

SMART CARD APPLICATIONS OVERVIEW AND A PROPOSAL FOR INTEGRATING DRIVING LICENSE CARD WITH CITIZENSHIP CARD

Bahar (Alakent) Karaođlan
E.Ü. Uluslararası Bilgisayar Enstitüsü
Bornova, İzmir, 35100 TÜRKİYE
E-mail: bahar@ube.ege.edu.tr

Kayhan ERCİYES
E.Ü. Uluslararası Bilgisayar Enstitüsü
Bornova, İzmir, 35100 TÜRKİYE
E-mail: erciyas@ube.ege.edu.tr

Abstract

Immense developments in electronics have made it possible to have memory storage and processor power in a single integrated chip. Packing this chip in a card made the card “smart”. Smart cards can act as payment vehicles, access keys, information managers and marketing tools. With new open and communication technologies these cards can be multifunctional and downloadable from the air.

Here, a survey of major smart card applications worldwide is introduced. Use of smart cards in a public transportation system involving buses and train in İzmir is presented as a case study. Then, a design for integrating MERNIS identity number project with citizenship card, driving license and restricted e-purse applications is proposed.

Key Words: Smart cards, memory cards, microprocessor cards, citizenship card, e-purse.

1. Introduction

The first plastic payment card for general use was issued in 1950 by The Diners Club. Entrance of Visa and Mastercard into the field led to a very rapid proliferation of plastic money. As the technology evolved so did the plastic cards and more applications became possible. Allen and Kutler (1997) group applications enabled by smart card technology under five categories:

1. Smart cards as payment vehicles
2. Smart cards as access keys
3. Smart cards as information managers
4. Smart cards as marketing tools
5. Smart cards as customized delivery systems.

The first improvement to the plastic card is the magnetic strip on the back of the card. This allowed digital data up to 1000 bits to be stored on the card in machine-readable form as a supplement to visual data. Identification of the cardholder, which has been done with signature, changed to be done with a secret personal identification number, PIN. PIN is

stored in the hosting system for security reasons. Data stored in magnetic strip may be destroyed, read or changed with an access to the equipment. This means only on-line transactions which result in considerable data flow are allowed.

Enormous development in electronics made it possible to store integrated data with arithmetic logic in a small chip measuring few square mm in dimensions. French PTT pioneered using microprocessor chip in card in 1984, by carrying out a field trial with telephone cards. Smart card with the ability of saving secret keys and executing cryptographic algorithms proved to be an ideal medium for financial transactions. The French banks were again first to implement the technology in 1984 (Rankl & Effing, 2000).

Completion of EMV (Europay, Master and Visa) specification in 1994 is an important milestone for the wide acceptance of smart cards to be used for financial transactions. Many different applications appeared in the market following the mass production of smart cards which resulted in low costs. Smart Card was prescribed as the access medium for the European digital cellular phone system (GSM). There are currently more than 20 European countries using electronic purse. Austria was the first country in the world to have a nationwide electronic purse system with the issue of multifunctional smart cards with POS functions, an electronic purse and optional additional applications in all of Austria in 1998 (Rankl & Effing, 2000).

The smart card's high degree of functional flexibility inspired completely new areas of use that extends beyond traditional card applications. With the downloading capability, existing applications can be improved and new ones may take effect without changing the card. Much work is being done to house all kinds of applications considered under e-purse and financial transaction on a single card. Smart card's use has been extended to the fields of integrated government services like social security, tax collecting, justice and other fields where personal information is needed.

As seen above even though the idea of using plastic cards appeared as early as fifties, wide acceptance comes in parallel with the evolutions in electronics and telecommunication that enabled fast, convenient and secure services.

Section 2 of this paper addresses technical aspect of smart cards and section 3 gives some applications. Section 4 is a case study for smart card use in İzmir transport system. Section 5 presents a proposal to integrate driving license card and fare payments onto citizenship identity card; and the last section is the conclusion.

2. Technical Aspects of Smart Cards

Cards can be classified into three groups: embossed cards, magnetic strip cards, smart cards.

Embossed Cards

The embossed characters on the card are visually readable and can be easily transferred to paper through a simple device. The simplicity of this technology requiring no electricity or communication line has made world wide proliferation of credit cards possible.

