团　　体　　标　　准

T/ EMCG 001.3-2019

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

2019－07－05 发布　　2019－07－05 实施

中关村网络安全与信息化产业联盟　发布

目　次

前　言

T/EMCG 001-2019《移动智能终端密码模块技术框架》分为5个部分：

第1部分：总则

第2部分：密钥加密本地保护技术架构

第3部分：密钥加密服务端保护技术架构

第4部分：密钥多端协同计算保护技术架构

第5部分：基于安全芯片的技术架构

本部分为T/EMCG 001-2019《移动智能终端密码模块技术框架》的第3部分。

本部分由中关村网络安全与信息化产业联盟企业移动计算工作组（EMCG）提出。

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

本部分主要起草单位：中关村网络安全与信息化产业联盟企业移动计算工作组（EMCG）、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/EMCG 001-2019《移动智能终端密码模块技术框架》的本部分的引用而成为本部分的条款。

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/EMCG 001-2019《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

参见GM/T0028-2014附录C给出的密码算法。

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。

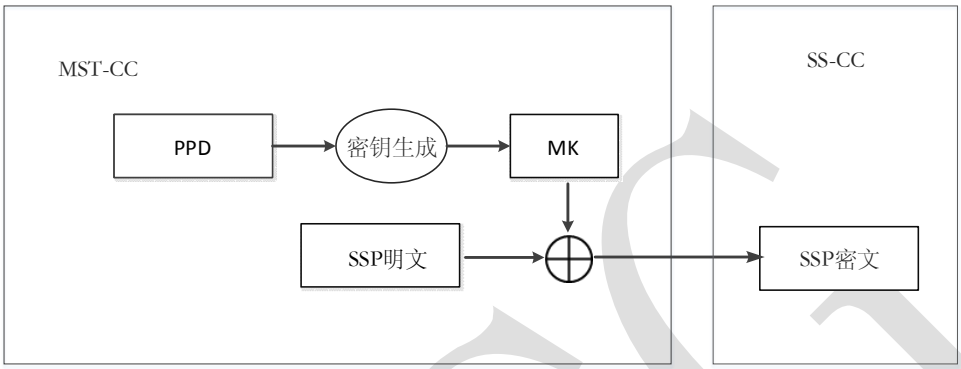

图1 CMMST-KEPOSS敏感安全参数保护原理

5.2 主要风险

CMMST-KEPOSS方案主要为防范以下风险而设计：

（1） 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。

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

（3） 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。

（1） MK 防护。通过 PPD 生成 MK，MK 只存在于内存中。

（2） 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。

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

（4） 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。

（5） 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。

（6） 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

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。

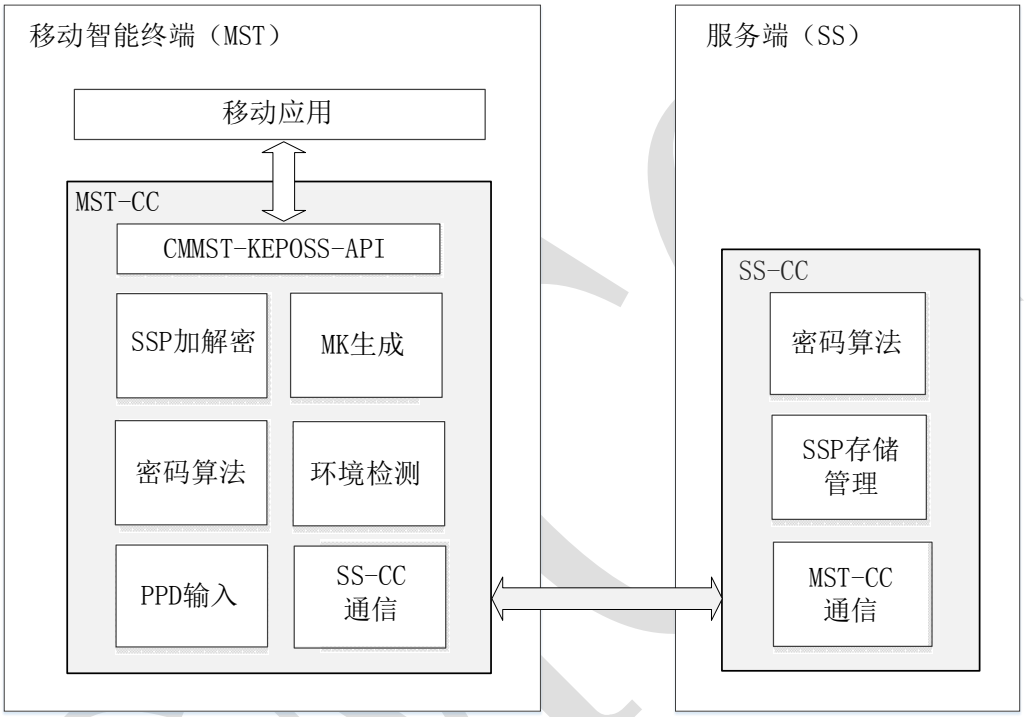

图2 CMMST-KEPOSS技术架构

6.1 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。

（1） 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。

（2） 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。

（3） 密码算法。实现核准的密码算法功能，如 SM2、SM3、SM4 算法。

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

（5） 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。

（6） 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。

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

6.2 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：

（1） 密码算法。实现核准的密码算法功能。如 SM2、SM3、SM4 算法。

（2） 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。

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

6.3 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 主要工作流程

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：

1) MST-CC 接收移动应用发起的初始化请求；
2) MST-CC 对自身进行自检；
3) 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；
4) MST-CC 生成 SSP，如公私钥对；
5) MST-CC 收集 PPD，如 PIN 码、手势码、指纹、人脸等；
6) MST-CC 使用 PPD 生成 MK 加密保护 SSP（如用户私钥）；
7) MST-CC 将明文 SSP 删除（如用户私钥）；
8) MST-CC 将 SSP 密文传给 SS-CC；
9) 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；
10) MST-CC 将用户 ID、用户公钥返回移动应用，初始化完成。

