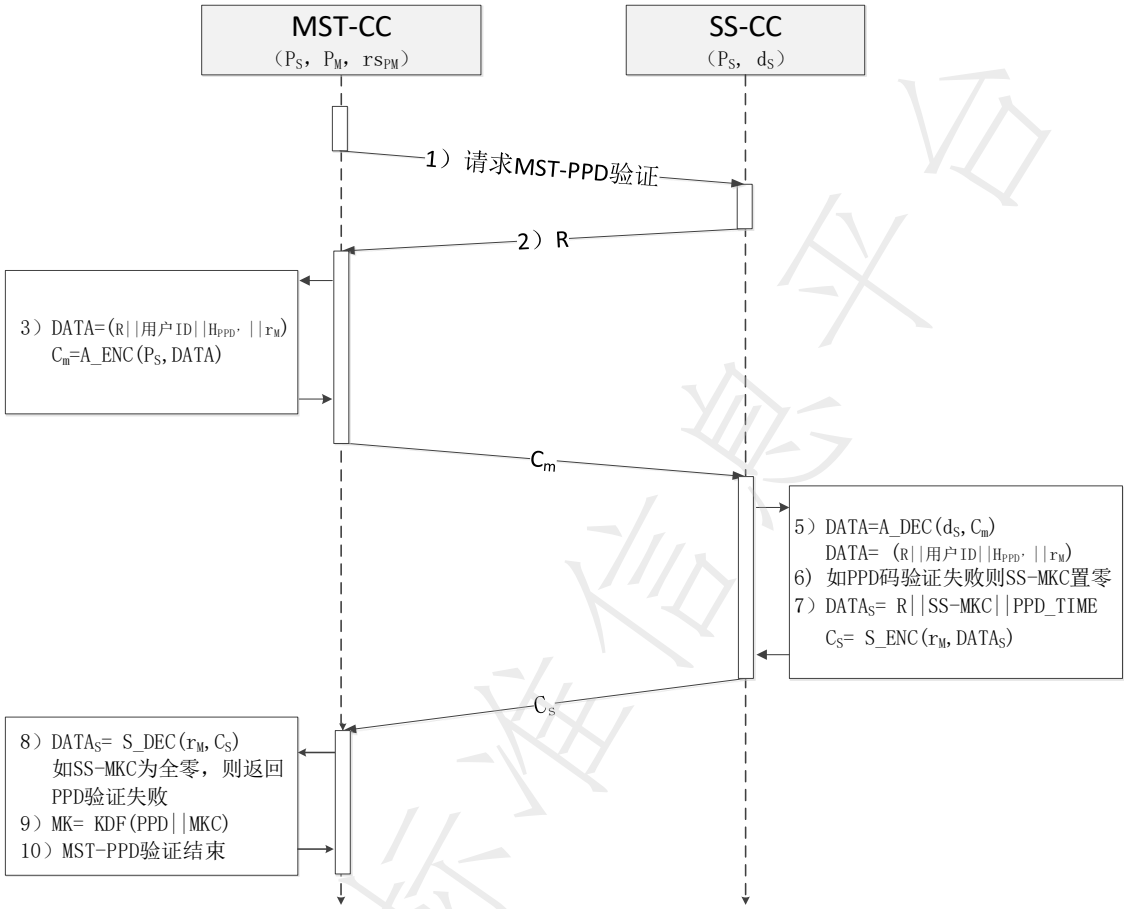

图 4 MST-PPD 验证流程

8 密码模块规格

8.1 概述

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。

8.2 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。

8.3 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。

8.4 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：

a) 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。

b) 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，可修改运行环境的操作系统采取以下措施满足GM/T 0028-2014 7.6.3安全一、二级模块要求：

a) 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。

b) MST-CC 须运行在合法的操作系统中，如未 root 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。

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

15.1 概述

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。

a） 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。

b） 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。

c） 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。

d） 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。

15.2 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。

15.3 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。

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

b) rM、rMS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。

c) PM、dM、PS、dS生成满足GM/T 0003.3-2012中相关要求。

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

e) KS由密码主管PIN衍生，且符合核准的密钥生成要求。

f) PPD由MST-CC用户人工产生。

g) 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。

h) 密码主管员PIN由密码主管员人工产生。

15.4 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。

15.5 敏感安全参数的输入输出

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

b) 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。

c) 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。

d) 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。

e) 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。

15.6 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。

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

b) 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。

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

15.7 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。

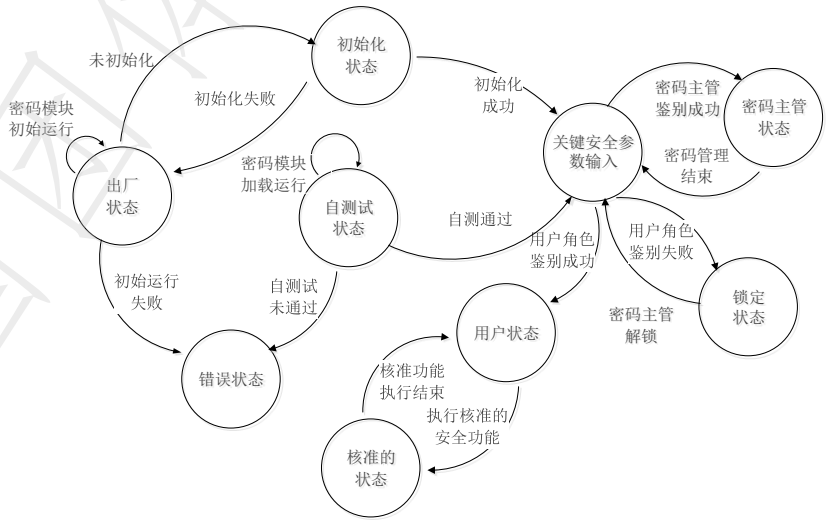

图5 CMMST-KELP有限状态图

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：

a） CMMST-KELP 安装、初始化和启动流程见 6.1.3.1 MST-CC 初始化流程。

b） 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。

a） 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）。

b） 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。

c） 将 SS-CC 的公钥部署在 MST-CC SDK 中。

d） MST-CC SDK 由 CMMST-KELP 移动应用开发者使用。

e） 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。

f） 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。

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

h） 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。

i） 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。

ICS 35.240
L70/84

Assosication Standard

T/ZSA 67.2-2019

Technical framework of cryptographic module for mobile smart terminal

Part 2：Key-encrypted local protection

Issue Date 12-31-2019 Inplemenation Date 03-01-2020

Issued by Zhongguancun Standardization Association

Contents

FOREWORD

T /ZSA 67-2019 "Technical framework of cryptographic module in mobile smart terminal" is divided into 5 parts:

Part 1: General

Part 2: Key-encryption local protection

Part 3: Key-encrypted protection on server side

Part 4: Key protection based on multi-party computation

Part 5: Based on security chip

This section is second part of T /ZSA 67-2019 "Technical framework of cryptographic module in mobile smart terminal".

