SED 2011
HIGH BUSINESS-TECHNICAL SCHOOL OF UZICE, SERBIA

4th International Conference
"SCIENCE AND HIGHER EDUCATION IN FUNCTION OF SUSTAINABLE DEVELOPMENT"
SED 2011
7th and 8th of October 2011, Uzice, Serbia

ADVANTAGES AND DISADVANTAGES IN IMPLEMENTATION OF SMART CARDS IN PAYMENT SYSTEM

Miroslava Jordović Pavlović
Technical school , Užice, Serbia, miroslavajp@gmail.com

Summary: Society has experienced the quickest changes in its history at the end of the last and the beginning of the millennium. There have been changes in the way in which many activities are being done, the changes in work structures, market and other fields. In this way, the industrial society evolved into informational. One of the significant trends in the development of technology is more frequent application of payment cards and greater electronic possibilities in this field, which enables new services. Unfortunately, as the card industry largely spread, the crime in misusing cards is becoming larger. Because of these reasons, the technology of producing these cards is continuously in progress. The migration from mag-stripe card to smart card became something inevitable and long-term plan of the most of European countries. This paper analyze the application of new technologies in card industry and estimates achievements.
Keywords: smart card, contactless card, EMV,NFC

1. INTRODUCTION

Credit cards appeared in the USA during 1920s, when some firms as petrol companies and chains of some hotels started to implement it in their business. These credit cards were of limited type, they could have been used only in selling/servicing objects of the company which edited them. The first universal credit card, which could have been used in various selling/servicing objects, was edited by Diner's. Club Inc. in 1950. The second significant card was launched by American Express Company in 1958. Later, banking system of credit cards appeared, where the bank approves to the account of the merchant the sum of money as soon as it receives the bill for sold goods, collecting the sum which will be counted to the card owner at the end of agreed period. The card owner pays this sum to the bank, total sum or in monthly rates with interest. The use of credit cards out of America has been spread recently, considering the fact that, until the end of 1970s, the level of their usage in Europe was low. The biggest companies in credit card business organized separate electronic clearing and accounting systems. Master Card and Visa have their own networks, which are used for verification of transactions all over the world. These networks are being spread and improved, simultaneously with the acceptance of credit cards by customers.

The conditions on the credit cards market in our country according to report of the Chamber of Economy of Serbia, from March 2011, says that after the intensive development in 2005 and 2006, in the last four years, the growth has been moderate but continuous. The total number of edited payment cards in Serbia, at the end of 2010, was 6.15 million, which is 2,3% more than at the end of 2009. On ATMs in 2010, there were 52.0 millions of transactions which value is 312.6 billion dinars, and on POS terminals, there were 64.2 millions of transactions which value is 141.6 billion dinars.

However, beside the positive trend of the card industry development, there is serious increase of the crime which is connected with these cards. According to that report of Chamber of Economy in Serbia in 2010, 707 crimes which are connected with credit cards were committed whereas in 2009, 393 crimes were committed.

Figure 1: Smart card

Bearing in mind that investment in developing new technologies was on a low level during the economic crisis, it can be expected that, in the future, by introducing of new technologies, better service to the costumers of the cards can be achieved as well as better safety of the whole system of the payment without cash. The transfer from mag-stripe cards to smart cards or chip technologies will have the main rate.

2. SMART CARD HARDWARE

Smart card is nothing other than PC in small package. The integrated circuit which is implemented in the card contains:

- Processor (CPU), which serves for calculations, with data width 8,16 or 32 bits and additional crypto coprocessor which serves for implementation and processing of the crypto algorithms and uses different set of protection mechanism.
- Read-Only Memory (ROM), memory where the operating system is stored, capacity of the ROM is 64 KB or more
- Random Access Memory (RAM) , memory for temporary storing
- Electronically Erasable and Programming Read-Only Memory (EEPROM), memory with data of interest (account number, certificates, keys, etc), capacity of EEPROM is 16-32 KB or more.
- Clock
- Input / Output device over which chip can communicate with environment (reader), the speed of the device is from 9.6 kbps to 115 kbps

3. SMART CARD SOFTWARE

Smart card has operating system and set of application which depend upon the firm which made them. It means that most of smart card applications have limited field for implementation, because application written for one operating system will not work on other. The standardization of operating system for smart cards solves the problem as well as agreement about the standards for applications. One of the ideas is existing of the Open operating system.

