ICS 03.220.20;35.240.15
R 85
备案号:

JT

中华人民共和国交通运输行业标准

JT/T 1059—2016

交通一卡通移动支付技术规范

Technical specification for mobile payment of transport card

2016-04-08发布　　2016-07-01 实施

中华人民共和国交通运输部　发布

总 目 次

R 85

备案号：

JT

中华人民共和国交通运输行业标准

JT/T 1059.8—2016

交通一卡通移动支付技术规范 第8部分：检测项目

Technical specification for mobile payment of transport card—Part8:Test specification

2016-04-08发布　　2016-07-01 实施

中 华 人 民 共 和 国 交 通 运 输 部　发布

目　　次

前　言

JT/T 1059《交通一卡通移动支付技术规范》分为8个部分：

——第1部分：总则；

——第2部分：安全单元；

——第3部分：近场支付；

——第4部分：远程支付；

——第5部分：客户端软件；

——第6部分：可信服务管理系统；

——第7部分：终端设备；

——第8部分：检测项目。

本部分为JT/T 1059的第8部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由交通运输部运输服务司提出。

本部分由交通运输信息通信及导航标准化技术委员会归口。

本部分起草单位：北京中交金卡科技有限公司、北京市政交通一卡通有限公司、南京市市民卡有限公司、银行卡检测中心、武汉城市一卡通有限公司、北京中电华大电子设计有限公司。

交通一卡通移动支付技术规范

第8部分：检测项目

1 范围

JT/T 1059的本部分规定了交通一卡通移动支付的可信服务管理系统、客户端、终端设备及安全单元的检测项目。

本部分适用于交通一卡通移动支付相关产品的试验、检测、产品认证及标准符合性检测。

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。

JT/T 978.7—2015 城市公共交通IC 卡技术规范第7部分：检测项目

JT/T 1059.1 交通一卡通移动支付技术规范第1部分：总则

JT/T 1059.2—2016 交通一卡通移动支付技术规范第2部分：安全单元

3 术语和定义

JT/T 1059.1及 JT/T 1059.2界定的以及下列术语和定义适用于本文件。

3.1

威胁 threats

任何强迫导致负面影响的行为，如机密信息的非授权泄露。

3.2

攻击 attack

为达到与安全保护相反的目标，行为实施者所进行的行为。

3.3

反向工程 reverse engineering

通过拆解、测绘和跟踪等技术手段对取得的产品(安全芯片和软件等)进行分析获得有关产品技术信息的行为。

3.4

单粒子效应　single event effect

高能带电粒子在器件的灵敏区内产生大量带电粒子的现象，又称单事件效应。

3.5

测试模式　test mode

安全芯片出厂时，进行必要的功能验证所需的一种安全芯片状态，包括圆片测试模式或固件测试模式，在测试模式下可对安全芯片的关键参数和敏感信息访问。

3.6

随机数发生器 random number generator

通过一些算法、物理信号、环境噪声等来产生没有关联性的数列的模块。

3.7

工作密钥 working key

通常指个人识别码加密密钥和校验码计算的密钥，也称为数据密钥。

3.8

终端主密钥 terminal master key

用于加密终端工作密钥的密钥。

3.9

身份鉴别 authentication

用来验证身份或证实信息完整性的过程。

3.10

密码键盘 encrypting PIN pad

用于自助个人识别码受理装置中安全输入个人识别码和加密的装置。

3.11

物理安全性 physical security

设备在物理构造上抵御攻击的能力。

3.12

密钥管理 key management

整个密钥生命周期中对密钥和相关参数的操作，包括生成、存储、分发、注入、使用、删除、销毁和存档等。

3.13

授权管理者 controlling authority

对安全单元内容拥有管理控制权限的角色。

3.14

加载文件 load file

传送加载到多应用安全单元上的某种文件，包含了加载文件数据块以及一个或者多个数据认证格式数据块。

3.15

组织安全策略 organizational security policies

一个组织为其运转而强制推行的一个或多个安全规则、过程、规范和指南。

3.16

个人化 personalization

安全单元发行者职责的最后流程，通过该流程配置安全单元、装载安全参数和设置密钥。个人化流程结束后，安全单元就可以完全操作并可发到最终用户手中。

3.17

安全属性 security attribute

用于执行评估对象安全策略的用户、主体、客体、信息或资源的特征。

3.18

评估对象　target of evaluation

作为评估主体的一个IT 产品或系统以及相关的指导性文档。

3.19

安全功能 security function

评估对象的一个或多个功能，用于执行评估对象安全策略的一组紧密相关的规则子集。

3.20

令牌 token

安全单元发行方出具的一个加密值。

3.21

可信路径 trusted path

用户能同一个评估对象安全功能进行信任通信，以支持评估对象安全策略的一种手段。

4 缩略语

以下缩略语适用于本文件。

AID——应用程序标识符(Application Identifier)

