A

Seminar report

on

Smart Card

Submitted in partial fulfillment of the requirement for the award of degree
Of Electronics

SUBMITTED TO: **SUBMITTED BY:**

www.studymafia.org www.studymafia.org

Preface

I have made this report file on the topic **Smart Card;** I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to ……..who assisting me throughout the preparation of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

Introduction

A smart card, a type of chip card is a plastic card embedded with a computer chip that stores and transacts data between users. The card data is transferred via a reader that is part of a computing system. Smart card-enhanced security systems are in use today throughout several key applications, including healthcare, banking, entertainment and transportation.

To various degrees, all applications can benefit from the added features and security that smart cards provide. According to Dataquest, the worldwide smart card market will grow to 6.8 Billion units and $11 Billion by 2006.

Introduction of smartcard technology has found its way to a number of proprietary financial applications like credit/debit card transit application, Personal Identification card, loyalty card for purchasing applications...etc . This paper covers smart card and mobile payment schemes that are available in the market.

With the introduction of high ended smart card like java card as SIM card, even mobile phone is also equipped with payment applications. The next section describes briefly about the existing payment schemes in market. Also we cover in brief the potential of mobile payment schemes in the coming years. In the final section gave a small survey result regarding the future of electronic payments.

Definition

It is believed that smart cards offer more security and confidentiality than the other kinds of information or transaction storage. Moreover, applications applied with smart card technologies are illustrated which demonstrate smart card is one of the best solutions to provide and enhance their system with security and integrity.

Different kinds of scheme to organise and access of multiple application smart card are discussed. The first and second schemes are practical and workable on these days, and there is real applications developed using those models. For the third one, multiple independent applications in a single card, there is still a long way to go to make it becomes feasible because of several reasons.

At the end of the paper, an overview of the attack techniques on the smart card is discussed as well. Having those attacks does not mean that smart card is unsecure. It is important to realise that attacks against any secure systems are nothing new or unique. Any systems or technologies claiming 100% secure are irresponsible. The main consideration of determining whether a system is secure or not depends on whether the level of security can meet the requirement of the system.

The smart card is one of the latest additions to the world of information technology. Similar in size to today's plastic payment card, the smart card has a microprocessor or memory chip embedded in it that, when coupled with a reader, has the processing power to serve many different applications. As an access-control device, smart cards make personal and business data available only to the appropriate users. Another application provides users with the ability to make a purchase or exchange value. Smart cards provide data portability, security and convenience. Smart cards come in two varieties: memory and microprocessor.

Memory cards simply store data and can be viewed as a small floppy disk with optional security. A microprocessor card, on the other hand, can add, delete and manipulate information in its memory on the card. Similar to a miniature computer, a microprocessor card has an input/output port operating system and hard disk with built-in security features.

On a fundamental level, microprocessor cards are similar to desktop computers. They have operating systems, they store data and applications, they compute and process information and they can be protected with sophisticated security tools. 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, which require strong security protection and authentication.

History

- **1968**

German inventor Jurgen Dethloff along with Helmet Grotrupp filed a patent for using plastic as a carrier for microchips.

- **1970**

Dr. Kunitaka Arimura of Japan filed the first and only patent on the smart card concept

- **1974**

Roland Moreno of France files the original patent for the IC card, later dubbed the “smart card.”

- **1977**

Three commercial manufacturers, Bull CP8, SGS Thomson, and Schlumberger began developing the IC card product.

