ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0156—2017

移动终端支付可信环境技术规范

Mobile terminal payment trusted environment specification

2017－12－11 发布　　2017－12－11 实施

中国人民银行　　发布

目　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由中国人民银行科技司提出。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准负责起草单位：中国人民银行科技司、中国金融电子化公司。

本标准参加起草单位：北京移动金融产业联盟、华为技术有限公司、中国人民银行广州分行、中国人民银行西安分行、中国银联、中国工商银行、中国农业银行、中国银行、中国建设银行、交通银行、支付宝（中国）网络技术有限公司、财付通支付科技有限公司、北京中金国盛认证有限公司、中金金融认证中心有限公司、银行卡检测中心、中钞信用卡产业发展有限公司、北京握奇数据股份有限公司、恒宝股份有限公司、展讯通信有限公司、北京中清怡和科技有限公司、北京小米科技有限责任公司、北京飞天诚信科技有限公司、北京豆荚科技有限公司。

本标准主要起草人：李伟、李兴锋、邬向阳、杨倩、聂丽琴、班廷伦、黄本涛、王禄禄、魏博锴、陈卫东、吴一兵、李承康、胡沐创、薛高、魏猛、胡达川、王小璞、常新苗、郭伟、谭颖、周思捷、吴永强、曾凯、安思宇、刘春彤、骆雄武、朱大磊、左爵希、何伟明、杜亮、辛业、辛知、叶轩、种衍雪、王兆国、付小康、张健、熊帅、王鑫、李欧、汪小八、郭丽娟、石玉平、赵李明、刘觅、刘航、常莹、金光日、刘立军、朱鹏飞、张志坚、韩鹏。

引　言

随着移动智能终端的普及和移动互联网快速发展，用户对移动金融接受程度和使用频率逐步提高，移动金融安全性如何得到有效保障成为有待解决的重要问题。推进移动终端支付可信环境相关标准制定有助于提升移动终端支付环境安全、推动金融与信息技术融合发展，对于行业健康持续发展及防范电信欺诈有着重要的指导意义。

移动终端支付可信环境技术规范

1 范围

本标准规定了移动终端支付领域可信环境的整体框架、可信执行环境、通信安全、数据安全、客户端支付应用等主要内容。

本标准适用于开展移动支付相关业务时对移动终端可信环境提出相关技术要求，也适用于移动终端支付可信环境的设计、开发、测试以及相关产品的评价等，智能POS终端可参照执行。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 32915 信息安全技术 二元序列随机性检测方法

JR/T 0089.2 中国金融移动支付 安全单元 第2部分：多应用管理规范

JR/T 0092 中国金融移动支付 客户端技术规范

JR/T 0098.3 中国金融移动支付 检测规范 第3部分：客户端软件

JR/T 0098.5 中国金融移动支付 检测规范 第5部分：安全单元（SE）嵌入式软件安全

3 术语和定义

下列术语和定义适用于本文件。

3.1

可信环境 trusted environment

个人移动终端上基于硬件和软件结合的安全技术，为移动支付相关业务提供的运行环境。

3.2

移动终端 mobile terminal

具有移动通讯能力的终端设备，通常指智能手机、平板电脑等。

3.3

回放保护分区（RPMB） replay protected memory block

一种可防回滚、防重放攻击的安全存储区，该区域除指定RPMB服务接口外不应通过其他方式访问。

3.4

可信OS trusted operating system

一个受可信硬件资源隔离保护的操作系统，该系统可为上层应用提供安全存储、加解密、生物特征识别等多种基础安全服务。

3.5

可信用户接口（TUI） trusted user interface

TEE为TA提供的与用户输入/输出设备安全交互的界面，保证TA与用户交互的敏感数据免受其他应用或恶意软件的攻击。

4 缩略语

下列缩略语适用于本文件。

eSE——嵌入式安全单元（embedded Secure Element）
inSE——内置安全单元（integrated Secure Element）
OTA——空中下载技术（Over-the-Air）
RBG——随机比特生成器（Random Bit Generator）
REE——富执行环境（Rich Execution Environment）
TA——可信应用（Trusted Application）
TEE——可信执行环境（Trusted Execution Environment）
TSM——可信服务管理（Trusted Service Management）
TUI——可信用户接口（Trusted User Interface）

5 移动终端支付可信环境概述

5.1 整体框架

移动终端支付可信环境框架如图1所示，一般包括REE、TEE与SE三部分应用运行环境，并共存于同一个终端上。根据终端提供的硬件隔离机制，分别为REE、TEE与SE提供各自所属的硬件资源，包括CPU、RAM、ROM、FLASH、总线接口与I/O控制器等，并基于所属硬件资源分别控制各自所属外部设备，如触摸屏幕、键盘、摄像头、NFC、指纹、虹膜设备等。移动终端支付可信环境检测要求见附录A、附录B。

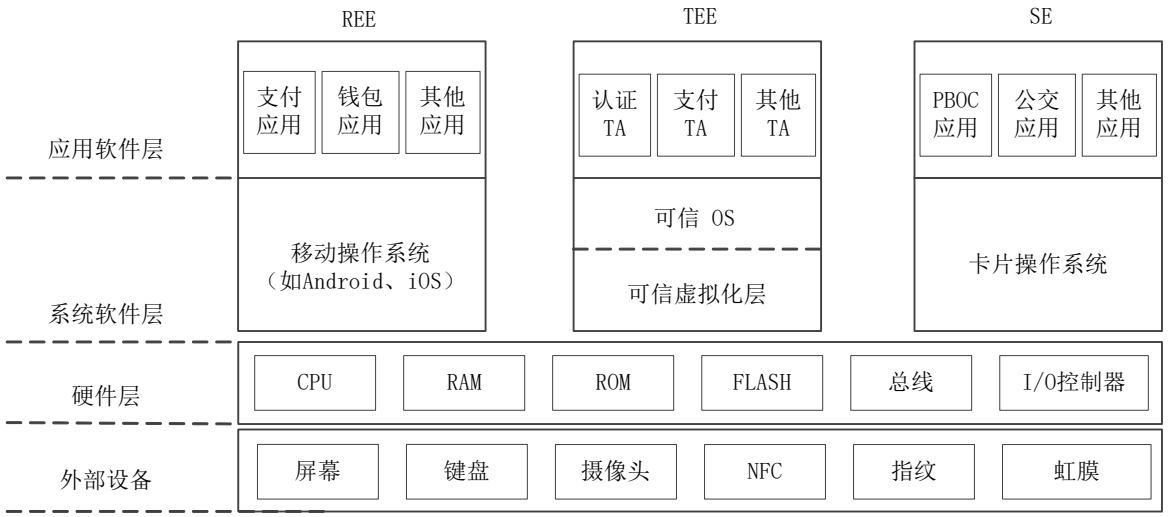

图1 移动终端支付可信环境框架示意图

通过业务使用场景不同，REE、TEE与SE在软件上各成相对独立的体系，从功能上，REE、TEE、SE逐级降低；从安全上，REE、TEE、SE逐级提高。通过REE、TEE、SE三者之间的可控相互访问机制，为移动终端支付提供功能与安全上的全方位服务体系。

5.2 REE

移动终端上直接面向用户提供支付、通信、娱乐、游戏、社交等各种各样功能的富执行环境，总体目标是以服务用户为主，注重便利、开放、功能强大的用户体验。其组成主要包括：

——应用软件层：包括各类应用，如手机银行、手机钱包等；

——系统软件层：移动操作系统，提供摄像头、FLASH、USB、触摸屏、蓝牙等相关驱动程序，并基于此向上提供一整套的系统服务、应用服务与管理框架，方便各种类型应用的开发与部署，其中对于支持 TEE 的终端，应提供访问 TEE 的通信驱动和 TEE 外部 API，支持其上运行的应用访问 TEE 应用。

5.3 TEE

与REE相隔离的安全区域，通过一组硬件和软件的组合，保证各种敏感数据在其中被安全传输、存储、处理，保证TA执行的机密性、完整性和数据访问权限端到端的安全。TEE的实现可以基于不同的技术，其组成主要包括：

——应用软件层：包括各种安全相关的可信应用，一般与对应 REE 应用相结合，为用户提供既便捷又安全的用户体验，可信应用以机构部署为主，如指纹、支付、身份认证等应用；

——系统软件层：充分利用硬件资源（如 CPU、RAM、FLASH、SPI 总线等）的可信性，实现受硬件隔离的系统执行环境，具备安全计算及其所属各种安全设备运行的资源调用能力，可提供下述功能：

- 安全加解密、安全存储、可信用户接口、可信身份认证等各种系统服务；
- 系统和应用安全的密钥体系；
- 与 REE、SE、外部设备的安全通信机制，并提供相应的访问控制；
- 提供可信虚拟化层，可支撑多个可信 OS 并存与运行。

5.4 SE

移动终端上的高安全运行环境，可在硬件与软件层面上防御各种恶意攻击，运行在其上的应用具备高安全性需求，如eSE、inSE。其组成主要包括：

——应用软件层：包括安全应用，如金融、公交、社保、电信等，应用采用预置或在 TSM 控制下安全获取与部署，通过 SE 开展金融安全的应用场景可参考附录 C；

——系统软件层：运行一种可验证的卡片操作系统，主要提供安全加解密、密钥存储等功能。

5.5 外部设备

可以被TEE控制和使用，用于扩展TEE功能的移动终端元器件，包括但不限于触摸屏、摄像头、指纹模块、蓝牙模块、NFC芯片等。从安全角度考虑，外部设备可划分为专享外设和共享外设。

