



基于 NFC 技术的移动支付系统设计方案

刘景文¹, 许玮¹, 吕伯轩¹, 王单¹, 聂雯莹¹, 樊宁²

(1. 普天信息技术有限公司, 北京 100080;

2. 中国电信股份有限公司广州研究院, 广东 广州 510630)

摘要: 分析了移动支付系统的不同支付模式的优缺点与安全性以及现有移动支付方案存在的不足, 并针对这些不足, 以票务系统为例, 提出了一种基于 NFC 和指纹识别技术的新型移动支付安全方案。介绍了方案的主要功能模块及数据流, 编程实现了完整的移动支付模拟系统, 并对系统的主要功能和完整流程进行了测试, 保障了安全性, 对搭建 NFC 移动支付系统有一定的借鉴意义。

关键词: 智能终端; 移动互联网; 移动支付; NFC; 指纹识别

中图分类号: TP391

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018098

Design of mobile payment system based on NFC

LIU Jingwen¹, XU Wei¹, LV Boxuan¹, WANG Dan¹, NIE Wenying¹, FAN Ning²

1. Potevio Information Technology Co., Ltd., Beijing 100080, China

2. Guangzhou Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China

Abstract: The advantages, drawbacks and security of different mobile payment models were analyzed, and the defects of the existing mobile payment schemes were pointed out. To solve the above problems, a new mobile payment scheme based on the NFC and fingerprint identification was designed. The main function modules and data flow of the scheme were introduced. The prototype of the mobile payment system was realized. The main function and the whole technological process were tested, and significant references for establishing NFC based mobile payment systems were also provided.

Key words: intelligent terminal, mobile internet, mobile payment, NFC, fingerprint identification

1 引言

自从 Android 和 iOS 操作系统成为智能手机主流的操作系统之后, 越来越多的开发者挖掘出

新型应用和服务^[1]。智能手机可以用来查询交通路线、个性化阅读, 甚至随时随地购物。用手机实现钱包或银行卡功能, 有两个要求必须要满足: 一是安全性, 二是便捷性。二维码支付手段已经

收稿日期: 2017-12-09; 修回日期: 2018-01-30

通信作者: 聂雯莹, niewenying@potevio.com

基金项目: 国家高技术研究发展计划 (“863” 计划) 基金资助项目 (No. 2015AA017205)

Foundation Item: The National High Technology Research and Development Program of China (863 Program) (No.2015AA017205)



越来越流行，但它的安全性有待提高，且其专利技术主要受到日本公司垄断^[2]，本文关注的重点是基于一种更加安全的 NFC（近场领域通信）技术的移动支付手段。

NFC 功能与手机支付结合成为一种被称为“NFC 近场支付”的新型移动支付方式^[3]。NFC 技术与传统产业结合能创造很多有价值的产品^[4]。

目前在中国很多大中城市，地铁出行已成为必不可少的交通选择。以北京为例，地铁购票方式有两种：第一种是直接自动售票机或窗口处购票，缺点是要准备零钱或者找回多个硬币，存放不方便；另外一种购票的方式是使用地铁交通卡，这种刷卡方式方便；但在退卡管理上，较为繁琐，需到为数不多的几个指定地点退卡，退卡后只能在一周后再次到退卡处取回卡内余额，一旦卡丢失则卡内的余额无法追回，若卡片内部线路损坏或失去磁性，则购卡押金不予退回，容易导致使用者利益损失。

针对传统地铁票务支付系统在技术、管理等方面的不足，本文将智能终端与移动互联网结合，配合完善的加/解密和数字签名技术，设计一种基于 NFC 的移动支付系统，弥补传统支付在便捷性与管理方面的不足，在确保安全性的基础上提升用户体验。

