doi：10.3969/j.issn.1672-6073.2017.01.022

基于金融标准的移动支付技术在宁波轨道交通的应用

湛维昭，张　森
（广州地铁设计研究院有限公司，广州 510010）

摘　要：随着移动支付技术的发展，快捷便利的支付方式成为城市轨道交通广大乘客对运营服务水平的迫切需求。分析宁波城市轨道交通实现手机移动支付的基本条件，即：手机终端内置近距离无线通信芯片、AFC系统能够识别处理IC卡数据及清分中心系统与手机之间的数据处理，重点介绍SWP－SIM技术实现方式、AFC系统读卡器选型、交易信息安全保障机制和基于金融标准的相关业务数据结构整体规划等工程实施关键技术及重难点，描述轨道交通实现移动支付功能的基本业务流程。

关键词：城市轨道交通；金融标准；qPBOC3.0标准；手机移动支付；自动售检票
中图分类号：F530.7　　**文献标志码**：A　　**文章编号**：1672-6073(2017)01-0106-04

Application of Mobile Payment Technology Based on Financial Standard to Ningbo Urban Mass Transit

ZHAN Weizhao, ZHANG Sen
(Guangzhou Metro Design & Research Institute Co., Ltd., Guangzhou 510010)

Abstract: With the development of mobile payment technology, fast and convenient payment has been urgently needed for urban mass transit passengers. The basic conditions are analyzed for the application of the mobile payment technology to Ningbo urban mass transit. The implementation modes of SWP-SIM technology, AFC system card reader selection, transaction information security mechanism and overall data planning based on financial standards are discussed as the key technologies and key points. The basic process of realizing the mobile payment for urban rail transit is also presented.

Keywords: urban rail transit; financial standard; qPBOC3.0 Standard; mobile payment; AFC system

1　研究背景

移动支付是指允许移动用户使用其移动终端（通常是指手机）对所消费的商品或服务进行账务支付的一种服务方式。继银行卡类支付、网络支付后，手机支付俨然成为新宠。随着移动互联网和近距离手机支付技术的快速发展，以及国内三大移动运营商对移动近距离支付应用的大力推广，手机移动支付的应用普及已经势不可挡。基于金融标准的IC卡[1]以智能、安全、便捷及多应用等特点受到世界各国的重视。2013年2月中国人民银行发布《中国金融集成电路（IC）卡规范（V3.0）》（以下简称qPBOC3.0），同年总行批准宁波市民卡作为全国金融多应用首批试点城市开展相关应用推广工作。与此同时，随着宁波轨道交通工程建设的进行，宁波轨道交通首次将手机NFC（近距离无线通信芯片）支付技术、城市一卡通技术、金融qPBOC3.0技术应用于城市轨道交通自动售检票（AFC）[2-3]领域，并成功建设和开通运营，以传统支付方式无法比拟的优势为乘客带来更快捷、更安全的支付体验。宁波在基于金融qPBOC3.0标准的手机移动支付技术应用于城市轨道交通方面取得了一定的成功。

2　城市轨道交通实现移动支付的基本条件

城市轨道交通为实现手机移动支付功能，在设计和工程建设时需具备以下基本条件。

收稿日期：2016-02-22　**修回日期**：2016-04-08
第一作者：湛维昭，男，硕士，高级工程师，从事城市轨道交通自动化领域研究和工程设计，zhanweizhao@dtsjy.com

1）市民手机终端需内置近距离无线通信芯片（near field communication，NFC）。NFC 技术[4]是一种短距高频的无线电技术，能够实现主动和被动两种读取模式，通信指标与轨道交通通用读卡器/票卡指标相符。

2）当移动支付作为一种新的支付方式后，手机票将作为一类新票种集成进入轨道交通 AFC 系统。AFC 系统能够识别处理基于金融标准的 IC 卡数据，并对手机中相关的交易数据进行处理。

3）城市轨道交通的线网清分中心系统还需新增与手机/银行卡数据管理中心（宁波为市民卡管理数据中心）的数据通信接口，在与轨道交通相关的手机移动支付中，对其交易数据进行清分处理。

3 工程实施的关键技术及重难点

基于金融标准的移动支付技术要在轨道交通取得成功应用，需对以下关键技术和重难点进行研究，并提出相应解决方案，如图 1 所示。

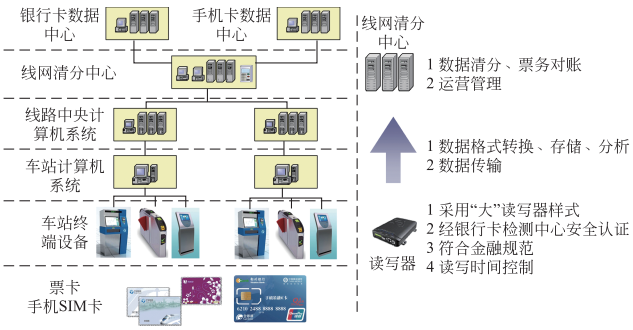

图 1　AFC 系统实现移动支付的关键技术及数据处理流程示意

Fig. 1　Flow diagram of key technology and data processing about mobile payment in AFC system

