Network Recharge Platform for Public Transport Smart Card Based on Mobile Devices

Xiaoli Wen[1,a], Haowei Su[1,b], Jinlong Cai[1,c] and Dabi Zou[1,d]

[1]Guangzhou Yangchengtong Co., Ltd, Donghuadong Rd, Yuexiu, Guangzhou, China

[a]elisy@163.com, [b]gzsuhw@tom.com,[c]cjl26scut@qq.com, [d]denic@mail.ustc.edu.cn

Keywords: Network recharge, Public transport, Mobile Devices, Security.

Abstract. In this paper, we propose a network recharge platform for public transport smart card based on mobile devices. The proposed platform is to cater the great need of smart card recharge services as the number of user growth. The architecture of proposed platform includes intelligent device, network recharge platform and core recharge system. The main realized business process of proposed system includes online account transfer and CPU card recharge. In order to promise the safe operation of proposed system, the security attention is paid in design and in deployment.

Introduction

In China, as the population grows, public transportation become more and more important for millions of commuters in big cities. The smart cards for ticketing of public transportation are widely used by commuters. Besides the use of ticketing, these smart cards are also used in many fields [1]. The operation company of public transportation smart cards should make good use of its resources to provide services for serving the public's need of smart cards. One of most important services is to recharge the store value smart card for users. As the development of technology and change of user demand, the method of providing recharge service became more convenience.

At first, the smart card operation company cooperated with merchants, who own many branches at the anthill in cities. In these branches, staffs of merchants provide recharge service to user. This operation pattern brought advantages for all parties. For the smart card company, it could spread its recharge points and provide recharge service in low cost. For merchants, attracting more users to their branches helps to gain more popularity and to improve sales volume. For user, they could find recharge point easily to recharge for their cards.

As the number of smart card users increases, user may need to wait for a long time to queue in order to recharge during peak time [2]. At the same time, the expansion of new charge point is limited. The smart card company provides a new self-services way to recharge. In new design, every smart card has two corresponding accounts. Besides the traditional offline account with its balance stored in smart card, it introduces the online account with its online balance stored in back-end database system. User could transfer to online account by bank or third-party payment channel. Then user charges the offline account of smart card from its online account by self-services equipment which operated by merchants.

Both ways of recharge mentioned before are based on the "smart card company – merchant – user" pattern. As the development of Internet technology and intelligent hardware, it is possible for smart card company to provide recharge service to user directly. This new pattern we define as "smart card company - user" pattern. Recent years, as the development of smart phone, it is convenient for user to get services from mobile applications. One of most important services among these applications is online payment, by which user could buy products or services, through third payment company. In addition, the smart card application scenarios of intelligence hardware become more and more mature. The applications of Near Field Communication (NFC) mobile phone with Android operation system become far more common [3]. Both reader/writer mode and card emulation mode are fit for smart card application. Besides NFC, blue tooth technology is also a good choose for communication between mobile phone and readers or other devices [4].

This paper will propose a network recharge platform base on "smart card company - user" pattern. The proposed platform which is operated by smart card company could provide services to user. At

the back end of platform, it connects between the core recharge system and user terminals. At the front end, smart card company provides static library or connection protocol to terminal application developers. The front end applications and different kinds of smart devices work together to complete recharge or other services. It is possible for developers take advantage of different kind of smart devices at the front end in the proposed platform.

This paper will first introduce some key technology of the proposed platform. Then the architecture of proposed network recharge platform will be introduced, followed with its components descriptions. The implementation effect of proposed system and the business process will be introduced. Finally, the paper will draw a conclusion based on above description.

Key Technology

Smart Card. There are mainly two kinds of public transport store-value card. The first is logic security card, which is also called M1 card. Another is micro chip card, which is also called smart card or CPU card. Compared to M1 card, CPU card is a newer technology and is a safer choice for both user and card operation company. The key point of card safe is key management system. Both logic security card and CPU card protect in-card data by key authentication. But they use different mechanisms to protect data.

For M1 card, its authentication mainly base on the KeyA and KeyB in every sector. The read/write control of every sector is implemented by various combinations of KeyA and KeyB. The mechanism of M1 card prevents invalid system to access data stored in the card. But it could not help system to authenticate to cards.