2 国内外发展现状

2011 年，谷歌发布了一款名为谷歌钱包的移动支付产品，由于使用 NFC 支付的 Android 手机需要内置 NFC 芯片，当时绝大多数的 Android 手机没有 NFC 功能^[5]。另外，谷歌在推广谷歌钱包之前，没有与零售商以及银行等达成一致，导致很多商店的 POS 机无法支持手机的 NFC 支付。谷歌钱包并没有达到预期目标。

苹果在 2015 年份正式发布了苹果支付产品。苹果支付克服了谷歌当时失败的几个因素^[6]。首先，iPhone 的 iOS 系统是闭源的，能够要求 iPhone

厂商支持 NFC^[7]。另外，苹果在推出苹果支付之前与零售商和银行等进行合作。

很多与 NFC 支付相关的机密数据都要保存在 SE 芯片中^[8]，SE 芯片可以看成一种硬件加密的元件，保障数据安全存储，NFC 支付的实现与 SE 芯片的功能密切相关。

SE 芯片主要有 4 种形态，分别介绍如下。

- SWP (single wire protocol) -SIM 卡，将 SE 芯片内置在 SIM 卡里。
- ESE (embedded secure element) 方案，在手机中加入一个独立于操作系统的存储芯片，加密并保存支付数据。
- microSD-SE 方案，SE 芯片内置于 SD 卡中。
- HCE (host-based card emulation, 主机卡模拟)，采用云服务器加密数据，是纯软件方案。摆脱了对手机厂商和通信运营商的硬件依赖，受到金融机构（发卡银行）的欢迎。

中国银联股份有限公司（以下简称银联）研发了一个被称为“云闪付”的产品，是一种 HCE 主机卡模拟模式，用于支付的机密数据存储在云端。国内移动运营商研发出一套用于公交系统的 NFC 移动支付体系，使用 SWP-SIM 卡内嵌 SE 芯片的模式保存支付数据。由于这种 SIM 卡硬件的特殊性，对于 Android 手机的 CPU 存在兼容性问题，未得到很好的普及。

本文以地铁票务支付为背景，分析传统支付和管理存在的几点缺陷，然后针对这些缺陷以 NFC 技术作为支撑重新设计了整个票务支付系统，并编程实现，该系统共分为五大模块，分别是加/解密模块、用户客户端模块、读卡终端模块、票务服务器模块和银行服务器模块，各个模块相互调用，彼此通信，共同实现了一个完整的地铁票务移动支付系统。本文所设计的基于 NFC 的移动支付方案对手机硬件的依赖程度不高，更易推广。

3 地铁票务支付系统的功能与模块设计

3.1 系统的性能需求

本文设计并模拟了地铁票务移动支付系统的完整流程,对设备的性能要求如下。

- 用户手机:手机为 Android 操作系统,系统版本应在 Android 4.4 以上,具有指纹识别器。
- NFC 终端的工作频率在 13.56 MHz 左右,误差不超过 7 kHz,工作范围在 5 cm 以内,最高速率为 424 kbit/s,最低速率为 115 kbit/s。
- 地铁票务服务器能够承载高并发 I/O 操作,能承受数千个客户端并发访问,同时与之相关的数据库也应具有良好的稳定性,不会因 I/O 操作频繁而崩溃。

本文将支付网络、Token 服务提供方、银行卡组织三者视作同一个“银行服务器”,以简化业务模型,该服务器同样能够承担高并发 I/O 操作。

3.2 系统的总体结构

整个系统分为 5 个主要模块,分别是用户客户端、地铁读卡终端、地铁票务服务器、银行服务器以及加/解密模块。

3.2.1 加/解密模块

为保证传输数据的安全性,两个通信实体之间的数据传输应加密。本系统的加/解密模块采用非对称密码算法和对称密码算法,使用数字签名算法实现数据完整性保护与消息源验证,从多个方面保障整个系统的安全性。

