A Programming Algorithm for Smart Multi-Application Card

Kamel H. Rahouma. Mostafa M. Rahouma and Khalid S. Salih
Electrical Engineering Department, Faculty of Engineering
Minia University, Minia, Egypt.
kamel_rahouma@yahoo.com

Abstract

In this paper, we present the concept of smart multi-application card (SMC). This type of cards can be used for different purposes. Here, we use the card for four different applications and purposes including the storing of medical insurance information, traffic and police services information. The card is also used as a personal identification card. We presented the ideas of the different applications together in one smart card. Thus, a person doesn't need to carry many cards in his wallet but rather a single card for different purposes.

The card is actually a hardware circuitry which is programmed for the intended applications. The hardware is distributed by the company "CardLogix" with a programing tool called "M.O.S.T.Toolz". The programming process aims to divide the card memory into a number of areas that match the number of required applications. These areas are used to store the information of the card holder belonging to the different applications. The information of these areas is linked to a database we designed to store the actual records of the card holder.

Owing to scarcity of SMC technology and resources in Egypt, it is important to facilitate importation process of these tools and to start this technology with the four fields mentioned earlier; personal identification, medical insurance, police and traffic systems that potentially can be expanded to many other fields in the nearby future. Application of our proposed system has the potentials to do and to leverage digital transformation of the country in most of the government sectors and their practices.

Keywords: *Smart Multi-Application Card, Smart Card Hardware, Smart Card Programming, Advantages of Smart Cards*

1. Introduction

As modern society has rapidly become information-based and credit-based after industrialization, the use of credit cards has increased to be as prevalent as cash with consequent increase in the number of credit cards carried by a regular person. Thus each person uses at least two or three cards, and in some cases, ten or more cards are held and used. Examples of service cards are identity card, traffic card and health insurance card, .etc.

Accordingly, a large number of credit cards are being issued and many are unnecessary and/or discarded, thereby generating unnecessary issuing costs and social costs. This causes consumers to avoid use of these cards due to inconvenient and complex card management. This may cause generation of unnecessary marketing costs to businesses.

On the counter side, the average number of cards that are actually used per consumer is only 1.4 despite the increased number of issued cards [1]. As a result, most credit cards issued to each consumer become dormant, check cards, cash cards, and prepaid cards or marketing

cards such as services cards and astronomical costs are being wasted on dormant or discarded cards.

Smart Multi-Applications Cards (SMC) are constructed to solve one or more of the above problems. Using a smart multi-application card, that includes many applications, makes it easy to be carried by the user and to dispense the rest of smart cards. We can use it in voting to eliminate the problem of traditional voting in elections. Additionally, health insurance and police services could be applied to SMC. All these are done in one multi-applications card as in

This paper includes six sections. Section (1) is an introduction and section (2) is a literature review. Section (3) illustrates the methodology of the paper and section (4) explains the results and discusses and compares them with the prior cards. Section (5) gives some conclusions and a list of the used references is given at the end of the paper.

