IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SMART CARDS

[1]Padmini Kaushik, [2]Shweta.N.Shrivastav, [3]Bipin.P.Lakhani, [4]Ishma.S.Sheikh
[1]Assitant professor, [2]engineering student , [3]engineering student, [4]engineering student
[1]Amravati,
[2]Amravati,
[3]Amravati,
[4]Amravati

1.1 Abstract

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.

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.

1.2 Introduction

It has been said that smart cards will one day be as important as computers are today. This statement contains a bit of an error because it implies that smart cards are not computers, when in fact, they are. Because smart cards are indeed tiny computers, it's difficult to predict the variety of applications that will be possible with them in the future. It's quite possible that smart cards will follow the same trend of rapid increases in processing power that computers have, following "Moore's Law" and doubling in performance while halving in cost every eighteen months.

Smart cards have proven to be quite useful as a transaction/authorization/identification medium in European countries. As their capabilities grow, they could become the ultimate thin client, eventually replacing all of the things we carry around in our wallets, including credit cards, licenses, cash, and even family photographs. By containing various identification certificates, smart cards could be used to voluntarily identify attributes of ourselves no matter where we are or to which computer network we are attached. According to Dataquest, the worldwide smart card market has grown 4.7 Billion units and $6.8 Billion by 2002.

1.3 What is smart card?

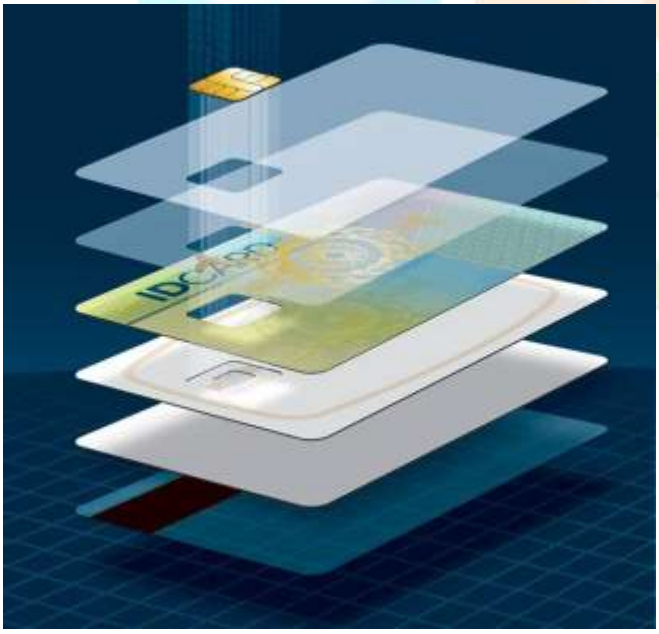
The smart card is one of the latest additions to the world of information technology. Similar in size to today's plastic payment card, the smart card has a microprocessor or memory chip embedded in it that, when coupled with a reader, has the processing power to serve many different applications. This chip is the engine room of the smart card, and indeed is what makes it 'smart'.

The information or data stored on the IC chip is transferred through an electronic module that

interconnects with a terminal or a card reader. This union between a conventional PVC card and a microprocessor allows an immense amount of information to be stored, accessed and processed either off-line or on-line. A smart card carries more information than can be accommodated on a magnetic stripe card. It can make a decision, as it has relatively powerful processing capabilities that allow it to do more than a magnetic stripe card (e.g., data encryption).

1.4 Card Construction

Mostly all chip cards are built from layers of differing materials, or substrates, that when brought together properly gives the card a specific life and functionality. The typical card today is made from PVC, Polyester or Polycarbonate. The card layers are printed first and then laminated in a large press. The next step in construction is the blanking or die cutting. This is followed by embedding a chip and then adding data to the card. In all, there may be up to 30 steps in constructing a card. The total components, including software and plastics, may be as many as 12 separate items; all this in a unified package that appears to the user as a simple device.



1.5 Block Diagram of Smart Card

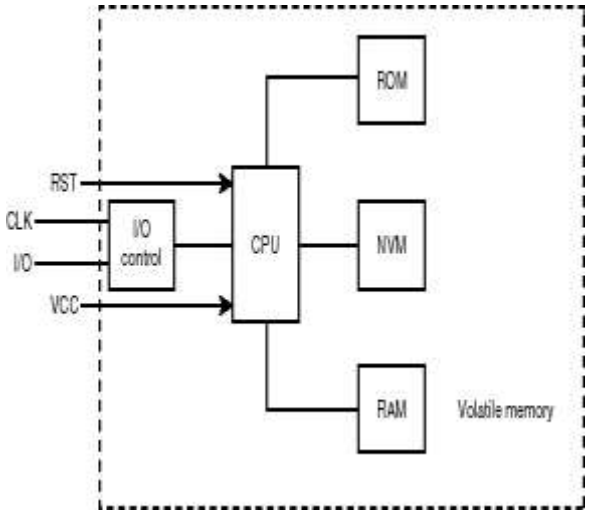


Figure (5.1): Elements of a smart card computer system

1.5.1 Memory System

Smart cards have a memory architecture that will be unfamiliar to most mainstream programmers. In fact, there are three kinds of memory on a smart card: read-only memory (ROM), nonvolatile memory (NVM), and a relatively tiny amount of random access memory (RAM). See Figure 2.

