ICS 35.240
L70/84

团　　体　　标　　准

T/ ZSA 67.3-2019

移动智能终端密码模块技术框架 第 3 部分：密钥加密服务端保护技术架构

Technical framwork of cryptographic module in mobile smart terminal
Part 3: Key-encrypted protection on server side

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3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、中国科学院信息工程研究所、奇安信科技集团股份有限公司、北京江南天安科技有限公司、江苏通付盾科技有限公司、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：傅文斌、王克、张凡、刘宗斌、张晶、李勃、鲁洪成、李向荣、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，如何安全的设计、实现和使用密码模块，如何保护敏感安全参数成为移动智能终端密码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。为防止加密密钥丢失，或密文密钥数据丢失对敏感安全参数安全构成威胁。本标准采用将移动终端用户个人特征数据与加密密钥绑定，并将密钥加密密文存储在服务端的方法，以保证密码模块敏感安全参数安全。

移动智能终端密码模块技术框架

第3部分：密钥加密云保护技术架构

1 范围

本标准针对采用密钥加密服务端保护技术的移动终端密码模块，规范其技术框架、工作流程，依据GM/T 0028-2014的密码模块规格、密码模块接口、角色、服务和鉴别、软件/固件要求、运行环境要求、密码模块物理安全、非侵入式安全、敏感数据管理、自测试、生命周期保障、对其他攻击的缓解等11个安全域要求，给出具体规范和应用示例。

本标准是GM/T 0028-2014在移动智能终端上实现密码模块的具体展开和补充，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。也可作为使用密码模块用户参考。

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。

GB/T 25069-2010 信息安全技术 术语

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 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

核准的密码算法 approved cryptographic algorithm

GM/T0028-2014附录C给出的密码算法，包括分组密码、流密码、非对称算法、杂凑函数。

3.2

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。

[GB/T 25069-2010，定义2.2.2.33]

3.3

CMMST-KEPOSS-API 接口

MST-CC为移动应用提供的接口，完成密码应用。

3.4

主密钥 master key；MK

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。

3.5

移动应用 mobile application

可在移动智能终端操作系统中进行安装使用运行的应用软件。本标准所述的移动应用是指调用密码模块服务的应用软件。

3.6

移动智能终端 mobile smart terminal；MST

能够接入移动通信网，提供应用软件开发接口，并能够安装和运行应用软件的移动终端。如手机、Pad。

3.7

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

部署在移动智能终端中的密码组件。本规范中 MST-CC 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

个人特征数据 personal profile data；PPD

只有用户个人知道或独具的因素，如PIN码，手势码；用户个人的生物特征，如指纹特征，脸部特征等。

3.9

Root

Root在本标准中特指在Android系统获取最高系统权限的一种技术手段。

3.10

敏感安全参数 sensitive security parameters；SSP

包括关键安全参数和公开安全参数。

[GM/T 0028-2014，定义3.82]

3.11

服务端密码组件 server side cryptographic component；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。

3.12

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。

3.13

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

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 概述

5.1 方案原理

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；CMMST-KEPOSS）技术架构是为保护移动智能终端（MST）密码模块敏感安全参数（SSP）而设计。其原理如图1所示。CMMST-KEPOSS将用户个人特征数据（PPD）经过密钥生成方法生成主密钥MK，使用MK对SSP（如用户私钥）进行加密，并传输到服务端密码组件（SS-CC）中保存，由于不持有加密密钥，SS-CC操作者不能获得用户SSP明文，从而保证SSP在CMMST-KEPOSS中的安全。

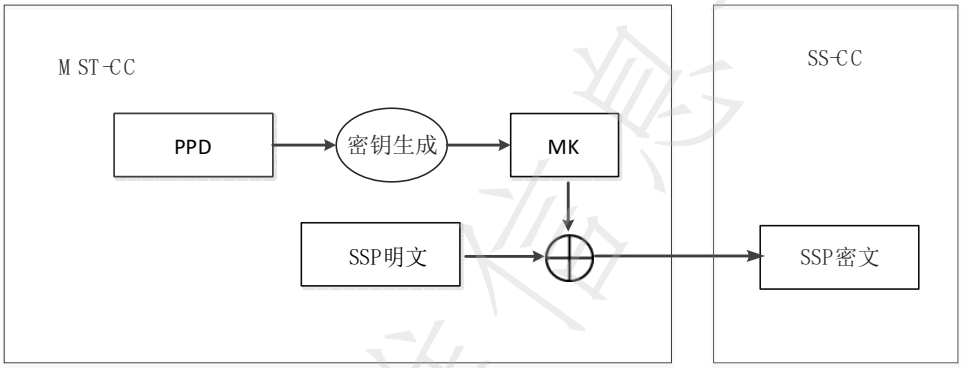


图1 CMMST-KEPOSS敏感安全参数保护原理

5.2 主要风险

CMMST-KEPOSS方案主要为防范以下风险而设计：

a）...MST-CC在可修改的运行环境中运行，操作系统以及不确定的第三方应用软件可能非法读取MST-CC敏感安全参数。

b）...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）...当移动智能终端密码模块用户丢失（或泄漏）其PPD以及移动设备时，非法用户可能冒充该用户进行密码操作。

5.3 安全措施

CMMST-KEPOSS架构至少采取以下安全措施以应对MST环境对SSP的威胁，满足GM/T 0028-2014标准一、二级要求。

a） MK 防护。通过 PPD 生成 MK，MK 只存在于内存中。

b） PPD 输入防护。采用输入试错锁定机制、界面劫持告警机制，软件加固机制等措施防止 PPD 输入时被劫持或泄露，PPD 只存在于内存中。

c） SSP 加密防护。采用核准的密码算法（SM4、SM3 算法），对 SSP 加密防护。

d） 通信连接保护。将 MST-CC 与用户数据、移动终端设备进行绑定，防止非法 MST-CC 与 SS-CC 进行通信。

e） MST-CC 运行环境保护。对移动终端设备进行完整性、合法性校验。如 root 检测，越狱检测等。

f） MST-CC 防护。采用软件加固、防动态调试、静态逆向等措施对 MST-CC 进行防护，保

证 MST 密码服务的安全性。

6 技术框架

6.1 概述

CMMST-KEPOSS技术框架由移动智能终端密码组件（MST-CC）及服务端密码组件（SS-CC）构成。MST-CC由移动应用调用，完成核准的密码算法功能，MST-CC将加密保护的SSP传给SS-CC保存。

CMMST-KEPOSS技术框架如图2所示。

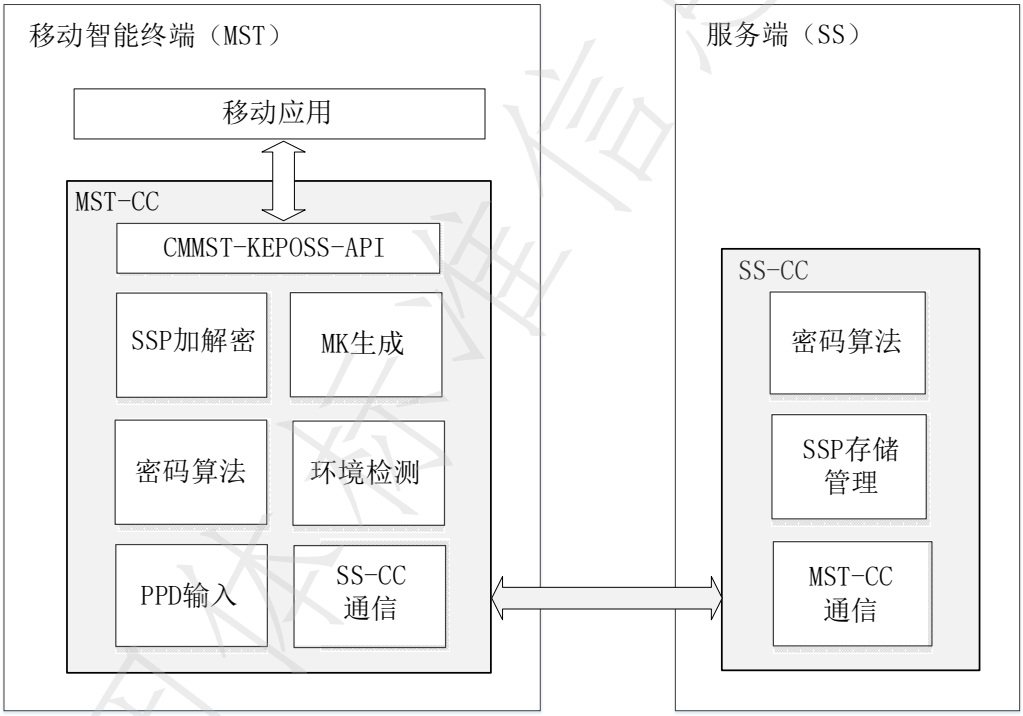


图2 CMMST-KEPOSS技术架构

6.2 移动智能终端密码组件（MST-CC）

MST-CC通过软件编译嵌入在移动应用中，移动应用通过独立进程调用MST-CC核准的密码服务功能，如数据加密、数据签名等。MST-CC至少包括完成以下功能的模块。

a）SSP 加解密。运用核准的密码算法对 SSP 进行加密，并上传至 SS-CC。移动终端本地不保存 SSP 信息。需要时，从 SS-CC 取回 SSP 密文进行解密使用。

b）MK 生成。使用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），以及移动终端用户 PPD，如 PIN 码、指纹、人脸、手势等数据生成 MK。

