CHAPTER 5
SMART CARD TECHNOLOGY

5.1 INTRODUCTION

Today's society is often illustrated as an information society. Technological developments, particularly in the areas of computers and telecommunications have fundamentally changed the nature of the modern organization. In the world of information technology, smart card is one of the latest add-ons.

5.1.1 Smart Card

A smart card, a type of chip card, is a plastic card that contains an embedded computer chip—either a memory or microprocessor type—that stores and transacts data. This data is usually associated with either value, information, or both and is stored and processed within the card's chip. The card data is transacted via a reader that is part of a computing system. Systems that are enhanced with smart cards are in use today throughout several key applications, including healthcare, banking, entertainment, and transportation. All applications can benefit from the added features and security that smart card provides.

5.1.2 Need for Smart Cards

Smart cards improve the convenience and security of any transaction and provide tamper-proof storage of user and account identity.
Smart card systems have proven to be most reliable than other machine-readable cards, like magnetic stripe and barcode, with many studies showing card read life and reader life improvements demonstrating much lower cost of system maintenance. Smart cards also provide vital components of system security for the exchange of data throughout virtually any type of network. They protect against a full range of security threats, from careless storage of user passwords to sophisticated system hacks (Ferrari 1998).

5.1.3 Working Principles of Smart Cards

A smart card contains more information than a magnetic stripe card and it can be programmed for different applications. Some cards contain programming and data to support multiple applications and some can be updated to add new applications after they are issued. Smart cards can be designed to be inserted into a slot and read by a special reader or to be read at a distance, such as at a toll booth.

To access the information stored in the smart card we require a Smart Card Reader. Smart card readers are the necessary interface between smart cards and information systems. They can be connected to PCs via serial or USB ports, integrated into computer keyboards, and now they can be integrated into laptops.

5.2 COMMUNICATION WITH THE OUTSIDE WORLD

A Smart Card and a Card Accepting Device (CAD) communicate via means of small data packets called APDUs (Application Protocol Data Units) illustrated in Fig.5.1. The following characteristics of interaction make it harder for third parties to attack the system successfully:
- Small bit rate (9600 bits per second) using a serial bi-directional transmission line (ISO standard 7816/3), half duplex mode for sending the information (data only travels in one direction at a time).

- The communication follows a sophisticated protocol, described below. However, every external device communicating with the card makes it more vulnerable to attack via the communication link.

![Communication Protocol](image)

Figure 5.1 APDU Protocol

The Smart Card and CAD use an mutual active authentication protocol to identify each other. The card generates a random number and sends it to CAD, which encrypt the number with a shared encryption key before returning it to the card. The card then compares the returned result with its own encryption. The pair may then perform the operation in reverse.

The Smart card receives commands from the reader, interprets the commands, executes them and sends the responses. The basic unit is used for the command and response transmission is known as Application Protocol Data Unit (APDU).
5.2.1 APDU Structure

Commands and responses are transferred in form of an APDU structure. The APDU is used for transfer of the command is known as command APDU, while APDU used for sending the response is known as response APDU.

5.3 COMMUNICATION MODES

There are two modes of communication between the reader and the card: contact mode and contactless mode.

5.3.1 Contact Mode

In the contact mode, the communication takes place through electrical connections between the reader and the smart card. T=0 and T=1 are the protocols used for the contact communication as defined in ISO 7816-3.

T=0 is a byte oriented, half duplex protocol, i.e., at one time either the card or the reader can transmit signals. When a reader sends the command then the card is in the receive mode. When the card sends the response the card is in the receive mode. Since this is byte oriented protocol, command and response APDUs are transferred using communication handshake for each byte.

T=1 is a block oriented communication protocol. At a time only one party can be in the sending mode and other one will be in the reception mode. The command and response APDUs are transferred using blocks. Some kinds of additional blocks are used for acknowledging the previously sent blocks and to control information exchange between the reader and the card. These additionally supported blocks apart from the blocks for APDUs transfer provide reliability in the communication.
5.3.2 Contactless Mode

In the contact-less mode, the card is not in physical contact with the reader and RF field is used for communication. The card generates power using this RF field. The same RF field is also used for exchange of APDUs between the card and the reader. This protocol is also half-duplex block oriented protocol.

5.4 TYPES OF CARDS

Before implementing the Smart Card, it is necessary to understand the significance and potentiality of Smart Cards, also necessary to put the technology into contest. There are different technologies available for this purpose. In fact, there are five types of Smart Cards.

1. Memory Cards
2. Processor Cards
3. Electronic Purse Cards
4. Security Cards
5. Java Cards

There are different types of plastic cards that fall under the umbrella of “Advanced Card Technologies”.