1）手机支付的核心安全元件（security element，SE）[5]是以芯片形式存在的具有加密/解密功能的逻辑电路，它能起到防止外部恶意解析攻击和保护数据安全的作用。根据 SE 芯片所处位置的不同，NFC 手机一般可分为 SE 在手机中的 NFC 芯片全终端技术、SE 在手机 SD 中的 SWP - SD 技术和 SE 在 SIM 卡中的 SWP - SIM 技术[6]三种，其中 SWP - SIM 技术可接受移动运营商及市民卡公司（银行业）双重密钥控制，安全可控性高，能兼顾各方对数据安全独立控制和发行运营维护统一管理的基本要求，而且产业链也较为成熟。经多方测试，宁波轨道交通工程最终选用 SE 在 SIM 卡中的 SWP - SIM 技术，如图 2 所示。

2）根据中国人民银行相关规定，轨道交通自动售检票系统“扣款终端机具”须取得银行卡检测中心金融

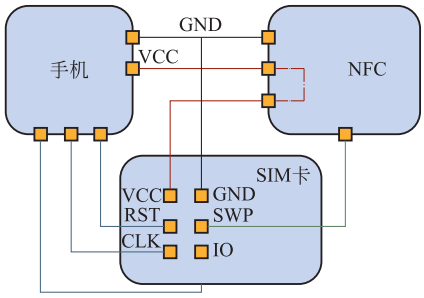

图 2　SWP - SIM 方案示意

Fig. 2　Schematic diagram of SWP - SIM program

检测安全认证[7]。qPBOC3.0 认证主要分为 Level1（电气部分）、Level2（应用部分）两部分检测[8]。目前行业内一般根据读写器逻辑流程处理位置不同将其分为“大”“小”读卡器两种类型，其中“大”读卡器是指票卡所有业务操作流程及逻辑判断由读卡器自配处理器完成，而不是由检票机/售票机的工控机（ECU）实现。为方便银行卡检测中心的安全检测认证，自动售检票系统读卡器选型应考虑采用行业“大”读卡器设计方案，这样实际工程可采用“大”读卡器作为“扣款终端机具”报送安全认证，而不需要整台检票机/售票机。

3）为满足安全认证的需要，“大”读卡器设计及产品开发应符合《金融银行卡部分符合中国金融集成电路（IC）卡规范 终端规范》，主要包括终端硬件、初始化应用、读写处理、交易处理、脱机认证、持卡人验证、联机处理等。

4）金融 qPBOC3.0 卡普遍采用 CPU 卡介质及非对称密钥，与以往轨道交通常用的 M1 卡及建设部标准对称密钥车票相比，CPU 卡处理速度及非对称密钥逻辑认证流程[9]相对复杂，读取时间较长。为避免出现轨道交通客流拥堵、刷卡失败率增加等风险，需在系统设计和产品制造时严格控制整笔交易时间指标在 500 ms 以内。宁波轨道交通工程分别采取了升级读卡器处理器（采用当时先进的 ARM9 处理器），多方协商精简金融卡离线交易流程，精简卡片存储数据结构等多种措施，最终确保宁波轨道交通对金融 qPBOC3.0 卡实测处理时间平均为 450 ms 左右。

4 信息安全保障机制

由于实际工程涉及轨道交通、金融、移动通信等多行业和多主体之间的数据信息交互，其信息安全保障及密钥设置机制尤为重要，主要体现在作为常规通信应用及金融应用载体的手机 SIM 卡上。因此在建设过程中应对各方数据信息集中点的 SIM 卡信息安全制定

严格安全保障机制，主要包括3方面。首先，SIM卡片应通过银行卡qPBOC3.0 EMV应用和(U)SIM卡应用的检测要求；其次，SIM卡片供应商应获得业务合作各方(即运营商、一卡通公司及银行业)共同认可；最后，SIM卡设置双重密钥控制以实现移动通信应用与金融应用独立共存。