c）密码算法。实现核准的密码算法功能，如 SM2、SM3、SM4 算法。

d）SS-CC 通信。完成 MST-CC 与 SS-CC 之间通信连接。

e）环境检测。在移动应用初始化 MST-CC 时，检测密码模块运行环境，如 MST-CC 完整性，

移动设备是否被 root、越狱等。

f） PPD 输入。收集移动应用用户个人特征数据（PPD），并采用输入试错锁定、界面劫持告警，以及软件加固等机制保护 PPD。

g） CMMST-KEPOSS-API。移动应用调用本接口调用 MST-CC，完成密码服务功能。

6.3 服务端密码组件 SS-CC

SS-CC由软件构成。SS-CC协同MST-CC完成密码模块SSP保护。SS-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功能。如 SM2、SM3、SM4 算法。

b） SSP 存储管理。接收 MST-CC 上传的 SSP 密文数据，并保存在数据库中管理。需要时，SSP 密文数据由 MST-CC 中的 SSP 加解密模块请求下载并脱密使用。

c） MST-CC 通信。完成 MST-CC 与 SS-CC 之间通信连接。

6.4 移动应用

移动应用是使用移动密码模块的应用软件。移动应用使用软件编译方式将MST-CC嵌入移动应用中调用密码模块功能。

7 工作流程

7.1 密码模块初始化流程

移动应用使用CMMST-KEPOSS时，移动应用用户先对密码模块进行初始化，再调用密码模块进行数据签名、验签、加密、解密等操作。

CMMST-KEPOSS初始化流程如图3所示：

a） MST-CC 接收移动应用发起的初始化请求；

b） MST-CC 对自身进行自检；

c） MST-CC 对本地运行环境进行环境安全检测并与 SS-CC 建立通信；

d） MST-CC 生成 SSP，如公私钥对；

e） MST-CC 收集 PPD，如 PIN 码、手势码、指纹、人脸等；

f） MST-CC 使用 PPD 生成 MK 加密保护 SSP（如用户私钥）；

g） MST-CC 将明文 SSP 删除（如用户私钥）；

h） MST-CC 将 SSP 密文传给 SS-CC；

i） SS-CC 生成用户 ID，将 SSP 密文、用户 ID 保存在数据库中，并将用户 ID 返回给 MST-CC；

j） MST-CC 将用户 ID、用户公钥返回移动应用，初始化完成。

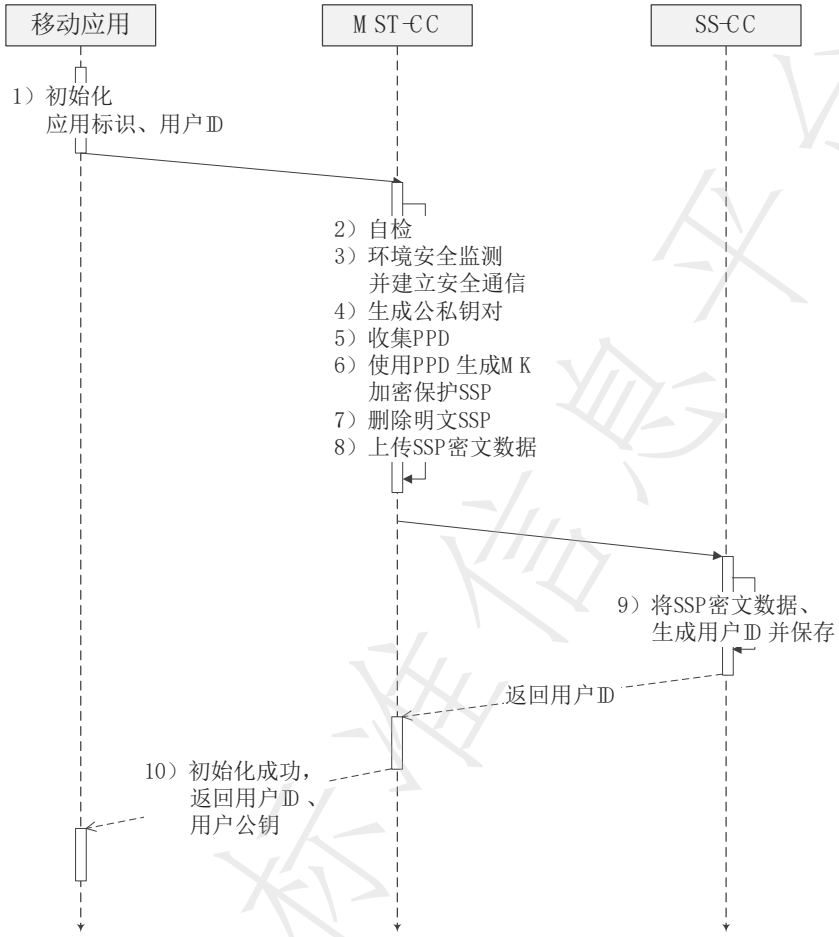


图3 CMMST-KEPOSS初始化流程

7.2 数字签名流程

数字签名流程如图4所示：

a） 移动应用向 MST-CC 发起签名请求，参数包括待签数据原文和用户 ID；

b） MST-CC 收集 PDD，如 PIN 码、手势码、指纹、人脸等；

c） MST-CC 向 SS-CC 发送用户 ID 请求私钥密文数据；

d） SS-CC 通过用户 ID 找出用户私钥密文，发送给 MST-CC；

e） MST-CC 使用 PDD 生成 MK 解密用户私钥密文，获得用户私钥；

f） MST-CC 使用用户私钥对待签数据进行签名；

g） MST-CC 删除用户私钥；

h） 移动应用获得签名数据，签名完成。

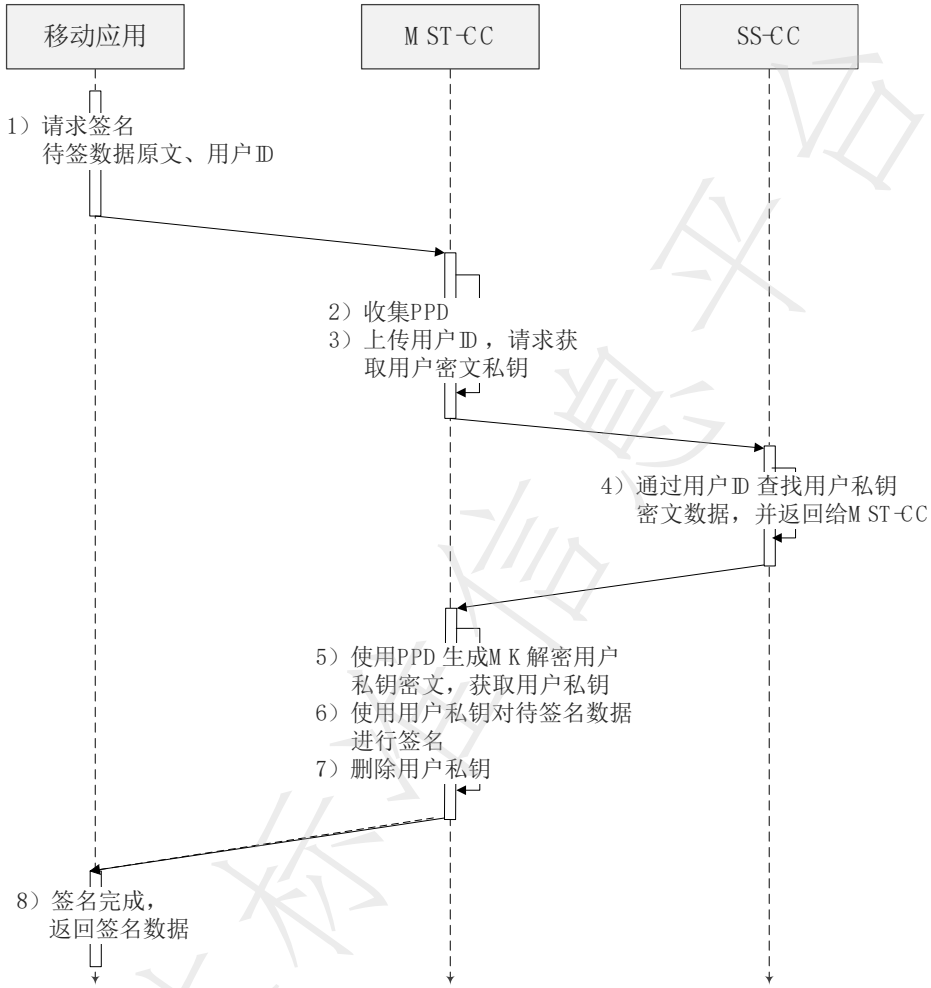


图4 CMMST-KEPOSS数字签名流程

7.3 签名验签流程

数字签名验签流程如图5所示：

a） 移动应用向 MST-CC 发起验签请求，发送用户公钥和待验签数据；

b） MST-CC 对待验签数据进行验签；

c） MST-CC 向移动应用返回验签结果。

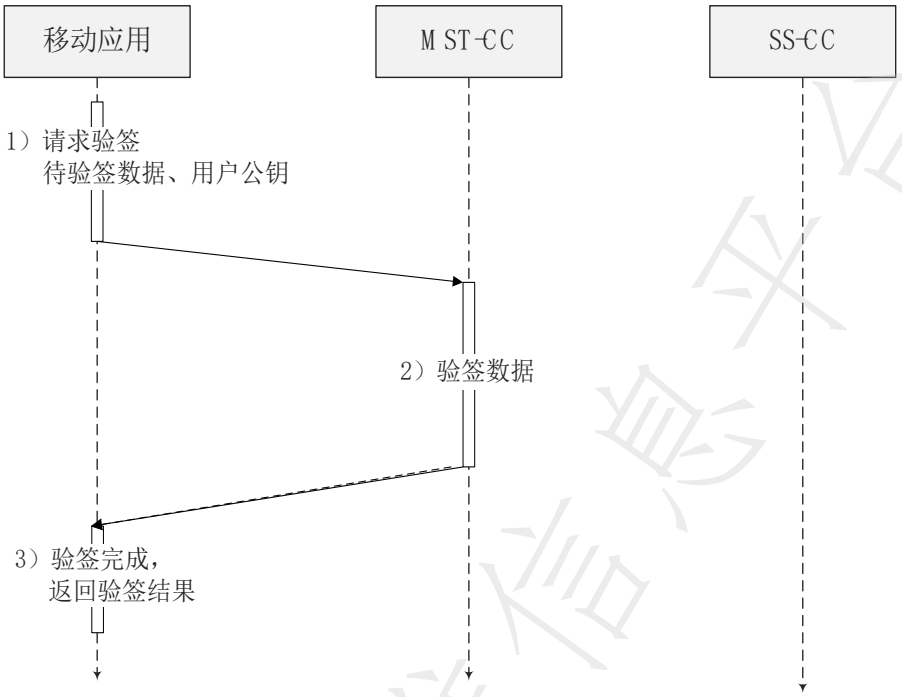


图5 CMMST-KEPOSS数字签名验签流程

8 密码模块规格

8.1 密码模块类型

CMMST-KEPOSS为软件密码模块，完成核准的SM2，SM3，SM4算法。

8.2 密码边界

CMMST-KEPOSS边界为MST-CC及SS-CC的可执行文件或文件集，见图2。

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。

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。

8.3 工作模式

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。

9 密码模块接口

9.1 物理和逻辑接口

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。

9.2 接口类型

须满足GM/T 0028-2014 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。

9.3 接口定义

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

10 角色、服务和鉴别

10.1 角色

CMMST-KEPOSS设立两种角色：SS-CC管理员、移动应用用户。

SS-CC管理员：负责SS-CC初始化，密钥密文数据库管理。

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。

10.2 服务

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	×	√

10.2.1 旁路能力

CMMST-KEPOSS不具备旁路能力或功能。

10.2.2 自启动密码服务能力

CMMST-KEPOSS不具备自启动密码服务能力或功能。

10.2.3 软件/固件加载

CMMST-KEPOSS不具备加载外部软件/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，还应具备以下角色鉴别机制：

SS-CC管理员：输入口令SS-CC方可执行操作。

移动应用用户：输入PPD后方可调用MST-CC完成密码服务。

11 软件/固件安全

a） MST-CC 自检时进行 MST-CC 完整性校验。

b） 使用 MST-CC 加固措施防止软件被动态调试和静态逆向分析。

12 运行环境

CMMST-KEPOSS运作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

遵照GM/T 0028—2014 7.6.3要求。

a） 安全一级

遵照GM/T 0028-2014 7.6.3中对应的安全一级要求。

b） 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。

13 密码模块物理安全

CMMST-KEPOSS不涉及物理安全要求。

14 非入侵式安全

CMMST-KEPOSS不涉及非入侵式安全要求。

15 敏感安全参数管理

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 0028-2014 7.9.1 中对安全一级,安全二级软件模块的要求，CMMST-KEPOSS 对以上敏感安全参数进行管理。

a）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。

b）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。

c）敏感安全参数（SSP）与移动应用用户PPD相关联。

