

ICS 33.060  
M 60

**YD**

# 中华人民共和国通信行业标准

YD/T 2778-2014

---

## 手机支付 可信服务管理平台测试方法

Mobile payment test methods for  
trusted service management platform

2014-12-24 发布

2014-12-24 实施

---

中华人民共和国工业和信息化部 发布



## 目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
3.1 术语和定义	1
3.2 缩略语	1
4 测试环境设备	2
4.1 测试网络拓扑	2
4.2 测试设备	2
5 可信服务管理平台功能测试	2
5.1 安全域管理	2
5.2 应用管理	3
5.3 用户管理	4
5.4 应用提供商管理	7
5.5 业务管理	9
5.6 SE管理	11

## 前 言

本标准按照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。本文件的发布机构不承担识别这些专利的责任。

本标准是移动支付系列标准之一。该系列标准的名称预计如下：

1. 手机支付 术语和定义
2. 手机支付 总体技术要求
3. 手机支付 基于13.56MHz近场通信技术的移动终端技术要求
4. 手机支付 基于13.56MHz近场通信技术的智能卡和内置安全模块技术要求
5. 手机支付 基于2.45GHz射频技术的智能卡技术要求
6. 手机支付 基于13.56MHz近场通信技术的非接触式销售点终端技术要求
7. 手机支付 基于2.45GHz射频技术的非接触式销售点终端技术要求
8. 手机支付 基于13.56MHz和2.45GHz双频的非接销售点终端技术要求
9. 手机支付 基于13.56MHz 近场通信技术的非接触射频接口技术要求
10. 手机支付 基于2.45GHz 射频技术的非接触射频接口技术要求
11. 手机支付 智能卡和内置模块安全技术要求
12. 手机支付 移动终端安全技术要求
13. 手机支付 可信服务管理平台技术要求
14. 手机支付 基于13.56MHz近场通信技术的移动终端测试方法
15. 手机支付 基于13.56MHz近场通信技术的智能卡和内置安全模块测试方法
16. 手机支付 基于2.45GHz射频技术的智能卡测试方法
17. 手机支付 基于13.56MHz近场通信技术的非接触式销售点终端测试方法
18. 手机支付 基于2.45GHz射频技术的非接触式销售点终端测试方法
19. 手机支付 基于13.56MHz和2.45GHz的双频非接销售点终端测试方法
20. 手机支付 基于13.56MHz近场通信技术的非接触射频接口测试方法
21. 手机支付 基于2.45GHz射频技术的非接触射频接口测试方法
22. 手机支付 智能卡和内置模块安全测试方法
23. 手机支付 移动终端安全测试方法
24. 手机支付 可信服务管理平台测试方法

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院、中国电信集团公司、中国移动通信集团公司、中国联通网络通信集团公司。

本标准主要起草人：逢淑宁、袁 琦、王 逊、姜志峰、王文超、陆 鸣、张 强、纪洪明。

# 手机支付

## 可信服务管理平台测试方法

### 1 范围

本标准规定了可信服务管理平台测试方法，主要包括安全域管理测试、应用管理测试、用户管理测试、应用提供商管理测试、业务管理测试、SE 管理测试。

本标准适用于可信服务管理平台。

### 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。

手机支付 可信服务管理平台技术要求

### 3 术语、定义和缩略语

#### 3.1 术语和定义

下列术语和定义适用于本文件。

##### 3.1.1

**安全域 Security Domain**

是一种具有特殊权限的应用。每个安全域负责管理自己的密钥，以确保来自于不同应用提供方的应用及数据可以在同一张卡片上共存，而不会破坏彼此的机密性及完整性。

##### 3.1.2

**主安全域 Issuer Security Domain**

也称“发卡方安全域”，作为发卡方对卡片内容进行管理时的操作代理，卡片必须实现此安全域应用。发卡方可以利用此授权程序加载、安装、删除发卡方或其他应用提供方的应用。发卡方安全域同卡上其他的安全域很相似。

##### 3.1.3

**辅助安全域 Supplementary Security Domian**

类似发卡方安全域，是某个应用提供方或控制机构在卡上的安全域。

##### 3.1.4

**发卡方 Card Issuer**

发放安全模块的发行和管理机构。安全模块可置于智能卡或终端中。

#### 3.2 缩略语

下列缩略语适用于本文件：

NFC	Near Field Communication	近场通信
SE	Secure Element	安全模块
SWP	Single Wire Protocol	单线协议