ARP——地址解析协议(Address Resolution Protocol)

DD_0S——分布式拒绝服务(Distributed Denial of Service)

DFA——差分错误分析(Differential Fault Analysis)

DoS——拒绝服务(Denial of Service)

DPA——差分功耗分析(Differential Power Analysis)

EEPROM——电可擦可编程只读存储器(Electrically Erasable Programmable Read-Only Memory)

EMA——电磁分析(Electro-Magnetic Analysis)

EPP——密码键盘(Encrypting PIN Pad)

FIB——聚焦离子束(Focused Ion Beam)

IP——网际协议(Internet Protocol)

IT——信息技术(Information Technology)

KEK——密钥加密密钥(Key Encryption Key)

PAMID——支付账户介质识别码(Payment Account Media Identifier)

PIN——个人识别码(Personal Identification Number)

QoS——服务质量(Quality of Service)

RAM——随机存储器(Random Access Memory)

ROM——只读存储器(Read-Only Memory)

SE——安全单元(Security Element)

SF——安全功能(Security Function)

SPA——简单功耗分析(Simple Power Analysis)

TMK——终端主密钥(Terminal Master Key)

TOE——评估对象(Target of Evaluation)

TOKEN——令牌化(Tokenization)

TSM——可信服务管理(Trusted Service Management)

WK——工作密钥(Working Key)

5 可信服务管理系统检测项目

5.1 基本要求

检测项目类型分为必测项、非必测项、适用必测项(若产品硬件或软件具备该功能或满足要求时为必测项目)。

5.2 功能检测项目

功能检测是验证交通一卡通移动支付 TSM平台业务功能正确性、检测系统业务处理准确性的测试。交通一卡通移动支付TSM平台功能检测项目见表1。

表 1 功能检测项目

序 号	检 测 项 目		检测项目说明
1	PAMID管理	PAMID生成	发行方TSM必测项
		PAMID查询	发行方TSM必测项
2	SE的生命周期管理	SE的个人化与注册	发行方TSM必测项
		SE的合法性检查	发行方TSM必测项
		SE的终止	发行方TSM必测项
		SE的挂失与解挂	发行方TSM必测项
		SE的锁定与解锁	发行方TSM必测项
		SE状态查询	发行方TSM必测项
		SE应用信息查询	发行方TSM必测项
		SE空间使用情况查询	非必测项
		SE状态同步	发行方TSM必测项
		SE重置	非必测项
		主安全域密钥更新	非必测项
3	辅助安全域 生命周期管理	辅助安全域的创建	发行方TSM必测项
		辅助安全域的删除	发行方TSM必测项
		辅助安全域的锁定/解锁	发行方TSM必测项
		辅助安全域密钥更新	发行方TSM必测项
		辅助安全域空间使用情况查询	非必测项
		应用查询	发行方TSM必测项

4	应用生命周期管理		
		应用下载与实例化	必测项
		应用个人化	应用提供方TSM必测项
		应用锁定/解锁	应用提供方TSM必测项
		应用删除	应用提供方TSM必测项
		远程管理指令同步	发行方TSM必测项
		SE应用同步	发行方TSM必测项
5	合作TSM管理	合作TSM管理	非必测项

表1（续）

序　号	检 测 项 目		检测项目说明
6	应用提供方管理	注册	应用提供方TSM必测项
		审核	应用提供方TSM必测项
		更新	应用提供方TSM必测项
		状态变更	应用提供方TSM必测项
7	应用管理	AID申请	应用提供方TSM必测项
		上传	应用提供方TSM必测项
		审核	应用提供方TSM必测项
		发布	应用提供方TSM必测项
		更新	应用提供方TSM必测项
		下架	应用提供方TSM必测项
8	支付业务公共电子认证证书管理	远程支付公共电子认证证书下载安装	非必测项
		近场支付公共电子认证证书下载安装	非必测项
9	报表管理	报表管理	非必测项

5.3　性能检测项目

性能检测项目是验证交通一卡通移动支付TSM 平台是否满足未来业务运行性能需求的检测项目，检测内容包括时间特性和资源利用性两方面。

交通一卡通移动支付TSM平台性能检测项目见表2。

表 2　性能检测项目

序　号	检 测 项 目			检测项目说明
1	时间特性	SE的生命周期管理	SE的个人化与注册	发行方TSM必测项
			SE的合法性检查	发行方TSM必测项
		辅助安全域生命周期管理	辅助安全域的创建请求	发行方TSM必测项
		应用生命周	应用查询	发行方TSM必测项