The section was drafted in accordance with the rules set out in GB/T 1.1-2009.

Please note that some contents in this document may involve patents. Zhongguancun Standardization Association shall not be held responsible for identifying such patents.

The section was proposed and under the jurisdiction of Zhongguancun Standardization Association - Technical Committee.

The main drafting companies of this section: Zhongguancun Cyberspace Affairs Industry Alliance, Qi'anxin Technology Group Co., Ltd., Institute of Information Engineering, Chinese Academy of Sciences, Beijing Jiangnan Tianan Technology Co., Ltd., PayEgis, Beijing Woqi Data Co., Ltd., Westone Information Industry Co., Ltd., Dingqiao Communication Technology Co., Ltd., etc.

The main drafters of this section: Zhang Fan, Wang Ke, Fu Wenbin, Liu Zongbin, Li Bo, Zhang Jing, Li Xiangrong, Lu Hongcheng, Zhang Lingchen, etc.

INTRODUCTION

In the environment of open mobile networks and portable mobile terminal systems, how to protect sensitive security parameters has become a core issue in the design and implementation of cryptographic software modules for mobile intelligent terminals. Encrypting and storing sensitive security parameters in mobile smart terminals is the main method to solve the security of software cryptographic modules. However, if the encryption key is easily obtained illegally or the quality of the key does not meet the requirements, it poses a threat to the security of sensitive security parameters. Therefore, this standard controls the secure generation and use of master keys to ensure the security of encryption keys with sensitive security parameters.

Technical framework of cryptographic module in mobile smart terminal

Part 2：Key-encrypted local protection

1 SCOPE

This section of T / ZSA 67-2019 "Mobile Smart Terminal Cryptographic Module Technical Framework" specifies the technical architecture of the mobile smart terminal crypto module (CMMST-KELP), which is encrypted by the key used by mobile smart terminal MST. The security principles and safeguards of the solution are given, the technical architecture components, examples of main workflows, and descriptions of the 11 security domains specified in GM / T 0028-2014 are given. Finally, application examples are given.

This standard is a specific expansion and supplement of GM / T 0028-2014 in the implementation of cryptographic modules in mobile smart terminals, and is applicable to guide the design of cryptographic module manufacturers and implementation of cryptographic modules for mobile smart terminals. It can also be used as a reference for using a password module in a mobile smart terminal.

2 NOMATIVE REFERENCES

The clauses in the following documents have become the clauses of this section after being referenced in this section of T / ZSA 67-2019 "Mobile Intelligent Terminal Cryptographic Module Technical Framework".

GM / T 0003.3-2012 SM2 elliptic curve public key cryptographic algorithm Part 3: Key exchange protocol

GM / T 0005- 2012 Randomness Test Specification

GM / T 0008-2012 Security chip password detection guidelines

GM / T 0019-2012 General Cryptographic Service Interface Specification

GM / T 0028-2014 Password module security technical requirements

T /ZSA67.1-2019 "Technical Framework of Mobile Smart Terminal Cryptographic Module Part 1: General Provisions"

3 TERMS AND DEFINITIONS

3.1 Asymmetric Key Pair

A pair of related keys, where the private key specifies the private transformation and the public key specifies the public transformation.

3.2 Critical Security Parameter；CSP

Security-related secret information, which is compromised or compromised if the information is leaked or modified. For example, mobile application user private key.

[GM/T 0028-2014，definition 3.15]

3.3 Cryptographic Supervisor

The server is the manager responsible for the operation of the cryptographic component.

3.4 PIN Cryptographic Supervisor PIN

The password supervisor's personal identification number is used to start the server-side password component.

3.5 Key Derivation Algorithm；KDA

Use a compliant key generation method (such as 5.4.3 in GM / T 0003.3-2012) to generate one or more shared key algorithms by acting on shared secrets and other parameters known to both parties.

3.6 Master Key；MK

It is a symmetric key, which is generated by a compliant key generation method, and is used to encrypt sensitive security parameters.

3.7 Mobile Smart Terminal Cryptographic Components；MST-CC

The cryptographic component deployed in the mobile smart terminal is either formed independently or together with the server-side cryptographic component (SS-CC) to form the mobile smart terminal password module.

3.8 PPD Mobile Smart Terminal Cryptographic Components PPD;MST-PPD

Personal characteristic data of the user of the mobile smart terminal password component.

3.9 Personal Profile Data；PPD

Personally known factors, such as PIN code, gesture code, and personal biometrics, such as fingerprints and facial features.

3.10 Public Security Parameter;PSP

Public information related to security, once modified, threatens the security of the cryptographic module. For example, the public key of the server-side cryptographic component in this standard.

[GM/T 0028-2014，definition 3.73]

3.11 Sensitive Security Parameter;SSP

Includes critical safety parameters and public safety parameters.

[GM/T 0028-2014，definition 3.82]

3.12 Server Side Cryptographic Components；SS-CC

The password component deployed in the server side, together with the mobile intelligent terminal password component (MST-CC), constitutes the mobile intelligent terminal password module.

3.13 MK Component；MKC

The server-side password component generates a master key with a certain length of random number (one MST-CC corresponds to one MKC) for the mobile intelligent terminal password component.

3.14 User Private Key

In an asymmetric key pair for a mobile application user, a key that should only be used by that user.

3.15 User Public Key

A key that can be made public in an asymmetric key pair for a mobile application user.