4 测试环境设备

4.1 测试网络拓扑

可信服务管理平台测试拓扑如图1所示。

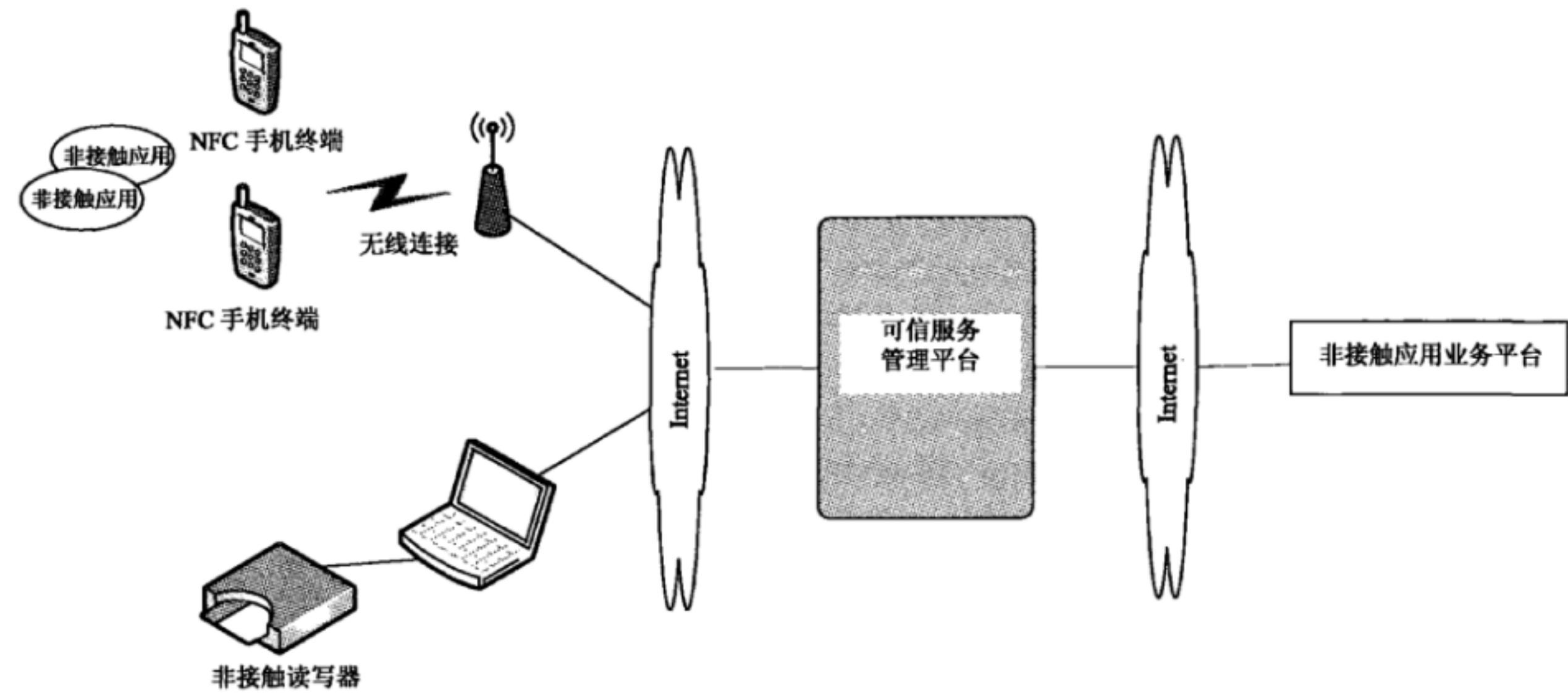


图 1 可信服务管理平台测试拓扑

被测对象是可信服务管理平台。可信服务管理平台通过Internet接入非接触业务应用平台，并向非接触业务应用平台提供非接触应用发行业务（例如公交卡、银行卡等卡模拟应用）。NFC手机终端通过WLAN或移动蜂窝等无线接入网络连接可信服务管理平台，实现SE及非接触应用的管理，其中NFC手机终端包括SWP方式支持近场支付的NFC手机终端和全终端方式支持近场支付的NFC手机终端；此外NFC手机终端也可通过非接触读写器连接可信服务管理平台，实现SE及非接触应用的管理。

4.2 测试设备

SWP方式支持近场支付的NFC手机终端	一台
全终端方式支持近场支付的NFC手机终端	一台
非接触应用（例如公交卡、银行卡等卡模拟应用）	若干
非接触应用业务平台	一套
专用非接触读写器	一台

5 可信服务管理平台功能测试

5.1 安全域管理

测试编号： 5.1
测试项目： 安全域管理
测试目的： 验证可信服务平台支持对安全域管理功能
预置条件： 1) 按照图 1 进行正确连接； 2) 系统管理员或业务管理员可以登陆可信服务管理平台
测试步骤： 以系统管理员或业务管理员身份登录到可信服务管理平台，查看和分配安全域的 AID。
预期结果： 可信服务管理平台可查看和分配安全域的 AID

## 5.2 应用管理

### 5.2.1 应用生命周期管理

测试编号： 5.2.1
测试项目：应用生命周期管理
测试目的：验证可信服务平台支持对应用生命周期管理功能
预置条件： 1) 按照图 1 进行正确连接； 2) 系统管理员或业务管理员可以登陆可信服务管理平台； 3) 可信服务管理平台中具有非接触应用（例如公交卡、银行卡等卡模拟应用）
测试步骤： 1) 以系统管理员或业务管理员身份登录到可信服务管理平台，选择一个非接触应用（例如公交卡、银行卡等卡模拟应用）； 2) 对应用进行配置、上载、审核、测试、发布、更新和归档操作
预期结果： 可对应用生命周期进行管理，应用进行配置、上载、审核、测试、发布、更新和归档操作成功

