NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

SMART CARD TECHNOLOGY

Graduation Project
COM- 400

Student: Waleed Farouk Sheikho

Supervisor: Halil Adahan

Nicosia-2004

Acknowledgment

I would like to thank Allah Almighty for enabling me to finalize this project work and I never quit asking Him to utilize me to serve and avail the Islamic nation and the entire Muslims all over the world with what I learn. Amen.

Moreover, I would never have been able to undertake this research project without the assistance of the person I trust, the one who was a friend, a teacher, an instructor, and a brother most of the time, Mr. Halil Adahan so a million thanks go to him, I will always remember him.

He answered me with satisfactorily details and with informative views about the matters whenever and wherever I needed to listen to something from someone about. So hats off again and again to the person most knowledgeable I have loved being taught by him.

I would also like to express my gratitude to the dean of the Engineering department at the NEU for he takes the efforts to create a stable educational environment enables the learners to get what knowledge and information they seek.

Additionally, I am also extremely grateful to my brother Nabeel who stepped in at the last hour as a proxy secondary supervisor and provided me with useful advices and references when it was required. Special thanks again Nabeel, with you I have had many in-depth discussions, regarding computing, my future, and other interesting topics.

Likewise, I never forget to show my appreciation and be thankful to my parents for enduring sacrifices which were necessary in the name of growing up, rising, and supporting their son to become a person honors the responsibility and does his tasks the best way it could be. That's too much! I love you both.

Left to mention at this piece, is my declaration that this document does not incorporate without acknowledgment any material previously submitted for a degree or a diploma in any university; and to the best of my knowledge it does not contain any materials previously published or written by another person except where due reference is made.

Abstract

The smart card is a device that can store and process considerable amounts of information. Most smart cards contain a microchip, which can hold detailed information associated with you such as your name, age, address and even your social security details (if a multipurpose one). Information on the chip can be "locked" with a PIN number, and protected through a range of encryption methods.

The microchip is segmented allowing data in each segment of the chip to be processed independently. One segment of the chip may contain police records that can only be accessed by the police department; the other segment may contain medical records for hospital to access, thus making it very difficult to forge as every separate piece of information on the card could only be accessed by that department.

A smart card resembles a credit card in terms of physical looks and size. The size of the card is determined by the international standard (ISO 7810). The ISO 7816 standard also defines the physical characteristics of the plastic, including the temperature range and flexibility, position of the electrical contacts and how the microchip communicates with the outside world. A smart card is a portable, secure (based on cryptography), intelligent and cheap way of manipulating and storing data.

Smart cards come in two varieties: memory cards and microprocessor cards. Memory cards simply store data. They can hold information thousands times greater than a magnetic stripe card; however its functionality is limited to basic applications such as phone cards.

A microprocessor card offers multiple functions such as encryption, advanced security mechanism, complex calculations, to add, delete and manipulate information in its memory etc. Today billions of smart cards are already in use of which most are memory cards.

Smart cards have existed in varies form back in 1974. Since then, with the motivated companies like Gemplus and Schlumberger, smart cards have received a great amount of attention in the control device market. According to the consulting firm Frost & Sullivan, more than 600 million smart cards were issued in 1996 and the market is expected to consume more than 21 billion smart cards in 2010. Such a rapid growth of 240% per year! will appeal to developers to focus on new applications and more trusty developments to make extremely huge profits.

Table of Contents

List of Abbreviations

IC	Integrated Circuits
ICC	Integrated Circuit Chip
COS	Card Operating System
LAN	Local Area Networks
PKI	Public Key Infrastructure
IATA	International Air Transportation Association
SCOS	Smart Card Operating System
ISO	International Organization for Standardization
EMV	Euro pay, MasterCard, and Visa
MULTOS	Multi-application Operating System
GSA	General Services Administration
GSM	Global System for Mobile Communications
EMEA	Europe, Middle East and Africa
PIN	Personal Identification Numbers
CPU	Central Processing Unit
RAM	Read Only Memory
ROM	Read Only memory
EEPROM	Electrically Erasable Programmable Read Only Memory
BIOS	Basic Input/Output System
DRAM	Dynamic RAM
FRAM	Ferroelectric RAM
SRAM	Static RAM
PDA	Personal Digital Assistant
CAD	Card Acceptance Device
I/O	Input/Output
RF	Radio Frequency
WORM	Write-Once/Read-Many
IEC	International Electro-technical Commission
WHQL	Windows Hardware Quality Labs
APDU	Application Protocol Data Units
VM	Virtual Machine
MEL	MULTOS Executable Language

CA	Certification Authority
ATR	Answer-To-Reset
API	Application Programming Interface
AAM	Application Abstract Machine
RISC	Reduced Instruction Set Computer
TLV	Tag Length Values
JCRE	Java Card Runtime Environment
AID	Applet Identifier
DPA	Differential Power Analysis
HO-DPA	High Order Differential Power Analysis
PGP	Pretty Good Privacy
DES	Data Encryption Standard
ANSI	American National Standards Institute
DEA	Data Encryption Algorithm
MAC	Message Authentication Code
SHA-1	Secure Hash Algorithm
DSA	Digital Signature Algorithm
SSL	Secure Sockets Layer
POS	Point-of-Sale
CCD	Charge-Coupled Device
DC	Direct Current
AC	Alternating Current
EDS	Electrostatic Discharge
IVR	Interactive Voice Response
DSV	Dynamic Signature Verification
FMR	False Match Rate
FAR	False Acceptance Rate
FNMR	False Non-Match Rate
FRR	False Rejection Rate
SIM	Subscriber Identity Modules
CA	Conditional Access
WAP	Wireless Application Protocol
HTML	Hypertext Markup Language

WML	Wireless Markup Language
TTP	Trusted Third Party
RFID	Radio Frequency Identification
HSPC	Hong Kong Shanghai Banking Corporation
IBM	International Business Machines Corporation

Appendix A- List of Figures

Introdu[illegible]

The [illegible] and shape to [illegible] two comp[illegible] card, [illegible] otherwise [illegible] pre-paid [illegible]

Smart [illegible] information [illegible] time of the [illegible]

A smart [illegible] (ICs) [illegible] technology [illegible] frequency [illegible] identification [illegible] microcontr[illegible] to complete [illegible]

The [illegible] communication [illegible] applications [illegible] appropriate [illegible] record, [illegible] interoperability [illegible] with a single [illegible]

Smart card [illegible] interoperability [illegible] data manag[illegible]

Introduction

The smart card that is described in this project work is a plastic card equal in size and shape to a credit card that contains an integrated microprocessor and memory. These two components allow the storing and processing of information in the card. A smart card, embedded with a microprocessor and a memory chip, can add, delete, and otherwise manipulate information on the card, while a memory-chip card (for example, pre-paid phone cards) can only undertake a pre-defined operation.

Smart cards, unlike magnetic stripe cards, can carry all necessary functions and information on the card. Therefore, they do not require access to remote databases at the time of the transaction.

A smart card is a credit card-sized device that contains one or more integrated circuits (ICs) and also may employ one or more of the following machine-readable technologies: magnetic stripe, bar code (linear or two-dimensional), contactless radio frequency transmitters, biometric information, encryption and authentication, or photo identification. The integrated circuit chip (ICC) embedded in the smart card can act as a microcontroller or computer. Data are stored in the chip's memory and can be accessed to complete various processing applications.

The memory also contains the microcontroller chip operating system (COS), communications software, and can also contain encryption algorithms to make the application software and data unreadable. When used in conjunction with the appropriate applications, smart cards can provide enhanced security and the ability to record, store, and update data. When implemented properly, they can provide interoperability across services or agencies, and enable multiple applications or uses with a single card.

Smart card technology can enable an organization to become more secure, efficient, and interoperable while delivering strong authentication and security, identity management, data management, customer support, and communications.

The ICC, the technology on a card that makes it a “smart card,” provides a number of functions. The smart card interchanges data with the outside world in two ways, either through gold plated contacts placed on one side of the card which has to be inserted in a reader and this is called the contact cards, or when we don’t have physical contact with the reader. The communication here is based on radio signals, using an antenna embedded in the card which has to be placed in the proximity of a contactless reader. This type of card is called contactless.

CHAPTER ONE: SMART CARD INTRODUCTION AND OVERVIEW

1.1 Introduction

The smart card that is described in this project work is a plastic card equal in size and shape to a credit card that contains an integrated microprocessor and memory. These two components allow the storing and processing of information in the card. A smart card, embedded with a microprocessor and a memory chip, can add, delete, and otherwise manipulate information on the card, while a memory-chip card (for example, pre-paid phone cards) can only undertake a pre-defined operation.

Smart cards, unlike magnetic stripe cards, can carry all necessary functions and information on the card. Therefore, they do not require access to remote databases at the time of the transaction.

A smart card is a credit card-sized device that contains one or more integrated circuits (ICs) and also may employ one or more of the following machine-readable technologies: magnetic stripe, bar code (linear or two-dimensional), contactless radio frequency transmitters, biometric information, encryption and authentication, or photo identification. The integrated circuit chip (ICC) embedded in the smart card can act as a microcontroller or computer. Data are stored in the chip's memory and can be accessed to complete various processing applications.

The memory also contains the microcontroller chip operating system (COS), communications software, and can also contain encryption algorithms to make the application software and data unreadable. When used in conjunction with the appropriate applications, smart cards can provide enhanced security and the ability to record, store, and update data. When implemented properly, they can provide interoperability across services or agencies, and enable multiple applications or uses with a single card.

Smart card technology can enable an organization to become more secure, efficient, and interoperable while delivering strong authentication and security, identity management, data management, customer support, and communications.

The ICC, the technology on a card that makes it a "smart card," provides a number of functions. The smart card interchanges data with the outside world in two ways, either through gold plated contacts placed on one side of the card which has to be inserted in a reader and this is called the contact cards, or when we don't have physical contact with the reader. The communication here is based on radio signals, using an antenna embedded in the card which has to be placed in the proximity of a contactless reader. This type of card is called contactless.

There are no batteries in a smart card; the power is provided from outside by the reader, be it contact or contactless. The CPU clocking also comes from the reader.

The memory is Electrical Erasable Programmable Read Only Memory double-EPROM, which will retain the contents even if there is no voltage applied. Some cards have only memory; an application can increase or decrease counters in the card. These IC memory cards can hold up to 1-4 KB of data, but have no processor on the card with which to manipulate that data. Thus, they are dependent on the card reader for their processing and are suitable for uses where the card performs a fixed operation. Memory cards represent the bulk of the 600 million smart cards sold last year, primarily for pre-paid, disposable-card applications like pre-paid phone cards. Memory cards are popular as high-security alternatives to magnetic stripe cards, later on this document a section was assigned to explain what a magnetic stripe card is and how it works.

Only those cards with chips that contain certain microprocessor logic are called smart cards. The two main characteristics of a smart card are its security and mobility. Since its mobility characteristic is obvious, I have concentrated on its security features. And this is obvious through assigning the third section of this project work to describe the security features of smart cards. Almost all the applications that use a smart card are based on the fact that it is very difficult to forge and to fake the card or to access protected data on the card. If for some reason or other the security of the smart card could be compromised, it would be almost impossible to justify its use.

The combination of smart card technology with web-based applications, electronic commerce, and other business uses of the Internet can improve the quality of life for citizens and employees.

The wide application fields of smartcards where discussed with rich amount of information and remarkable facts in the third section of this document, and this is because it is important to mention that government, financial services, transportation, telecommunications, healthcare, education, retail, and many other industries are planning to or already using smart cards as a means of providing better security and improved services to its customers and users.

Left to say in this introduction of this project work, the smart card technology provides a toolbox of enhanced capabilities that can be used to implement a smart identification card, including functions, such as:

1. **Access Control Tool:** Smart cards can provide significantly enhanced security features that allow the card to operate as an authentication token for secure logical access to terminals and networks, such as local area networks (LANs) and the Internet, as well as for physical access to buildings, rooms, parking lots, transit and other facilities.

2. **Payment Tools:** Smart cards can serve as credit, debit, or stored-value payment and/or payment token instruments and provide the capability to access financial accounts and transfer funds between accounts.

3. **Information Storage and Management Tools:** Depending upon the size of the ICC, smart cards can store and manage data to assist with various applications. For example, medical information stored on a smart card can be accessed by an authorized medical official in the event of an emergency or on a routine medical visit. On-card information availability can reduce the amount of time spent locating hard-copy paperwork. If the medical event were a life-threatening emergency, the information would be immediately accessible, possibly saving critical time.

4. **Enhanced Secure Access Capabilities:** The use of sophisticated technologies such as biometrics and Public Key Infrastructure (PKI) further enhances the security of identity verification in granting physical and logical access. PKI uses public and private keys for digital signatures and email encryption and decryption.

If the digital signature is verified using the signer's public key, then the recipient knows that it was signed by the owner of the public/private key pair and that it has not been changed in any way since it was signed. This assures both the sender and recipient that the information has not been altered. Biometrics use physical characteristics (e.g., fingerprint, hand geometry, iris scan and voice/facial recognition) to authenticate an individual's identity. PKI and/or biometrics can be used to more accurately identify an individual.

1.2 The Evolution of Smart Cards

Smart card technology has been around for the last few decades. It essentially evolved from the financial community's desire to replace older, less efficient transaction means. For example, the credit card evolved as an alternative to the small loan. Now it appears the smart card may become the replacement for traditional paper checks and currency.

The driving factors of the growing interest in smart cards include the declining cost of smart cards and the growing concern that magnetic stripe cards can not provide the protections necessary to thwart fraud and security breaches. This security issue alone may propel smart card technology to the forefront of business transactions.

1.2.1 History of Smart Cards

The ancestor of data storage cards is most probably the calling card. The first plastic based card was issued by Diners Club in 1950. By the end of the fifties two other firms joined the initiation: American Express and Carte Blanche. The first *credit card* was issued by the Bank of America; this is what became VISA later on. Interbank launched another system called MasterCard. However, these early cards were only capable of 'storing' embossed identification items (names, numbers, codes etc).

The first cards with magnetic stripes were developed by the International Air Transportation Association (IATA) in the 1970's. On this type of card the magnetic stripe stored 210 bit/inch of information, which means about 80 alphanumeric (7-bit) characters.

(For the sake of compatibility, today's magnetic stripes are divided into three regions. The first region corresponds to the original stripe, storing read-only information.

The second region can hold additional 40 digits with an information density of 75 bit/inch. The third region is read-writeable and may contain 107 digits.) A much higher amount of data can be stored on Optical cards. An optical memory card looks 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. But once written, the data cannot be changed or removed. Thus, this type of card is ideal for record keeping. Optical cards are used mainly in the medical sector where storage of the patient's medical records and perhaps even of X-ray photographs is needed other usages is to store files of driving records, or travel histories.

These cards have no processor in them; both reading and writing (and positioning of course as well) are done optically, enabling a higher level of precision and thus higher information density. Also, typically the whole surface of the card is used for holding data. This way, capacity of some megabytes can be achieved. On the other hand, manufacturing costs of such cards are quite high.

The next step in the evolution of cards was the appearance of chipcards i.e. cards based on the application of microelectronic circuits. The first attempts toward chipcard technology are marked by the establishment of Innovatron in 1974. Bull produced its first card possessing a microprocessor in 1979. On this card, the processor was in a separate chip, which proved to be an insecure solution. However, it was only in the 1980's that the improvement of the technology made it possible to integrate all circuits on a single chip. In France for instance, chipcards are used since 1986 in public payphones.

Of course the improvement did not stop since then. The first chipcards were memory cards. They contained only memory modules which were controlled by the contacts. Generic cards were chipcards too. They received instructions from the outside which were processed by the card's operating system.

Nowadays chipcards possess more and more memory and computation power. This makes it possible that the cards not only execute commands from the outside but also be able to run separate programs.

These are **programmable smart cards**. They introduce the concept of a possibly multitasking, multithreaded, multi-user smart card operating system (SCOS). This way, access to the data stored on the card is controlled by the card itself. Thus, the smart card itself can guarantee for security, instead of delegating this responsibility to the possibly entrusted terminal.

Generally, it is said that a number of parallel trends occurring in computing, microelectronics, cryptography and financial services in the early 1960s acted as the catalysts to the emergence of Smart Cards. When mentioning persons credit is given to Arimura in Japan in the beginning of the 1970s and Roland Moreno of France in the period 1973-74 for introduction of smart cards. However, Jurgen Dethloff tables details of his own work in the late 1960s when an outlook is taken by people concerned.

When some leading corporations became involved in a Smart Card project in 1981 they investigated prior patents that had been published. It was found that Ellingboe (Ellingboe Jules K, 1967) had filed a patent application in October 1967 which was abandoned and refilled in 1970. It covered not merely the contact Smart Card essentially as we know it now, but also a contactless card with inductive or capacitive coupling to a reader.

The first cards originated as embossed and magnetic stripe cards suitable for both eyeball reading and magnetic readers. The standard dimensions originated with International Air Transportation Association (IATA) and led to the International Organization for Standardization (ISO) a standard on magnetic stripe cards for identification.