4 SYMBOL AND ACRONYMS

CC	Cryptographic Components
CMMST	Mobile Smart Terminal Cryptographic Components
CMMST-KELP	CMMST of Key-Encrypted Local Protection

CSP	Critical Security Parameter
KDA	Key Derivation Algorithm
MK	Master Key
MKC	Master Key Component
MST	Mobile Smart Terminal
MST-CC	Mobile Smart Terminal Cryptographic Components
MST-PPD	Mobile Smart Terminal Personal Profile Data）
PIN	Personal Identification Number）
PPD	Personal Profile Data
PSP	Public Security Paramete
SDK	Software Development Kit
SS	Server Side
SSP	Sensitive Security Parameter
SS-CC	Server Side Cryptographic Components
SS-MKC	Server Side Master Key Component

5 OVERVIEW

5.1 Plan Principles

CMMST of key-encrypted local protection (CMMST-KELP) technology structure is designed for mobile intelligent terminals (MST) using software cryptographic modules. CMMST-KELP provides approved cryptographic services to mobile applications through the mobile smart terminal cryptographic component (MST-CC). CMMST-KELP uses the master key (MK) to encrypt the key security parameters (CSP) of the cryptographic module, such as the user's private key,then stores it in the MST, and adopts a number of security measures to achieve security objectives of T / ZSA 67.1-2019 "Technical framework of cryptographic module in mobile smart terminal Part 1: General Principles ", meeting the security requirements of GM / T 0028-2014 level 1 or level 2 cryptographic modules.

CMMST-KELP uses a master key generated in a secure manner to encrypt the CSP and is protected in the MST. When the MST-CC is initialized, the mobile smart terminal cryptographic component (MST-CC) and the server-side cryptographic component (SS-CC) generate the mobile smart terminal personal property data (MST-PPD) and the server-side master key component (SS-MKC), MST-CC combines PPD and MKC locally, generates MK through key derivation algorithm (KDA), and encrypts CSP with MK. CMMST-KELP key encryption protection principle is shown in Figure 1.

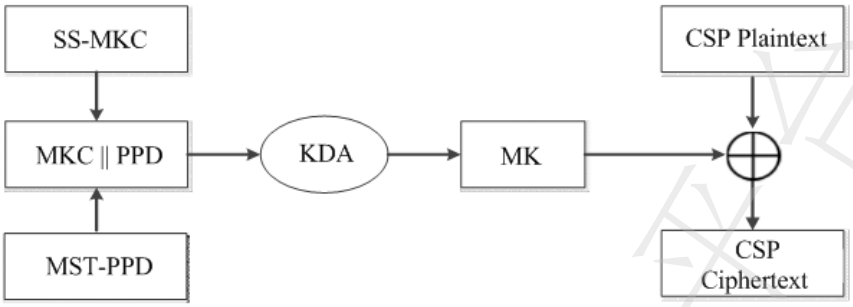

Figure 1 CMMST-KELP Key Encryption Protection Principle

5.2 Security Risks

The CMMST-KELP solution is designed mainly to prevent the following risks:

(1) Illegally generate MK : MK can be generated illegally when MST-PPD and SS-MKC are leaked at the same time.

(2) MK intensity: MST-CC operates in a modifiable operating environment, and MK generation is susceptible to interference, affecting key quality, resulting in insufficient encryption strength.

(3) Operating environment: MST-CC operates in a modifiable operating environment, and MST-CC sensitive security parameters may be read illegally.

(4) Communication: MST-CC communicates with SS-CC through the open channel. SS-MKC information can be intercepted and replayed when being passed, which causes the leak of SS-MKC.

5.3 Security Measures

CMMST-KELP adopts the following security measures to prevent the security risks faced by the cryptographic module and meets the requirements of the level 1 or level 2 cryptographic module in the GM / T 0028-2014 standard.

(1) The mobile terminal and server side jointly guarantee the security of the master key.

Mobile terminal MST-CC completes PPD input, generate MK, cryptographically store sensitive security parameters, and communicate with SS-CC securely;

SS-CC completes the generation of SS-MKC and the verification of MST-PPD, etc.

(2) MST-CC and SS-CC software code protection.

Take mitigation of dynamic and static analysis and attack methods to protect the CMMST-KELP code. Including code, data integrity detection, anti-dynamic debugging, executable code obfuscation, etc.

(3) Operational border protection.

MST-CC runs in an independent process space of the operating system, and mobile applications exchange information with MST-CC through the inter-process communication mechanism of the operating system.

(4) Communication protection. MST-CC and SS-CC secure channels are established by using the preset SS-CC public key method.

6 TECHNICAL STRUCTURE

CMMST-KELP consists of the mobile terminal cryptographic component MST-CC and the server side cryptographic component SS-CC. The mobile application calls the MST-CC SDK interface to complete the approved cryptographic service. MST-CC has a built-in SS-CC public key, and uses this public key to establish MST-CC and SS-CC encrypted channels, MST-CC initialization, MST-PPD verification, and data loading functions.

SS-CC completes MST-PPD verification, cryptographic supervisor PIN output and other functions. The SS-CC cryptographic supervisor issues management control instructions to MST-CC to complete corresponding management functions.

CMMST-KELP technology structure is shown in Figure 2:

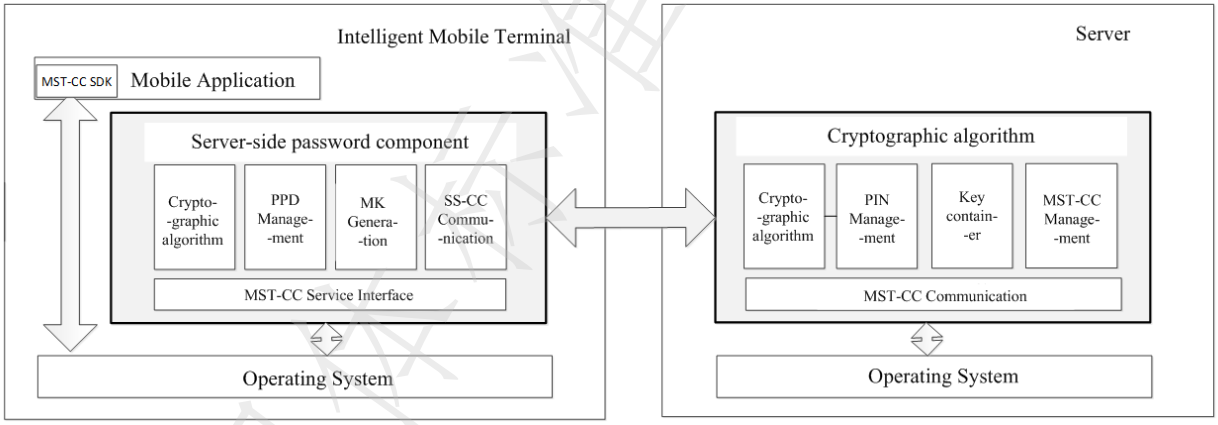

Figure 2 CMMST-KELP technology structure

MST-CC includes modules that at least perform the following functions:

(1) Cryptographic algorithm. Implement approved cryptographic algorithms, such as SM2, SM3, SM4.

