International Journal of Smart Home
Vol.7, No.5 (2013), pp.103-114
http://dx.doi.org/10.14257/ijsh.2013.7.5.11

Design and Implementation of In-House Electronic Money Using Java Cards

Hyun Joo Kim [1], Soo Jong Lee [2] and In Chul Shin[3]

[1] *Dept. of Electronics & Electrical Engineering Graduate School Dan-kook University, South Korea*
[2]*Dept. of Computer Engineering Hyupsung University, South Korea*
[3]*Dept. of Electronics & Electrical Engineering Dan-kook University, South Korea,*
[1]*chopin@uhs.ac.kr,* [2]*sjlee@uhs.ac.kr,* [3]*char@dankook.ac.kr*

Abstract

Spread of the IT and Internet served as an important turning point for consolidating digital economy growth and for building national economy's competitiveness worldwide. Among them, emergence of e-money grew into important issue of e-commerce, and it can be considered futuristic currency revolution that replaces traditional payment methods such as cash, check and others. Recently, e-money for supporting SNS(Social Network Service) service is very popular among the young generation members. Likewise, diverse e-currencies provide many conveniences as they consolidated as a culture in our everyday life.

This research designed and implementation in-house e-money using Java Card technology. In-house e-money is e-money that is used in one organization, and charging, payment, adjustment and refund take place within the organization. We focused mostly on the e-money security since e-money is personal asset. In other words, we used by realizing Java Card based technology with superb security and by developing e-money Java applet to ensure safe e-money management. Moreover, algorithm for hash encryption was applied to transmit data safely within the organization when it comes to charging, authorization, adjustment and refund. Algorithm for hash encryption was applied to transmit data safely. E-money will now consolidate its position as a part of our everyday life. Furthermore, hopefully, e-money of the in-house method will be utilized to create profit and as a new business culture.

Keywords: *e-currency, e-cash, e-money, in-house, payment, security, Java Card*

1. Introduction

The widespread use of IT(information technology) and the Internet has provided an important opportunity to reestablish the competitive advantage of developing a digital national economy across the world [1]. The birth of electronic money has become an important issue of e-commerce. This is the currency revolution of the future that will replace the traditional approval tool of cash and checks. Recently, various concepts of electronic money have been presented. In particular, electronic money that supports a SNS(social network service) has received a significant response from the young generation. The use of electronic money in Korea has also increased since 2000. It is used for making payments at toll booths, malls, convenience stores, subways, and parking lots. T-money, a transportation card with advanced payment, and transportation cards with deferred payment built in the IC(integrated circuit) chip of a credit card are widely used today. However, the importance of the safety of electronic money made with digital data has been emphasized from the beginning. Since electronic money is used as an approving tool in the virtual range through

ISSN: 1975-4094 IJSH

networks, thereby creating a new business paradigm, its importance and necessity are increasing considerably. However, electronic money has many risks such as people cannot directly check the transaction like as in the case of any traditional transactions.

Therefore, more attention needs to be paid on the development of a safer security technology and the practicality of electronic money. In this study, we plan to implement electronic money with a Java card method using an in-house method. Currently, the Java card is considered safe worldwide and is mainly used in the financial sector. However, in-house electronic money with a Java card method is rarely used in Korea. Electronic money for the in-house use suggested in this study is used in only one organization and charged, approved, balanced, and refunded in the organization. Further, we have focused on the safety of electronic money. We utilize the Java card technology that is approved for its safety worldwide and a hash encryption algorithm for the safe transfer of material. Moreover, if electronic money with an in-house method is activated in organizations, it will lead to profit and be developed as a new business model for the electronic money market.

2. Related Study

2.1. Electronic Money

2.1.1. Definition: In general, electronic money is used with the concept of "performing money functions with electronic equipment." [2]. Further, it is "value information that is described with a digital signal that a bank sends to guarantee face value." [3]. It is defined as "money that is provided to the issuer in advance; a certain monetary value is saved in an IC chip or a computer communication network built in a plastic card to be used in the information communication network." [4]. Electronic money is used in various forms.

2.1.2. Type of Electronic Money: Electronic money used in Korea can be classified into IC chips, networks, online and offline, open and close, advanced payment, and credit cards [2, 4]. Electronic money with a smartcard IC chip is mostly used in the financial sector.