Before very long a wide variety of card shaped products using other technologies than magnetic recording began to appear. In the late 1960s there were products available which contained coded conductor tracks. Some came from the British company Counting Instruments Ltd of Borehamwood and were utilized by the Post Office and other organizations with large fleets of vans and Lorries.

The system enabled authorized drivers to collect petrol and other fuel for their vehicles. Other trends in the 1960s that helped make Smart Cards feasible were the miniaturization of electronic calculators and the reduction in the size and complexity of integrated circuit semiconductor memory to the point where it was small enough and cheap enough to be incorporated in a bank card.

Having set the scene as a nascent technology the stage was ripe to move from the invention phase to overcome the perceived barriers to introduce true Smart Card products. These barriers were perceived as: Agreement on international standards for Smart Cards, the reduced card cost, and the establishment of competitive advantage over existing and other new card storage media, e.g. optical recording.

IC contact cards, an original French invention, though still pretty much a cutting edge technology has been with us for well over 20 years. Since the 1970s, the history of smart cards has reflected steady advances in chip capabilities and capacity, as well as increases in the number and variety of applications.

1.2.2 Present Technology

In 1968, German inventors Jürgen Dethloff and Helmut Grötrupp applied for the first ICC-related patents. Similar applications followed in Japan in 1970 when Dr. Kunitaka Arimura filed the first and only patent on the smart card concept and in France in 1974 when Ronald Moreno filed the original patent for the IC card, later dubbed as the "smart card". In 1984, filed trials of ATM bank cards with chips were successfully conducted. By 1986, many millions of French telephone smart cards were in circulation. Their number reached nearly 60 million in 1990. In 1994, Europay, MasterCard, and Visa (EMV) published joint specifications for global microchip-based bank cards, and Germany began issuance of 80 million serial memory chip cards as citizen health cards. In 1995, over 3 million digital mobile phone subscribers worldwide began initiating and billing calls with smart cards. In 1996 over 1.5 million VisaCash stored value cards were issued for the Atlanta Olympics, MasterCard and Visa began sponsorship of competing consortia to work on solving the problems of smart card interoperability; two different card solutions were developed: the JaveCard backed by Visa, and the Multi-application Operating System (MULTOS) backed by MasterCard.

In September 1998, the U.S Government's General Services Administration and the United States Navy joined forces and implemented a nine-application smart card system and card management solution at the Smart Card Technology Center in Washington, DC. The Technology Centers primary purpose was to demonstrate and evaluate the integration of multi-application smart cards with other types of technology, showcasing systems available for use in the Federal Government. In the same year, Microsoft also announced its new Windows smart card operating system.

In 1999, The U.S Government's General Services Administration (GSA) has been involved in the Smart Access Common ID Project. This project aimed to establish a contract vehicle for use by all Federal agencies to acquire a standard, interoperable employee identification card, from one or more vendors, capable of providing both physical and logical (system/network) access to all Federal employees. The United States Government represented by the GSA began a true multi-application Java card pilot in Washington, DC, metropolitan area.

The Smart Card brings a variety of benefits to users. It provides security functions like encryption and electronic signatures, stores up to 100 or more times the information than typical magnetic strip cards, and reduces tampering and counterfeiting through high security mechanisms. It can also be disposable or reusable. Today, about 3 billion cards have been issued worldwide with 10% of them in the US.

Because of the size and shape of these devices, Smart Cards lend themselves to applications where personal identity, convenience, mobility and security are key factors. Smart Cards are used all over the world as personal identification cards for corporate building security systems and PC equipment access control. Smart Cards are also used as credit or debit cards. The use of a microprocessor chip enhances the level of automation and security, making credit or debit cards a Smart Card. In automating the transportation area, with billions of transport transactions occurring each day, Smart Cards have easily found a place in this rapidly growing market, such as mass transit ticketing, urban parking, electronic toll collection, and airline applications. Sometimes, Smart Cards are used in customer loyalty or retention-marketing programs, like a frequent flyer card that the end-user inserts into a machine before boarding a plane so frequent flyer miles are added to your frequent flyer Smart Card.

In Europe, Smart Cards are used as small-change debit cards at convenience stores and for phones systems. Currently, about 80 countries throughout the world use Smart Cards in payphones. The Global System for Mobile Communications (GSM) radiotelephone system originated in Europe. The system allows each national operator to keep control of the security and payment aspects, but at the same time facilitates cross border use of mobile phones. The GSM subscribers can insert a Smart Card into any GSM phone for personal use since secure data concerning the GSM subscription is held in the Smart Card, not in the telephone.

In Singapore, the Cash Card is a Smart Card that acts as an electronic purse; one that holds electronic money. In fact, it is replacing coins and bank notes for everyday purchases such as movies, parking, museums, gas, telephones, vending machines, retail outlets and fast food restaurants. The Cash Card is available in several different initial values of $20, $50, and $100 and can be reloaded.

In the US, Smart Cards are being used to increase the quality of service in healthcare and reducing its cost by improving the efficiency of handling medical and administrative information. They are useful in a wide range of situations in the medical field.

Smart cards are now becoming part of everyday life and are involved in everyday actions. This is because the features that make smart cards so appealing for application developers are their diminutive size, their ability to store data in a secure manner and to run small programs. Whereas originally used for banking and telecommunication applications, in the last few years we have come to use smart cards in a much broader sense; they have become *enablers* for a wide range of e-business systems. Nowadays, and especially in European Union member countries people are able to use a smart card to do one of the following daily life processes in a high secure level, comfortable way:

Dial a connection on a mobile telephone and be charged on a per-call basis. Establish your identity when logging on to an Internet access provider or to an online bank. Pay for parking at parking meters or to enter subways, trains, or buses. Provide hospitals or doctors personal data without filling out a form. Make small purchases at electronic stores on the Web (a kind of cyber cash). Buy petrol at a petrol station

Over a billion smart cards are already in use. Currently, Europe is the region where they are most used. Ovum, a research firm, predicts that 2.7 billion smart cards will be shipped annually during the current year. Another study forecasts a $26.5 billion market for recharging smart cards by 2005. Compaq and Hewlett-Packard are reportedly working on keyboards that include smart card slots that can be read like bank credit cards.

An inexorable shift in the world's card-payment business to ‘smart’ credit and debit cards is underway, spurred by their superiority to magnetic-stripe technology in combating fraud, and by a change in liability rules that is motivating banks to replace their cards by the end of 2005. Global smart card shipments are expected to increase substantially, from 1.7 billion to 4.1 billion units, with revenues up from US$2.2bn to $7.9bn between 2000 and 2006.

Currently the Europe, Middle East and Africa (EMEA) region accounts for 50% of card shipments, but Asia-Pacific is catching up. North America is a late-starter in the smart card market due to the wider acceptance of magnetic-stripe technology. The majority of smart cards today are in closed schemes providing single applications, e.g. SIM cards for mobile phones. However, adding more memory and processing power increases costs between US$4 and US$9 per card is typical, but enables multiple applications. Among the most important of these will be access control, both physical and online and authentication of messages by digital signature, etc. With e-commerce expected to exceed US$1.4 trillion in sales by 2004, smart cards are proving the best technology for providing consumers with the online security, protection and portability they demand.

1.2.3 Smart Card of the Future

Now let's examine, what is realistic from the features of the ideal smart card, and what capabilities exist in the cards on the market today. Today's cards have 8-32 kilobytes of memory. This is likely to increase in the future in parallel with the development of IC technology. Computational power has a closer limit though. Controlling overheating has always been a problem in case of microelectronics but in case of cards the problem is even larger. The card's shape is restricted and plastic may not melt. The authors believe that computational power will increase in the future, but will not increase dramatically.

Neither will smart cards' speed nor their storage capacity increase over that of PCs'. Real-time encryption of speech or video is far beyond the capabilities of today's cards, and the authors believe that it will not be possible in the near future. Supplying cards with cryptographic hardware is a question of price thus it is a question of mass production. Security and portability are the two areas where cards can be better used than PCs.

The possession of an own power supply probably has technical limitations, so cards are not likely to have one in the near future. This implies the absence of a timer too. However, non-card-shaped devices such as iButton do have such possibilities. Transaction management and power supply are two alternatives. On Java Cards the previous one is supported by the programming environment.

The lifetime of cards is not measured in decades nowadays. However, iButton is a device designed for hard circumstances (rock climbing, swimming), and its estimated lifetime is much larger than that of smart card. However, the technology of programmable smart cards is new so no long-term experience is available. The Java Card specification defines an environment, where applets may enter and leave the card dynamically.

However, these applets cannot interact with each other. The applications of Microsoft Smart Card for Windows may share data among each other, but the card's file system needs to be re-designed before a new application is downloaded.

The ideal smart card would have to be a compromise between these two, but security and robustness remain vital. The authors believe that although technology does not have the proper tools for this today, a solution will be found for this problem in the future.

JavaCard and Microsoft Smart Card for Windows both use high-level languages today; this seems to be the trend of development. Documentation for the cards is incomplete; the main tool of manufacturers is unfortunately still "security by obscurity". Smart cards are not likely to have an own user interface in the future.

However, their future is closely connected with that of mobile phones. Mobile telephony already gave a boost to the improvement of smart cards, and this rapidly developing area is where programmable smart cards are mostly used in practice today. Combining the power of smart cards with the user interface and network connection of mobile telephones new possibilities may arise. SIM cards already offered the users various applications in the past, and there is more to come when imagining that a computer fits just inside someone's wallet.

1.3 Smart Cards

Imagine the power of a computer, the speed and security of electronic data, and the freedom to carry that information, anywhere, on earth. Imagine a computer so small - it fits inside a plastic card like the credit card you carry in your wallet. And you imagine the Smart Card. A smart card is a card that is embedded with either a microprocessor and a memory chip or only a memory chip with non-programmable logic. Traditionally, the smart card has been used only for electronic identification and storage of personal data. However, the smart card of today contains a fully operational processor, and the increase in the memory capacity of the smart card makes it possible for the processor to run complex applications. The microprocessor card can add, delete, and manipulate information on the card, while a memory-chip card can only undertake a pre-defined operation.

These tiny cards contain the computer technology necessary to process and store such personal information, and promise to make life easier for both consumers and industry as their acceptance continues to grow. Smart cards are secure, compact and intelligent data carriers. Though they lack screens and keyboards, smart cards should be regarded as specialized computers capable of processing, storing and safeguarding thousands of bytes of data.

The smart card that we describe here is a plastic card equal in size and shape to a credit card that contains an integrated microprocessor and memory. These two components allow the storing and processing of information in the card. A smart card is not just an enhanced magnetic stripe card. It is different from all other types of card technology because of the existence of a microprocessor. This gives the smart card several attributes that, collectively, distinguish it from alternatives. The term "smart card" is used as an umbrella term for a variety of technologies. All cards conform to the same form factor (that of a standard credit card), and contain an integrated circuit chip, but the functions performed by that chip and the methods used to communicate with it vary. Their most useful attribute is their portability, they represent a piece of technology which the user can carry with them and use in a variety of different locations and applications.

1.3.1 Magnetic Stripe Cards

The magnetic stripe card, adopted by major credit card companies in the late 1970s consists of a plastic card with a thin stripe of magnetic material embedded in its surface. Small spots along the stripe are magnetized in varying degrees to form a code representing the stored data. A magnetic stripe card can store up to 240 characters of information. The magnetic stripe is divided into three tracks, according to international standards, each of which has been designed for different applications. One of the tracks is designated a read/write track and, with appropriate terminal equipment, can be updated.

The magnetic stripe card has proven to be exceedingly successful over the years. It is widely used in the world of banking for credit and debit cards, and to provide access to automated banking machines. In addition, the magnetic stripe card has been adopted for many different non- financial applications (e.g., club membership identification and health cards). Its two main strengths are low production costs and established standards. However, there are also several drawbacks:

1. The magnetic stripe can be damaged by scratching or exposure to a magnetic field.

2. The cards are easy to counterfeit, and the cards are typically limited to one application per card

Generally, magnetic stripe card systems use Personal Identification Numbers (PINs) in order to authenticate cardholders. It is unusual to store extremely sensitive information on a magnetic stripe card as the data can be easily read by unauthorized means, although for additional security, it is possible for a limited amount of information to be encrypted. Another identified deficiency is the limited amount of information that can be stored on a magnetic stripe card. Limited storage capacity in turn limits the ability to introduce new features to the technology.

In an attempt to address this issue, an enhanced magnetic stripe card has been developed. By reducing the width of each track and by using higher density recording, significantly greater amounts of data can be stored (e.g., a digitized signature for extra security).

If we turn a credit card around, chances that we will see a black stripe, approximately half inch wide, running across it. This back stripe, consisting of three tracks of magnetic particles bonded to the card substrate, in the core of a magnetic stripe card. The magnetic stripe cards were introduced to:

- Store data in machine-readable form
- Minimize paper utilization in financial transactions
- Allow for automation

As explained before, the magnetic stripe consists of three tracks. A track is divided into tiny domains, each domain being one-75th of an inch long. To store data on magnetic stripe card, the particles in a domain are magnetized in a particular fashion (figure below). If within a domain the polarization of the particles doesn't change, then there is no flux reversal and it represents a 0. But if the polarization changes, then there is a flux reversal and it represents a 1. The arrows in the domains represent the polarization of the magnetic particles in the domain

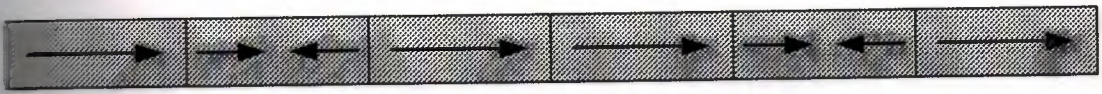


Figure 1.1: Magnetic stripe with domains.

When the magnetic stripe card is read, based on flux reversals the reader gets the data stored on it. The magnetic stripe shown in previous figure would be read as **0 1 0 0 1 0** The length of a magnetic stripe is around 4 inches and it consists of three tracks. Each track is made of domains 1/75th of an inch long. Each domain represents one bit. Hence the total data carrying capacity of a magnetic stripe card is just 900-1000 bits.

The main problem with magnetic stripe cards is data can be easily read and altered by anyone with access to the right kind of equipment. Card Skimming is the name given to the process of reading data of a valid card and copying it bit for bit on another card. Readers for magnetic stripe cards cost around $100 while encoders (writers) come for as cheap as $1000. As a result of this drawback, these cards cannot be used storing confidential information

1.3.2 Memory Cards and Microprocessor Cards

Smart cards are available in two basic types, the distinguishing feature being whether the card has a microprocessor, as, Central Processing Unit (CPU) or not. Cards without a CPU are called memory cards and those with are called intelligent cards, chip cards or microprocessor cards. The general usage of the term smart card is usually for cards with a CPU. Each type of card, with its own particular characteristics relating to cost, operational simplicity or functional superiority has application in particular segment of the market. Although it is the most important to focus this document on microprocessor cards, I will have to describe both types of cards for completeness.

Let us first talk about Memory Cards and give a view of its contents and application areas. These Memory Cards are used for single function application, they are implemented when a fixed operation needs to be done every time, memory cards are inexpensive, and typically used in phone card type prepayment applications. Access to data is managed by a security module in the chip which guards against the data being erased or written to.

In payment cards, reducing the card's value is done by the chip and is irreversible. After use the card is discarded, although presently there is a more graceful destination to the international collectors market. The simple technology enables these cards to be manufactured very cheaply and costs below US$1 per card in large quantities. This makes it still more expensive than magnetic stripe cards, which cost much less than US$1, but are cheaper than microprocessor cards. The simple technology also makes it possible for the reader devices to be manufactured cheaply. At first it may seem an obvious candidate for moving on to smart card technology. However, extra investment may be required to overcome incompatibilities in terminal infrastructure, and differences in programming APIs. A later migration to microprocessor card technology may also prove costly in the long-term due to the nonstandard proprietary nature of memory cards.

The International Organization for Standardization has concentrated its efforts on microprocessor cards and there is very little effort to standardize memory cards within the industry.

The cards memory for storing data can range from a few hundred bytes up to 8 KB. A more intelligent version of these cards is available, that is capable of providing more security by authenticating itself, (for example, correctly responding to a random number challenge request from the terminal). This type of card is also capable of PIN verification, but is very limited in their flexibility. Application Areas: Telecommunications, pre-payment, health insurance number, vending machines, car parking, public transport, frequent flyer cards, simple loyalty schemes. Examples of Implementation: European phone cards, German health insurance card.

Microprocessor cards are able to provide read/write function and enhanced security with a CPU. They are more expensive than memory cards costing around US$5-15. With microprocessor cards you can write and update the data, once the cards access conditions are met.

The way a microprocessor cards internal architecture is designed bears a striking resemblance to PCs. The familiar building blocks of a PC are present in this type of smart cards: CPU, ROM, RAM, I/O port and in this case an EEPROM rather than disk for storage.