15.1 随机比特生成器

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-KEPOSS敏感安全参数须满足GM/T 0028-2014 7.9.3中对安全一级,安全二级软件模块的要求生成。

a）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 0003.3-2012中相关规定。

b）MK由PPD通过合规的密钥产生方法（如GM/T 0003.3-2012中5.4.3规范）产生，其过程在MST-CC MK生成模块中执行。

c）PPD由MST-CC PPD输入模块输入生成。

15.3 敏感安全参数的建立

CMMST-KEPOSS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。

15.4 敏感安全参数的输入和输出

须满足GM/T 0028-2014 7.9.5中对安全一级,安全二级软件模块的要求。

a）d_M和P_M由MST-CC内部自动生成。

b）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。

c）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。

对于安全二级密码模块还至少具备以下输入、输出措施：

a）d_M以加密的形式输入给通信模块。

b）PPD输入防护须采用输入试错锁定机制，设置试错次数。

15.5 敏感安全参数的存储

须满足GM/T 0028-2014 7.9.6中对安全一级,安全二级软件模块的要求。

a）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。

b）P_M存储在移动应用中，只有验证用户PPD后才可使用。

c）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。

d）SS-CC不以明文形式存储d_M。

e）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。

15.6 敏感安全参数的置零

CMMST-KEPOSS中没有未受保护的SSP。满足GM/T 0028-2014 7.9.7中对安全一级,安全二级软件模块的要求不需置零。

16 自测试

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。

17 生命周期保障

17.1 配置管理

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。

安全一级、二级的CMMST-KEPOSS至少具备以下配置管理功能：

a） 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。

b） 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。

c） 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。

d） 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。

e） 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。

f） MST-CC 须支持初始化密码模块以允许绑定用户。

g） 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。

h） 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。

i） MST-CC 须支持注销以销毁内存中的 SSP。

j） SS-CC 须支持注销移动应用标识以结束 MST-CC 生命周期。

17.2 设计

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

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-KEPOSS有限状态模型至少包括下列状态：

a） 出厂状态：CMMST-KEPOSS集成（安装）后尚未使用时所处状态。

b） 自测试状态：CMMST-KEPOSS正在执行自测试时所处的状态。

c） 初始化状态：CMMST-KEPOSS密码模块初始运行后进入“初始化状态”。

d） 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。

e） 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。

f） 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。

g） 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。

h） 错误状态。当密码模块遇到错误状况时转到此状态。

CMMST-KEPOSS有限状模型如图6所示：

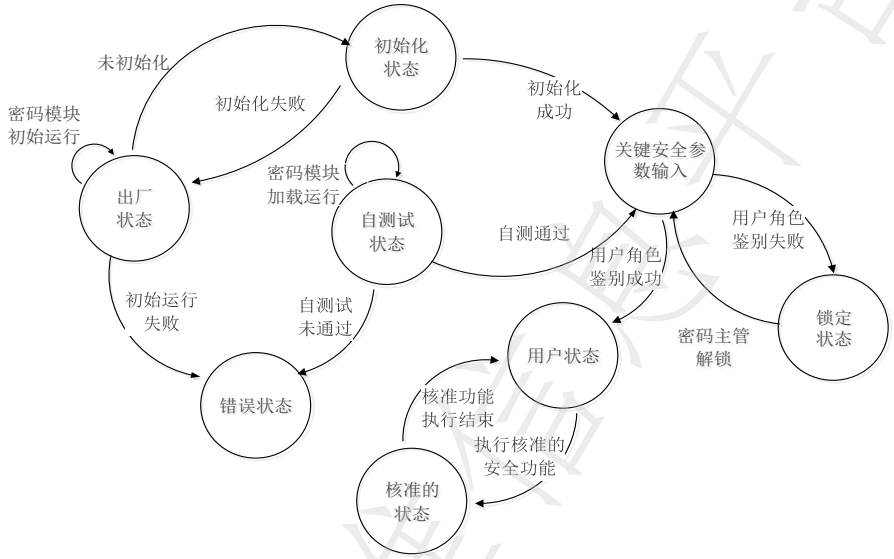


图6 CMMST-KEPOSS有限状态模型图

17.4 开发

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

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

满足GM/T 0028-2014 7.11.7中对安全一级,安全二级软件模块的要求。其中：

a） 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。

b） 安全二级

满足GM/T 0028-2014 7.11.7中对应的安全二级要求。

17.7 生命终止

满足GM/T 0028-2014 7.11.8中对安全一级,安全二级软件模块的要求。

17.8 指南文档

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

满足GM/T 0028-2014 7.12中对安全一级,安全二级软件模块的要求。

附 录A
（资料性附录）
应用示例（手机银行转账汇款身份认证）

在以往的手机银行应用中使用外设密码设备（如蓝牙盾）进行交易签名。本示例通过使用CMMST-KEPOSS密码模块实现免外设密码模块完成资金交易，以满足金融电子认证规范要求。

基于CMMST-KEPOSS移动智能终端密码模块实现手机银行转账汇款技术架构如图7所示。

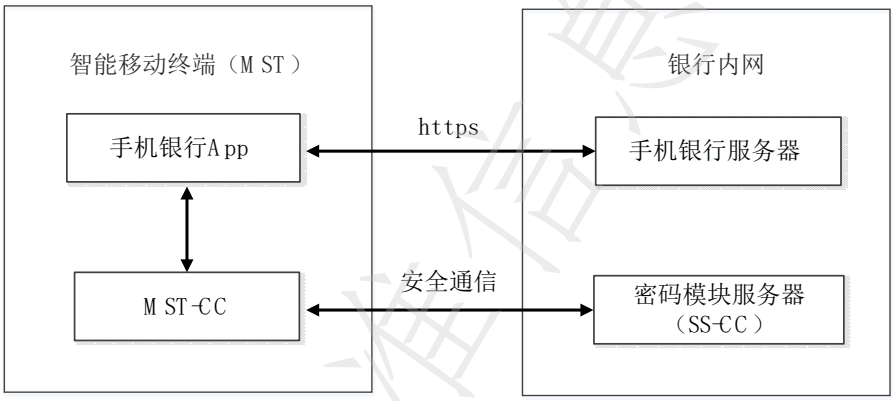


图7 基于CMMST-KEPOSS实现手机银行转账汇款的技术架构

手机银行App接入CMMST-KEPOSS技术架构完成转账汇款身份认证流程：

a) 手机银行开通转账汇款、选择认证方式等时对MST-CC初始化。初始化MST-CC时，MST-CC先进行自检，自检完成后，进行SSP生成、加密和存储（具体流程见本文档7.1章节）；

b) 在用户使用手机银行App进行转账汇款时，手机银行要求用户先进行身份认证。手机银行调用MST-CC的数字签名流程对转账汇款的业务数据进行签名；再调用MST-CC的签名验签接口获得转账汇款的业务数据（具体流程见本文档7.2、7.3章节）；