With better hardware, CPU card could support more complicated transaction process. In the process of data exchange, CPU card protect its data by transmission and validation of MAC1, MAC2 and TAC. The safe mechanism of CPU card could complete mutual authentication of validation between card and system. By taking advantage of this mechanism, CPU card is much safer than M1 card.

PKI. Public Key Infrastructure (PKI) is a platform to provide public key to encrypt and to decrypt data and to provide digital signature service. The core recharge system of smart card company uses PKI system to make authentication of terminals, and to provide protection of key in order to make sure the confidentiality, integrity and non-repudiation in transaction.

In our previous work, we proposed a network recharge system which was composed by smart card secure reader, network platform and operator system. Before distributing secure reader to users, readers are initialized, including installing the necessary PKI certificates [5]. In order to take advantage of different kind of intelligent devices, it is impossible to initialize PKI certificate in user's devices. So in this paper, we propose no PKI in user's device, which is considered as "unreliable". PKI is embedded in the network recharge subsystem of network recharge platform in order to protect the safety of data, which will be mentioned as followed.

Intelligent Devices. NFC is a kind of short distance and high frequency wireless connection technology. The operating frequency of NFC is 13.56MHz [6]. NFC has three kinds of operation mode. The first kind is write/read mode. For application of public transportation card, it is possible to use NFC devices which install relating software application to complete transactions with smart card. The second kind is card emulation mode. NFC device could emulate smart card and work as a normal smart card. The third is peer-to-peer (P2P) mode [7].

Presently, the main operation systems of mobile phone are Android and iOS. For devices with Android, user and developer could take advantage of NFC function to implement smart card application. For iOS device, the interface of NFC function is not open to developer.

Besides NFC technology, the Bluetooth communication is also a good choice for smart card application. Developer could use Bluetooth to make connection between smart phone and different kind of devices which could be reader or smart card. For example, user could recharge his smart hand ring with smart card function through Bluetooth connection by smart phone. Almost every smart phone has the Bluetooth connection function which is open to developers; it is easy for them to

develop customization application. Moreover, the devices connected to smart phone could be various.

System architecture

To complete recharge CPU card by mobile devices, there are several components need to work together. These components include intelligent device, network recharge platform and core recharge system, as shown in Fig. 1. Every component will be introduced in detail as follow.

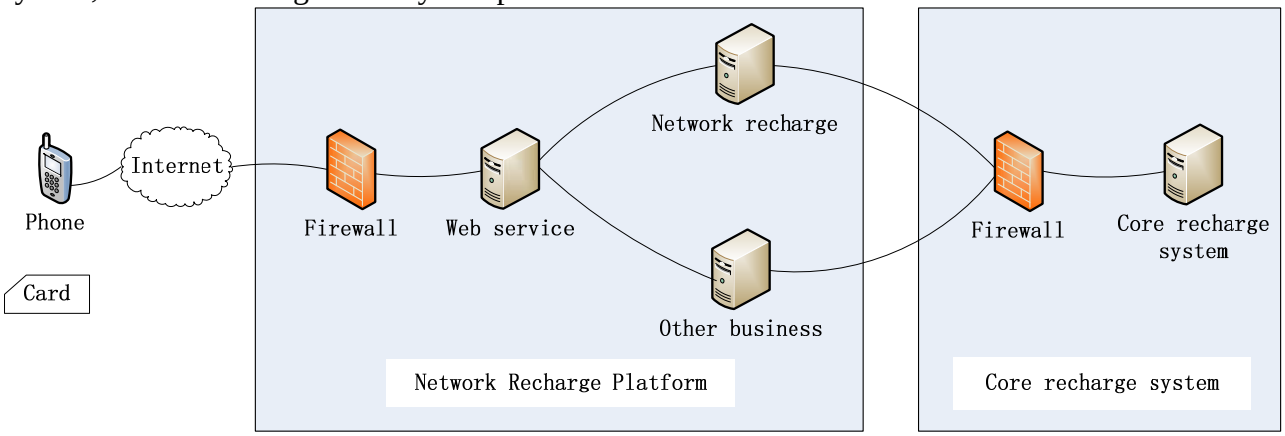

Fig. 1 System architecture of proposed network recharge platform

Intelligent device. At the front end, user needs to own a phone or other intelligent device with network connection. To get services from smart card company, the smart phone could install APP with SDK provided by smart card company or other way to connect server of smart card company. The intelligent devices are various. For example, the smart phone with NFC could be a reader to exchange data with CPU card. A reader which communicates with smart phone by Bluetooth could be used as terminal in proposed system architecture.