6 可信执行环境

6.1 概述

6.1.1 总体架构

可信执行环境总体架构见图2。

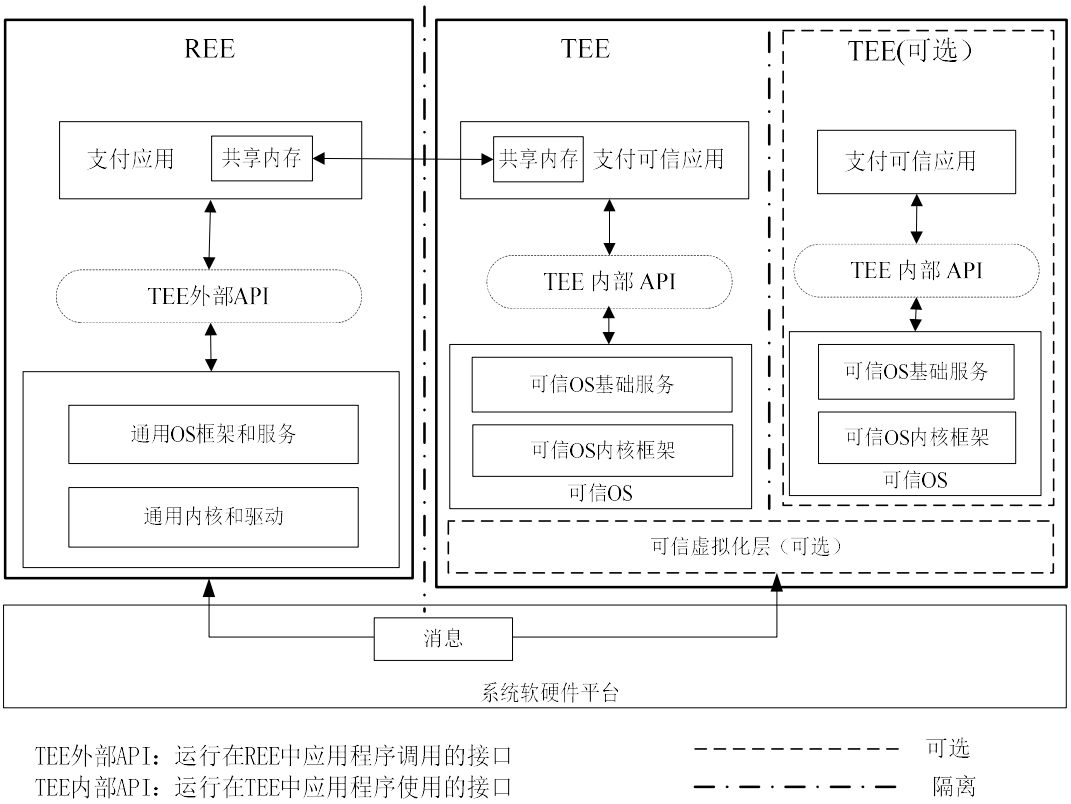

图2　可信执行环境总体架构图

6.1.2　安全目标

可信执行环境的安全目标如表1所示：

表1　可信执行环境安全目标及描述

安全目标	描述
启动安全	安全启动从可信代码开始，通过签名校验方法来保证信任链的传递，TEE启动过程的完整性通过上一阶段签名校验来保证。
存储安全	通过硬件的隔离和系统的控制，保护高安全性数据的存储安全，如用户数据、设备数据等。
通信安全	通过加密、隔离、认证等方式，对终端内不同实体间的通信通道、终端同外界的通信通道的数据传输进行安全性保护。
访问控制	通过访问权限的设置等方式保证功能和数据不被非法访问或者不恰当的访问。
系统配置	通过软硬件结合的安全措施保证终端的安全配置不被更改并具备相应的提示机制。
运行安全	通过对固件、密钥、永久数据等数据的保护策略保证TEE自身的安全性，为运行在其上的可信应用提供安全保护。
应用管理	通过生命周期管理、访问验证等措施保证对运行在其上的可信应用进行安全管理。

6.1.3　硬件安全要求

6.1.3.1 防止物理攻击

TEE 应具有一定的防物理攻击能力，物理攻击方式包括但不限于非侵入式攻击、半侵入式攻击，如旁路攻击、错误注入攻击等。

6.1.3.2 安全调试

应对设备调试接口进行相应的管控，只能通过授权控制的模式对内部敏感数据进行访问。

6.2 可信 OS

6.2.1 可信 OS 内核组成

提供了OS基本核心功能，包括进程调度管理、时间管理、进程间通信管理、中断管理、内存管理、外设驱动管理等。

提供了OS的系统级功能，包括用户态和内核态的可操作性定义、系统调用访问控制和权限管理、可信应用隔离和管理等。

6.2.2 可信 OS 基础服务

提供系统级的安全服务，见表2。

表2 可信 OS 基础服务

服务名称	功能简述
安全存储	提供基于文件操作的存储功能及接口，包含文件创建、打开、关闭、写入、读取、删除、重命名等。
加解密	提供密码算法功能及接口，包含摘要算法、信息验证码算法、对称加解密算法、非对称加解密算法、随机数算法、密钥衍生等。
安全时间	提供获取 TEE 系统时间和 REE 系统时间等时钟接口。
TA 管理	提供 TA 的下载、安装、更新、删除等功能。
SE 服务	提供与 SE 之间的操作及相关通讯接口。
生物特征识别	提供生物特征提取、模板存储和比对，以及针对比对结果的访问控制等功能。
REE 监测	提供对 REE 安全性的监测。
TUI	提供可信的用户交互接口。

6.3 安全启动

安全启动过程是指通过签名验证方法来检验TEE启动过程的每一个阶段，以确保TEE中运行软件镜像的完整性，防止对软件进行未被授权修改或恶意修改。安全启动代码应进行完整性验证，当验证通过后执行安全启动过程。安全启动过程保证了TEE的安全功能被正确地初始化，并且这个初始化过程不受REE恶意应用的攻击，同时保证固件的版本符合TEE版本更新策略。

同时，安全启动也伴随着一个信任链，即整个过程开始于一个可信代码（即这个代码的完整性受到保障）或者信任根，之后在执行其他代码之前都要验证其真实性。对于在安全启动过程中哪些代码需要被验证本部分不做具体定义。安全启动的代码可以通过OTA以代码镜像的方式进行更新。为了保证代码更新的安全性，在更新代码之前应验证更新镜像的真实性和完整性。

6.4 安全存储

6.4.1 功能要求

TEE应提供安全存储功能，例如将数据存储在安全存储器中，或对数据进行加密存储。
安全存储应提供以下基本功能：创建、打开、关闭、写入、读取、删除、重命名等。

6.4.2 安全要求

安全存储应满足如下安全要求：
——保证所保存数据的机密性、可用性、一致性和原子性；
——数据只能由数据管理者访问；
——安全存储所使用密钥应由根密钥衍生；
——保证安全存储所使用密钥的机密性和完整性；
——安全存储所使用密钥只能由密钥管理者访问和处理。

6.5 加解密服务

6.5.1 功能要求

加解密服务提供密码算法接口，使得应用可以通过该服务接口执行密码运算。密码运算应符合6.6.1.10的要求。

6.5.2 安全要求

加解密服务应符合表3所示的要求。

表3 加解密算法安全要求

算法	安全要求
摘要算法	应使用SHA256及以上强度算法。
对称密码算法	AES算法的密钥长度应为128bit及以上。 3DES算法的密钥长度应为128bit及以上。
非对称密码算法	RSA算法的密钥长度应为2048bit及以上。 椭圆曲线算法的密钥长度应为224bit及以上。 DSA算法的密钥长度应为2048bit及以上。 ECDSA算法的密钥长度应为224bit及以上。
随机数生成器	应符合GB/T 32915规范的规定。