c) 手机银行App获得转账汇款的业务数据后请求手机银行服务器，手机银行服务器根据业务数据进行转账汇款。

手机银行App接入CMMST-KEPOSS技术架构完成转账汇款身份认证流程图8所示。

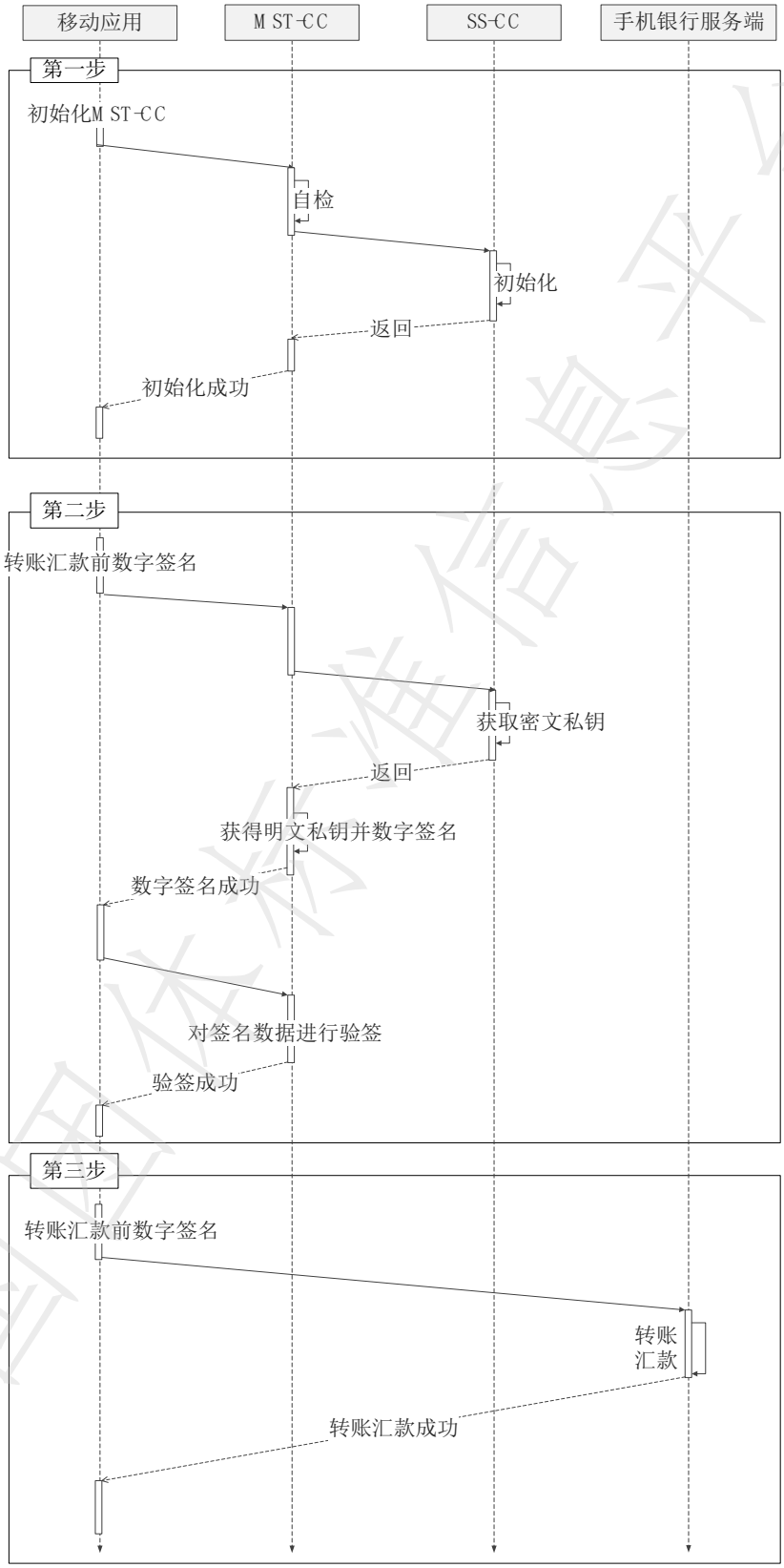


图8 基于CMMST-KEPOSS技术架构手机银行转账汇款业务流程

参考文献

[1] GM/T 0029-2014 签名验签服务器技术规范

ICS 35.240
L70/84

Assosication Standard

T/ZSA 67.3-2019

Technical framwork of cryptographic module in mobile smart terminal

Part 3: Key-encrypted protection on server side

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 the third 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, Institute of Information Engineering, Chinese Academy of Sciences, Qi'anxin Technology Group Co., Ltd., 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: Fu Wenbin, Wang Ke, Zhang Fan, Liu Zongbin, Zhang Jing, Li Bo, Lu Hongcheng, Li Xiangrong, Zhang Lingchen, etc.

INTRODUCTION

In the environment of open mobile networks and portable mobile terminal systems, how to securely design, implement, and use cryptographic modules, and how to protect sensitive security parameters have become the core issues in the design and implementation of cryptographic modules for mobile smart terminals. Encrypting and storing sensitive security parameters in mobile smart terminals is the main method to solve the security of software cryptographic modules. To prevent the threat to the security of sensitive security parameters be posed by the loss of encryption keys or the loss of ciphertext key data. This standard adopts the method of binding the personal property data of the mobile terminal user with the encryption key, and storing the key encrypted ciphertext on the server side to ensure the security of the sensitive security parameters of the cryptographic module.

Mobile smart terminal cryptographic module technology framework

Part 3: Key-encrypted protection on server side

1 SCOPE

This standard is for mobile terminal cryptographic modules that use key encryption server-side protection technology to standardize its technical framework and workflow. According to 11 security domain requirements including GM / T 0028-2014 cryptographic module specifications, cryptographic module interfaces, roles, services and authentication, software / firmware requirements, operating environment requirements, cryptographic module physical security, non-intrusive security, sensitive data management, self-testing, life cycle assurance, and mitigation of other attacks, specific specifications and application examples are given.

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

2 NORMATIVE 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".

GB / T 25069-2010 Information Security Technology Terms

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

GM / T 0028-2014 Cryptographic module security technical requirements

T / ZSA 67-2019 “Technical framework of cryptographic module in mobile smart terminal Part 1: General Principles"

3 TERMS AND DEFINITIONS

3.1 Approved Cryptographic Algorithm

The cipher algorithms given in GM / T0028-2014 Appendix C include block ciphers, stream ciphers, asymmetric algorithms, and hash functions.

3.2 Asymmetric Key Pair

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

[GB / T 25069-2010, definition 2.2.2.33]

3.3 CMMST-KEPOSS-API Interface

MST-CC provides an interface for mobile applications to complete cryptographic applications.

3.4 Master Key；MK

Symmetric keys, generated by a compliant key generation method, are used to encrypt sensitive security parameters.

3.5 Mobile Applications

The operating applications can be installed and used in the mobile smart terminal operating system. The mobile application mentioned in this standard refers to the application software that calls the cryptographic module service.

3.6 Mobile Smart Terminal；MST

The mobile terminal capable of accessing a mobile communication network, providing an application software development interface, and capable of installing and running application software. Such as mobile phones, Pad.

3.7 Mobile Smart Terminal Cryptographic Component；MST-CC

The cryptographic component deployed in a mobile smart terminal. In this specification, MST-CC and the server-side cryptographic component (SS-CC) together constitute the mobile smart terminal cryptographic module.

3.8 Personal Profile Data；PPD

Only the user personally knows or unique factors, such as PIN code, gesture code; the user's personal biological characteristics, such as fingerprint characteristics, facial characteristics, etc.

3.9 Root

Root in this standard refers to a technical means to get the highest system permissions in the Android system.

3.10 Sensitive Security Parameters；SSP

Includes critical security parameters and public security parameters.
[GM / T 0028-2014, definition 3.82]

3.11 Server Side Cryptographic Component；SS-CC

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

3.12 User Private Key

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

3.13 User Public Key

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

4 SYMBOLS AND ACRONYMS

The following symbols and acronyms apply to this document.

API	application program interface
APP	application
CSP	ritical security parameter
CMMST	cryptographic module of mobile smart terminal
CMMST-KEPOSS	CMMST of key-encrypted protection on server side
P_M	user public key
d_M	user private key
MK	master key
MST	mobile smart terminal
MST-CC	mobile smart terminal cryptographic components
PIN	personal identification number
PPD	personal profile data PPD
PSP	public security parameter
SDK	software development kit
SSP	sensitive security parameter
SS-CC	server side cryptographic components

5 OVERVIEW

5.1 Solution Principle

The CMMST of key-encrypted protection on server side (CMMST-KEPOSS) technology structure is designed to protect the sensitive security parameters (SSP) of the mobile smart terminal (MST) cryptographic module. Its principle is shown in Figure 1. CMMST-KEPOSS generates master key MK from the user's personal characteristic data (PPD) through the key generation method, uses the MK to encrypt the SSP (such as the user's private key), and transmits it to the server-side cryptographic component (SS-CC) for storage. Because the encryption key is not held, the SS-CC operator cannot get the user's SSP plaintext, thereby ensuring the security of the SSP in CMMST-KEPOSS.