2.1.3. Advantages and Disadvantages of Electronic Money: Electronic money that provides monetary value with electronic symbols reduces social cost and is portable and comfortable. First, it reduces the need to carry money around. Second, it saves one from various fees for financial transactions. Third, it reduces the transaction cost with a direct transaction with a seller. Fourth, it simplifies the way of storing money and reduces the danger of theft and loss. Lastly, it can be tracked down to where it is used when it is lost [5]. However, security should be considered before electronic money can be introduced.

2.1.4. Domestic and Overseas Trends of Electronic Money: In Korea, K-cash, Mybi, and Visa-cash that are electronic money have been issued in banks since 2008. In particular, the Mybi transportation card that was developed from Busan is considered to be a very successful case. However, Mybi did not get developed further because of its compatibility issue. Currently, T-money is used with the cooperation of the financial sector. In overseas cases, European electronic money is relatively well distributed but is less distributed than expected. In the UK, CEPS (Euro electronic money) mainly with Mondex is supplied. In Hong Kong, Otopus is used in convenience stores, and electronic money is used for transportation. Singapore has set up electronic road pricing (ERP) with Cash-card [5].

2.1.5. In-House Electronic Money Service Implementation Cases: The domestic cases of implementation of in-house electronic money are as follows. In-house electronic money is operated with the principle of usage only in an organization. Thus, colleges were very appropriate models for implementation of in-house electronic money. In this study, the in-house electronic money implementation cases were investigated centering on colleges. The implementation of in-house electronic money in colleges can be divided into cases using cyber money and the type with connection to the financial sector. Among domestic colleges, school A was jointly operating with bank N using K-Cash. School A issued ID cards from bank N, which were converted into electronic money used at school A from the bank account connected to bank N. B University used electronic by using pre-paid transportation cards. School C which used cyber money had the electronic money stored at server and not the smart card ID card.

2.2. Java Card

A Java card is a smartcard that is structured with the Java programming language and can execute programs. It integrates the technology of a smartcard into technology of a Java card. In general, a Java card works in memory, communication, security, application and the memory is composed of 1K RAM, 24K ROM, and 16K EEPROM [6, 7].

2.2.1. Structure of Java Card: A Java card requires a Java card virtual machine (JCVM) to support and execute instructions in the Java language [8]. JCVM is a divided into off-card and on-card VM. Figure 1 shows the structure of the Java card. The bottom has a hardware and operation system. Further, a Java card consists of a set of classes that are made for applets to be developed by ISO7816, the standard related to smartcards. Three major packages of the Java card are java.lang, javacard.framework and java card.security and the extension package is javacardx.crypto [9].

2.2.2. Java Card Applet: A Java applet is an application program that operates in a Java card. Multiple applets can be run on one Java card. An applet with various functions can be implemented using AID. The applet is downloaded and used in the EEPROM of the card. For differentiation, it communicates with JCRE and the application program of the Java card by exchanging with the APDU(Application Program Data Unit) 5 bytes or more of data. Communication between an external application program and an applet is structured using the command APDU and the response APDU [9]. In this study, we have implemented electronic money for an in-house use on a Java card applet.

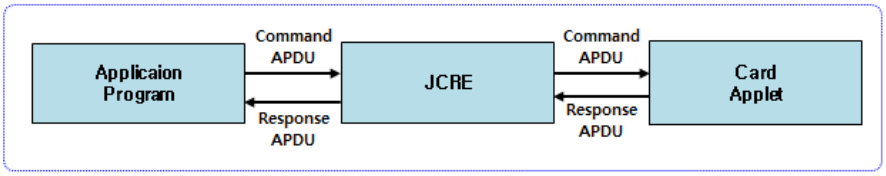

Figure 1. Java Card Applet Communication

2.3. Hash Function

A hash function generates strings with a certain length with an n-bit output. This function is a method to cut or substitute data or change the location of data [10, 11]. This generates a result, which is called a hash value. In a hash function, if two hash values are different, the original data of the hash value are different as well. However,

the opposite cannot be established. A hash function is determined depending on how small the hash conflict that occurs in the entry range is. If there is considerable conflict, it is difficult to differentiate between the different data.