5.4.1 Embossed Plastic Card

The embossed plastic card can be understood from a visual inspection. The issuer is identified through the print and card colour. The embossed lettering usually shows the name of the holder along with other significant data such as identification or account number. Transfer of
information via embossing may seem primitive but the simplicity of the system has made worldwide proliferation possible. There is a signature style on the back of this plastic card which shows a typical signature of the cardholder to allow the personal identification.

5.4.2 Magnetic Strip Card

The main advantage of magnetic technology over embossing is reduction of paper documents. The magnetic Stripe Card can store up to 245 characters of information. The magnetic strip is divided into three parts according to international standard (parts 2, 4 and 5 of ISO7811) each of which has been designed for different applications. One of the tracks is designated a read and write track, with updated appropriate terminal equipment. The magnetic strip card has proven to be exceedingly successful over the years.
5.4.3 Memory Card

The memory Card is more advanced which has a microchip or integrated circuit with fixed memory functions, but no processing power. Memory Cards are less expensive and less functional than Micro Processor Card. They contain EEPROM and ROM, as well as some address and security logic. Typical Memory Card Applications are pre-paid telephone cards and health insurance cards.

5.4.4 Smart Cards

Integrated Circuit Cards are known as Smart Cards. These cards follow the ISO 7816 Series Standard. The importance of this Stored Card is to protect against unauthorized access and tampering. Memory functions such as reading, writing and deleting can be linked to specific conditions, controlled by both hardware and software.

Smart Card may be equipped with three types of memory depending upon the usage.

**Read Only Memory (ROM)** - Non-volatile memory containing information loaded at the manufacturing stage, which cannot be altered.

**Random Access Memory (RAM)** - Volatile memory, which retains its contents only while power, is applied.
Programmable Read Only Memory (PROM) - Non-volatile memory, the contents of which can be programmed depending upon the usage.

5.4.5 Memory Cards

Memory card contain EEPROM and ROM memory, as well as some address and security logic, exists to prevent writing and erasing of the data. Complex designs allow for memory read access to be restricted. Example: pre-paid telephone cards and health insurance cards.

5.4.6 Microprocessor Card

Microprocessor Card is the most secure type card. It has a built-in Operating System in its microprocessor. The Central Processing Unit (CPU) uses RAM as its working memory and the data is stored in EEPROM, size in modern cards varies from 1 KB to 1 MB and constitutes a dominating factor specifying the card capabilities. It has the capability to perform independent calculations and therefore it can store several applications. The card can be used in various areas, e.g. banking payment systems, Motor Insurance, Health Insurance, transportation systems, etc.

5.4.7 Cryptographic Coprocessor Card

Technically, these cards are in the category of microprocessor card. They are different from other type card because of the functionality. A cryptographic coprocessor is a hardware module, which includes a processor and the same is used for encryption and related processing. These cards are programmed with various security features to prevent unauthorized retrieval of data.
5.4.8 Contact Smart Card

Contact smart card is embedded with a single integrated circuit chip that contains memory or memory plus a microprocessor. The microprocessor is less expensive and they offer less security. The microprocessor contains an "intelligent" controller used to securely add, delete, change, and update information contained in memory. This type of card is used in a wide variety of applications including network security, vending, meal plans, loyalty, electronic cash, government IDs, campus IDs, e-commerce, health cards, and many more.

5.4.9 Contactless Smart Card

Unlike Contact Smart Card, contactless smart cards contain an embedded antenna attached to the chip for reading and writing information contained in the chip's memory. They need only be passed within range of a radio frequency acceptor to read and store information in the chip. The range of operation varies from 2.5" to 3.9" (63.5mm to 99.06mm) depending on the acceptor. This type of card is in a wide variety of application like student identification, electronic passport, vending, parking, tolls, etc.
5.4.10 Proximity Cards (Prox Card)

Like Contactless cards, Proximity cards communicate through an antenna. They have a greater range of operation. The range of operation for proximity cards varies from 2.5” to 20” (63.5mm to 508mm) depending on the reader. A small amount of information can be read with prox cards such as an identification code that is usually verified by a remote computer; but the disadvantage is that the information cannot be written back. These cards are used where fast, hands-free operation is preferred.

5.4.11 Hybrid Cards

Hybrid card is the combination of two or more embedded chip technologies such as a contactless smart chip with its antenna, a contact smart chip with its contact pads, and/or a proximity chip with its antenna -- all in a single card. The contactless chip is used for fast transaction times and/or mass transit application. The contact chip can be used for higher levels of security applications. The individual electronic components are not connected to each other even though they share space in a single card.
5.4.12 Combi Cards

The combi card have one smart chip embedded in the card that can be accessed through either contact pads or an embedded antenna. This card provides ease-of-use and high security in a single card product. These types of cards can be applied in the areas of mass transit applications.