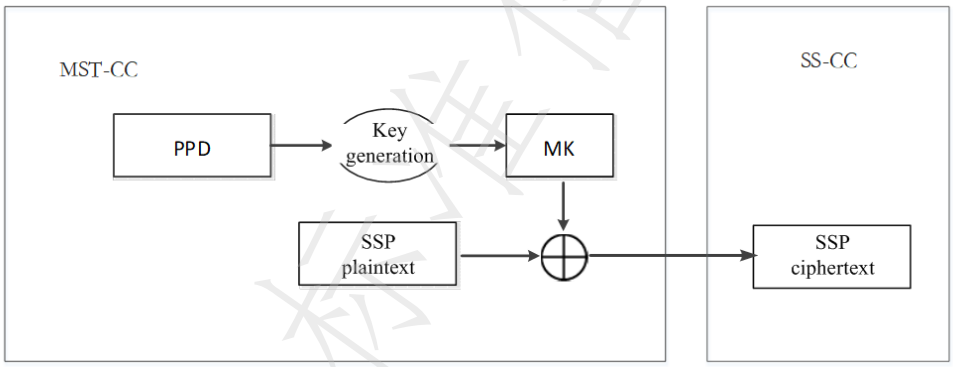


Figure 1 CMMST-KEPOSS Sensitive Security Parameter Protection Principle

5.2 Key Risks

The CMMST-KEPOSS plan is designed to prevent the following risks:

(1) MST-CC operates in a modifiable operating environment. The operating system and uncertain third-party application software may illegally read MST-CC sensitive security parameters.

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

(3) When the user of the mobile smart terminal cryptographic module loses (or leaks) his PPD and mobile device, an illegal user may impersonate the user for cryptographic operations.

5.3 Security Measures

The CMMST-KEPOSS structure adopts at least the following security measures to respond to the threat of the MSP environment to the SSP and meet the level 1 and level 2

requirements of the GM / T 0028-2014 standard.

(1) MK protection. Generate MK through PPD, MK only exists in memory.

(2) PPD input protection. The input trial-and-error lock mechanism, interface hijacking alarm mechanism, and software hardening mechanism are adopted to prevent PPD from being hijacked or leaked during input. PPD only exists in memory.

(3) SSP encryption protection. Adopt approved cryptographic algorithms (SM4, SM3 algorithms) for SSP encryption protection.

(4) Communication connection protection. Bind MST-CC with user data and mobile terminal equipment to prevent illegal MST-CC from communicating with SS-CC.

(5) Environmental protection of MST-CC operation. Check the integrity and legality of the mobile terminal equipment. Such as root detection, jailbreak detection, etc.

(6) MST-CC protection. Software reinforcement, anti-dynamic debugging, static reverse and other measures are adopted to protect MST-CC to ensure the security of MST cryptographic service.

6 TECHNICAL FRAMEWORK

6.1 Overview

The CMMST-KEPOSS technology framework consists of a mobile smart terminal cryptographic component (MST-CC) and a server-side cryptographic component (SS-CC). MST-CC is called by the mobile application to complete the approved cryptographic algorithm function. MST-CC passes the encrypted SSP to SS-CC for storage.

CMMST-KEPOSS technology framework is shown in Figure 2.

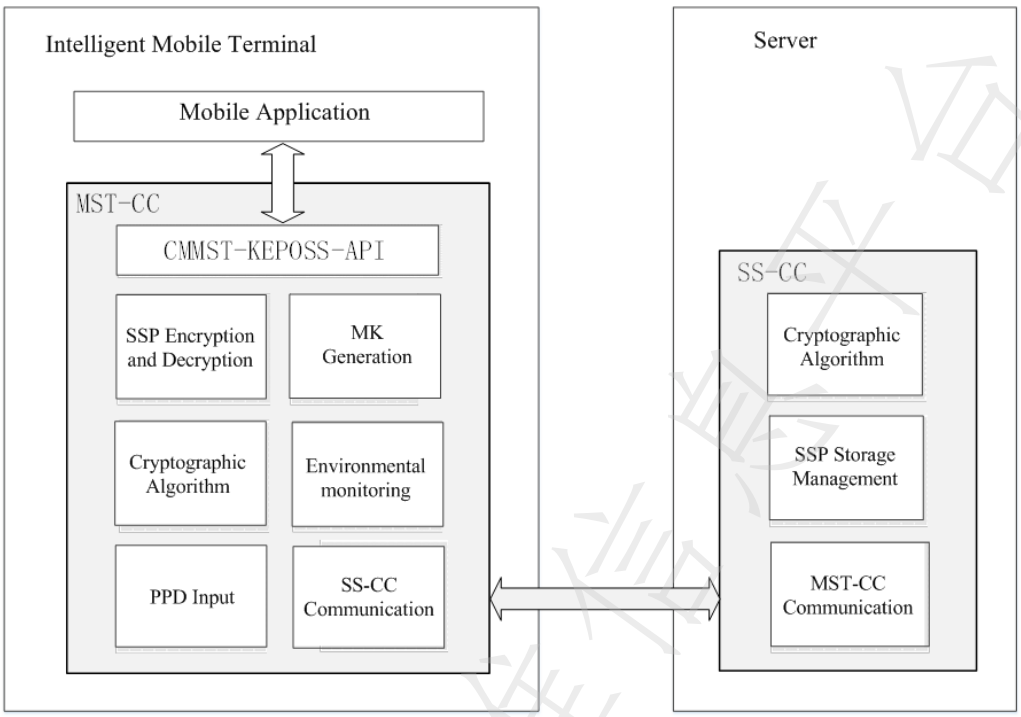


Figure 2 CMMST-KEPOSS Technology Structure

6.2 Mobile Smart Terminal Cryptographic Component (MST-CC)

MST-CC is embedded in the mobile application through software compilation. The mobile application invokes the cryptographic service functions approved by MST-CC through independent processes, such as data encryption and data signature. MST-CC includes modules that at least perform the following functions.

(1) SSP encryption and decryption. The SSP is encrypted using an approved cryptographic algorithm and uploaded to SS-CC. The mobile terminal does not save SSP information locally. When needed, retrieve the SSP ciphertext from SS-CC for decryption.

(2) MK generation. Use the key generation mechanism (such as GMT 0003.4-2012 SM2 elliptic curve public key cryptographic algorithm) that complies with relevant national requirements, and mobile terminal user PPD, such as PIN code, fingerprint, face, gesture and other data to generate MK.

(3) Cryptographic algorithm. Implement approved cryptographic algorithm functions, such as SM2, SM3, and SM4 algorithms.

(4) SS-CC communication. Complete the communication connection between MST-CC and SS-CC.

(5) Environmental testing. When the mobile application initializes the MST-CC, it detects the operating environment of the cryptographic module, such as the integrity of the MST-CC, and whether the mobile device has been rooted or jailbroken.

(6) PPD input. Collect personal characteristic data (PPD) of mobile application users, and use mechanisms such as input trial and error lock, interface hijacking alert, and software hardening to protect PPD.

(7) CMMST-KEPOSS-API. The mobile application calls this interface to call MST-CC to complete the cryptographic service function.

6.3 Server-side cryptographic component SS-CC

SS-CC consists of software. SS-CC cooperates with MST-CC to complete the cryptographic module SSP protection. SS-CC includes at least modules that perform the following functions:

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

(2) SSP storage management. Receive the SSP ciphertext data uploaded by MST-CC and save it in the database for management. When needed, the SSP ciphertext data is requested to be downloaded by the SSP encryption and decryption module in the MST-CC and decrypted to be used.

(3) MST-CC communication. Complete the communication connection between MST-CC and SS-CC.

6.4 Mobile Application

A mobile application is application software that uses a mobile cryptographic module. The mobile application uses software compilation to embed the MST-CC in the mobile application to call the cryptographic module function.

7 WORK FLOW

7.1 Cryptographic Module Initialization Process

When the mobile application uses CMMST-KEPOSS, the mobile application user first initializes the cryptographic module and then calls the cryptographic module to perform data signing, signature verification, encryption, and decryption operations.

The CMMST-KEPOSS initialization process is shown in Figure 3:

1) MST-CC receives the initialization request initiated by the mobile application;
2) MST-CC performs self-test on itself;
3) MST-CC performs environmental security inspection on the local operating environment and establishes communication with SS-CC;
4) MST-CC generates SSP, such as public and private key pair;
5) MST-CC collects PPD, such as PIN code, gesture code, fingerprint, face, etc .;
6) MST-CC uses PPD to generate MK encryption to protect SSP (such as user private key);
7) MST-CC deletes the plaintext SSP (such as the user's private key);
8) MST-CC transmits the SSP ciphertext to SS-CC;

9) SS-CC generates user ID, stores SSP ciphertext and user ID in the database, and returns user ID to MST-CC;
10) MST-CC returns the user ID and user public key to the mobile application, and initialization is completed.