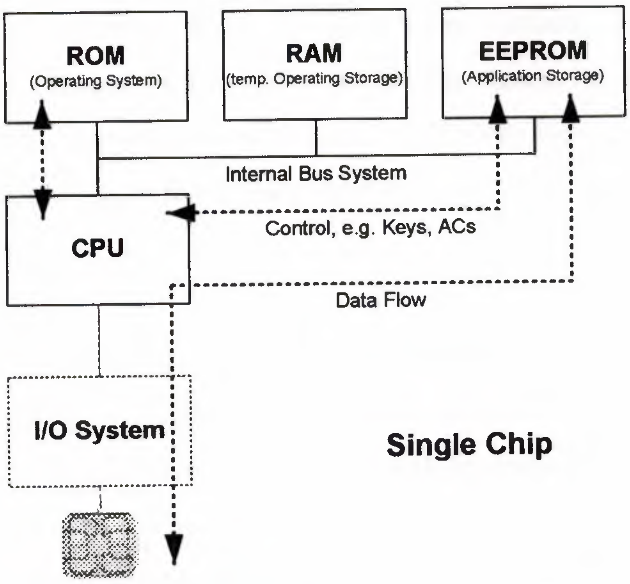


Figure1.2: Smart Card Internal Architecture

Smart Card is a small plastic card which contains a microchip, some amount of memory and the necessary communication channels. The micro chip adds processing power to it. Processing is done on data, which is present in specialized memory cells. These memory cells can be either volatile or non-volatile. Any information which should last, unless modified by some application, should be present in the non-volatile memory. The volatile memory is used for temporary storage, such as variables in a program.

There is an operating system called Card Operating System (COS), which is similar to the ordinary disk operating system, which handles all the resources on the card. So the COS acts as a resource allocator on the card. This takes care of the security among different applications residing on the same card. This is also used to load and delete applications, provided that the required authentication and privileges are given.

1. **CPU (Central Processing Unit):** The CPU is usually an 8-bit to 32-bit microprocessor with a 16-bit address bus. This makes it possible for this type of processor cards to address up to a maximum of 64 KB.

2. **RAM (Read Only Memory):** The RAM is volatile memory that requires power to maintain the data. It provides working storage for the CPU. Usually the size of the RAM is about 256 bytes. RAM, is used as a temporary storage register by the chip's microcontroller. For example, when a PIN is being verified, the PIN sent by the terminal or PIN pad is temporarily stored in RAM. The reason for this small size is that RAM memory takes up more space per byte than the EEPROM or ROM memory and is deliberately kept small to meet the specification for smart card chips, which are limited in total size to 25mm^2.

3. **ROM (Read Only memory):** The ROM contains the smart card's operating system and is loaded during chip production. The software loaded is called a ROM-mask. The ROM size can vary from a few KB to around 32 KB depending on the operating system function. When speaking of the operating systems the question that is likely to be asked is whether the card has provision for an operating system upgrade post-issuance. Since the operating system is in the ROM, there is no possibility for upgrading the ROM with a new version after the card is issued.

(However, the card can execute code written in the EEPROM, which in the broad sense of the word could be used as an operating system upgrade, although it's very rarely done in practice. Writing application code requires intimate knowledge of the CPU, which is closely guarded and requires specialist knowledge and skill.)

4. **EEPROM (Electrically erasable programmable read only memory):** this is nonvolatile memory and is used to hold all data and programs much like a PC hard disk. (i.e., it does not lose its data if power is shut off) and is read/write memory for the storage of data. Access to the EEPROM memory is controlled by the chip's operating system. EEPROM can currently contain 128 kilobytes (Kbytes) of memory with the potential for more than 256 Kbytes. EEPROM may contain data such as a PIN that can only be accessed by the operating system. Other data, for example, a card's serial number, can be written to EEPROM during card manufacture. EEPROM is typically used for application data and for certain filtered functions. Most of the EEPROM memory is used to store user data such as a biometric, purse balance, special use authorization or payment tokens, loyalty tokens, demographic information, and transaction records. EEPROM can be rewritten from tens to hundreds of thousands of times and can be programmed or erased in either blocks or bytes. The operating system provides file protection by restricting access to the EEPROM. EEPROM sizes can vary in size, and typically this size is selected based on application needs.

Some chip manufacturers provide components with a combination of ROM, flash memory and EEPROM, so it would be one good idea to briefly explain what a Flash memory is.

5. **Flash Memory:** (sometimes called "flash RAM") is a type of constantly-powered, non-volatile memory that can be erased and reprogrammed in units of memory called *blocks*. Flash memory is often used to hold control code such as the basic input/output system (BIOS) in a personal computer. When the basic I/O system (BIOS) needs to be changed (rewritten), the flash memory can be written to in block (rather than byte) sizes, making it easy to update. Since flash products are generic and applications can be downloaded at the last step of the production flow, they add flexibility and can provide faster time-to-market.

While features vary among different products, flash memory is usually lower cost than EEPROM but current products generally can't be programmed and erased as many times and usually can't program or erase single bytes of memory.

Flash memory gets its name because the chip is organized so that a section of memory cells are erased in a single action or "flash." The erasure is caused by Fowler-Nordheim tunneling in which electrons pierce through a thin dielectric material to remove an electronic charge from a *floating gate* associated with each memory cell. A form of flash memory is available today that holds two bits (rather than one) in each memory cell, thus doubling the capacity of memory without a corresponding increase in price.

6. **FRAM:** (ferroelectric RAM, also called Fe-RAM) is another non-volatile memory technology. FRAM can read data thousands of times faster at far lower voltage than other non-volatile memory devices. FRAM is random access memory that combines the fast read and write access of dynamic RAM (DRAM), the most commonly used memory in personal computers, with the ability to retain data when power is turned off (as do other non-volatile memory devices such as ROM and flash memory). Because FRAM is not as dense as DRAM and static RAM (SRAM) (i.e., it cannot store as much data in the same space), it is not likely to replace these technologies.

However, because it is fast memory with a very low power requirement, it is expected to have many applications in small consumer devices such as personal digital assistants (PDAs), handheld phones, power meters, smart cards, and security systems. FRAM is faster than flash memory. It is also expected to replace EEPROM and SRAM for some applications and has the potential to become a key component of future wireless products. However, unlike EEPROM or flash memory, FRAM is not yet a proven high-density mass production technology for smart cards.

The following example will further explain the functions of the memory types listed above. A commonly used microcontroller chip card would have its operating system stored in ROM. The operating system or command set would respond to commands, such as "read a record," "write a record," and "verify PIN," sent to the card by a terminal or reader.

Information such as fund balances, card serial number, and demographic information are stored in EEPROM. The CPU performs all processing functions, such as encryption, while RAM serves as a temporary register for information. During PIN verification, the PIN is temporarily stored in RAM. Since RAM memory is volatile, as soon as a card is powered off, all information stored in RAM is lost. When evaluating card types for a particular application, the amount of memory in various components is important.

The EEPROM capacity of a card is critical because a larger capacity EEPROM can store a greater number of application records and transaction files. The amount of ROM is also important because a larger capacity ROM can contain a more sophisticated operating system, which facilitates complex card and system operations. There is also a relationship between ROM and EEPROM in some cards because several vendors allow custom code extending the ROM's operating system to EEPROM.

While this technique increases the card's functionality, it decreases the amount of EEPROM available for application and transaction storage. Conversely, more established and accepted applications can be included in ROM in future chip versions, freeing up EEPROM space for additional applications and expansion.

7. **I/O Port:** Manages the flow data between the Card Acceptance Device (CAD) and the microprocessor. The I/O port is used to transfer the data in a serial fashion, bit by bit. The default speed is 9600 bits per second; some cards support higher speeds.

8. **Co-Processor:** The more advanced cards are provided with a co-processor which perform the exponential and modular operations on integers when handling encryption procedures, for example with digital signatures.

Usually the card uses an ISO 7816-defined file structure to store and protect the data. This file structure and protection mechanism enables different applications to store data in a single card with fire-walling between the applications.
Microprocessor cards are extremely versatile and have found a wide portfolio of applications.

Application Areas: access control, loyalty programs, electronic cash, airline ticketing, and credit card, secure messaging, ID card, for details refer to the third section of this project work, a few examples of implementation are: Dutch Student Card, Hilton Hotels Check-in, Digital Signature Card, German Geldkarte, Diabcard and many others alive.

Both memory and microprocessor cards are available as contact or contactless cards. As the name implies, the main difference is in the method of communicating with the reader device. Contact smart cards require insertion into a reader device. Contactless cards require close proximity to a receiver device, but there is no insertion. This leads us to the next section where types of Smart Cards are studied

1.4 Smart Card Types

These tiny computers can be classified on basis of various parameters, we had discussed the classification on basis of Card Components in the 1.3.2 section, and we shall discuss the classification based on Card interface and Smart Card OS in this section. The classification is better depicted in figure 1.3

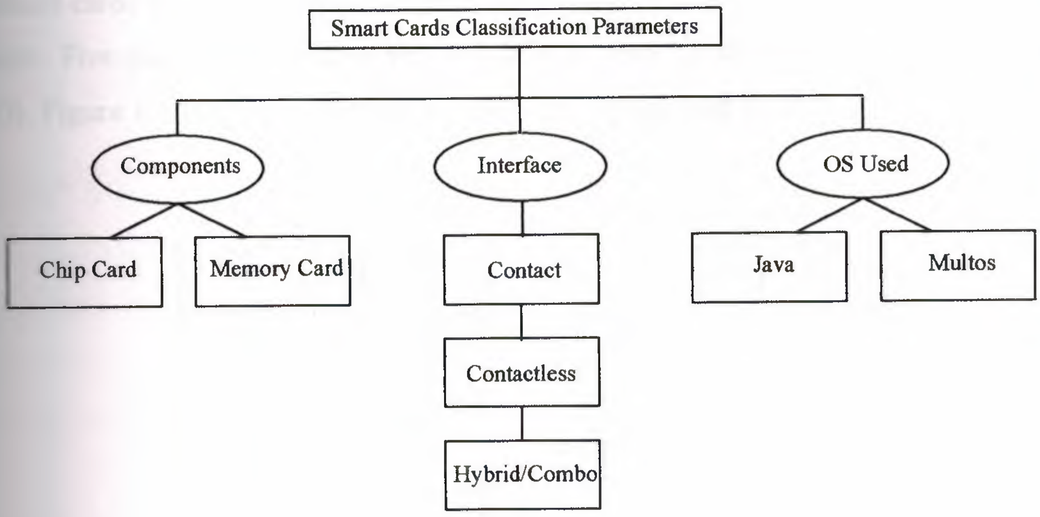


Figure 1.3: Classification parameters of Smart Cards

1.4.1 Contact Cards

Contact smart cards are the most popular card-connection design. The card must be inserted into a reader and must make a physical contact with the reader contacts in order to receive power and a clock signal for the chip to operate. The power to the card is switched on or off under the control of the host application or the reader. The reader may lock the card in place to avoid accidental removal before a transaction is completed. There is no restriction on the amount of data transferred or a time limit apart from a usability point of view. The chip contacts have to adhere to the standard specified by ISO 7816-2.

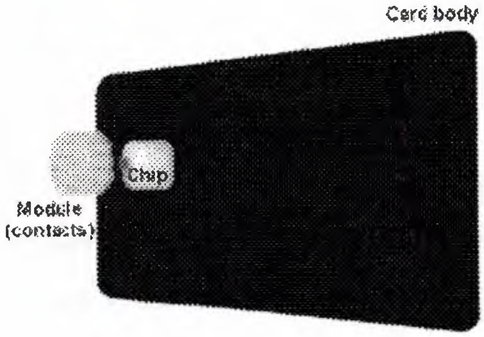


Figure 1.4: Contact Smart Card

Contact cards use an eight-pin contact, micro module to physically connect to the card reader. Five pins are defined as Vcc (+5 VDC), reset, clock, ground, and input/output (I/O). Figure 1.5, shows an example of a typical contact card module.

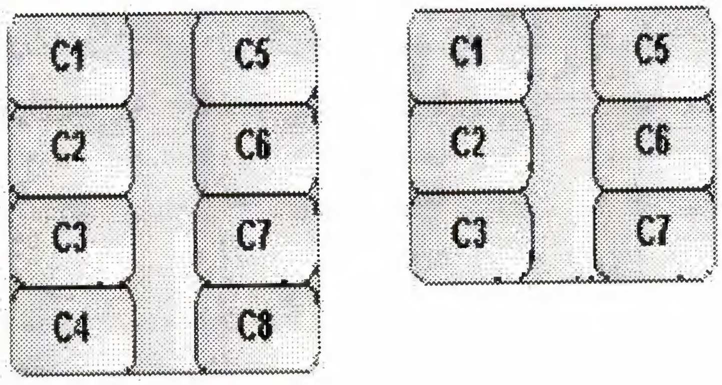
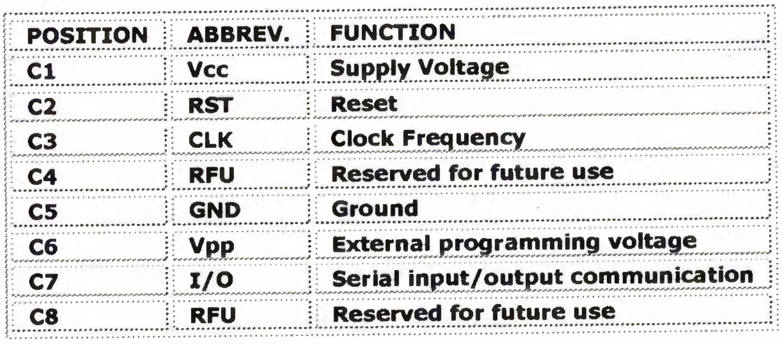


Figure 1.5: Electrical contacts are typically numbered C1 through C8 from top left to bottom right, as shown here both for 6 and 8 contact shapes

In Table1.1 I list for contacts a standard abbreviation and a short function description.



POSITION	ABBREV.	FUNCTION
C1	Vcc	Supply Voltage
C2	RST	Reset
C3	CLK	Clock Frequency
C4	RFU	Reserved for future use
C5	GND	Ground
C6	Vpp	External programming voltage
C7	I/O	Serial input/output communication
C8	RFU	Reserved for future use

Table 1.1: Mechanical contacts of a smart card and corresponding functions

The Vcc is used to supply voltage to the chip. The Vcc supply voltage is specified at 5 volts ± 10%. Vcc is between 4.5-volt and 5.5-volt. There is an industry push for smartcard standards to support 3 volt technology because all mobile phone components are available in a 3 volt configuration, and smartcards are the only remaining component which require a mobile phone to have a charge converter. It is theoretically possible to develop 3-volt smartcards, but interoperability with current 5-volt systems would be a problem. Nonetheless, a wider voltage range handling 3 to 5 volts will probably become mandatory in the near future.

The RST is used for the reset signal to reset the address counter and the microprocessor. A reset without removing power called warm reset. A cold reset takes place if the power is removed then reapplied. CLK is used to external clock signal, from which the microprocessor clock is derived. GND is used for ground connection. I/O is used to transfer data between the smart card and the reader device in a half-duplex mode.

The Vpp contact was used several years ago for high voltage signal, which is necessary to program the EEPROM. However, with the advent of charge pumps that exist on the chip, the Vpp contact is rarely used today.

1.4.2 Contactless Cards

The reliability of smartcard contacts has improved over the years, to very acceptable levels which are higher than magnetic stripe cards. Yet, careless handling and very frequent use can take its toll on the gold contact surface, leading to eventual failure of the chip contacts. Contacts are one of the most frequent failure points any electromechanical system due to dirt, wear, etc. The contactless card solves this problem and also provides the issuer an interesting range of new possibilities during use. Cards need no longer be inserted into a reader, which could improve end user acceptance. No chip contacts are visible on the surface of the card so that card graphics can express more freedom. Still, despite these benefits, contactless cards have not yet seen wide acceptance. The cost is higher and not enough experience has been gained to make the technology reliable. Nevertheless, this elegant solution will likely have its day in the sun at some time in the future. Contactless cards manage to avoid this pitfall, as they do not require insertion into a card reader and can work up to several centimeters away from the reading device. This lends itself naturally to applications such as mass transit and access control.

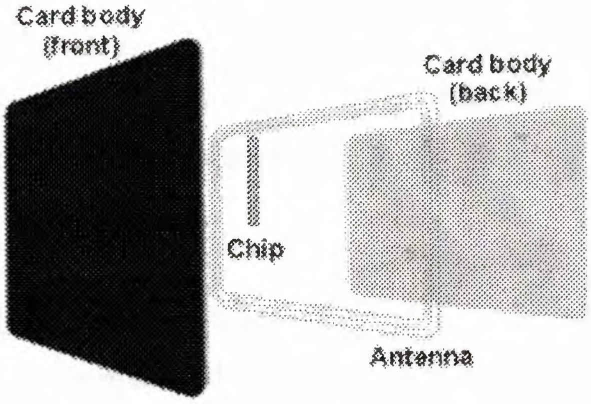


Figure1.6: Contactless Smart Card

The above contactless cards are called passive since they have to derive the power externally. There are contactless cards that derive the power from an embedded battery and these are active contactless cards used, for example, at motorway toll gates, supporting greater distances between the card and the reader.

This type of contactless cards tends to cost more than contactless cards without built-in battery. Contactless cards with their specialized readers tend to cost more than contact cards. The chip derives the power to work from capacitive coupling (close coupling) or inductive coupling (remote coupling). Inductive coupling works on the principle of a transformer where one coil induces current in another coil. The frequency of transmission is usually in the range of a few MHz. The chip is able to transmit a data signal by changing its resistance, which is picked up by the card reader and is interpreted as a data signal.