5.4.13 Optical Memory Card

These cards can store more megabytes of data, but the disadvantage with these type cards is that it can only be written once and never erased with today’s technology. The devices used for reading and writing are very expensive but these can be applied in the areas like health care where large amounts of data must be stored.
5.4.14 Java Card

Java Card is a smart card that is capable of running Java byte codes so that cards become more powerful and the same card will be able to run some of the applications as a user run on his/her personal computer. Java Card was introduced by Schlumberger and submitted as a standard by JavaSoft recently. Schlumberger has the only Java card on the market currently and the company is the first Java Card licensee. As a smart card with the potential to set the overall smart card standard, Java Card is comprised of standard classes and APIs that let Java applets run directly on a standard ISO 7816 compliant card. Java Cards enable secure and chip independent execution of different applications.

5.4.15 Smart Card Market

According to “The Freedonia Group Inc.”, Cleveland, global demand for smart cards is projected to increase 11% each year through 2006 for a total market value of $58 billion, an improvement over a sluggish early 2000 for the smart card market illustrated in Figure 5.2 and Figure 5.3.

A new report “World Smart Card” published by the same group mentioned that smart card issue is expected to double to almost four billion units over the next few years.
Figure 5.2 World Smart Card Demand by Region

Figure 5.3 World Smart card demand by application
5.5 MEMORY MANAGEMENT

This thesis refers to the Advanced Card System (ACOS 3) smart card. The 16KB EEPROM (Electrically Erasable Programmable Read Only Memory) memory area provided by the card chip is basically segregated into Internal Data Memory and User Data Memory.

- The Internal Data memory is used for the storage of configuration data and is used by the card operating system to manage certain functions.
- The User Data memory stores the data manipulated in the normal use of the card under control of the application.

5.5.1 Data Files

Access to both the Internal Data Memory area and the User Data Memory area is possible within the scope of data files and data records. Data files in the Internal Data Memory are referred to as Internal Data Files. Data files in the User Data Memory are called User Data Files given in Figure 5.4.

Data Files are the smallest entity to which individual security attribute can be assigned to control the read and write access to the data stored in the EEPROM.
Data Files are composed of Data records. A Data record is the smallest data unit that can individually be addressed in a Data File. Each Data File contains N Data records. The record number must be specified when a record is read from or written to a file. A Data File can contain up to 255 records. The record length can be different for different files but is always fixed within a file.

5.5.2 User Data File

User data files are allocated in the personalization stage of the card life cycle. The data stored in a User Data File can be read through the READ RECORD Command and updated through the WRITE RECORD command. A User Data File can contain up to 255 records of 255 bytes record length each. User will be able to access these records as long as it fits the 16KB capacity of the card.

5.6 DATA FILE ACCESS

The process of Data File access is identical for Internal Data File and for User Data File.

5.6.1 Select File

The SELECT FILE command can be executed any time. If the specified file does not exist the card returns an error code and does not change the status of currently selected file.
To select a data file for subsequent READ RECORD and WRITE RECORD commands.

**Command:**

<table>
<thead>
<tr>
<th>CLA</th>
<th>INS</th>
<th>P1</th>
<th>P2</th>
<th>P3</th>
<th>DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>A4</td>
<td>00</td>
<td>00</td>
<td>02</td>
<td>File ID</td>
</tr>
</tbody>
</table>

**Response**

<table>
<thead>
<tr>
<th>SW1</th>
<th>SW2</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>6A</td>
<td>82</td>
<td>File does not exist</td>
</tr>
<tr>
<td>90</td>
<td>00</td>
<td>Internal data file has been selected</td>
</tr>
<tr>
<td>91</td>
<td>nn</td>
<td>User data file has been selected</td>
</tr>
</tbody>
</table>

The SELECT FILE command is carried out as follows:

<table>
<thead>
<tr>
<th>Card Accepting Device</th>
<th>Command/Response</th>
<th>Card</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SELECT FILE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OK / Error</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Check whether file exist</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Close Currently Selected file</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select New File</td>
<td></td>
</tr>
</tbody>
</table>
The following code is used for selecting the file.

' Select User File
Call SelectFile(HiAddr, LoAddr)

If retcode <> ModWinsCard.SCARD_S_SUCCESS Then

   Exit Sub

End If

'Function call for Select File
Private Function SelectFile(ByVal HiAddr As Byte, ByVal LoAddr As Byte) As Long

   Dim indx As Integer
   Dim tmpStr As String
   apdu.Data = array
   Call ClearBuffers()
   apdu.bCLA = &H80        ' CLA
   apdu.bINS = &HA4        ' INS
   apdu.bP1 = &H0          ' P1
   apdu.bP2 = &H0          ' P2
   apdu.bP3 = &H2          ' P3
   apdu.Data(0) = HiAddr      ' Value of High Byte
   apdu.Data(1) = LoAddr      ' Value of Low Byte
   apdu.IsSend = True
   Call PerformTransmitAPDU(apdu)

   End Function
5.6.2  Read Record

The READ RECORD command can be executed once a file has been selected through the SELECT FILE command is illustrated in Figure 5.5.