		期管理		
			应用下载请求	必测项
			应用个人化请求	应用提供方TSM必测项
2	资源利用性	检测过程中服务器资源占用情况		必测项
		压力解除后服务器资源释放情况		必测项

5.4 安全性检测项目

5.4.1 物理安全

交通一卡通移动支付TSM平台物理安全检测项目见表3。

表 3 物理安全检测项目

序 号	检 测 项 目		检测项目说明
1	物理位置选择	机房和办公场地所在建筑物	必测项
		建筑物内机房位置	必测项
2	物理访问控制	机房设置电子门禁系统	必测项
		来访人员申请和审批	必测项
		机房划分区域管理	必测项
		重要区域第二道电子门禁系统(增强要求)	非必测项
3	防盗窃和防破坏	主要设备放置	必测项
		设备固定	必测项
		通信线缆铺设	必测项
		介质保管	必测项
		机房防盗报警系统	必测项
		机房监控报警系统	必测项
4	防雷击	避雷装置	必测项
		防雷保安器	必测项
		交流电源地线	必测项
5	防火	火灾自动消防系统	必测项
		耐火建筑材料	必测项
		采用区域隔离防火措施	必测项
6	防水和防潮	水管安装	必测项
		防雨水措施	必测项
		防水检测和报警	必测项
7	防静电	接地防静电措施	必测项
		防静电地板	必测项
		静电消除器(增强要求)	非必测项
8	温湿度控制	温湿度自动调节设施	必测项
		供电线路防护设备	必测项

9	电力供应		
		备用电力供应	必测项
		冗余电力电缆线路	必测项
		备用供电系统	必测项
10	电磁防护	防止电磁干扰	必测项
		线缆隔离铺设	必测项
		关键区域电磁屏蔽(增强要求)	非必测项

5.4.2 网络安全

交通一卡通移动支付TSM平台网络安全检测项目见表4。

表 4 网络安全检测项目

序 号	检 测 项 目		检测项目说明
1	结构安全	主要设备网络冗余	必测项
		设备网络冗余(增强要求)	非必测项
		网络安全路由	必测项
		网络安全隔离	必测项
		网络拓扑结构	必测项
		IP子网划分	必测项
		QoS保证	必测项
2	访问控制	网络域安全隔离和限制	必测项
		地址转换和绑定	必测项
		内容过滤	必测项
		访问控制	必测项
		网络流量及连接数控制	必测项
		会话网络连接控制	必测项
		远程拨号访问控制	必测项
3	安全审计	日志信息	必测项
		网络对象审计分析	必测项
		日志权限和保护	必测项
		审计跟踪极限(增强要求)	非必测项
		集中审计(增强要求)	非必测项
4	边界完整性检查	非法连接阻断和定位	必测项
5	入侵防范	网络ARP欺骗攻击	必测项
		信息窃取	必测项
		DOS/DDOS攻击	必测项
		网络入侵防范机制	必测项
6	恶意代码防范	恶意代码防范措施	必测项
		定时更新	必测项
		网络设备用户身份鉴别	必测项

7	网络设备防护		
		主要网络设备用户组合身份鉴别	必测项
		身份鉴别信息不可伪造(增强要求)	非必测项
		登录口令安全性	必测项
		登录地址限制	必测项

表4（续）

序　号	检 测 项 目		检测项目说明
7	网络设备防护	登录失败处理	必测项
		远程管理安全	必测项
		权限分离	必测项
8	网络安全管理	网络日常维护	必测项
		网络设备软件更新	必测项
		漏洞扫描	必测项
		设备最小服务配置	必测项
		外部连接	必测项
		移动设备的网络接入控制	必测项
		定期检查违规行为	必测项

5.4.3　主机安全

交通一卡通移动支付TSM平台主机安全检测项目见表5。

表 5　主机安全检测项目

序　号	检 测 项 目		检测项目说明
1	身份鉴别	用户身份标识和鉴别	必测项
		口令复杂度	必测项
		登录失败处理	必测项
		远程管理的传输模式	必测项
		用户标识唯一	必测项
		用户身份信息组合鉴别技术	必测项
		鉴别警示信息设置(增强要求)	非必测项
2	访问控制	用户身份鉴别信息不可伪造(增强要求)	非必测项
		访问控制策略	必测项
		管理用户角色权限分配	必测项
		特权用户权限分离	必测项
		默认账户访问权限控制	必测项
		账户控制	必测项