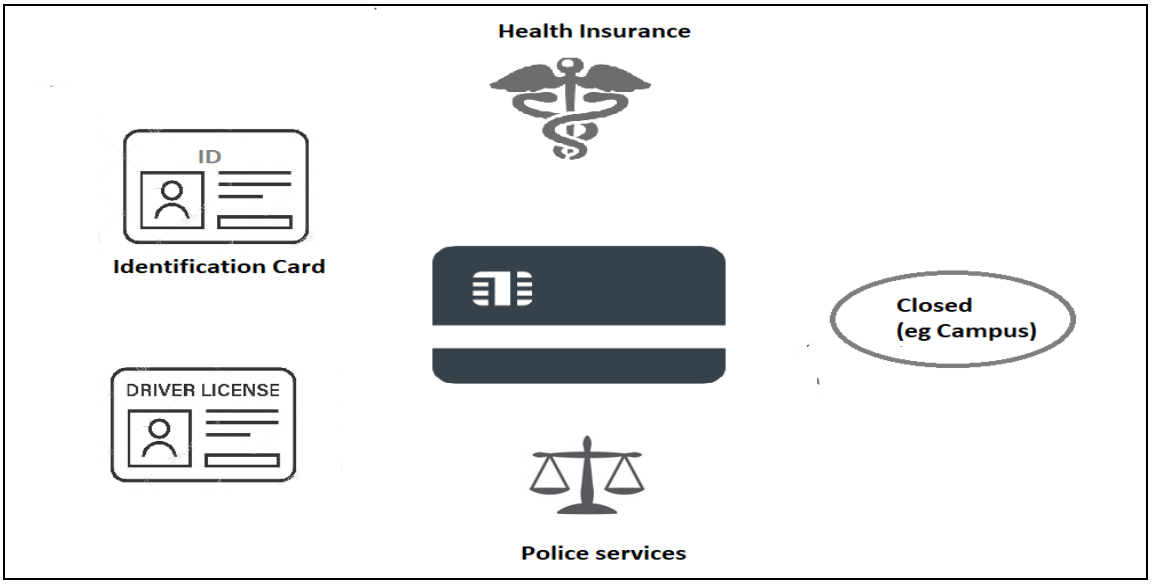

Figure (1): Smart card file structure for the included study fields of medical insurance, police services and traffic services in addition to personal identification card. Furthermore, there is a closed file structure that could be boosted later with any needed additional field

2. A literature review

Looking at the historical background of SMC system use, we found that it was introduced 1st by a Japanese company in 1998. There is no doubt that the Japanese industrial and technical revolutions put that country in the frontline of almost every electronic development [2,3]. Almost two years later, Marlowe; an American engineer introduced a similar SMC to the Japanese one and applied it to the Nova Southeastern University system [4]. In 2004, Ornar and Diuhari worked on implementing the smart multi-application card in the service of education environment to facilitate the provided services [5]. In 2007, At Multimedia University in Malaysia, Abid et al, implemented the smart multi-application card as Health Card, Electronic Purse and Access Control card that was presented with the Java Card Runtime Environment (JCRE). [6]. In a study done by S. Farag at University of Anbar in Iraq in 2008, he built a number of different secure applets for smart card where each applet was designed for a specific task. Three packages were designed; the first package is the “Secure Wallet” which represented

the electronic money storage card for financial services such as banks. The second package is "Card Connection". This package was designed to be used in prepaid communication applications such as telephone, internet, etc. The third package was "Health Care", which represented the medical file for the card carrier. It was used in hospital, clinic and medical establishments [7].

Instead of carrying several cards, one can carry only one card that simultaneously contain an ID, a credit card, a stored-value cash card, and a repository of personal information such as telephone numbers or medical history. Currently smart card implementations can be seen around the world but they are not unified i.e. each developer uses different programming standards and data structures, therefore a variety of smart cards exist in our society today. An example can be seen in Singapore where they have variety of smart card for the same purpose i.e. storing monetary value. One called E2 Link which is used for their public transport system and is also usable in some food courts while the other cash cards are used for their toll system, parking and supermarkets. This is a problem that exists today and one that needs to be noted or fixed. Bodake et al. created a multipurpose card system in which they used a single card that can handle number of technologies. In this paper, we are providing the concept of bringing different applications together in one smart card. Thus, the person doesn't need to carry different cards for different purposes. Instead, s/he can carry one card and use the same card for different purposes. In this paper, we are introducing a smart card, which will work for different purposes like voting, attendance and transportation (ticketing). It will also work as a personal ID [8].

To authorize user or device using the smart card securely, the smart card is configured upon initialization or a request for authentication, and a special key as the personal identification number (PIN) or password should be entered by the user and is encrypted before transmission to the smart card via a smart card reader. The smart card then decrypts the PIN or password to authorize the user. Preferably, the smart card is configured to provide a public key to the user input device, which then encrypts a concatenation or other combination of the user-input PIN or password before transmission to the smart card. The smart card reader thus never receives a copy of the PIN or password, allowing the smart card to be used with untrusted smart card readers [9].

With the fast development of campus informationization, the complexity of consumption types and identification of college teachers and students also increases, which raises more stringent requirements to college management. Weichun illustrates the overall planning of campus smart card system, discussing the construction target and technical requirements of campus card system, designing the general framework and putting forward the design plan of the construction of campus smart card system [10].

Smart cards are used in information technologies as portable integrated devices with data storage and data processing capabilities. As in other fields, smart card used in health systems became popular due to their increased capacity and performance. Their efficient use with easy and fast data access facilities leads to wide implementation particularly in security systems [11].

Kardas and Tunali introduced a smart card based healthcare information system. The system uses smart card for personal identification and transfer of health data and provides data communication via a distributed protocol which is particularly developed for this study. Two smart card software modules are implemented that run on patient and healthcare professional smart cards respectively. In addition to personal information, general health information about

the patient is also loaded to patient smart card. Health care providers use their own smart cards to be authenticated on the system and to access data on patient cards. Stored encryption keys and digital signature keys on smart cards of the system are used for secure and authenticated data communication between clients and database servers over distributed object protocol. System is developed on Java platform by using object oriented architecture and design patterns [11].