- **1979**

Motorola developed first single chip Microcontroller for French Banking

- **1982**

World's first major IC card testing

- **1992**

Nationwide prepaid card project started in Denmark

- **1999**

Federal Government began a Federal employee smart card identification

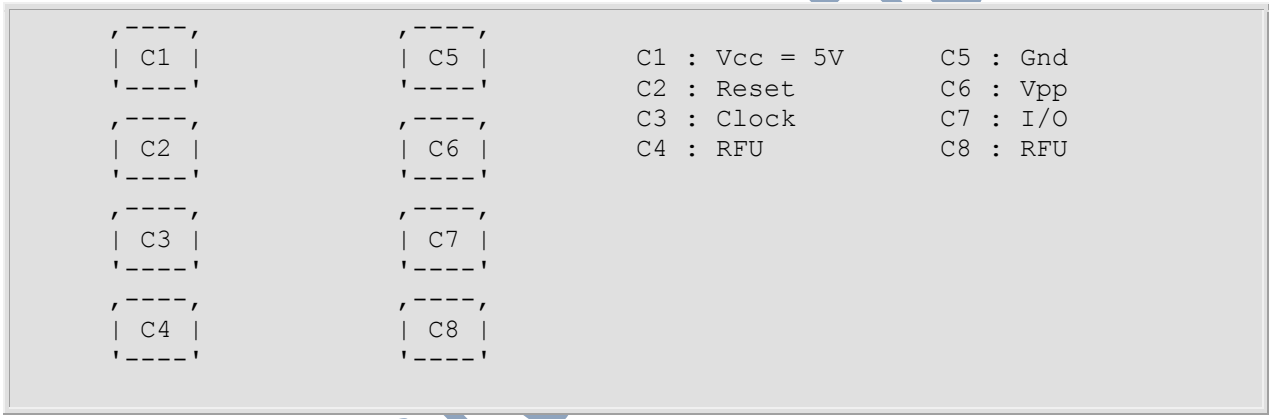
Classification of Smart Cards

Due to the communication with the reader and functionality of smart cards, they are classified differently.

Contact vs Contactless

As smart cards have embedded microprocessors, they need energy to function and some mechanism to communicate, receiving and sending the data. Some smart cards have golden plates, contact pads, at one corner of the card.

This type of smart cards are called *Contact* Smart Cards. The plates are used to supply the necessary energy and to communicate via direct electrical contact with the reader. When you insert the card into the reader, the contacts in the reader sit on the plates. According to ISO7816 standards the PIN connections are below:



- I/O : Input or Output for serial data to the integrated circuit inside the card.
- Vpp : Programing voltage input (optional use by the card).
- Gnd : Ground (reference voltage).
- CLK : Clocking or timing signal (optional use by the card).
- RST : Either used itself (reset signal supplied from the interface device) or in combination with an internal reset control circuit (optional use by the card). If internal reset is implemented, the voltage supply on Vcc is mandatory.
- Vcc : Power supply input (optional use by the card).

The readers for contact smart cards are generally a separate device plugged into serial or USB port. There are keyboards, PCs or PDAs which have built-in readers like GSM cell phones. They also have embedded readers for GSM style mini smart cards.

Some smart cards do not have a contact pad on their surface.The connection between the reader and the card is done via radio frequency (RF). But they have small wire loop embedded inside the card. This wire loop is used as an inductor to supply the energy to the card and communicate with the reader. When you insert the card into the readers RF field, an induced current is created

in the wire loop and used as an energy source. With the modulation of the RF field, the current in the inductor, the communication takes place.

The readers of smart cards usually connected to the computer via USB or serial port. As the contactless cards are not needed to be inserted into the reader, usually they are only composed of a serial interface for the computer and an antenna to connect to the card.

The readers for contactless smart cards may or may not have a slot. The reason is some smart cards can be read upto 1.5 meters away from the reader but some needs to be positioned a few millimeters from the reader to be read accurately.

There is one another type of smart card, combo card. A combo card has a contact pad for the transaction of large data, like PKI credentials, and a wire loop for mutual authentication. Contact smart cards are mainly used in electronic security whereas contactless cards are used in transportation and/or door locks.