6.6 密钥体系

6.6.1 密钥管理

6.6.1.1 概述

密钥包括根密钥、设备密钥、业务密钥。
密钥生命周期的管理包括密钥生成、使用和销毁。

6.6.1.2 随机数生成

随机数生成方式，应遵循GB/T 32915中的相关规定。

6.6.1.3 密钥生成

TEE应根据指定的密钥算法生成对称密钥和非对称密钥。

被生成的业务密钥包括：用于保护数据的数据加密密钥和用于保护其他密钥的密钥加密密钥。

6.6.1.4 密钥导入

通过安全方式导入到TEE安全存储区域中的密钥，应使用密钥加密密钥进行保护。

6.6.1.5 根密钥

根密钥是移动终端密钥体系的根，应符合以下要求：

——根密钥应使用硬件保护或硬件隔离技术保证安全性；

——硬件隔离的根密钥产生因子只可由独立的处理器运算生成；

——硬件保护的根密钥产生因子不可被任何软件访问，由通用处理器运算生成并进行扰乱保护；

——硬件隔离和硬件保护的根密钥应和REE隔离，不可被REE直接访问；

——根密钥不可直接从硬件中读和写；

——只有具备系统权限的可信应用可使用根密钥衍生出其他密钥。

6.6.1.6 设备密钥及设备身份证书

设备密钥应符合以下要求：

——应由根密钥在 TEE 中产生，或者随机生成后以密文形式注入设备的安全存储区域；

——可用于保护业务密钥，保证信任链的传递；

——可用于设备身份证明。

设备身份证书应符合以下要求：

——应在 TEE 或 SE 中产生，或者在出厂前预置；

——应保存在 TEE 或者 SE 环境中；

——可用于设备身份证明。

6.6.1.7 数据加密密钥

数据加密密钥长度应至少保证128bit。

数据加密密钥应使用RBG方法随机生成，密钥的强度应至少等同于128bit的AES密钥强度。

6.6.1.8 密钥加密密钥

密钥加密密钥的长度应至少保证128bit。强度应不弱于数据加密密钥。

密钥加密密钥宜基于口令的密钥衍生方式生成，或者用RBG方法生成，或者利用其他密钥来组合生成。

6.6.1.9 密钥销毁

程序运行时产生的明文密钥数据（密钥加密密钥、会话密钥等），在生命周期结束后应进行销毁，清除密钥的目标源和存储位置，销毁所有不再需要的明文密钥材料。

销毁方式分以下几种情况：

——对于易失性闪存，销毁应通过单一的用 RBG 生成的伪随机数或全 0 直接覆写，并随后进行一次读验证；

——对于非易失性 EEPROM（电可擦只读存储器），销毁应通过单一的用 RBG 生成的伪随机数直接覆写，并随后进行一次读验证；

——对于其他非易失性闪存，销毁应通过单一的用全 0 直接覆写，或一个块擦除，并随后进行一次

读验证；

——对于除了闪存和 EEPROM 的非易失性存储器，销毁应通过三次或更多次覆写，每次用不同的随机数。

6.6.1.10 密码算法

应支持国家密码管理机构认可的商用密码算法。

6.6.2 密钥存储

6.6.2.1 密钥可用性

TEE应为设备密钥和业务密钥提供安全存储能力，防止未经授权的应用对密钥访问。

6.6.2.2 密钥保密性

功能要求：TEE应保护密钥的安全性，密钥不应明文存储。

一般安全要求：密钥加密存储在TEE的安全存储区域内。

增强安全要求：密钥加密存储在RPMB区域或者SE中。

6.6.2.3 密钥完整性

TEE应为所有的数据加密密钥和密钥加密密钥提供完整性保护。

6.7 访问控制

6.7.1 概述

访问控制包括以下三种类型：

——TA 对客户端应用的访问控制：即限制未被授权的客户端应用访问 TA；

——TA 间的访问控制：即限制未被授权的 TA 访问其他 TA；

——TEE 基础服务的访问控制：即限制未被授权的 TA 使用基础服务。

6.7.2 功能要求

访问控制对 TEE 的功能要求如下：

——TEE 应维护一组访问规则，当某个客户端应用访问运行在 TEE 上的某个 TA 时，TEE 应根据这些访问规则来判断本次访问是否被允许；

——TA 应维护一组访问规则，当被其他 TA 访问时，被访问的 TA 可根据这些访问规则来判断本次访问是否被允许；

——TEE 应维护一组基础服务访问规则，当某个 TA 调用基础服务时，TEE 应根据这些访问规则来判断本次调用是否被允许。

6.7.3 安全要求

6.7.3.1 TA 对客户端应用的访问控制

访问控制要求如下：

——TEE 应能识别运行于 REE 之上的各个客户端应用，并获得客户端应用的标识；

——TEE 应保证访问控制规则的机密性和完整性；

——TEE 应能处理访问控制规则发生冲突的情况；

——访问控制规则导入移动终端的过程应是安全可信的。

6.7.3.2 TA 间的访问控制

安全要求如下：

——TEE 应提供接口，使被访问的 TA 能够获得访问 TA 的标识；

——TEE 应保证 TA 的标识在同一个终端上是唯一的、不可伪造的。

6.7.3.3 TEE 基础服务的访问控制

对TEE的安全要求如下：

——TEE 应对 SE 访问基础服务实施访问控制；

——TEE 应对生物特征采集设备的基础服务实施访问控制；

——访问控制规则导入移动终端的过程应是安全可信的。

6.8 TUI

6.8.1 功能要求

一般情况下，用户安全交互涉及的输出要求包括：

——显示文本、图像等；

——进行 LED、声音等指示。

输入要求：

——接受键盘输入信息；

——接受触摸屏输入信息；

——接受生物识别信息，例如指纹等。

为满足如上用户交互的要求，TUI会调用移动终端上的相关部件来进行用户交互，这些部件包括但不限于移动终端上的话筒、键盘、触摸屏、LED指示灯、指纹传感器等。

6.8.2 安全要求

一般要求：

——TUI 所调用的部件处于工作状态时，不能接收 REE 的访问请求，并且不能接收通知事件；

——当相关部件控制权属于 TUI 时，应由 TEE 来决定是否将这些部件的控制权交给 REE；

——TUI 应包含安全指示器，通过安全指示器呈现的安全指示信息使用户可识别当前显示的是 TEE 的界面，而不是 REE 的界面；

——TEE 应为用户提供设置通用安全指示信息的接口，通用安全指示信息可以是文字、图片、声音等，通用安全指示信息可被 TEE 中所有 TA 访问；

——在用户进行通用安全指示信息设置时，TEE 应首先判断终端当前是否处于安全状态，处于安全状态，才允许执行配置流程，安全状态检测应包括：

- 检测终端是首次启动；
- 检测终端 TEE 尚未个人化；
- 检测终端未取得系统中唯一超级用户权限（检测终端未被 Root）；
- 检测终端未安装来源非法或无法判断来源是否可信的应用。

增强要求：

TEE 应为用户提供设置个性化安全指示信息的接口，个性化安全指示信息只可以被 TEE 中特定的 TA 访问。

6.9 TA 应用管理

6.9.1 功能要求

TA应用管理主要是对TA生命周期进行管理，应包括但不限于安装、更新、锁定、解锁以及卸载，过程应保证原子性。状态转换应由TA管理服务器触发，或者直接在TEE上触发。

TA安装：应把TA应用加载到TEE指定的安全存储区，并创建可执行文件。TA安装可以通过预置或OTA两种方式。

TA更新：应安装一个新版本的TA应用到原有版本应用的安全存储区，并保留原有版本应用的数据。TA更新过程可通过OTA方式实现。

TA锁定（可选）：应将TA的生命周期状态更新到锁定状态，在这种状态下TA无法使用，也不能被管理，直到其被解除锁定状态为止。

TA解锁（可选）：应将TA的生命周期状态更新到锁定状态以外其他活动状态，在这种状态下TA应用正常运行。

TA卸载：应将指定TA从TEE的可操作应用列表中移除，并且释放包括TA可执行文件数据在内的所有和TA有关的数据。

6.9.2 安全要求

TA应用生命周期的配置转换有效提升TA应用和数据操作的安全性，包括安装、更新、锁定和解锁、卸载四个过程。

安装过程安全要求：

——预置安装，在 TEE 启动过程中，TEE 应验证 TA 的完整性、合法性，并安全加载到安全内存中运行；

——OTA 安装，OTA 安装应包含下载和安装两个过程，在下载过程中应对应用加密和签名处理以保证 TA 机密性、完整性和可用性，在安装过程中 TEE 应验证 TA 完整性、合法性，并安全加载到安全内存中运行。

更新过程安全要求：

——OTA 更新，对于包分发模式，应通过客户端应用或 REE 系统进行更新；

——对 TA 独立分发模式，应通过 TA 管理服务器进行更新；

——TA 更新安全要求应和 TA 安装安全要求一致。

锁定和解锁过程安全要求：

——在 TA 应用升级更新时，可以将其从正常状态迁移到锁定状态，从而确保应用升级更新时候数据的一致性和完整性，在升级更新完毕后再将其恢复为原始活动状态继续运行；

——锁定和解锁过程，其状态应是持久状态，确保其不会受到终端断电的影响，并且从其他状态到此状态的迁移也应是原子的，确保 TA 及其数据状态在状态转换过程中保持一致。

卸载过程安全要求：

应保证不残留任何应用相关的信息，尤其是应用数据等敏感信息。

6.10 TA 跨平台应用中间件（可选）

6.10.1 概述

一种独立的系统软件、服务程序或可编程应用接口，是可信OS功能抽象过后的运行时主要表现形式。其应屏蔽底层不同硬件平台及其不同可信OS种类所导致的差异，并为可信应用提供统一编程接口，以有效支持TA的跨平台兼容部署与运行。TA跨平台应用中间件框架如图3所示。

图3　TA 跨平台应用中间件框架图

6.10.2　功能要求

TA跨平台应用中间件应具备表4的功能要求。

表4　TA 跨平台应用中间件功能列表

功能点	功能要求
应用跨平台部署	中间件为达到跨平台部署应具备以下功能： ——中间件应能实现在不同硬件平台及不同可信OS上兼容运行，并提供统一应用编程接口给上层TA应用使用，以满足上层TA应用统一开发的需求； ——为高效实现跨平台部署，可采用虚拟机方式实现。
应用文件格式	中间件应提供一种统一的应用文件格式，该格式内数据结构应为中间件所识别和解析。该统一的可执行文件格式，是实现应用跨平台的必备条件。
访问控制	中间件应为其上层TA间、或者上层TA与REE应用间提供访问控制机制，进而确保中间件上TA在不同访问链接间的隔离性，以及不同应用间数据的正常可信交互。
数据存储	中间件应为上层可信应用提供基于数据存储的事务机制和原子操作能力，以确保中间件之上应用在通过中间件完成数据存储操作的时候，能够实现数据存储的一致性和完整性。
资源管理	为中间件上每个TA提供一种操作和管理可信OS资源的机制，具体功能包括： ——可有效管理每个TA对可信OS的资源的申请与释放，确保资源的正确申请和释放； ——可对各TA应用间运行通信时建立的会话资源进行管理。
生产维护	提供一种远程更新方式，实现对中间件的升级维护，以应对潜在Bug及其相应功能的升级服务，应包括以下两个功能： ——应能够通过远程更新方式，实现对 TA 跨平台中间件的升级和维护； ——应提供相应的手段与机制确保 TA 跨平台中间件及其上应用能可信、可靠的下载和安装。

6.10.3　安全要求

TA跨平台应用中间件应具备表5的安全要求。

表5　TA 跨平台应用中间件安全要求列表

功能点	安全要求
应用跨平台部署	应用跨平台部署应具备以下安全要求： ——应确保不同平台上应用运行时数据资源的一致性和完整性； ——可采用应用间防火墙机制来保障中间件运行时应用数据和资源的安全运行；

表 5　TA 跨平台应用中间件安全要求列表（续）

功能点	安全要求
应用跨平台部署	——保证一个TA在资源与数据运行出现问题时，不会影响和危害到其他TA的正常运行； ——抵御TA之间可能存在的互相恶意攻击威胁。
访问控制	访问控制应具备以下安全要求： ——确保可信应用相互之间资源与数据的隔离性，防止相互之间代码及数据的泄漏； ——只有指定客户端应用能够访问 TA，客户端应用所访问功能数据应按需进行限制； ——任何TA不能以任何方式访问其他TA、代码及元数据。
数据存储	数据存储应具备以下安全要求： ——中间件及其上应用在进行数据存储操作时，应根据需要完成对存储数据的加密并确保数据本身的隔离性、安全性、一致性和完整性； ——每个TA数据存储空间可被该应用的所有实例所共享，但应与其他TA应用相隔离。
资源管理	资源管理应具备以下安全要求： ——在TA进行可信OS资源操作时，应确保TA应用对资源的安全操作，并在资源操作完成后安全释放所用资源； ——应确保TA应用间通信时所建立会话的安全性，并在通信完成时及时销毁会话。
生产维护	生产维护应具备以下安全要求： ——确保TA跨平台部署中间件更新后，原有数据的安全性与一致性； ——应提供相应的手段与机制来确保中间件及其上应用能可信、可靠的下载和安装。

6.11　可信虚拟化（可选）

6.11.1　概述

通过相应虚拟化技术在终端可信硬件平台上实现的一层软件虚拟化功能模块，可向上提供多个具备可信计算能力、可信地址与数据空间、可信外设能力等的虚拟运行环境。可信虚拟化架构如图4所示。