Koul and Pathak reported implementation and simulation of a smart card reader design on Xilinx Spartan-3E FPGAboard. This smart card reader design is in compliance with ISO/IEC 7816-3 standard. The code is described in Verilog at RTL level. A smart card reader hardware was used for verification purpose. The Smart Card reader design worked in synchronization with the hardware [12].

Different SMC security systems exist. In our card, card holder verification (CHVs) Password Files can store a password or PIN. They are used to control access to EFs and Purse Files. CHVs typically contain a password or PIN known only by the user or the system that interacts with the card.

Automated Teller Machine (ATM) has been incorporated in our way of life and is is still being adopted globally by banks. However, password (PIN; Personal Identification Number) which is the main authentication for ATM transactions represents the weakest link in the computer security chain [14]. Adebayo et al. designed and simulated an enhanced e-banking system where customer can access multiple accounts over different banking institutions with a single ATM card and fingerprint authentication. A match-on-card technique was employed that relies on a one-to-one matching, where the data from the ATM fingerprint sensor is compared only to the one template stored on the user's ATM card. Results showed that of the 150 attempts made on the simulated ATM machine over a period of ten days, 108 correct accepts (CA) by genuine users and zero (0) false accept (FA) were recorded. The classifier accuracy from the confusion matrix is 0.90667, which is approximately 91% and user authentication time was low as 0.92 seconds. The match-on-card approach employed for user authentication will resolve the privacy concern of users. The system offers a convenient approach to the users as they have access to multiple accounts with a single ATM card, It is secured and will further help to eliminate ATM theft. Future research will help to dwarf ATM-card authorization by introducing palm and finger vein authentication in financial transactions [14].

Smart card is one of the greatest achievements in the world of information technology. Smart cards have many applications such as health, ID verification and access control, electronic purse card, banking card, payphone card, passport card and license card. Since, there are many kinds of smart cards, it is difficult to carry and protect them. Losing one card means losing a lot of important information. As everyone knows, carrying and protecting one smart card is easier and more comfortable than carrying two or more smart cards. Multipurpose smart card is a smart card with many different applications in one smart card [15]. Multipurpose smart card would be giving all services and making data processing and data transfer more efficient and secure. Nusrath chose three most important cards such as health card, and passport cards to be combined in one smart card and find an encryption method to make it secure enough. Also, it should be efficient in transferring information. The advanced encryption standard algorithm should be effective encryption system for these three applications in a multipurpose smart card [15].

3. The Methodology

In the present work we have used the CARD C7 (M.O.S.T. Card®) distributed by CardLogix [16]. We discuss here the hardware of this card. We designed the software programming of the card using the "MOSTToolz" tool in addition to an interface. These processes are explained in the following subsections.

3.1. Hardware Interfaces

The Reader requires a physical connection to the cards. This is made by inserting the card into the reader. This is the most common reader type for applications as ID and Stored Value. The card-reader communication is often ISO 7816 T=0 only. Communication between card and reader has the advantage of direct coupling to the reader and it is considered more secure. The other advantage is to increase the card speed in getting the data [17].

A contact reader is primarily defined by the method of its interface to a personal computer (PC) through the method of Universal Serial Bus (USB) ports. All cards and readers that follow ISO 7816-3 standards have a standardized set of commands that enable communication for central processing unit (CPU) cards. These commands, called APDUs (Application Protocol Data Units) at a very low level, or they can be scripted into application program interfaces (APIs) which enable the user to send commands from an application to a reader. These layers of software can enable effective application communication with smart cards and readers from more than one manufacturer. For ISO7816 processor cards, the personal computer/smart card (PC/SC Workgroup) interface is often employed, but it has limitations. This is especially important if you have both memory and microprocessor cards that are used in the same system [18].

3.2. The card general workflow algorithm

1) Open SMC program
2) Connect card reader and select “card reader” from SMC program
3) Insert SMC inside the card reader
4) Read the needed details according to the using institute/facility that appears on the interface e.g. reading medical insurance details upon visiting the hospital/doctor’s clinic and displays the data on the computer screen
5) Take the SMC out of the SMC reader
6) Personal details will disappear from the screen and the program will spontaneously wait for repeating the same steps with another card as in Figure (2).

