Smart Card Technology used in Secured Personal Identification Systems

VALENTIN SGÂRCIU, MĂDĂLIN ŞTEFAN VLAD
Faculty of Automatic Control and Computers,
"Politehnica" University of Bucharest,
313, Spaiul Independentei, Sector 6, Bucharest,
ROMANIA

Abstract: The paper presents an application developed for Java Card smart cards, with multiapplication support. Although the multiapplication support was not exemplified, the use of smart card for personal identification has some advantages, the most important beeing its security. In this paper are shown the structure of the application, various security systems, which ensure the access to a objective to only the designated people, who have rights to enter in the certain objective.

Keywords: Smart Card, Automatic Personal Identification, Data transmission, Database Conectivity, Integrated System

1. Introduction

The smart card, an intelligent token, is a credit card sized plastic card embedded with an integrated circuit chip. It provides not only memory capacity, but computational capability as well. The self-containment of smart card makes it resistant to attack, as it does not need to depend upon potentially vulnerable external resources. Because of this characteristic, smart cards are often used in different applications that require strong security protection and authentication.

For examples, smart card can act as an identification card that is used to prove the identity of the cardholder. It also can be a medical card that stores the medical history of a person. Furthermore, the smart card can be used as a credit/debit bankcard that allows off-line transactions. All of these applications require sensitive data to be stored in the card, such as biometrics information of the card owner, personal medical history, and cryptographic keys for authentication, etc.

In the near future, the traditional magnetic strip card will be replaced and integrated together into a single card by using the multi-application smart card, which is known as an electronic purse or wallet in the smart card industry. The smart card is becoming more and more significant and will play an important role in our daily life. It will be used to carry a lot of sensitive and critical data about the consumers ever more than before when compared with the magnetic strip card. Therefore, there are many arguments and issues about whether or not the smart card is secure and safe enough to store that information. This has always been a source of controversy.

Besides the capacity, the microchip on the smart card allows the implementation of cryptographic and authentication algorithms, so that information stored on it can be secured and protected. Therefore off-line transactions are possible while the magnetic stripe card requires on-line database verification. As a result, many companies are going to develop or enhance their services by using the smart card as it provides more storage space and offers more security and confidentiality when compared with the traditional magnetic stripe card.

An important issue in the smart card industry is the capability of the smart card, which makes the integration of multiple applications into a single smart card feasible. In the concerns of access control, this paper discusses different infrastructure of multiple application smart card, and tries to develop both procedural and technical mechanisms to implement such a system in the terms of data ownership and management, data directory configuration and partitioning, security and data sharing, and system application expansion, etc.

2. Card Structure and Functions

Foward, we will refer to contactless smartcards which are the most interesting as model and the safest from the stored data and user point of view, because they are temper proof resistant and intense using and they generally have a 10 years guarantee.

Refering to the card functioning, this is, in principle, a microcontroller equipped with processor, ROM and Flash memory which variates, based on the model, from 1kB to 16 kB. The whole microdevice is powered from the external antenna through the electromagnetic field generated current of the reader antenna over the smartcard antenna. The antenna serves for the communication between the microprocessor and the reader and for the

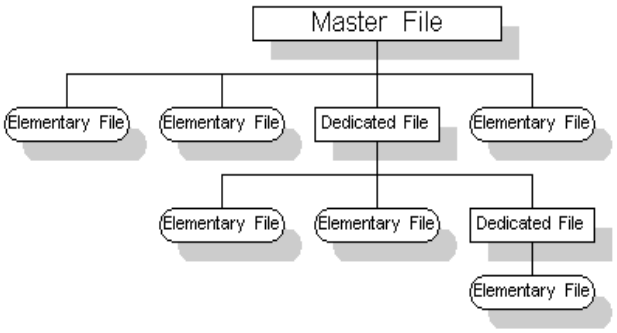

Fig 1. File organization system structure for Smart Card

alimentation of the whole microcontroller, so external power sources are no longer needed. This contributes to the smartcard viability.

The embeded ROM memory serves for storing an Operating system, which offers several functions both for communication encrypting between card and reader and for file operations or small programs executions. The structure of keeping files is a classical one, with an arborescent form, as shown in the fig.1. There are tree types of files:

- master files – simillar with FAT;
- dedicated files – simillar with a directory;
- elementary files – simillar with binarry files.

It also must be mentioned that any file has its own password and encryption key, so that, if the smartcard is used for several applications, one of the application cannot access, under no circumstances, other application's files.

