团　　体　　标　　准

T/EMCG 001.5-2019

移动智能终端密码模块技术框架
第 5 部分：基于安全芯片的技术架构

Technical framework of cryptographic module in mobile smart terminal
Part 5: Based on security chip

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5部分。

本部分由中关村网络安全与信息化产业联盟企业移动计算工作组（EMCG）提出。

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

本部分主要起草单位：中关村网络安全与信息化产业联盟企业移动计算工作组（EMCG）、北京握奇数据股份有限公司、鼎桥通信技术有限公司、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、江苏通付盾科技有限公司、北京江南天安科技有限公司等。

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

引　言

在开放移动网络和便携移动终端系统环境中，对于安全性要求较高的机构（如政府、军队），需要在移动智能终端上使用高安全等级的密码模块，以保护其在移动网络环境下的信息安全。传统硬件密码模块技术在移动智能终端中应用仍具有重要意义。如何在移动智能终端中安全、有效使用硬件密码模块需要建立相应的产业标准，以促进国家密码技术产业发展。

移动智能终端密码模块技术框架
第5部分：基于安全芯片的技术架构

1 范围

T/EMCG 001-2019《移动智能终端密码模块技术框架》的本部分规范了移动智能终端（mobile smart terminal；MST）使用的基于安全芯片的移动智能终端密码模块（CMMST-BSC）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GM/T 0028-2014中规定的11个安全域描述。

本规范适用于指导密码模块生产厂家设计、实现移动智能终端密码模块，也可作为使用移动智能终端密码模块的参考。

2 规范性引用文件

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

GM/T 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 0016-2012 智能密码钥匙密码应用接口规范

GM/T 0017-2012 智能密码钥匙密码应用接口数据格式规范

GM/T 0028-2014 密码模块安全技术要求

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

3 术语和定义

3.1

核准的安全功能 approved security function

GM/T 0028-2014《密码模块安全技术要求》中附录C中给出的安全功能，如密码算法。

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

密码模块 cryptographic module

实现了安全功能的硬件、软件和/或固件的集合，并且被包含在密码边界内。

[GM/T 0028-2014，定义3.18]

注：本标准中的密码模块均指GM/T 0028-2014所规范的密码模块。

3.4

移动智能终端密码组件 mobile smart terminal cryptography component；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。本标准中包括可信应用、安全芯片、密码模块物理保护等组件。

3.5

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。

[GM/T 0028-2014，定义3.73]

3.6

安全芯片 security chip

含有密码算法、安全功能，可实现密钥管理机制的集成电路芯片。

[GM/T 0008-2012，定义3.1.3]

3.7

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]

3.8

可信应用 trusted application；TA

运行在TEE环境中的应用程序。

3.9

可信执行环境 trusted execution environment；TEE

可信执行环境是驻留在移动智能终端的主处理器上的安全区域，提供与设备上的通用操作系统(例如Android）并存的运行环境，并且向通用操作系统提供例如敏感数据的安全存储、核准的安全功能、可信用户界面等安全服务。

3.10

可信用户界面 trusted user interface；TUI

TEE的组成部分，能够独占访问移动智能终端的显示、输入设备，在可信环境下使用图形界面方式与用户交互敏感信息或敏感操作，保护用户的敏感信息不被泄露、敏感操作不被劫持。

4 符号和缩略语

下列符号和缩略语适用于本文件。

CC	密码组件（cryptography component）
CMMST	移动智能终端密码模块（cryptographic module of mobile smart terminal）
CMMST-BSC	基于安全芯片的移动智能终端密码模块(CMMST based on security chip)
FPC	柔性电路板（flexible printed circuit）
MST-CC SDK	移动智能终端密码组件客户端软件开发套件
PCB	印刷线路板（printed circuit board）
PIN	个人身份标识码（personal identification number）
PPCCC	密码模块物理保护组件（physical protect components of cryptography component）
SDK	软件开发套件（software development kit）

5 概述

基于安全芯片的移动智能终端密码模块（CMMST base on security chip；CMMST-BSC）技术框架，是为移动智能终端（MST）提供较高安全级别密码模块而设计。CMMST-BSC采用移动端安全模型以保护CMMST敏感安全参数。为满足GM/T 0028安全二级要求，使用CMMST-BSC方案的MST应配置安全芯片及可信执行环境（trusted execution environment；TEE）；为满足GM/T 0028安全三级要求，使用CMMST-BSC方案的MST还应配置密码模块物理保护组件（physical protect components of cryptography component；PPCCC），宜配置生物识别组件。

CMMST-BSC使用的安全芯片应满足GM/T 0008—2012《安全芯片密码检测要求》中安全等级二级以上要求。安全芯片在其物理安全边界内加密存储密码模块关键安全参数（CSP），在受控安全机制下执行核准的安全功能；TEE OS提供访问安全芯片的可信信道，用于密码模块操作员输入CSP（如PIN码）；PPCCC对安全芯片内CSP实施保护，防止CMMST-BSC被非法物理入侵导致CSP泄露；生物识别组件用于采集和处理用户的生物特征数据。CMMST-BSC技术框架采取以下安全措施以实现T/EMCG 001.1-2019《移动智能终端密码模块技术框架 第一部分：总则》提出的安全目标，满足GM/T 0028-2014《密码模块安全技术要求》中安全二级或安全三级的要求。