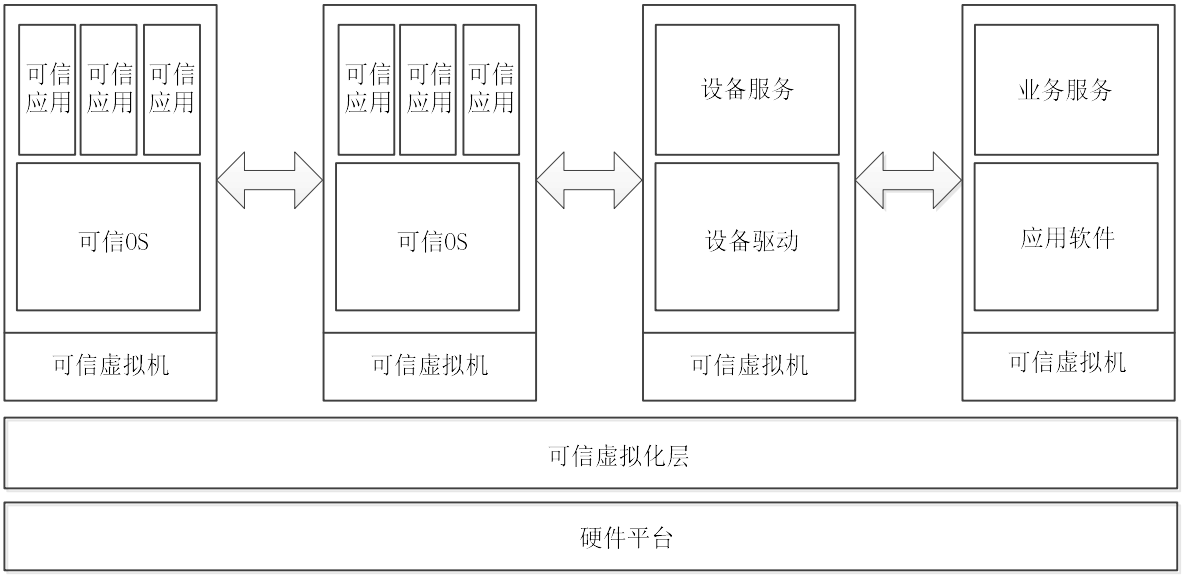

图4　可信虚拟化架构层

6.11.2 功能要求

可信虚拟化层应具备表6的功能要求。

表6 可信虚拟化层功能列表

功能点	功能描述
可信虚拟机	为每个虚拟机提供专属内存、外设、存储等资源，支持以下三种软件部署： ——可信OS：基于可信虚拟机直接部署本标准描述的可信OS； ——设备服务：基于可信虚拟机直接部署各种外设驱动程序及其对应的设备服务，如指纹驱动服务等； ——业务服务：基于可信虚拟机直接部署具体的业务场景应用，直接为用户提供业务服务。
数据通信	提供一种网络通信机制，支持不同可信虚拟机相互间的数据通信，具体功能包括： ——创建网络通道：为两个需要通信的可信虚拟机提供网络通道动态链接的方法； ——断开网络通道：根据需要，可信虚拟机一方可随时断开与任意一方可信虚拟机的网络通道。
密钥体系	为每个可信虚拟机提供根密钥，支持各可信虚拟机基于各自根密钥建立各自的密钥体系。
资源配置与访问	根据机构所开展业务需求，为可信虚拟机提供所需硬件资源的配置与访问能力，包括RAM、FLASH、各种外设等。
REE访问	提供与REE间的数据访问机制，允许REE上应用访问各自对应的可信虚拟机服务，并正确且安全地管理每个REE应用及其对应可信虚拟机服务的访问链接。
生产维护	提供一种远程更新方式，实现对可信虚拟化层的升级维护，以应对潜在Bug及其相应功能的升级服务。

6.11.3 安全要求

可信虚拟化层应具备表7所示的安全要求。

表7 可信虚拟化层安全要求列表

功能点	安全描述
可信虚拟机	可信虚拟机应具备以下要求： ——确保可信虚拟机相互之间软硬件资源的隔离性，防止相互之间代码及数据的泄漏； ——任何一个可信虚拟机运行出现问题，都不应影响其他可信虚拟机的正常运行； ——确保对可信虚拟机之间可能存在的恶意攻击和危险进行抵御。
数据通信	数据通信应具备以下要求： ——确保每个网络通道的隔离性与数据安全性，防止数据泄漏； ——防止网络通信数据被第三方监听、破坏、篡改等恶意行为； ——提供访问控制能力，确保可信虚拟机不被恶意访问。
密钥体系	密钥体系应具备以下要求： ——根密钥存储区应基于可信环境下的硬件存储保护机制，保证根密钥数据的机密性和完整性，抵御一定程度的硬件攻击； ——确保各可信虚拟机间根密钥的相互隔离和不可相互访问，防止数据泄漏。
资源配置	资源配置应具备以下要求： ——确保各可信虚拟机之间资源配置信息的隔离性，防止泄漏风险； ——确保资源配置信息的安全性，防止被篡改、破坏等。
硬件操作	硬件操作应具备以下要求：

表 7　可信虚拟化层安全要求列表（续）

功能点	安全描述
硬件操作	——确保不同硬件内存映射表间的相互隔离性； ——确保硬件内存映射表不被非法篡改、破坏等恶意行为。
REE访问	REE访问应具备以下要求： ——确保链接建立与释放后的相应资源的申请与释放； ——确保不同访问链接之间的隔离性，确保REE与可信虚拟机间数据的正常可信交互； ——对于访问链接数，在某一时刻所存在数量是基于实现定义的，其可根据运行时资源限制进行调整。
生产维护	生产维护应具备以下要求： ——应提供相应的手段与机制来确保可信虚拟机初始镜像可信、可靠的下载与安装； ——确保更新后，原有可信虚拟机中数据的安全性与一致性。

7　通信要求

7.1　REE 与 TEE 的通信要求

REE与TEE之间的通信采用共享内存或消息的方式，应满足如下要求：

——REE 无法访问 TEE 的安全内存；

——TEE 可以访问 REE 的非安全内存，但不应具备对该内存的执行权限；

——通信过程中，共享内存不能被其他第三方应用访问；

——通信结束后，共享内存应失效或被清除。

7.2　TEE 与数据采集设备的通信安全

7.2.1　数据采集设备处于 REE

应满足如下安全要求：

——对于具有处理单元的数据采集设备：TEE 与数据采集设备之间的通信应建立安全通道，保证通信的完整性和机密性；

——对于不具有处理单元的数据采集设备：本标准不建议这类数据采集设备应用于支付业务。

7.2.2　数据采集设备处于 TEE

应满足如下安全要求：

——防止 REE 访问、篡改该类设备的数据，只有 TEE 可以访问该类设备；

——防止其他未授权 TA 访问、篡改该类设备的数据，TEE 应保证授权 TA 访问该类设备的原子性和独占性。

7.3　TEE 与 SE 的通信安全

应满足如下安全要求：

——防止其他未授权 TA 访问、篡改通信数据，TEE 应保证授权 TA 访问 SE 的原子性；

——TEE 与 SE 之间的通信应建立安全通道，保证通信的完整性和机密性。

8 数据安全

8.1 数据安全保护功能

8.1.1 数据录入

应提供数据输入即时加密功能，用于用户输入密码时的数据保护，支持的支付应用应符合JR/T 0092中的相关要求。

应提供数据输入防护功能，防止密码等敏感数据明文显示，保证敏感数据不被移动终端的其他设备或程序非授权获取和篡改，支付的应用应符合JR/T 0092中的相关要求。

8.1.2 数据访问

应支持数据访问控制功能，根据访问控制策略保证敏感数据仅供授权用户或授权应用组件访问，支付的应用应符合JR/T 0092中的相关的要求。

8.1.3 数据存储

应提供数据存储安全保护功能和接口，支付的应用应符合 JR/T 0092 中的相关的要求，包括但不限于：

——敏感数据限量、限时存储的功能；

——敏感数据显示时屏蔽部分内容的功能；

——清除敏感数据功能，身份认证、交易等敏感数据使用后应及时清除。

8.1.4 数据传输

应提供数据传输安全保护功能和接口，支付的应用应符合JR/T 0092中的相关的要求，包括但不限于：

——数据加密功能；

——基于密码技术的数据完整性校验功能。

密码算法应符合本标准6.6.1.10的要求。

8.2 内部数据安全要求

8.2.1 TEE ID

TEE应具有对应的ID数据，该数据通常存储于TEE的RPMB。TEE ID可由系统其他部分（例如：TA和其他软件）读取且应禁止被非法篡改。

8.2.2 随机数

生成的随机数应符合GB/T 32915规范中的相关规定。

8.2.3 TA 数据安全

应保证 TA 代码数据的真实性和完整性。TA 代码应具有防止反汇编的能力，增加攻击难度。

应保证 TA 调用 TEE 提供的相关服务时使用的数据的真实性、完整性、原子性和机密性，并和移动设备绑定。

TA数据的储存存在以下三种安全等级：

——数据安全等级 2：储存位置为安全内存并使用加密算法加密过的数据，安全性最高；

——数据安全等级 1：储存位置为安全内存但未使用加密算法加密过的数据或者储存位置为非安全区但使用加密算法加密过的数据，安全性中等；

——数据安全等级 0：储存位置为非安全区且未使用加密算法加密过的数据，不具有任何安全性。

敏感数据应当保证使用安全等级 1 以上的储存方式。除了特殊情况外，敏感数据不能存在过长时间，或使用次数过多。当对敏感数据的操作结束时，或者存在来自外部的取消操作请求时，内部缓存的敏感数据应被立刻清除。

8.2.4 TEE 数据安全

应在安全启动、安全隔离、密钥管理、安全存储等方面采取措施，确保在 TEE 中动态和静态存储数据的机密性、完整性和可靠性，包括但不限于：

——应保证 TEE 运行时数据（包括但不限于执行变量、运行时上下文）的完整性、机密性；

——应保证 TEE 持久性数据（包括但不限于 TEE 加密密钥）的真实性和完整性。当数据有效性验证失败时，删除该持久性数据；

——应保证 TEE 镜像数据（包括但不限于字节码文件和版本号）的真实性和完整性；

——应保证用于设备上电启动、验证 TEE 有消息并激活 TEE 安全服务的 TEE 启动代码数据的完整性。

9 安全单元

在移动终端上，运行在REE上的REE应用和运行在TEE上的TA都会访问SE，这两种情况都需要实施一定的访问控制措施。

TEE应提供SE访问的基础服务，并对TA提供调用接口。根据SE访问控制规则，TEE应实现如下功能：

——在 TEE 的 SE 访问服务里，应具有实施 SE 访问控制的强制检查模块，该模块从 SE 中获取 SE 访问规则，并根据访问者的 ID（TA 的 UUID）和被访问者的 ID（SE 中的应用的 AID）来判断访问是否被允许，当访问被允许时，TA 才可以执行对 SE 的访问操作，否则 TA 对 SE 的访问将被拒绝；

——访问控制措施的实施对 TA 而言是透明的；

——TEE 应保证 TA 的 UUID 在同一个终端上是唯一的、不可伪造的；

——SE 访问控制强制检查模块应具备处理访问控制规则发生冲突的能力。

TA 对 SE 的访问控制也可通过认证的方式实现。例如 TA 与 SE 利用事先约定的认证密钥，由 SE 对 TA 进行认证，认证成功后，TA 才可以执行后续的 SE 访问操作。该访问控制方法属于应用级的策略，本标准不做具体的定义。

注：REE 应用对 SE 的访问控制机制不在本标准范围之内。本标准只关注 TA 对 SE 的访问控制。

10 客户端支付应用

10.1 概述

客户端支付应用是运行在REE上的应用，通过调用TEE外部接口和TA进行通信，完成与支付相关的功能。

10.2 TEE 外部接口安全性要求

TEE外部接口是一个底层通信接口，接口的设计目标应使得REE的客户端支付应用可以与TEE中的TA进行交互，同时应满足表8所示安全性要求。

表8　外部接口安全性要求

安全性要求	备注
防伪装攻击	防止第三方伪装成合法者，调用系统接口，进行恶意操作。
防篡改攻击	防止输入的参数值在传输过程中被修改。
防重放攻击	防止通过重复发送一个已经被目的主机接收过的包达到欺骗系统的目的，通常在身份认证过程中发生。
防数据信息泄漏	防止数据在传输过程中被截获。如：截获用户登录请求，截获账号、密码等。
线程访问安全	避免多线程情况下，出现数据不一致或者数据被改变污染。
清空敏感数据缓存	退出接口时应对敏感数据的缓存进行清除。
避免内存泄露	内存泄露会导致数据泄露，较严重的会导致系统崩溃。
边界检查	对传入参数要做严格的边界检查。