Writing to a card requires much more power (up to 10 times more) and hence the range is reduced to about 10 cm maximum for inductive coupling cards and about a few millimeters for capacitive coupling cards. Because there is a very short amount of time for the transaction to complete (up to 200ms if the user walks by the reader), the data transmission is limited to a few hundred bytes. These cards are therefore suited for single applications that require a faster transaction speed than contact cards can offer, like mass transit or access control.

The different methods developed to optimize the contactless solution have, however, resulted in incompatibility between different systems. The applications of standards are in process (ISO 10536 for close coupling cards and ISO 14443 for remote coupling) and with no established standard the card is likely to be closely tied to the manufacturer's own reader. The contactless smart cards operate at 4.9 MHz, 6.6 MHz or 13.5 MHz frequencies.

1.4.3 Combi Cards/Dual Interface Cards

Combi cards also have a contact and contactless surface but the two interfaces are connected and have access to one shared data area via a microprocessor or logic module. The contact surface is always controlled by a microprocessor. The shared data area may be controlled by a microprocessor or a logic module. An example where the shared memory is controlled by a logic module is the Mifare Plus combi card. An example where it is controlled by a microprocessor is the Mifare II. Both are produced by Philips/Mikron.

Dual interface cards have one processor chip that can be operated through I/O ports, the contact and the contactless. The smart card software controls the port usage by application; for example, loading the e-purse via contact side only, spending of small amounts through any port. The disadvantage of a contactless/combi card over a contact card is the increased cost required to implement the antenna into the plastic card, and more expensive readers that need to have Radio Frequency (RF) transmitter/receivers. Combi card performance is likely to be slower than a contactless card because the RF unit has to get the data via the CPU.

Another disadvantage with this type of card is that communication can be interrupted by removing the card from the RF field, or it can be possibly traced or disturbed.

1.4.4 Optical Cards

For applications where a very large amount of storage capacity is required, optical memory cards are available, which can store for instance X-ray images of a patient. These cards usually have a microprocessor chip embedded and use the smart card security to protect the optical data from unauthorized access. The optical card provides some megabytes of Write-Once/Read-Many (WORM) storage. Data can be read by appropriate devices and is not protected, unless it is encrypted.

1.5 Smart Card Standards

Smart cards themselves usually are a small part of a much more complex system. There are usually complex networks of card terminals connecting to other backend host computers that process the information from transactions occurring at the card terminals. Companies investing in this infrastructure have a vested interest in standardizing the system components to guarantee the longevity of the system. Without standards, different manufacturer's components would not interoperate. The smart card systems would not be generally accepted because users would be forced to carry around many different, non-interoperable smart cards. This is an untenable situation for both users and manufacturers.

Standards are keys to ensuring interoperability and compatibility in an environment of multiple card and terminal vendors. Integrated circuit card standards have been underway since the early 1980s on both national and international levels. Basic worldwide standards for smart cards have been and continue to be established by the International Organization for Standardization, which has representation from over seven nations. A brief explanation of each legal issue of smart card standards is provided in this section, the most popular party is the ISO specifications and thus I have been concerned with it rather than else parties.

Smart-card standards define the operation of the technology, and promote product interoperability between smart-card manufacturers. Because there are a variety of smart-card applications requiring different solutions, several standards were needed to define smart-card technology.

1- ISO/IEC 14443-1: The ISO and International Electrotechnical Commission (IEC) specification for contactless cards that changes the contact description to an antenna, and defines the protocol for communication over the air.

2- ETSI: The European Telecommunications Standards Institute specification that defines a smaller-sized smart card to fit into GSM phones.

3- EMV: The integrated circuit card specification for payment systems, which is managed, maintained, and enhanced by Europay International, Master Card International, and Visa International (EMV). This standard defines the way smart cards interchange in a payment terminal by disallowing the reader to be transparent. This increases security by preventing reading of the card for low-level information. This condition conflicts with Microsoft's Windows Hardware Quality Labs (WHQL) specification, which requires full ISO 7816 compliance.

4- PC/SC: This PC/SC Workgroup specification builds on existing EMV and ISO 7816-X specifications by defining the smart-card reader/writer abstraction layer. This is a complementary specification that defines low-level device interfaces, device-independent application APIs, and resource management, which allows multiple applications to share smart-card devices attached to a system.

5- JavaCard: This specification defines the way the Java Virtual Machine is implemented so that an end user can run any Java applet on the smart card. The Java Card Forum drives this specification.

6- WHQL: the Microsoft WHQL facility defines the guidelines for products that are compliant with Microsoft OSs. The focus is to ensure that devices work in the Windows environment, and are compatible with other devices. WHQL requirements for smart cards require full ISO 7816 compliance.

7- ISO 7816-X: The dominant standard for contact smart cards consisting of ten sections that detail the physical, electrical, mechanical, and application programming interface (see Table 1.2). All other smart-card specifications are variations of this standard.

The International Organization for Standardization (ISO) 7816-X specification defines the complete characteristics of smart-card technology. Other specifications alter elements of the ISO 7816-X specification to meet specific application requirements. The ISO 7816 series is the international standard for integrated circuit cards.

Part 4 of ISO 7816 is from an application developer's point of view, the most important part of the standard as it specifies the standard communication protocol data units, termed Application Protocol Data Units (APDUs). Moreover, ISO 7816-4 describes how the data storage on a smart card might be organized as a file system.

Although ISO 7816 does a very good job of laying the ground work for smart cards, it is not very specific where the really interesting part is concerned: interoperability. Most of the APDU definitions contained in ISO 7816-4 are optional, and-being a true ISO standard-ISO 7816-4 leaves a lot of loopholes open so that we can create a smart card for which we can claim compliance to ISO 7816, yet, aside from our own application no other application will be able to talk to our card. In addition, nobody can force any given smart card provider to implement the later parts of ISO 7816

PartNo.	Date Approved	General Description
7816-1	1987	Governs the physical dimensions of the card (width, length, and thickness), which are those of a standard credit card.
7816-2	1988	Governs the dimensions and locations of the chip contacts.
7816-3	1989 with two amendments in 1992 and 1994	Governs the electronic signals and transmission protocols in term of electrical characteristics, transmission protocols, and the format of the card "Answer to Reset".
7816-4	In Progress	Governs inter-industry commands and responses to include the Application Protocol Data Unit (the command exchange format independent of the transfer protocol), historical characters of the Answer to Reset, file structures and access methods, data object oriented commands, and secure messaging format.
7816-5	1994 with one amendment in progress	Provides for a registration system for application identifiers, which allow terminals to select unambiguously an application in a card.
7816-6	1996	Governs data elements for interchange.
7816-7	1999	Governs Smart Card Query Language. Commands to support a relational database on a card.
7816-8	In Progress	Governs security related inter-industry commands.
7816-9	In Progress	Inter-industry enhanced commands.
7816-10	In Progress	Governs synchronous cards.

Table1.2: International Organization for Standards Smart Card Standards

1.6 Smart Card Hardware

In this section of this project work I will go through the architecture of a smart card and the physical and electrical properties. The card is made of three elements: a plastic card, a printed circuit, and an integrated circuit chip. Figure 1.7 shows the physical elements of the smart card.

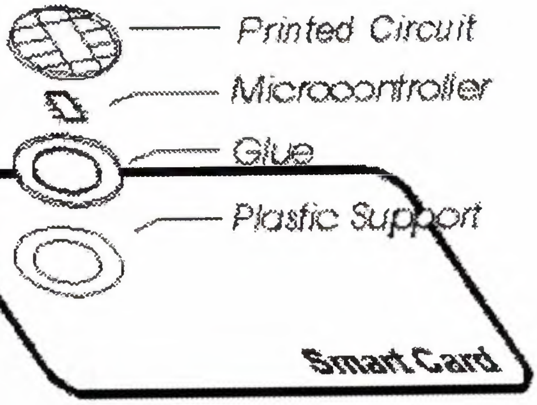


Figure 1.7: Physical Elements of the Smart Card

Several forms and sizes were specified for plastic cards. The two most important forms for smart card are ID-1 and ID-000. The form ID-1 has the size of a credit card and is used for most of the applications. The forms called ID-000 are mostly used in mobile phones and for Security Access Modules in terminals.

Designated as ID-1, a smart card is described in ISO 7810 as having physical dimensions of 85.6 mm x 54 mm, with a corner radius of 3.18 mm and a thickness of 0.76mm.

ISO 7810 also addressed embossing, magnetic stripes, and other physical properties; however, because the standard was developed in 1985, it did not address chip placement. Consequently, smart card chip placement is defined in ISO 7816-2, which was released in 1988.

The main reason for the size and shape of the smart card is to make it geometrically compatible with magnetic strip cards. This allow for using the same card either as smart card in new applications or as magnetic strip card in legacy applications.

For application where the compatibility to standard magnetic stripe cards is not an issue, physically secure small cryptographic units are available in other forms like a ring or button (for example Dallas semiconductor's iButton or as token directly attachable to the universal serial bus). Electrical contacts are typically numbered C1 through C8 from top left to bottom right.

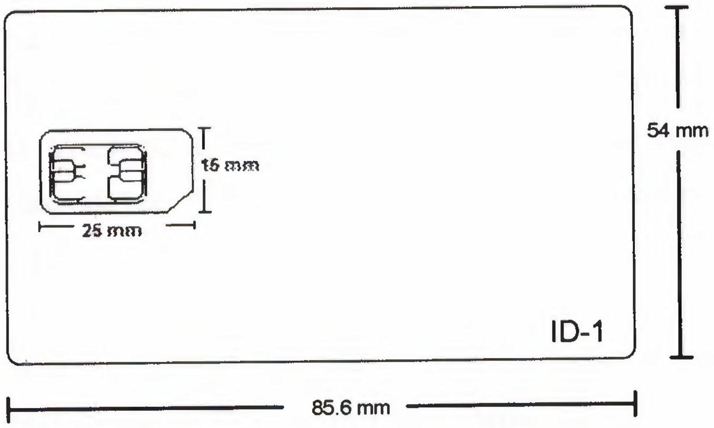


Figure 1.8: The size of the smart card ID-000 and ID-1

CHAPTER TWO: INTRODUCTION TO SMART CARD SOFTWARE AND OPERATING SYSTEMS

2.1 Introduction

A typical configuration for a smart card system consists of a host computer with one or more smart card readers attached to hardware communications ports. Smart cards can be inserted into the readers, and software running on the host computer communicates with these cards using a protocol defined by ISO 7816-4 [ISO4] and 7816-8 [ISO8]. The ISO standard smart card communications protocol defines Application Protocol Data Units (APDUs) that are exchanged between smart cards and host computers.

This APDU based interface is referred to as the "virtual card edge" and the two terms are used interchangeably. Client applications have traditionally been designed to communicate with ISO smart cards using the APDU protocol through low-level software drivers that provide an APDU transport mechanism between the client application and a smart card.

ISO 7816-4 [ISO4] defines a hierarchical file system structure for smart cards. Smart cards that conform to ISO 7816-4 [ISO4] are therefore known as "file system" cards. The Card Operating System program of a file system card is usually hard coded into the logic of the smart card integrated circuit during the manufacturing process and cannot be changed thereafter.

In recent years other smart card architectures have been created that allow developers to load executable programs onto smart cards after the cards have been manufactured.

As one example, Java Card defines a Java Virtual Machine (VM) specification for smart card processors. Developers can load compiled Java applets onto a smart card containing the Java Card VM, programmatically changing the behavior of the card.

A virtual machine card is one that can be extended by loading executable programs after the card has been manufactured.

This Specification uses the term "virtual machine smart card" in the general sense. A virtual machine smart card can theoretically be programmed to support any communications protocol, including the APDU based protocols of the ISO standards.

Since 1997, Java Card and MultOS (which stands for "Multiple Operating System") have advanced the smart card market considerably. Together, they have focused attention on the important smart card standards debate, creating the means for developers to separate applications from the physical card and load applications onto the card after it has been issued.

MULTOS (which stands for "Multiple Operating System") is an operating system that allows multiple application programs to be installed and to reside separately and securely on a smart card.

Each program is isolated by the operating system so that no application can interfere with another one. Whereas earlier smart card systems did not allow new applications to be installed or old ones deleted, MULTOS makes this possible. Updates or patches can also be installed as needed. Each application is platform-independent due to the implementation of a virtual machine. Developers write applications for MULTOS smart cards using the MULTOS Executable Language (MEL).

Before MULTOS, application developers had to write a separate version of the application for each type of smart card and the consumer needed a separate smart card for each application. With MULTOS, several applications can reside on one smart card regardless of the microchip used.

Security for MULTOS smart cards is enabled by the MULTOS Certification Authority (CA), which issues cryptographic keys for each MULTOS smart card and all MULTOS applications. These keys prevent unauthorized applications from being loaded into a card or deleted without the issuer's permission. A group of leading international organizations, openly licenses the MULTOS specification. MasterCard, Mondex, Europay, and Discover favor MULTOS. MultOS is the more mature technology, with an infrastructure in place to guarantee interoperability.

2.2 Overall System and Card Life Cycle

The advent of plastic cards had been greeted with expectations to simplify the way we conduct payment or personal identification. Since then, an ever-increasing amount of plastic from a multitude of vendors has been filling up our wallets. The advanced capability of smart cards promised to alleviate and solve this problem by supporting more than one function on the cards.

Multi-application smart card operating systems such as MULTOS, the Java Card or Windows for Smart Cards are continuing this objective to support a variety of applications from different vendors from a single smart card. The level of success of tackling this predominantly political issue, the lack of cooperation among card issuers, by using a technological approach remains to be seen.

If a single smart card is to be shared among different companies or institutions for identification and authentication of the individual cardholder, then trust issues need to be addressed and resolved. Who is authorized to load or delete applications on a multi-application card? The card issuer may be in a position to compromise the security of applications or data that other, possibly rival companies are storing on the card. The more entities are involved in using or modifying the card during its lifetime, the more complex a trust model must be developed.

The technological aspects of smart cards have been hailed ever since their arrival on the marketplace. Relatively tamper-resistant computers small enough to fit in everybody's wallet are indeed some kind of technological sensation. One is quick to forget that smart cards can only be a small element in a larger distributed system. They are thin clients at best, which typically only start to operate when inserted into a card-accepting device (or reader).

These readers are usually part of a terminal, which typically exchanges data with the card and sends it on to a host on a network. This network should be physically secure, and system design should reflect limitations of physical access control. Secure end-to-end communication from card to host is often employed, if the network itself cannot be trusted.

"A system can only be as secure as its weakest link". If card, reader, terminal and network are deemed to be secure, how about the host computer holding the customer database? The majority of credit card numbers were not stolen by eavesdropping networks, but by attacking customer databases directly on the web servers or server database back-ends. Security issues have been discussed in the third section of this project work

Finally, the overall system should allow for fallback and recovery in the event of a failure during a transaction. Two-stage commit techniques or transaction rollback methods need to be implemented to allow canceling of interrupted sessions.

Moving now to describe the phases a smart card has in its life cycle. Generally, a smart card is passing a number of stages throughout its life. From a security perspective, each of these stages introduces the card to a different scenario in which it has to face different vulnerabilities.

Obviously, attacks on the integrity of a card are easier the earlier in its lifecycle they are conducted. It would be perfect to control theft of cards and components throughout the manufacturing stage, since complete smart cards are almost impossible to counterfeit.

The following stages in the lifecycle of a smart card can be recognized:

1. Chip design
2. Manufacturing and testing
3. Customization / pre-personalization (initialization)
4. Personalization
5. Issuance
6. Loading and validation
7. Use
8. Application loading/unloading
9. End of life

When a smart card is manufactured, it's in an empty state with the exception perhaps of providing some information about itself (protocol, operating system version etc.) to the card terminal.

Card serial numbers and keys are initialized during the manufacturing stage and cannot be changed afterwards. A fabrication lock is "blown" after chip manufacturing, making it physically impossible to tamper with these values. A card manufacturer then embeds this chip into the card in the pre-personalization stage, before which, the card cannot be used with an application.

It must first go through a setup process called initialization. This is similar to formatting a PC hard disk and creating files and directories common to all the machines.

The file layout, which is a representation of the smart card applications that we require, is generated by giving a sequence of instructions to the smart card processor chip. To enable thousands of cards to be prepared this way, the instructions are stored in a file called an initialization table (or in an initialization script).

During initialization, the cards EEPROM memory is erased and files and directories are created according to the layout that's specified. In addition, some data common to all the cards being issued may also be loaded into the EEPROM memory locations during the initialization.

Depending on the operating system/card supplier, the layout generating procedure is accomplished using different methods. One method uses a simple tool to manually create the card structure, file by file and save the commands in a script file. A card simulation tool may be provided to enable the layout to be tested without using a real card. The script is later given to the card supplier, who uses internal merging tools to create commands for each card and uses these in the card production process.

In another method, the layout is generated quite easily using a high-level language to create a layout file. This is later compiled into the necessary instruction tables using a layout compiler. Simple keywords allow different chip processors and operating systems to be specified.