NVM is where the variable data such as account numbers, number of loyalty points, or amount of e-cash is stored. NVM can be read and written by application programs, but it cannot be used like RAM. Although it can be written, the purpose and the performance of the action is totally different. NVM gets its name from the fact that it retains its contents when power is removed from the card.

There is some RAM on a smart card, but not very much Read-only memory is where the smart card operating system is stored. General-purpose Here, one finds various utility routines such as doing communication and for maintaining an on-card file system along with encryption routines and special-purpose arithmetic routines. Code and data are placed in read-only memory when the card is manufactured and cannot be changed; this information is hardwired into the card.

This is the most precious resource on the smart card from the card software developer's point of view. Even when using a high-level language on the smart card, the programmer is acutely aware of the need to economize on the use of temporary variables. Furthermore, the RAM is not only used by the programmer's application, but also by all the utility routines, so a programmer has to be aware not only of

how much RAM he is using, but also how much is needed by the routines he calls.

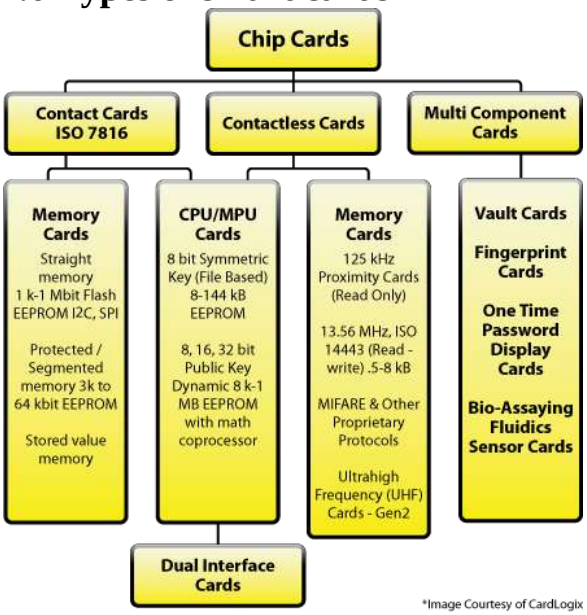
1.5.2 Central Processing Unit

For earlier 8-bit microcontroller, the central processing unit in a smart card chip is typically using the Motorola 6805 or Intel 8051 instruction set. These instruction sets have the usual complement of memory and register manipulations, addressing modes, and input/output operations. CPUs execute machine instructions at the rate of about 400,000 instructions per second (400 KIP), although speeds of up to 1 million instructions per second (1 MIP) are becoming available on the latest chips. The demand for stronger encryption in smart cards has outstripped the ability of software for these modest computers to generate results in a reasonable amount of time. Typically 1 to 3 seconds is all that a transaction involving a smart card should take; however, a 1024-bit key RSA encryption can take 10-20 seconds on a typical smart card processor. As a result, some smart card chips include coprocessors to accelerate specifically the computations done in strong encryption. (Scott Guthery & Tim Jurgensen, 1998)

1.5.3 Smart Card Input/output

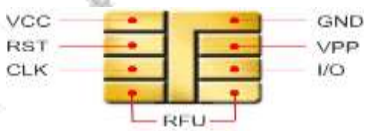
The input/output channel on a smart card is a unidirectional serial channel. The smart card hardware can handle data at up to 115,200 bps, but smart card readers typically communicate with the card at speeds far below this. The communication protocol between the host and the smart card is based on a master (host) and slave (smart card) relationship. The host sends commands to the card and listens for a reply. The smart card never sends data to the host except in response to a command from the host

1.6 Types of smart cards



1.6.1 Contact smart card

These are the most common type of smart card. Electrical contacts located on the outside of the card connect to a card reader when the card is inserted. This connector is bonded to the encapsulated chip in the card. The cards have embedded on them a small gold plate approximately the size of an Australian 5-cent coin, commonly called the 'module'. When the card comes into contact with the reader, it makes contact with several electrical connectors on the module that transfer the information to and from the chip. Contact smart cards are inserted into a smart card reader, making physical contact with the reader. They have a small gold plate about ½" in diameter on the front, instead of the magnetic strip on the back of a credit card.