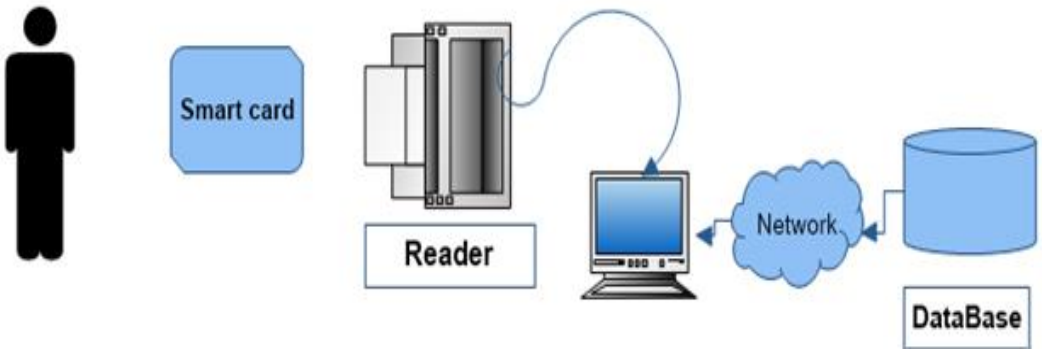

Figure (2): Block diagram of the work flow of the smart multi-card application system

3.3. Card Programming

The "M.O.S.T.Toolz" tool is used to program the card. [16] The different processes are explained in the following subsections. Through this tool, the card is divided into files, each of which has its own address. Then, an interface is designed with the program to deal with the multi-application card in the "C #" programming language. So, the interface contains the choice of the card reader device, which reads the contents of the card according to each section of the card. For example, the medical section consists of files with a large area, so we use a database connected to the program and it is stored on a server as shown in

The SMC has a master file (MF) named "3F00". Programmer can divide MF memory to a number of detected files (DF) in order to put different applications on DF. Subsequently, each piece of information e.g. name, date of birth (DoB), etc. is put in element file (EF). Also, the MF"3F00" includes identification information e.g. identification number, name, DoB and photo as in

Card programming is done through a software tool produced by the company that produces the card. The tool name is MOSTToolz [14], which is specialized for the card programming. We will divide the card electrically erasable programmable read-only memory (EEPROM) into several sections such that each section contains a specific application. Each section has a title in the memory. The memory used to save applications includes files with different functions and names; MF, DF and EF as explained before. In our proposal, the memory is divided into 4 sections in addition to some empty space for any future applications as being shown in

Figure (3). The algorithm of programming the card has the following steps:

1) Create a file on the MF (3F40, 3F41, 3F42 and 3F43) that has the following EF files in table (1), where these data have no DF and they are created Create a EF under a path MF directly to share it.

Table (1): The used element files in the main file of the card

No.	EF files	Abbrev	Length (Bytes)
1	Citizen's name	CN	100
2	Citizen's national ID number	NID	75
3	Age & Birthday	ABD	40
4	Sex (Male/Female)	SEX	20

2) Create a DF file on the MF at the memory address (3000) named ID for information about the person's address and work. This DF has two element files shown in table (2)

Table (2): The used element files for the citizen's identification (ID) information

No.	EF files	Abbrev	Length (Bytes)
1	Citizen's address	ADD	100
2	Citizen's work	CW	100

3) Create a DF file on the MF at the memory address (3100) named MEDI "Medical Insurance" for information about the person's driving license and medical insurance information. This

DE file has EF files shown in table (3). This section is linked to the database to view more data because there is limited memory.

4) Create a DF file on the MF at the memory address (3200) named PS "Police services" for the person's police information. This DE file has EF files as shown in table (4). This section is linked to the database to display more data upon needed because there is limited memory in SMC.

Table (3): The used element files for the citizen's medical insurance (MEDI) information

No.	EF files	Abbrev	Length (Bytes)
1	Medical Insurance	MEDI	8
2	Insurance Number	INO	100
3	Blood Type	BT	20
4	Previous & Current Diseases	HD	1000
5	Previous Operations	PO	2000
6	Previous and Current Medicines	PCM	1000
7	Advance Hospitalization	AH	1000

Table (4): The used element files for the citizen's police service (PS) information

No.	EF files	Abbrev.	Length (Bytes)
1	Previous felony	PF	100
2	Prior arrest	PA	100
3	Total prison period	TPP	100

5) Create a DF file on the MF at the memory address (3300) named TS "Traffic services" for the person's traffic information. This DE file has the EF files shown in table (5). This section is linked to the database to view more data because there is limited memory.

Table (5): The used element files for the citizen's traffic service (TS) information

No.	EF files	Abbrev.	Length (Bytes)
1	Driving license	DL	8
2	License ID	LID	100
3	Start date	SD	20
4	End date	ED	20
5	Previous traffic violations	PTV	1000
6	Red light violations	RLV	100

The previous tables are gathered in table (6) and Figure (3) shows the file structure of the card and the memory places of these files.

