CS2K707(P) Seminar Report

on

Smart Card

Submitted In Partial Fulfilment Of The Degree Of

Bachelor Of Technology

by

Partha Bag
Y1.215, S7 CSE

Department of Computer Science & Engineering
National Institute of Technology, Calicut
2004 Monsoon

National Institute of Technology, Calicut
Department of Computer Science & Engineering

Certified that this Seminar Report entitled

Smart Card

is a bonafide report of the Seminar presented by

Partha Bag
Y1.215, S7 CSE

in partial fulfilment of the degree of
Bachelor of Technology

Mr.Vinod P.
Seminar Coordinator
Lecturer
Dept.of Computer Science & Engineering

Dr.V.K.Govindan
Professor and
Head
Dept.of Computer Science & Engineering

Abstract

An integrated circuit card (ICC), more popularly known as a smart card, temper-resistant, computer programmable data storage. It has the exact shape and size of a debit(ATM) card, but can hold 4KB-64KB of information and perform modest amount of data processing as well. Smart card ensures data security and integrity. By data security we mean that the data value or computation contained on the card can be accessed by the authorised person or department. Data integrity gurantees that the value of the data stored on the card is defined at all the times and is not corrupted. This property must hold even if power to the smart card is cut during the computation involving the information on the card.

Contents

1 Introduction **1**

2 Smart Card Architecture **2**
2.1 Types of available cards 2
2.1.1 Memory cards 2
2.1.2 Microcontroller cards 2
2.1.3 Contactless cards 2

3 Elements of a smart card **3**
3.1 Central processing unit 3
3.2 Memory units 3
3.3 Input/Output 3
3.4 Interface Devices 4
3.5 Selecting right option 4

4 Standards and Specification **4**

5 Security and Cryptography **6**

6 Operating System and Card-Terminal Interface **7**
6.1 File System 7
6.2 Smart card software 7
6.2.1 Card Software 7
6.2.2 Host Software 7

7 The Future in the industry **9**

8 Conclusion **10**

1 Introduction

France was early to use the smart card in the world, its researches on 1970's reflected a national effort to use this technology. France was unsuccessful to use this technology. But this didn't stop use of smart cards over the markets. France was trying to reduce the money tranaction over telecommunication and the smart card showed its potential to reduce the money transaction. The term smart card was coined by French publicist Roy Bright in 1980, however it was invented by two German engineers in 1967 and 1968, Jurgen Dethloff and Helmut Grottrupp. They filed for a patent in February 1969 but were only granted the patent in 1982 titled "Identifikanden/Identifikationsschalter". Independently, Kunitaka Arimura of the Arimura Technology Institute in Japan filed for a smart card patent in Japan in 1970. The following year, Paul Castrucci of IBM filed an American patent titled "Information Card". A French journalist, Roland Moreno filed 47 smart card related patents in 11 countries between 1974 and 1979.

2 Smart Card Architecture

2.1 Types of available cards

Smart cards that are currently available on the market can be classified into the three categories below. Cards with:

- surface contacts connected to a memory-only integrated circuit chip (IC) - memory cards.
- surface contacts connected to an IC chip containing a microprocessor - microcontroller cards.
- an electromagnetic connection to an IC chip containing a microprocessor - contactless cards.

2.1.1 Memory cards

The earliest smart cards were memory cards that contained an integrated circuit chip only containing nonvolatile memory and the necessary circuitry to read and write to the memory. These cards are dependent on the smart card reader or the computer for processing. They still comprise the majority of smart cards in use today. They are inexpensive and provide a modest level of security. Memory cards are suitable for applications that perform fixed operations. Examples of memory cards include pre-paid phone cards and high-security alternatives to magnetic stripe cards.

Memory cards use a synchronous communication protocol between the reader and the smart card. The communication channel is always under the control of the reader. A variation on the memory card is the logic card. This card incorporates security enhancements through the provision of memory addressing circuitry that requires a shared secret between the reader and the smart card chip.