### 5.2.2 应用操作权限管理

测试编号： 5.2.2
测试项目：应用操作权限管理
测试目的：验证可信服务平台支持对应用操作权限管理功能
预置条件： 1) 按照图 1 进行正确连接； 2) 系统管理员或业务管理员可以登陆可信服务管理平台； 3) 应用提供商已在可信服务管理平台中上传了非接触应用（例如公交卡、银行卡等卡模拟应用）
测试步骤： 1) 以系统管理员或业务管理员身份登录到可信服务管理平台，选择一个非接触应用（例如公交卡、银行卡等卡模拟应用）； 2) 对应用提供商进行接口操作该非接触应用的权限配置
预期结果： 可对应用提供商进行接口操作非接触应用的权限配置，包括能否发起应用下载请求、能否发起应用删除请求、能否发起设置应用状态请求，应用个人化请求操作

5.3 用户管理

5.3.1 用户信息管理

测试编号： 5.3.1
测试项目：用户基本信息管理
测试目的：验证可信服务平台支持对用户的基本信息管理功能
预置条件： 1) 按照图 1 进行正确连接； 2) 系统管理员或业务管理员可以登陆可信服务管理平台； 3) 可信服务管理平台已录入用户信息
测试步骤： 1) 以系统管理员或业务管理员身份登录到可信服务管理平台，查看是否提供用户基本信息管理界面； 2) 在用户基本信息管理界面中查看和修改用户身份、联系方式等个人信息
预期结果： 1) 可信服务管理平台能够提供用户基本信息管理界面。 2) 可以成功查看和修改个人信息

5.3.2 用户自服务

5.3.2.1 手机支付客户端方式

测试编号： 5.3.2.1.1
测试项目：用户自服务操作的用户应用发现
测试目的：验证可信服务平台支持用户的应用发现功能
预置条件： 1) 按照图 1 进行正确连接； 2) 可信服务管理平台中有可供下载的非接触应用
测试步骤： 用户通过 NFC 手机终端（SWP 方式支持近场支付的 NFC 手机终端/全终端方式支持近场支付的 NFC 手机终端）手机支付客户端登录到可信服务管理平台，查看适配用户 SE 的可下载应用
预期结果： 用户可以成功查看可下载的应用



测试编号： 5.3.2.1.2
测试项目：用户自服务操作的业务操作功能
测试目的：验证可信服务平台支持用户的业务操作功能
预置条件： 1) 按照图 1 进行正确连接； 2) 可信服务管理平台中有可供下载的非接触应用
测试步骤： 用户通过 NFC 手机终端（SWP 方式支持近场支付的 NFC 手机终端/全终端方式支持近场支付的 NFC 手机终端）手机支付客户端登录到可信服务管理平台，使用应用下载、删除、更新和锁定功能等
预期结果： 用户可以使用应用下载、删除、更新和锁定等功能操作

测试编号： 5.3.2.1.3
测试项目：用户自服务操作的查询功能
测试目的：验证可信服务平台支持用户的查询功能
预置条件： 1) 按照图 1 进行正确连接； 2) 可信服务管理平台中有用户的应用下载等业务操作记录
测试步骤： 用户通过 NFC 手机终端（SWP 方式支持近场支付的 NFC 手机终端/全终端方式支持近场支付的 NFC 手机终端）手机支付客户端登录到可信服务管理平台，查询已下载应用、使用空间、可用空间、SE 设备信息、应用的相关信息和自己的操作记录等
预期结果： 用户可以成功查询已下载应用、使用空间、可用空间、SE 设备信息、应用的相关信息和自己的操作记录等

## 5.3.2.2 门户网站方式（可选）

测试编号： 5.3.2.2.1
测试项目：用户自服务操作的用户应用发现
测试目的：验证可信服务平台支持用户的应用发现功能
预置条件： 1) 按照图 1 进行正确连接； 2) 可信服务管理平台中有可供下载的非接触应用
测试步骤： 用户登录到可信服务管理平台门户网站，查看适配用户 SE 的可下载应用
预期结果： 用户可以成功查看可下载的应用

测试编号： 5.3.2.2.2
测试项目：用户自服务操作的业务操作功能
测试目的：验证可信服务平台支持用户的业务操作功能
预置条件： 1) 按照图 1 进行正确连接； 2) 可信服务管理平台中有可供下载的非接触应用
测试步骤： 用户登录到可信服务管理平台门户网站，使用应用下载、删除、更新和锁定功能等
预期结果： 用户可以使用应用下载、删除、更新和锁定等功能操作

测试编号： 5.3.2.2.3
测试项目：用户自服务操作的查询功能
测试目的：验证可信服务平台支持用户的查询功能
预置条件： 1) 按照图 1 进行正确连接； 2) 可信服务管理平台中有用户的应用下载等业务操作记录
测试步骤： 用户登录到可信服务管理平台门户网站，查询已下载应用、使用空间、可用空间、SE 设备信息、应用的相关信息和自己的操作记录等
预期结果： 用户可以成功查询已下载应用、使用空间、可用空间、SE 设备信息、应用的相关信息和自己的操作记录等