10.3　其他要求

应满足JR/T 0092中的相关要求。

11　外部设备

11.1　安全目标

外部设备主要负责采集、处理用户的个人信息，包括生物识别信息和屏幕输入的密码等。此类信息用于登录或支付过程中的用户身份验证。外部设备还应保证敏感信息的安全采集、处理和传输。

如果用户的身份验证在外部设备完成，外部设备应具有和TEE内部组件相同的安全要求，保证敏感信息的存储安全和比对安全，比对结果应采用加密方式，保证传输过程数据不被篡改或泄露。

11.2　安全要求

11.2.1　生物特征采集安全要求

基本要求：

——生物特征传感器硬件与移动设备硬件相对隔离，无法通过移动设备读取生物特征信息；

——采集过程在独立的逻辑域或物理域中实现。

增强要求：

生物识别系统具备防伪造生物特征数据能力。

11.2.2　生物特征存储安全要求

生物特征存储应符合以下安全要求：

——存储过程在独立的逻辑域或物理域中实现；

——不存储生物特征原始数据，只存储经过单向变换的数字生物特征，且该特征不能被还原成生物特征原始数据；

——生物特征数据使用设备相关的密钥加密存储；

——生物特征数据仅本地存储；

——生物特征数据仅在身份鉴定通过后可被修改；

——生物特征标识与设备标识进行绑定；

——提供对生物特征数据彻底删除的功能；
——从移动终端删除用户应确保用户时，对应的生物特征数据被删除。

11.2.3 生物特征识别安全匹配

生物特征识别安全匹配应符合以下要求：
——匹配过程在独立的逻辑域或物理域中实现；
——匹配结果采取安全方式进行传输，防止篡改和窃取；
——设定最大匹配失败次数，防止暴力破解；
——失败次数大于最大失败次数后，采取相应失败处理机制。

12 移动终端支付可信环境生产要求

12.1 概述

本章规定了终端厂商在生产支持本标准可信环境的终端时所应遵守的基本要求。

12.2 管理要求

12.2.1 组织要求

应成立安全管理组织，明确职责，保证TEE密钥个人化的安全要求及密钥个人化安全制度的实施。

12.2.2 人员要求

对于与密钥相关的关键岗位职员应进行严格选择，并保证兼职员工、临时工等人员不得从事这些关键岗位的工作。

12.2.3 安全要求

与密钥处理直接相关人员的工作行为应被监控，保证单独的人员（或未授权人员）不能访问加密系统密钥或安全介质数据。

12.3 网络要求

用于连接密钥数据接收处理、加密设备或系统、准备系统、数据库等网络应为一个隔离的独立网络。

12.4 机房及系统要求

12.4.1 机房出入安全控制

机房应执行高安全区-生产区安全要求，所有的出入应使用门禁系统进行控制，并保证其内最少有两名或以上工作人员。对于非授权工作人员或来访人员出入机房，授权人员应全程陪同，做好登记签名。

12.4.2 主机安全

与密钥处理相关的主机设备淘汰或者另作他用时，应在安全管理人员监督下删除相关数据，并做好记录，未经授权，不得随意动任何主机设备。

12.4.3 机房环境安全

数据机房内应安装安放监控报警装置，实行24小时监控，监控录像至少保存三个月，并除监控设备外，禁止携带或使用摄影、录像、录音等与工作无关的记录设备。

12.4.4 数据备份与恢复

应提供一套完善的机制与策略，做好数据的定时备份，实现灾难数据恢复。

12.4.5 数据传输

为防止在各机构间传送的数据信息丢失、修改或被盗用，机构之间传送数据信息应当受到控制，通常情况下应使用专线、数据盘邮寄和人工递送方式。

12.4.6 数据安全

在数据接收后，生产企业应将加密数据及时转移至内部处理网络，删除接收设备上的数据。

12.5 密钥管理要求

在可信执行环境之外执行的加密和解密操作应在硬件加密模块上进行。

12.6 硬件加密设备要求

应使用国家密码管理部门许可的硬件加密设备。

13 移动终端支付可信环境安全分级分类

13.1 安全能力级别总则

移动终端除了出厂必带的REE操作系统之外，还可根据安全需求选择支持TEE或者SE环境；根据所支持的运行环境的不同，将移动终端支付可信环境安全能力从低到高分为三个级别，并规定了每个级别应具备的安全能力的最小集合。

当安全能力为一级时，移动终端仅运行REE环境，其REE环境应具备13.2条所描述的全部能力。

当安全能力为二级时，根据移动终端所包含的运行环境及每种环境所具备的能力不同，二级安全能力进一步分为A、B、C、D四个类别。当为二级A类，移动终端同时包括REE和SE两种运行环境，其中REE环境应具备13.2条所描述的全部能力，SE环境应具备13.4条所描述的SE基础安全能力集合要求中的全部能力；当为二级B类，移动终端同时包括REE和TEE两种运行环境，其中REE环境应具备13.2条所描述的全部能力，TEE环境应具备13.3条所描述的TEE基础安全能力要求集合中的全部能力；当为二级C类，移动终端同时包括REE和TEE两种运行环境，其中REE环境应具备13.2条所描述的全部能力，TEE环境应具备13.3条所描述的TEE基础安全能力和扩展安全能力中两个集合中的全部能力；当为二级D类，移动终端同时包括REE、TEE和SE三种运行环境，其中REE环境应具备13.2条所描述的全部能力，TEE环境应具备13.3条所描述的TEE基础安全能力要求集合中的全部能力，SE环境应具备13.4条所描述的SE基础安全能力集合要求中的全部能力。

当安全能力为三级时，移动终端同时包括REE、TEE和SE三种运行环境，其中REE环境应具备13.2条所描述的全部能力，TEE环境应具备13.3条所描述的基础安全能力和扩展安全能力两个集合中的全部能力，SE环境应具备13.4条所描述的SE基础安全能力和扩展安全能力两个集合中的全部能力。

移动终端支付可信环境安全能力级别总则见表9。

表9　可信环境安全能力级别总则

安全能力级别		安全能力要求				
		REE基础能力集合	TEE基础能力集合	TEE扩展能力集合	SE基础能力集合	SE扩展能力集合
一级		■				
二级	A类	■			■	
	B类	■	■			
	C类	■	■	■		
	D类	■	■		■	
三级		■	■	■	■	■

13.2　REE 基础安全能力要求集合

REE环境，详见5.2条描述，作为移动终端出厂必带的操作系统，如果未被进行未经授权的修改，则默认为达到REE基础安全能力要求。

运行在REE环境中的支付应用客户端应符合JR/T 0092中的相关要求。

13.3　TEE 安全能力要求集合

TEE 基础安全能力要求集合见表 10。

表10　TEE 基础安全能力要求

类别	能力项	备注说明
硬件安全	防止物理攻击	详见6.1.3.1
	安全调试接口管控	详见6.1.3.2
启动安全	启动代码的数据安全	详见8.2.4
	启动过程安全	详见6.3
存储安全	密钥存储	详见6.6.2
	非密钥的数据密钥	详见6.4.2
运行安全	随机数生成	详见6.6.1.2
	密钥生成	详见6.6.1.3
	密钥导入	详见6.6.1.4
	根密钥	详见6.6.1.5
	设备密钥	详见6.6.1.6
	数据加密密钥	详见6.6.1.7
	密钥加密密钥	详见6.6.1.8
	密钥销毁	详见6.6.1.9
	密码算法要求	详见6.6.1.10
	TEE数据安全	详见8.2
通信安全	REE与TEE的通信安全	详见7.1
	TEE与数据采集设备间的通信安全	详见7.2
访问控制	TA访问控制	详见6.7.1
	REE监测	详见6.2.2
	TA间访问控制	详见6.7.3.2

表 10　TEE 基础安全能力要求（续）

类别	能力项	备注说明
访问控制	基础服务访问控制	详见6.7.3.3
系统配置	安全时间	详见6.2.2
TA管理	TA数据安全	详见8.2.3
	TA生命周期管理	详见6.9

TEE 扩展安全能力要求集合见表 11。

表11　TEE 扩展安全能力要求

类别	能力项	备注说明
TEE 系统能力扩展	对 TEE 平台进行远程管理	详见 6.9.1 中对更新操作的描述
TA 管理能力扩展	对 TA 进行远程管理	详见 6.9
访问控制能力扩展	TEE 平台与 SE 之间的安全访问机制	详见 9 若移动终端不包括 SE，则扩展安全能力要求集合不包括此项
外部通信能力扩展	TEE 与 SE 之间的安全通道	详见 7.3 若移动终端不包括 SE，则扩展安全能力要求集合不包括此项
用户交互接口能力	可提供 TUI 能力	详见 6.8

13.4　SE 安全能力要求集合

SE基础安全能力集合应符合JR/T 0089.2相关规定，SE扩展安全能力要求集合见表12。

表12　SE 扩展安全能力要求

类别	能力项	备注说明
与 TEE 之间的访问控制	配合 TEE 对 SE 的访问控制机制的实施的能力	详见 9 TEE 对 SE 进行访问控制机制的实施，需要 SE 具备相应配合的能力
与 TEE 之间的通信安全	配合 TEE 与 SE 之间创建安全通道的能力	详见 7.3 TEE 与 SE 创建安全通道，需要 SE 侧具备相应配合的能力

附 录 A
（规范性附录）
检测规范

A.1 测试条件

默认环境条件（温度、湿度等）是指常温20±3℃，相对湿度在20%-80%RH之间。如无特殊说明，后续案例均采用此环境条件。

A.2 移动终端支付可信环境安全概述

移动终端支付可信环境整体框架参见图1，主要包括REE、TEE和SE三部分。其中，每个部分又可分为应用软件层、系统软件层、硬件层和外部设备四个层次。移动终端支付可信环境的整体安全性取决于REE、TEE和SE各自的安全性，以及集成的安全性。