VCC - Power Supply Voltage
RST - Reset the Microprocessor
CLK - Clock Signal
GND - Ground
VPP - Programming or Write Voltage
I/O - Serial Input/Output Line
RFU - Future Use

Figure (4.2) Card module

Vcc : The supply voltage that drives the chips and is generally 3 volts. However that in the future we are likely to see a move towards 1 volt taking advantage of advanced semiconductor technology and allowing much lower current levels to be consumed by the integrated circuit.

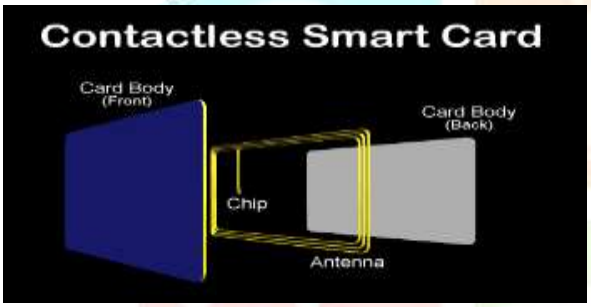
GND : The substrate or ground reference voltage against which the Vcc potential is measured.

RST: The signal line that is used to initiate the state of the integrated circuit after power on.

The CLK signal is used drive the logic of the IC and is also used as the reference for the serial communications link. There are two commonly used clock speeds 3.57 MHZ and 4.92 MHZ
The Vpp connector is used for the high voltage signal that is necessary to program the EPROM memory.
Last, but by no means least is the serial input/output I/O connector. This is the signal line by which the chip receives commands and interchanges data with the outside world.

1.6.2 Contactless Smart Card

These are smart cards that employ a radio frequency (RFID) between card and reader without physical insertion of the card. Instead, the card is passed along the exterior of the reader and read. Types include proximity cards which are implemented as a read-only technology for building access. These cards function with a very limited memory and communicate at 125 MHz Another type of limited card is the Gen 2 UHF Card that operates at 860 MHz to 960 MHz



1.6.3 Dual Interface Cards

These are cards with both a contact and a contactless interface. These may incorporate two non-communicating chips - one for each interface - but preferably have a single, dual-interface chip providing the many advantages of a single e-purse, single operating architecture, etc. A combi card combines the two features with a very high level of security. An example is using the same cad for multiple applications:- contact cards for authenticating secure information over the information network and contactless cards to get access to secure work areas. Contactless and combi-card architectures have many advantages, but it will be several years before the main and traditional contact card-based schemes start to migrate to these technologies

1.6.4 Hybrid Cards

Hybrid cards can be any combination of contact, contact-less and magnetic stripe cards. Since 1982 the French banks have used the combination of chip and magnetic stripe cards as a bank credit card, allowing the banks to migrate to smart chip cards (Scott Guthery & Tim Jurgensen, 1998). They get the advantage of a more secure card while allowing a reasonable time to upgrade locations from magnetic stripe. There are even some hybrid cards that contain a microchip, magnetic stripe, bar code, optical code, picture and signature panel all in one card.

1.7 Classification of Smart card

1.7.1 Memory Card

Memory cards simply store data. They do not have any processing capability and can be viewed as a small floppy disk with optional security. The main storage area in such cards is normally EEPROM (Electrically Erasable Programmable Read-Only Memory), which - subject to defined security constraints - can have its content updated, and which retains current contents when external power is removed. Memory cards can be either memory only or can have security logic using passwords and pin codes. Memory cards can hold from 103 bits to 16,000 bits of data, but have no processor on the card with which to manipulate that data. Memory cards are further divided into 2:-

Straight memory cards:

These cards just store data and have no data processing capabilities. They should be regarded as floppy disks of varying sizes without the lock mechanism.

Protected/Segmented memory cards:

These cards have built-in logic to control the access to the memory of the card. Sometimes referred to as intelligent memory cards these devices can be set to write protect some or the entire memory array. Some of these cards can be configured to restrict access to both reading and writing. This is usually done through a password or system key. Segmented memory cards can be divided into logical sections for planned multi-functionality.

Stored value memory cards:

These cards are designed for the specific purpose of storing value or tokens. The cards are either disposable or rechargeable. Most cards of this type incorporate permanent security measures at the point of manufacture. These measures can include password keys and logic that are hard-coded into the chip by the manufacturer. For simple applications such as a

telephone card the chip has 60 or 12 memory cells, one for each telephone unit. A memory cell is cleared each time a telephone unit is used. Once all the memory units are used, the card becomes useless and is thrown away. This process can be reversed in the case of rechargeable cards.

1.7.2 Microprocessor Smart Card

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, card operating system (COS) and hard disk with built-in security features. These cards have on-card dynamic data processing capabilities. Within the card is a microprocessor or microcontroller chip that manages this memory allocation and file access This type of chip is similar to those found inside all personal computers and when implanted in a smart card, manages data in organized file structures, via a card operating system this software controls access to the on- card user memory. Their data storage capacity ranges from 300 bytes to 32,000 bytes with larger sizes expected with semiconductor technology advances. The current generation of chip cards has an eight-bit processor, 16KB read-only memory, and 512 bytes of random-access memory.