Data from only one record can be read in each READ RECORD operation. The number of bytes to be read is specified in the command. The maximum number of bytes to be read is equal to the record length. If the number of bytes read is smaller than the record length, the first N bytes of record returned by the card.

To read a number of bytes up to the record length from one record in the currently selected file.
Command

<table>
<thead>
<tr>
<th>CLA</th>
<th>INS</th>
<th>P1</th>
<th>P2</th>
<th>P3</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>B2</td>
<td>Record Number</td>
<td>00</td>
<td>LEN</td>
</tr>
</tbody>
</table>

Response

<table>
<thead>
<tr>
<th>Data</th>
<th>SW1</th>
<th>SW2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 1 .. Byte N</td>
<td></td>
<td>Status</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SW1</th>
<th>SW2</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>6A</td>
<td>83</td>
<td>Record not found - File too Short</td>
</tr>
<tr>
<td>67</td>
<td>00</td>
<td>Specified length is larger than record length</td>
</tr>
<tr>
<td>69</td>
<td>85</td>
<td>No File selected</td>
</tr>
<tr>
<td>6F</td>
<td>00</td>
<td>I/O error, data to be accessed resides in invalid address</td>
</tr>
</tbody>
</table>

The READ RECORD command is carried out as follows:

Card Accepting Device | Command/Response | Card |
----------------------|------------------|------|
WRITE RECORD          | Record No., Data | Check file access condition |
|                      | OK/Error         | Check file record length    |
|                      |                  | WriteRecord Data            |
The following code is used to read record:

Call readRecord(rec, dataLen)

If retcode <> ModWinsCard.SCARD_S_SUCCESS Then

    Exit Sub

End If

' Display data read from card to textbox

tmpStr = 

indx = 0

While (RecvBuff(indx) <> &H0)

    If indx < txtData.MaxLength Then

        tmpStr = tmpStr & Chr(RecvBuff(indx))

    End If

    indx = indx + 1

End While
5.6.3 Write Record

The WRITE RECORD command can be executed one time in a file has been selected through the SELECT FILE command is illustrated in Figure 5.6.

Data can be written to only one record in each WRITE RECORD operation. The number of bytes to be written in the record is specified in the command. The maximum number of bytes to be written is equal to the record length. If the number of bytes to be written is smaller than the record length, the first N bytes of record are overwritten with the new data. The remaining bytes in the record are not modified.
To write a number of bytes up to the record length to one record in the currently selected file.

**Command**

<table>
<thead>
<tr>
<th>CLA</th>
<th>INS</th>
<th>P1</th>
<th>P2</th>
<th>P3</th>
<th>DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>D2</td>
<td>Rec. No</td>
<td>00</td>
<td>Len</td>
<td>Byte 1.. Byte N</td>
</tr>
</tbody>
</table>

**Response**

<table>
<thead>
<tr>
<th>SW1</th>
<th>SW2</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>6A</td>
<td>83</td>
<td>Record not found - File too Short</td>
</tr>
<tr>
<td>67</td>
<td>00</td>
<td>Specified length is larger than record length</td>
</tr>
<tr>
<td>69</td>
<td>85</td>
<td>No File selected</td>
</tr>
<tr>
<td>6F</td>
<td>00</td>
<td>I/O error, data to be accessed resides in invalid address</td>
</tr>
</tbody>
</table>

The WRITE RECORD command is carried out as follows:

<table>
<thead>
<tr>
<th>Card Accepting Device</th>
<th>Command/Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>WRITE RECORD</td>
<td>Check file access condition</td>
</tr>
<tr>
<td>Record No., Data</td>
<td>Check file record length</td>
</tr>
<tr>
<td>OK/Error</td>
<td>WriteRecord Data</td>
</tr>
</tbody>
</table>
Write data from text box to card

tmpStr = txtData.Text

For indx = 0 To Len(tmpStr) - 1
    tmpArray(indx) = Asc(Mid(tmpStr, indx + 1, 1))
Next indx

Call writeRecord(1, rec, dataLen, Len(tmpStr), tmpArray)

If retcode <> ModWinsCard.SCARD_S_SUCCESS Then
    Exit Sub
End If

lstOutput.Items.Add("Data read from Text Box is written to card.")

lstOutput.SelectedIndex = lstOutput.Items.Count - 1

End Sub
5.7 SUMMARY

This chapter presented the basics of smart card technology. It discussed about the various types of smart cards. This thesis exploits Advanced Card System ACOS 3 Smart card. It presents how the memory is segregated into Internal Data Memory and User Data memory. It also covered how the read and write operations are performed in the ACOS 3 smart card using ACR 38 Smart card Reader/Writer.