3.2.2 用户客户端模块

客户端 App 安装在用户手机上,为用户提供交互操作,主要包括 5 个部分。

(1) 用户注册

用户注册需要的内容包括有效手机号、短信验证码、登录密码、身份证等。

(2) 用户登录

用户登录需要用户名与密码,本系统有找回

密码功能。

(3) NFC 支付—银行卡绑定子模块

用户输入银行卡信息,发送到银行服务器,银行服务器验证信息,生成与银行卡信息一一对应的支付口令(PaymentToken)并返回给用户客户端,PaymentToken 是后续 NFC 支付的凭证。

(4) 进/出站子模块

单击“进/出站”按钮后,会出现一个窗口,用户经过指纹识别确认后,客户端允许 NFC 读卡器读取 PaymentToken 信息。

(5) 查看历史订单模块

用户可查看历史出行记录,包含订单编号、创建时间、进出站名称、票价、逗留时间等。

3.2.3 地铁读卡终端模块

地铁读卡终端作为 NFC 读卡器,除了具有 NFC 功能之外,还通过一个电子屏幕向用户呈现提示信息。该模块实现以下功能。

(1) 设置站点名称

在终端主界面中,有两个下拉列表用来分别选择地铁线路和详细的站点名称。

(2) NFC 读卡器

地铁读卡终端最重要的功能是使用 NFC 通信从客户端中读取支付数据。

(3) 信息显示

从服务器收到响应数据,根据不同的状态码显示不同的提示信息,主要包括进站成功信息、进站失败信息、余额不足信息、出站成功信息等。

3.2.4 银行服务器模块

银行的服务器主要完成两个功能,一是根据用户提交的银行卡信息生成对应的 PaymentToken,并把该口令(Token)与用户信息关联;二是验证该 Token 是否与一个有效的银行账户关联,另外还要验证该 Token 的有效期。

(1) 生成 PaymentToken

在银行服务器数据库中已存在“银行账户信息表”(见表 1),该信息表中的内容主要是用户在



表 1 银行账户信息表 tb_accountinfo

字段名	数据类型	说明
id	整数	该字段作为主键，是区分各个记录的唯一标识
user_name	字符串	银行账户的户主姓名
card_no	字符串	银行卡卡号
user_number	字符串	户主的身份证号
phone_no	字符串	户主的手机号码

银行柜台前为银行卡开户时所填写的各类信息。

PaymentToken 验证时需要访问的数据表见表 2，NFC 支付时用来验证 Token 的有效性。

生成 PaymentToken 的过程：银行服务器收到用户发来的银行卡信息之后，在表 1 中查找是否存在该账户。若存在，则生成 Token，然后在数据库中建立表 2，分别把银行卡卡号、PaymentToken、Token 的有效期这 3 个信息存入表 2 中。最后向客户端返回 PaymentToken。

(2) 验证 PaymentToken

在验证 PaymentToken 阶段，银行服务器从地铁票务服务器接收数据，主要内容包括用户的 PaymentToken、地铁票价、地铁商户的 PaymentToken。首先，通过 PaymentToken 在表 2

中查询与之对应的银行卡卡号 card_no 和 Token 的有效期 val_token。若 val_token 在有效期内，再通过 card_no 从表 3 取出用户的账户余额 (money)，做一次金额相减的操作：

$$\text{money} = \text{money} - \text{地铁票价} \quad (1)$$

然后更新 money 记录。最后，根据地铁票务服务器提供的卡号，在表 3 中取出对应的余额，做地铁票价的计算，更新数据。

这样就完成了一次支付票价的结算过程。最终银行的服务器向地铁票务的服务器发送扣款成功或失败的状态码。

3.2.5 地铁票务服务器模块

本模块是整个系统中最繁忙的模块，因为需不断与其他的 3 个通信实体进行数据传递，下面

表 2 银行账户与 PaymentToken 的映射表 tb_paytoken

字段名	数据类型	说明
id	整数	该字段作为主键，是区分各个记录的唯一标识
card_no	字符串	银行卡卡号
token	字符串	与银行卡卡号一一对应的 PaymentToken
val_token	字符串	Token 的有效日期，截止到年月日，格式为 yyyy-MM-dd