		重要信息敏感标记(增强要求)	非必测项
		敏感标记信息访问控制(增强要求)	非必测项
3	安全审计	审计范围	必测项
		审计的事件	必测项
		审计记录格式	必测项

表5（续）

序　号	检 测 项 目		检测项目说明
3	安全审计	审计报表生成	必测项
		审计进程保护	必测项
		审计记录保护	必测项
		集中审计(增强要求)	非必测项
4	剩余信息保护	鉴别信息清除	必测项
		记录清空	必测项
5	入侵防范	入侵行为记录和报警	必测项
		重要程序完整性保护	必测项
		最小安装原则	必测项
6	恶意代码防范	防恶意代码软件	必测项
		不同恶意代码库	必测项
		防恶意代码软件统一管理	必测项
7	资源控制	接入控制	必测项
		超时锁定	必测项
		主机资源监控	必测项
		单个用户资源使用限度控制	必测项
		系统服务水平监控和报警	必测项
8	可信路径	身份鉴别信息传输(增强要求)	非必测项
		系统访问信息传输(增强要求)	非必测项
9	系统安全管理	访问控制策略	必测项
		系统漏洞扫描	必测项
		系统补丁	必测项
		系统管理员权限	必测项
		操作日志管理	必测项

5.4.4　数据安全

交通一卡通移动支付TSM平台数据安全检测项目见表6。

表 6　数据安全检测项目

序　号	检 测 项 目	检测项目说明

1	数据完整性	传输过程数据完整性	必测项
		存储过程数据完整性	必测项
2	数据保密性	数据加密传输	必测项
		数据加密存储	必测项

表6（续）

序　号	检 测 项 目		检测项目说明
3	备份和恢复	本地备份和恢复	必测项
		异地备份	必测项
		关键链路冗余设计	必测项
		数据备份记录	必测项
		备份数据定期检查	必测项
4	报文安全	报文完整性验证	必测项
		报文私密性	必测项
5	安全算法	对称加密算法	必测项
		非对称加密算法	必测项
		杂凑算法	必测项
6	密钥管理	密钥生成	必测项
		密钥传输	必测项
		密钥存储	必测项
		密钥备份	必测项
		密钥恢复	必测项
		密钥归档	必测项
		密钥销毁	必测项
		密钥更新	必测项

5.4.5 TSM 应用安全

交通一卡通移动支付TSM平台的TSM 应用安全检测项目见表7。

表 7 TSM 应用安全检测项目

序　号	检 测 项 目		检测项目说明
1	身份鉴别	用户身份标识和鉴别	必测项
		用户身份组合鉴别技术	必测项
		身份标识唯一性和复杂度检查	必测项
		登录失败处理	必测项
		用户身份组合鉴别技术不可伪造（增强要求）	非必测项
		访问控制策略	必测项

2	访问控制		
		访问控制覆盖范围	必测项
		默认账户访问权限控制	必测项
		用户角色权限	必测项
		敏感标记设置(增强要求)	非必测项

表7(续)

序　号	检 测 项 目		检测项目说明
2	访问控制	敏感标记信息资源访问控制(增强要求)	非必测项
		禁止默认账户访问(增强要求)	非必测项
3	可信路径	身份鉴别信息安全传输路径	必测项
		资源访问信息安全传输路径	必测项
4	安全审计	审计范围	必测项
		审计保护	必测项
		审计记录格式	必测项
		审计报表生成	必测项
		集中审计接口(增强要求)	非必测项
5	剩余信息保护	鉴别信息清除(增强要求)	非必测项
		记录清空(增强要求)	非必测项
6	通信完整性	通信完整性(增强要求)	非必测项
7	通信保密性	会话初始化验证	必测项
		通信过程中加密	必测项
		加解密运算和密钥管理(增强要求)	非必测项
8	抗抵赖	数据原发证据	必测项
		数据接收证据	必测项
9	应用容错	数据有效性验证	必测项
		自动保护	必测项
		敏感信息回退清除	必测项
		页面异常信息处理后显示	必测项
		异常详细信息日志	必测项
		自动恢复(增强要求)	非必测项
10	资源控制	自动结束会话	必测项
		最大并发会话连接数限制	必测项
		多重并发会话限制	必测项
		时间段内并发会话控制	必测项
		限额分配(增强要求)	非必测项
		系统服务水平最小值检测报警	必测项
		服务优先级设定(增强要求)	非必测项

11	应用服务器安全	防止网站身份被仿冒	必测项
		未授权存取动作防范	必测项
		防范应用内容被篡改	必测项