3.4. Database Design

Regarding the database, we have created database shown in figure 4F in order to accommodate a big variety of information related to the facilities/institutions in which the card will be used. ID number was the primary key that links the card sections and the main external database and we have four tables; 1- personal identification table, 2- police services table, 3- traffic and traffic license table, and 4- medical insurance table as shown in Figure (4).

3.5. User Interface

As for the user's interface, we have worked with the C# language to establish an interface to connect card reader to our computer. Furthermore, this interface allows us to read the card

data according to the facility which is the identity, medical insurance, traffic services or police services. We have relied on dealing with the card through "Winplex API" [16].

As smart cards are becoming more common, they are being used in more and more applications. Unfortunately, the task of actually building a Windows application that uses a smart card can be quite daunting. If a programmer chooses to work with the base level Microsoft smart card components, they will requires the programmer to have a great deal of knowledge of the Microsoft application program interfaces (APIs), limit the types of cards the programmer can choose to use, and add unnecessary complexity for the programmer. CardLogix has developed the Winplex API as an alternative to the Microsoft approach for developing smart card applications under Windows [16].

Table (6): Summarizing the file structure of the card. These files are linked to the database

	First level files					Second level files			
	File Type	Memory Address	Abbrev.	Usage	Length	File Type	Abbrev.	Usage	Length
Mail file (MF)	EF1	3F40	CN	Citizen's name	100				
	EF2	3F41	NID	Citizen's national ID number	75				
	EF3	3F42	ABD	Age & Birthday	40				
	EF4	3F43	SEX	Sex (Male/Female)	20				
	DF1	3000	ID	Identification information		EF1	ADD	Citizen's address	100
						EF2	CW	Citizen's work	100
	DF2	3100	MEDI	Medical insurance		EF1	MEDI	Medical Insurance	8
						EF2	INO	Insurance Number	100
						EF3	BT	Blood Type	20
						EF4	HD	Previous & Current Diseases	1000
						EF5	PO	Previous Operations	2000
						EF6	PCM	Previous & Current Medicines	1000
						EF7	AH	Advance Hospitalization	1000
	DF3	3200	PS	Police services		EF1	PF	Previous felony	100
						EF2	PA	Prior arrest	100
						EF3	TPP	Total prison period	100
	DF4	3300	TS	Traffic services		EF1	DL	Driving license	8
						EF2	LID	License ID	100
						EF3	SD	Start date	20
						EF4	ED	End date	20
						EF5	PTV	Previous traffic violations	1000
						EF6	RLV	Red light violations	100