4. EMV SPECIFICATIONS OPEN THE DOOR FOR SMART CARDS IN PAYMENT

Three of the leading card associations—Europay, MasterCard, and Visa (EMV)—began working on specifications for smart card-based debit and credit payments. First released in 1996, the EMV specifications provide a strong, yet flexible framework—opening the door to the widespread use of smart cards in payment. By creating a much-needed base for interoperability between chip cards and terminals on a global basis, these specifications provide a reliable global framework for the growth of smart card payment applications. In addition, EMV-based smart cards offer a solid foundation for a broad selection of payment-related and non- payment applications such as stored value, e-purse, and loyalty. Over time, these value-added applications promise to deliver greater financial benefits in new revenues than the savings available from the reduction in fraud.

The EMV specifications focus on the interactions between smart cards and payment terminals. (Note—The specifications *do not* address the exchange of information between POS terminals and the host computers at processing centers.) The specifications are designed to apply to a variety of terminals and devices, such as bank automated teller machines (ATMs), POS terminals, electronic cash registers, and PCs. EMV specifications cover elements such as general physical characteristics of terminals, the terminal–card interface, transaction processing, data management, and of course—data security requirements.

Interoperability is achieved by granting two levels of "Type Approval":

Level 1—Applies to the mechanical, electrical, and logical interfaces between chip cards and payment devices

Level 2—Governs all application software. The EMV specifications envision that there likely will be multiple payment, payment-related, and even non- payment applications on each chip card—ranging from traditional debit and credit applications to other value-added solutions.

5. SMART CARD - READER COMUNICATION

According to the method of communication between the smart card and the reader, there are three types of cards that can be distinguished:

- Contact card or card with direct reading of data. This card has a contact chip in which the data reading is performed by placing card into reader.
- Contactless card or card with indirect reading of data. This card has a contactless chip in which the communication is done indirectly, via integrated antenna with a range up to 10 cm, usually up to 4 cm.

- Card with combined reading of data (dual interface). This card has a chip in which the reading can be performed by direct contact and contactless communication with the reader as well.

6. EXAMPLES OF SMART CARD USAGE

Smart card enables personalization in the way that user of card chooses.
Example 1: Every morning you go to your favourite café to have cup of coffee. After you have finished your coffee, you want to pay by smart card. Kind waitress, after putting your card in reader, informs you that it is your 10 coffee, which is free of charge, so that you don't have to pay.
It is loyalty application. The number of users of this function increases almost every day.
Example 2: You have to go to a business trip abroad. On air travel site you confirm the booking for a certain flight. They ask you to insert your smart card, if you have one, into the reader, which is connected with your PC. In this way, you will avoid so many questionnaires. There is the information on the card about which seat you want, that you are a vegetarian, etc. Soon afterwards you are informed that your e-ticket is waiting for you at the airport. Of course, when you go to the airport, there is always a traffic jam, but it is not a problem, any more. You arrive a couple of minutes before your flight, you go to the place where is the reader for your card, you put your card in the reader and you board the plane.
Example 3: You are a student, away from your home and you run out of money but you need it urgently. You phone your home and you tell your mother that you need money to buy a book for your exam. Your mother, after thinking about it, insert her smart card into the terminal, you insert yours into the terminal and a certain amount of money is transferred to your card.
Example 4: You want to bay some CDs. Over the Internet you go to a site of some music on line shop. After you have chosen a CD, all you have to do is to insert your smart card into the reader and everything is finished.
You don't have to fill in your account number, name, surname, address or other data. Everything is fast, simple and safe.
All the data, necessary for functioning of these examples, are implemented in only one multifunctional smart card. Content of the smart card (or the whole card) can be placed into a mobile phone (the SIM card, the phone's memory, the SD card) and thus, instead of standard form of a plastic card, the user has all in a mobile phone, always with him and always ready for use. There are many examples. As for the service itself, it is available with some other technologies, but with a smart card, it becomes much easier.