为更好地处理SIM卡密钥控制权及有效保障信息安全，实现手机支付功能的SIM卡密钥数据结构应符合Java Card和GP规范。依据GP规范，SIM卡双重密钥分为卡片主控密钥(KMC)和金融应用密钥(ADMK)，如图3所示。考虑到手机SIM卡一般由移动运营商发行，因此卡片主控密钥由移动运营商掌握。主控密钥可对移动通信区域各类业务数据进行所有处理和操作，可以创建或完全删除金融应用整体区域，但不能对金融业务内部数据进行读取、修改或其他操作。金融应用密钥由一卡通公司掌握，一卡通公司可对卡中金融业务应用的区域内部所有数据进行处理或操作。在这种模式下，移动运营商与一卡通公司(银行业)之间权责清晰，双方的各自应用能独立共存，从而确保各自数据的安全。

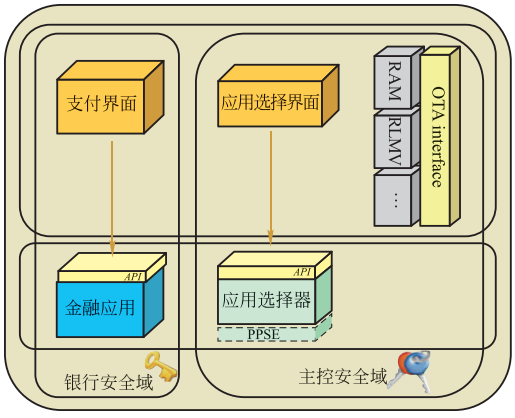

图3 SIM卡密钥数据结构示意

Fig. 3 Diagram of SIM card key data structure

5 金融卡中有关业务的数据结构整体规划

与旧标准相比较，2013年2月正式颁布的qPBOC3.0在第14部分“基于借记贷记应用的小额支付扩展应用”中新增加金融扩展行业的应用内容，分配了专门的扩展应用文件模板，从而满足了金融IC卡在地铁、公交、高速公路收费、停车收费、铁路(高铁)等领域的多种应用。金融IC卡为扩展实现小额消费多行业应用，需要针对各个行业的实际应用，在IC卡数据层面进行相应的数据结构整体规划。

实际工程在遵循qPBOC3.0金融扩展行业交易规范的基础上，首先应采用金融扩展行业多应用产品数据模板规划出金融扩展应用公共信息区的数据结构，主要记录发卡相关信息、行业标识、设备代码和存款金额等，其中在行业标识中为城市轨道交通业务规划出专门的识别代码，具体内容如表1所示。

表1 金融扩展应用公共信息区的数据结构

Tab. 1 Data structure of public information area for financial expansion application

数据项	长度/bytes	记录描述
发卡行信息记录	51	发卡行机构标识、地区代码、行业代码、行业卡号、卡类型等
持卡人信息记录	80	姓名、性别、证件类型、证件号码、联系方式等
本地区公共信息记录	30	行业标识、交易时间、设备代码、存款金额等
跨地区公共信息记录	30	(可预留)行业标识、交易时间、设备代码、存款金额等

此外还应专门规划轨道交通扩展应用信息区的数据结构，主要记录轨道交通领域各类应用的相关信息，例如进出站信息、换乘信息、交易信息和其他内部记录信息等，如表2所示。

表2 轨道交通扩展应用信息区的数据结构

Tab. 2 Data structure of information area of expansion application for rail transit

数据项	长度/bytes	记录描述
轨道交通信息记录	21	ID标识、复合消费和预授权消费标识、行业标识、有效期
进出站信息记录	65	进出站状态、进站时间、进站设备编号、出站时间、出站设备编号、交易金额、拒绝原因码、拒绝时间、交易数据、MAC等
内部换乘信息记录	30	线路标识、交易时间、设备码、交易金额等
内部服务信息记录	30	线路标识、交易时间、设备码、金额、操作员代码、交易类型
内部使用信息记录	25	累计交易次数、累计交易金额、优惠限制日期、折扣信息等
轨道交通专有交易日志	38	交易类型、交易时间、设备编号、交易金额、交易前余额等

当读卡器对金融IC卡进行数据读写时，程序首先处理金融扩展应用公共信息区的内容，当辨识出轨道交通行业的识别代码后，处理程序将跳转读取金融卡中轨道交通扩展应用信息区的内容并进行相应的数据程序处理。