3. Tranceiver Structure and Functions

A smart card reader/writer have a principal scheme as shown in the next picture, in which we can see:

- *the interface unit* contains a card reader in which can be accessed both smart cards and contact cards;
- *intelligent transceiver* – the heart of the device – is made around a microprocessor, and it manages read/write functions from/to smart card, as well as communication with the local PC or radio communication with the central calculator from the administrative headquarters;
- *extern power supply* is insured by a low voltage source – with double power supply (accumulator and network pile) and the status of the device is shown with the four leds. They have the following signification: PWR – powered device, TRANS – transmission indicator, REC – receive indicator, CONTACT – accept indicator of the smart card which is in the device.

The reader contains an interface for RS232 and offers communication functions for that (safely message transmission/receiving inssurance). This interface doesn't offer though the securization for transmission on the serial line. It is assumed that this line was already protected (it isn't in sight).

For contactless smartcards, the reader is not outside, except for its antenna and the link cable between them can have approx. 33m (with coaxial

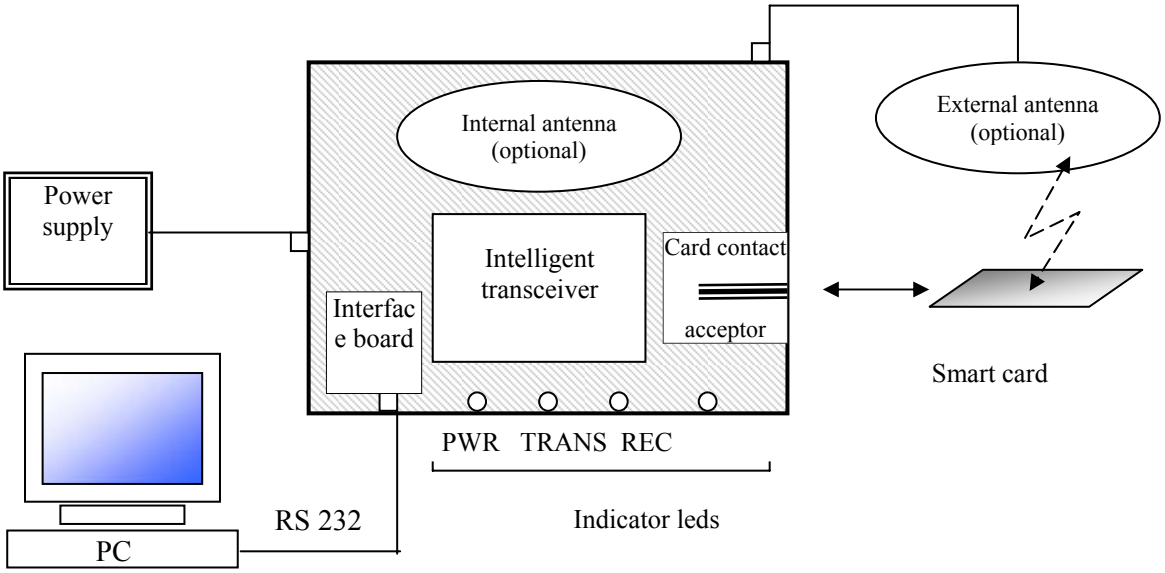

Fig 2. Application using Smart Card

cable), which is sufficient for sefety amplasament of the reader.

4. PC Applications Structure and Functions

The application is basically composed of four functional modules, as shown in the fig.3. This modules interact beteween them based on the relationships described in the figure. Foward, we will describe every single module and the type of interactions with other modules.

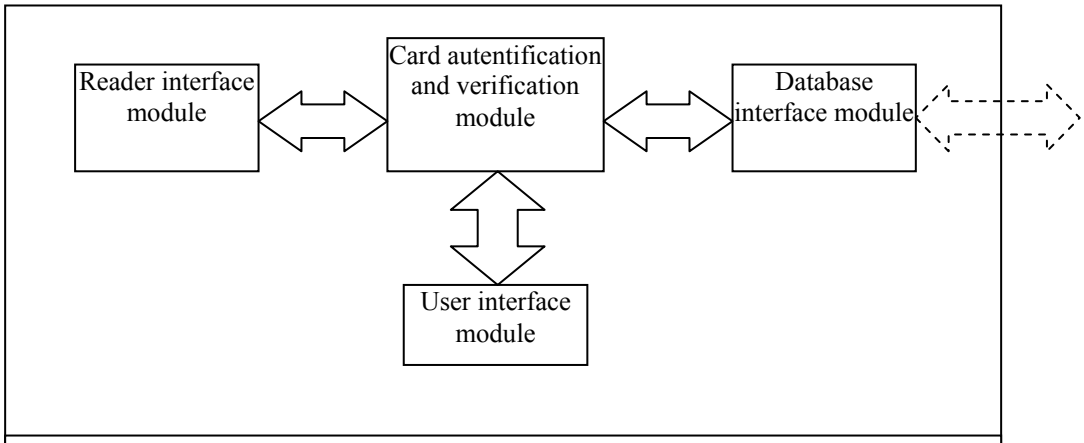

Fig 3. Application structure.