7. INTELLIGENT ARGUMENTS FOR SMART CARDS IN PAYMENT

As it is already mentioned, one of the main advantages of smart cards is multifunctional card, thanks to many applications which can be implemented into the card. Among them is already mentioned loyalty application, fast checking of customer's paying abilities, effective paying operations while baying goods and services. Intelligent credit cards enables paying and charging without the use of papers, electronic transfer of the means in the real time between bank account of buyers and sellers over computer networks. There are personal data in EEPROM about the owner, account number, certificates etc.
One big advantage of smart card technology is safety. The security of a smart card includes four components: body of a card, chip architecture, operating system and applications. Body of a card contains some visual features that are visible to a man. These are holograms, relief settings, ultraviolet text, laser engraving, and so on. The techniques of security features implementation are common for all types of cards; they are not specific only for the smart cards. The other components such are chip architecture, operating system and application, protect data and programs stored on the card.
Mechanisms for the protection of smart cards are numerous and include both hardware and software levels of their functioning. In the process of developing a smart card, security measures to ensure the integrity of the data on it, are being introduced: Development of a smart card processor architecture; Development of operating systems for smart cards; The principle of split knowledge; Security at physical level of the card; Encoding Memory

1. Development of smart card processor architecture has taken place recently. It involves a small number of people working under strictly controlled conditions. The systems used for development are completely separated from the outside world. Chip design and its mechanisms of protection are submitted for testing to the independent organizations. They reveal intentional and unintentional oversights and errors in terms of safety, thus reducing the possibility of attack from the developing system itself. The layout of the components on a chip is very important for attackers, if they look for the physical aggression on the card data. The unique chip number that is placed in WROM memory, with the sensors and the protective layers, represents a hardware security element. The chip number is used in the formation of a key. Also the chip

number is used in the formation of cards "black list", which is then used for marking and removing the suspicious cards from the system.

2. Computers that are used to develop operating systems for smart cards are in a completely isolated network, without any possibility of external access. Development tools such as translator and simulator are subject to verification and testing. Two different programmers are often engaged in order to ensure validity of the translation software. The time of development of the operating system can be significantly reduced by introducing additional commands for the purposes of testing. Those commands can often read vital parts of the memory, bypassing security mechanisms. Carelessness may cause them remain in the operating system, which can be used for later attacks.
3. The principle of split knowledge (secret sharing) is opposed to the principle that everyone knows everything about everything. The tables, program code and configuration data are loaded to the EEPROM memory. The chip manufacturer, who receives the final ROM code for the output of production masks, does not have complete knowledge of the operating system, because he is not familiar with parts of the operating system stored in EEPROM. The ROM code analysis can not fully detect security mechanisms and functions of the operating system. In this way, the software is fully protected from internal attacks.
4. The smart card chip design does not allow use of standard cells developed for mass production of semiconductor components, in order to prevent quick and easy copying.
5. Most commonly applied method to protect data stored in a memory is memory encoding. The main secret is in the method and the key by which memory is encoded. By simple, unauthorized access to the memory space, the attacker will see incomprehensible values. Card encryption key must be unique for each card, or even based on a dynamic change of encryption methods, in order to achieve higher level of security. Various methods are used; the standard methods of encryption such as DES, Triple DES, RSA and so on. The text can be encrypted by a combination of two keys - public key and a secret card key. It is necessary to apply the same combination of keys for decoding.