## 5.4 应用提供商管理

### 5.4.1 基本信息管理

测试编号： 5.4.1
测试项目：应用提供商基本信息管理
测试目的：验证可信服务平台支持对应用提供商的注册及审核功能
预置条件： 按照图 1 进行正确连接
测试步骤： 1) 应用提供商登录到可信服务管理平台的门户页面，查看是否提供应用提供商注册界面； 2) 在注册界面中填写应用提供商注册信息并提交； 3) 以系统管理员或业务管理员身份进入可信服务管理平台，查看是否提供应用提供商注册审核管理界面； 4) 在应用提供商注册审核管理界面中，对提供符合要求信息的应用提供商，进行审核通过操作，对提供不符合要求信息的应用提供商，进行审核不通过操作
预期结果： 1) 可信服务管理平台能够提供应用提供商注册界面； 2) 对提供符合要求信息的应用提供商，可信服务管理平台审核通过，应用提供商注册成功； 3) 对提供不符合要求信息的应用提供商，可信服务管理平台审核不通过，应用提供商注册失败

### 5.4.2 安全域申请

测试编号： 5.4.2
测试项目：应用提供商安全域申请
测试目的：验证可信服务平台支持应用提供商的安全域申请功能
预置条件： 1) 按照图 1 进行正确连接； 2) 应用提供商在可信服务管理平台已注册账号
测试步骤： 1) 应用提供商使用已注册账号登录到可信服务管理平台，查看是否提供安全域申请界面； 2) 在安全域申请界面中填写安全域申请信息并提交； 3) 以系统管理员或业务管理员身份进入可信服务管理平台，查看是否提供应用提供商安全域申请审核管理界面； 4) 在应用提供商安全域申请审核管理界面中，对提供正确信息的应用提供商，进行审核通过操作，对提供不正确信息的应用提供商，进行审核不通过操作
预期结果： 1) 可信服务管理平台能够提供安全域申请界面； 2) 对提供正确信息的应用提供商，可信服务管理平台审核通过，应用提供商申请安全域成功； 3) 对提供不正确信息的应用提供商，可信服务管理平台审核不通过，应用提供商申请安全域失败



## 5.4.3 应用申请

测试编号： 5.4.3
测试项目：应用提供商应用申请
测试目的：验证可信服务平台支持应用提供商的应用申请功能
预置条件： 1) 按照图 1 进行正确连接； 2) 应用提供商在可信服务管理平台已注册账号
测试步骤： 1) 应用提供商使用已注册账号登录到可信服务管理平台，查看是否提供应用申请界面； 2) 通过应用申请界面提交一个非接触应用； 3) 以系统管理员或业务管理员身份进入可信服务管理平台，对应用申请进行审核
预期结果： 1) 可信服务管理平台能够提供应用申请界面； 2) 非接触应用被提交至可信服务管理平台，应用提供商的应用申请成功。

## 5.4.4 应用提供商自服务

测试编号： 5.4.4.1
测试项目：应用提供商自服务操作的所属安全域信息查询和配置
测试目的：验证可信服务平台支持应用提供商对所属安全域信息查询和配置功能
预置条件： 1) 按照图 1 进行正确连接； 2) 应用提供商在可信服务管理平台已注册账号
测试步骤： 1) 应用提供商使用已注册账号登录到可信服务管理平台，查看是否提供所属安全域管理界面； 2) 应用提供商查询所属安全域信息； 3) 应用提供商配置所属安全域信息
预期结果： 1) 可信服务平台提供所属安全域管理界面； 2) 应用提供商能够成功查询所属安全域信息； 3) 应用提供商能够成功配置所属安全域信息

测试编号： 5.4.4.2
测试项目：应用提供商自服务操作的所属应用信息查询和配置
测试目的：验证可信服务平台支持应用提供商对所属应用信息查询和配置功能
预置条件： 1) 按照图 1 进行正确连接； 2) 应用提供商在可信服务管理平台已注册账号
测试步骤： 1) 应用提供商使用已注册账号登录到可信服务管理平台，查看是否提供所属应用管理界面； 2) 应用提供商查询所属应用信息； 3) 应用提供商配置所属应用信息； 4) 应用提供商升级所属应用
预期结果： 1) 可信服务平台提供所属应用管理界面； 2) 应用提供商能够成功查询所属应用信息； 3) 应用提供商能够成功配置所属应用信息； 4) 应用提供商能够成功升级所属应用

## 5.5 业务管理

### 5.5.1 业务数据管理

测试编号： 5.5.1
测试项目：业务数据管理
测试目的：验证可信服务平台支持对业务数据管理功能
预置条件： 1) 按照图 1 进行正确连接； 2) 系统管理员或业务管理员可以登陆可信服务管理平台
测试步骤： 1) 以系统管理员或业务管理员身份登录到可信服务管理平台，查看是否提供业务数据管理界面； 2) 2、在业务数据管理界面中查看和配置应用提供商、应用、安全域和签约关系等数据
预期结果： 1) 可信服务管理平台能够提供业务数据管理界面； 2) 系统管理员或业务管理员可以成功查看和配置应用提供商、应用、安全域和签约关系等数据