A.3 TEE功能检测

A.3.1 概述

本条为TEE基本功能检测项，TEE扩展功能检测项见附录B.1。

A.3.2 CA与TA数据交互功能

A.3.2.1 共享内存的使用

检测目的：CA与TA对共享内存访问是否具有有效性和一致性。
通过标准：CA与TA读写共享内存数据有效一致。

A.3.2.2 共享内存的管理

检测目的：是否可以对共享内存进行创建并进行访问限制、对数据类型进行设置。
通过标准：共享内存可以正确被创建并符合当前设置的访问限制与数据类型设置。

A.3.2.3 CA对TA的异常的捕获

检测目的：CA是否可以正确调用指定的TA获取相应的反馈信息。
通过标准：CA正确调用指定的TA并获取相应的反馈信息。

A.3.2.4 CA对TA的调用与反馈

检测目的：CA是否可以成功捕获TA抛出的各种类型的异常信息。
通过标准：CA可以成功捕获TA抛出的各种类型的异常信息。

A.3.2.5 CA对TA的数据传递

检测目的：TA在被调用时是否可以成功获取CA所提交的数据并正确解析。
通过标准：TA可以正确解析CA所提交的数据。

A.3.3 数据的存储

A.3.3.1 临时数据的创建

检测目的：临时数据是否可以成功创建。
通过标准：临时数据可以成功创建。

A.3.3.2 临时数据的使用

检测目的：临时数据所存储数据的有效性、对临时数据的读、写及设置用途限制等相关功能是否成功。
通过标准：临时数据正确被读写以及执行相关操作。

A.3.3.3 临时数据的销毁

检测目的：临时数据是否在TA执行完毕之后进行销毁。
通过标准：临时数据在TA执行完毕后应被成功销毁并且销毁之后不可被访问。

A.3.3.4 持久化数据的创建

检测目的：持久化数据是否可以成功创建。
通过标准：持久化数据可以成功被创建。

A.3.3.5 持久化数据的使用

检测目的：持久化数据所存储数据的有效性、一致性、独占性以及对持久化数据的读、写、设置用途、访问权限设置等相关功能是否成功。
通过标准：持久化数据正确被不同TA读写以及执行相关操作。

A.3.3.6 持久化数据的存储

检测目的：持久化数据是否具有持久性。
通过标准：持久化数据存储的数据应具有持久性，与不同TA在受限情况（用途控制、独占）下共享。

A.3.3.7 持久化数据的销毁

检测目的：持久化数据是否可以人工进行销毁。
通过标准：持久化数据可以被成功销毁并且销毁之后不可被访问。

A.3.3.8 临时数据的管理

检测目的：是否可以限制临时数据的用途（特定算法或数据流）。
通过标准：在使用临时数据时应进行用途限制。

A.3.3.9 持久化数据的管理

检测目的：是否可以限制持久化数据的用途（特定算法或数据流）并对持久化数据进行访问控制。
通过标准：在使用持久化数据时应进行用途限制和访问控制。防止REE访问、篡改该类设备的数据，有且仅有TEE可以访问该类设备。

A.3.4 加解密算法实现

A.3.4.1 对称加解密算法

检测目的：验证对称加解密算法（如AES、DES、3DES）实现。
通过标准：正确实现对称加解密算法。

A.3.4.2 消息摘要算法

检测目的：验证消息摘要算法（如SM3、SHA256、SHA384、SHA512）实现。
通过标准：正确实现消息摘要算法。

A.3.4.3 密钥交换算法

检测目的：验证密钥交换算法（如DH、ECDH）实现。
通过标准：正确实现密钥交换算法。

A.3.4.4 随机数

检测目的：验证随机数算法实现。
通过标准：正确实现生成随机数。

A.3.4.5 签名及签名认证

检测目的：验证使用非对称密钥对消息的摘要数据进行签名以及签名认证操作的实现（如SM2、DSA、ECDSA）。
通过标准：正确实现签名验签。

A.3.5 时间管理

A.3.5.1 查询REE系统时间

检测目的：验证TEE查询REE系统时间的准确性。
通过标准：正确获取REE的系统时间。

A.3.5.2 获取TEE系统时间

检测目的：验证获取TEE系统时间的准确性。
通过标准：正确获取TEE的系统时间。

A.3.6 读取环境信息

检测目的：TA是否可以获取可信环境的相关信息（可包括但不限于当前客户信息、TEE自身环境信息、当前TA配置信息）。
通过标准：TA正确获取可信环境的相关信息。

A.4 TEE安全检测

A.4.1 概述

本条为TEE基础安全检测项，TEE扩展安全检测项见附录B.2。

A.4.2 TEE硬件层安全

A.4.2.1 密码算法

检测目的：验证TEE硬件层所执行的密码算法符合相应的算法标准（如3DES、RSA等）。

检测过程：检查TEE硬件层的对称密码或非对称密码算法是否符合相应的密码算法标准。

通过标准：TEE硬件层应按照相应的算法标准正确执行密码算法。

A.4.2.2 随机数生成器

检测目的：验证TEE硬件层随机数生成器产生的随机数具备足够的随机性。

检测过程：验证TEE硬件层产生随机数的质量，进行GB/T 32915、AIS 20/AIS 31、NIST SP800-22或FIPS PUB 140-2标准化的测试。

通过标准：满足标准化测试的要求。

A.4.2.3 异常检测机制

检测目的：验证TEE硬件层具备足够的异常检测机制，且能按照其容错机制进行相应的处理。

检测过程：检查TEE硬件层产生异常时是否具备相应的检测机制，包括环境异常检测、程序执行异常检测和逻辑模块异常检测，并按照TEE硬件层的容错机制进行相应的处理。

通过标准：TEE硬件层能够对常见的异常进行检测，并按照其容错机制进行相应的处理。

A.4.2.4 存储器访问控制

检测目的：验证TEE硬件层存储器访问控制策略的有效性。

检测过程：检查TEE硬件层存储器访问控制策略。

通过标准：TEE硬件层具备且遵循存储器访问控制策略。

A.4.2.5 总线传输安全

检测目的：验证TEE硬件层具备足够的保护机制以防止其传输系统的物理位置被探测或修改。

检测过程：尝试定位TEE硬件层传输系统，并评估其物理位置探测的难易等级和总线加密防护强度。

通过标准：TEE硬件层应具有较强的物理防护机制防止传输系统位置被探测，传输系统应采用总线加密、极性反转、总线校验等安全机制，防止总线信息泄露。

A.4.2.6 寄存器管理

检测目的：验证TEE硬件层寄存器管理策略的有效性。

检测过程：检查TEE硬件层寄存器管理策略。

通过标准：TEE硬件层具备且遵循寄存器管理策略。

A.4.2.7 启动流程

检测目的：验证TEE硬件层启动过程中，对其工作环境、完整性等安全机制具备有效的自检机制。

检测过程：评估TEE硬件层的启动过程。

检测标准：TEE硬件层启动过程中，能够对其工作环境和完整性执行有效检验。如果发生异常，TEE硬件层应处于复位或不可用状态。

A.4.2.8 调试

检测目的：验证TEE硬件层具备安全调试的能力。

检测过程：检查TEE硬件层的调试接口的相应控制策略。

通过标准：TEE硬件层应防止通过调试接口非法访问内部的敏感信息。

A.4.2.9 中断处理

检测目的：验证TEE硬件层具备中断处理的能力。

检测过程：检查TEE硬件层的中断级别与分类的管理机制。

通过标准：TEE硬件层应保证在特定的运行状态或异常报警等情况发生时，按照优先级进行中断处理。

A.4.2.10 可信存储

检测目的：验证TEE硬件层具备可信存储的能力。

检测过程：检查TEE硬件层的存储器对可信存储和非可信存储的区分策略。

通过标准：TEE硬件层应防止可信存储和非可信存储被混合使用，应严格区分可信存储和非可信存储的物理界限。

A.4.2.11 物理防护

检测目的：验证TEE硬件层具备足够的物理防护机制。

检测过程：检查TEE硬件层中敏感信号的物理防护机制和布线约束规则。

通过标准：TEE硬件层中敏感信号线应采用底层金属层布线或金属层遮挡等物理防护机制。

A.4.2.12 侧信道分析

检测目的：验证TEE硬件层在执行密码算法时具备抗侧信道分析的能力。

检测过程：参考TEE硬件层设计文档，尝试对其进行侧信道攻击。

通过标准：TEE硬件层在执行密码算法时无法通过侧信道分析的方式获取密钥等敏感信息。

A.4.2.13 错误注入

检测目的：验证TEE硬件层具备防错误注入攻击的能力。

检测过程：参考TEE硬件层设计文档，尝试对其进行错误注入攻击。

通过标准：TEE硬件层应具备防错误攻击的能力，无法通过错误注入的手段获取密钥等敏感信息。

A.4.3 TEE系统软件层安全

A.4.3.1 应用识别

检测目的：验证TEE系统软件层具备TA和CA识别的能力。

检测过程：参考TEE系统软件层设计文档，执行应用识别操作。

通过标准：TEE系统软件层应确保TA的ID的唯一性，并能够区分TA和CA。

A.4.3.2 密钥管理

检测目的：验证TEE系统软件层具备密钥管理机制。

检测过程：参考TEE系统软件层设计文档，执行密码管理中相关操作。

通过标准：TEE系统软件层应根据密钥创建者的设定，限定密钥的用途。TEE系统软件层应根据符合相关标准的特定密钥生成算法和特定密钥长度来产生密钥，并根据符合相关标准的特定密钥分发方法来分发密钥。TEE系统软件层销毁密钥后，已销毁的密钥信息不可被获得。

A.4.3.3 TEE标识

检测目的：验证TEE系统软件层具有唯一ID，且不可被更改。

检测过程：尝试获取或使用、对比、更改TEE系统软件层的ID。

通过标准：TEE系统软件层应具有唯一ID，且该ID是不可被更改。

A.4.3.4 启动流程

检测目的：验证TEE系统软件层具备安全启动的能力。

检测过程：执行TEE系统软件层的启动流程，并尝试对其进行攻击。

通过标准：TEE系统软件层应通过一个安全的初始化流程启动。

A.4.3.5 实例化时间单向性

检测目的：验证TEE系统软件层具备实例化时间不可逆的能力。

检测过程：多次获取TEE系统软件层的实例化时间，并将结果进行比较。

通过标准：TEE系统软件层应提供TA的实例化时间，该时间在TA实例化期间是不可逆的。

A.4.3.6 安全操作

检测目的：验证TEE系统软件层具备正确执行安全功能，且不受异常状态影响的能力。

检测过程：执行TEE系统软件层的安全功能，确认安全功能的执行不会受到异常状态的影响。

通过标准：TEE系统软件层应实现安全功能的正确操作，不受异常情况的影响，具备安全服务的访问控制，不会泄露敏感信息。

A.4.3.7 随机数

检测目的：验证TEE系统软件层使用的随机数具备足够的随机性。

检测过程：验证TEE系统软件层产生随机数的质量，进行GB/T 32915、AIS 20/AIS 31、NIST SP800-22或FIPS PUB 140-2标准化的测试。