The initialization is usually carried out as part of the chip embedding process during card production. This gives added security, since the process is carried out under strictly controlled environments, possibly certified by banking and credit card organizations.

The second step is called personalization, where information unique to the cardholder such as name and account number is written to the card. The reason for a two-step process is to provide a technical and cost-efficient process. The personalization process can be a complex and slow operation.

It has to load the correct data (for example, name, and specific keys) into the smart card maintaining data confidentiality and also needs synchronizing with other card surface information and possibly magnetic strip data. Another benefit of this two-stage process comes from being able to conduct the personalization in more secure premises using cards already initialized. After the personalization process the cards are ready for delivery to the cardholder.

Personal data isn't stored in the card before it enters the personalization stage. Cardholder data, which usually resides with an end-user company, is now transferred in a secure manner from a database to the card. Cryptographic keys are then derived or generated in the HSM host or inside a personalization device.

Personalization devices (or card personalization machines) are useful if asymmetric keys are used, which require only the public key to be stored on the host, while the corresponding private key can be discarded after transfer to the card. Again, blowing a "personalization lock" completes this stage, preventing later modification or extraction of sensitive information.

After personalization, it's the turn of the issuance stage. The Issuance is rather non-technical and involves postal dispatch of cards and PINs. Despite its relative simplicity, this is often the weakest link in the overall system, due to the possibility of postal interception. At the instance the cardholder gains possession of the card, much of the system security is left to the strength of tamper resistance that the card is commonly associated with.

Loading and validation applies in situations in which a monetary value is associated or stored within a card. The process may involve loading and top-ups, which may be performed offline or in online transactions

Compared to other stages, the actual use phase of the card is relatively straightforward. Issues during use of a card encompass not only authentication, but also logging of use, audit, error-recovery, and a whole range of measures in the event of card loss of theft. Such an incident must be reported, and should lead to timely invalidation of the card. If the authentication procedure is decentralized, the card could be placed on a "hotlist", which is distributed to all terminals.

Procedures for re-issuing cards may not be able to reflect upon dynamic data, which was exclusively stored in the lost card. In case the eligibility of a cardholder to access a specific service is no longer desired, MULTOS cards can block the specific functionality of a part of the card, without affecting other applications.

A card usually reaches the end of its life at a given expiry date, usually printed on the card. This is a regarded as final protection against misuse and a method to allow for infrequent technological upgrades, rather than to annoy customers. On multi-application cards, all loaded applications should expire no later than the card itself (or the master application in case of MULTOS).

2.3 Smart Card Software

To write and read data to a smart card or to execute a command on a smart card, it is necessary to have a physical connection with the card. To make the connection with the contact card, it has to be inserted in a smart card acceptance device. In this chapter we given an overview of the different type of the card acceptance device.There are a wide variety of acceptance device available on the market. We can distinguish two groups.

1. Reader
2. Terminal

The smart card reader is basically a connector between the smart card and the device communicating with the card.
In contrast to this, a terminal is a computer on its own and can operate standalone without being attached to another device. A reader can usually also write data to a card.

Smart card readers often have their own housing and are connected to the serial, parallel, or USB-port of a computer. Other reader types are integrated in a keyboard or fit into a PCMCIA slot. Another reader type has the size of 3.5" diskette and is inserted into a diskette drive to be connected to a computer.

In addition to the card slot and the computer interface, a smart card reader can also have a display and a PIN-pad. The main use of the PIN-pad is to enter a PIN (personal identification number), which is sent to the smart card to identify the card owner.

Most reader has only one slot for a smart card. For special applications like a medical patient card, which can only be accessed upon authorization through a doctor card, the reader can have a second card slot.

The advantages of a smart card terminal over a smart card reader attached to a computer are a tighter control of the smart card access. A terminal can be sealed to prevent tampering with the hardware. The software installation can be tightly control by special schemes which could not be applied to a general-purpose computer.

Such a secure and protected system is desirable for payment transaction, for example. For a payment transaction, the customer want to be certain that no manipulation of the hardware or software would draw more money from the card than she authorized. Some purse scheme requires a special smart card for the merchant which is inserted in one of the slots of the terminal. In these schemes, the money is transferred from the customer's card to the merchant's card, or the merchant card authenticates the terminal to the customer's card.

Often, a merchant accept payment from more than one purse scheme. To use a separate terminal for each scheme accepted would increase the cost and take up more desk space. Therefore it is common that terminal have one slot for the customer's card and four or more slot for the merchant's card. With such a terminal, the merchant can accept several different electronic purses with a single device. A terminal is a computer on its own, with a processor and memory. Today a high-end terminal typically has a 32-bit processor and up to 1 megabyte of memory.

Most of the payment terminals are not only capable of executing smart card transactions, they can also perform credit and debit transaction based on data read from a magnetic stripe.

Terminals are available in different enclosures. The most common kind is tabletop device, which u might have seen at your gas station or local grocery store. A tabletop device is mainly used for payment or credit transactions made while the customer visit the merchant. When the merchant visit the customer, e.g. to a deliver a pizza, the merchant preferably uses a portable payment terminal. Portable terminal can perform off-line transaction. Some are also capable of using mobile data network for on-line transaction. Many terminals can also be extended with additional features like ticket printers.

In the same way we can draw cash from an ATM, we can load an electronic purse at an unattended load device. Using this kind of unattended terminal is very similar to using a traditional ATM. In addition to loading an electronic purse, this type of terminal can often be used to change passwords, to check the card balance, to print statements, to lock or unlock the purse card, to pay bills, and more.

2.3.1 Communication between Card and Terminal

When the card is inserted into the reader, the terminal detects this and sends a Reset signal. Upon the receipt of the Reset signal, the card sends an Answer-To-Reset (ATR), as an answer to the previous signal.

This ATR contains the information to identify the type of the card and the protocol that should be followed to communicate with the card. From now, the reader communicates with the card in that particular protocol. So obviously, if the terminal doesn't support the protocol required by a card then the reader will not be able to read the card.

After this the card will authenticate the reader and then the reader will authenticate the card. In this way a two-way authentication is established between the reader and the card.

A new session is then started. This will be followed with the normal operation. In this, commands and responses are exchanged between the reader and the card. When two computers communicate with each other, they exchange data packages, which are constructed following a set of protocols. Similarly, smart cards communicate with outside world using their own data packages, particularly consist of sets or units of commands and responses. This is what is called the Application Protocol Data Units (APDUs). After the required operation is done, the terminal ends the session.

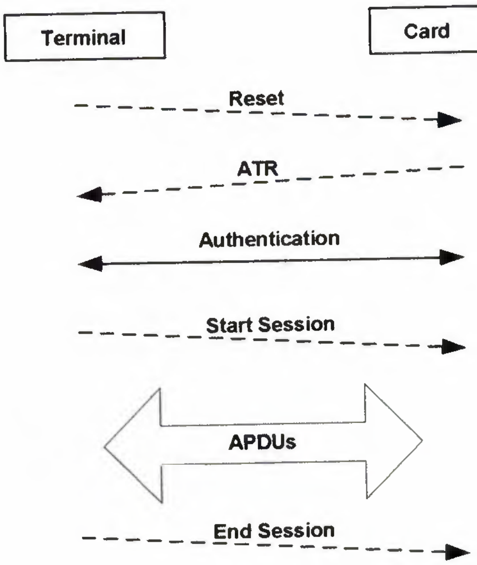


Figure2.1: Communication between card and terminal

2.3.2 Format of APDUs

All communication between a smartcard and smartcard reader is performed using he block protocols defined in the ISO standard[14]. This protocol layer is implemented y the firmware inside the reader, so a software developer need only be concerned with the protocol used to communicate between the reader and its host computer (at the driver level), and for exchanging messages with a smartcard in the reader (at the application level). A typical protocol stack is shown in figure 2.2

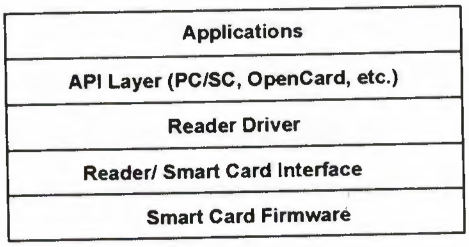

Applications
API Layer (PC/SC, OpenCard, etc.)
Reader Driver
Reader/ Smart Card Interface
Smart Card Firmware

Figure2.2: Protocol Stock for a Smart Card Environment

Each smartcard reader manufacturer is free to design whatever protocol they choose for communication with their hardware, so an important element in the high-level Application Programming Interface (API) design was to abstract away the manufacturer-specific protocol and provide a consistent interface through which all smart card readers can be communicated with. Similarly, smartcard manufacturers frequently implement proprietary features in their designs, but all cards provide the ability to exchange the APDUs described in the ISO standard.

It was decided that the smart card APIs can implement proprietary features provided there is a consistent method for the exchanging of Command APDU and Response APDU pairs.

To ensure cross-compatibility between different reader and smartcard implementations, standard interfaces and base classes were defined from which all manufacturer-specific classes must be derived. All communication with the smartcard is achieved by exchanging Command APDU and Response APDU classes through the Smart card Reader interface.

Thus, APDUs are packets of data that are exchanged between the CAD and a smart card. APDUs are the standard means of communication for smart cards. There are two types, Command APDUs which specify an operation to be performed by a smart card; and response APDUs which contain the smart card's reply (status and, optionally, data) to an operational request. The ISO7816 standard specifies that communication between a host application and a smart card is done through APDUs. An APDU is a packet of data that follows a specific format:

- A command APDU starts with a header and is optionally followed by a body. The header contains fields that specify the operation to be performed by a smart card. The body includes any data that accompanists the request; it also indicates the maximum number of data bytes expected in response to the command.

- A response APDU optionally begins with a body that contains any data returned in response. The response APDU ends with two mandatory bytes that specify the processing state of the card.

The following tables illustrate command and response APDU formats respectively. APDU structure is described in ISO 7816, part 4.

Command APDU						
Mandatory Header				**Conditional Body**		
CLA	**INS**	**P1**	**P2**	**Lc**	**Data field**	**Le**

Table 2.1: Command APDU

Response APDU		
Conditional Body	**Mandatory Trailer**	
Data Field	**SW1**	**SW2**

Table 2.2: Response APDU

The CLAss byte is used to indicate the class of the command, which determines whether Secure Messaging is being used. The INStruction byte determines which command is being executed, and two command-related parameter bytes P1 and P2 are also supplied. Lc contains the length of the Data parameter, and the Le field indicates the length of expected response data.

Every response APDU contains two status bytes SW1 and SW2 after the response data.

2.3.3 'T= ' Card Communication Protocol

When the card is first powered on, the card responds with an ATR indicating the type of communication protocol it is prepared to use. The standards have made provision for 15 possible data transmission protocols, each designated as a 'T = ' followed by a number between 1 to 15. Currently two protocols T=0 and T=1 are most commonly used.

The T=0 is an implementation first used in the French pay phone system which was later standardized. Its adoption by other phone companies (example GSM) has given it a boost and is by far the most common protocol in use today. It was designed for early systems and used a simple byte-by-byte transmission technique that had minimum memory requirements. The T=1 protocol uses a block (a sequence of bytes) during its transmission and is more suited for secure messaging and modern sophisticated interfacing devices. The T=14 is used in Germany payphones and the remaining protocols are not yet defined or are in the process of being prepared. The EMV standard addresses both T=0 and T=1 protocols.

Some readers are designed to handle only one type of protocol, whereas others are designed to automatically switch protocols and handle both types of cards. When selecting a card it is usual to adopt the T=1 protocol unless there is a requirement to use T=0 cards to maintain compatibility with the terminal infrastructure.

2.4 Smart Card Operating Systems

In this section I will cover the well established file system cards and then concentrate on the new operating system structure, which support multi-independent application code development. The new operating systems, Java Card, MultOS and Smart Card for Windows, are the primary candidates for multi-application.

2.4.1 Multi-Application Frameworks

Smart Cards were primarily used for authentication, and they have been changing the way in which authentication is carried out. But this is an under-utilization of the resources on the card. To make efficient utilization of the resources, more than one application can be hosted on the card to make it a multi-purpose card.

To achieve this, there should be support both at the card-level and the card terminal-level. This supporting infrastructure is called a Framework. This Section of this project work aims at comparing different Frameworks, which are currently available in the Smart Card industry. Frameworks can be classified into three types, based on the level at which they are providing the necessary infrastructure. They are:

2.4.1.1 On-Card Frameworks

They provide the necessary infrastructure at the card level. They define the architecture of the card in such a way that multiple applications can be hosted securely on the same card. Care should be taken that one application on the card cannot adversely affect the operation/existence of other applications residing on the same card. Examples of these include:

- Java Card
- MULTOS
- Windows for Smart Cards

2.4.1.2 Off-Card Frameworks

They provide the necessary infrastructure at the terminal level. They should also deal with issues at the management level. This framework should be able to support different policies followed by the card issuer. The card issuer should be able to allow/disallow specific applications to be hosted on the card. To achieve this, the framework should maintain a repository of information to allow inter-operability of the cards. Examples of these include:

- Open Card
- PC / SC
- eESCC
- NICSS

2.5 MULTOS Operating System

2.5.1 Introduction

This section will provide an overview of the MULTOS OS from the technical point of view. It will introduce important aspects of the technology of smart cards operating systems in general, as they are described in standards, and it will show how these are implemented in the MULTOS platform.

This section begins with introducing the smart cards files and the file structure of the MULTOS OS. It will talk about the different types of files and applications and the different ways to refer to them. Then, it will talk about how the communication is achieved between them and the reader devices. Finally, it will mention the fundamental commands that MULTOS uses to handle files and communications.

It also will talk about the MULTOS Application Abstract Machine (AAM) and its meaning, and show how the AAM defines the memory map that all MULTOS applications see. It will provide an overview of the memory architecture in MULTOS and the way applications and data are placed and referenced in memory. Finally, it will provide a short introduction to some features of the MULTOS Executable Language (MEL).

MULTOS as was mentioned stands for Multiple Operating System. It is an operating system for smart cards and it allows multiple application programs to be installed and to run on the same card securely and independently. In the past, smart card systems did not allow inserting various application programs on one smart card. Also, they could not delete the old application program and then add a new one to replace it as well. So, separate smart card for each application is necessary. But with MULTOS, several application programs, updates and patches can all be installed in a smart card and all the installed programs are separated from each other simultaneously and securely.

By using the virtual machine, each application program can be installed to the platform independently. Besides, to allow application programs written by different standards store and run on the same operating system and smart card, a standard API between the operating system and application programs is established.

Normally, MULTOS application programs are written in the C and Java programming language; but to assist application developers in writing applications to run on MULTOS, MULTOS Executable Language (MEL) was developed, which is a Reduced Instruction Set Computer (RISC) language specific to MULTOS.

On the other hand, firewall systems have been installed to ensure information cannot be accessed without authorization. Each new service or application is kept rigorously separate by the firewalls from any other program already on the card, so that the operation of one application cannot interfere with the operation of the others.

Thus, service providers do not need to co-operate, trust each other and share the information of cardholder, and this can provide the highest level of security for the cardholder. Besides, security is provided by a requirement in MULTOS implementation license, which requires all the MULTOS silicon providers to prove security, tamper resistance and interoperability by passing a rigorous testing and evaluation process.

MULTOS is licensed openly and controlled by MAOSCO Consortium, which is a group of leading international organizations, such as Fujitsu, MasterCard International, Mondex International, Europay International, and Discover Financial Services.

Due to the open nature, this allows anyone to issue MULTOS smart cards, write application programs, implement the operating system on a specific chip, manufacture smart cards or provide value added products, which support MULTOS.

2.5.2 The MULTOS Card's Architecture

The MULTOS card is a multi-application smart card and therefore it combines a microprocessor and memory in which different applications can be stored and executed independently and data can be stored and manipulated. In addition, applications in a MULTOS card are not only independent from each other but also from the underlying hardware. MULTOS achieves that by defining an architecture which consists of four layers, as the following picture shows.

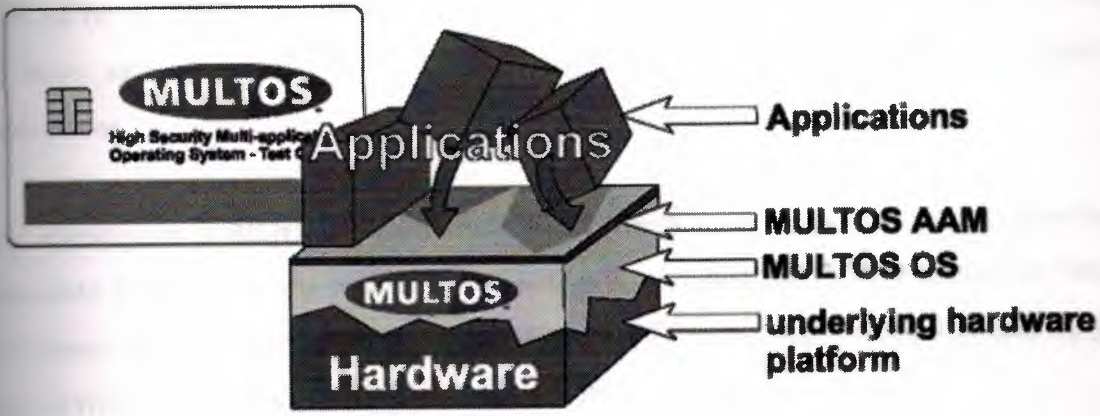

MULTOS
High Security Multi-applica
Operating System - Test C
Applications
MULTOS
Hardware
Applications
MULTOS AAM
MULTOS OS
underlying hardware platform

Figure 2.3: The MultOS Architecture

1. **Applications:** MULTOS can load and execute different applications. Each application is locked in its own memory space and cannot interfere with memory allocated in a different application. All MULTOS applications are executed in a language called MULTOS Executable Language (MEL) that is written in Assembly but applications can also be written in a high level programming language, such as C, and compiled into MEL.