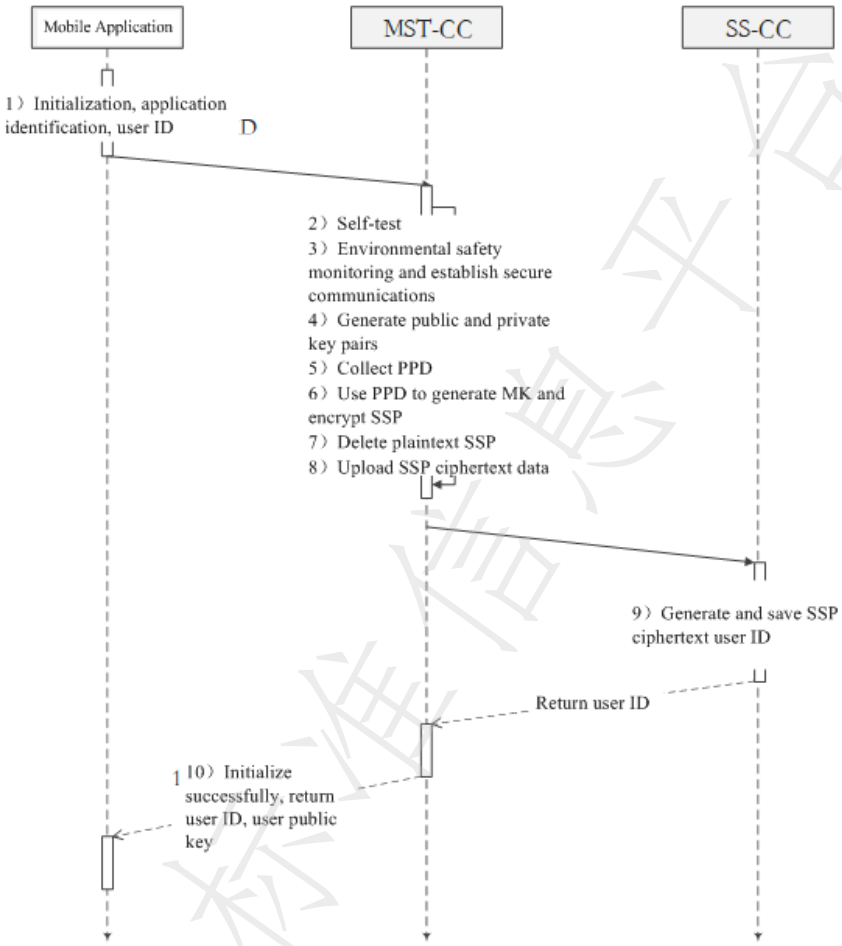


Figure 3 CMMST-KEPOSS Initialization Process

7.2 Digital Signature Process

The digital signature process is shown in Figure 4:

1) The mobile application initiates a signing request to MST-CC, and the parameters include the original text of the data to be signed and the user ID;
2) MST-CC collects PDD, such as PIN code, gesture code, fingerprint, face, etc .;
3) MST-CC sends the user ID to the SS-CC requesting the private key ciphertext data;
4) SS-CC finds the user's private key ciphertext by user ID and sends it to MST-CC;
5) MST-CC uses PDD to generate MK to decrypt the user's private key ciphertext and obtain the user's private key;
6) MST-CC uses the user's private key to sign the signed data;
7) MST-CC deletes the user's private key;
8) The mobile application obtains the signature data and the signature is complete.

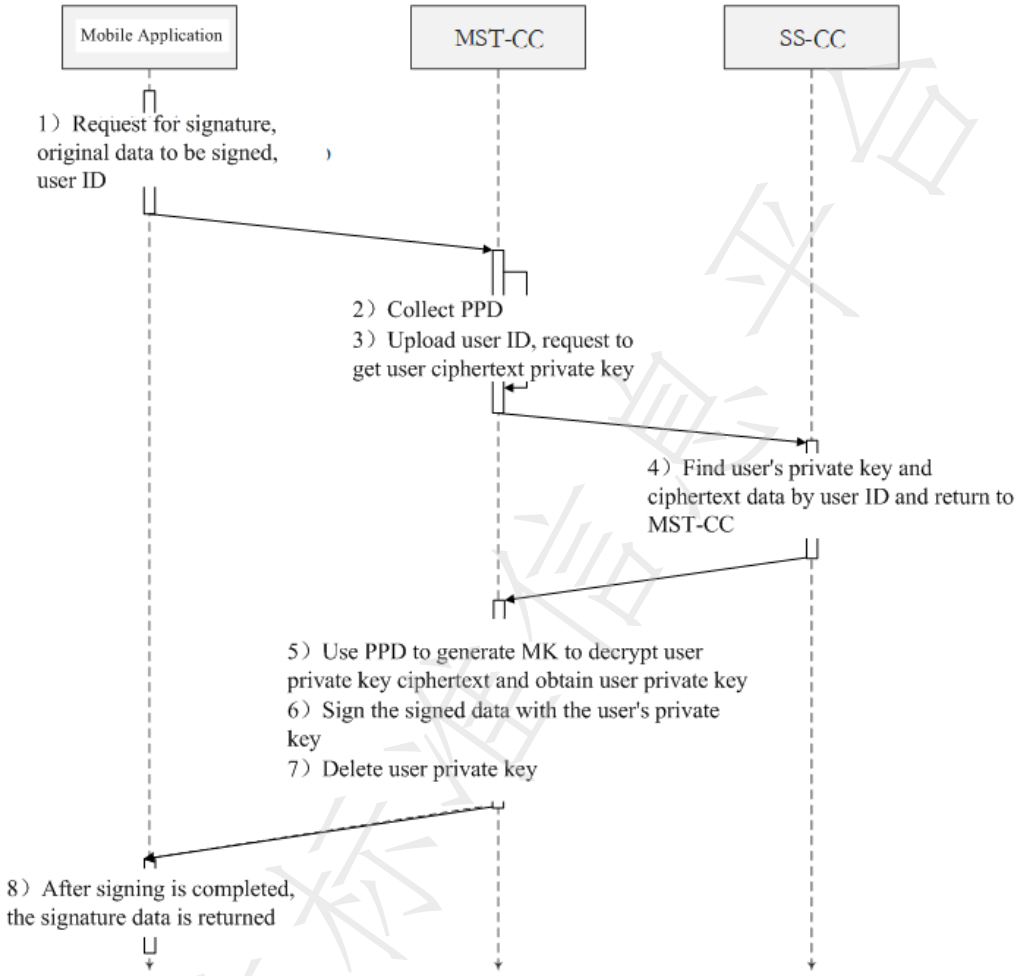


Figure 4 CMMST-KEPOSS Digital Signature Process

7.3 Signature Verification Process

The digital signature verification process is shown in Figure 5:

1) The mobile application initiates a signing request to the MST-CC and sends the user's public key and data to be checked;

2) MST-CC shall verify the signature data;

3) MST-CC returns the verification result to the mobile application.

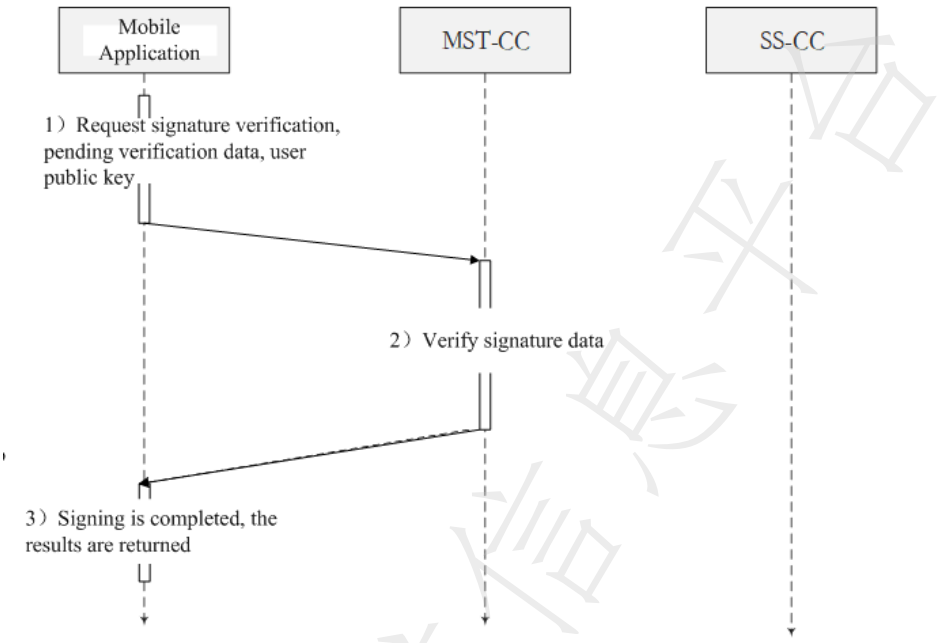


Figure 5 CMMST-KEPOSS Digital Signature Verification Process

8 CRYPTOGRAPHIC MODULE SPECIFICATIONS

8.1 Cryptographic Module Types

CMMST-KEPOSS is a software cryptographic module that completes the approved SM2, SM3, and SM4 algorithms.

8.2 Cryptographic Boundary

The CMMST-KEPOSS boundary is the executable file or file set of MST-CC and SS-CC, as shown in Figure 2.

MST-CC includes modules that at least complete the following functions: SSP encryption and decryption, MK generation, cryptographic algorithms, SS-CC communication, environmental security detection, PPD input, CMMST-KEPOSS-API.

SS-CC includes modules that at least complete the following functions: cryptographic algorithms, SSP storage management, and MST-CC communication.

8.3 Working Mode

Must meet the requirements of GM / T 0028-2014 7.2.4 for the security level 1 and security level 2 software modules.

9 CRYPTOGRAPHIC MODULE INTERFACE

9.1 Physical and Logical Interfaces

CMMST-KEPOSS logical interfaces are distributed on MST-CC and SS-CC, the two logical interfaces are of the same type.

9.2 Interface Types

It must meet the requirements of GM / T 0028-2014 7.3.2 for security level 1 and security level 2 software modules. CMMST-KEPOSS is a software module that provides API calls to mobile applications.

9.3 Interface Definition

Please refer to GM / T 0019-2012 General Cryptographic Service Interface Specification for CMMST-KEPOSS interface definition.

10 ROLES, SERVICES AND IDENTIFICATION

10.1 Roles

CMMST-KEPOSS establishes two roles: SS-CC supervisor, mobile application user.

SS-CC supervisor: responsible for SS-CC initialization, key ciphertext database management.

Mobile application users: perform cryptographic functions, such as data signature, data verification, data encryption, and data decryption.

10.2 Service

The services provided for SS-CC supervisors and mobile application user roles are shown in Table 1:

Table 1 CMMST-KEPOSS Roles and Services

Service	Description	SS-CC manager	User
SS-CC Initialization	Initialize SS-CC to provide operation basis for MST-CC.	√	×
Initialization of MST-CC	Initialize MST-CC	×	√
Data Signature	Provide data signature for mobile applications	×	√
Data Verification	Provide data signature verification for mobile	×	√

	applications		
Data Encryption	Provide data encryption for mobile applications	×	√
Data Decryption	Provide data decryption for mobile applications	×	√

10.2.1 Bypass Capability

CMMST-KEPOSS does not have bypass capabilities or functions.