3. Design and Implementation of Electronic Money for In-House Use

3.1. Overview of Proposed System

Electronic money for the in-house use considered in this study is generated using a Java card method and can be used in one organization. Further, it is possible to charge, approve, balance, and refund cash with electronic money in the organization. As electronic money is used as money, it should have the characteristics of commodity money. Therefore, electronic money should not be easily forged. Further, electronic money has digital information with value, and its original and copy should be clearly differentiated. Moreover, the transaction details of the user should not be disclosed.

3.2. Development Environment of Electronic Money for In-House Use

The electronic money proposed in this study can be used in the considered organization only. This plan allows electronic money to be used in a university. A university that includes bookstore, various types of rental stores, and a shuttle bus service is a very good model for the application of electronic money in this study. The following describes what to prepare and the development environment of the proposed system before using electronic money in the organization.

※ Preparation

- User: Issued smartcard (plastic card on which a Java applet can be installed)
- Unmanned charger: Automatic charge system to charge electronic money
- Rental shop: POS(Point to Sales) system to pay with electronic money
- Web service: Web system to check the payment details of the user and the rental stores
- SAM: SAM to approve, pay, charge, and approve transactions
- Smart card

Table 1. Proposed System Development Environment

Classification	Content
Main Operating System	IBM P-750 AIX 6.1 CPU: 3.7GHz POWER7 * 4cpu HDD : 146.8GB,Kernel : 64bit
Terminal and PC Operating System	CPU: ntel 1.66GHz, RAM: 1G HDD:40G Kernel : 32bit
Development Language	JAVA, JDK 1.6
Database and Web server	Oracle11g / Web Sphere 6.1

3.3. System Structure and Flow of Electronic Money for In-House Use

The structure and the service flow for the electronic money for the in-house use considered in this study is illustrated in Figure 2.

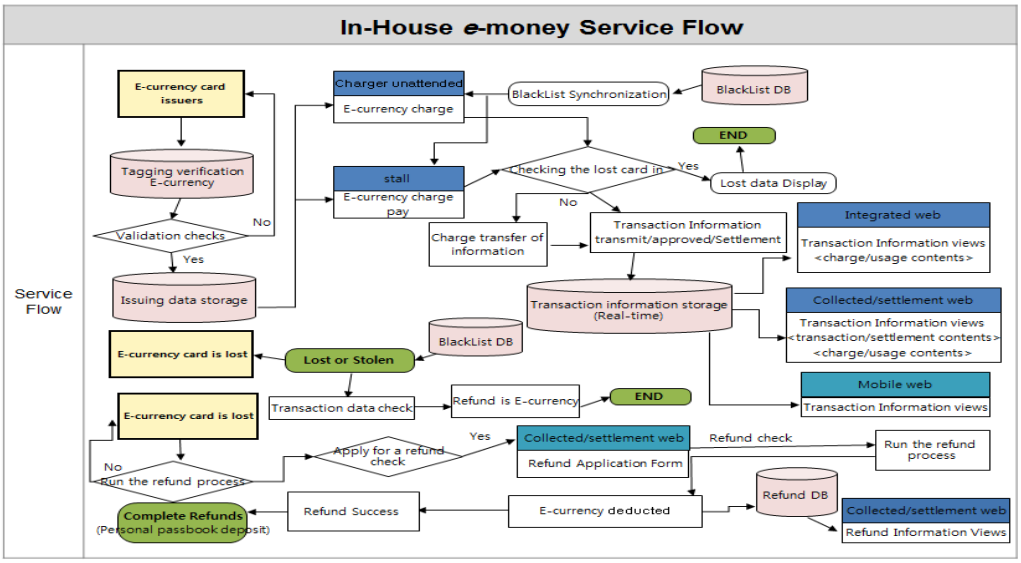

Figure 2. Flow of In-House Electronic Money Service

3.4. Encryption Transfer of Electronic Money for In-House Use

In this study, we used an encryption method with a hash function for the safe transfer of an authorized transaction of electronic money. When using electronic money for in-house use, the material is transmitted with a main server only to authorize a safe charge or transaction. Hash encryption was used twice to transmit safe data in order to prevent illegal abuse during this process. The identification information of a user and the information of service identification that a user attempted to use were hashed first. It was encrypted for the second time with this resulting value and the resulting value that was hashed with the shared secret key that the main system of the electronic money held. The payment and transaction information was safely transmitted. This encryption method is used currently in the i-pin service and is approved for its safety. This study applied this and used electronic money data transmission encryption.