Reader interface module

This module is designed for easier communication with the reader, according to the describbed communication protocol [1]. Obviously, the main function of this module is communication with the smartcard reader, returning a variable set which coresponds wtih the card stored data. This module also signals the presence of a card in front of a reader.

Card autentification and verification module

Basically, this module encrypt/decrypt the keys used in tranzactions and saves in the database the card returned informations and the hacking attempts. For writting informations into the database , it is used the Microsoft JET engine, to access an Access database, which is presented as a separate module.

The module send and receive the necessary messages for the current system state showing from the user interface module.

User interface module

In fact, this module is the form showed by the program for serving the user to personal identification. This contains the follwing fields:
Field in which is displayed ”Mr.” or “Mrs.”
First Name:identificated person first name
Last Name:identificated person last name
Age: person age(for the ladies, this parameter can miss)
Function: identified person function inside the belonging institution
Department: department inside the institution in which the person activates
Activ: if the person is on holidays or not
Field in which is displayed ”acces granted” or “access restricted”

Database interface module

In fact, this module is an Access database with its tables and relationships. The database was created so it can be used also by another application, for example an automatic hour count or an automatic statistic of peple circulation in a building.

5. Software Application Structure

The software application is composed from data structures and functional objects which interact. The application is distributed between the PC type host computer and the smart card resources, which has memory and microprocessor.

The data structure, at the host computer level, is organized as an Access relational database. DATA database tables are presented, generally, in the next table, in which is indicated the location of the data on the smart card

Automatic personal identification application, along with the identification, contains the necessary functions for preparing several data for another application, such as access control and/or automatic hour count. Therefore, smart card readers/writers are seen as being located at access doors level, in the database structure.

TABLE	FIELD	LOCATION	SEMNIFICATION
ACCESSTABLE	Reference No	BD	Refererence number
	Event date	BD	Event date (access date)
	type	BD	Event type
	state	BD	State
	literal	BD	Explicative text
	cardnum	BD	Card number
	doornum	BD	Door number
	nodenum	BD	Network node number
	eventmsg	BD	Event message
	eventtime	BD	Event moment
ALARMS	index	BD	Alarm index
	alarm a	BD	Alarm text
CONFIG	index	BD	Access index
	doornum	BD	Door number
	doorname	BD	Door name
	Dir	BD	Access direction
	nodenum	BD	Network number node
	security_level	BD	Security level
	security_alert	BD	Alert type
	Port	BD	Host communication port
	Baud	BD	Transfer rate
	portstring	BD	Port number
HOURS	tip_program	BD	Working program type
	Start1	BD	Start of the program 1
	Stop1	BD	End of program1
	Start2	BD	Start of program2
	Stop2	BD	End of program2
	alarm_code	BD	Alarm code
PERSONAL	Pin	BD+SC	Personal identification number
	Card_code	BD+SC	Card code
	lnume	BD+SC	Owner's last name
	fname	BD+SC	Owner's first name
	Age	BD	Owner's age
	bdate	BD+SC	Owner's birthday
	Sex	BD+SC	Owner's sex
	function	BD+SC	Owner's function
	department	BD+SC	Working Department
	program_type	BD+SC	Owner's program type
	Activ	BD+SC	Owner's state (activity/nonactivity)
	security_level	BD+SC	Security level access

Next, it is presented a DATA database example as it is seen by the ACCESS component inside the Microsoft Office package.

D:\data.mdb 8 march 2006
Table: accesstable Page: 1

Properties

Date Created: 28/02/2006 04:26:52 PM Def. Updatable: True
Last Updated: 07/03/2006 12:25:31 PM OrderByOn: False
RecordCount: 2

Columns

Name	Type	Size
ReferenceNo	Number (Long)	4

AllowZeroLength: False

	Attributes:	Fixed Size	
	Collating Order:	General	
	ColumnHidden:	False	
	ColumnOrder:	Default	
	ColumnWidth:	Default	
	Decimal Places:	Auto	
	Default Value:	0	
	DisplayControl:	Text Box	
	Ordinal Position:	1	
	Required:	False	
	Source Field:	ReferenceNo	
	Source Table:	accesstable	
eventdate		Date/Time	8
	AllowZeroLength:	False	
	Attributes:	Fixed Size	
	Collating Order:	General	
	ColumnHidden:	False	
	ColumnOrder:	Default	
	ColumnWidth:	2580	
	Format:	Short Date	
	Ordinal Position:	2	
	Required:	True	
	Source Field:	eventdate	
	Source Table:	accesstable	
type		Number (Long)	4
	AllowZeroLength:	False	
	Attributes:	Fixed Size	
	Collating Order:	General	
	ColumnHidden:	False	
	ColumnOrder:	Default	
	ColumnWidth:	Default	
	Decimal Places:	Auto	
	Default Value:	0	
	DisplayControl:	Text Box	
	Ordinal Position:	3	
	Required:	False	
	Source Field:	type	
	Source Table:	accesstable	
state		Number (Long)	4
	AllowZeroLength:	False	
	Attributes:	Fixed Size	
	Collating Order:	General	