2. **MULTOS AAM:** The Application Abstract Machine or Virtual Machine (VM) is sitting on top of the OS and provides an Application Programming Interface (API) that ensures that all applications will be executed the same way in every platform. The API contains a set of library functions and instructions that are called primitives. AAM provides this hardware independency by translating the MEL applications into MULTOS OS specific commands, which are then executed.

3. **MULTOS OS:** The MULTOS Operating System is sitting on top of the hardware and provides the communication between MEL applications and the underlying silicon hardware through the AAM. It also performs the memory management by handling the loading, deleting and executing of the applications.

4. **Hardware:** The hardware platform consists of the microprocessor and the memory. The memory has volatile and non-volatile modules. Volatile memory, such as RAM, looses its data when the electrical power is turned off whilst non-volatile memory, such as ROM or EEPROM, can retain the data even though no electricity is provided to it. As we have said, the AAM hides the differences of the hardware from the actual applications.

The memory in a MULTOS card and in any smart card in general is not directly accessible by the operating system. Instead, files are created and the OS uses these files to interact with the memory, such as in any modern PC operating system. The following section will describe the MULTOS OS file structure.

MULTOS is a multi-application operating system that runs on a variety of smart card hardware platforms from different manufacturers. This operating system is burned into the silicon chip at the time of manufacture. More specifically, the operating system is stored in the ROM of the chip. MULTOS consists of the Kernel and a Virtual Machine, where applications run. Figure 2.4 illustrates the construction of MULTOS card.

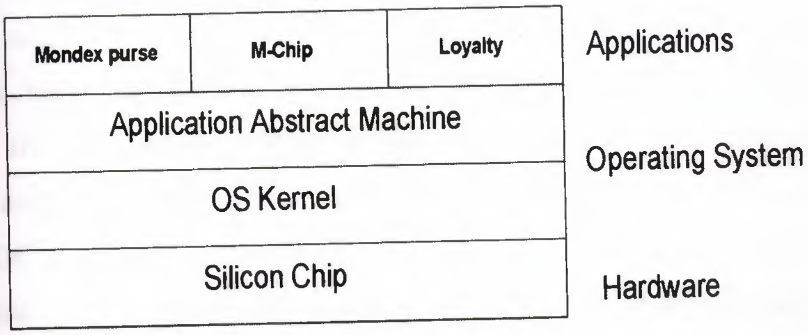


Figure2.4: Construction of MULTOS Card

2.5.3 MULTOS File Structure

The ways files are organized in MULTOS derive from the standard smart cards file structure as it is defined by ISO 7816-4. Thus, it is important to examine the manner in which the smart card files are organized in general and then extend this to the MULTOS file structure.

2.5.3.1 Smart Card Files

The file structure in a smart card in hierarchically organized in a similar way is on a PC. Therefore, there is a root directory, which can store data files and executables or sub-directories. ISO 7816 defines three types of smart card files: *Master Files (MF)*, *Elementary Files (EF)* and *Dedicated Files (DF).*

The root directory is a Master File (MF). The MF is the highest-level file and all other files are either in the same level or in sub-directories. The Master File is the one that is selected when the smart card is powered or reset except for the case where a shell application has been placed to the root level, which logically replaces the MF and is selected instead.

Elementary files are the data files. There are different types of Elementary Files according to the logical structure they adopt but all of them serve one purpose and that is to store data. The Elementary Files cannot have child files within them. They can abstractly be though as the ordinary files that a modern OS uses.

In a similar way, a Dedicated File can be though as a directory, which contains other files that can be either Elementary or Dedicated files as well. In addition, executable applications are also dedicated files. In ISO 7816, there is not a distinction between executables and directories since in reality there doesn't have to be a command that executes a DF. Logically, when a DF is used as a directory it seems as it holds other files but these files are considered rather embedded in it than belonging to it. The following diagram shows an example of the file structure that smart card banking application can have.

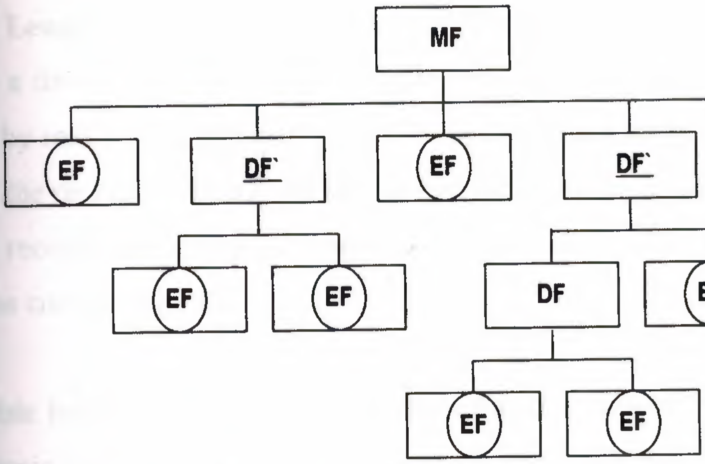


Figure 2.5: ISO 7816 File Structure

MF: The root directory. It contains all the applications directories. Note that in a multi-application smart card (like MULTOS) it can contain more than one sub-directory.

DF`: The main directory of the application. It contains all the executables and data of the application.

DF: Those DFs are sub-directories of the application and can represent different accounts for a banking application.

EF: represent data files of each DF, can be account information for instance. Elementary files can have different logical data structures and therefore the way that data are organized within them can vary. ISO 7816 defines four different types of Elementary Files:

1. **Transparent:** A transparent file is the most simple to understand since it has no structure at all. The data within it are just a block of continuous bytes and are read or written by specifying an offset and length in the file. The programmer must specify a special character to separate logical records in a transparent file. The ISO 7816 *Read Binary* command can be used to access a transparent file. Within MULTOS the ATR (Answer to Reset) file (and not the command) is a Transparent file.

2. Fixed Length: A fixed length file is divided in a number of records that each of them has a fixed length. Data in a fixed length file are organized in those records and accessed by reading a number of bytes from each record using the record number. The length of the records is usually limited to 255 bytes and so is the number of records in a file. The record numbers are enumerated from 1 where the record number 0 usually defines the current record.

3. Variable length: A variable length file is the nest step where data are organized in records again but this time the record length is not fixed. The length of one record can be different than the length of another record and therefore, this kind of files can manage the memory in a more efficient manner. The number of records is, again, often 255 bytes but unlike fixed length files, reading a number of bytes in a record accesses the data in a variable length file. The usual way to implement that is through Tag Length Values (TLV) records.

The Tag Length Values are a method to store data and reference to them. Each value represents a piece of information, which contains three fields. The first is the *Tag,* which specifies what the information relates to (e.g. it may be the Application ID). The second is the *Length,* which specifies the number of bytes of the value associated with the Tag and the third is the *Value,* which represents the value itself. For example the TLV [13,02,15,21] is used to store *02 bytes* of the *tag 13* and these bytes are *15 and 21*. In a similar way when you want to access data, you define the tag and the length of the data and the values are returned.

4. Cyclic Files: Cyclic files are similar to the fixed length files with the difference that after the last file is parsed the pointer shows back to the first record. In this way the programmer can overwrite records in a cyclic file once he reads the eof (end of file). A 'ten record' cyclic file, for instance, holds information for the last 10 records. A programmer can implement this to ordinary fixed length files as well by using a programming technique. Therefore, cyclic files are not used in MULTOS.

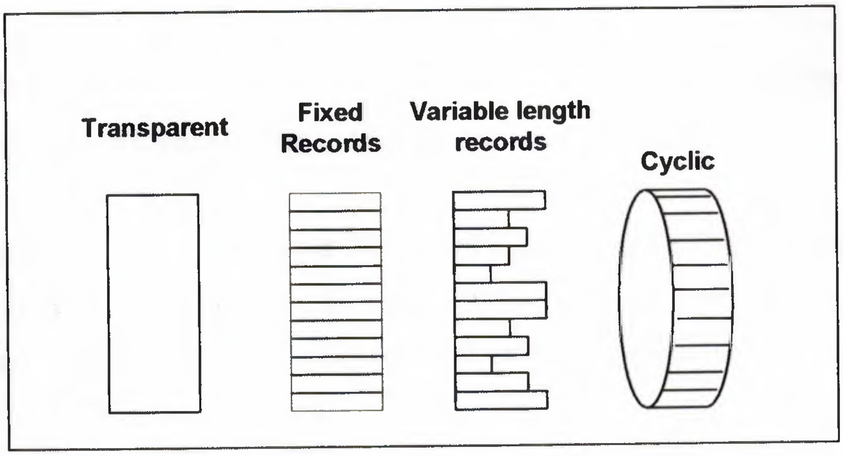


Figure: 2.6 Smart Card File Types

Moving now to have an idea about the MULTOS file structure after discussing the way the smart card and its several files are structured according to the ISO standard.

MULTOS does not support a hierarchical file structure on the card. The MULTOS file structure consists of a Master File, a DIR File, an Answer to Reset (ATR) File, and the Applications

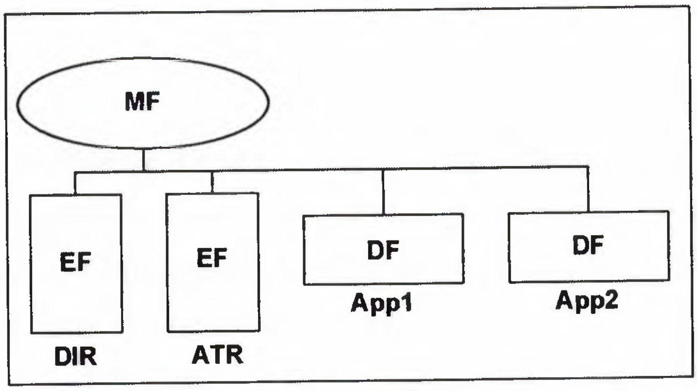


Figure 2.7: MULTOS File Structure

1. **DIR File** This is an Elementary File maintained by MULTOS. It contains information on the applications that have been loaded onto the card, such as the Application ID. This information is stored in records, one record per application, which are ordered in the same sequence as the applications are loaded. This file is readable by applications and terminals, but not editable.

2. ATR File The Answer To Reset File is an Elementary File maintained by MULTOS. Each application is granted an entry in this file.

3. Application This is a Dedicated File, formed by the code components where the executable code is stored in binary format, and the data component where the data for the application is stored in a free format. In MULTOS, an application may be:

- **Standard** This is the normal type of application, where an active file section is required.
- **Shell** This is a standard application that is implicitly selected instead of the Master File once loaded.

The basic level of file access in MULTOS is:

1. Select Master File.
2. Select DIR File.
3. Read Application ID.
4. Select Application.

2.5.4 Application Development and Loading in MULTOS

In today's fast moving business world, new applications are developed in as little as 3 to 4 months. Given the card life cycle of up to 3 years, it is desirable to update code or to add new applications after a card has been issued.

The MULTOS operating system allows for loading, updating or deleting applications on the card throughout its use. This ability has a number of implications for security, which are discussed in greater detail in subsequent chapters. To protect the operating system and other already loaded applications from rogue code being transferred, a card issuer may insist on a secure environment for the loading process.
The card issuer or cardholder should be able to authenticate and trust the application issuer and the downloading station.

MULTOS "focuses on very tight control by the card issuer of everything that happens to the card". New applications must be approved of and digitally signed to maintain control by the card issuer. The loading process is illustrated in Figure 2.1.

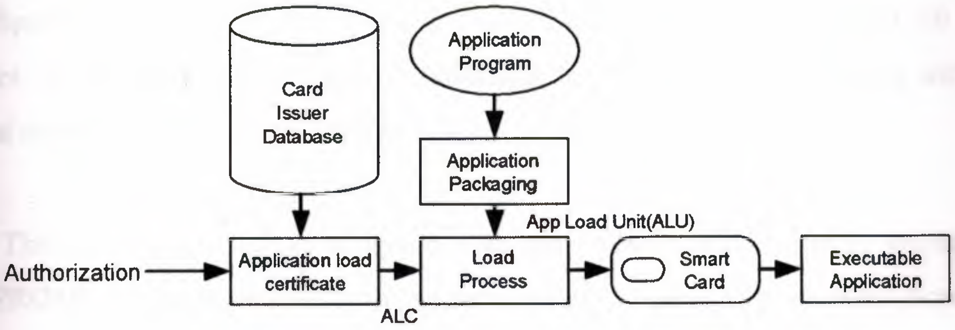


Figure 2.8: Application Loading Procedure

MULTOS makes use of public key infrastructures and digital certificates from card issuers for verification purposes. All applications are verified, although not in content but at least in terms of origin, before loading onto a card. A multi-application card management system is employed to monitor, control and manage applications and associated versions on each card. The concept of "firewalling" is supposed to prevent applications from overwriting or accessing each other.

2.5.5 Application Abstract Machine (AAM)

Operating System Services are available to application programs in the form of an Application Abstract Machine (AAM), which in turn, is a virtual, hardware-independent target platform implemented in software.

This virtual platform enables developers to write applications that are portable across all MULTOS implementations without knowing anything about the actual underlying hardware. Applications are written in MEL, or in a higher level language (C or Java) which is then compiled into MEL. The AAM consists of three sections:

1. **Memory** The AAM provides each MULTOS application with its own memory space to hold code and data. Its architecture defines two independent memory spaces:

- **Code Space** This is a block of memory that contains the application's byte code. It consists of up to 64K bytes of contiguous, non-volatile store (usually EEPROM), addressed from 0. This space can only be executed.

- **Data Space** This is a block of 64K, addressed from 0 to 65535 using a 16 bit Segment Address that has no direct relationship to the location of the data within physical memory. This space is divided in three areas:

- **Static** This area contains all of an applications non-volatile data (currently stored in an EEPROM). This area is private to the application and cannot be accessed directly by the terminal or any other application. Applications are allocated a fixed static area when they are loaded onto the MULTOS card, the size of which is specified by the Application Load Certificate.

- **Public** This area is used by the application to communicate with terminals and other applications, and it is held in the RAM.

- **Dynamic** This area is an application's volatile data area, held in the RAM. It is private to an application; it cannot be accessed by terminals or other applications. This area is divided in two parts:

- **Session Data** This part is located at the bottom of the dynamic area, and it represents local variables for the application. Its size is fixed when an application is loaded onto a MULTOS card. The exact number of bytes of session data that an application requires is specified by the ALU and ALC.

- **Stack** This part is located at the top of the dynamic area. Its size is fixed by the amount of physical memory available and does not have to be reserved by an application.