In design, intelligent devices are considered as “unreliable” in data exchange protection. There are two main functions of devices. The first is to send APDU commands to CPU card and receive card response. The second is to communicate with server. In the recharge process of exchange data with server, intelligent devices is to in charge of extract APDU command from server and to packaging server data from APDU response.

Network recharge platform. The network recharge platform is the core component of proposed system. The platform is deployed at the side of smart card company. It is mainly composed by web server, network recharge subsystem and other business subsystem.

Web server is mainly to communicate with intelligent devices. It receives http request from terminals and distribute to different subsystems according to the type of business request. After subsystems finish processing data, the web server packaging data and send back to terminals. In order to deal with huge currency volume, the web server could be improved to a subsystem that has functions of load balancing and flow control.

The network recharge subsystem is mainly to deal with the request data relating to recharge services from web server. The network recharge subsystem is equipped with PKI cards. The PKI card could help to promise the safety of recharge procession by a good mechanism of key management. The session key which is to encrypt and decrypt data communicated with core recharge system of each recharge process is managed by network recharge subsystem. Through this design, the network recharge subsystem could promise the safety of recharge process. It could avoid the bad effect of unsafe problems brought by “unreliable” terminal. In future, the role of PKI card could be substituted by encryption equipment in order to increase ability to process data and to improve the concurrency of recharge services.

Other business processing system is mainly to deal with request data of other business. Besides recharge services, the smart card company also provides other services to user. These services

include transfer to online account by bank or third-party payment channel. Other business processing system transfers some request to core recharge system according to the type of business request.

Core recharge system. For old pattern of recharge, the smart card company has established a core recharge system. The core recharge system provides stable services of recharge and other business.

By taking advantages of the mechanism of both CPU card and PKI, the safety of CPU card recharge provided by the core recharge system could be promised. For CPU card recharge, the core system is response to make authentication and to calculate the MAC1, MAC2 and TAC of CPU card during data exchange. Once failed to authenticate during recharge, the core system will end the process of recharge in order to avoid invalid terminal or invalid card to retry. On the other hand, the PKI system holds the session key for every process when terminals communicate with the core recharge system. The session key is to encrypt and decrypt the message exchanged in recharge process. The session key will update when the terminal sign up to the core recharge system or when the session key is time-out.

Besides recharge, the core recharge system also deals with other business relating to recharge. One of most important business is the online account management. The core system processes the transfer request and adds value to the card online account. The card online account is one of funding source when recharging offline account of card. If user chooses to use online account to recharge, the core recharge system will deduct the balance of online account.

Business Process

The business process realized by proposed network recharge platform mainly includes transfer of online account and CPU card recharge. The detail of these business processes will be introduced as follow.

Online account transfer. Online account transfer is to add value for the smart card online account. There are three parties to take part in the process of online account transfer, as shown in Fig. 2. The first is the terminal. It mainly means the back end server of cooperator and the smart phone with app which could receive services from the smart card company. The second is the third party pay company which could be banks or other network third party pay company. It is the funding source of transfer the money from third party pay account to smart card online account. The third is the proposed platform operated by smart card company.

There are three steps to perform online account transfer. The first is the terminal to create transfer order from proposed platform. Then terminal finishes payment at third party pay side. After finishing payment successfully, the third party pay side will send a pay notice to proposed platform. It the pay notice information sent by third party pay side passes validation, proposed platform will add value for the online account of smart card.