## 5.5.2 鉴权与授权

测试编号： 5.5.2
测试项目：鉴权与授权
测试目的：验证可信服务平台支持对业务的鉴权与授权功能
预置条件： <ol style="list-style-type: none"> <li>1) 按照图 1 进行正确连接；</li> <li>2) 应用提供商在可信服务管理平台已注册账号；</li> <li>3) 系统管理员或业务管理员可查看可信服务管理平台后台日志</li> </ol>
测试步骤： <ol style="list-style-type: none"> <li>1) 应用提供商使用已注册账号登录到可信服务管理平台，提交一个非接触应用进行应用发行操作；</li> <li>2) 系统管理员或业务管理员查看可信服务管理平台后台日志</li> </ol>
预期结果： <ol style="list-style-type: none"> <li>1) 后台日志中可查看可信服务管理平台对应用提供商、业务平台、签约关系进行鉴权的信息；</li> <li>2) 后台日志中可查看可信服务管理平台对业务平台调用的应用发行能力进行授权的信息</li> </ol>

## 5.5.3 系统管理

测试编号： 5.5.3
测试项目：系统管理
测试目的：验证可信服务平台支持系统管理功能
预置条件： <ol style="list-style-type: none"> <li>1) 按照图 1 进行正确连接；</li> <li>2) 拥有系统管理员登陆账号</li> </ol>
测试步骤： <ol style="list-style-type: none"> <li>1) 以系统管理员身份登录到可信服务管理平台，查看是否提供系统管理界面；</li> <li>2) 在系统管理界面中查询、增加、修改和删除业务管理员；</li> <li>3) 3、在系统管理界面中分配业务管理员角色权限</li> </ol>
预期结果： <ol style="list-style-type: none"> <li>1) 可信服务管理平台能够提供系统管理界面；</li> <li>2) 能够查询、增加、修改和删除业务管理员；</li> <li>3) 能够分配业务管理员角色权限</li> </ol>

## 5.6 SE 管理

### 5.6.1 SE 数据信息

测试编号： 5.6.1
测试项目：SE 数据信息管理
测试目的：验证可信服务平台支持对 SE 数据信息管理功能
预置条件： 1) 按照图 1 进行正确连接； 2) NFC 手机终端（SWP 方式支持近场支付的 NFC 手机终端/全终端方式支持近场支付的 NFC 手机终端）通过手机支付客户端或专用非接触读写器与可信服务管理平台连接； 3) 系统管理员或业务管理员可以登陆可信服务管理平台
测试步骤： 以系统管理员或业务管理员身份登录到可信服务管理平台，查看 SE 数据信息
预期结果： 可查看 SE 数据信息，SE 数据信息包括批次、密钥等静态信息以及已下载应用和可用空间等动态信息

### 5.6.2 SE 管理渠道

测试编号： 5.6.2
测试项目：SE 管理渠道
测试目的：验证可信服务平台支持非接触读卡器方式和空中两种 SE 管理渠道
预置条件： 1) 按照图 1 进行正确连接； 2) NFC 手机终端中（SWP 方式支持近场支付的 NFC 手机终端/全终端方式支持近场支付的 NFC 手机终端）安装了手机支付客户端
测试步骤： 1) 启动 NFC 手机终端中的手机支付客户端，查看 NFC 手机终端与可信服务管理平台的连接情况； 2) NFC 手机终端与专用非接触读写器进行刷卡操作，查看 NFC 手机终端与可信服务管理平台的连接情况
预期结果： 1) NFC 手机终端可通过手机支付客户端与可信服务管理平台连接。 2) NFC 手机终端可通过专用非接触读写器与可信服务管理平台连接

## 5.6.3 SE 安全域管理

## 5.6.3.1 安全域创建

测试编号： 5.6.3.1
测试项目：SE 辅助安全域创建
测试目的：验证可信服务平台支持对 SE 辅助安全域创建功能
预置条件： <ol style="list-style-type: none"> <li>1) 按照图 1 进行正确连接；</li> <li>2) NFC 手机终端（SWP 方式支持近场支付的 NFC 手机终端/全终端方式支持近场支付的 NFC 手机终端）通过手机支付客户端或专用非接触读写器与可信服务管理平台连接；</li> <li>3) 应用提供商使用已注册账号登录到可信服务管理平台；</li> <li>4) 系统管理员或业务管理员可查看可信服务管理平台后台日志</li> </ol>
测试步骤： <ol style="list-style-type: none"> <li>1) 应用提供商通过可信服务管理平台进行安全域创建申请；</li> <li>2) 应用提供商通过可信服务管理平台自服务操作查询所属安全域信息；</li> <li>3) 系统管理员或业务管理员查看可信服务管理平台后台日志</li> </ol>
预期结果： <ol style="list-style-type: none"> <li>1) SE 辅助安全域创建成功，应用提供商可查看到此 SE 辅助安全域信息；</li> <li>2) 后台日志中记录的安全域创建操作流程符合《可信服务管理平台技术要求》第 7.4 节中的流程图</li> </ol>