通过标准：TEE系统软件层应使用TEE硬件层随机数生成器产生的随机数，且该随机数满足标准化测试的要求。

A.4.3.8 运行时数据机密性

检测目的：验证TEE系统软件层具备保证运行时数据机密性的能力。

检测过程：检查TEE系统软件层运行时的数据，验证其能够防止非法泄露。

通过标准：TEE系统软件层应保证运行时数据的机密性，TA数据和密钥未发生非法泄露。

A.4.3.9 运行时数据完整性

检测目的：验证TEE系统软件层具备保证运行时数据完整性的能力。

检测过程：检查TEE系统软件层运行时的数据，验证其能够防止非法篡改。

通过标准：TEE系统软件层应保证其固件和运行时数据、TA的代码和数据等在易失性存储器中运行时未被非法篡改。

A.4.3.10 TA真实性保护

检测目的：验证TEE系统软件层具备验证TA代码真实性的能力。

检测过程：检查TEE系统软件层对TA代码真实性的校验过程，验证该校验过程的有效性。

通过标准：当TA被装载到安全存储区域后，TEE系统软件层应执行真实性验证，验证通过TA后方可被加载。

A.4.3.11 TA隔离

检测目的：验证TEE系统软件层具备隔离TA的能力。
检测过程：执行TA操作，尝试访问其他TA的资源，验证TA之间隔离机制的有效性。
通过标准：TEE系统软件层应保证每个TA仅能访问自己的执行和存储空间。

A.4.3.12 TEE数据保护

检测目的：验证TEE系统软件层具备保证TEE持久性数据的真实性、完整性、机密性的能力。
检测过程：尝试获取、篡改TEE持久性数据。
通过标准：TEE系统软件层应确保TEE持久性数据的真实性、完整性、机密性。

A.4.3.13 TEE隔离

检测目的：验证TEE系统软件层具备保护其执行和存储的空间和资源的能力。
检测过程：尝试通过REE和TA获取TEE系统软件层执行和存储的空间和资源。
通过标准：TEE系统软件层应防止REE和TA获取其执行和存储的空间和资源。

A.4.3.14 可信存储

检测目的：验证TEE系统软件层具备为TA提供可信存储的能力。
检测过程：尝试执行可信存储操作，并获取、篡改TA存储的数据和密钥。
通过标准：TEE系统软件层应为TA的通用数据/密钥提供可信存储服务，保证其机密性、真实性和一致性，对存储内容的修改操作具备原子性。TEE系统软件层的可信存储应与设备绑定。

A.4.3.15 回滚保护

检测目的：验证TEE系统软件层具备防止未经授权回滚的能力。
检测过程：执行TEE系统软件层的回滚操作。
通过标准：只有通过认证的用户方可执行TEE系统软件层的回滚操作。

A.4.3.16 TA持久时间的单向性

检测目的：验证TEE系统软件层具备为TA提供持续性时间的能力。
检测过程：获取TEE系统软件层为TA提供的持续性时间。
通过标准：TEE系统软件层应能够为TA提供持续性时间，且不受TEE系统软件层复位的影响。

A.4.3.17 调试

检测目的：验证TEE系统软件层的调试功能只有通过认证的用户才能使用。
检测过程：尝试使用TEE系统软件层的调试功能。
通过标准：只有通过认证的用户方可使用TEE系统软件层的调试功能。

A.4.4 TA安全

A.4.4.1 安全审计

检测目的：验证 TA 提供方法记录安全相关事件的方法，以便帮助管理者发现潜在的攻击或发现由于 TA 安全特性的错误配置而陷入易被攻击的状态。
检测过程：审查厂商提交的文档，验证厂商已声明TA具备安全审计功能，并执行安全审计功能。
通过标准：TA具备安全审计功能，能够为相关可审计事件生成审计记录。

A.4.4.2 启动流程

检测目的：验证TA的启动流程具备自检的功能。

检测过程：审查厂商提交的文档，验证厂商已声明TA具备自检功能，并启动TA。

通过标准：TA的启动流程应具备自检功能，包括敏感信息和密钥的检查。

A.4.4.3 内存清除

检测目的：验证TA具备内存清除的功能。

检测过程：审查厂商提交的文档，验证厂商已声明TA具备内存清除功能，并使用TA处理敏感信息。

通过标准：TA在使用完敏感信息后应立即对其进行清除。

A.4.4.4 逻辑异常

检测目的：验证 TA 具有抵抗逻辑操纵和修改的结构，保护自己免受逻辑异常侵害。

检测过程：审查厂商提交的文档，验证厂商已声明TA具备逻辑异常的处理，对TA进行逻辑异常攻击。

通过标准：TA可以抵抗通过逻辑操作对安全特性的攻击，不会受到逻辑异常的影响而泄露任何敏感信息。

A.4.4.5 密钥使用

检测目的：验证TA具备安全使用密钥的能力。

检测过程：审查厂商提交的文档，验证厂商已声明TA对密钥的使用满足安全要求，并执行TA的密钥操作。

通过标准：TA对密钥的使用遵循TEE系统软件层的安全要求，或者根据密钥的用途使用。

A.4.4.6 生命周期

检测目的：验证TA具备检测当前生命周期状态和限制命令执行的能力。

检测过程：审查厂商提交的文档，验证厂商已声明TA具备生命周期管理功能，并在TA的不同生命周期执行命令。

通过标准：TA的设计和执行应保证命令只用于与之对应的生命周期中。

A.4.4.7 安全操作

检测目的：验证TA具备正确执行安全功能，且不受异常状态影响的能力。

检测过程：审查厂商提交的文档，验证厂商已声明TA能够正确执行安全功能，不受异常状态影响，并在异常状态下执行TA安全功能。

通过标准：TA能够遵循TEE系统软件层的安全要求正确执行安全功能，或者执行安全功能时能够不受异常状态影响。

A.4.4.8 可信存储

检测目的：验证TA具备安全存储数据和密钥的能力。

检测过程：审查厂商提交的文档，验证厂商已声明TA具备可信存储功能，并执行TA的可信存储。

通过标准：TA能够遵循TEE系统软件层的安全存储要求，或者能够对其存储的数据和密钥的机密性、真实性和一致性提供保护，同时对存储内容的修改操作具备原子性。TA的可信存储应与设备绑定，即数据只能由创建时同一设备、TEE上的经授权的同一TA进行访问和修改。

A.4.4.9 回滚保护

检测目的：验证TA具备防止未经授权回滚的能力。

检测过程：审查厂商提交的文档，验证厂商已声明TA具备回滚保护能力，并执行TA的回滚操作。

通过标准：只有通过认证的用户方可执行TA的回滚操作。

A.4.4.10 防重放

检测目的：验证TA具备防止重放攻击的能力。

检测过程：审查厂商提交的文档，验证厂商已声明TA具备防重放保护，并尝试进行重放攻击。

通过标准：TA能够保护其资源并防止重放攻击，当受到重放攻击时，能够作出相应的响应，其资产不会受到危害。

A.4.5 TEE外部设备安全

A.4.5.1 指纹模块-传感器

检测目的：验证指纹模块-传感器具备唯一识别ID，且不可被篡改。

检测过程：检查传感器是否具备唯一识别ID，该ID应体现型号及版本等信息，验证其无法被篡改。

通过标准：每颗传感器应具有唯一ID，表示其型号及版本信息，且不可被篡改。

A.4.5.2 指纹模块-硬件模块

A.4.5.2.1 合法性认证

检测目的：验证指纹模块-硬件模块具备合法性认证的能力。

检测过程：检查硬件模块与上游设备的合法性认证过程，验证该过程校验硬件模块的合法性，并且硬件模块具备唯一ID。

通过标准：指纹模块-硬件模块应有唯一ID，并且与其上游设备之间进行合法性认证。

A.4.5.2.2 指纹模板存储

检测目的：验证指纹模块-硬件模块或其上位机驱动对指纹模板的存储提供保护。

检测过程：检查指纹模板的存储过程，验证指纹模板是加密存储的，只有需要调用模板时才解密使用。

通过标准：指纹模板应加密储存，需要调用模板时解密使用。

A.4.5.2.3 数据传输安全

检测目的：验证指纹模块-硬件模块与上游设备之间的数据传输安全性。

检测过程：检查硬件模块与上游设备之间的数据传输协议，验证该协议能保证通信数据的机密性、完整性和真实性，能防止重放攻击，并且使用的安全协议版本不低于TLS 1.2。

通过标准：应保证通信数据的机密性、完整性和真实性，并能防止重放攻击，使用的安全协议版本应不低于TLS 1.2。

A.4.5.2.4 密钥管理

检测目的：验证指纹模块-硬件模块具备密钥管理能力。

检测过程：检查硬件模块的密钥体系，验证该体系的合理性以及用于加密指纹信息和进行设备合法性认证的密钥的有效性。

通过标准：指纹模块-硬件模块应建立合理的密钥体系，用于加密指纹信息和进行设备合法性认证。

A.4.5.2.5 密码算法

检测目的：验证指纹模块-硬件模块的密码算法满足相关算法标准（如3DES、RSA等）。

检测过程：检查对称密码或非对称密码算法是否符合相应的密码算法标准，验证使用的密钥长度符合安全要求。

通过标准：指纹模块-硬件模块应提供对应的对称和非对称算法功能，密钥长度应符合安全要求。

A.4.5.2.6 随机数

检测目的：验证指纹模块-硬件模块产生的随机数具备足够的随机性。

检测过程：验证指纹模块-硬件模块产生随机数的质量，进行GB/T 32915、AIS 20/AIS 31、NIST SP800-22或FIPS PUB 140-2标准化的测试。

通过标准：指纹模块-硬件模块产生的随机数满足标准化测试的要求。

A.4.5.2.7 固件更新

检测目的：验证指纹模块-硬件模块具备固件更新的能力。

检测过程：检查硬件模块的固件更新过程，验证该过程能够加密验证更新固件的完整性，并且在验证失败时，能够拒绝固件更新。

通过标准：指纹模块-硬件模块应加密验证更新固件的完整性，如果验证未通过，应拒绝固件更新。

A.4.5.2.8 逻辑异常

检测目的：验证指纹模块-硬件模块具备处理逻辑异常的能力。

检测过程：检查硬件模块的逻辑异常处理过程，验证其在处理逻辑异常时不会泄露敏感信息。

通过标准：指纹模块-硬件模块应不受逻辑异常的影响，包括但不限于非预期命令序列、未知命令、错误设备模式下的命令、错误参数或数据等。

A.4.5.2.9 内存清除

检测目的：验证指纹模块-硬件模块具备内存清除的能力。

检测过程：检查硬件模块的敏感信息处理过程，验证敏感信息使用完成后会立即清空内部保存的敏感信息。

通过标准：指纹模块-硬件模块的敏感信息在使用完成后，应及时清空其在内部保存的敏感信息。

A.5 REE安全检测

应满足JR/T 0098.3的要求。

A.6 安全单元SE检测

应满足JR/T 0098.5的要求。

A.7 集成安全检测

检测目的：验证移动终端的安全能力级别。

检测过程：根据移动终端集成的REE、TEE和SE的安全能力，评估移动终端的安全能力级别。

通过标准：移动终端的安全能力级别与其集成的REE、TEE和SE的安全能力一致。

附 录 B
（规范性附录）
检测规范扩展部分

B.1 TEE功能检测扩展部分

B.1.1 TUI

B.1.1.1 TUI PIN码输入

检测目的：验证TUI PIN码输入（如应用的支付验证、SE应用的用户验证、浏览敏感数据的权限认证、改变设备状态或能力的权限认证等）。
通过标准：正确实现PIN码由TUI传入。