（1）密码模块关键安全参数防护。在具有物理保护措施的安全芯片中加密存储 CSP。

（2）密码算法执行环境防护。在具有物理保护措施的安全芯片中执行核准的安全功能。

（3）生物特征数据防护。在具有物理保护措施的安全芯片中加密存储生物特征数据，在安全芯片中执行生物特征比对和校验。

（4）密码模块可信信道防护。利用 TEE 的可信用户界面（TUI）功能，在 MST 上提供密码模块人机交互可信信道，保护操作员在 TUI 界面中输入 CSP 的完整性和机密性，保护 TUI 界面中显示输出信息的完整性和机密性。

（5）密码模块访问控制防护。至少包括：安全芯片对操作员进行基于角色或身份的鉴别、安全芯片仅接受从 TEE 环境发起的会话连接、TEE 环境校验 TA 程序的完整性与真实性、TA 验证外部访问者的合法性。

（6）密码模块物理保护。PPCCC 通过在 MST 中部署拆卸检测装置及置零电路，在检测到 MST 受到物理入侵时触发置零信号，将安全芯片内所有 CSP 置零。

6 技术架构

CMMST-BSC技术框架由MST-CC SDK、密码功能TA、安全芯片以及密码模块物理保护组件构成。MST-CC SDK由移动应用调用，将密码功能请求发送给密码功能TA；密码功能TA提供TUI功能，保护操作员输入的CSP与屏幕输出的敏感信息的完整性和机密性；密码功能TA与安全芯片建立会话连接，由安全芯片执行核准的安全功能、保护密码模块CSP。PPCCC对安全芯片内CSP实施保护，防止CMMST-BSC被非法物理入侵导致CSP泄露。

CMMST-BSC技术框架如图1所示。

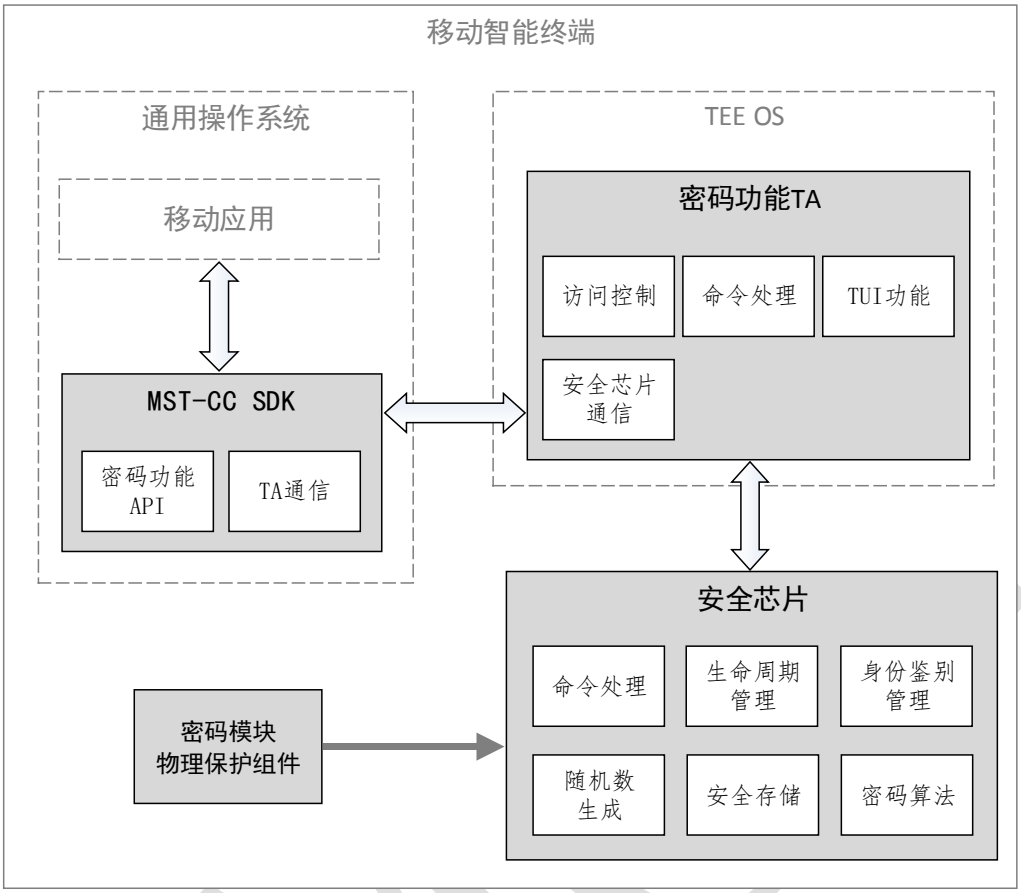

图1 CMMST-BSC技术架构

6.1 MST-CC SDK

MST-CC SDK通过密码功能API接口向移动应用提供核准的安全功能，如生成随机数、生成密钥、数据加密、数据签名等。MST-CC SDK至少包含完成以下功能的模块：

（1）密码功能 API。移动应用通过调用密码功能 API 接口请求密码服务功能。

（2）TA 通信。负责向 TEE 环境请求加载运行 TA 程序，与 TA 程序建立安全会话通道，与 TA 程序进行指令与数据通信。

6.2 密码功能 TA

密码功能TA是运行在TEE可信执行环境中的密码功能可信应用程序。TEE为密码功能TA提供安全执行环境，保护TA完整性，对不同TA的运行资源和存储数据提供隔离机制。密码功能TA至少包含完成以下功能的模块：