1.7.3 Optical Memory Card

Optical memory cards look like a card with a piece of a CD glued on top, which is basically what they are. Optical memory cards can store up to 4 MB of data. These cards can carry many megabytes of data, but the cards can only be written once and never erased with today's technology. Thus, this type of card is ideal for record keeping for example medical files, driving records, or travel histories.

1.8 Steps for the Smart Cards Transaction

Step 1: Connection

In a smart card system for contact cards, the card is inserted in a reader device. Contactless cards need only be passed near a target.

Step 2: Authentication of the card

The card generates a message to the reader, which confirms that it is a valid card. The message may be encrypted for security purposes. The reader can also check the card against a list of stolen cards and if necessary lock it so that it can no longer be used.

Step 3: Authentication of the reader

The reader sends a message to the card, which is checked against pre-programmed codes to establish if the reader is valid. If the card is not satisfied that the reader is valid, it can prevent the reader gaining access to the information held on the card.

Step 4: Selecting an application

A single smart card may support many different applications, which may be inter-related or quite distinct. The desired application can be selected by the cardholder, by a person with access to the reader, or chosen automatically by the reader or the card depending on the form of the initial authentication.

Step 5: Identifying security requirements

The card is able to define the security requirements for the selected application. The card can enforce different levels of security for different purposes or for different persons or organizations.

Step 6: Authenticating the card-holder

This can be done by either requiring the cardholder to enter a PIN (personal identification number) or some sort of biometric information (for example; fingerprints, retina scan or signature dynamics). The card keeps the relevant information to make a comparison in a secret area. It can make the comparison without divulging to the cardholder the data it holds for the authentication procedure.

Step 7: The transaction

The transaction is generated by manual entry or by an automated process. The card or reader checks and authorizes the transaction.

Step 8: Transaction record

The card generates a record of the transaction and transmits it electronically to the reader. The record may be used in another part of the system (for example; to allow the service provider to collect actual payment from a bank in a stored value application); by a third party to the transaction for other purposes (for example; collecting statistics); or as back up data storage in case the card is lost or damaged.

Step 9: Hard copy

A paper record (such as a receipt) can be generated by the reader for the cardholder or the service provider.

1.9 Access Control

- The smart card access control system covers file access mainly. Each file is attached by a header, which indicates the access conditions or requirements of the file and the current status as well.
- Levels of Access Conditions
  - Always (ALW): Access of the file can be performed without any restriction.
  - Cardholder verification 1 (CHV1): Access can only be possible when valid CHV1 value is presented.
  - Cardholder verification 2 (CHV2): Access can only be possible when valid CHV2 value is presented.
  - Administrative (ADM): Allocation of these levels and the respective requirements for their fulfillment are the responsibility of the appropriate administrative authority.
  - Never (NEV): Access of the file is forbidden.
  - Two counters have to be implemented for each of the cardholder verification numbers (CHVs), There are three states in the management of the PIN, which are described below.

1. PIN has been presented: Files or functions, which have PIN presentation as a pre-requisite or condition, can be carried out. Every time the PIN is presented correctly, the PIN counter will be reset to the maximum number of tries, three for example.

2. PIN has not been presented or was presented incorrectly: The PIN counter will be decremented by one after each incorrect PIN was presented. All the operations or instructions, which require PIN presentation, will be invalidated. If the PIN counter reaches zero, then the PIN will be blocked.

3. PIN is blocked: In this state, all the operations require PIN presentation and even the PIN presentation instruction itself is blocked. Unblock PIN instruction has to be carried out. If correct unblocking PIN is presented, the PIN counter will be reset to the maximum number of tries and backed to the first state. However, if invalid unblocking PIN is presented, the unblock PIN counter will be decremented by one and when this counter reaches zero, the PIN can never be unblocked again.

1.10 Advantages

1. Larger memory.
2. High levels of security
3. Reduced fraud
4. Organized information
5. Reliability
6. Upper management information
7. Information Security
8. Ease of use without need for connections online or via telephone
9. User comfort

1.11 Disadvantage

1. Discomfort to retrieve information from a stolen card.

2. Bank fees associated with credit card.

1.12 Application of Smart card

1. Financial Application
2. Telephone Payment Card
3. Government Application
4. Health Application
8. Information Security
9. Communication and Entertainment

1.13 Conclusion

Smart card is an excellent technology to secure storage and authentication. If an organization can deploy this technology selecting the right type of solutions which is cross platform compatible and supports the standards required, it would be economical as well as secure. This technology has to be standardized and used in various applications in an organization not just for physical access or information access.

.