Smart card is based on the control of the access to the data which are stored in EEPROM by its own security operating system in ROM. In EEPROM you can find private RSA key, which will contribute to a higher level of safety by the use of asymmetric algorithms of the crypto protection. System that are designed well use various security measures. In order to use a card, it is necessary to know the code for activation, PIN. The existence of PIN decreases the possibility of card misuse in the case the card is stolen or lost. Identification by PIN code is safer than any other way of identification, because of the reason that PIN code never travels by network. Instead of PIN, it is possible to use the finger print for the identification of the owner. By using this method, the level of security is higher and the identification process is technically more simple. The only problem is to provide reader which supports this. Card reader can also check the authenticity of smart card by sending a chosen word to smart card. It is required from the card to sign the sent word by its private key which only it possesses, to return the sent word to "outside world" where, by public card key verification is being done. How the data will be protected depends on the processor possibilities and free memory space. The more progressive processor and more free space in memory the possibilities for protection are greater.

Mag-stripe card can be easily cloned, differently cloning of smart card is almost impossible. This fact will significantly reduce misusing of the smart card.

8. CONTACTLESS SMART CARD

We find contactless cards most interesting for our analysis, given that they are the ones that are current in the payment card system, today. Especially, because of the fact that they can be used in mobile phones for the use of mobile payments.

The antenna in a contactless card is situated in the card body. The power supply of such chip card is done by an internal battery, or electromagnetic induction through the built-in antenna. The data are transmitted to a reading device through electromagnetic field and are modulated by amplitude or phase modulation. The chip achieves no mechanical contact with the reader. That means there is no possibility of electric or power shock, and thus the life of the smart card is extended. Because of the potential short-time transactions, only limited amounts of data are transferred.

Figure 2: Master Card's Pay Pass is active in 36 countries

Contactless cards have only few limits. The main drawback is the maximum distance up to 10 cm or usually 4 cm, which is required in relation to the reader. The sensitivity to mechanical damage increases if it comes to bending and twisting the plastic card base. An important drawback is the high price and complete standardization, especially in field of mobile payments (NFC standards) .

Although, leading card organizations announce set of standards for the contactless

payments, the standards for contactless cards are still under construction. Near Field Communications is one of this standard.

The question is: why they have not been implemented yet?

Mobile payments enabled by Near Field Communications technology for years have been a concept for a business reality. NFC technology is a communications-based network that allows users to make mobile payments by placing a radio microchip-equipped smart phone in front of a corresponding point-of-sale (POS) unit at a merchant.

Carriers, platform providers and financial services companies have indicated their interest in commercializing mobile payments, yet challenges remain to getting systems off the ground. Furthermore, the complex and interlocking set of relationships among the parties involved mean business models are still being tested, and it is far from certain that any such effort will find mass-market acceptance. James Anderson, a board member of the NFC Forum and the head of mobile product development at MasterCard, said in December 2010, that, just like with credit cards, NFC interoperability is crucial to creating a global ecosystem. There is also envision for making different displays and parts of stores NFC-enabled, not just POS terminals at the register. For instance, an end-cap display in a retail store could be NFC-enabled so that customers could purchase goods placed there.

Other players in the mobile industry also are ramping up their own potential mobile payment solutions. Nokia, which currently has four commercial NFC-enabled handsets, plans to bring NFC capabilities to more of its Symbian phones next year, said Nokia's team. Further, Google integrated NFC support into Android 2.3, and analysts speculate it could start its own mobile payments initiative. Research In Motion has made similar comments about its BlackBerry platform. A bigger push could come from Apple. Apple named NFC veteran Benjamin Vigier as product manager of its mobile commerce unit in August 2010, and also filed for several NFC-related patents earlier this year.

Figure 3: Nokia's 6131 sports NFC technology

The system, through the lens of an actual user's progress through an NFC purchase, works like this:

Step 1 A customer buys an NFC-enabled smart phone from a carrier.

Step 2 The customer links their phone to their bank or credit card account through a secure, over-the-air provisioning process provided by their carrier. Then, that customer's personal profile is generated, and is loaded onto their phone.