3.5. Implementation of Electronic Money for In-House Use

Users, rental shops, and a charging place for the electronic money should be prepared in order to use electronic money in an organization and to implement electronic money for in-house use in this study. A university with a bookstore, cafeteria, various rental shops, and a shuttle bus service is a good model for the application of electronic money in this study. Further, members of the university should be issued smartcards onto which Java applets can be installed to implement the developed electronic money in this study. After the smart card is issued, the user can convert cash into electronic money with an unmanned charger installed in the institute. Further, the faculty can charge electronic money by deducting wages instead of paying cash. The charged electronic money can be used in a bookstore, cafeteria, café, or shuttle bus service on campus. Moreover, members can pay with the smart card through in-house POS(Point of Sales) in rental shops. The user and the cafeteria owner can check the transaction details with electronic money in the web system.

3.5.1. Issuing Electronic Money SAM: SAM should be issued to use electronic money for in-house use. Various types of SAM is installed in the issuing equipment and the

payment terminal, the charging terminal with the security module that is necessary for the transaction of authorization, payment, and charging of electronic money for in-house use. SAM plays a role in encrypting and generating a signature value to authorize, pay, and charge an electronic money card for in-house use. The SAM used in this study can be sub-divided into payment SAM, charging SAM, issuing PerSAM, and authorization CSAM. Figure 3 shows the diagram of SAM equipped to each terminal device used for the in-house electronic money system.

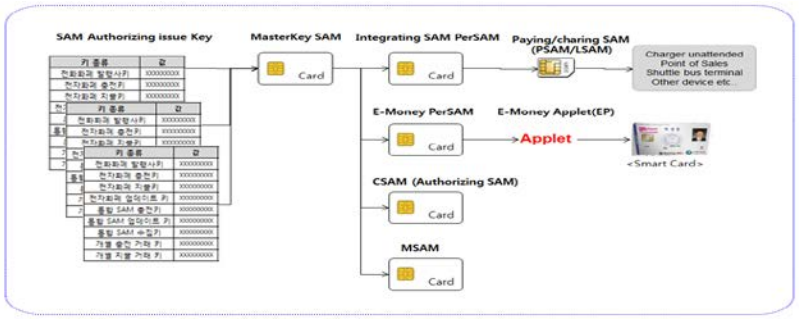

Figure 3. In-House Electronic Money Issued SAM Diagram

3.5.2. Charging Electronic Money: Members of the university charge cash for a user identification card that has an electronic money Java applet and is issued in advance for electronic money. Cash charging is possible in an unmanned charging place or a manned charging POS terminal in the university. Also, in order to provide user convenience for the school staff, the system was designed so that post-paid charge is available without cash. Figure 4 shows a process to charge cash with electronic money in an unmanned charging place in the university. The method of use is as follows. Screen①: insert electronic money card in the charge position and click cash charge button. Screen②: the electronic money balance will be displayed; then insert cash. As in screen③, cash will be deposited. Screen④: the deposited amount is shown on the screen, and the receipt can be printed. Figure 4 is the school staff post-paid charge screen, which emphasizes security by checking personal confidential information to cover cases of card theft.

Figure 4. Electronic Money Charge Process & for School Staff Process

3.5.3. Paying and Checking Usage Detail of Electronic Money: Members A member can pay by using electronic money through a charged smartcard at various rental shops, cafeteria, café, shuttle bus service, and restaurants in the university. Figure 5 shows the process for making payments by using electronic money at various rental shops in the university.Further, the user and the rental owner can check the usage detail of the individuals and the rental shops for each use through an Internet-based system in real time. The method of use in Figure 5 can be explained as follows. Screen①: Click the button in the shape of electronic money. Screen②: when the restaurant menu appears on the screen, click the menu and quantity and click the payment button. Screen③: as shown in the screen, contact the electronic money at the center of the main with the card shape. Electronic money will be deducted as in the screen. Screen④: after use, the remaining amount is displayed on the screen and the receipt can be printed.