Yet another variation on the memory card is the optical card. Optical cards can store up to 4MB of data. However, once written, this data cannot be changed or removed. These cards are suited for applications requiring record keeping (such as medical, driving or travel records). Existing optical cards do not contain a processor. The card readers use non-standard protocols and are expensive.

2.1.2 Microcontroller cards

These are also known as "chip cards" as they contain a microprocessor chip and can process data on the card. The current generation of microprocessor cards has the equivalent processing power of original IBM-XT computers (with slightly less memory capacity). Examples of microprocessor cards include cards that hold money, cards that provide secure access to networks, and cards that secure cellular telephones from fraud.

2.1.3 Contactless cards

These cards make use of an electromagnetic signal for communication between the reader and the smart card. The power required to run the chip is transmitted at microwave frequencies from the reader. These cards offer greater ease of use for certain applications where possession of the card is sufficient for card use (e.g. toll stations, identification etc.).

3 Elements of a smart card

The Central Processing Unit (CPU), memory and Input/Output electronics are assembled into one integrated circuit chip. Figure1 below illustrates the organisation of these components on the card. The simple packaging provides all the capabilities required of smart cards in a very small package. In addition, it conceals the interconnections between the various component elements making it difficult for an observer to intercept these signals.

3.1 Central processing unit

Traditionally this is an 8-bit microcontroller but increasingly more powerful 16 and 32-bit chips are being used. However, none have multi-threading and other powerful features that are common in standard computers. Smart Card CPUs execute machine instructions at a speed of approximately 1 MIPS. A coprocessor is often included to improve the speed of encryption computations.

3.2 Memory units

There are three main types of memory on cards:

- RAM. 1K. This is needed for fast computation and response. Only a tiny amount is available.
- EEPROM (Electrically Erasable PROM). Between 1 to 24K. Unlike RAM, its contents are not lost when power is on. Applications can run off and write to it, but it is very slow and one can only read/write to it so many (100 000) times.
- ROM. Between 8 to 24K. The Operating System and other basic software like encryption algorithms are stored here.

3.3 Input/Output

This is via a single I/O port that is controlled by the processor to ensure that communications are standardized, in the form of APDUs (A Protocol Data Unit).

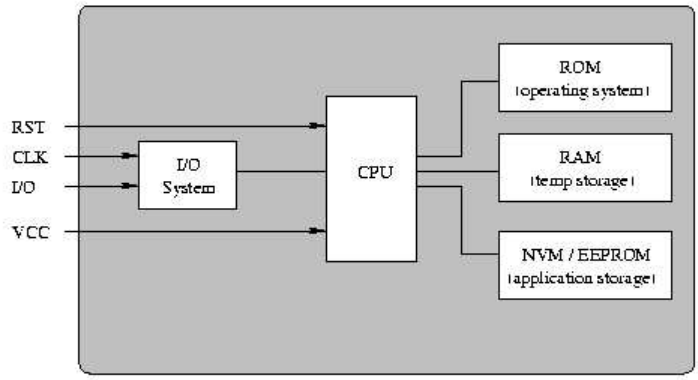

Figure 1: Layout of a smart card integrated chip

3.4 Interface Devices

Smart Cards need power and a clock signal to run programs, but carry neither. Instead, these are supplied by the Interface Device - usually a Smart Card Reader - in contact with the card. This obviously means that a Smart Card is nothing more than a storage device while being warmed in your pocket. In addition to providing the power and clock signals, the reader is responsible for opening a communication channel between application software on the computer and the operating system on the card. Nearly all Smart Card readers are actually reader/writers, that is, they allow an application to write to the card as well as read from it. The communication channel to a Smart Card is half-duplex. This means that data can either flow from the IFD to the card or from the card to the IFD but data cannot flow in both directions at the same time. The receiver is required to sample the signal on the serial line at the same rate as the transmitter sends it in order for the correct data to be received. This rate is known as the bit rate or baud rate. Data received by and transmitted from a Smart Card is stored in a buffer in the Smart Card's RAM. As there isn't very much RAM, relatively small packets (10 - 100 bytes) of data are moved in each message.