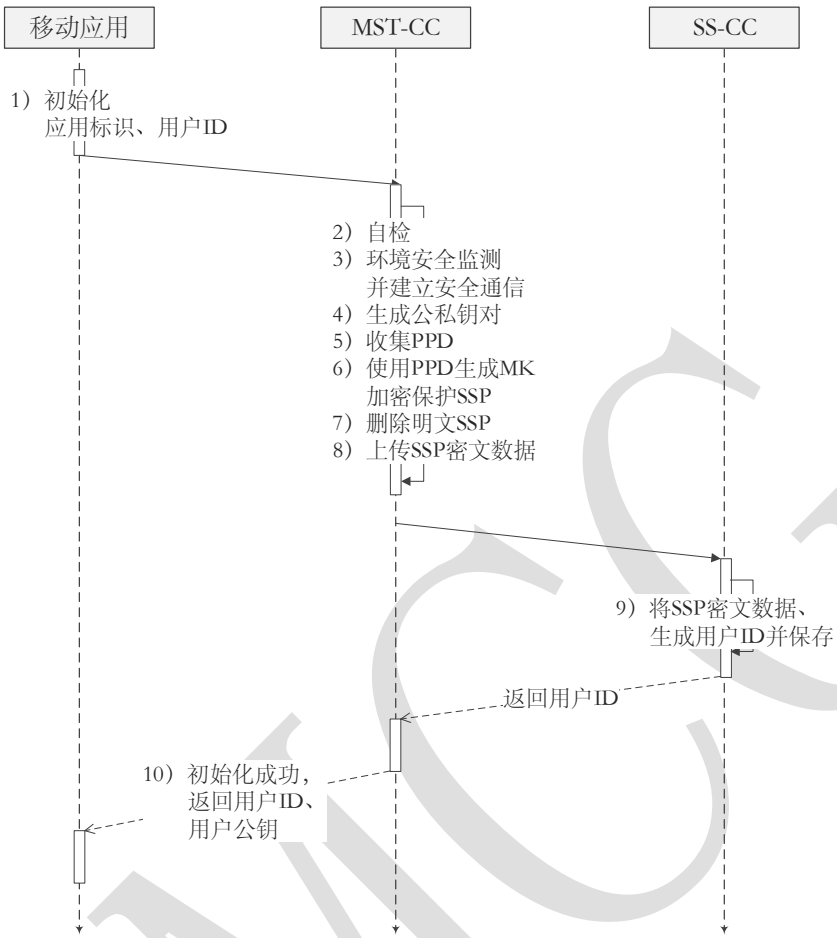

图3 CMMST-KEPOSS初始化流程

7.2 数字签名流程

数字签名流程如图4所示：

1) 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；
2) MST-CC 收集 PDD，如 PIN 码、手势码、指纹、人脸等；
3) MST-CC 向 SS-CC 发送用户 ID 请求私钥密文数据；
4) SS-CC 通过用户 ID 找出用户私钥密文，发送给 MST-CC；
5) MST-CC 使用 PDD 生成 MK 解密用户私钥密文，获得用户私钥；
6) MST-CC 使用用户私钥对待签数据进行签名；
7) MST-CC 删除用户私钥；
8) 移动应用获得签名数据，签名完成。