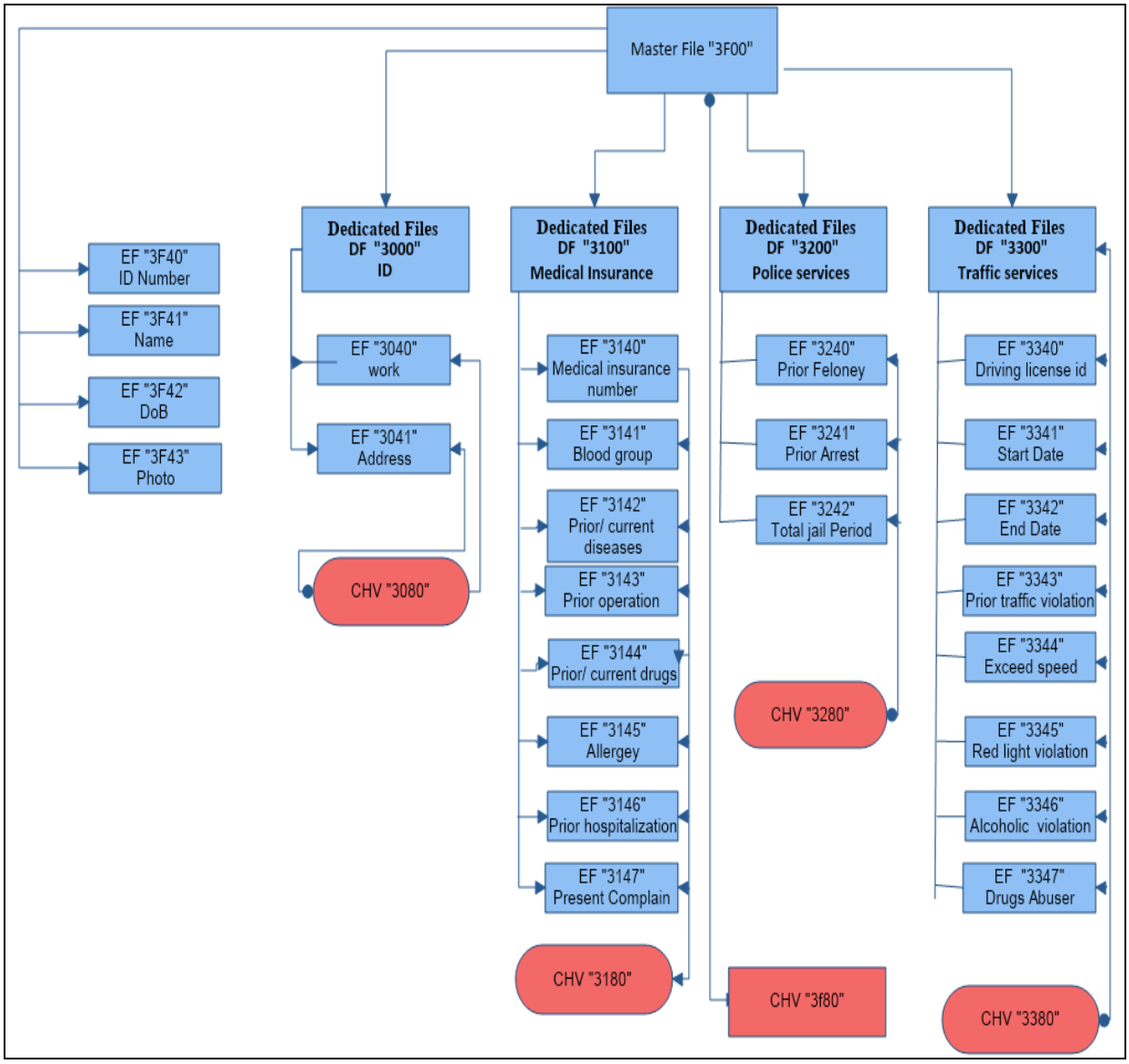

Figure (3): Detailed card master file (MF) structure for the included study fields of Medical insurance, police services and traffic services (DF: detected file. EF: element file, Number between quotation marks reflects the address in the memory (EEPROM))