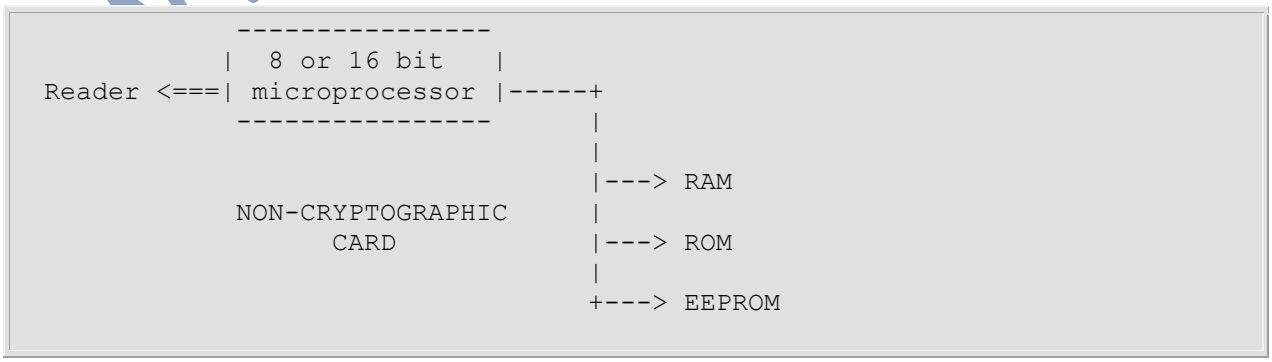
Memory vs Microprocessor

The most common and least expensive smart cards are memory cards. This type of smart cards, contains EEPROM(Electrically Erasable Programmable Read-Only Memory), non-volatile memory. Because it is non-volatile when you remove the card from the reader, power is cut off, card stores the data.

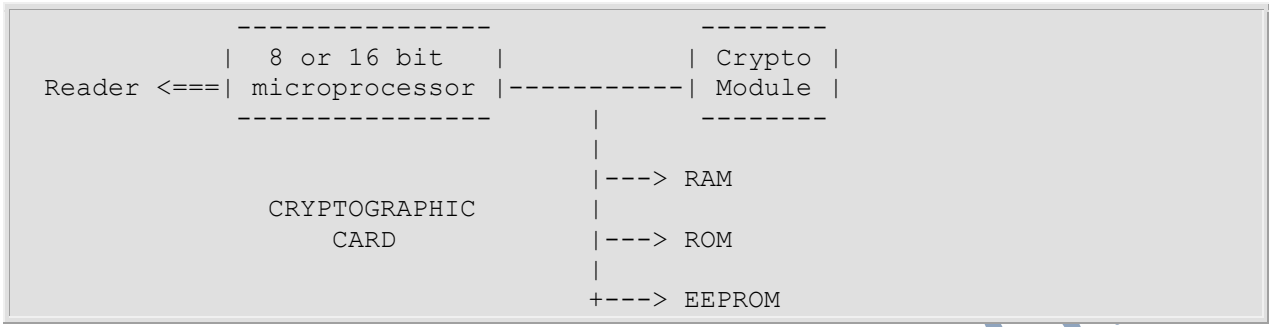
You can think of EEPROM, inside, just like a normal data storage device which has a file system and managed via a microcontroller (mostly 8 bit). This microcontroller is responsible for accessing the files and accepting the communication. The data can be locked with a PIN (Personal Identification Number), your password.

PIN's are normally 3 to 8 digit numbers those are written to a special file on the card. Because this type is not capable of cryptography, memory cards are used in storing telephone credits, transportation tickets or electronic cash.

Microprocessor cards, are more like the computers we use on our desktops. They have RAM, ROM and EEPROM with a 8 or 16 bit microprocessor. In ROM there is an operating system to manage the file system in EEPROM and run desired functions in RAM.



As seen in the diagram above all communication is done over the microprocessor, There is no direct connection between the memory and the contacts. The operating system is responsible for the security of the data in memory because the access conditions are controlled by the OS.



With the addition of a crypto module our smart card can now handle complex mathematical computations regarding to PKI. Because the internal clock rate of microcontrollers are 3 to 5 MHz, there is a need to add a component, accelerator for the cryptographic functions.

The crypto-cards are more expensive than non-crypto smart cards and so do microprocessor card than memory cards.