Figure 5. Shop Electronic Money Payment Process

3.5.4. Use of POS at Leased Stores*:* Leased stores in university have respective POS for use of in-house electronic money. When the electronic money user wants to use in-house electronic money, POS is used for the payment. The following Figure 6 is the screen of POS installed in each leased store in schools. POS used in leased stores is operated in two forms. The former is POS for calculating the sum amount, and the latter is POS used per menu. Screen① of Figure 6 is POS calculating the sum amount, and Screen② is POS screen used per menu.

Figure 6. POS for Leased Stores

3.5.5. Requesting Payment of Rental Shops: Each rental shop in the university can check the usage detail of electronic money in the POS system and the web system. The

rental shops can request cash from the university by using this checking process. Moreover, the university provides the same service as credit card companies with charging a service fee. Figure 7 shows a process for checking the usage details of electronic money at rental shops. Accessing integrated collection settlement system, it is divided into system management, service management and trade settlement management. System management enables remote management of each equipment used for electronic money, and trade settlement management manages the electronic money charge amount collected from unmanned charging stations and sales of leased stores used at each leased stores.

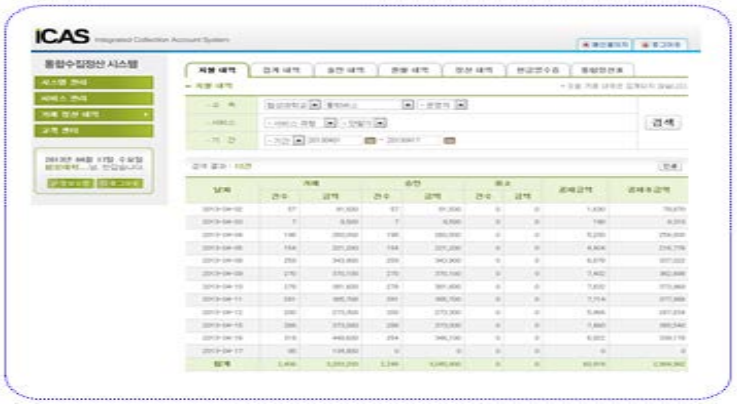

Figure 7. Electronic Money ICAS Settlement System

3.5.6. Loss and Refund of Electronic Money: Electronic money can be classified as personal property. Therefore, in-house electronic money should be refunded upon an individual's request. Moreover, when smartcard charged with electronic money is lost, the loss can be safely reported in order to prevent the lost electronic money from being used. The loss report of electronic money can be made through integrated management system for user. Figure 8 shows the loss report screen in integrated system. After loss report of electronic money, using it at the terminal device will display a screen as in Figure 9.

Figure 8. Electronic Money Loss Report Screen

Figure 9. Electronic Money Terminal Device Loss Display Screen

3.5.7. Electronic Money Integrated Management System for Use: Electronic money can be classified as personal property. Thus, in-house electronic money supports integrated management system to the user for efficient operation. Figure 10 is the integrated system provided to the user, which provides electronic money loss report and electronic money usage history in real time.

Figure 10. Electronic Money Terminal Device Loss Display Screen

4. Conclusion

Electronic money for the in-house use considered in this study can be used in organizations only. Most of the electronic money in Korea uses the (MF)Mifare method that has become the center of controversies recently. In this study, we implemented electronic money by using the Java card method whose safety has been approved worldwide. A Java card, as we know, is considerably safe for financial transactions. Moreover, in-house electronic money requires authorization for safe charging and transactions. The material for this authorization is always

transferred using the main server. Hash encryption has been used twice to transfer safe data and prevent illegal abuse that can be made during the transfer. Further, in-house electronic money can reduce the expensive fee of credit cards and the deposit of electronic money charges in rental shops in organizations. As the central operating body of in-house electronic money can earn user fees, it can be utilized as a tool for making a profit. However, small and mid-sized organizations should consider the initial costs of operating electronic money systems in organizations that come with a high installation cost. Therefore, if a big central operating body supplies the electronic money system for in-house use to small and mid-sized organizations, like T-money, this can be used as another source of profit because all the institutes can standardize some of the operational processes of the in-house electronic money.