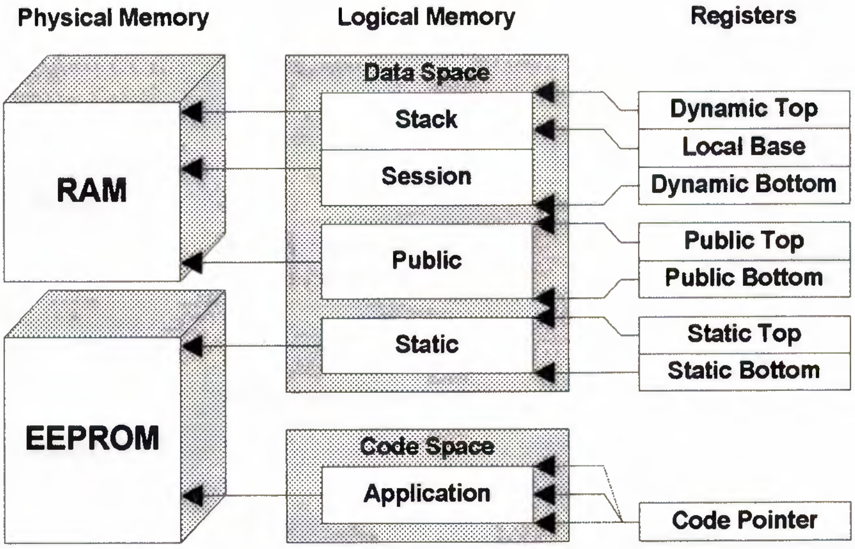
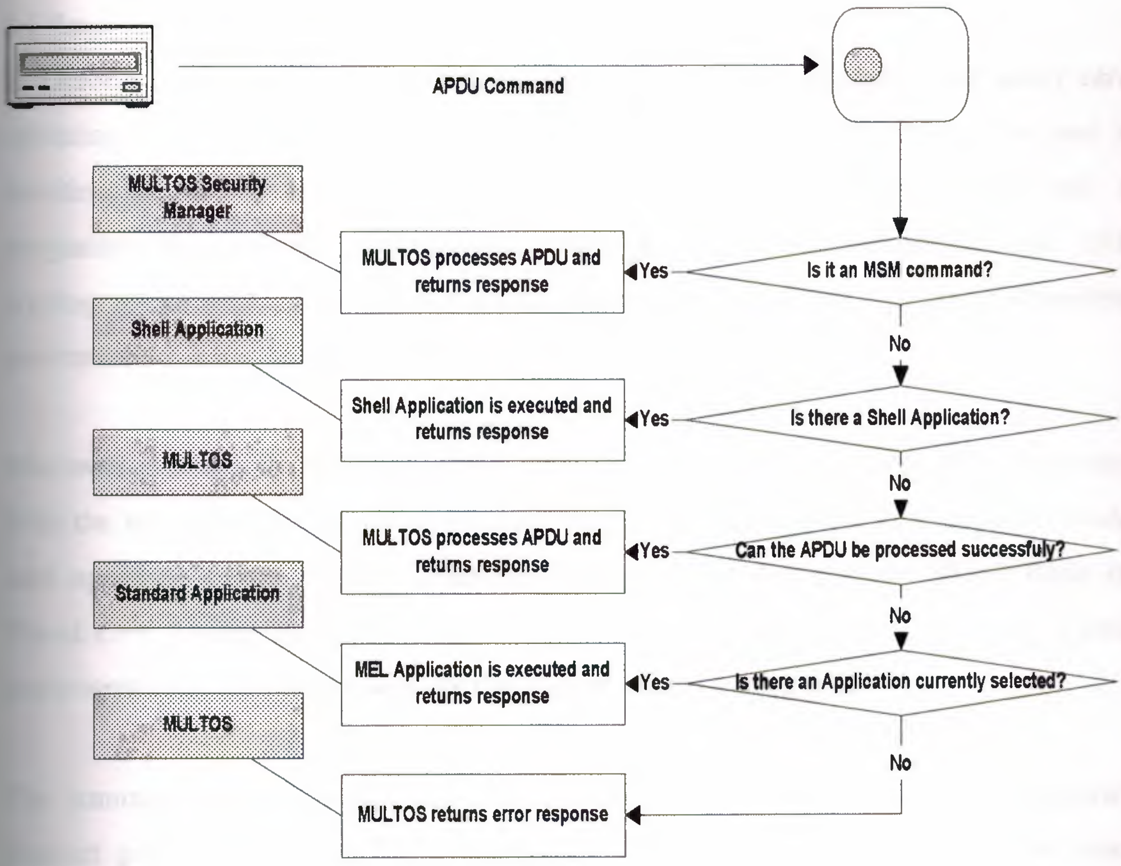


Figure 2.9: MULTOS AAM memory architecture

2. **Registers** Nine registers are provided by the Application Abstract Machine. Seven address registers and two control registers. Tagged Addressing is used by MULTOS to allow applications to access memory. This method consists of an address register and an offset. The address register points to the top or to the bottom of each memory area, and the offset refer to a relative address within the memory area. The register's value is provided by MULTOS, whilst the offset is provided by the application developer.

3. **Input Output (I/O)** The I/O architecture for a smart card is based upon a command-respond pair. The terminal sends a command to the smart card, which in turn, processes the command and returns a response. The handshake is always initialized by the terminal. When a smart card is powered on, it replies to the terminal by sending a string of bytes, referred as the Answer to Reset (ATR). Once the ATR has been processed, and any negotiations over communications protocol have been performed, then commands may be sent to the smart card.



APDU Command
MULTOS Security Manager
MULTOS processes APDU and returns response
Yes
Is it an MSM command?
No
Shell Application
Shell Application is executed and returns response
Yes
Is there a Shell Application?
No
MULTOS
MULTOS processes APDU and returns response
Yes
Can the APDU be processed successfuly?
No
Standard Application
MEL Application is executed and returns response
Yes
Is there an Application currently selected?
No
MULTOS
MULTOS returns error response

Figure 2.10: Command Routing in AAM

These commands are sent in packages called Application Protocol Data Units (APDU). When an APDU is sent to the smart card, MULTOS determines where this APDU will be processed. Either MULTOS will process the command, or the command will be routed to an application for processing (Fig. 2.9). The sequence of checks that are carried out to determine where the command APDU is processed is called Command Routing.

2.6 Smart Card for Windows

In October 1988, Microsoft announced that it would enter the market of smart card operating systems with a new product called Smart Card for Windows. The card is combination of a traditional ISO 7816-4 compliant operating system and a programmable platform. The core provides a file system, access control. I/O, cryptographic services, an API and a selection of ISO commands. An optional runtime environment allows the addition of custom-developed application.

Microsoft provides the developers with all components needed to write the application. With the smart card for Windows product, Microsoft enables other companies to create card operating system using a Windows based smart card toolkit for Visual Basic or Visual C++. Using this toolkit, the developer can select the desired operating system components and then creates a mask that can be loaded onto a card.

The command set is customizable. The first version of the smart card for Windows product provides ISO and EMV commands; GSM commands are planned for later release. The file system of a Smart Card for Windows is based on a reduced version of the DOS FAT file system. The number of partition and the partition size can be set during creation.

An extensive list of cryptographic services is available for the developer to select. The internal API is language-neutral. The first version of the Runtime Environment is Visual Basic interpreter; the support of C++ is planned. This Runtime Environment provides the flexibility and advantages known also from Java Card and Multos

2.7 Java Card Overview

2.7.1 Introduction

Smart cards have been available for a while but a standard to unify cards of different vendors has been missing. Java Card provides smart card vendors and users with technology that allows flexible use of smart cards with Java application interface.

To date, card manufacturers have developed their own proprietary solutions and programming languages for the smart card environment. The wide range of possibilities in smart card applications has given rise to the need to develop a commonly accepted solution, which can be used for developing applications that suit the smart cards of all manufacturers. The Java Card has been designed for this purpose, and all interested parties in the field have been able to take part in the standardization process.

The Java Card specifications enable JavaTM technology to run on smart cards and other devices with limited memory. The Java Card API allows applications written for one smart card platform enabled with Java Card technology to run on any other platform. The Java Card Application Environment is licensed to smart card manufacturers, representing more than 90 percent of the worldwide smart card manufacturing capacity.

Using Java technology in smart cards introduces several benefits. First, Java Card technology applets will run on all cards developed using the Java Card Application Environment and multiple applications can run on a single card. Besides, the installation of applications provides card issuers with the ability to dynamically respond to their customer's changing needs after the card has been issued and the Object-Oriented methodology of the Java Card technology provides flexibility in programming smart cards. Finally, the Java Card API is compatible with formal international and industry-specific standards.

Particularly, a Java Card is a smart card that can load and execute programs written in Java. Thus, a Java Smart Card is a credit card sized device which stores and processes data via the integrated circuit containing microprocessor and memories embeds inside a plastic card. Java smart card is I/O capable so it can communicate with the outside world.

The major difference between Java smart card and conventional smart card is that Java smart card is specified for running under Java programs whereas conventional smart cards use programs written in other languages

This is a new approach with smart cards. The traditional smart card only contains user data files; the programs that execute in the card are already provided by the operating system vendor. The Java Card tries to solve some of the shortcomings of the traditional smart cards

Today, smart cards applications are written in languages that are proprietary to smart card vendor and do not interoperate. This is a great obstacle for the wide acceptance of smart cards. The "write once, run anywhere" capability of Java offer a solution to this problem. The Java Card Application Programming Interface (API), which is based on an open API that is available to the entire market, will run on any Java-compatible cards. Therefore applications written using this approach will run everywhere a Java smart card is found.

Instead of just a small handful of specialist programmers that was available before, hundreds of thousands of Java programmers can now use the existing development environments to write applications for Java smart cards.

Previously, an application written in assembly language, compiled into machine code and burned into a ROM could take up to a year to debug and deploy. The interpreted nature of the Java language allows applications be written and trailed in a matter of days, eliminating the mask creation cycle required for conventional smart card projects. This approach speeds up and simplifies the development of smart card applications.

Conventional smart cards can only be used in applications they are originally designed for. A Java smart card has the ability to upgrade and load in new applications by downloading Java applets. Applets are small code objects that are small enough to fit several into the limited memory of smart cards.

Java is a secure language. It ensures applets from different sources work and play well with each other on a smart card. Data considered private by one applet will not be accessed by another. Also, the Java Card API insists that any applet be cryptographically signed by the card issuer. This ensures rogue applets are not accepted by a card, reducing the risk of hackers breaking into the card.

2.7.2 Java Card Architecture

A Java Card is a smart card capable of running Java programs. As shown in the Figure 2.11, Java Card VM is built on top of a specific integrated circuit and native operating system implementation.

The JVM layer hides the manufacturer's proprietary technology with a common language and system interface. The Java Card framework defines a set of API classes for developing Java Card applications and for providing system services for applications. A specific industry or business can supply add-on libraries to provide a service or to refine the security and system model.

Like in Internet, Java Card applications are called applets. Multiple applets can reside on one card. However, it's important to keep in mind that smart cards are not personal computers. A smart card has limited memory resources and computing power. Java Card is not simply a stripped-down version of the JDK.

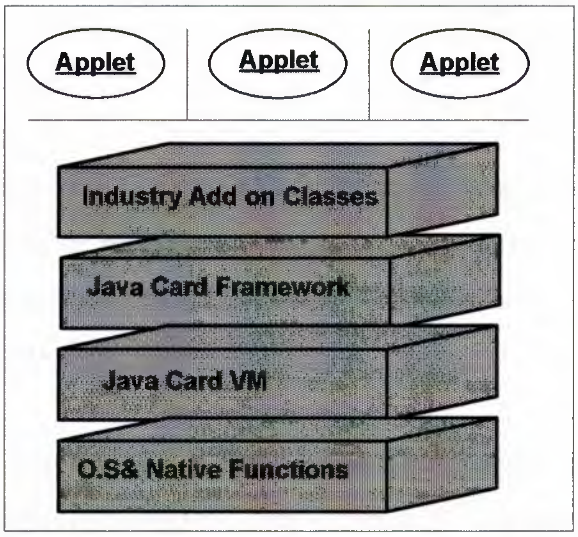


Figure 2.11: Java Card System Architecture

The JVM is implemented in the Java Card's ROM. JVM controls access to all smart card resources, such as memory and I/O, and thus essentially serves as the smart card's operating system. The JVM executes a Java byte code subset on the smart card, ultimately providing the functions accessible from outside, such as signature, log-in, and loyalty applications. Figure 2.11 shows the various layers of Java card software implementation.

2.7.3 Life Cycle of Java Smart Card

The lifetime of a Java Card starts when the native OS, Java Card VM, API classes libraries and optionally, applets are burned into ROM. This process of writing permanent components into the chip is called masking. After masking, the Java Card goes through initialization and personalization. In initialization, general data is loaded into card's non-volatile memory.

This data is not specific to individual; an example might be the manufacturer's name. Personalization involves assigning a card to a person. Both physical and electronic personalization can occur. In electronic personalization, for example, your personal key, name and pin number are loaded into the card's non-volatile memory.

At this point, the Java Card is ready for use. An issuer or retailer distributes the card. Cards sold by a retailer are general-purpose, in which case personalization is often omitted. Now you can insert your card into a reader and send commands to the applets residing on the card or download more applets or data onto the card.

The Java Card's internal JVM boots up, when a smart card terminal activates the hardware and establishes communication with the card. Physical lifetime of a card ends when the card is expired or blocked due to an unrecoverable error. An unrecoverable error may occur for instance when the card is broken physically or someone attempts to hack the card and security features blocks the data.

Unlike Java on workstations, Java Card Virtual Machine runs forever. Most of the information must be preserved when the card is removed from the reader. JCVM creates objects in EEPROM to hold the persistent information. When the power is not provided, the VM runs in an infinite clock cycle.

An applet's life time starts when it is properly installed and registered with the system's registry table and ends when it is removed from the table. Space of a removed applet may or may not be used depending whether garbage collection is implemented on the card. An applet is in an inactive stage until it is selected by terminal. Objects are created in the persistent memory, for example in EEPROM.

They could be lost or garbage-collected if other persistent objects do not reference them. In any case, it's a thousands times slower to write to EEPROM than RAM. Temporary objects are created into RAM. They are accessed frequently, and their persistence is not needed. Temporary objects disappear outside the card reader.

2.7.4 Java Smart Card Security features

One of the most important aspects of Java is that it is a secure language. It provides data integrity and security by deterring malicious programs. Similar to other object oriented programming languages like C++, Java provides access control to methods and instances of variable. Access to all methods and instances of variable are controlled through access modifiers, which define a level of access control for each method.

A method can be declared to be public, protected, private or private protected. A public method is accessible by any class, a protected method is accessible by methods in the same subclass or package, a private method is only accessible by corresponding object methods and a private protected method is only accessible by subclasses. These rules help to secure the system by restricting the access of critical objects by entrusted codes.

Java is a strongly typed language and is more strongly typed than C++. It allows for extensive compile-time checking for potential type-mismatch problems. All references to methods and variables are checked to ensure that the objects are of the appropriate type, preventing the forging of access to objects to get around the access control.

The compiler also checks to make sure that the program does not access any uninitialized variables. This mechanism further protects the smart card from malicious programs. The Security Manager class is not supported on Java smart card. Language security policies are implemented by the Virtual Machine itself. The Java Card Virtual Machine (Java Card VM) checks every Card byte code every time it is executed.

This ensures that the code is well formed – that it does not overflow or underflow the stack or contains illegal byte codes, for example. The Java Card VM also ensures a Java program on a smart card never escape from the Java smart card sandbox. A Java smart card sandbox is a program that runs Java programs.

When a Java program is running in the sandbox, there are a number of restrictions on what it can do. For example, it has no access to the local file system. If the Java program tries to do anything it is not authorized, the sandbox will stop running it. This restricts the data that is available to a program and keeps one program from interfering with another. There are no pointers which can be access by the programmers or users, so malicious programs cannot forge pointers to memory

2.7.5 Java Card Applications

Java Card Runtime Environment (JCRE) refers to the Java Card virtual machine and the classes in the Java Card framework. Each applet within the Java Card are associated with unique applet identifier (AID).

After an applet is loaded and linked with libraries on the card, JCRE calls the applet's install method as the last step in the applet installation process. An applet is ready to use. It remains inactive until it is explicitly selected by sending a select applet signal. A Java Card applet is compiled using a regular Java compiler. The compiler output is input into Java Card converter which enforced Java Card subset compliance, performs name resolution and initial address linking, and optimizes the Java byte code to be suitably running on a Java Card VM.

With increased security functions, a Java Card can be used as stored value card, credit/debit card with reduced transaction costs. Because Java Card allows the storage of information about multiple applications, it can be used to access all the accounts of a customer, reducing the number of cards needed.

Cardholders can dial the bank and download some money onto the stored value cards when needed. With the development of Java Cards, the cashless automatic teller machine could be a mobile phone, a par TV set-top box, an Internet kiosk, a home PC or a merchant's terminal.

As well as carrying information about the telephone number of the cardholder and the suite of services it can access, a Java smart card provides the necessary encryption functions to ensure security of the subscriber's account and protects the mobile phone from fraudulent use. The card can be upgraded by downloading new functions to the card in real time.

A Java smart card can provide a portable, customized health care file with medical emergency data, personal identification and insurance information. It reduces paper work and streamlines insurance payments. With different levels of access to the card, more information can be added for emergency purposes, while retaining confidentiality.

Purely software-based security is inadequate when passwords are guessed, stolen or hacked. With combination of a password and smart card based authentication, users have additional protection for their information. By inserting the smart card and entering a PIN number, the computer can determine the access rights of a user to a computer network. This helps prevent unauthorized access to the network resources.

The operating system is the software component that manages the hardware's resources such as the various types of memory, the CPU, as well as the flow of data between all the subparts of the chip. There are many types of operating systems, which can differ in their architecture:

- *Integrated systems,* in which case the user applications and the system applications are mixed in a single cumbersome piece of software. Old fashion development style and is difficult to maintain.

- *Exokernels,* which are a different approach that tries to offer the most direct and flexible access to the hardware from the application. The basic idea is to put the thinner logical layer between the applications and the hardware. The OS is in charge of authorizing the application but it does not get involved in the way in which the application accesses the resources.

- *Virtual machines, which* provide a great level of abstraction, add an extra logical layer between the user application and the hardware. One of its most remarkable features is portability. The use of high-level language to develop its applications makes development easier, faster and cheaper.

Each one of these solutions offers a particular response to security issues in smart cards. However is it quite safe to say that the most widespread model in use is the last one.

The application, the most visible part, it offers a service to the cardholder; its implementation depends entirely in the operating system on which is going to run. To achieve a maximum level of security it is crucial as in any other information system to consider the security in its globosity, not underestimate any part of the smart card in its role in the security of the whole system.

2.8.2 A Classification of Attacks on Smart Cards

In order to provide a global view of tactics adopted by attackers, it is convenient to classify them in some categories, Figure 2.12 below, gives us an overview.