Magnetic Strip Cards

The disadvantage of handling paper receipts with the embossed cards is overcome by encoding the card data on a magnetic strip on the back of the card. The magnetic strip is read by pulling it across a read head. Storing capacity of the magnetic strip is 1000 bits which is more than enough to store the embossed data. The main drawback of this technique is that the encoded data on the magnetic strip can easily be altered without leaving any trace.

Smart Cards

Smart cards appear as memory cards, microprocessor cards and hybrid cards.

Memory cards: These cards are prepaid. The value stored electronically in the chip is decreased by the amount of charge each time it is used. Application data is stored in EEPROM, identification data is stored in ROM and the integrated security logic protects stored data against tampering. Applications are telephone cards, public transport, vending machines, cafeterias, car parks, hotels, health insurance and the like. Disadvantage is that cards are not reusable. They are to be discarded when empty. Memory cards are optimized for single application. For this reason they are inflexible but inexpensive.

Microprocessor cards: are smart cards with embedded integrated circuits that can store, transmit and process data. Data transmission can be done via contacts on the card or via electronic fields without contacts. These cards have larger memory capacity, up to 32 KB or more. The processing power of smart cards gives them the versatility needed to make payments, to configure cell phones, TV's and video players and to connect to computers via telephone, satellite or the Internet any time, anywhere in the world.

Using a chip on a card is more often for security reasons: to secure data stored in them and in other computer systems. Security criteria are safety, non-delivery, accuracy, data integrity, confidentiality, impersonation and repudiation. The security of modern cryptographic algorithms can be standardized and published, provided that appropriate systems are used to keep the keys secret. Security is particularly important in smart card systems for two reasons:

- many applications are in finance and payment,
- confidentiality of personal identification and health.

Some major capabilities of smart cards can be listed as:

- Secure access to some web-based information and the ability to download multiple applications on a single card.
- More storage capacity
- Increased security and protection from fraud.
- Higher reliability
- Microchip flexibility that offers a wide range of memory and processing capabilities specific to each card's need.

Interoperability is the key ingredient for the success of smart cards. This means requirement for standardization in hardware and applications. Hardware standards specify physical and communications dimensions of smart cards. International Standards Organization (ISO) 7816 is a global standards for physical characteristics of cards and contacts, transmission protocols, commands for interchange and rules for applications and data elements. ISO 10536 specifies similar standards for contactless cards. There are ISO standards available for message interchange, card accepting devices and security architecture.

Smart cards can be read by conventional card reader or by wireless terminals. Devices similar to floppy disk allow smart cards to be read by PC disk drive. Electronic modules embedded in smart cards have contacts by which messages are exchanged between the card's IC chip and the card reader. Authentication, validation and transaction processing takes place between the card and the card reading terminal and these transactions are transmitted to central computer located at the other end of the smart card infrastructure such as payment servers in banks, traffic control centers or mobile phone centers, credit card companies, transit authorities, governments and other service providers (Fig. 1).

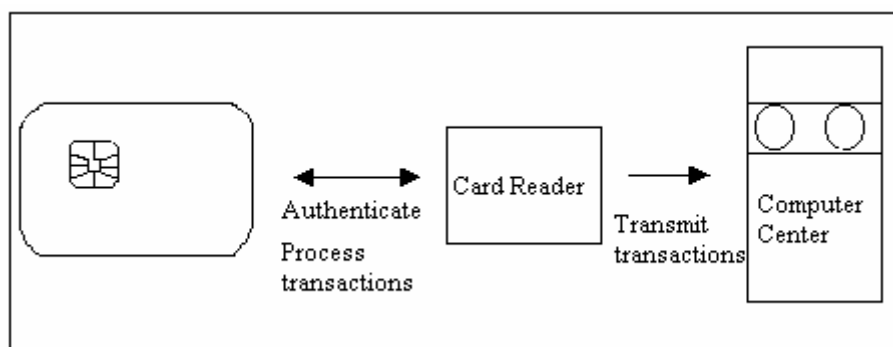


Fig. 1. Smart Card Processing Infrastructure

An interoperable and multi-platform application programming interface (API) is needed for smart cards to carry out diverse functions. Open standards like Java smart card API provides these interfaces.