3.5 Selecting right option

As a system is built, whether it be a healthcare, financial services, or telecommonication, a specific set of option must be chosen and trade-offs made to maximize the available memory and limited processing abilities of the smart card.The following options should be considered in the decision-making process:

- Use of dedicated coprocessors.
- size of silicon.
- Operating systems.
- File Structures.
- Security.
- Terminals.
- Processing speed.
- Testing methodology.

4 Standards and Specification

ISO 7816 series of standards and the ETSI SCP standards are the most important and relevant for SmartCard application programmers. ISO stands for the International Standards Organization while ETSI stands for the European Telecommunications Standards Institute. There are several other standards as well:

- ISO 7810 - Identification cards (Physical characteristics).
- ISO/IEC 7812 - Identification of issuers.
- ISO/IEC 10536 - Identification Cards (Contactless).
- ISO/IEC 10373 - Identification cards (Test methods).
- ISO/IEC 14443 - Remote-coupling communication cards (Contactless).
- ISO TC 68 - Banking and related financial services.
- EN 742 - Identification cards.

- EN 726 Terminal Equipment (TE) - Requirements for IC cards and terminals for telecommunication use. The standard is the technical basis for SmartCards in Europe.

The last two standards are issued by the European Committee for Standardization (CEN). In particular, EN 726 is a tribute to the major role that telecommunications companies in Europe played in the early days of Smart Card Technology.

Smart Cards are becoming increasingly important in banking and e-commerce, thanks largely to the EMV standard defined in 1994 by Mastercard and its European subsidiary Europay, and Visa. Recently, a European-issued SmartCard was used in chip terminals in South America for payment.

5 Security and Cryptography

One of the primary reasons that smart cards exist is for security. The card provides a computing platform on which information can be securely stored. Moreover, computations can also be carried out securely. Consequently, smart cards are ideally suited to enhance the security of other systems. Some examples of these applications include physical access systems and financial systems (including electronic commerce applications).

The information stored on a smart card can be configured such that access to it can be strictly controlled by the card holder, the card issuer, or the provider of any specific applications on the card. Access control is generally implemented by requiring a key or PIN to access certain files. These keys are stored in key files on the card. Only the smart card can access these key files for comparison with the key obtained from the smart card reader or user. Smart cards provide a variety of useful security features, including:

- Storage of passwords for access to computer systems, networks etc.
- Storage of keys, public and private, for encrypting information to ensure its privacy.
- Storage of keys, public and private, for authenticating identity.
- Storage of information to be transported without the cardholder being able to access or change that information in any way.
- Performance of encryption algorithms for authenticating identity.
- Performance of encryption algorithms for ensuring the privacy of information.

The authentication procedure may be simple (e.g. demonstrating the possession of a shared secret such as a PIN) or may be complex (e.g. demonstrated the ability to encode a message offered known as a challenge with a particular key and algorithm). If the authentication process does not complete successfully, all further communication is blocked. A record of all failed attempts may be kept on the card. Once a certain number of consecutive failures is reached, the card may destroy itself and its contents completely.

The encryption of transaction information is often referred to as bulk encryption. In general, smart cards are not involved in bulk encryption processes. Encryption and decryption is computationally intensive. In addition, some cryptographic algorithms require significantly more computation than others do. In particular, public-key encryption is far more intensive that symmetric key encryption. However, a few cards are specifically built for this purpose and are equipped with a dedicated processor (known as a crytoprocessor) which performs the encryption. An example of this type of smart card is the Cryptoflex smart card manufactured by Schlumberger. The Cryptoflex can perform encryption using the following algorithms: DES, triple DES and RSA 1024 public-key encryption.

Encryption can be applied to all messages to and from the smart card or alternatively only to particular messages. Generally smart card programmers do not have to design new authentication or encryption algorithms. Instead, they use the facilities that are built into the smart card which, is provided with a certain level of assurance of correctness.