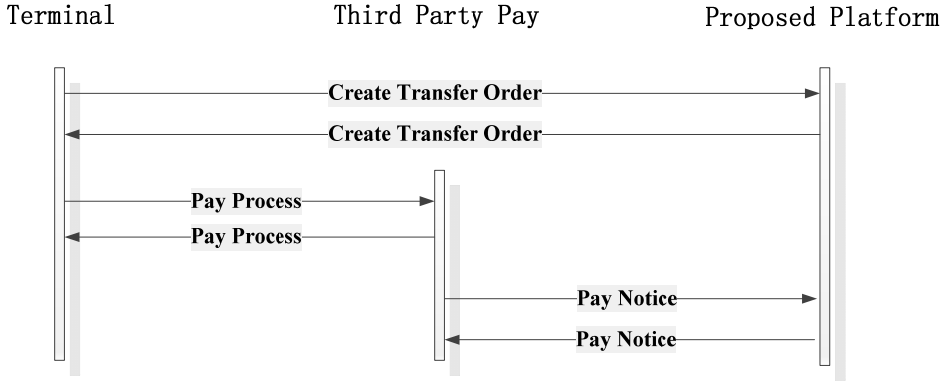

Fig. 2 Business process of online account transfer

CPU card recharge. To complete CPU card recharge, there are also three parties to take part in, as shown in Fig. 3. The first is CPU card, which is the aim to recharge. The second is terminal, which it is defined as before. The third is the proposed platform operated by smart card company.

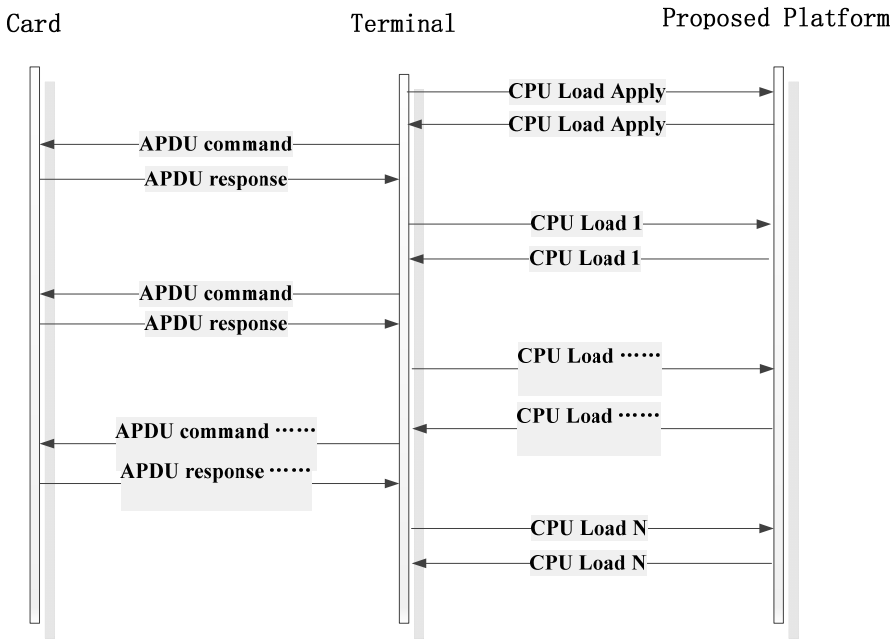

Fig. 3 Business process of CPU card recharge

The procedure of CPU card recharge mainly contains two parts. The first is the terminal applies CPU card load from proposed platform. The second is to process CPU load. For the first step of procedure, terminal send a request to proposed platform to perform CPU load apply. In this step, proposed platform will record relating information to recharge, such as recharge amount, card number, and user identification. After process the request of CPU load apply, the proposed platform responses some information, which includes recharge order number, APDU command set, the step of recharge procedure, to terminal in order to continue the CPU card recharge procedure. After finishing the first step, the terminal send request of CPU load to proposed platform, including information about which step of procedure, and APDU response from CPU card. The platform decides whether the procedure should be continued. The procedure is controlled by a flag in the response of CPU load. The terminal exchanges information among card and platform continuously until the platform send information to terminal to end the procedure.

The procedure of CPU card recharge is controlled by the proposed platform. The platform takes in charge of sending APDU command set and the explanation of APDU response. Moreover, the platform communicates to core recharge system and makes some logic control of the recharge procedure. As the terminal is not controlled by smart card company, the logic of terminal is designed as simple as it can. The terminal is mainly to follow the control flag from platform to exchange information between terminal and CPU card, and to communicate with proposed platform.

Security Discussion

For internet application, the security scheme should be paid more attention, especially for transaction relating to fund security. In this part, card transaction security and communication security will be mentioned.

Card transaction security. In the design of proposed platform, the reader used to exchange information with smart card is not controlled by smart card company. The terminal reader and application is considered as “unreliable”, that means that it may be attacked by illegal users and the information sent by terminal should be verified. What’s more, there may be other attacks such as insider attack, shared session attack causing the unsecure of smart card [8].