(2) PPD management. Responsible for MST-PPD input and verification.

(3) MK generation. Responsible for generating MK from MST-PPD (such as PIN code) through a key generation mechanism (such as "GMT 0003.4-2012 SM2 Elliptic Curve Public Key Cryptography Algorithm" 5.4.3) that complies with relevant national requirements.

(4) SS-CC communication. Responsible for establishing a secure communication connection with the SS-CC, where the SS-CC public key is preset.

(5) MST-CC service interface. MST-CC interfaces with mobile applications, including data interfaces, control interfaces and status output interfaces.

SS-CC includes modules that at least perform the following functions:

(1) Cryptographic algorithm. Implement approved cryptographic algorithms, such as SM2, SM3, SM4.

(2) PIN code management. Responsible for cryptographic supervisor PIN verification and start SS-CC.

(3) Key container. Stores files that manage sensitive security parameters. All sensitive security parameters in SS-CC are encrypted and stored in the key container. The key container can only be used after the cryptographic master PIN verification is passed.

(4) MST-CC management. Complete MST-PPD verification and SS-MKC generation.

(5) MST-CC communication. Provides communication connection interface with MST-CC.

CMMST-KELP provides a software interface for mobile applications to call MST-CC through the MST-CC SDK. MST-CC runs in an independent process space of the operating system, and mobile applications exchange information with MST-CC through the inter-process communication mechanism of the operating system.

7 WORK FLOW

7.1 Overview

This section only provides the MST-CC initialization and MST-PPD verification process. The other cryptographic services (such as data encryption and decryption, data signature, etc.) are the same as general cryptographic modules. The exchange data described in the following process is only necessary data defined to ensure the security of the process, and the manufacturer of the cryptographic module can add it as needed.

Symbol Descriptions:

KDF ()-key derivation algorithm

A_ENC (KEY, DATA)-Use public key to encrypt data DATA

A_DEC (KEY, ENC_DATA)-use the private key to decrypt the data DATA

Hash (DATA)-calculate the hash value of DATA

S_ENC (KEY, DATA)-encrypt data with symmetric key KEY

S_DEC (KEY, ENC_DATA)-Decrypt DATA with symmetric key KEY

||——Means "merge"

7.2 Initialization Process

MST-CC must be initialized when it runs for the first time.

The SS-CC public key Ps is built-in when the MST-CC software is released. The user has entered the PPD. The SS-CC has been started. The SS-CC storage key Ks has been generated by the cryptographic supervisor PIN

Basic steps of MST-CC initialization process:

1) MST-CC self-test;

2) MST-CC requests initialization from SS-CC;

3) SS-CC gets random number R and sends it to MST-CC;

4) MST-CC generates MST-CC public and private key pairs (P_M, d_M), and calculates the PPD hash value HPPD;

5) MST-CC uses P_S to encrypt (R || HPPD || PM) to get C_M;

6) MST-CC sends data C_M to SS-CC;

7) The SS-CC receives this data and uses its own private key d_S to decrypt C_M to get (R || HPPD || PM).

8) SS-CC generates user ID and SS-MKC, (HPPD || SS-MKC || PM || PPD attempts) is encrypted with K_S, and stored in key container with user ID as index;

9) SS-CC gets C_S using PM encryption (R || SS-MKC || user ID);

10) SS-CC sends C_S to MST-CC;

11) MST-CC uses the private key d_M to decrypt the C_S and gets (R || SS-MKC || user ID);

12) MST-CC stores the user ID as the identity of MST-CC;

13) MST-CC takes (PPD || SS-MKC) as a parameter and calculates with KDF () to get MK;

14) MST-CC uses MK to encrypt CSP (such as d_M) and save it in the key container;

15) Complete initialization.

The MST-CC initialization flowchart is shown in Figure 3.