6 Operating System and Card-Terminal Interface

The operating system found on the majority of Smart Cards implements a standard set of commands (usually 20 - 30) to which the Smart Card responds. Smart Card standards such as ISO 7816 and CEN 726 describe a range of commands that Smart Cards can implement. Most Smart Card manufacturers offer cards with operating systems that implement some or all of these standard commands (and possibly extensions and additions). The relationship between the Smart Card reader and the Smart Card is a master/slave relationship. The reader sends a command to the Smart Card, the card executes the command and returns the result (if any) to the reader and waits for another command.

Microsoft released a miniaturized version of Windows for Smart Cards in late 1998, and early versions of a Gnu O/S have been released.

6.1 File System

Most operating systems also support a simple file system based on the ISO 7816 standard. A Smart Card file is actually just a contiguous block. Files are organized in a hierarchical tree format. Once a file is allocated, it cannot be extended and so files must be created to be the maximum size that they are expected to be. Each file has a list of which parties are authorized to perform which operations on it. There are different types of files: linear, cyclic, transparent, SIM, etc. The usual create, delete, read, write and update file operations can be performed on all of them. Certain other operations are supported only on particular types of files.

6.2 Smart card software

Smart card software can be categorised into two types:

- Card software
- Host software

This section describes the purpose of each of these.

6.2.1 Card Software

Card software or card-side software is software that runs on the smart card itself. Card software provides computational services for applications that access the data contained in the card. It also protects this data from applications that may attempt to access it incorrectly. Card software implements the data, security properties and policies of a particular smart card. It is usually classified into application software and system software. Application software uses the computational and data storage capabilities of a smart card in the same manner as any computer. Application-specific software is typically written in:

- Assembly language for the chip architecture of the microprocessor found embedded in the smart card.
- A high-level language that can be interpreted directly on the card or compiled into assembly language and loaded onto the card.

System software explicitly uses and may contribute to the data integrity and data security properties of the particular smart card.

6.2.2 Host Software

Host software runs on a computer that is connected to a smart card. Host software is also referred to as reader-side software. It mostly includes end-user application software, system

software that supports smart cards and smart card readers. Host software is usually written in a high-level programming language such as C, C++, Java, Pascal etc. and linked with commercially available libraries and device drivers to access smart cards and readers.

In order for a host smart card program to conduct business with a smart card it must first ensure that the particular smart card is authentic. To complete the mutual authentication, the program must then convince the smart card that it is authentic.

7 The Future in the industry

Credit, debit, ATM, loyalty and membership cards have changed our lives and the the way we conduct. The smart card industry is quickly maturing, moving from an analog physical card environment to an electronic one. As a consequence, an entirely new type of landscape has been created. This environment will be far more better secure than today's magnetic-strip and paper-based transactions. The future trend we expect to see include the following:

- Electronic Commerce
- Improved Technologies
- New time constrains
- New skill sets
- Easy-to-use application
- A merging of dicipline
- An increased role of boimetrics
- A growing array of application
- More sophisticated security
- A greater diversity in the development and innovation of smart card application

8 Conclusion

Smart card will greatly contribute to the data warehousing and data mining, and elcetronic commercial transaction. These cards support various applications. There should be increase in the application it offers in the near future. At least for the near future, we believe smart card technological advances are likely to out pace legal and ethical concern, but to become a universal identification card there should be more research on privacy and security.

References

[1] Berinto, S. Smart cards:The intelligent way to security, Network Computing 9,9(May 15,1998), 168.

[2] Fletcher, P. Europe holds a winning hand with smart cards, Electronic Design 47,1 (Jan. 11, 1998)76.

[3] Husemann, D. The Smart Card: Don't leave home without it, IEEE Concurrency 7, 2(April-June 1999), 24-27.

[4] Jain, A., Hong, L. and Pankanti, S. Biometric identification. Commun. ACM 43, 2(Feb. 2000), 90-98.

[5] Shelfer, K.M. and Procaccino, J.D. Smart Card Evolution. Communications of the ACM vol.45,no.7(July 2002),83-88.

[6] Dreifus, H. and Monk, J.T., Smart Cards, John Wiley and Sons, Inc.