表 3 银行账户与对应账户剩余金额的映射表 tb_accountmoney

字段名	数据类型	说明
id	整数	该字段作为主键，是区分各个记录的唯一标识
card_no	字符串	银行卡卡号
money	浮点小数	账户内剩余的金额
record_time	字符串	记录最后一次操作该记录时的时间，格式为年月日时分秒

分别阐述本模块的各个功能以及与其他 3 个模块之间的信息传递，如图 1 所示。

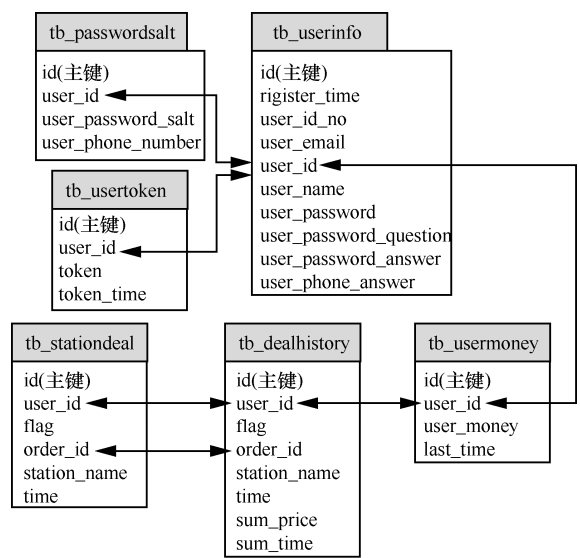


图 1 地铁票务服务器模块信息表的联系

(1) 用户账号注册

在客户端模块，用户填写注册信息，该信息被发送到地铁票务服务器模块，该模块会根据注册信息生成几张不同的数据表（见表 4~表 9），分别用于处理不同的业务。

表 4 处理的内容是生成用户对应的个人信息，其中最重要的字段是 user_id，它相当于账户的指纹，后续很多数据库的操作用到这个 ID。

表 5 记录的内容是地铁票务系统中独有的一个电子钱包信息。

用户注册成功后，地铁票务服务器给用户客户端返回一个登录口令（LoginToken），这样用户再次登录时，直接验证 LoginToken 的有效性即可。表 6 是用户注册成功之后自动生成的记录 Token 信息的数据，Token 需设定有效期（设置为 7 天）。

表 4 用户个人信息数据表 tb_userinfo

字段名	数据类型	说明
id	整数	该字段作为主键，是区分各个记录的唯一标识
register_time	字符串	用户注册的时间信息，具体格式为 yyyy-MM-dd-HH-mm-SS
user_id	字符串	用户的 ID，是地铁票务系统中该账户唯一的标识
user_password	字符串	经过消息摘要算法处理后的密码，其逆运算不是密码明文

表 5 用户的钱包余额记录表 tb_usermoney

字段名	数据类型	说明
id	整数	该字段作为主键，是区分各个记录的唯一标识
user_id	字符串	用户的 ID，是地铁票务系统中该账户唯一的标识
user_money	浮点小数	账户中钱包的金钱余额，它与银行账户中的余额相互独立
last_time	字符串	最后一次生成更新该记录的时间

表 6 账户的 token 记录表 tb_usertoken

字段名	数据类型	说明
id	整数	该字段作为主键，是区分各个记录的唯一标识
user_id	字符串	用户的 ID，是地铁票务系统中该账户唯一的标识
token	字符串	用户账户对应的 LoginToken
token_time	字符串	最后一次生成 LoginToken 的时间，用来验证有效性



(2) 用户登录

用户登录客户端，输入账号和口令。若通过验证，服务器根据 `user_id` 从表 6 中取出对应的 `token_time`，即 Token 的最后一次生成时间。如果 `token_time` 与系统当前时间差小于 7，说明 Token 有效，直接跳转到客户端的功能主界面；否则，重新登录。