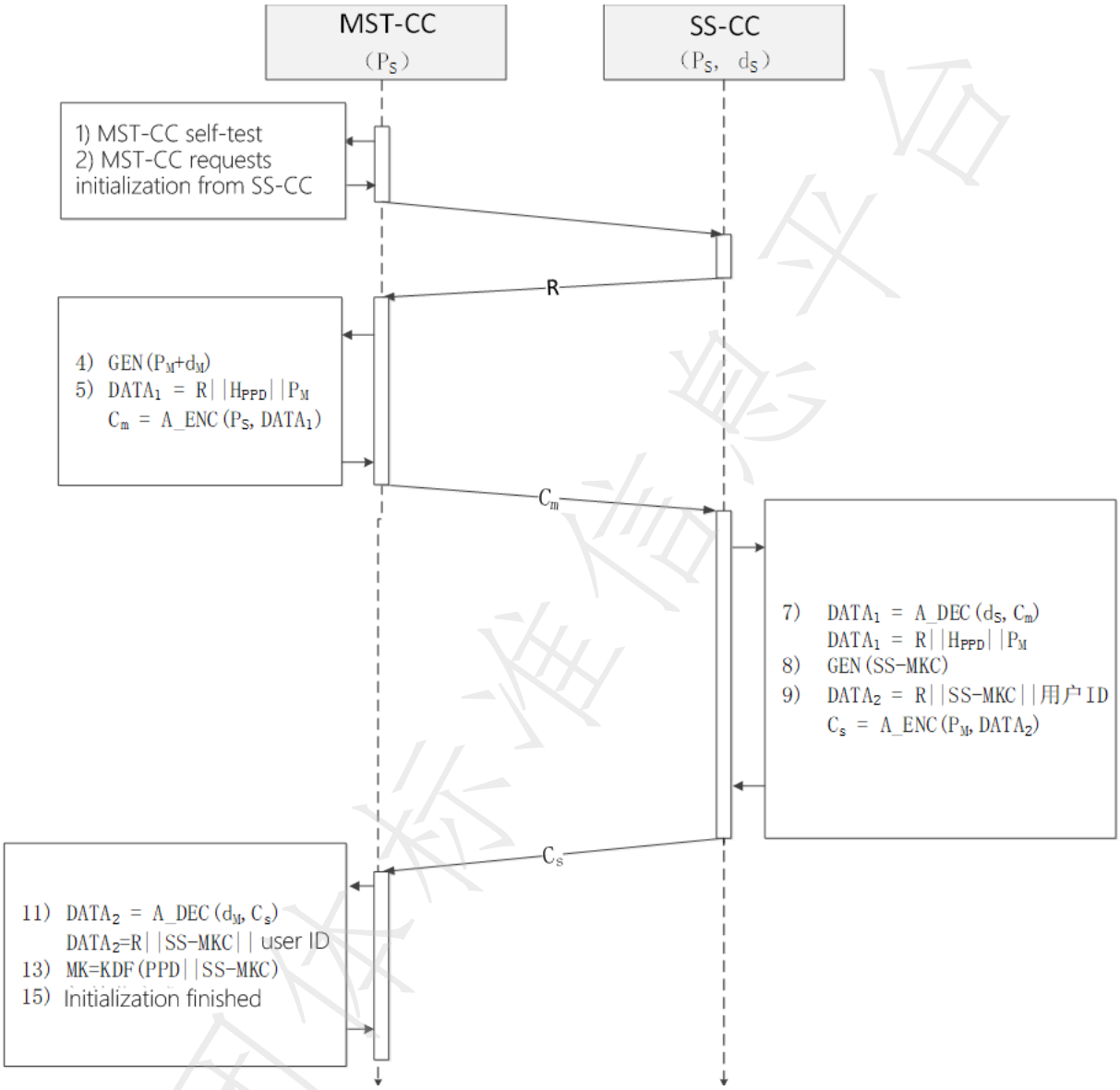

Figure 3 MST-CC Initialization Flowchart

7.3 Verification Process

Before getting the SS-MKC, MST-CC cannot open the user's private key in the key container, MST-CC cannot provide the cryptographic service, and the MST-PPD must be inputted on users receiving the mobile application and then verify its correctness, after which MST-CC can provide the cryptographic service only if the user's private key in the key container is decrypted.

Before verifying MST-PPD, MST-CC has:

P_S——SS-CC public key

User ID-mobile application user identification

H_{PPD}'-hash value of MST-PPD to be verified

The MST-PPD verification process is shown in Figure 4:

1) MST-CC requests MST-PPD verification from SS-CC;

2) SS-CC sends random number R to MST-CC;

3) MST-CC uses P_S to encrypt (R || User ID || HPPD′ || rM) to get CM, where r_M is a random number;

4) MST-CC sends data CM to SS-CC;

5) SS-CC uses its own private key d_S to decrypt the C_M and gets (R || user ID || HPPD′ || rM);

6) SS-CC gets the corresponding data of MST-CC (HPPD || SS-MKC || PM || PPD attempted times) from the key container according to the user ID, and decrypts with K_S to verify the consistency of H_{PPD}′ and H_{PPD}, PPD attempted numbers. If one of the above conditions is not met, make MKC nulled (identifying that MST-PPD verification fails) and modify the PPD attempted numbers.

7) SS-CC uses r_M to encrypt (R || SS-MKC || PPD attempts) to get C_S, and sends C_S to MST-CC;

8) MST-CC uses r_M to decrypt C_S to get (R || SS-MKC || PPD attempts); if SS-MKC is nulled, it returns the PPD verification failure result with the PPD attempted numbers; otherwise the process will still continue;

9) MST-CC takes (PPD || SS-MKC) as a parameter, uses KDF () to calculate and get MK, and uses MK to decrypt sensitive security parameters (such as d_M) in the key container;

10) MST-PPD verification is over.