（1）访问控制。密码功能 TA 被加载运行时，应先检查发起连接的 App 的合法性，例如检查 App 包名、App 签名等信息，与预先登记的 App 信息进行比对，如果不一致应告警并拒绝提供服务。

（2）命令处理。密码功能 TA 接收来自 MST-CC SDK 的命令请求，执行核准的安全功能后向 MST-CC SDK 返回响应数据。

（3）TUI 功能。密码功能 TA 通过调用 TEE 的 TUI 接口实现可信用户界面功能。TUI 可独占访问移动智能终端的显示、输入设备，在可信环境下与用户交互敏感信息和敏感操作，

防止用户敏感信息被泄露、敏感操作被劫持。

（4）安全芯片通信。密码功能 TA 通过调用 TEE 的安全芯片通讯接口与安全芯片建立会话连接，操作安全芯片执行核准的安全功能。

6.3 安全芯片

本部分采用的MST安全芯片嵌入在MST中，负责敏感安全参数的生成和安全存储、以及执行核准的安全功能。安全芯片符合GM/T 0008—2012《安全芯片密码检测准则》安全等级二级以上的技术要求。

MST安全芯片至少包含完成以下功能的模块：

（1）命令处理。负责接收来自密码功能 TA 的指令与数据，执行核准的安全功能后向密码功能 TA 返回响应数据。

（2）生命周期管理。负责安全芯片生命周期管理。

（3）身份鉴别管理。负责登记、存储和校验密码模块操作员的鉴别信息。安全芯片具有基于角色或基于身份的鉴别功能，例如利用 PIN、生物特征信息等方法对操作员身份进行鉴别。

（4）随机数生成。应具有多个相互独立的物理随机源，生成的随机数应能满足 GM/T 0005 规定的随机性检测要求。

（5）安全存储。负责加密存储密码模块敏感安全参数。

（6）密码算法。负责执行核准的安全功能。

6.4 密码模块物理保护组件

PPCCC通过在MST中部署拆卸检测装置及置零电路，在检测到MST受到物理入侵时触发置零信号，将安全芯片内所有CSP置零，防止安全芯片被非法物理介入导致CSP泄露。

拆卸检测装置安装在MST的物理结构上（如外壳、PCB板、FPC板、IC卡座、焊盘等），如防拆开关、防拆触点、防拆导线、距离传感器、光线传感器、温度传感器等。拆卸检测装置与安全芯片的置零信号引脚连接，当发生外壳与PCB板分离、结构件位移、光线温度环境变化等情况时，拆卸检测装置触发置零信号，安全芯片对内部存储的所有CSP执行置零操作。

7 主要工作流程示例

7.1 SM2 公私钥对生成流程

CMMST-BSC技术框架生成核准的密码算法SM2公私钥对流程如图2所示。

1) 移动应用通过 MST-CC SDK 向密码功能 TA 发起生成密钥对请求；
2) 可选的，密码功能 TA 生成 TUI 页面，要求用户确认授权当前操作；
3) 密码功能 TA 向安全芯片发送生成密钥对指令；
4) 安全芯片负责生成 SM2 密钥对并加密存储密钥对数据；
5) 安全芯片向密码功能 TA 返回公钥数据；
6) 密码功能 TA 向 MST-CC SDK 返回公钥数据。