(3) 地铁进/出站的数据处理

用户的进/出站操作由地铁读卡终端模块从数据库中取出 `user_id` 字段值，服务器生成订单信息数据表，分别是订单实时信息表和订单历史信息表，作为后续查询历史订单之用。

4 系统测试与分析

4.1 测试环境

(1) 模拟用户客户端模块

物理设备选用“Nexus 5x”的 Android 手机，其系统版本是 Android 6.0，对应的 API 版本号是 23，该手机同时具有 NFC 功能和指纹识别器这两个物理硬件。

(2) 模拟地铁读卡终端

用另一部 Android 手机来模拟地铁闸机的读卡终端，这里选用“华为荣耀 6”，其系统版本是 Android 4.4，该手机具有 NFC 功能，可作为读卡终端使用。

(3) 模拟两个服务器

地铁票务服务器与银行服务器运行在 Tomcat 7.0 上。与服务器通信的数据库使用免费版的 MySQL。

4.2 加/解密模块的测试

在客户端与服务端加密通信的场景下，通过 ECDH 密钥协商协议生成一个共享密钥，AES 算法使用共享密钥对数据明文进行加/解密。

设有一个字符串：116hthgs6456463254y154894gfdsg6541564642gfsgf63184796

字符串长度为 53，该数据以加密形式从客户端传输到服务端。

加解密测试步骤如下所示。

步骤 1 服务器端的公钥和私钥

服务器端公钥：

```
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEvc86FHkS8MgDIUawslzmjo3U27IKAHFLNE
LR5ze67W/1b4P/8CawIAuPTTr/BiEHjjBbsEVHkGX
d35z5Xs42OZA==
```

服务器端私钥：

```
MEECAQAwEwYHKoZIzj0CAQYIKoZIzj0DAQcEJzAlAgEBBCDdbtNBYjsrUY1MbwjVh/Tyszu
Il/EP5VPY/8+tx/jvitw==
```

步骤 2 客户端的公钥和私钥

客户端公钥：

```
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEXaLUQ64oZl0ETThYAAFATncE36yvxvwuFt
UoX8KVn+RJ1eLO6J5Pl1FSCumeGiJyXsc+yTDM
dUNDuqHOOge0CVg==
```

客户端私钥：

```
MEECAQAwEwYHKoZIzj0CAQYIKoZIzj0DAQcEJzAlAgEBBCAjOCLnHlhpIkIrtFek1gAlTFG
XZEdK4d3xD0oKrDjetA==
```

步骤 3 客户端与服务端端的共享密钥

```
TTn2QN8s24/51OUutviECbCmCnEERNlnule
wOOicPrg=
```

步骤 4 客户端使用该共享密钥对待测试字符串加密的密文

```
5jyqnlXnH0hrOx2nVptmpwYGuTz8i/CyyBP/
mnT/ICm6MR55POnEWLvjtgSEM0E0PHzoEVH/
ZtxAcn/6H6V2xg==
```

步骤 5 服务器端使用该共享密钥解密

```
116hthgs6456463254y154894gfdsg654156464
2gfsgf63184796
```

本系统也通过了数字签名和数字证书的验证测试。

4.3 用户客户端模拟地铁卡的测试

初次打开用户客户端 App，进入登录界面。

此时用户还没有自己的账号，单击“新用户？立即注册”，进入注册界面。用户注册的测试用例见表9。

表9 用户注册的测试用例

类别	具体内容
昵称	谈笑有鸿儒
有效手机号	123456789
登录密码	admin123
身份证	370753442424525325
密保问题	您的父亲姓名是什么
答案	无白丁