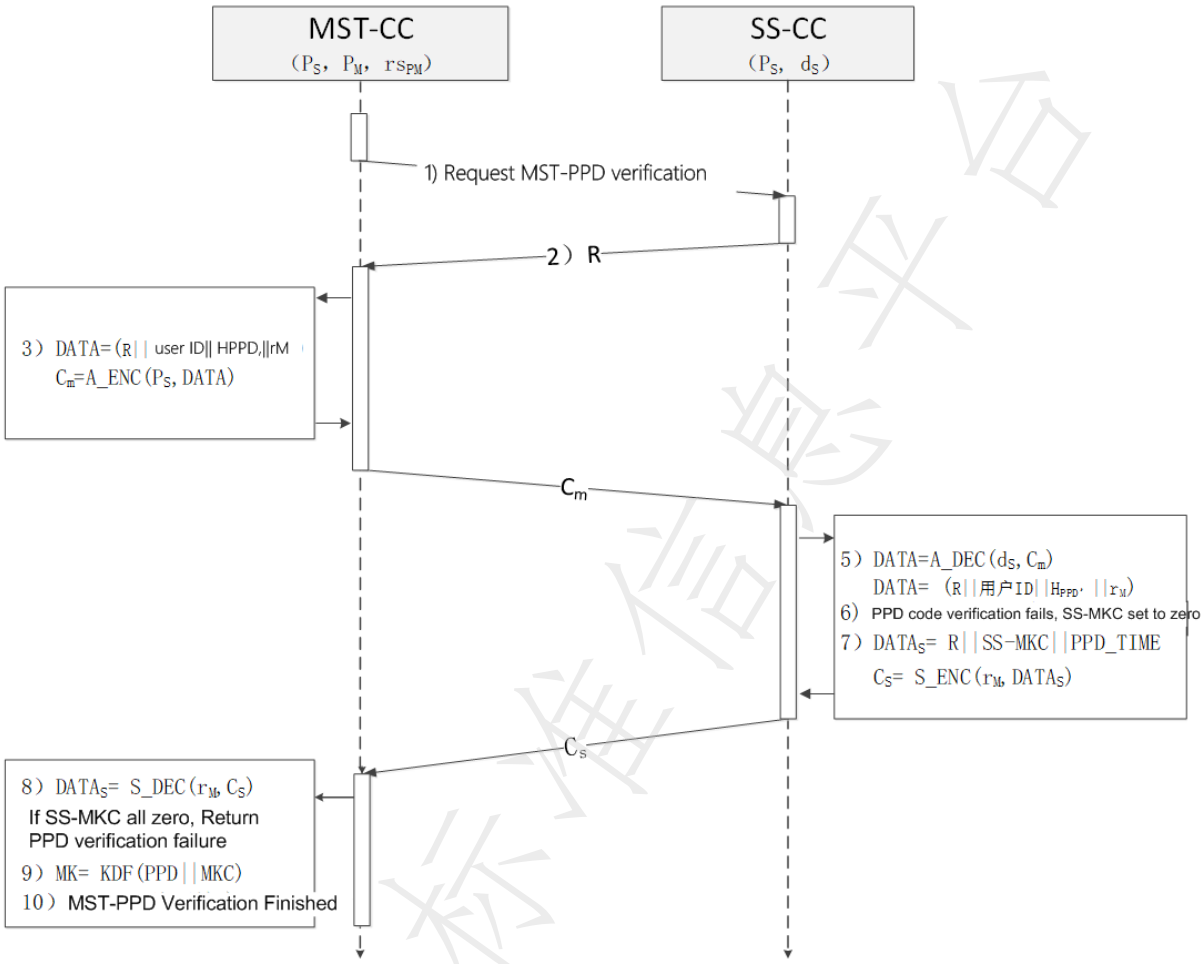

Figure 4 MST-PPD Verification Flowchart

8 CRYPTOGRAPHIC MODULE SPECIFICATIONS

8.1 Overview

CMMST-KELP uses the approved cryptographic algorithms SM2, SM3, and SM4 within its cryptographic boundaries to implement the functions declared by the module, including data digest calculation, symmetric key encryption and decryption, asymmetric key encryption and decryption, and signature / verification,etc.

8.2 Cryptographic Module Types

CMMST-KELP is a software module type and must meet the requirements of GM / T 0028-2014 Section 7.2.2 on software modules.

8.3 Cryptographic Boundary

CMMST-KELP boundary is the executable file and file set of MST-CC, SS-CC. as shown in figure 2.

MST-CC includes modules that complete the following functions: cryptographic algorithms, PPD management, MK generation, SS-CC communication, and MST-CC service interface.

SS-CC includes modules that perform the following functions: cryptographic algorithms, PIN management for cryptographic supervisors, key containers, MST-CC management, and MST-CC communication.

MST-CC and SS-CC run in a separate process space and use the operating system interprocess communication interface to exchange data outside the cryptographic boundary. MST-CC and SS-CC complete data exchange through communication module.

The MST-CC SDK is not within the boundaries of cryptographic security, for example, it is a dynamic link library that can be integrated into mobile applications.

8.4 Work Module

The normal working state of CMMST-KELP is implemented in accordance with GM / T 0028-2014 7.2.4.2.

9 CRYPTOGRAPHIC MODULE INTERFACE

9.1 Physical and Logical Interface

The CMMST-KELP logical interface is distributed on MST-CC and SS-CC, and the two types of logical interfaces are the same.

9.2 Interface Types

The CMMST-KELP interface type is a software or firmware module interface (SFMI) type.

9.3 Interface Definitions

Please refers to GM / T 0019-2012 General Cryptographic Service Interface Specification for the interface definition of CMMST-KELP .

9.4 Trusted Channel

There is no requirement for CMMST-KELP.

10 ROLES,SERVICES AND IDENTIFICATION

10.1 Roles

CMMST-KELP has two roles: mobile application user and cryptographic supervisor.

Mobile application users: MST users, use MST-CC to implement key generation, data signature / signature verification, encryption and decryption, etc.

Crypto Officer: Responsible for operating SS-CC and CMMST-KELP system management.

10.2 Services

CMMST-KELP provides the necessary services in accordance with the requirements of GM / T 0028-2014 7.4.3.1 for the security level 1 and security level 2 software modules. SS-CC must also provide operation services for the role of cryptographic supervisor, including user management and security policy management (such as MST-PPD verification times setting).

10.2.1 Bypass Capability

CMMST-KELP does not provide bypass capability or functionality.

10.2.2 Self-starting Cryptographic Service Capability

CMMST-KELP does not provide self-starting cryptographic service capabilities or functions.

10.2.3 Software / Firmware Loading

CMMST-KELP does not provide the ability to load external software / firmware.

10.3 Identification

In addition to meet the requirements of GM / T 0028-2014 7.4.4 for the security level 1 and security level 2 software modules, the following role-based authentication needs to be supported:

Mobile application users must input the MST-PPD and be authenticated by the SS-CC before calling the MST-CC cryptographic service;

PIN code needs to be entered by SS-CC verified cryptographic supervisor before performing the operation;

11 SOFTWARE / FIREWARE SECURITY

In addition to meet the requirements of GM / T 0028-2014 7.5 for security level 1 and security level 2 software modules, CMMST-KELP software security measures also include but not limited to:

(1) The CMMST-KELP approved integrity algorithm is used to protect MST-CC and SS-CC programs.

(2) Take mitigation of dynamic and static analysis and attack methods to protect the CMMST-KELP code. For example, code and data integrity detection, anti dynamic debugging prevention, executable code obfuscation, etc.

12 OPERATING ENVIRONMENT

CMMST-KELP runs in a modifiable operating environment. The operating system that can modify the operating environment adopts the following measures to meet the requirements of GM / T 0028-2014 7.6.3 security level 1 and level 2 modules:

(1) MST-CC and SS-CC run in independent process space, and mobile applications exchange information with MST-CC through the inter-process communication mechanism of the operating system.

(2) MST-CC must run in a legal operating system, such as a non-root operating system.

(3) SS-CC must run on the host that has taken corresponding protection measures in process design, hardware configuration, etc., and has basic physical security protection.