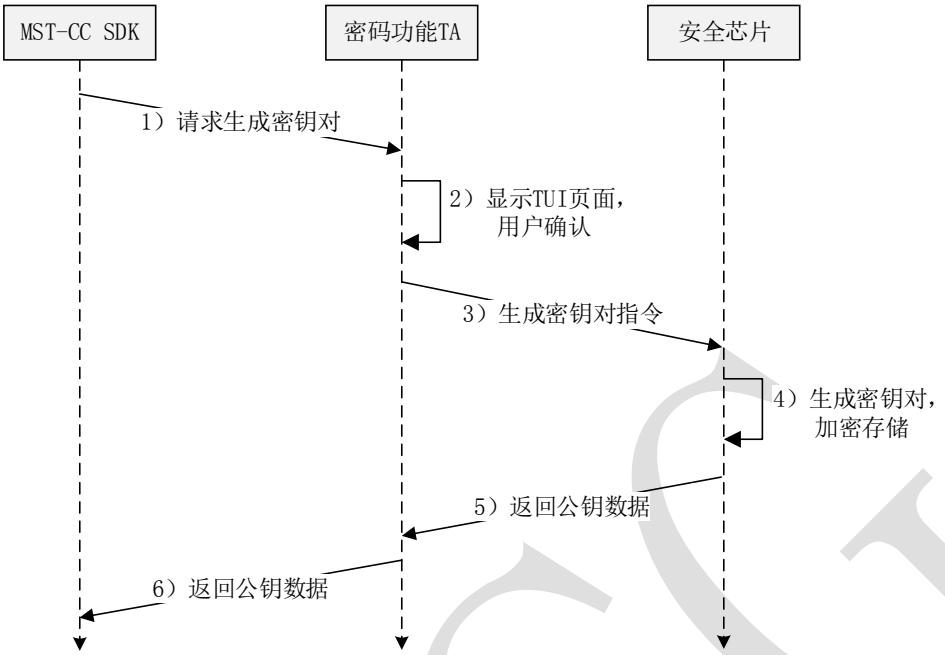

图2 CMMST-BSC技术架构的SM2公私钥对生成流程

7.2 数字签名流程

CMMST-BSC技术框架数字签名流程如图3所示。

1) 移动应用通过 MST-CC SDK 向密码功能 TA 发起签名请求，包括密钥标识、待签名数据等信息；
2) 可选的，密码功能 TA 生成 TUI 页面，请求用户复核待签名信息、确认授权执行签名功能；
3) 密码功能 TA 在 TUI 页面中请求用户输入 PIN 码或指纹等生物特征；
4) 密码功能 TA 向安全芯片发送用户鉴别指令；
5) 安全芯片负责验证用户的鉴别信息，并返回验证结果；
6) 如果鉴别成功，密码功能 TA 向安全芯片发送签名指令；
7) 安全芯片负责用指定的私钥对待签名数据进行签名，返回签名结果；
8) 密码功能 TA 向 MST-CC SDK 返回签名结果。

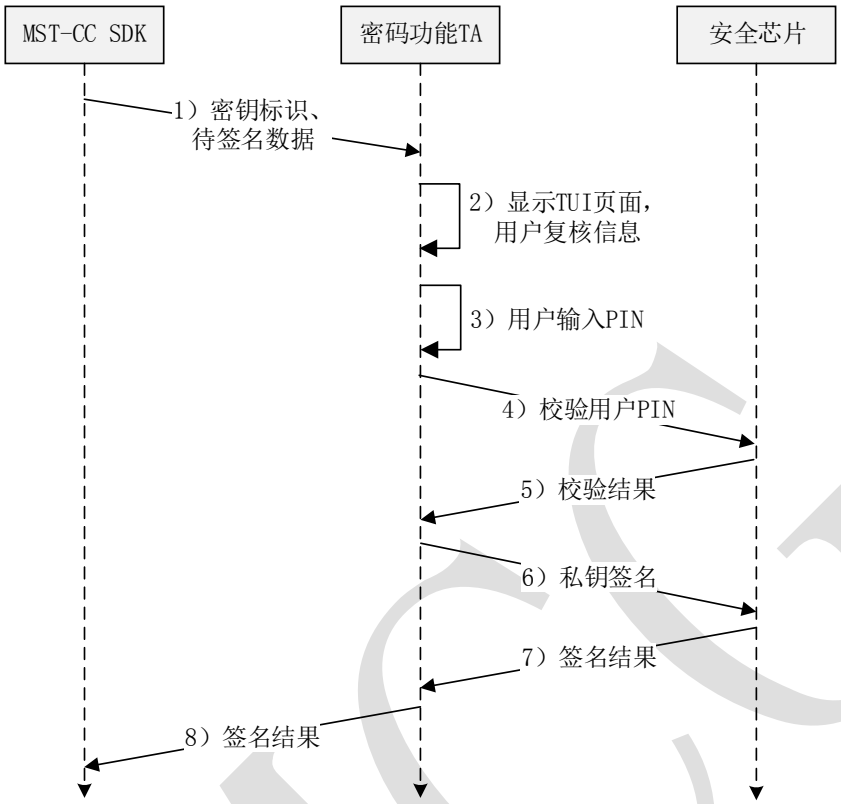

图3 CMMST-BSC技术架构的数字签名流程

7.3 数据加密流程

CMMST-BSC技术框架加密流程如图4所示。

1) 移动应用通过 MST-CC SDK 向密码功能 TA 发起生成加密密钥请求；
2) 密码功能 TA 向安全芯片发送生成加密密钥指令；
3) 安全芯片负责生成加密密钥，并返回密钥标识；
4) 密码功能 TA 向 MST-CC SDK 返回密钥标识；
5) 移动应用通过 MST-CC SDK 向密码功能 TA 发起数据加密请求，包括加密密钥标识、待加密的明文数据等信息；
6) 密码功能 TA 向安全芯片发送数据加密指令；
7) 安全芯片负责用加密密钥对明文数据进行加密，并返回密文数据；
8) 密码功能 TA 向 MST-CC SDK 返回密文数据。

