Development and Performance Analysis of Multifunctional City Smart Card System

Vedat Coskun, Fahri Soylemezgiller, Busra Ozdenizci, Kerem Ok

***Abstract*—**In recent years, several smart card solutions for transportation services of cities with different technical infrastructures and business models has emerged considerably, which triggers new business and technical opportunities. In order to create a unique system, we present a novel, promising system called Multifunctional City Smart Card System to be used in all cities that provides transportation and loyalty services based on the MasterCard M/Chip Advance standards. The proposed system provides a unique solution for transportation services of large cities over the world, aiming to answer all transportation needs of citizens. In this paper, development of the Multifunctional City Smart Card system and system requirements are briefly described. Moreover, performance analysis results of M/Chip Advance Compatible Validators which is the system's most important component are presented.

***Keywords*—**Smart Card, M/Chip Advance Standard, City Transportation, Performance Analysis.

I. Introduction

TODAY smart cards are utilized in a wide range of service domains including finance, health, government, and transportation. Appropriate standardization on interoperability and security of smart cards has an important impact in this development. The use of smart cards as an alternative mean for public transportation services has become a viable option for many countries.

Up to now, several smart card solutions have been proposed and implemented in public transportation with different technical requirements and business models [1]. One of the most popular implementation is the Oyster smart card by Transport for London [2], [3] which is a contactless smart card and can be used on buses, trams, tubes, London Overground, riverboats, and national rail within London. Similar to Oyster Card, some other cities also performed their own public transportation solution such as Nottinghamshire Card [4], YOR-Card [5] for West Yorkshire Region, Istanbulkart [6] for Istanbul, and so on. Also it is possible to see different smart card systems and models in one city.

However, it is seen that payment cards of banks are not efficiently used in supporting transportation services due to some technical and business challenges (e.g., requirement of a citizen who uses that public transportation smart card as a customer of a bank to deposit his/her card, or credit card verification and authorization problems in offline transactions, applying discount problems).

One of the reasons behind this is that the existing standards provided by EMV (Europay/Mastercard/Visa) are mainly focusing on payment and financial standards. They do not support the transportation, loyalty or other type of services on the same smart card.

In this paper, we explain the developed Multifunctional City Smart Card system and performance analysis results of the system's most important component; M/Chip Advance compatible Validators is presented briefly. Proposed city smart card's most challenging feature is that it is based on a new emerging technology; M/Chip Advance introduced by MasterCard [7]. M/Chip Advance standard aims to improve existing transportation and loyalty services significantly by adding payment services on the same smartcard. The presented city smart card system takes advantage of M/Chip Advance standards and creates a multi-application debit card by integrating transportation and loyalty services to the payment services.

II. Multifunctional City Smart Card System

According to the city smart card, users obtain their personalized city smart cards easily from card issuers (i.e., transportation authority, authorized vendors and other distribution channels), and can simply deposit their debit cards using authorized POS and kiosk machines or other appropriate loading systems. Hence, the debit card with enough deposit is ready to be used in transportation, loyalty as well as contact and contactless payment services. The card securely stores transportation information such as latest balance data, vehicle usage information, subscriptions, and discount information, as well as loyalty/membership data of the citizen on relevant slots on M/Chip Advance compatible smart cards. Major features of the city smart card are listed below:

- Compatibility with global specifications so that it can be used all over the world,
- Consisting of data slots for loyalty services, not only for public transportation and debit card services,
- Balance record and other valuable data can be stored on it,
- Have contact and contactless interfaces to support all type transactions,
- High speed and high security,
- Can be personalized easily by the card issuer.

Vedat Coskun is with Information Technologies Department, Işık University, Turkey (phone: +90216 528 7193; e-mail: vedatcoskun@isikun.edu.tr).
Fahri Soylemezgiller is with [1]PROVUS Information Technologies, Istanbul, Turkey.
BusraOzdenizci is with Information Technologies Department, Işık University, Turkey.
Kerem Ok is with Information Technologies Department, Işık University, Turkey.
M/Chip project is funded by TÜBİTAK and Provus A.S.

III. Usage of Multifunctional City Smart Card

A. Distributing City Smart Card

There are several options for obtaining the M/Chip Advance compatible smart cards. The users can obtain their own personalized city smart cards directly from transportation authority in that city, authorized vendors or other distribution channels.

B. Depositing City Smart Card

There are also many alternatives for depositing M/Chip Advance based debit cards. Users can deposit their smart cards by cash or with their other payment cards through proprietary software POS machines which are located in certain places of the city such as transportation authority's ticket offices and kiosk machines. Users can also deposit their card using remote loading techniques such as money order from banks, EFT, the virtual POS and automatic payment orders. Another way is to perform online depositing transactions from ATM or contact/contactless POS machines of banks. Since the balance is stored on the chip, the balance information needs to be transferred to the issuing system in online ATM and POS transactions. In this case, verification of the balance information and some cryptology operations and advanced systems is built on the back end of the card system.

C. Using City Smart Card

The smart card which has enough deposit amounts can be used for public transportation and debit payment services. If it includes loyalty services on other slots, it can be used for the loyalty and membership services of the companies as well.