13 CRYPTOGRAPHIC MODULE PHYSICAL SECURITY

CMMST-KELP has no physical security requirements.

14 NON-INVASIVE SECURITY

CMMST-KELP has no requirements for this.

15 SEVSITIVE SECURITY PARAMETER MANAFEMENT

15.1 Overview

CMMST-KELP sensitive security parameters include:

MST-CC key security parameters:

r_M——the randomly generated symmetric key used for the communication encryption between MST-CC and SS-CC;

d_M——MST-CC user private key;

MST-PPD-Personal property data of MST users;

MK——MST-CC master key;

MST-CC public security parameters:

P_M——MST-CC public key;

P_S——SS-CC public key;

S_S-CC key security parameters:

d_S——SS-CC private key;

r_{MS}——Randomly generated symmetric key used for SS-CC and MST-CC communication encryption;

SS-MKC——MK key component generated by SS-CC, each MST-CC corresponds to one SS-MKC;

K_S——Symmetric key, used for SS-CC encrypted storage of sensitive security parameters, generated by the cryptographic supervisor PIN;

Cryptographic Supervisor PIN-generated manually by cryptographic supervisor, used to generate K_S to start SS-CC work;

SS-CC public security parameters:

PS——SS-CC public key;

PM-MST-CC public key.

In accordance with the requirements of GM / T 0028-2014 7.9 for the security level 1 and security level 2 software modules, CMMST-KELP manages these sensitive security parameters.

(1) MST-CC key security parameter protection prevent unauthorized access, use, disclosure, modification and replacement.

——d_M is encrypted and stored in the cryptographic container file by MK;

——MK is generated by the combination of MST-PPD and SS-MKC;

—— MST-PPD is kept by users;

——r_M is temporarily generated and used in the module but not be saved.

(2) SS-CC key security parameter protection prevent unauthorized access, use, disclosure, modification and replacement.

——The SS-MKC and SS-CC private key d_S are encrypted and stored in the cryptographic container;

——K_S is generated by the cryptographic supervisor PIN and is not permanently saved;

——r_{MS} is temporarily generated and used but not saved.

(3) MST-CC make security parameter protection public to prevent unauthorized modification and replacement.

——P_S is built into the MST-CC code segment, and integrity check is performed on the code segment when the MST-CC starts;

——P_M is saved by mobile application.

(4) SS-CC make security parameter protection public to prevent unauthorized modification and replacement.

——P_S and P_M are protected by SS-CC private key signature.

15.2 Random Bit Generator

CMMST-KELP must meet the requirements of GM / T 0028-2014 7.9.2 for security level 1 and security level 2 software modules.

15.3 Generation of Sensitive Security Parameters

CMMST-KELP sensitive safety parameters are generated in accordance with the requirements of GM / T 0028—2014 7.9.3.

(1) All sensitive safety parameters of CMMST-KELP are generated in MST-CC and SS-CC.

(2) r_M and r_{MS} are generated using approved random bit generators, such as GM / T 0005-2012 randomness detection specifications.

(3) The generation of P_M, d_M, P_S, and d_S meets the relevant requirements in GM / T 0003.3-2012.

(4) MK is derived from KDA. KDA and it meets the relevant requirements of 5.4.3 in GM / T 0003.3-2012.

(5) K_S is derived from the cryptographic supervisor PIN and meets the approved key generation requirements.

(6) PPD is generated manually by MST-CC users.

(7) SS-MKC is generated using an approved random bit generator, such as the GM / T 0005-2012 randomness detection specification.

(8) The cryptographic supervisor PIN is manually generated by the cryptographic supervisor.

15.4 Establishment of Sensitive Safety Parameters

CMMST-KELP sensitive safety parameters are established in accordance with the requirements of GM / T 0028—2014 7.9.4.

15.5 Input and Output of Sensitive Safety Parameters

CMMST-KELP sensitive safety parameters comply with GM / T 0028—2014 7.9.5 requirements for input and output.

(1) The PPD is manually entered into the cryptographic module by the user through the mobile application MST-CC SDK interface.

(2) The cryptographic supervisor PIN is manually entered into the cryptographic module by the cryptographic supervisor through the server software SS-CC SDK interface.

(3) The PIN input of PPD and cryptographic supervisor must meet the requirements of sensitive security parameters directly entered in GM / T 0028-2014 7.9.5.

(4) The transmission of r_M and r_{MS} between MST-CC and SS-CC is encrypted and protected with an approved cryptographic algorithm.

15.6 Storage of Sensitive Safety Parameters

CMMST-KELP sensitive security parameters are stored in accordance with GM / T 0028—2014 7.9.6 requirements.

(1) CSP of MST-CC encrypted storage is bound to PPD. CSP cannot be used without verification.

(2) CSP of SS-CC encrypted storage is all associated with cryptographic supervisor PIN. The CSP cannot be used if the binding verification fails.

(3) The integrity of the PSP in MST-CC and SS-CC is guaranteed by MST-CC code data integrity test.

15.7 Nulling Sensitive Safety Parameters

Complying with the requirements of GM / T 0028—2014 7.9.7, CMMST-KELP has no unprotected sensitive security parameters, and it does not need to be set to null.

16 SELF-TEST

CMMST-KELP must meet the requirements of GM / T 0028-2014 7.10 for security level 1 and security level 2 software modules. The MST-CC self-test must be performed during MST-PPD initialization and MST-CC startup. SS-CC shall perform code data integrity self-test before providing security services.

17 LIFE CYCLE ASSURANCE

17.1 Configuration Management

CMMST-KELP shall meet the requirements of GM / T 0028-2014 7.11.2 for security level 1 and security level 2 software modules.

17.2 Design

CMMST-KELP must meet the requirements of GM / T 0028-2014 7.11.3 for the security level 1 and security level 2 software modules.

17.3 Finite State Model

The state of CMMST-KELP refers to the state where MST-CC and SS-CC are co-located, and its finite state model is shown in Figure 5:

——Factory state. The unused state after the cryptographic module is integrated (installed).

——Initial state. The cryptographic module enters the "initialized state" after initial operation.

——Self-test status. The state the cryptographic module was in when it was performing a self-test.