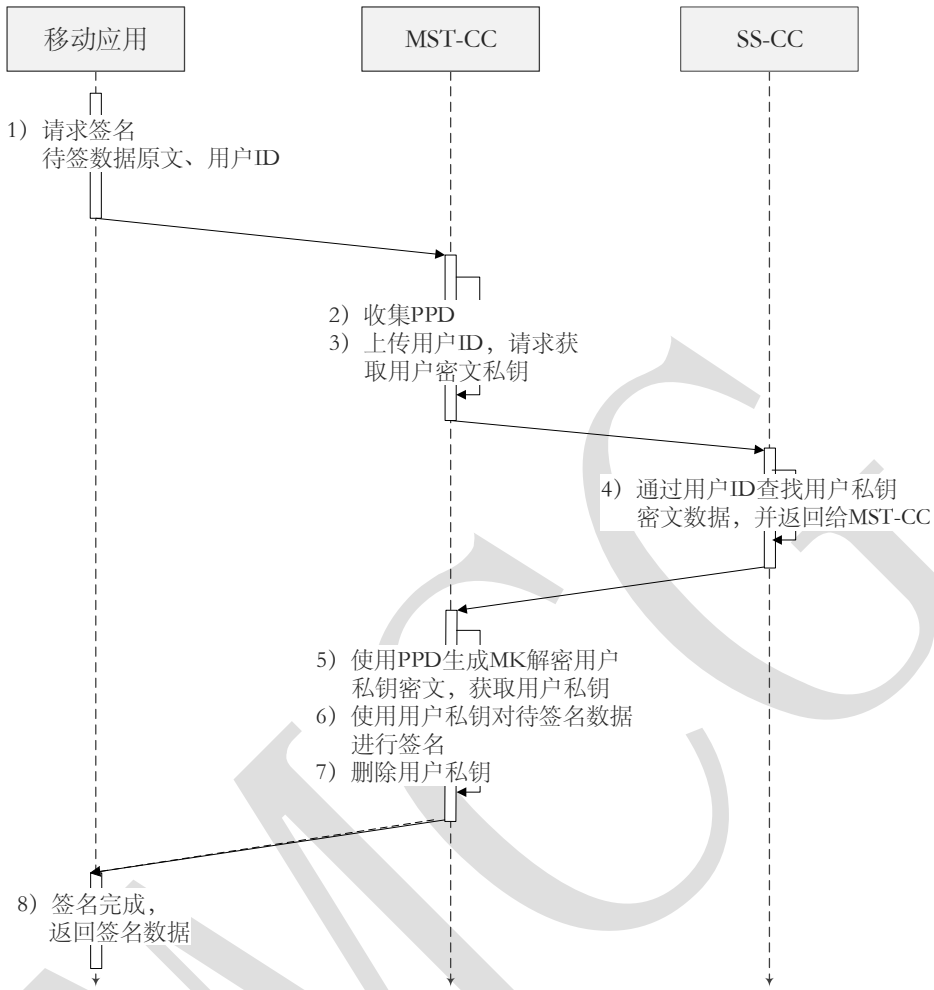

图4 CMMST-KEPOSS数字签名流程

7.3 签名验签流程

数字签名验签流程如图5所示：

1) 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；
2) MST-CC 对待验签数据进行验签；
3) MST-CC 向移动应用返回验签结果。

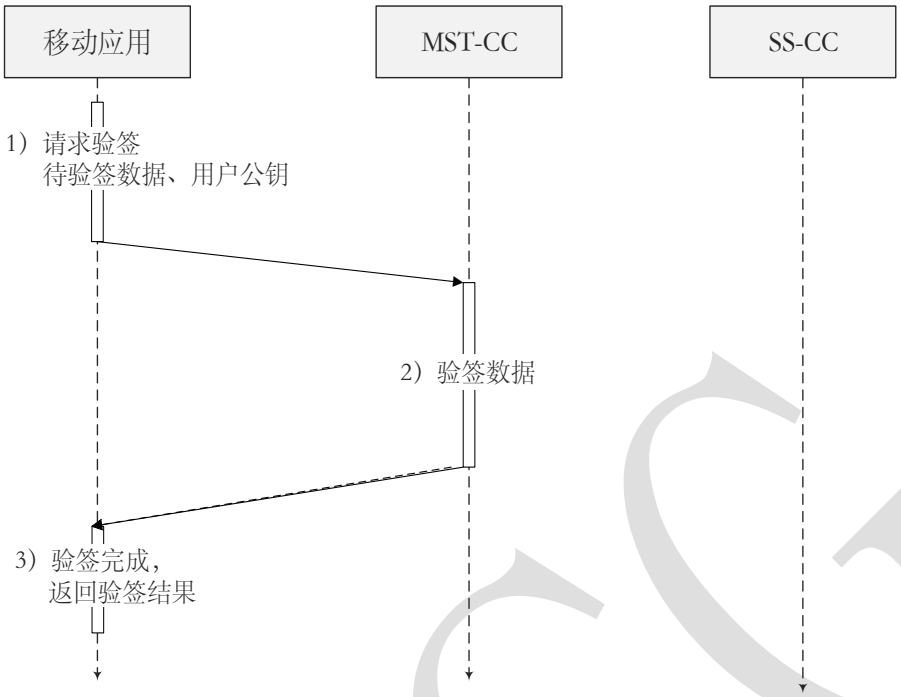

图5 CMMST-KEPOSS数字签名验签流程

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

（1）MST-CC 自检时进行 MST-CC 完整性校验。

（2）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。

（1）安全一级

遵照GM/T 0028-2014 7.6.3中对应的安全一级要求。

（2）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。

（1） 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。

（2） 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。

（3） 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。

（1） 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。

（2） 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。

（3） 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。

（1） d_M和P_M由MST-CC内部自动生成。

（2） 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。

（3） 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：

（1） d_M以加密的形式输入给通信模块。

（2） 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。

（1） 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。

（2） P_M存储在移动应用中，只有验证用户PPD后才可使用。

（3） 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。

（4） SS-CC不以明文形式存储d_M。

（5） 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：

（1） 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。
（2） 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。
（3） 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。
（4） 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。
（5） 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。
（6） MST-CC 须支持初始化密码模块以允许绑定用户。
（7） 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。
（8） 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。
（9） MST-CC 须支持注销以销毁内存中的 SSP。
（10）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：