6 实现移动支付功能的基本业务流程

城市轨道交通实现移动支付功能的基本业务流程可分为以下几个环节，如图4所示。

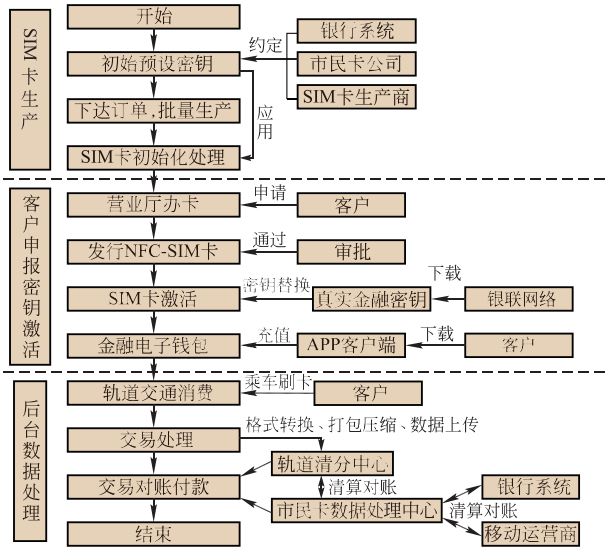

图 4　轨道交通实现移动支付功能的基本业务流程

Fig. 4　Basic flow chart of mobile payment function in rail transit

6.1　SIM 卡生产环节

1）产品投产前，由银行、市民卡公司与 SIM 卡生产商约定 NFC 手机 SIM 卡中金融应用的初始预设密钥信息，并确认金融应用安装的相关参数。

2）移动运营商、市民卡公司和银联共同向 SIM 卡供应商下达订单进行批量生产。

3）SIM 卡生产商进行卡片信息初始化处理，使用事先约定的初始预设金融密钥创建金融应用的预设实例。

6.2　客户申报和金融密钥激活环节

1）客户在移动运营商指定的营业厅提出办卡申请，经对客户 NFC 手机核对无误，在申报审批通过后运营商按照业务流程向客户发放 NFC－SIM 卡。

2）在指定的移动运营商营业网点对客户资料进行核对之后，通过专线连接银联网络系统并调用银行卡服务接口，进行远程应用下载。应用下载的指令是以密文形式传输，并由 SIM 卡中的过程密钥进行解密，传输过程中的信息安全可以得到有效控制。最终将金融应用的预设密钥替换[10]为金融业务使用的真实密钥，从而完成对 SIM 卡中银行金融应用密钥的完全激活。

3）完成以上操作后客户手机 SIM 卡将开通金融功能，用户便可使用相应的 APP 软件客户端，对 SIM 卡中金融电子钱包进行预存充值等操作。

6.3　用户使用及系统后台数据处理环节

1）在实际使用过程中，客户使用 NFC－SIM 卡手机在轨道交通车站通过右侧刷卡位置进行进/出站消费的终端操作。

2）在轨道交通 AFC 系统的进/出站检票机中，读卡器将记录相应刷卡信息，并根据刷卡使用情况计算出相关的交易数据，同时还会对手机支付交易数据进行格式转换、打包压缩、数据上传等操作。

3）交易数据通过自动售检票车站及线路中央计算机系统上传至线网清分中心，实现交易清算、数据对账入库和统计处理等功能。线网清分中心与市民卡数据处理中心进行交易核对后完成账务清算、付款等工作。宁波市民卡系统负责与移动运营商和银行系统进行数据对接，完成最终的交易对账结算。

7　结语

通过轨道交通 1 号线工程的建设，宁波市首次成功将基于金融 qPBOC3.0 标准的手机移动支付技术应用于城市轨道交通领域，为广大乘客带来了更快捷、更便利和更安全的崭新消费体验，提升了宁波轨道交通整体运营服务水平。宁波城市轨道交通基于金融标准的移动支付技术的成功应用经验可为国内其他城市轨道交通工程提供参考借鉴。

参考文献

[1] 徐飞，曹奇英. PBOC2.0 新型金融 IC 卡读卡器的设计与开发[J]. 单片机与嵌入式系统应用，2012(1)：35－37.
XU Fei, CAO Qiying. PBOC2.0 New Financial IC gard reader [J]. Microcontrollers & embedded systems, 2012(1): 35－37.

[2] 闫鸣宇，陈楠. 移动支付在城市轨道交通中的应用研究[J]. 铁路通信信号工程技术，2016，13(3)：72－75.
YAN Mingyu, CHEN Nan. Application of mobile payment in urban rail transit[J]. Railway signaling & communication engineering, 2016, 13(3): 72－75.

[3] 李道全. 城市轨道交通 AFC 系统支付方式现状及发展[J]. 都市快轨交通，2016，29(1)：59－62.
LI Daoquan. Situation and development of AFC system payment methods in urban rail transit[J]. Urban rapid rail transit, 2016, 29(1): 59－62.

[4] 孟健，陈少芳. 基于 NFC 手机支付的应用研究[J]. 电子商务，2008(8)：70－75.
MENG Jian, CHEN Shaofang. Research on the application of mobile payment based on NFC. E－Business journal[J]. 2008(8): 70－75

[5] 翁晓军. 基于 NFC 技术的手机支付平台设计与研究[J]. 网络安全技术与应用，2013(12)：15－16.
WENG Xiaojun. Design and research of NFC technology platform for mobile phone payment based on[J]. Network security technology & application, 2013(12): 15－16.

（下转第 128 页）