## 5.6.3.2 安全域删除

测试编号： 5.6.3.2
测试项目：SE 辅助安全域删除
测试目的：验证可信服务平台支持对 SE 辅助安全域删除功能
预置条件： <ol style="list-style-type: none"> <li>1) 按照图 1 进行正确连接；</li> <li>2) NFC 手机终端（SWP 方式支持近场支付的 NFC 手机终端/全终端方式支持近场支付的 NFC 手机终端）通过手机支付客户端或专用非接触读写器与可信服务管理平台连接；</li> <li>3) 应用提供商使用已注册账号登录到可信服务管理平台；</li> <li>4) 应用提供商已创建 SE 辅助安全域；</li> <li>5) 系统管理员或业务管理员可查看可信服务管理平台后台日志</li> </ol>
测试步骤： <ol style="list-style-type: none"> <li>1) 应用提供商通过可信服务管理平台选择一个 SE 辅助安全域，进行安全域删除申请；</li> <li>2) 应用提供商通过可信服务管理平台查询所属安全域信息；</li> <li>3) 系统管理员或业务管理员查看可信服务管理平台后台日志</li> </ol>
预期结果： <ol style="list-style-type: none"> <li>1) SE 辅助安全域删除成功，应用提供商查询所属安全域信息中不包括此 SE 辅助安全域信息；</li> <li>2) 后台日志中记录的安全域删除操作流程符合《可信服务管理平台技术要求》第 7.5 节中的流程图</li> </ol>



## 5.6.3.3 安全域密钥更新

测试编号: 5.6.3.3.1
测试项目: SE 主安全域密钥更新
测试目的: 验证可信服务平台支持对 SE 主安全域密钥更新功能
预置条件: 1) 按照图 1 进行正确连接; 2) NFC 手机终端 (SWP 方式支持近场支付的 NFC 手机终端/全终端方式支持近场支付的 NFC 手机终端) 通过手机支付客户端或专用非接触读写器与可信服务管理平台连接; 3) 系统管理员或业务管理员可以登陆可信服务管理平台; 4) 系统管理员或业务管理员可查看可信服务管理平台后台日志
测试步骤: 1) 系统管理员或业务管理员通过可信服务管理平台选择 SE 主安全域, 进行安全域密钥更新申请, 并提供一个安全域密钥; 2) 系统管理员或业务管理员通过可信服务管理平台查询 SE 主安全域信息; 3) 系统管理员或业务管理员查看可信服务管理平台后台日志
预期结果: 1) SE 主安全域密钥更新成功, 系统管理员或业务管理员可查看到此 SE 主安全域信息, 其中密钥为更新后的安全域密钥; 2) 后台日志中记录的安全域密钥更新操作流程符合《可信服务管理平台技术要求》第 7.6 节中的流程图

测试编号: 5.6.3.3.2
测试项目: SE 辅助安全域密钥更新
测试目的: 验证可信服务平台支持对 SE 辅助安全域密钥更新功能
预置条件: 1) 按照图 1 进行正确连接; 2) NFC 手机终端 (SWP 方式支持近场支付的 NFC 手机终端/全终端方式支持近场支付的 NFC 手机终端) 通过手机支付客户端或专用非接触读写器与可信服务管理平台连接; 3) 应用提供商使用已注册账号登录到可信服务管理平台; 4) 应用提供商已创建 SE 辅助安全域; 5) 系统管理员或业务管理员可查看可信服务管理平台后台日志
测试步骤: 1) 应用提供商通过可信服务管理平台选择一个 SE 辅助安全域, 进行安全域密钥更新申请, 并提供一个安全域密钥; 2) 应用提供商通过可信服务管理平台查询所属安全域信息; 3) 系统管理员或业务管理员查看可信服务管理平台后台日志
预期结果: 1) SE 辅助安全域密钥更新成功, 应用提供商可查看到此 SE 辅助安全域信息, 其中密钥为更新后的安全域密钥; 2) 后台日志中记录的安全域密钥更新操作流程符合《可信服务管理平台技术要求》第 7.6 节中的流程图

## 5.6.3.4 安全域锁定/解锁

测试编号: 5.6.3.4.1
测试项目: SE 主安全域锁定/解锁
测试目的: 验证可信服务平台支持对 SE 主安全域锁定/解锁功能
预置条件: 1) 按照图 1 进行正确连接; 2) NFC 手机终端 (SWP 方式支持近场支付的 NFC 手机终端/全终端方式支持近场支付的 NFC 手机终端) 通过手机支付客户端或专用非接触读写器与可信服务管理平台连接; 3) 系统管理员或业务管理员可以登陆可信服务管理平台
测试步骤: 1) 系统管理员或业务管理员通过可信服务管理平台选择 SE 主安全域, 进行安全域锁定申请; 2) 系统管理员或业务管理员通过可信服务管理平台查询 SE 主安全域信息; 3) 系统管理员或业务管理员通过可信服务管理平台选择 SE 主安全域, 进行安全域解锁申请; 4) 系统管理员或业务管理员通过可信服务管理平台查询 SE 主安全域信息
预期结果: 1) 步骤 1) 后, SE 主安全域锁定成功, 步骤 2) 后系统管理员或业务管理员可查看到此 SE 主安全域信息, 其中安全域状态为锁定; 2) 步骤 3) 后, SE 主安全域解锁成功, 步骤 4) 后系统管理员或业务管理员可查看到此 SE 主安全域信息, 其中安全域状态为未锁定