——Cryptographic supervisor status. The status SS-CC cryptographic supervisor is in when it is in module management and key management (such as replacing the SS-CC public and private key pair). In this state, MST-CC cannot perform password services.

——Crucial security parameter input status. The state when MST-CC receives the user's personal property data (PPD).

——Locked status.If crucial security parameters are inputted by mistake, it will enter this state. This state can only be unlocked by the cryptographic supervisor of to return to the state of crucial security parameter input.

--User status. The state of the mobile app when it uses the cryptographic module for approved cryptographic services.

——Approved status. The state where the cryptographic module is performing the approved cryptographic function. When the cryptographic service is completed, it exits this state and returns to the user state.

——Error status. Go to this state when the cryptographic module is in an error condition.

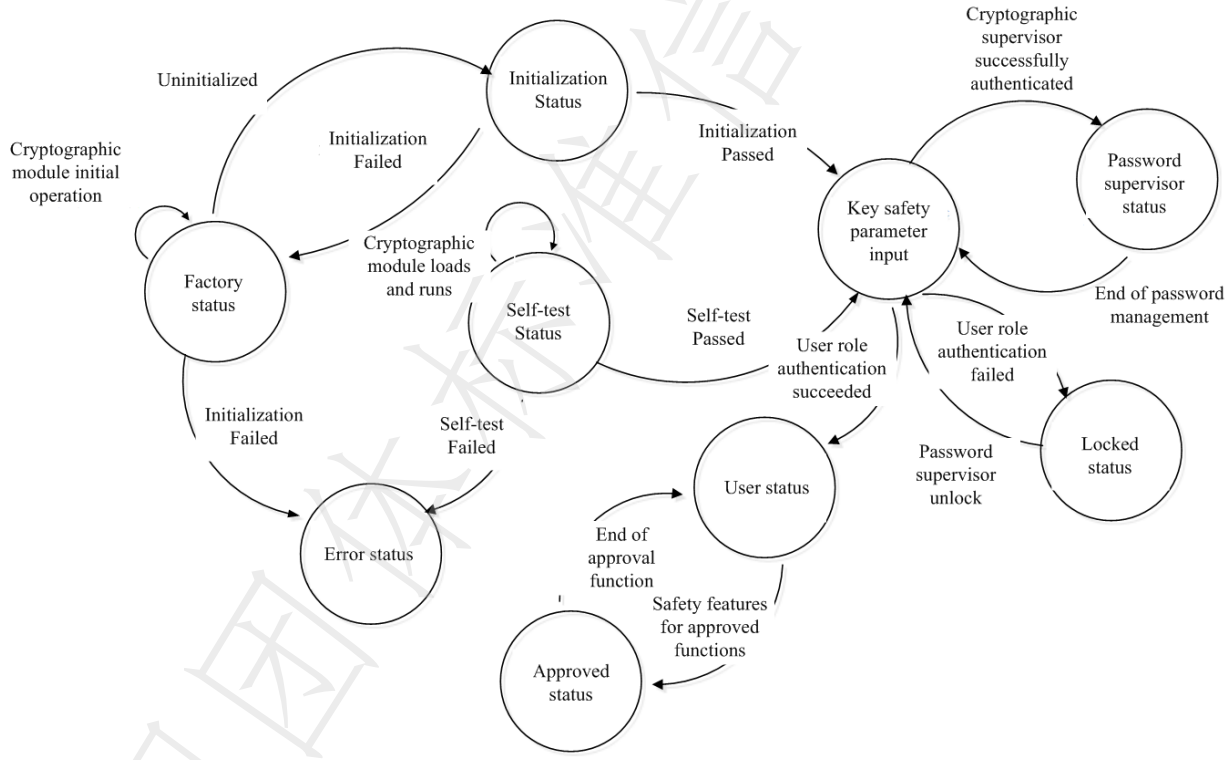

Figure 5 Cmmst-kelp Finite State Diagram

17.4 Development

CMMST-KELP must meet the requirements of GM / T 0028-2014 7.11.5 for security level 1 and security level 2 software modules.

17.5 Manufacturer Test

CMMST-KELP must meet the requirements of GM / T 0028-2014 7.11.5 for security level 1 and security level 2 software modules.

17.6 Distribution and Operation

CMMST-KELP takes the following measures for distribution:

(1) For the process of CMMST-KELP installation, initialization and startup, see 6.1.3.1 MST-CC initialization process.

(2) SS-CC can check the integrity of MST-CC code during MST-CC module initialization to ensure that MST-CC has not been tampered with.

17.7 Life Termination

Sensitive security parameters in encrypted storage in MST-CC can be cleared by the cryptographic supervisor role through instructions issued by SS-CC.

17.8 Guide Document

CMMST-KELP shall meet the requirements of GM / T 0028-2014 7.11.9 for security level 1 and security level 2 software modules.

18 MITIGATION OF OTHER ATTACKS

CMMST-KELP has no requirements for this.

Appendix A

(Informative appendix)

Application example

The mobile application can complete the CMMST-KELP cryptographic module integration as following methods.

(1) The CMMST-KELP developer provides the CMMST-KELP system to the user (the ownership of the CMMST-KELP system belongs to the user).

(2) CMMST-KELP users run SS-CC for the first time. SS-CC generates its own public and private key pair, and master key, and uses the master key to encrypt and store its private key.

(3) Deploy the SS-CC public key in the MST-CC SDK.

(4) The MST-CC SDK is used by CMMST-KELP mobile application developers.

(5) Mobile application developers integrate CMMST-KELP into mobile applications to provide cryptographic services for mobile applications, such as information encryption and decryption, data signing and verification.

(6) When a mobile application integrated with MST-CC is installed for the first time after running on a mobile terminal, the user of the mobile application enters MST-PPD for initial registration.

(7) After registration, SS-CC sends information such as SS-MKC to MST-CC.

(8) The MST-CC combines the local MST-PPD and SS-MKC to generate the storage encryption master key MK based on the issued data, and then cryptographically store the sensitive security parameters of the mobile application cryptographic module with MK. The MST-CC initialization process is described in section 7.1 of this standard.

(9) When restarted, there is no need to perform the initialization operation. Only the MST-PPD is used to activate the MST-CC to call the MST-CC cryptographic function.