B.1.1.2 TUI登录

检测目的：验证TUI登录功能的实现。
通过标准：正确实现登录认证。

B.1.1.3 敏感信息展示

检测目的：验证通过TUI正确展示敏感信息。
通过标准：实现敏感信息通过TUI正确展示。

B.1.1.4 第三方资源信息展示

检测目的：验证通过TUI正确展示包括远程服务、外部设备输出信息等第三方资源信息。
通过标准：正确实现第三方资源通过TUI进行信息展示。

B.1.2 生物识别设备

B.1.2.1 生物识别设备的认证

检测目的：验证通过生物识别设备进行身份认证。
通过标准：正确实现通过生物识别设备进行身份认证。

B.1.2.2 生物识别设备模板数据交互

检测目的：验证TEE与生物识别设备敏感模板数据（指纹样品模板）的交互。
通过标准：正确实现TEE与生物识别设备成功进行敏感数据交互。

B.1.3 TEE与SE的交互

B.1.3.1 TEE对SE的管理及SE相关信息的获取

检测目的：验证TEE能够正确获取SE的相关信息（如存在多SE的情况下可以选择指定SE）。
通过标准：TEE可以选择指定SE并获取相关信息。

B.1.3.2 TEE与SE的安全通道

检测目的：验证TEE与SE进行数据交互所需的安全通道的建立与关闭。

通过标准：TEE与SE进行数据交互时能成功建立安全通道并在通讯结束后进行关闭。

B.1.3.3 TEE与SE的数据交互

检测目的：验证TEE与SE能够通过APDU指令进行数据的交互。

通过标准：TEE与SE可以通过APDU指令进行数据的交互。

B.2 TEE安全检测扩展部分

B.2.1 TUI安全属性

检测目的：验证TEE系统软件层提供的TUI具有安全属性。

检测过程：TUI显示时，验证CA无法操作当前显示界面。验证TUI的显示内容无法通过截屏方式被获取到。

通过标准：CA无法操作TUI显示界面。TEE中只能通过TUI显示内容。

B.2.2 TUI安全输入和显示

检测目的：验证TEE系统软件层提供的TUI输入和显示具有安全防护的能力。

检测过程：CA或者非授权TA对TUI中用户输入信息和显示信息尝试访问时，应被阻止。

通过标准：TUI中用户输入信息和显示信息不能被CA或非授权TA读取和修改。

B.2.3 TUI安全标识

检测目的：验证TEE系统软件层提供的TUI具有提供安全标识的能力。

检测过程：当TUI处于显示状态或者使用TUI提供的键盘或虚拟键盘进行输入时，验证TEE系统软件层提供了安全标识，表明当前的显示界面处于安全显示状态。验证CA无法获取安全指示的信息。

通过标准：TUI正常工作时，TEE系统软件层提供了如指示灯、图片或声音等安全标识，表明当前显示已处于安全显示状态，且安全指示的信息无法被CA获取到。

B.2.4 TEE与SE之间的安全访问控制

检测目的：验证TEE具备为特定TA提供访问特定SE应用的能力。

检测过程：检查TEE为TA提供的SE应用访问控制策略，验证只有已授权的TA可以访问特定SE应用，其他TA无法访问。

通过标准：只有已授权的TA可以访问特定的SE应用，其他TA不能访问特定的SE应用。

B.2.5 TA和SE应用之间的安全通道

检测目的：验证TA和SE应用之间具备安全通道。

检测过程：检查TA和SE应用的通信过程，验证只有建立安全通道后，方可访问SE应用，通信过程应保证完整性。

通过标准：只有建立安全通道后，方可访问SE应用，通信过程应保证完整性。

附 录 C
（资料性附录）
手机银行应用场景

C.1 概述

本附录描述了承载于TEE和SE上的电子认证体系，对现有手机银行等业务的交易进行保护的场景进行描述。

C.2 环境初始化

对于TEE和SE的环境初始化过程可以采用预置和动态加载方式，初始化完成后，手机TEE和SE应该具备实现电子认证的服务能力。但无论采用哪种方式，均应该保证TEE及SE的环境出于商业银行的独立控制下。动态加载方式的具体流程如图C.1所示。

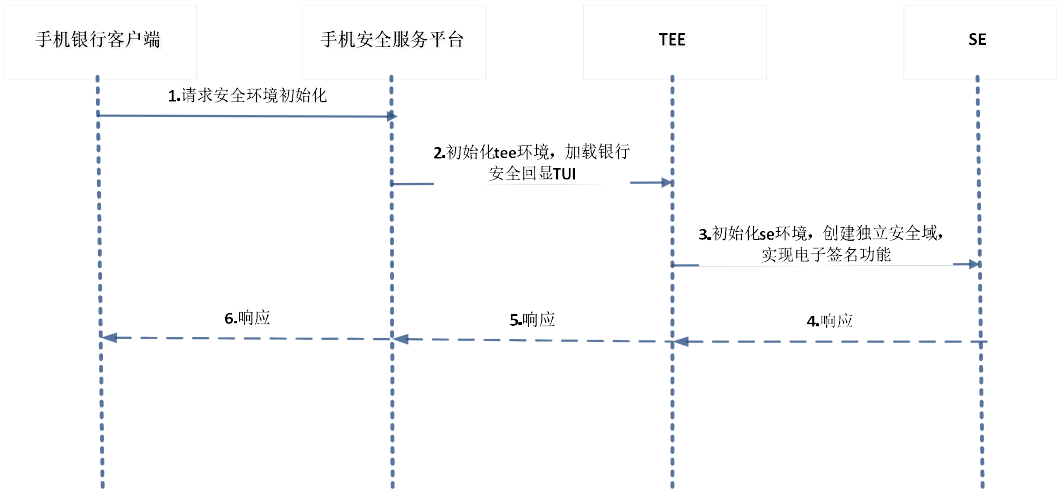

图 C.1 手机银行 TEE+SE 认证业务流程图

步骤1：用户通过客户端软件向手机安全服务平台请求安全环境初始化；

步骤2：手机安全服务平台向TEE进行环境初始化，并加载银行安全回显TUI；

步骤3：手机安全服务平台通过TEE向SE进行环境初始化，并创建属于银行的独立安全域，实现电子签名功能；

步骤4：SE完成初始化后，并返回结果给TEE；

步骤5：TEE将SE返回的结果及TEE环境初始化结果返回给安全服务平台；

步骤6：手机安全服务平台将结果返回给客户端软件，完成可信环境初始化工作。

C.3 手机银行交易签名/验签

在交易过程中采用TEE环境对手机银行交易信息进行确认，并由SE中存储的私钥对交易数据计算签名数据，并将签名数据、公钥证书、交易信息等一起返回给商业银行进行交易验证，完成交易。基于TEE和SE的电子认证交易的具体流程如图C.2所示。

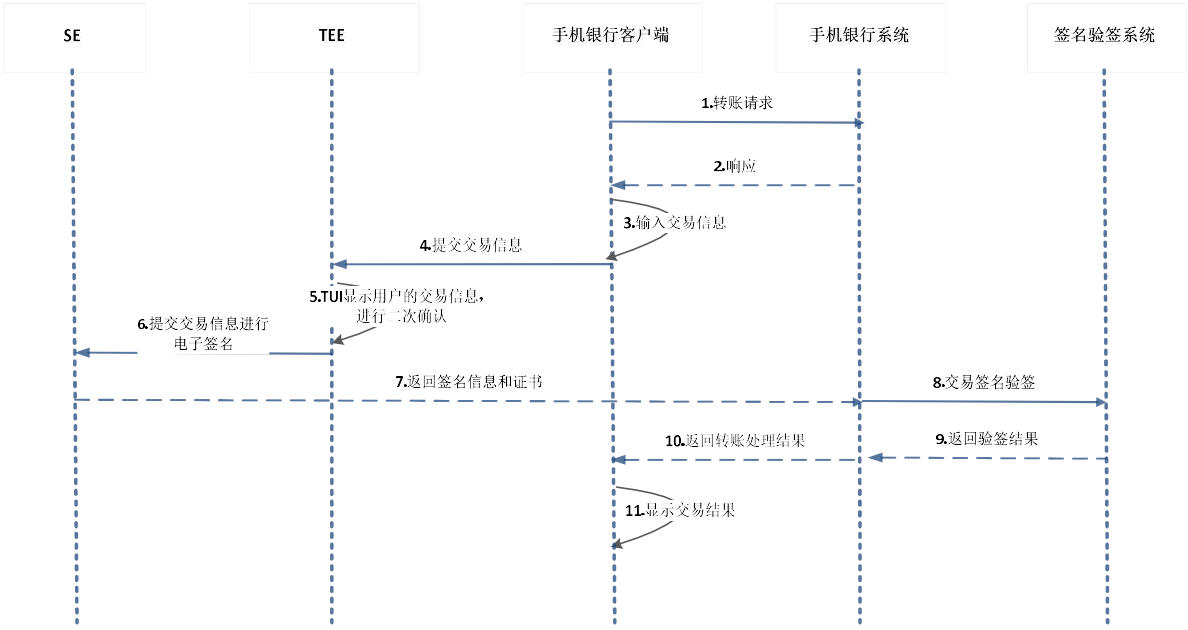

图 C.2 手机银行基于 TEE/SE 电子认证流程图

步骤1：用户通过客户端软件向手机银行系统发起转账请求；

步骤2：手机银行系统返回响应给客户端软件；

步骤3：用户根据客户端软件提示输入转入/转出账户信息、账户密码等信息，并确认交易；

步骤4：将交易信息发送给TEE系统，请求TUI回显；

步骤5：TEE系统中通过银行的TUI显示交易信息，用户进行二次确认；PBOC应用返回转账交易签名结果、公钥证书等认证数据给客户端软件；

步骤6：通过TUI确认后，将交易信息提交到SE进行交易签名，在SE内私钥进行签名处理；

步骤7：SE返回签名数据给手机银行系统；

步骤8：手机银行系统将签名数据和认证数据发送签名验签系统进行验签请求；

步骤9：手机银行签名验签系统返回转账交易验签结果；

步骤10：手机银行系统根据签名验证结果，完成交易处理，并返回转账交易结果给客户端软件；

步骤11：客户端软件将交易结果显示给用户。