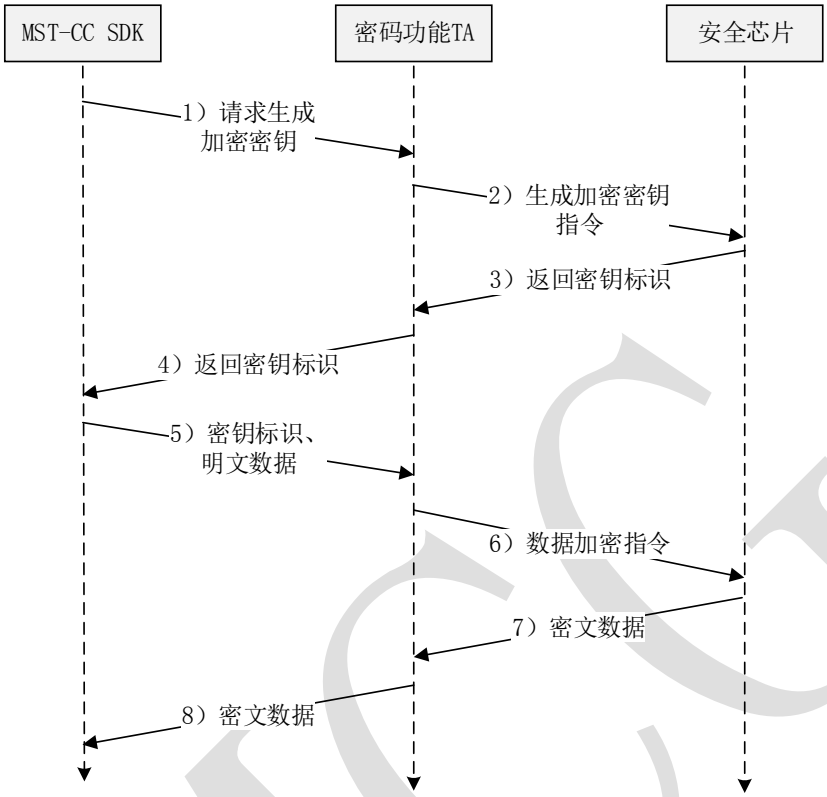

图4 CMMST-BSC技术架构的数据加密流程

8 密码模块规格

8.1 密码模块类型

遵照GM/T 0028—2014，CMMST-BSC技术框架定义的密码模块为一种混合软件模块，使用核准的SM2，SM3，SM4算法，实现分组密码、非对称密码、杂凑函数、实体鉴别、密钥管理和随机数生成器等核准的安全功能。

8.2 密码边界

对于安全二级，CMMST-BSC技术框架定义的密码模块边界包括：

（1）密码功能 TA。

（2）安全芯片。

对于安全三级，CMMST-BSC技术框架定义的密码模块边界还包括密码模块物理保护组件（PPCCC）。

CMMST-BSC技术框架定义的密码模块边界中各组件关系如图5所示：

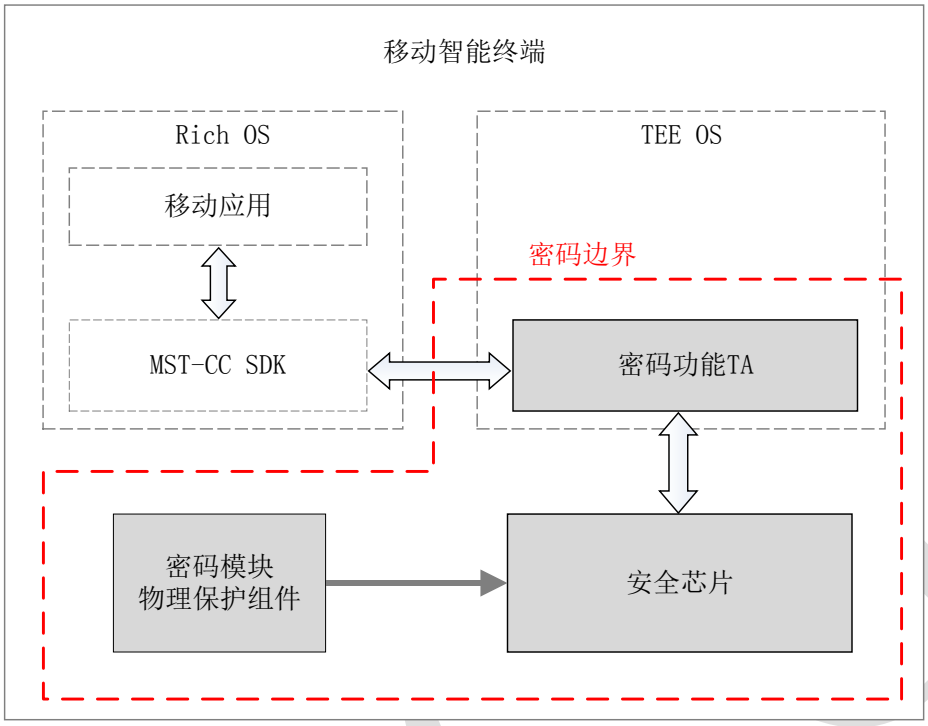

图5 CMMST-BSC技术架构的密码边界示意图

8.3 工作模式

遵照GM/T 0028—2014中7.2.4条款要求。

9 密码模块接口

9.1 接口类型

遵照GM/T 0028—2014，CMMST-BSC技术框架定义的密码模块接口，是由密码功能TA提供的逻辑接口实现的混合软件模块接口（HSMI）。

9.2 接口定义

CMMST-BSC技术框架定义的密码模块接口应遵照GM/T 0017—2012《智能密码钥匙密码应用接口数据格式规范》中对密码应用接口数据格式的要求。

9.3 可信信道

遵照GM/T 0028—2014中7.3.4条款要求，对于安全二级：

（1）安全芯片应仅接受来自 TEE 环境发起的会话连接，拒绝除 TEE 环境之外的其他软、硬件模块发起的会话连接。

（2）操作员需要向密码模块输入未受保护的明文 CSP、密钥分量以及鉴别数据时，应启用 TEE 的 TUI 功能，在 TEE 环境的保护下进行 CSP 输入或实体鉴别。