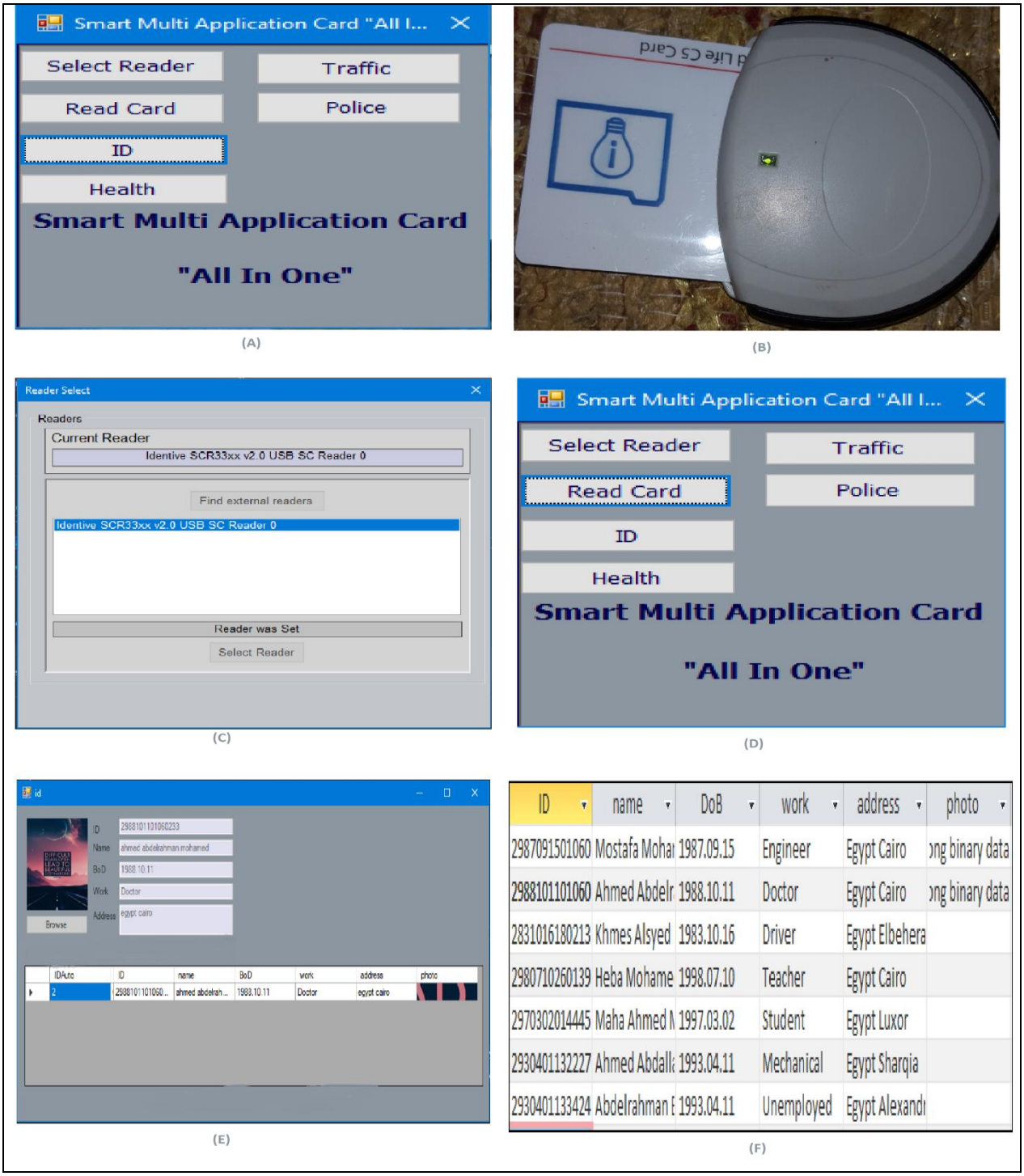

Figure (4): Illustration of the programing/working flow of our smart multi-card application system (A. The program interface for the identity section, B. Smart card insertion into the card reader and illumination of the LED upon pressing "Read Card" button, C. Program interface for identifying the smart card reader via the USB port, D. Read card information interface, E. ID Application interface, F. Sample fictitious database based on the proposed questions and needed data obtained from relevant officials in the investigated field)

4. Results and Discussion

A stepwise approach to our proposed system is shown in Figure (4A - 4E). We put a sample fictitious database based on the proposed questions and needed data obtained from relevant officials in the three investigated fields; medical insurance, police and traffic systems. A screenshot of the dataset is shown in Figure (4E). It is to be noted that the primary key used to link all the investigated fields is "card identification number".

The card has many advantages which mainly aim to monitor the citizens' activities. For example, the medical records of the card holder can help so much in saving his life when he faces any accident or health complications. Also, the police systems can easily reach people required for the justice. Traffic systems can also follow up the records of the card holder for licensing. These capabilities make it easy to obtain statistics which help the stakeholders to develop and improve the public services.

Up to our knowledge, the smart multi-card technology is almost never used in Egypt. Thus it is important to start this technology with the four fields mentioned earlier which are the personal identification, medical insurance, police and traffic systems. We herein are setting a system in some fields that potentially can be expanded to many other fields.The SMC hardware is not available in the Egyptian markets and should be imported. Proper thinking about the "importing obstacles" should be done before wide scale application of SMC system.

Compared with prior SMCs, our current card has larger CPU (16-bit 3.57 MHz) making it faster, higher RAM (2048 bytes), higher ROM (1024 Kbytes) and higher EEPROM (144 Kbytes). Furthermore, our card uses MULTOS operating system and PC/SC SCard software and has four applications and four institutions per card. Table 7 and Table 8 show comparisons between four cards and our card from the points of CPU, RAM, ROM, EEPROM, operating system, openness, separate seed, and number of applications.

Table (7): A comparison of hardware of prior smart multi-applications cards with our card

	CPU (Bits, MHz)	**RAM Byte**	**ROM KB**	**EEPROM KB**	**Operating System**	**Software**	**No. of Applications**
Japan (Agarwal)	**(8, 5)**	**256**	**64**	**4**	Java Card	OpenCard	2 & 1 (Bank)
USA (Marlowe, 2000)	**(8, 2)**	**512**	**256**	**16**	Java Card	Global Platform	7 & 1 (High Education (University))
Malaysia (Abid, 2007)	**(8, 2.57)**	**1024**	**512**	**82**	Java Card	Java Card	3&3 (Access Control, E-Purse, Health)
Iraq (Sofyan Faraj, 2008)	**(16, 2)**	**1024**	**256**	**68**	Java Card	PC/SC SCard Software	3 & 3 (E-Wallet, Card Connection*, Health)
Current Project	**(16, 3.75)**	**2048**	**1024**	**144**	**MULTOS**	PC/SC SCard Software	4 & 4 (ID, Police, Traffic and Medical insurance)

* "Designed to be used in prepaid communication applications such as telephone, Interne"

The symbols in table (7) are defined as follows: CPU: Central Processing Unit, RAM: Random Access Memory, ROM: Read-Only Memory, EEPROM: Electrically Erasable

Programmable Read-Only Memory. Notice that applications on all cards are separated from each other, but the programmer allows the card to share some parameters of the other applications

It is clear from table (7) that the new card has more hardware features that make it possible to program more applications on the card. Also, The new card has more software features such as multi-operating systems that allow more applications with different frames.