The security mechanism of CPU card provides a solution for “unreliable” terminal. CPU card integrates microprocessor (CPU), memory cell including RAM, ROM and EEPROM, and card operation system (COS) [9]. Compared with M1 card, CPU card has ability to perform more complicated calculation and data procession. In the procedure of CPU card recharge, MAC1, MAC2

and TAC are to make authentication and validation between card and core recharge system. MAC1 and TAC are sent by CPU card while MAC2 is sent by core recharge system. For the same CPU card, the values of MAC1, MAC2 and TAC change for every transaction. It is impossible for invalid user to break the secret key of CPU card by intercepting the message of transaction. The safe mechanism of CPU card helps to protect data safety in the case of using “unreliable” terminal, even encountering invalid user tries to make fake trading or to tampering with data.

Communication security. To complete recharge services, message is need to pass among several components. The communication security among these components is an important aspect to protect data security. In this part, the communication security of between terminal and web server, between network recharge subsystem and core recharge system will be discussed.

The web server of proposed platform is open to receive request data from different terminals. The main method to protect data is to validate the sign of massage. The proposed platform provides services to different cooperators of smart card company. To manage these cooperators to connect to proposed platform, smart card company deploys a key and a channel code to every cooperator. The key is to encrypt message combined with MD5 algorithm to protect data security.

The network recharge subsystem and core recharge system are mainly in recharge of processing message of recharge services. The key to encrypt and decrypt data between these two parts are maintained by the mechanism of PKI. The data for transmission is encrypted by 3DES algorithm using the session key. The session key updates frequently in order to enhance security level avoiding brute force attack to get the session key.

Conclusion

The number of smart card user in public transportation become bigger and bigger. One of most important topics in operation is to provide convenient recharge services to users. The technology development of mobile internet and the intelligent devices provides a possible solution to establish an open network recharge platform to provide recharge services to user by taking advantage of different kinds of intelligent devices. This paper introduces a net recharge platform for smart card. The pattern of the recharge operation mode is called “smart card company - user”.

The proposed platform is established based on the core recharge system that provide card recharge services for all smart card of company. It provides services to different kinds of terminals through internet connection. Main services of proposed system include online account transfer, CPU card recharge and complaint submission. As discussion, there are several mechanisms to promise the safety of system.

References

[1] J. Chen, and C. Wang: Exploratory factor analysis approach for understanding consumer behavior toward using Chongqing City Card, Advanced Data Mining and Applications Lecture Notes in Computer Science, Vol. 6441 (2010), p. 561-567.

[2] D. G. Chandra, R. Prakash, and S. Lamdharia: Mobile Ticketing System for Automatic Fare Collection Model for Public Transport. 2013 5th International Conference on Computational Intelligence and Communication Networks (CICN), (2013), p. 600-603.

[3] S. Dwivedi and J. R. D'Souza: Prototype for Multiple applications using Near Field Communication (NFC) technology on Android device. 2015 International Conference onAdvances in Computing, Communications and Informatics (ICACCI), (2015), p. 38–43.

[4] J. F. Ensworth and M. S. Reynolds: Every smart phone is a backscatter reader: Modulated backscatter compatibility with Bluetooth 4.0 Low Energy (BLE) devices. 2015 IEEE International Conference on RFID (RFID), (2015), p. 78-85.

[5] H. W. Su, X. L. Wen, J. L. Cai and D. B. Zou: Open Network Recharge System Architecture for Public Transportation Card, Applied Mechanics and Materials, Vol. 373-375 (2013), p. 1954-1961.

[6] P. Pourghomi and G. Ghinea: Managing NFC Payment Applications through Cloud Computing, 2012 International Conference for Internet Technology and Secured Transactions, (2012), p. 772-777.

[7] L. Mainetti, L. Patrono and R. Vergallo: IDA-Pay: An innovative micro-payment system based on NFC technology for Android mobile devices. 2012 20th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), (2012), p. 1-6.

[8] Y. Kim, Y. Choi and D. Won: Security Improvement on Smart card-based Remote User Authentication Scheme using Hash Function, 2014 International Conference on Information Science and Applications (ICISA), (2014), p. 1-4.

[9] Y. Wu and Y. Sun: Analysis and Research to Security Testing of Smart Card, 2009 International Conference on Electronic Commerce and Business Intelligence, (ECBI), (2009), p. 99-101.