IV. Development of Multifunctional City Smart Card System

To enable the city smart card model, the following requirements for the system are carried out:

- *Preparation of Personalization Data:* The personalization data is redesigned and prepared for the M/Chip Advance compatible smart cards since M/Chip Advance is a new standard that requires new data elements and production of new keys and certificates.
- *Creating Advanced Algorithms for Reading and Writing on Data Slots:* Since EMV standards are mainly focused on payment operations, these standards become insufficient for carrying large amount of data on the smart card chip for supporting services like transportation and loyalty. M/Chip Advance technology enables carrying large data (i.e., 160 bytes for data storage fields) on the smart card chip. With advanced and optimized algorithms, the data can be read from/written on these data slots of the smart card which are created during personalization of the card phase.
- *Creating and Activating Data Slots:* All of the smart card's all slots are created during the card's personalization process and each slot is protected by a key. The issuer of the city smart card which is generally the transportation authority in the city reserves one or more slots on the card for its own usage. The transportation authority tracks all the transactions on its own validators that are performed by the users. All transaction and balance information is stored the chip of the card.
- *Assigning Data Slots:* Remaining data slots of the smart card can be assigned to other companies such as gasoline companies or supermarkets for promoting loyalty/membership services. The card issuer can make business agreements with other companies and providing the data slot(s) key to the company. Hence companies do not need to produce and create loyalty smart cards by themselves. The loyalty information is also stored on the card and the company updates the information on the corresponding slot through proprietary terminal software.
- *Development of M/Chip Advance Compatible Validators:* The transportation authority also needs to develop proprietary software and terminals for enabling the transportation service. These validators need to read/write and update information on the city smart cards.

V. Analysis of M/Chip Advance Compatible Validators

For development of validator software, first M/Chip Advance compatible EMV Kernel is uploaded and then M/Chip Advance smart card operating features are built on these validators. Then the required tests are performed; for different terminals and different products, validator software is observed, and some development and improvements for increasing the performance is done. Fig. 1 illustrates an EMV work flow in detail. Table I shows the EMV Kernel's processing times on different terminals (i.e., notebook, mini PC, validator) and different products (i.e., MasterCard M/Chip Advance, MasterCard M/Chip Advance (without IDS) and MasterCard PayPass).

- According to Tables I and II, on some EMV steps due to too much encryption operations and data exchange, it is seen that there is some time loss between terminal and smart card.
- For all three smart card products, validator shows the worst performance when compared with other two terminals (i.e., notebook and mini PC).
- On *Select Application* step, processing times differences is seen between smart card products (i.e., MasterCard M/Chip Advance, MasterCard M/Chip Advance (without IDS) and MasterCard PayPass). M/Chip Advance smart cards' response duration is longer than the others due to existence of IDS mechanism on M/Chip Advance smart cards. There is no IDS mechanism on PayPass smart cards, so operation duration is shorter.
- On *Select Application* step, the terminal selects the relevant application on the smart card. There are two methods to perform this process. The first one is that, terminal sends SELECT command and PSE (Payment System Environment) command to the smart card. Then, with READ RECORD command, terminal reads all the applications on the smart card and lists them. Then,

terminal sends again SELECT command to the card and selects the appropriate application from the list. The second method is that, terminal sends the supported applications to the smart card in sequence with SELECT command. When the card gives positive response for an application, the process starts. For achieving maximum performance, both methods are experienced and analyzed on terminals. The second method is selected due to minimum data exchange between smart card and terminal, and this method is improved for achieving the best performance.

TABLE I
EMV KERNEL PROCESSING TIMES ON DIFFERENT TERMINALS

	Notebook	Mini PC	Validator
M/Chip Advance	555 ms	578 ms	755 ms
M/Chip Advance (without IDS)	451ms	453ms	637ms
Paypass	450ms	453ms	617ms