Hybrid Cards

One card can make use of several different technologies. Lufthansa Air Travel Project uses a multi-application card with a magnetic strip, embossing, a hologram, a memory chip with contacts, and a memory chip without contacts. The card allows the customer to automatically download an airline ticket on the card, access credit, prepay telephone tolls, and automatically stores the frequent flyer number. The contactless chip allows the passenger to board the plane by passing within 10 cm of the card reader. A large number of different applications can be served by this card without compatibility problems with earlier types of cards (Wesley & Wilke, 1997).

3. Applications

Use of smart cards in government, health, transportation and e-purse is given in the following paragraphs:

Government

With decreasing budgets and increasing demands, governments need to improve the administration of services, streamline operations and reduce the costs. They challenge operating with greater efficiency, security and confidentially to conduct, health, finance, transportation, education, concessions/benefits, access control and other functions for an increasingly mobile group of citizens. Smart cards represent a new technology for self service electronic delivery of government services and information with a promise of providing accurate, up-to-date and secure information.

Norway uses smart cards to streamline voting administration and reduce the problems of electoral fraud (http://www.ipc.on.ca/english/pubpres/sum_pap/papers/smcard-e.htm). The state of Ohio is piloting a multiple application smart card that will be used for benefits, vehicle registration, water craft drivers' licenses, game hunting licenses, professional licenses, a senior citizen retail discount program, inquiries for state services information, and federal applications (Zimmerman, et. al, 1997). States of Ohio and Wyoming are testing smart card technologies to deliver government benefit payments (Choi & Whinston, 1998). In some parts of South Africa family benefits are paid in cash by using smart card (Hendry, 1997).

Health

Majority of cards in health sector are insurance cards without any medical application. The dominant motive for using health cards is the control of costs and reducing fraudulent claims. Major requirement in this application is the verification of person claiming medical service is insured and to co-relate claims for payment with both individual patient records and the doctor's accounts. Health care card standards intend to create a common computing framework to identify patients, query their medical, process payments and allow health care management in a distributed environment. Electronic Medical Record Standards are also needed to be developed to facilitate interoperability between health care institutions both within national and international platforms.

The *Versicherungskarte* in Germany is issued to everyone covered by health insurance. The write protected memory of the card can be read in by any authorized health center, but it can only be written to by the insurer. An authentication area identifies the owner insurer of the card.

In France the *Sesame* cards are issued to citizens by the National Health Insurance Scheme to identify the cardholder to the doctor and to provide proof of insurance. The medical reports are held separately and the card is also used to convey prescriptions from the physician to the pharmacist. Every terminal dials over X.25 network to the social security office to record the service performed or prescriptions dispensed. These records are then correlated with the claims of the patient (Hendry, 1997).

Transportation

An efficient public transportation service requires seamless journeys, with passengers traveling on a single ticket across several operators' services. Contactless cards are preferred for public transportation for speed of boarding. The city of Seoul, Korea, is the largest user of contactless cards on buses. In an open system used in Atlanta credit cards are used to pay fares but the card validation is not done real-time (Dinning, 1997).

4. Application in İzmir, Turkey- A Case Study

The İzmir Municipality Transportation System has recently started using the smart card in its buses and the underground system (<http://www.kentkar.com.tr>). As in a typical transport system, the following components are found in this application:

1. The Smart Card
2. The Card Charging Points
3. The Validator
4. Auxiliary Computer Systems
5. The Municipality Main Computer System
6. The Bank

This is an application of a typical electronic purse. The following are done in sequence :

1. The card charger master first pays the bank and charges his/her master card with the required amount.
2. He/She then transfers this credit to the local charging machine. This can also be done online via the communication lines as shown in Fig.2
3. When a passenger loads his/her card from the charging device a small fraction of this amount is transferred to the passenger's card.
4. The passenger gets on the bus, performs a transaction with the validator on the bus during which the fare is decreased from the card and the information about transaction is stored in the memory of the validator
5. At the end of the day, all the memory packs of the validators in the buses in use that day are taken to the auxiliary computer systems of the municipality to be read to these computers. These computers have on-line connections to the main computer of the municipality and transfer the bus information to the main computer at the end of each day.
6. The main computer stores this information in its database. It also has an on-line connection to the main computer of the bank. So, by the use of appropriate software, the account of the municipality is credited with the respective amount of passenger transactions