Based on the utilization possibilities of automatic identification application, on the host computer, associated with other specific applications such us control access or automatic time sheet, an interactive diagram may be describe between these and the application implemented on the smart card. (figure 4). The difference from the other types of cards (magnetic, bar code etc) consist in fact that on the smart card can be applications witch carries through himself processor, including communication protocol, opposite from data organize into a fix structure. On the smart card level can coexist applications witch executes considering dialog partner with card too. In these conditions the level of smart card data protection is very high, by using sophisticated access key and through cryptographic algorithms of information, witch can be different function of applications on the smart card.

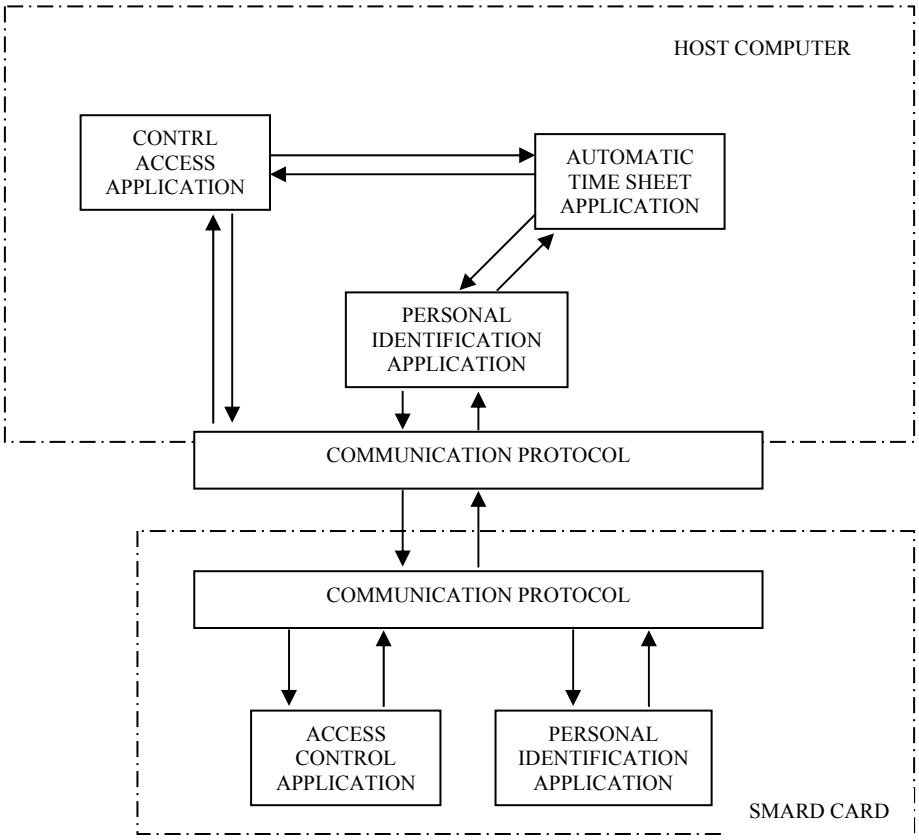

Figure 4. Variant of interactive diagram

6. Concluding Remarks

The application of automatic personal identification was developed on a PC configuration type IMB Pentium II, such transceiver was use the variant SCI 5000 EYECON SMART TRANSMITTER with contact interface and antenna for contact less interface, the smart cards being OTI's manufacture. For software developer were use: operating system Windows 2000, MS Visual C++, MS Visual Basic, MS Access, EYECON ActivX.

There were developing programs for control access and personal automatic identification conforming interactive diagram from figure 4, witch were require very good in conditions of real simulations for a variety types of test games.

References

[1] V. Sgarciu (coord) - Programs system used in public and private service domain, using advanced technologies based on smart cards, Research Internal Report, Dec 2000

[2] W. Rankl - Smart Card Handbook, John Willey, 1997

[3] U. Hansmann - Smart Card Application Development Using Java, John Willey, 1999

[4] Z. Chen - Java Card Technology for Smart Cards: Architecture and Programmer's Guide, John Willey, 2000

[5] Siu-cheung Charles Chan - An Overview of the Java Security, http://home.hkstar.com/ ~alanchan/ papers/javaSecurity/index.html

[6] M. Vlad Cartelele inteligente ale viitorului - 1,2,3,4, PC World Romania, 2001

[7] M. Vlad, V. Sgarciu, M. Ceaparu Integrated system used in automatic personal identification to a reobot mainframe. IAD 2003 Proceedings, 2003