Step 3 When that customer finds something to buy in a store, they wave their phone over an NFC-capable POS terminal that is connected to a payment network operated, for example, by Discover.

Step 4 The customer's account information, along with other dynamic data, is securely passed to the terminal. Then the terminal performs a "challenge," asking the phone if it is OK to accept the amount.

Step 5 That command then gets routed from the merchant to an acquiring bank affiliated with the payment network. Then the payment goes through the secure payment network to the customer's issuing bank to determine if the payment can be authorized.

Step 6 The process goes back through system in an instant, and a customer can walk out and go home with their purchase.

Figure 4: user progress through an NFC purchase

Where are the problems?

- All along this route, various players are trying to get a piece of the value of the customer's transaction.
- Gloria Colgan, senior vice president of emerging payments at Discover Financial Services, said: "There's any number of different form factors and different point-of-sale systems. You have complexity up and down the stream. So getting change through that system is not easy."
- Jaymee Johnson, the director of strategic development for T-Mobile, said:"We love the idea of mobile, but we need one standard. What we can't have is a bunch of different standards where it works differently on every carrie.''

9. CONCLUSION

1. Migration from magnetic stripes to smart cards is a complex process; it requires extensive changes in infrastructure of the issuer of payment cards. There are particularly large changes in the system for preparing data for personalization (part of the system that provides keys, certificates, additional parameters) because smart card provides a lot more than the magnetic one, but the personalization process is more complicated. To enable smart card personalization, additional information and applications should be provided.
2. Significant investments are required in part for smart cards acceptance. Upgrading of the existing infrastructure for acceptance (this mainly refers to the POS terminals) is generally not possible, but the equipment for acceptance must be replaced with the new one. In addition to changes in the place of acceptance, smart card technology requires changes in all other parts of the system in which processing of the transactions initiated by the smart card is performed.
3. Well-established specifications for magnetic stripe cards allow these cards to be used in virtually any card-based POS device worldwide. Smart card technology is relatively new and not yet as widespread as the technology of magnetic stripe cards. As for the most developed European countries, we can say that the migration to smart technology is complete, in other countries migration is in different stages, while in the USA for example, migration actually has not even started due to the specifics of the market and the place and role of the United States in the world. Smart cards in Serbia have been around for a long time. Migration on the side of acceptance is 100% completed while on the side of issue, there are banks that have not started the process, but it should be noted that all the major banks have completed it. What lies ahead in Serbia is migration of the national Dina Card to smart technology. The start of the Dina Card migration is planned for the beginning of 2012.
4. We should also make sure that it is not sufficient to implement the latest technology only on the issue side, if it is not accompanied by the acceptance side. The safest (and therefore the most expensive) card is almost equally as vulnerable to any other, if acceptance position (POS terminal) can not provide the smart card reception - or even if the acceptance of smart card is provided, but the application itself at the reception area is not in accordance with the latest standards (or keys are not loaded in the required length), it is possible that the card is rejected simply because of incompatibility.
5. Although the multifunctional smart card (example of possible multi-usage: in-store payments, loyalty points collecting, advanced identification, driver's license, payment of public transport ...)is advantage, has not essentially become mass real, not for technical reasons. Sometimes it is not easy to harmonize the desires and needs of multiple institutions while using a single payment card, so it usually uses only one function of the smart card, or sometimes just two.
6. Standardization in the payment cards system has been solved by EMV specification. What is not resolved completely is the standardization in the field of contactless payments, in particular contactless payments by mobile phones. This is currently under intensive construction since all predictions are pointing in the direction of replacement plastic payment cards with payment via mobile phone. Migration to mobile phone payments is much more complex process than the migration from magnetic stripe to smart card, because it involves another factor, the factor that has not been there before - a mobile operator.

REFERENCES

[1] http://www.E-trgovina.co.rs ,author dipl.ing. Branislav Popovic
[2] http://www.fiercemobilecontent.com
[3] http://www.pks.rs
[4] http://www.verifonedevnet.com