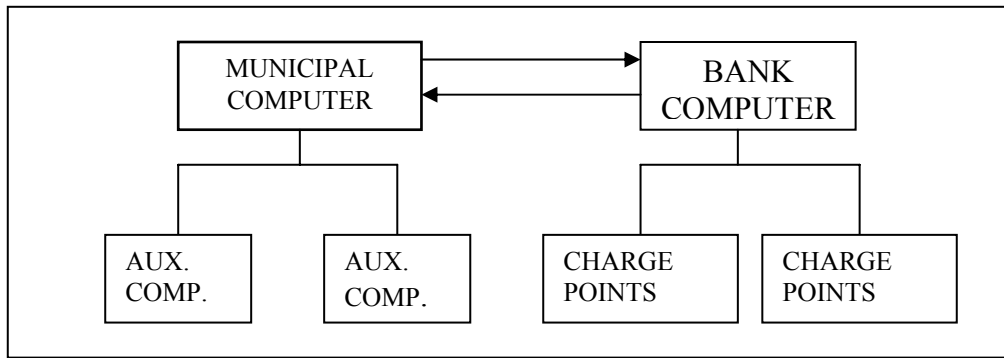


Fig. 2. Operation of the İzmir Municipality Transportation Card

The operation of this system is depicted in Fig.2. The İzmir Municipality has about 1500 buses which carry about 1.5 million passengers daily. The size of this system is considered large when compared to world standards. Before the use of the smart card, frauds such as false ticket or other were unavoidable in a system of this size. The smart card application has prevented these almost completely due to the nature of the operation and also the highly secure low-level protocols adopted by the card and the validator during the transaction. It also has prevented blocking of passengers during getting on the bus, therefore provided faster operation. The integration of the card to the recently installed underground system of İzmir has been accomplished. There were and still are maintenance problems naturally such as training of the drivers, technical staff etc. Transfer ticket passenger problem remains to be solved efficiently. The experience gained from this application is that the smart card has provided ease of use, secure, reliable and easy to follow and stored transactions. The statistics of the transport system are now in a very suitable format for analysis and take necessary actions to enhance the service.

5. Proposal for Additional Functionality on Citizenship Identity Card

MERNIS project (<http://www.nvi.gov.tr/mernis/main.htm>) aims at giving each Turkish citizen a unique identity number to enable access to central data bases for population, tax, health and military service through the same number. Work is under way to design efficient, convenient and secure identity card. In this section a proposal is presented to integrate driving license card on the identity card together with some e-purse applications.

Contactless microprocessor cards are preferred because they are easier to use, less subject to wearing out and enable faster boarding in fare payment. The memory layout of the card is as shown in the figure. Card issuer's code is stored in ROM by the issuer of the card. Application programs and their related data can only be written by the official owners of the application under security controls.

This information being available on the card makes off-line processing possible which means faster service. Depending on the nature of the application, central databases may be updated either simultaneously or in batch mode at predetermined time intervals. Personal information can be read by any authority requiring the information. Identification between

the card and the cardholder can be done by a photograph on the card or biometric measures.

Driving License Application. Traffic police should have a laptop with card reader attached. After authentication in both directions police can access to driving license, violations or to the health file on the card. The violations file consists of violation records for which the driver is punished according to the number of times it is done like speed violation and having alcohol in blood while driving. If the card holder is stopped because of such a violation, violation file is accessed, new violation is recorded on the card and in a file in the laptop and the person is ticketed or punished accordingly. This record is printed on paper and the record of the person is updated at the central police station computer in batch form once or twice a day. If the police is suspicious of the person, additional information like crime records can be accessed on line through ID number of the person. Access rights of the police is shown in the chart.

Health file consists of records related to emergency health information like blood type, allergies, and chronicle diseases like diabetes, epilepsy and other diseases that require special treatment. In case of an accident health information is needed for emergency treatments. This file can also be accessed at the hospitals .