测试编号: 5.6.3.4.2
测试项目: SE 辅助安全域锁定/解锁
测试目的: 验证可信服务平台支持对 SE 辅助安全域锁定/解锁功能
预置条件: 1) 按照图 1 进行正确连接; 2) NFC 手机终端 (SWP 方式支持近场支付的 NFC 手机终端/全终端方式支持近场支付的 NFC 手机终端) 通过手机支付客户端或专用非接触读写器与可信服务管理平台连接; 3) 应用提供商使用已注册账号登录到可信服务管理平台; 4) 应用提供商已创建 SE 辅助安全域
测试步骤: 1) 应用提供商通过可信服务管理平台选择一个 SE 辅助安全域, 进行安全域锁定申请; 2) 应用提供商通过可信服务管理平台查询所属安全域信息; 3) 应用提供商通过可信服务管理平台选择一个 SE 辅助安全域, 进行安全域解锁申请; 4) 应用提供商通过可信服务管理平台查询所属安全域信息
预期结果: 1) 步骤 1) 后, SE 辅助安全域锁定成功, 步骤 2) 后应用提供商可查看到此 SE 辅助安全域信息, 其中安全域状态为锁定; 2) 步骤 3) 后, SE 辅助安全域解锁成功, 步骤 4) 后应用提供商可查看到此 SE 辅助安全域信息, 其中安全域状态为未锁定



## 5.6.4 SE 生命周期管理

测试编号: 5.6.4
测试项目: SE 生命周期管理
测试目的: 验证可信服务平台支持对 SE 生命周期查询功能
预置条件: 1) 按照图 1 进行正确连接; 2) NFC 手机终端 (SWP 方式支持近场支付的 NFC 手机终端/全终端方式支持近场支付的 NFC 手机终端) 通过手机支付客户端或专用非接触读写器与可信服务管理平台连接; 3) 系统管理员或业务管理员可以登陆可信服务管理平台
测试步骤: 1) 以系统管理员或业务管理员身份登录到可信服务管理平台, 对 SE 状态进行查看。 2) 系统管理员或业务管理员通过可信服务管理平台进行 SE 锁定操作; 3) 系统管理员或业务管理员通过可信服务管理平台查询 SE 状态; 4) 系统管理员或业务管理员通过可信服务管理平台进行 SE 解锁操作; 5) 系统管理员或业务管理员通过可信服务管理平台查询 SE 状态
预期结果: 1) 步骤 1) 后可查看 SE 状态为 SECURED ; 2) 步骤 3) 后可查看 SE 状态为 CARD_LOCKED; 3) 步骤 5) 后可查看 SE 状态为 SECURED

## 5.6.5 SE 应用管理

## 5.6.5.1 应用发行

测试编号: 5.6.5.1
测试项目: SE 应用发行
测试目的: 验证可信服务平台支持对 SE 应用发行功能
预置条件: 1) 按照图 1 进行正确连接; 2) NFC 手机终端 (SWP 方式支持近场支付的 NFC 手机终端/全终端方式支持近场支付的 NFC 手机终端) 通过手机支付客户端或专用非接触读写器与可信服务管理平台连接; 3) 可查看可信服务管理平台后台日志
测试步骤: 1) 操作员通过手机支付客户端或专用非接触读写器, 获取可信服务管理平台中应用列表; 2) 操作员请求下载一个非接触应用, 可信服务管理平台获取用户请求后, 下载应用; 3) 操作员以系统管理员或业务管理员身份进入可信服务管理平台, 检查用户 SE 状态; 4) 查看可信服务管理平台后台日志
预期结果: 1) 手机支付客户端或专用非接触读写器显示应用列表; 2) 非接触应用下载成功且个人化成功; 3) 可信服务管理平台显示 SE 中状态为 “已个人化”, SE 减少空间为应用的大小; 4) 后台日志中记录的应用下载操作流程符合《可信服务管理平台技术要求》第 7.1.1 节中的流程图; 5) 后台日志中记录的应用个人化操作流程符合《可信服务管理平台技术要求》第 7.1.2 节中的流程图

## 5.6.5.2 应用删除

测试编号： 5.6.5.2
测试项目： SE 应用删除
测试目的： 验证可信服务平台支持对 SE 应用删除功能
<p>预置条件：</p> <ol style="list-style-type: none"> <li>1) 按照图 1 进行正确连接；</li> <li>2) NFC 手机终端（SWP 方式支持近场支付的 NFC 手机终端/全终端方式支持近场支付的 NFC 手机终端）通过手机支付客户端或专用非接触读写器与可信服务管理平台连接；</li> <li>3) 可查看可信服务管理平台后台日志</li> </ol>
<p>测试步骤：</p> <ol style="list-style-type: none"> <li>1) 操作员通过手机支付客户端或专用非接触读写器，获取可信服务管理平台中用户已下载应用列表；</li> <li>2) 操作员请求删除一个非接触应用，可信服务管理平台发起对此非接触应用的删除；</li> <li>3) 操作员以系统管理员或业务管理员身份进入可信服务管理平台，检查用户 SE 状态；</li> <li>4) 查看可信服务管理平台后台日志</li> </ol>
<p>预期结果：</p> <ol style="list-style-type: none"> <li>1) 手机支付客户端或专用非接触读写器显示已下载应用列表；</li> <li>2) 非接触应用删除成功；</li> <li>3) 可信服务管理平台显示 SE 中不包含被删除的应用；</li> <li>4) 后台日志中记录的应用删除操作流程符合《可信服务管理平台技术要求》第 7.2 节中的流程图。</li> </ol>