（3）密码模块需要向操作员输出 CSP 或鉴别数据时，应启用 TEE 的 TUI 功能，在 TEE 环境的保护下进行 CSP 输出。

（4）TEE 的 TUI 功能在启用时，应提供 TUI 功能状态指示器。

对于安全三级，除安全二级的要求外，还应：

（1）TA 与安全芯片之间的指令与数据通信使用加密算法保护，防止在通信链路上非授权的修改、替换和泄露。

（2）安全芯片使用的物理端口应与其他物理端口实现物理隔离。

（3）应采取有效手段保护 TUI 功能状态指示器的输出不被仿冒或篡改。

（4）使用生物识别技术等基于身份的鉴别手段应用于所有使用可信信道的服务。

10 角色、服务和鉴别

10.1角色

遵照GM/T 0028—2014中7.4.2条款要求，CMMST-BSC技术框架的密码模块应支持密码主管角色和用户角色。

密码主管角色与用户角色的责任与分工应遵照GM/T 0017—2012中的规定。

10.2服务

遵照GM/T 0028—2014中7.4.3条款要求,其中，

CMMST-BSC技术框架的密码模块可不具备旁路能力。

对于安全三级：

（1）应提供基于身份的鉴别服务功能，例如采用生物识别的身份鉴别技术。

（2）密码模块为操作员提供显示模块版本号、显示状态等服务时，应利用 TEE 环境保护状态指示器的输出，例如使用 TUI 功能显示模块版本号、状态等信息。

10.3鉴别

遵照GM/T 0017—2012中7.4.4条款要求,

对于安全二级：

规定的设备认证密钥鉴别机制与用户PIN鉴别机制，分别对密码主管角色与用户角色进行基于角色的鉴别。

对于安全三级：

应实现对担任用户角色的操作员进行基于身份的鉴别。

11 软件/固件安全

遵照GM/T 0028—2014中7.5条款要求,

——密码模块边界中的软件组件包括密码功能TA。

——密码功能TA应具有TEE平台发行方的数字签名，TEE环境加载密码功能TA时应核验签名，保证加载的TA镜像的完整性。

12 运行环境要求

遵照GM/T 0028—2014中7.6条款对安全二级、安全三级的要求，其中：

（1）密码功能 TA 处于受限制的运行环境，MST 使用的 TEE OS 应是经过认证的。

（2）安全芯片是不可修改的运行环境。

13 物理安全

遵照GM/T 0028—2014中7.7条款对安全二级、安全三级的要求。

CMMST-BSC技术框架中的安全芯片部件应符合GM/T 0028—2014中7.7.1对单芯片密码模块的安全要求。

对于安全三级：

（1） 安全芯片部件应具有GM/T 0028－2014中7.7.4.2提到的环境失效保护特性或经过GM/T 0028－2014中7.7.4.3提到的环境失效测试。

（2） MST中应配置密码模块物理保护组件（PPCCC）。PPCCC在MST中部署拆卸检测装置及置零电路，拆卸检测装置安装在MST的物理结构上（如外壳、PCB板、FPC板、IC卡座、焊盘等），如防拆开关、防拆触点、防拆导线、距离传感器、光线传感器、温度传感器等。当发生外壳与PCB板分离、结构件位移、光线温度环境变化等情况时，拆卸检测装置触发置零信号，安全芯片对内部存储的所有CSP执行置零操作，防止安全芯片被非法物理介入导致CSP泄露。

（3） PPCCC应具有2条以上置零信号回路以避免因拆卸检测装置被破坏导致置零电路失效。

14 非入侵式安全

遵照GM/T 0028－2014中7.8条款对安全二级、安全三级的要求。

15 敏感安全参数管理

CMMST-BSC技术框架中涉及的CSP至少包括：

安全芯片中的随机比特生成器的状态信息、密码主管角色和用户角色的PIN、与用户角色关联的非对称密钥对中的私钥、与用户角色关联的对称密钥等；

涉及的PSP至少包括：安全芯片唯一标识编号、与用户角色关联的非对称密钥对中的公钥、与用户角色关联的数字证书、TA访问控制配置信息及完整性校验数据等。

遵照GM/T 0028－2014中7.9.1条款要求，

（1） CMMST-BSC技术框架的密码模块应在安全芯片内部存储CSP。

（2） 采用基于角色或基于身份的鉴别机制管理密码模块中SSP的访问、使用和修改。

（3） 应为不同角色或身份的操作员指定相应的SSP操作权限，防止非授权操作员访问明文CSP，防止非授权操作员修改PSP。

（4） 应管理SSP与该SSP相应的操作员的角色或身份的关联关系，防止未经关联的操作员访问、使用、泄露、修改和替换SSP。

15.1随机比特生成器

遵照GM/T 0028—2014中7.9.2条款要求，

安全芯片中应包含满足国家密码管理主管部门相关要求的随机比特生成器。如果核准的安全功能、敏感安全参数生成或敏感安全参数建立方法需要随机值，则安全芯片中的随机比特生成器应当用于提供这些值。

15.2敏感安全参数的生成

遵照GM/T 0028—2014中7.9.3条款要求，其中：

（1） 签名私钥应在安全芯片内部生成，在整个生命周期中不应导出到安全芯片外部。

（2） 角色或身份的鉴别信息应存储在安全芯片内部，在安全芯片内部执行鉴别功能。

15.3敏感安全参数的建立

遵照GM/T 0028—2014中7.9.4条款要求。

15.4敏感安全参数的输入和输出

遵照GM/T 0028－2014中7.9.5条款要求，其中：

（1） 应利用TUI功能接口实现GM/T 0028－2014 7.3.2中规定的软件模块接口，作为人机交互可信信道，保护操作员在TUI界面中输入信息的完整性和机密性；保护TUI界面中显示输出信息的完整性和机密性。