10.2.2 Self-starting Cryptographic Service Capability

CMMST-KEPOSS does not have the ability or function of self-starting cryptographic service.

10.2.3 Software / Firmware Loading

CMMST-KEPOSS does not have the ability to load external software / firmware.

10.3 Identification

In addition to meeting the requirements of GM / T 0028-2014 7.4.4 for the security level 1 and security level 2 software modules, it should also have the following role identification mechanism:

SS-CC supervisor: Enter the password then SS-CC can perform the operation.

Mobile application users: After entering PPD, MST-CC can be called to complete the cryptographic service.

11 SOFTWARE / FIRMWARE SECURITY

(1) MST-CC integrity check is checked during MST-CC self-test.

(2) Use MST-CC hardening measures to prevent the software from being dynamically debugged and statically reversed analyzed.

12 OPERATING ENVIRONMENT

CMMST-KEPOSS operates in a modifiable operating environment.

12.1 Operating System Requirements That Can Modify The Operating Environment

Comply with the requirements of GM / T 0028—2014 7.6.3.

(1) Security level 1

Comply with the corresponding safety level 1 requirements in GM / T 0028-2014 7.6.3.

(2) Security level 2

On the basis of security level 1, the following measures are added:

a) MST-CC shall run in a separate process space;

b) MST-CC must run in a legitimate operating system, such as an unrooted or jailbroken operating system;

c) 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-KEPOSS does not involve physical security requirements.

14 NON-INVASIVE SECURITY

CMMST-KEPOSS does not involve non-intrusive security requirements.

15 SENSITIVE SECURITY PARAMETER MANAGEMENT

CMMST-KEPOSS sensitive security parameters (SSP) include:

d_M-user private key

P_M-user public key

MK-master key

PPD-user personal property data

It must meet the requirements of GM / T 0028-2014 7.9.1 for the security level 1 and security level 2 software modules. CMMST-KEPOSS manages the above sensitive security parameters.

(1) The key security parameters (CSP) d_M, MK, and PPD are protected within the cryptographic module to prevent unauthorized access, use, disclosure, modification, and replacement. The d_M is encrypted by an approved cryptographic algorithm and stored in SS-CC.

(2) The public security parameter (PSP) PM is stored in the MST-CC to prevent unauthorized modification and replacement.

(3) Sensitive security parameters (SSP) are associated with mobile application user PPD.

15.1 Random Bit Generator

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

15.2 Generation of Sensitive Security Parameters

CMMST-KEPOSS sensitive security parameters must be generated in accordance with the requirements of GM / T 0028-2014 7.9.3 for the security level 1 and security level 2 software modules.

(1) d_M and P_M are generated by the SSP encryption and decryption module inside the MST-CC, and the generation conforms to the relevant regulations in GM / T 0003.3-2012.

(2) MK is generated by PPD through a compliant key generation method (such as the 5.4.3 specification in GM / T 0003.3-2012), and the process is performed in the MST-CC MK generation module.

(3) The PPD is generated by the input of the MST-CC PPD input module.

15.3 The Establishment of Sensitive Security Parameters

CMMST-KEPOSS sensitive security parameters must meet the requirements of GM / T 0028-2014 7.9.4 for the security level 1 and security level 2 software modules.

15.4 Input and output of Sensitive Security Parameters

Must meet the requirements of GM / T 0028-2014 7.9.5 for security level 1 and security level 2 software modules.

(1) d_M and P_M are automatically generated by MST-CC.

(2) PPD is manually input by the PSD input module (UI) of MST-CC, and PPD is not output outside the password module.

(3) MK is generated by MK-CC's MK generation module. It is cleared after being used and is not outputted outside the cryptographic module.

The security level 2 cryptographic module also has at least the following input and output measures:

(1) d_M is input to the communication module in the encrypted form.

(2) PPD input protection must use the input trial and error lock mechanism to set the number of trial and error.

15.5 Storage of Sensitive Security Parameters

Must meet the requirements of GM / T 0028-2014 7.9.6 for security level 1 and security level 2 software modules.

(1) Encrypt d_M with MK, and use a variety of PPDs (such as PIN code, gesture code, fingerprint, etc.) as MK generation factors.

(2) P_M is stored in the mobile application and can only be used after verifying the user's PPD.

(3) The d_M of the MST-CC does not appear in plain text in the non-volatile storage of the MST. The d_M needs to be uploaded to the SS-CC for storage.

(4) SS-CC does not store d_M in clear text.

(5) When encrypting d_M, the key length of the symmetric encryption algorithm used is at least 32 bits, and the block length is at most 256 bits.

15.6 Nulling Sensitive Safety Parameters

There is no unprotected SSP in CMMST-KEPOSS. It meets the requirements of GM / T 0028-2014 7.9.7 for the security level 1 and security level 2 software modules and does not need to be nulled.

16 SELF-TEST

Meet the requirements of GM / T 0028-2014 7.10 for security level 1 and security level 2 software modules.

The MST-CC performs a self-test of the MST-CC during initialization and each startup, including MST-CC integrity, mobile terminal integrity (not be rooted), and so on.

17 LIFE CYCLE GUARANTEE

17.1 Configuration Management

Meet the requirements of GM / T 0028-2014 7.11.2 for security level 1 and security level 2 software modules.

CMMST-KEPOSS with security level 1 and level 2 has at least the following configuration management functions:

(1) MST-CC, SS-CC development process and related documents need to use the configuration management system.

(2) MST-CC, SS-CC related code and related documents need to be carried permission separation in the configuration management.

(3) MST-CC and SS-CC need to be carried permission separation in configuration management according to different module codes.

(4) The configuration management system maintains changes to the CMMST-KEPOSS identification and version, or revision of each configuration entry.

(5) The SS-CC shall support the establishment of a mobile application identity and a preset communication key for secure communication to start the MST-CC life cycle.

(6) MST-CC shall support initialization of the cryptographic module to allow binding users.

(7) MST-CC shall support binding users to allow mobile application users to use the cryptographic module cryptographic application.

(8) MST-CC shall support unbinding and logout of users to prohibit mobile application users from using the cryptographic module cryptographic application.

(9) MST-CC shall support logout to destroy SSP in memory.

(10) The SS-CC shall support the logout of the mobile application identity to end the MST-CC life cycle.

17.2 Design

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

Meet the requirements of GM / T 0028-2014 7.11.4 for the security level 1 and security level 2 software modules The CMMST-KEPOSS finite state model includes at least the following states:

(1) Ex-factory status: The status when CMMST-KEPOSS is integrated (installed) and not yet used.

(2) Self-test status: The status of CMMST-KEPOSS when it is performing self-test.

(3) Initialization status: The CMMST-KEPOSS cryptographic module enters the "initialization state" after initial operation.

(4) User status: The status when the mobile application uses CMMST-KEPOSS for approved cryptographic services.

(5) Approved status. CMMST-KEPOSS is in the status when it is performing the approved cryptographic function. When the cryptographic service is completed, it exits this status and changes to the user state.

(6) Input status of key security parameters. The status when MST-CC receives the user's personal property data (PPD), and when the user enters the correct PPD, it will return to the user status.

(7) Locked state: CMMST-KEPOSS will enter the locked state when the number of PPD errors entered by the user reaches a certain threshold.

(8) Error status. Go to this status when the cryptographic module is in an error condition.

The CMMST-KEPOSS finite state model is shown in Figure 6:

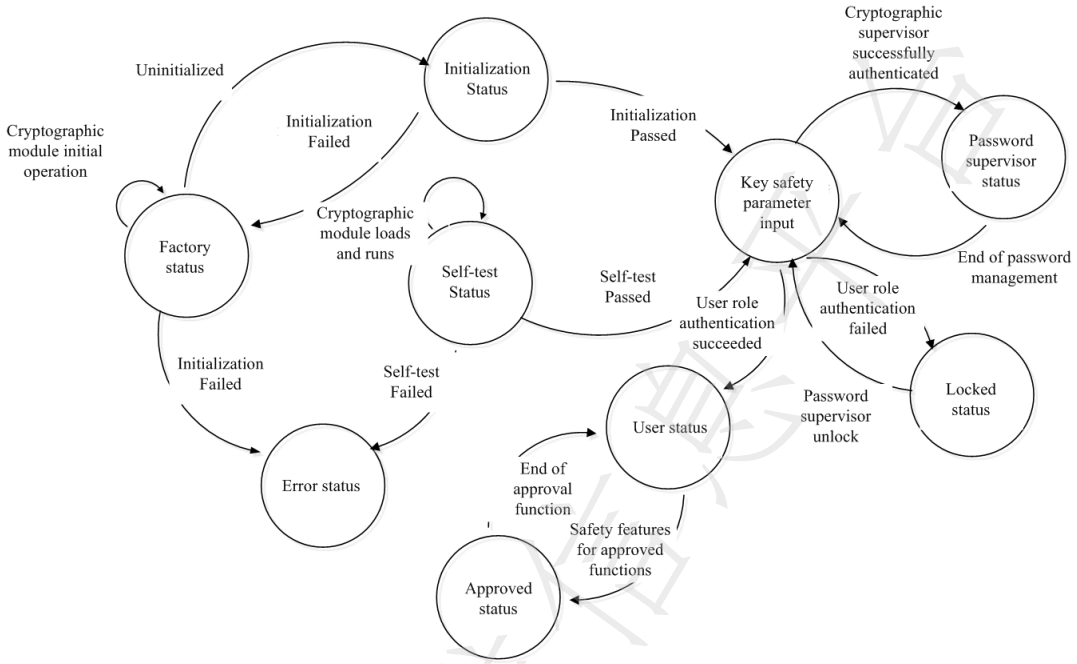


Figure 6 CMMST-KEPOSS Finite State Model

17.4 Development

Meet the requirements of GM / T 0028-2014 7.11.5 for security level 1 and security level 2 software modules.