## 5.6.5.3 应用锁定/解锁

测试编号： 5.6.5.3
测试项目： SE 应用锁定/解锁
测试目的： 验证可信服务平台支持对 SE 应用锁定/解锁功能
<p>预置条件：</p> <ol style="list-style-type: none"> <li>1) 按照图 1 进行正确连接；</li> <li>2) NFC 手机终端（SWP 方式支持近场支付的 NFC 手机终端/全终端方式支持近场支付的 NFC 手机终端）通过手机支付客户端或专用非接触读写器与可信服务管理平台连接；</li> <li>3) 可查看可信服务管理平台后台日志</li> </ol>
<p>测试步骤：</p> <ol style="list-style-type: none"> <li>1) 操作员通过手机支付客户端或专用非接触读写器，获取可信服务管理平台中用户已下载应用列表；</li> <li>2) 操作员请求锁定一个非接触应用，可信服务管理平台发起对此非接触应用的锁定；</li> <li>3) 操作员以系统管理员或业务管理员身份进入可信服务管理平台，检查用户 SE 状态；</li> <li>4) 操作员请求解锁步骤 2) 中被锁定的非接触应用，可信服务管理平台发起对此非接触应用的解锁；</li> <li>5) 操作员以系统管理员或业务管理员身份进入可信服务管理平台，检查用户 SE 状态；</li> <li>6) 查看可信服务管理平台后台日志</li> </ol>
<p>预期结果：</p> <ol style="list-style-type: none"> <li>1) 手机支付客户端或专用非接触读写器显示已下载应用列表；</li> <li>2) 步骤 2) 后，非接触应用锁定成功；</li> <li>3) 步骤 3) 后，可信服务管理平台显示 SE 中此应用被锁定；</li> <li>4) 步骤 4) 后，非接触应用解锁成功；</li> <li>5) 步骤 5) 后，可信服务管理平台显示 SE 中此应用未锁定；</li> <li>6) 后台日志中记录的应用锁定操作流程符合《可信服务管理平台技术要求》第 7.7 节中的流程图，应用解锁操作流程符合《可信服务管理平台技术要求》第 7.8 节中的流程图</li> </ol>



## 5.6.5.4 应用升级

测试编号： 5.6.5.4
测试项目： SE 应用升级
测试目的： 验证可信服务平台支持对 SE 应用升级功能
<p>预置条件：</p> <ol style="list-style-type: none"> <li>1) 按照图 1 进行正确连接；</li> <li>2) NFC 手机终端（SWP 方式支持近场支付的 NFC 手机终端/全终端方式支持近场支付的 NFC 手机终端）通过手机支付客户端或专用非接触读写器与可信服务管理平台连接；</li> <li>3) SE 中已安装一个非接触应用，可信服务管理平台中存在此应用的更新版本；</li> <li>4) 可查看可信服务管理平台后台日志</li> </ol>
<p>测试步骤：</p> <ol style="list-style-type: none"> <li>1) 操作员通过手机支付客户端或专用非接触读写器，获取可信服务管理平台中用户已下载应用列表；</li> <li>2) 操作员请求升级一个非接触应用，可信服务管理平台发起对此非接触应用的升级；</li> <li>3) 操作员以系统管理员或业务管理员身份进入可信服务管理平台，检查用户 SE 状态；</li> <li>4) 查看可信服务管理平台后台日志</li> </ol>
<p>预期结果：</p> <ol style="list-style-type: none"> <li>1) 手机支付客户端或专用非接触读写器显示已下载应用列表；</li> <li>2) 非接触应用升级成功；</li> <li>3) 可信服务管理平台显示 SE 中应用状态为“已个人化”，应用版本为更新版本；</li> <li>4) 后台日志中记录的应用升级操作流程符合《可信服务管理平台技术要求》第 7.3 节中的流程图</li> </ol>





中华人民共和国  
通信行业标准  
手机支付  
可信服务管理平台测试方法  
YD/T 2778-2014

\*

人民邮电出版社出版发行  
北京市丰台区成寿寺路11号邮电出版大厦  
邮政编码: 100164  
北京康利胶印厂印刷  
版权所有 不得翻印

\*

开本: 880 × 1230 1/16 2015年12月第1版  
印张: 1.5 2015年12月北京第1次印刷  
字数: 39千字

15115 • 609

定价: 15元

本书如有印装质量问题, 请与本社联系 电话: (010)81055492