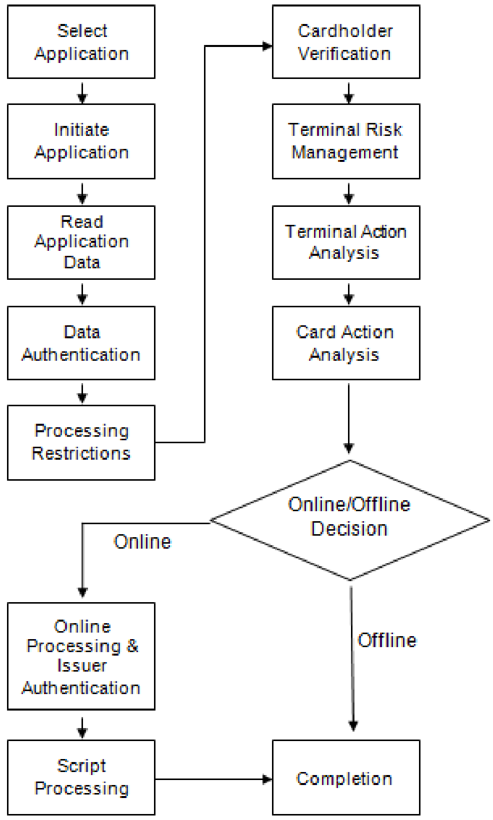

Fig. 1 EMV Work Flow

TABLE II
OPERATING RATES ON EACH EMV WORK FLOW STEPS

	Notebook			Mini PC			Validator		
	MChip Advance	MChip Advance (without IDS)	PayPass	MChip Advance	MChip Advance (wihtoutIDS)	PayPass	MChip Advance	MChip Advance (without IDS)	PayPass
Select Application	62ms	61ms	37ms	62ms	62ms	46ms	75ms	74ms	52ms
Initiate Application	52ms	33ms	34ms	63ms	31ms	32ms	69ms	47ms	40ms
Read Application Data	120ms	119ms	130ms	125ms	110ms	140ms	219ms	220ms	239ms
Data Authentication	0ms	0ms	1ms	0ms	0ms	0ms	22ms	22ms	22ms
Processing Restrictions	0sm	0ms	0ms	0ms	0ms	0ms	0ms	0ms	0ms
Cardholder Verification	0ms	0ms	0ms	0ms	0ms	0ms	0ms	0ms	0ms
Terminal Risk Management	0ms	0ms	0ms	0ms	0ms	0ms	0ms	0ms	0ms
Terminal Action Analysis	0ms	0ms	0ms	0ms	0ms	0ms	0ms	0ms	0ms
Card Action Analysis	321ms	237ms	248ms	328ms	250ms	235ms	370ms	274ms	264ms
Completion	0ms	1ms	0ms	0ms	0ms	0ms	0ms	0ms	0ms
Total	555ms	451ms	450ms	578ms	453ms	453ms	755ms	637ms	617ms

- On *Initiate Application* step, there are significant processing time differences on terminals as well as on smart cards. The M/Chip Advance smart cards with IDS mechanism is performing the operation in a long time (~20 ms more) when compared with others.
- On *Data Authentication* step, DDA (Dynamic Data Authentication) is generally performed. Our smart cards also support more advanced authentication mechanism called CDA (Combined Data Authentication). On notebooks and Mini PCs usage of this technique does not create any time loss, however on validators for all smart card products approximately 22ms time loss is seen due to occurrence of RSA encryption algorithm twice.
- Steps of *Processing Restrictions, Cardholder Verification, Terminal Risk Management* and *Terminal Action Analysis* are performed successfully.
- The most spent time is on Card Action Analysis step. On this step, CDA and IDS operations are performed on both smart cards and terminals which create significant time differences.
- It is seen that in all experiments length of IDS data slots has direct impact on the operating rate, processing time (Table III).

TABLE III
PROCESSING TIME OF M/CHIP ADVANCE SMART CARD USING IDS AND NOTEBOOK AS TERMINAL

IDS Length	160 byte	80 byte	40 byte
Processing Time	615 seconds	575 seconds	555 seconds

VI. CONCLUSION

City smart card is one of the first transportation smart card implementations over the world which uses the new emerging standard; M/Chip Advance technology. M/Chip Advance enables to use transportation and loyalty services on the same smart card concurrently and also enable to use all MasterCard based payment cards in transportation and loyalty transactions. Moreover the city smart card is not restricted to a region, a city or even a country on the contrary to the existing business solutions.

Since the city smart card is based on global standards (i.e., EMV and M/Chip Advance), it can be used on all POS and ATM systems over the world, which provides a global and unique business solution. Another important improvement is that the card provides large data storage slots on its chip. The number of the data slots depends on the capacity of the chip.

In performance analysis of the validators, it is seen that due to too much encryption operations and data exchange, there is some time loss between terminal and smart card on some steps. Also it is seen that length of IDS data slots has direct impact on the processing time.

For improvement of this study, M/Chip Advance smart card alternatives from different smart card suppliers in the market can be examined in terms of performance and the same tests can be performed. Similarly different validator models can be examined in terms of performance after upload of M/Chip Advance compatible EMV Kernel.

REFERENCES

[1] Coskun, V., Ok K., and Ozdenizci, B., "Near Field Communication (NFC): From Theory to Practice", Chapter 2, Chapter 4 and Chapter 9, John Wiley and Sons, ISBN: 978-1-1199-7109-2, February 2012.

[2] Osyter Online, Transport for London, https://oyster.tfl.gov.uk/oyster/entry.do/. Access date: 28 December 2013.

[3] London P., The London Oyster Card, Proceedings of the Transport Card Forum, Smartex, Newcastle, November 2003.

[4] My Citycard, http://www.citycardnottingham.co.uk/. Access date: 28 December 2013.

[5] Keith B., What do Bus and Rail Operators Want from Smart Cards?, Proceedings of the Transport Card Forum, Smartex, Newcastle, November 2003.

[6] IETT, Istanbulkart, http://skart.iett.gov.tr/. Access date: 28 December 2013.

[7] V. Coskun, B. Ozdenizci, F. Soylemezgiller, M. Kalender, "Multifunctional City Smart Card based on M/Chip Advance Technology", *The Conference on Web Based Management*, pp. 469-472, Schangai, China, 21-23 September 2012.