Relation between SIM card and Smart card

Subscriber Identification Module (SIM) is a smartcard which is being used by the mobile phone to identify each mobile device with other. This Card is provided by the mobile network provider. Each SIM card contains a unique key. Mobile phone will use data encrypted with this key to communicate with its network.

The Mobile equipment (ME) will talk to the SIM card for the encryption in some standardized way. The ME talk to the SIM in some format viz APDU (see Appendix). When the user connects to the mobile network, the mobile equipment requires executing some command for authorizing/authenticate the user.

This is done by the application inside SIM card. For this purpose the ME initiate a set of gsm standard commands in some particular order and achieve the result. The GSM pecification standardized the communication with the SIM. For more details regarding the security see Appendix.

For a GSM mobile phone the steps and procedure for all the functions are standardized by the GSM mobile community. This Standard is defined in GSM11.11. SIM card contain an application which can respond to the command which are initiated by the ME.
In short SIM card is a smartcard with an application which implement the gsm11.11 specification.

With the technological advancement in the area of smart card especially with java card, it is possible to implement more than one application in the same java card.

This enables the java card to be used as SIM card as well as smartcard for payment application.

Application of Smart Card

- **Payment System**
  A payment function is an integral part of most smart card applications because most services accessible by smart cards must be paid one way or the other.

- **Smart Networking**
  Smart card technologies provide strong security through encryption as well as access control, based on identification technologies such as biometrics.

- **National ID / Authentication**
  In the wake of 9/11 attack a need has been felt in many countries for tamperproof ID cards and a secure authenticating device. Many countries all over the world are trying out, and implementing, the smart card option as a national identity card.

- **University Identification**
  The traditional student ID card can be replaced by an all-purpose chip-based student ID card, containing a variety of applications such as electronic purse for vending and laundry machines), and for use as a library card, and meal card.

- **Financial Applications**
  Smart cards are being used as an electronic purse, or epurse, to replace coins for small purchases in vending machines and over-the counter transactions. This area is growing rapidly in Europe and the U.S.

- **Retail & Loyalty**
  Smart cards are used to record the transactions of the customer, which are helpful in implementation of loyalty programs.Consumer reward/redemption is tracked on a smart loyalty card that is marketed to specific consumer profiles and linked to one or more specific retailers serving that profile set.

- **Communication Applications**
  The chip-based cards help secure the initiation of calls and the identification of callers (for billing purposes) on any Global System for Mobile Communications (GSM) phone

- **Transportation**
  Mass transit fare collection systems are using smart tickets, which are easy to load and redeem for a fare. These smart tickets can be disposable -that means use and throw away- or can be given only to regular travelers.

Advantages of Smart Card

- Flexibility
- Security
- Portability
- Increasing data storage capacity
- Reliability.

Disadvantages of Smart Card

- NOT tamper proof
- Can be lost/stolen
- Lack of user mobility – only possible if user has smart card reader every he goes
- Has to use the same reader technology
- Can be expensive
- Working from PC – software based token will be better
- No benefits to using a token on multiple PCs to using a smart card
- Still working on bugs

Conclusion

The smart card being most secure and proven for its security, but was not popular amount the payment schemes. The financial institutions were watching the developments in the area of smart card, until it get mature.

But inspite of its proven capability in the area of security, smart card failed to get enough popularity. One of the reasons of it is the lack of acceptance by the user.
The penetrations of mobile device like mobile phone and PDA have made a significant impact in the area of e commerce.

The mobile operators are also try to sell “Hard” their product by providing additional value added services. Even the Customer wants to have useful application in their mobile devices. The financial institutions are looking for a new revenue generation business and M-Commerce is one of those new areas.

Steps are taken by the financial organization to set the standards for m-commerce. From the above discussion it is evident that the financial institute, mobile operator and customer are looking towards a reliable, flexible and proven frame work for mobile commerce.
\
If this frame work is in place and supported by financial institutes, then customer will trust the new scheme and mobile commerce is going to be new area of commerce.