（2） 设置PIN、修改PIN、校验PIN等功能应通过TUI功能接口保护操作员输入的鉴别信息。

15.5敏感安全参数的存储

遵照GM/T 0028－2014中7.9.6条款要求，

（1） 应将SSP的存储与该SSP相应的操作员的角色或身份关联起来，例如利用操作员的鉴别信息作为密钥对SSP加密后存储。

（2） 应采用基于角色或基于身份的鉴别机制管理密码模块中SSP的访问、使用和修改。

（3） 应为不同角色或身份的操作员指定相应的SSP操作权限，应禁止非授权操作员访问明文CSP，应禁止非授权操作员修改PSP。

15.6敏感安全参数的置零

遵照GM/T 0028－2014中7.9.7条款对安全二级、安全三级的要求。

16 自测试

遵照GM/T 0028－2014中7.10条款要求，

（1） CMMST-BSC技术框架的密码模块的自测试涉及密码功能TA的自测试和安全芯片的自测试。

（2） 密码功能TA在被TEE环境加载后执行运行前自测试，如果自测试失败，密码功能TA加载失败，停止提供密码功能服务。

（3） 安全芯片在模块上电后执行运行前自测试，如果自测试失败，安全芯片上电失败，停止提供密码功能服务。

（4） 安全芯片在执行核准的密码功能前执行条件自测试，如果自测试失败，停止提供核准的密码功能服务。

17 生命周期保障

17.1配置管理

遵照GM/T 0028－2014中7.11.2条款对安全二级、安全三级的要求。

17.2设计

遵照GM/T 0028－2014中7.11.3条款要求。

17.3有限状态模型（FSM）

遵照GM/T 0028－2014中7.11.4条款要求。

CMMST-BSC的有限状态模型如图6所示：

——电源开启状态：密码模块接通电源启动运行。

——自测试状态：密码模块正在执行自测试时所处的状态。

——初始化状态：密码模块执行初始化所处的状态。

——密码主管状态：执行密码主管服务所处的状态。

——用户状态：授权用户获得安全服务、执行密码操作或执行其他核准的功能所处的状态。

——关键安全参数输入状态：将CSP输入至密码模块时所处的状态。

——核准的状态：执行核准的密码功能时所处的状态。

——错误状态：当密码模块遇到错误状况时所处的状态。

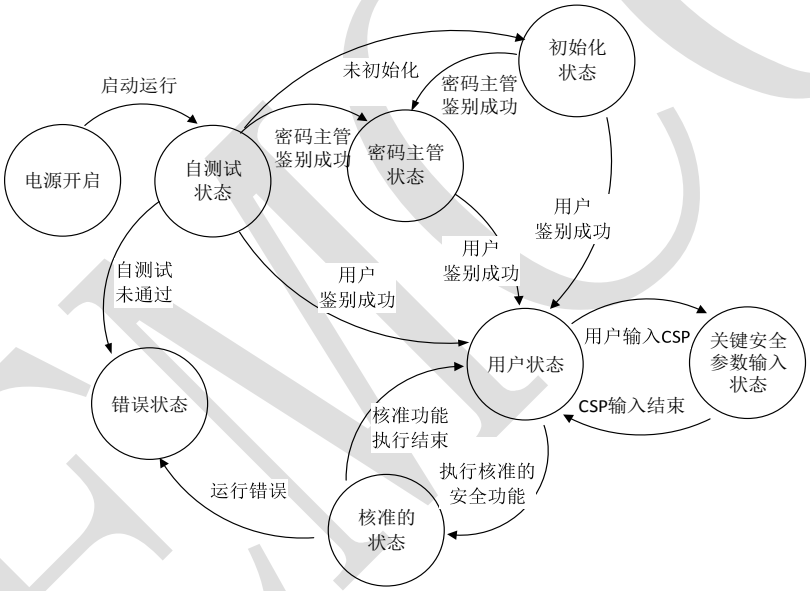

图6 CMMST-BSC有限状态模型图

17.4开发

遵照GM/T 0028－2014中7.11.5条款对安全二级、安全三级的要求。

17.5厂商测试

遵照GM/T 0028－2014中7.11.6条款对安全二级、安全三级的要求。

17.6配送与操作

遵照GM/T 0028－2014中7.11.7条款对安全二级、安全三级的要求。

CMMST-BSC采取以下措施进行配送：

（1） 如果在生产环境初始化安全芯片，由生产商担任密码主管角色，在MST出厂前完成SSP下载与密码模块初始化。

（2） 如果支持出厂后初始化安全芯片，应采取加密等手段建立用于配送SSP和初始化数据的可信信道，由操作员担任密码主管角色完成SSP下载与密码模块初始化。

（3） 密码功能TA的可执行镜像应采取加密、数字签名等手段保证在配送过程中的完整性。

（4） 初始化密码模块应使用由安全芯片内部密钥建立的可信信道。

17.7生命终止

遵照GM/T 0028－2014中7.11.8条款对安全二级、安全三级的要求。