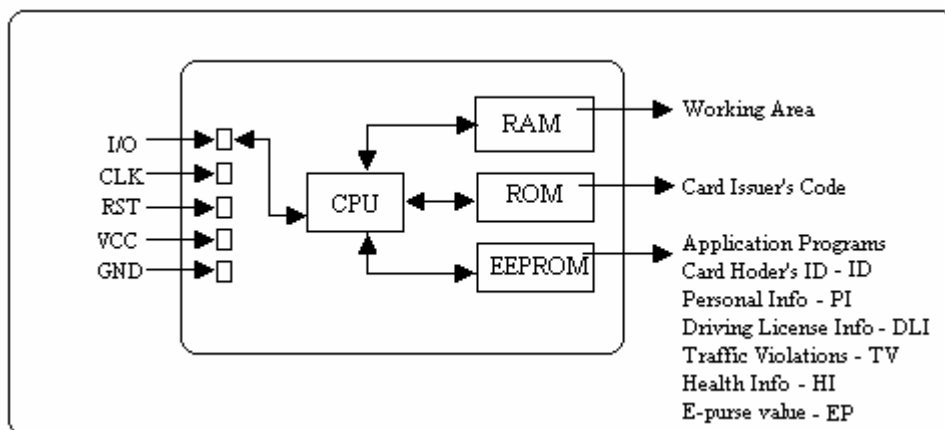


Fig. 3. Memory Layout of the Multifunctional Smart Card

E-Purse Application is restricted to fare payments at busses, train, fairies, payments for parking lots and toll collection at highways as a start. Cards can be loaded by ATM's. Table below shows tasks performed on the card, on the terminal and on the computer center side for this application.

Card	Terminal	Computer center
Authenticate the terminal	Authenticate the card	
Send ID, CIC, purse value	If purse value is sufficient <ul style="list-style-type: none"> • Decrease it by the amount • Write to a file ID,CIC, amount, date, time • Send the value to the card • Display the value • Open the barrier otherwise reject	
Update the purse value	Read and display.. open the gate?	
	Send the transactions to the related card issuer in regular time intervals.	Update the retailers accounts

Table 1. Tasks Performed by the Smart Card, the Terminal and the Computer

Access control of the records in memory is summarized in Table 2.

	CIC	ID	PI	DLI	TV	HI	EP
Card Issuer	r, w	r	r	-	-		r, w
Authorized pop. office	-	r, w	r, w	-	-		-
Health centers	r	r	r	-	-	r, w	-
Driving License Office	-	r	r	r, w	r, w	r	-
Traffic Police	-	r	r	r	r, w	r	-
Pay stations	r	r	-	-	-	-	r

Table 2. Access control of the Records in the Memory

Applications can be updated and new ones can be downloaded on the card after it is issued. All writing processes should be carried out on-line to a trusted system. To authenticate the application issuer offline, the card must carry the public key of a certification authority. The terminal should also be authenticated.

6. Conclusion

Using a single card for every kind of process nationally and internationally is the promise of the future. European Union countries are on their way for developing standards for financial transactions and medical care that will be valid in all union countries.

Decisions for adapting smart card technology by governments and private sectors are based on the security, convenience, economic benefits and customization of the smart cards.

A survey of smart card applications, and a detailed structure of a case in İzmir, Turkey where the smart card is used in the transportation system is presented in this paper. We

have also proposed a combination of restricted citizenship identity card and e-purse application that can be implemented.

As people get used to using smart cards and the applications settle and work smoothly more applications can be downloaded as need arises.

References

- Allen, C.A., Kutler, J. “*Overview of Smart Cards ant the Industry*” in Smart Cards: Seizing Strategic Business Opportunities, Allen, C. and Barr, W.J. (ed.) chapter 1, McGraw Hill, 1997
- Rankl, W., Effing, W. “Smart Card Handbook”, Wiley, 2000.
- Wesley, R., Wilke, C. “*Travel and Entertainment*”in Smart Cards: Seizing Strategic Business Opportunities, Allen, C. and Barr, W.J. (ed.) chapter 12. McGraw Hill, 1997
- Zimmerman, J.R., Moore, J., Tarbox, J. D. “*Smart Cards in Government*”, in Smart Cards: Seizing Strategic Business Opportunities, ed. Allen, C. and Barr, W.J. chapter 10. McGraw Hill, 1997
- Choi, Y.S., Whinston, A.B. “Smart Cards: Enabling Smart Commerce in the Digital Age”, May 1998. <http://cism.bus.utexas.edu/works/articles/smartcardswp.html>
- Hendry, M. Smart Card Security and Applications, Artech House, Inc., 1997.
- Dinning, M. Transportation, in Smart Cards: Seizing Strategic Business Opportunities, ed. Allen, C. and Barr, W.J. chapter 11. McGraw Hill, 1997