17.5 Test

Meet the requirements of GM / T 0028-2014 7.11.6 for security level 1 and security level 2 software modules.

17.6 Distribution and Operation

Meet the requirements of GM / T 0028-2014 7.11.7 for the security level 1 and security level 2 software modules. among them:

(1) Security level 1

Mobile applications use software compilation to embed MST-CC in mobile applications and install them in mobile terminals together with mobile application software. The initialization process of the cryptographic module can be seen in section 7.1 of this document.

(2) Security Level 2

Meet the requirements for the security level 2 in GM / T 0028-2014 7.11.7.

17.7 Life Termination

Meet the requirements of GM / T 0028-2014 7.11.8 for security level 1 and security level 2 software modules.

17.8 Guide Documents

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

Meet the requirements of GM / T 0028-2014 7.12 for security level 1 and security level 2 software modules.

Appendix A

(Informative appendix)

Application example (mobile bank transfer and remittance identity authentication)

In previous mobile banking applications, peripheral cryptographic devices (such as Bluetooth shields) were used to sign transactions. This example uses the CMMST-KEPOSS cryptographic module to implement a peripheral-free cryptographic module to complete fund transactions to meet the financial electronic certification specification requirements.

The CMMST-KEPOSS-based mobile smart terminal cryptographic module used to implement mobile bank transfer and remittance technology structure is shown in Figure 7.

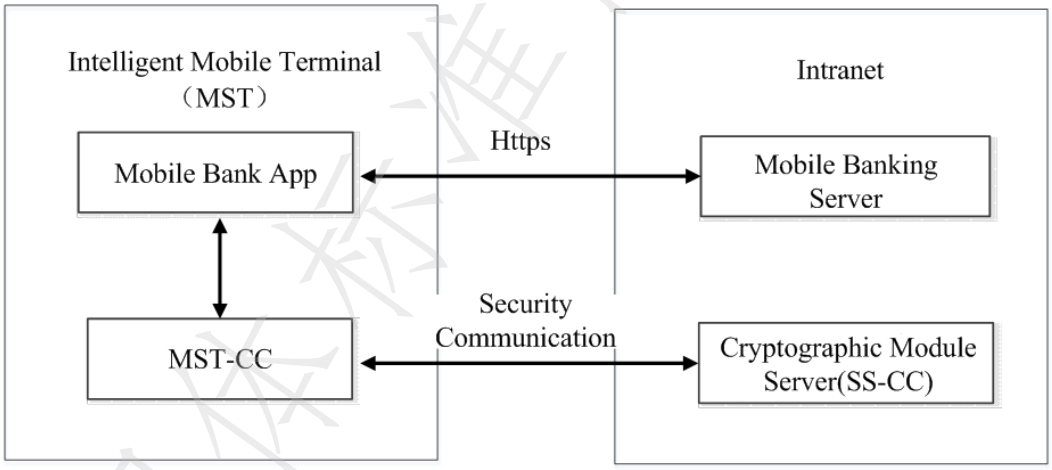


Figure 7 The CMMST-KEPOSS-based mobile bank transfer and remittance technology structure

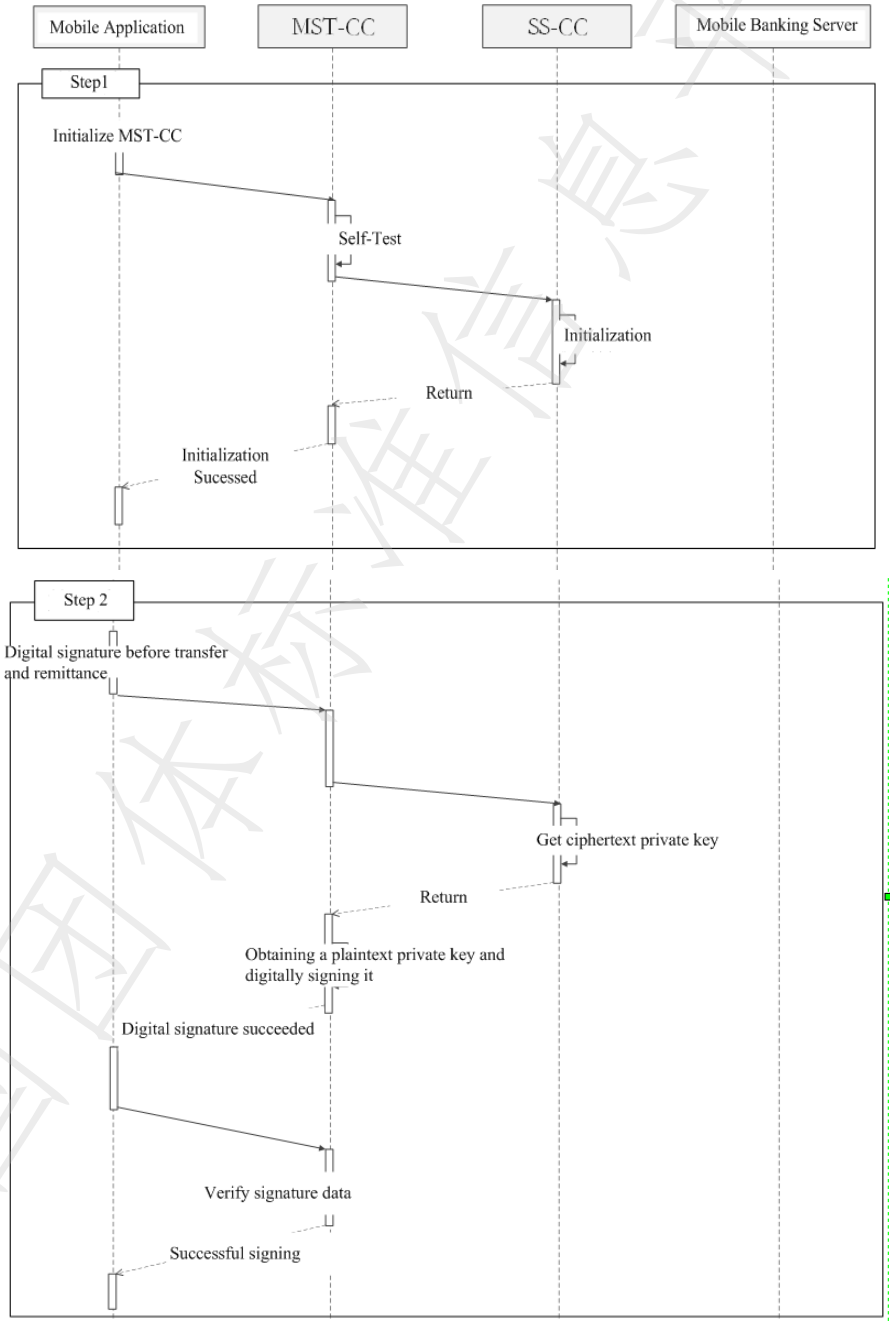
Mobile Banking App accesses CMMST-KEPOSS technology structure to complete the transfer and remittance identity authentication process:

1) MST-CC is initialized when mobile bank opens transfer and remittance, selects authentication method, etc. When the MST-CC is initialized, the MST-CC firstly performs a self-test, after that, the SSP is generated, encrypted, and stored (please refer to section 7.1 of this document for details);

2) When a user uses the mobile banking app to transfer, mobile banking requires the user to perform identity authentication first. Mobile Banking calls the MST-CC digital signature process to sign the business data of the transfer and remittance; and then calls the MST-CC's signature verification interface to get the business data of the transfer and remittance (please refer to section 7.2 and 7.3 of this document for details);

3) The mobile banking app requests the mobile banking server after getting the business data of the transfer and remittance, and the mobile banking server performs the transfer and remittance according to the business data.

The flowchart of mobile banking App accessing the CMMST-KEPOSS technology structure to complete the transfer and remittance identity authentication is shown in Figure 8.



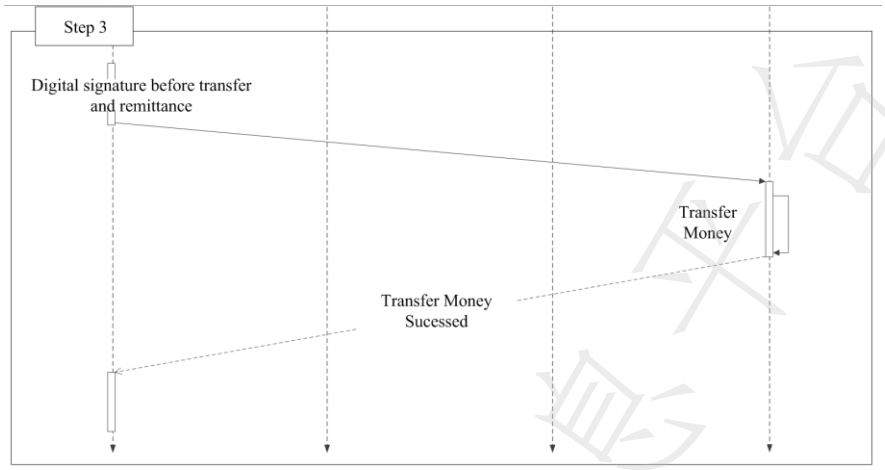


Figure 8 CMMST-KEPOSS-based Technology Structure Mobile Bank Transfer and Remittance Business Process

BIBLIOGRAPHY

[1] GM / T 0029-2014 Technical specifications for signature verification server