（1） 出厂状态：CMMST-KEPOSS集成（安装）后尚未使用时所处状态。
（2） 自测试状态：CMMST-KEPOSS正在执行自测试时所处的状态。
（3） 初始化状态：CMMST-KEPOSS密码模块初始运行后进入“初始化状态”。
（4） 用户状态：当移动应用使用CMMST-KEPOSS进行核准的密码服务时所处的状态。
（5） 核准的状态。CMMST-KEPOSS正在执行核准的密码功能时所处的状态，当密码服务完成后退出此状态，转到用户状态。

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

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

（8） 错误状态。当密码模块遇到错误状况时转到此状态。

CMMST-KEPOSS有限状模型如图6所示：

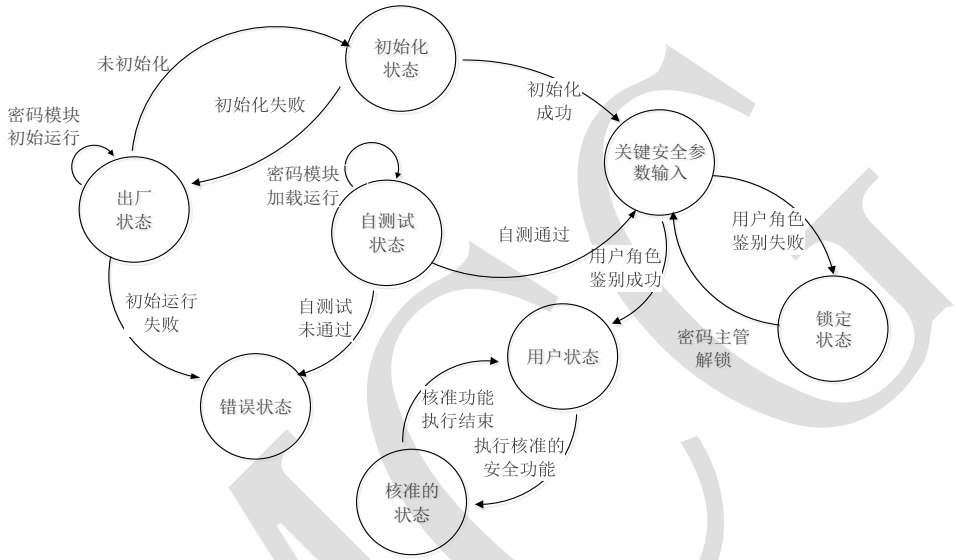

图6 CMMST-KEPOSS有限状态模型图

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：

（1）安全一级