References

[1] B. Jayaprakash Kar, "A Novel Fair Tracing E-cash System based on Elliptic Curve Discrete Logarithum Problem", Internal Journal of security and Its Applications, http://www.techrepublic.com/whitepapers/a-novel-fair-tracing-e-cash-system-based-on-elliptic-curve-discrete-logarithm-problem/32493152, vol. 3, no. 4, **(2009)**, pp. 9.
[2] K. Yong Gab, "A Study on the Current Use and Popularization of e-money", Dan-kook University, **(2004)**, pp. 3, 6-13, http://www.riss.kr/search/detail/DetailView.do?p_mat_type=be54d9b8bc7cdb09&control_no=5d3df813f593d3feffe0bdc3ef48d419#redirect
[3] Y. J. Song, "Domestic and International Trends and Prospects of e-money", Institute of Electronics Engineers of Korea, http://www.dbpia.co.kr/Journal/ArticleDetail/311598, vol. 29, no. 11. **(2002)**, pp. 20
[4] H. S. Hong, "A Study on the Current Use and the Direction for Electronic Cash in Korea", Dan-Kook University, http://www.riss.kr/search/detail/DetailView.do?p_mat_type=be54d9b8bc7cdb09&control_no=2eaab38dedeea43fffe0bdc3ef48d419, **(2005)**, pp. 3.
[5] G.-H. Ki, "The Current Situation of IC-card type electronic money and corresponding policy directions", The e-Business Studies, http://www.dbpia.co.kr/Article/1603364, vol. 9, no. 2, **(2008)**, pp. 164-169.
[6] Y.-T. Jang and K.-Y. Yoo, "Design and Implementation of Offline Electronic Cash System using JAVA Card", Korea Institute of Information Scientists and Engineers, http://www.dbpia.co.kr/Article/449799, vol. 26, no. 2, **(1999)**, pp. 547,
[7] Y.-S. Song and I.-C. Shin, "Diversification of User Authentication by Writing Applet on Java Card", Institute of Korea Electrical and Electronics Engineers, http://scholar.ndsl.kr/schDetail.do?cn=JAKO200923557658307, vol. 13, no. 4, **(2009)**, pp. 452.
[8] A. A. Sere, J. Iguchi-Cartigny and J.-L. Lanet, "Evaluation of Countermeasures Against Fault Attacks on Smart Cards", Internal Journal of security and Its Applications, http://www.sersc.org/journals/IJSIA/vol5_no2_2011/4.pdf, vol. 5, no. 2, **(2011)**, pp. 49.
[9] Y.-S. Song and J.-Y. Lee, "Design and Implementation of File System API based on Java Card", The Journal of Information Technology, http://scholar.ndsl.kr/schDetail.do?cn=JAKO200709906220048, vol. 10, no. 3, **(2007)**, pp. 61.
[10] P.-L. Cayrel, G. Hoffmann and M. Schneider, "GPU Implementation of the Keccak Hash Function Family", Internal Journal of security and Its Applications, http://link.springer.com/chapter/10.1007/978-3-642-23141-4_4#, DOI: 10.1007/978-3-642-23141-4_4, vol. 5, no. 4, **(2011)**, pp. 123.
[11] Y.-S. Jeong, Y.-T. Kim and G.-C. Park, "Design of Guaranteeing System of Service Quality through the Verifying Users of Hash Chain", Internal Journal of security and Its Applications, http://link.springer.com/chapter/10.1007/978-3-642-20998-7_40# DOI: 10.1007/978-3-642-20998-7_40, , vol. 4, no. 2, **(2011)**, pp. 13-14.

Authors

Hyun-Joo Kim is a doctor's degree student of Electronics & Electrical Engineering graduate school, Dankook University, Yongin-si, Gyeonggi-do, Korea. Her recent interests are in cryptographic algorithms, java card, i-Pin security, Information Security, security in general and cloud computing. She can be reached at chopin@uhs.ac.kr. ** first author, corresponding author.

Soo-Jong Lee, is a professor of the division of Computer Engineering at Hyupsung University, Hwaseong-Si Kyeonggi-Do, Korea. He received his Ph.D. degree in Electronic & Computer Engineering at Yonsei University, Korea. His recent interests are in signal processing algorithms, image processing, data Communication algorithms, cryptographic algorithms, security in general and cloud computing.

In-Chul Shin is a professor of the division of Electronics & Electrical Engineering at Dankook University, Yongin-si, Gyeonggi-do, Korea. He received his Ph.D. degree in Electronics Engineering at Korea University, Korea. His recent interests are in cryptographic algorithms, java card, Parallel Processing, Information Security, security in general and cloud computing. He can be reached at char@dankook.ac.kr.