17.8指南文档

遵照GM/T 0028－2014中7.11.9条款要求。

18 对其他攻击的缓解

遵照GM/T 0028－2014中7.12条款要求。

附录 A
应用示例（移动警务系统密码应用）

本附录给出CMMST-BSC在移动警务行业中的应用示例。

A.1 应用需求

移动警务系统密码应用需求：

（1） 具备密钥和证书管理功能。

（2） 采用国产商用密码算法进行数据加解密，并符合 GM/T 0034 标准技术要求。

（3） 使用统一签发的根证书。

（4） 采用硬件密码模块（设备）对重要信息进行保护。

A.2 应用平台

移动警务业务密码应用场景包括证书管理和通信加密，需要硬件密码模块的提供密码安全服务。

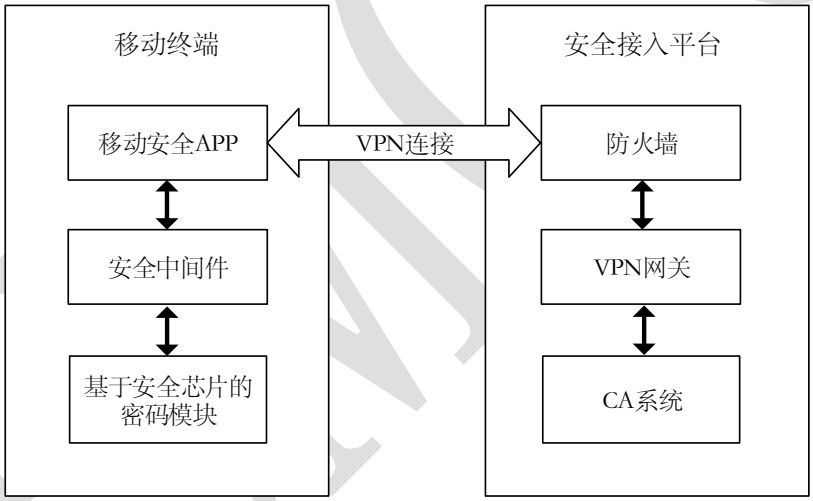

图7 基于CMMST-BSC技术架构的警务密码服务平台

A.3 密码模块应用

密码模块应用包括：

（1） 安全芯片实现 SM2/SM3/SM4 等密码算法和 GM/T0016-2012 智能密码钥匙应用接口规范。

（2） 警务密码 TA 实现警务 App 和安全芯片的通信接口，转发信令和数据。

（3） 警务密码 SDK 在 Android 下提供国密 API 接口及第三方 APK 使用的密码服务。

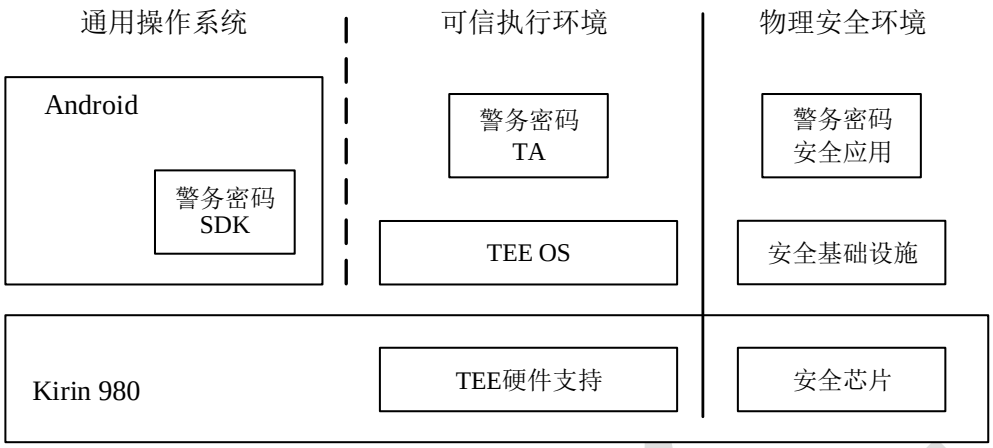

图 8 基于CMMST-BSC技术架构的警务加密应用方案框架

A.4 证书管理应用

证书管理应用流程如下：

（1） 警务密码 SDK 通过 TA 对安全芯片进行访问，要求生成签名密钥对（SM2/RSA）。

（2） 安全芯片生成签名密钥对（SM2/RSA），并对密钥进行安全存储，将公钥返回至警务密码 SDK。

（3） 警务密码 SDK 使用公钥生成证书申请请求，生成过程中将调用安全芯片，对请求使用签名私钥进行签名，安全芯片对请求信息使用签名私钥进行签名并返回签名值（签名过程，包含对信息进行 Hash 计算，算法为 SM3/SHA1）。

（4） 警务密码 SDK 将证书申请请求发送至平台的 CA 系统，从 CA 系统接收证书响应消息（消息包括签名证书、加密证书、经过签名公钥和临时对称密钥加密的加密密钥对）。

（5） 警务密码 SDK 解析证书响应消息，将签名证书、加密证书、密文加密密钥对下发至安全芯片。

（6） 安全芯片接受签名证书、加密证书、解密加密密钥对后安全存储。

A.5 通信加密应用

在通信加密中，首先需要使用安全芯片中的签名证书和签名密钥对实现身份认证，并使用加密证书和加密密钥对实现临时对称密钥的安全下发，此后移动终端可使用临时对称密钥进行通信数据的加解密等功能。其流程如下：

（1） 移动 VPN 客户端请求与平台建立 VPN 隧道，首先需要调用安全芯片，获取签名证书、加密证书，并使用签名私钥对消息进行签名。

（2） 移动 VPN 客户端对收到的消息，需要调用安全芯片验证消息的合法性。

（3） 移动 VPN 客户端接收到临时对称密钥下发消息时，需要调用安全芯片解密获得临时对称密钥，解密后的临时对称密钥不做永久存储，通信结束后销毁。

（4） 移动 VPN 客户端对发送的明文数据使用临时对称密钥进行加密。

（5） 移动 VPN 客户端对收到的密文数据使用临时对称密钥进行解密。