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

（2）安全二级

满足GM/T 0028-2014 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。

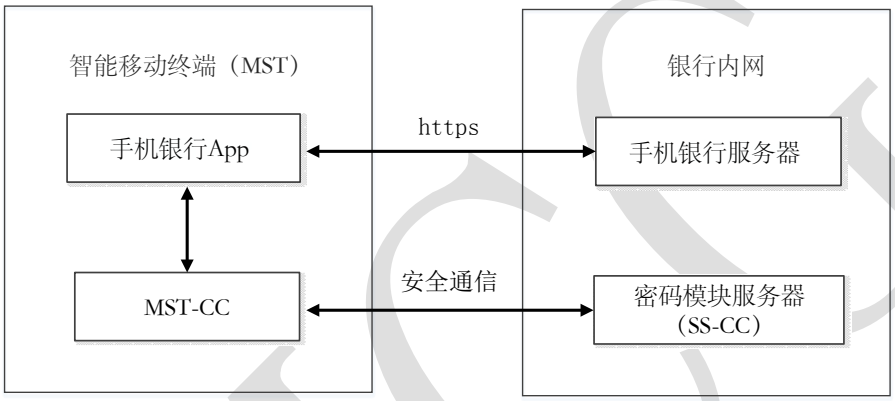

图7 基于CMMST-KEPOSS实现手机银行转账汇款的技术架构

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：

1）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）；

2）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）；

3）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。

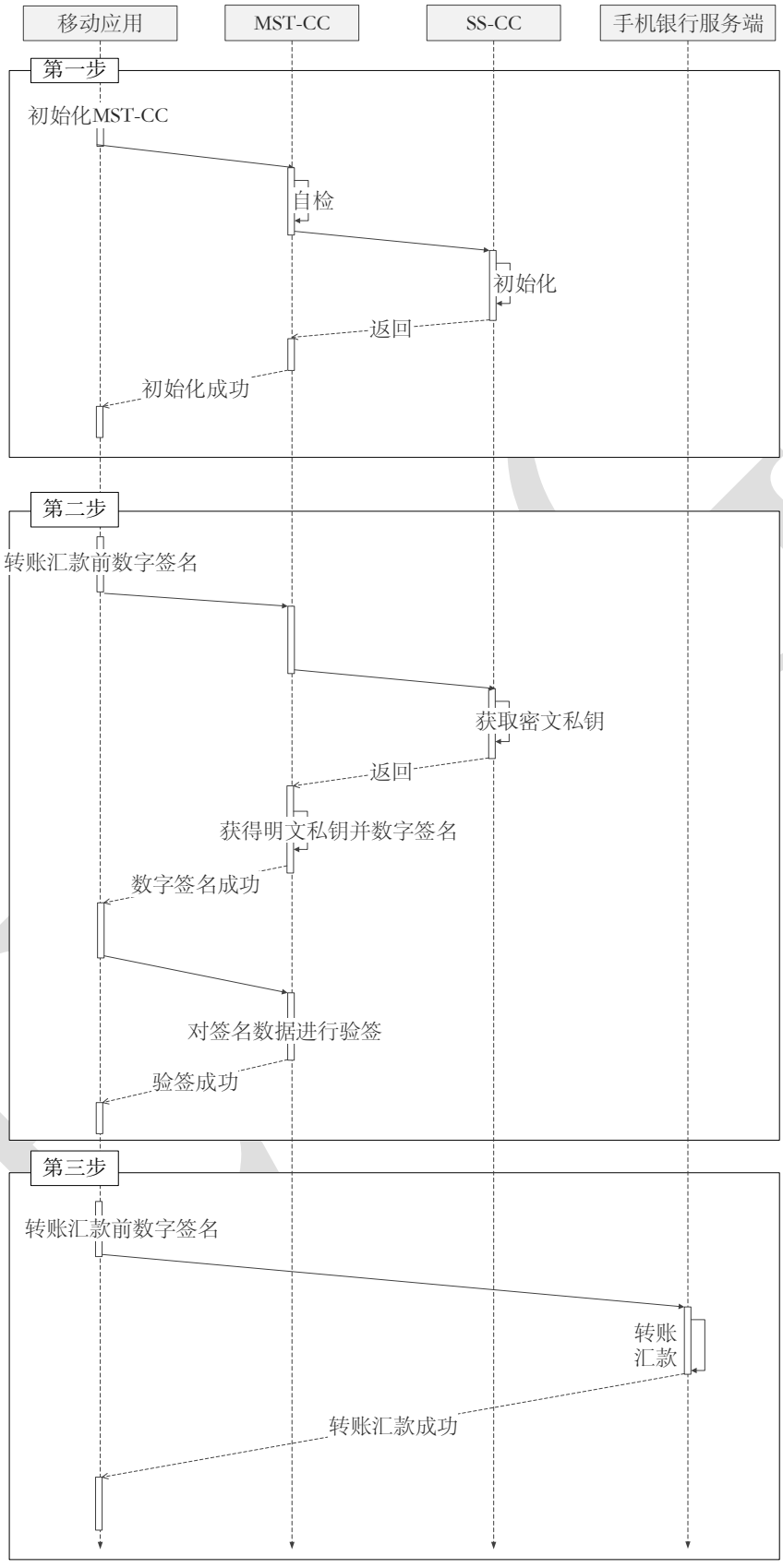

图8 基于CMMST-KEPOSS技术架构手机银行转账汇款业务流程

参考文献

[1] GM/T 0029-2014 签名验签服务器技术规范