5. Conclusions

In this work, we introduced the concept of the smart multi-application card, which can be used to work in different purposes as medical insurance, traffic and police services. The card can also work as a personal ID. We presented the idea of different applications together in one smart card. Thus, a person doesn't need to carry many cards in his wallet but rather a single card for different purposes.

The card is programmed by dividing its memory into a number of areas that match the number of applications it will work in. A special programming tool is delivered with the card by its inventor. We programmed the card and linked the different memory files to a database we designed also to have the card holder's records.

The card increases the capabilities of monitoring the citizens' activities. For example, when the government has data on the state of health of all citizens, it will be easier for them to study diseases in a specific place for a certain age, so that it is easy for them to obtain statistics by the specialists and put the proper future health plans by policy makers and stakeholders. Also, in the police systems, it is easier for the police officer to verify the person who is required by justice, and thus, it will help in achieving the goal of saving time and efforts in addition to get data about criminal distribution in different cities of the country and criteria of criminal citizens as age, gender. Application of our proposed system has the potentials to do and to leverage digital transformation of the country in most of the government sectors and their practices

References

[1]. Bae JH, Bae JH, inventors; BRILLIANTTS Co Ltd, assignee. Smart multi-card. United States patent US 10,032,101. 2018 Jul 24.

[2]. Smart Commerce Japan (1998). What is SCJ? https://www.icr.co.jp/newsletter/topics/1998/t98J007.html Last modified December, 1998. Accessed April 1,2020.

[3]. Agarwal T, Security System with the Smart Card Authentication; Accessed 3/15/2020; URL: www.efxkits.co.uk/smart-card-authentication-security-system/

[4]. Marlowe J. M., Smart Card Systems: Development of a Paradigm for a University-Wide Smart Card Student Identification System, 2000

[5]. Ornar and Djuhari (2004): "Multi-purpose student card system using smart card technology", IEEE Xplore, a Conference Paper · January 2004

[6]. A. Abid ,OBJECT SHARING IN MULTI-FUNCTION JAVA SMART CARD Multimedia University, Cyberjaya, 2007.

[7]. Sufyan T. Faraj, Investigation Of Java Smart Card Technology For Multi-Task Applications, University of Anbar, Iraq, 2008

[8]. Aditya Bodake; Viraj Baviskar; Ashwini Bodake; Shital Bhoite and N. J. Kulkarni (2012): "Multipurpose Smartcard System", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 9, November 2012, pp. 175-178.

[9]. Brown MK, Adams NP, Little HA, inventors; BlackBerry Ltd, assignee. System and method for encrypted smart card PIN entry. United States patent US 7,735,132. 2010 Jun 8.

[10]. Weichun Lv (2013): "Design of Campus Smart Card System"; Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation (ISCCCA-13), Published by Atlantis Press, Paris, France., PP. 483-486.

[11]. Kardas G. and E. T. Tunali (2006): "Design and implementation of a smart card based healthcare information system"; Computer Methods and Programs in Biomedicine · February 2006

[12]. Koul Y. and A. Pathak (2016): "Design and FPGA-based implementation of Smartcard Reader", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 5, Issue 2, February 2016, pp. 586-590.

[13]. M.O.S.T Toolz Microprocessor Card Development Kit User Guide www.cardlogix.com Mike Hendry Multi-application Smart Cards Technology and Applications ,2008

[14]. Adebayo A.-A., Omidiora, E.O.; Olabiyisi, S.O. and Ojo J. A. (2012): "Enhanced E-banking System with Match-on-Card Fingerprint Authentication and Multi-account ATM Card"; The Journal of Computer Science and its Applications, Vol. 19(2); Dec. 2012, pp. 14-22.

[15]. Nusrath A (2015): "Multipurpose Smart Card using Advanced Encryption Standard Algorithm", International Journal of Emerging Technologies in -Computational and Applied Sciences (IJETCAS), pp. 115-118.

[16]. www.smartcardbasics.com · www.cardlogix.com

[17]. Qabs UM, Al-Naima FM. Design and implementation of a smart card simulator. In2008 International Conference on Computer and Communication Engineering 2008 May 13 (pp. 217-220). IEEE.

[18]. Katashita T, Hori Y, Sakane H, Satoh A. Side-channel attack standard evaluation board SASEBO-W for smartcard testing. Power. 2012;3(2012):400.