信息填写成功后，单击“完成注册并登录”按钮，系统返回主界面，新用户的钱包余额是0。单击“钱包充值”按钮，即可跳转到充值业务。

该地移动支付系统既可使用独立的钱包余额功能，也可绑定银行卡，如图2与图3所示。



图2 用户设置界面



图3 绑定银行卡界面

进/出站时进入主功能界面，单击“我要进站/出站”按钮，即可显示指纹识别界面，提示用户将手指放在指纹识别器上，也可以使用口令完成身份验证。

此时，把手机贴近地铁读卡终端，即可完成进/出站操作。各个服务器能够正常生成数据表，并记录相关的订单信息，良好地实现了基本的地铁票务处理流程。

5 结束语

与智能终端、移动互联网融合的移动支付显示出支付多样化的趋势，银行、金融公司、电子商务公司等纷纷进入这一领域，本文分析了基于NFC支付技术的发展现状与采用不同技术模式所遇到的瓶颈，并针对目前地铁票务系统存在的几点不足，以NFC技术作为支撑、采用密码机制，结合指纹识别技术，重新设计了地铁票务系统，并编程实现，按照注册、充值、进/出站流程对系统的安全性及可用性进行了测试，满足NFC用户使用要求，提升了用户体验。

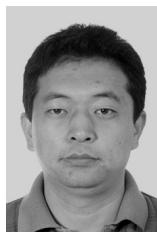
参考文献：

- [1] 陈洋. 基于移动支付服务价值的互联网支付用户渠道转移行为研究[D]. 镇江: 江苏大学, 2016.
CHEN Y. Research on channel transfer behavior of Internet payment users based on the value of mobile payment service[D]. Zhenjiang: Jiangsu University, 2016.
- [2] 施文杰. 基于PKI技术的二维码安全性研究[D]. 淮南: 安徽理工大学, 2017.
SHI W J. Research on security of two-dimensional code based on PKI Technology[D]. Huainan: Anhui University of Science & Technology, 2017.
- [3] ONDRUS J. Clashing over the NFC secure element for platform leadership in the mobile payment ecosystem[J]. International Journal of General Systems, 2015, 29(4): 1-6.
- [4] SCHURMANN D, DECHAND S, WOLF L. OpenKeychain: an architecture for cryptography with smart cards and NFC rings on Android[J]. The ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2017, 3(99): 1-24.

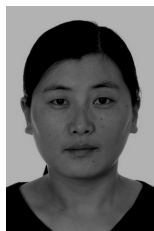


- [5] KAUFFMAN R J, LIU J, MA D. Investment timing for mobile payment systems[C]//The 14th Annual International Conference on Electronic Commerce, August 7-8, 2012, Singapore. New York: ACM Press, 2012: 169-170.
- [6] 孟小楠. Apple Pay 的支付安全性分析[D]. 北京: 北京交通大学, 2017.
MENG X N. Analysis of payment security of Apple Pay[D]. Beijing: Beijing Jiaotong University, 2017.
- [7] TAN D J J, CHUA T W, THING V L L. Securing Android: a survey, taxonomy, and challenges[J]. ACM Computing Surveys, 2015, 47(4): 58.
- [8] WOOL A, KANONOV U. Secure containers in Android: the Samsung KNOX case study[C]//The Workshop on Security and Privacy in Smartphones and Mobile Devices, October 24, 2016, Vienna, Austria. New York: ACM Press, 2016: 3-12.

[作者简介]



刘景文（1974-），男，博士，普天信息技术有限公司技术总监、高级工程师，主要研究方向为移动互联网技术、应用和安全。



许玮（1983-），女，普天信息技术有限公司解决方案经理、高级工程师，主要研究方向为基于行业的信息通信。



吕伯轩（1979-），男，普天信息技术有限公司研发部总经理、高级工程师，主要研究方向为基于行业的信息通信。

王单（1977-），女，博士，普天信息技术有限公司产品经理、高级工程师，主要研究方向为无线通信专网及物联网关键技术。

聂雯莹（1983-），女，普天信息技术有限公司标准化工程师、助理研究员，主要研究方向为基于行业的信息通信标准。

樊宁（1983-），女，中国电信股份有限公司广州研究院系统分析师，主要研究方向为云计算安全、移动互联网安全及SDN/NFV安全等。