Obviously, the attacker has a broad range of tactics to choose from, and is not limited to a single choice. He can easily combine them to increase his chances to achieve his goal.

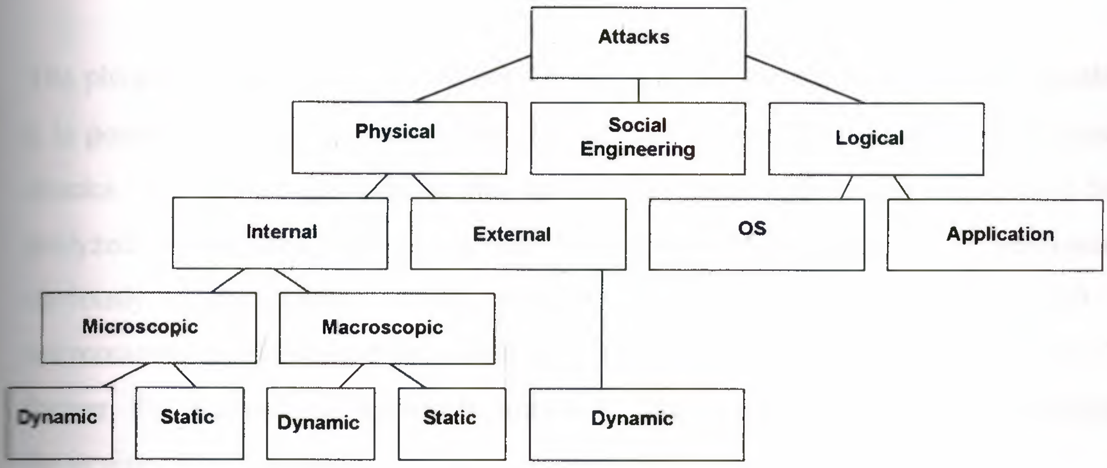


Figure2.12: Attacks on Smart Cards

1. Social engineering: attacks are by all means the most effective and cheap way to obtain confidential information. The necessary technical knowledge is minimal; the only limit is the ingenuity and imagination of the attacker at exploiting the human being inherent weaknesses. The attack can consist of impersonation a system administrator, a bank employee, a policeman, or simply looking above the shoulders at the victim when the PIN is typed, or by stealing or replacing the smart card. There are an infinite of possibilities.

2. Physical attacks: are probably the most difficult to achieve. The target the first two components from Fig 1.x mentioned earlier: The card body and the chip itself. Attacks on the body of the card are quite straightforward and is only the first step in a further analysis of the chip. On the other hand, the physical attacks on the chip itself offer a very large spectrum of possibilities. Most of them require a high level of knowledge and above all they require facilities that are only available in high-tech semiconductor laboratories, or affordable by very wealthy organizations.

The security provided by the card body can be easily defeated. The aim is to obtain a closer physical access to the chip for subsequent analysis. First the chip is removed from the card body with a sharp knife, and then the remaining resin epoxy particles can be dissolved by bathing the chip in fulmic acid citric (>98% NHO3). Finally, shaking the chip in acetone will totally clean the chip. Some people might think that this naked chip is entirely readable. Fortunately, secure smart cards, have many security features to prevent illegitimate access to the data that they hold.

The physical attack on the chip offers a broad variety of approaches. Roughly speaking, it is possible to split the attacks into two sub categories: internal and external physical attacks. The former depends on the size of the component of the chip that is being analyzed or modified. The attack can be qualified as macroscopic or microscopic, obviously a microscopic attack requires expensive and rare devices such has micromanipulators, focused ion-beam, high precision lasers, electron microscopes. The former, the macroscopic approach deals with components more humanly workable as far as size.

The necessary equipment is more common and cheaper. However, a wrong manipulation can easily physically destroy the chip. Both attacks can be realized dynamically or statically. In the first case, the chip is analyzing in real time when it is operating, in the other case, the chip's operating system is not running. The external attack involves a smart card reader-writer to communicate with the chip through its input output contacts. It does not consist in uploading or downloading any piece of software. It just sends selected unusual sequences of electric signals and the exploits the output.

3. The logical attacks: Since the modern smart cards have all the basic components of a computer, they work in the same fashion. This means that certain kinds of attacks commonly used in computers are likely to work in the smart card world. At least in their basic principles, roughly speaking, they consist at downloading a malicious code, which is going to circumvent the protection provided by the operating system or the virtual machine, in order to interact with other application. Moreover they access protected memory addresses to read sensitive data they retrieve them through the card's input output contacts to the attacker's computer.

2.8.3 Description of the Most Common Attacks on Chips

2.8.3.1 Physical Attack

These attacks target platform weaknesses; they don't deal with flaws in design or implementation of operating systems or applications that run on top of them.

2.8.3.1.1 Internal Physical Attacks

To perform these analyses and or attack, a physical access to the internal component of the smart card is necessary. To do so, the chip has to be removed from the plastic card following the process previously described.

2.8.3.1.2 Internal Physical Microscopic Attacks

The equipment involved in such an attack ranges from light or ion microscopes, laser cutter micromanipulators and chemical etching installations. These equipments are beyond the reach of most people. Very few organizations are wealthy enough to afford them as well as the necessary expertise to use them.

Before attempting one of these attacks it is necessary to take away the chip from the plastic card as explained before. One possible target could be the internal structure of the chip. Fortunately due to its size, around 0.5, µm it is nearly impossible to extract any information from them. Nowadays standard lithographic manufacturing industries can easily produce such a thin structure.

Another interesting target is the RAM. It is widely admitted that what it contains is lost once the power supply is switched off. Some destructive techniques allow access their information on the RAM once the chip is switched off. This can be achieved when RAM is cooled to the temperature of –60 C°. Another option is to use electron microscopes in conjunction with contrast-enhancing processes to read (its physical state) directly the content of the RAM. An easy countermeasure is to keep sensitive data for the least time possible in the RAM, by overwriting at memory areas many times. Additionally it is possible to scramble the lay out of the memory to make the analysis of the memory meaningless.

2.8.3.1.3 Internal Physical Macroscopic Attacks

The smart card chip contains a more exposed target. The busses that carry the data from the CPU to the memory of the chip, by construction, are bigger, and therefore easier to physically tap on in order to get some valuable information. An efficient countermeasure is to scramble the layout of the busses to make the visual analysis harder.

An unusual feature of a smart card is that before being delivered to the final client it has to get through a number of tests in order to assure that it works properly. To do so the smart card is kept in a special state called test mode, in which it has additional functionality useful to analyze its state. Once this checking has ended, before the smart card is put in the field, a physical fuse is blown to switch the smart card into user mode with more restrictive functionality.

A potential attacker has a lot to gain by putting a smart card back into test mode. He can have access to a wealth of information because of the current state of the smart card. The practice is to physically bridge the damaged fuse to reverse the protective process. One countermeasure consists in handwriting the user mode state into the ROM, or making use of test pads during the fabrication process of the smart card. These solutions make the fuse useless.

2.8.3.2 External Physical Attacks

These types of attacks can be performed without use of rare expensive equipment like in the internal attacks. It is not necessary to remove the chip from its protective plastic card. The attacker only uses the chip's input output contact and other physical emission like electromagnetic radiations.

Some of the attacks that used to work on older generation of smart cards are by monitoring the energy input in the smart card. Varying the voltage or the frequency of the energy supply can force the chip to work in an unsafe fashion.

The chip is designed to work within a range of voltage values, as well as within a certain frequency, typically 1 MHz. Modern smart card check the values of energy input to prevent these attacks. Some sophisticated cards even have their own clock.

Measuring the variation of the temperature or the electromagnetic radiation of the chip while operating, though an accurate acquirement of such physical data is tricky and its interpretation even more tricky can also deduce some information.

A more popular and efficient attack is the so-called SPA (Simple Power Analysis). Basically it consists in measuring the current consumption of the CPU. This attack takes advantage of the fact that not all machine instructions are equals in term of CPU current consumption when executed. Hence by analyzing the current consumption the attacker can draw some relevant conclusions on which the CPU executes instruction. An even more sophisticated version is the DPA (Differential Power Analysis), which consists of the measuring of the current consumption of the CPU twice, first with processing known data, then unknown data.

The comparison of the results can lead the attacker to find out the content of the unknown data. Finally, the ultimate version of the current consumption analysis is the so-called HO-DPA (High Order Differential Power Analysis). It is very similar to the DPA but it takes more parameters into account such as electromagnetic radiation and temperature variation. These attacks are very serious threats, though a number of efficient countermeasures exist, by using hardware and software.

2.8.3.3 Logical Attacks

Modern smart cards offer the possibility to download new applications into them once in the field. This feature is very useful to better meet the ever changing needs of the customers in real-time. All it takes is to develop a new application, which perform the new functionality, then download it through a trusty terminal.

It is no longer necessary to replace all the smart card in the field. This provides a great responsiveness as well as a cheaper solution.

The drawback is that this feature also provides a world of possibilities to attackers. They can use this to perform an attack, which has proven to be highly effective in the field of conventional computers, the Trojan horse attack.

Measuring the variation of the temperature or the electromagnetic radiation of the chip while operating, though an accurate acquirement of such physical data is tricky and its interpretation even more tricky can also deduce some information.

A more popular and efficient attack is the so-called SPA (Simple Power Analysis). Basically it consists in measuring the current consumption of the CPU. This attack takes advantage of the fact that not all machine instructions are equals in term of CPU current consumption when executed. Hence by analyzing the current consumption the attacker can draw some relevant conclusions on which the CPU executes instruction. An even more sophisticated version is the DPA (Differential Power Analysis), which consists of the measuring of the current consumption of the CPU twice, first with processing known data, then unknown data.

The comparison of the results can lead the attacker to find out the content of the unknown data. Finally, the ultimate version of the current consumption analysis is the so-called HO-DPA (High Order Differential Power Analysis). It is very similar to the DPA but it takes more parameters into account such as electromagnetic radiation and temperature variation. These attacks are very serious threats, though a number of efficient countermeasures exist, by using hardware and software.

2.8.3.3 Logical Attacks

Modern smart cards offer the possibility to download new applications into them once in the field. This feature is very useful to better meet the ever changing needs of the customers in real-time. All it takes is to develop a new application, which perform the new functionality, then download it through a trusty terminal.

It is no longer necessary to replace all the smart card in the field. This provides a great responsiveness as well as a cheaper solution.

The drawback is that this feature also provides a world of possibilities to attackers. They can use this to perform an attack, which has proven to be highly effective in the field of conventional computers, the Trojan horse attack.

It consists of using a computer connected to a terminal to communicate with the smart card. Then through this terminal the attacker can download a malicious application into the smart card. Once running, this application can access protected memory areas containing sensitive data. All the difficulty lies in the defeating security functions of the operating system. Once this data is in the possession of the malicious application it can be sent back to the computer.

The malicious code could also perform modification in the EEPROM of the smart card, not just read protected information like in the previous case, but write in protected areas. It depends on the ability of the developer and the strength of the security of the operating system.

The countermeasure preventing these attacks depends on the security model implemented by the operating system and the type of the operating system.

CHAPTER THREE: SMART CARD SECURITY AND APPLICATIONS

3.1 Introduction

Smart cards have come to play an ever increasing role in our lives. We use them in electronic banking, to keep health care data, for mobile telephony, and in many other applications. The most important aspect of smartcards is their security, users and card issuers have to agree that the level of security provided by a smartcard platform is enough to prevent malicious or sly agents from abusing their trust in a card application.

Smart cards are used primarily in applications requiring high security, such facilities access or in applications handling sensitive information such as financial applications. Thus, a criminal could benefit financially by trying to break the security controls that are designed into a smart card. In this chapter, primarily, we will look at the security controls that are in place in a smart card, both in human-readable and machine-readable form, to prevent such attacks. By discussing security principles that are enforced by the smart card, we can provide an obvious vision of what cryptographic techniques to be applied so that privacy and authenticity concepts are ensured.

Smart cards have the richest tool set of security options available for cards. For multiple application cards, physical separation of data and firewall protection ensures that only authorized persons can access data and this protection can be implemented right down to each individual data field.

The cost of using paper, plastic or magnetic stripe credit, debit, or government benefit such as health cards, is that they are vulnerable to fraud. Smart cards will be more secure than the cards we carry now. The chips are hard to counterfeit. Tampering with the cards, such as trying sequences of personal identification number (PIN), can cause them to self-destruct. The personal lock on the card, the 'shared secret,' the PIN code or biometric, will mean there is less reason to steal them in the first place, as they can't be unlocked unless one allows the access codes to be known. As always, a user should not leave codes where others can find them. Smart cards can be used to securely store a person's passwords and codes.

The use of smartcards in security-sensitive applications heavily influences the design and handling of the card silicon and software alike. Microcontrollers used in smartcards are specifically designed to restrict access to stored information and to prevent the card from being used by unauthorized parties. To accomplish this, each microcontroller manufacturer includes its own set of security features, many of which are never discussed since they are useful only if potential hackers do not know that they exist.

Smart card devices are designed to work only in well-characterized operating environments, since one attack scenario involves attempts to force cards to operate outside normal operating voltage or clock frequency ranges, in hopes of uncovering weaknesses that can be exploited. Most devices therefore detect and reset whenever they are pushed outside their normal operating ranges. A card's reactions upon sensing attempt at fraudulent access range from ignoring the access request to locking up the card from all future use. Other features provide special functionality to areas of memory or make it difficult to access portions of memory or circuitry directly. Such techniques as memory-scrambling, hidden layers and dummy circuitry may be added to confuse hackers.

Since computers and networks are becoming so central to our lives in this digital age, many new security challenges are arising. This is the era of full connectivity, both electronically and physically. Smart cards can facilitate this connectivity and other value added capabilities, while providing the necessary security assurances not available through other means.

On the Internet, smartcards increase the security of the building blocks Authentication, Authorization, Privacy, Integrity, and Non-Repudiation. Primarily, this is because the private signing key never leaves the smartcard so it's very difficult to gain knowledge of the private key through a compromise of the host computer system. In a corporate enterprise system, multiple disjointed systems often have their security based on different technologies. Smartcards can bring these together by storing multiple certificates and passwords on the same card. Secure email and Intranet access, dial-up network access, encrypted files, digitally signed web forms, and building access are all improved by the smart card.

In an Extranet situation, where one company would like to administer security to business partners and suppliers, smart cards can be distributed which allow access to certain corporate resources. The smartcard's importance in this situation is evident because of the need for the strongest security possible when permitting anyone through the corporate firewall and proxy defenses. When distributing credentials by smartcard, a company can have a higher assurance that those credentials can not be shared, copied, or otherwise compromised.

Some reasons why smart cards can enhance the security of modern day systems are:

1. **Public Key Infrastructure (PKI) is better than passwords:** smartcards enhance PKI systems are more secure than password based systems because there is no shared knowledge of the secret. The private key need only be known in one place, rather than two or more. If the one place is on a smart card, and the private key never leaves the smartcard, the crucial secret for the system is never in a situation where it is easily compromised. A smart card allows for the private key to be usable and yet never appear on a network or in the host computer system.

2. **Smart cards increase the Security of Password Based Systems:** Though smart cards have obvious advantages for PKI systems, they can also increase the security of password based systems. One of the biggest problems in typical password systems is that users write down their password and attach it to their monitor or keyboard. They also tend to choose weak passwords and share their passwords with other people. If a smart card is used to store a user's multiple passwords, they need only remember the PIN to the smartcard in order to access all of the passwords. Additionally, if a security officer initializes the smart card, very strong passwords can be chosen and stored on the smart card. The end user need never even know the passwords, so that they can't be written down or shared with others.

3. **Two-Factor Authentication and more:** Security systems benefit from multiple factor authentications. Commonly used factors are: something you know, something you have, something you are, and something you do. Password based systems typically use only the first factor, something you know. Smart cards add an additional factor, something you have.

Two-factor authentication has proven to be much more effective than single because the "Something you know" factor is so easily compromised or shared. Smart cards can also be enhanced to include the remaining two features. Prototype designs are available which accept a thumbprint on the surface of the card in addition to the PIN in order to unlock the services of the card. Alternatively, a thumbprint template, retina template, or other biometric information can be stored on the card, only to be checked against data obtained from a separate biometric input device. Similarly, something you do such as typing patterns, handwritten signature characteristics, or voice inflection templates can be stored on the card and be matched against data accepted from external input devices.

4. Portability of Keys and Certificates: Public key certificates and private keys can be utilized by web browsers and other popular software packages but they in some sense identify the workstation rather than the user. The key and certificate data is stored in a proprietary browser storage area and must be export/imported in order to be moved from one workstation to another. With smart cards the certificate and private key are portable, and can be used on multiple workstations, whether they are at work, at home, or on the road. If the lower level software layers support it, they can be used by different software programs from different vendors, on different platforms, such as Windows, UNIX, and Mac.

5. Auto-disabling PINs versus Dictionary Attacks: If a private key is stored in a browser storage file on a hard drive; it is typically protected by a password. This file can be "dictionary attacked" where commonly used passwords are attempted in a brute force manner until knowledge of the private key is obtained. On the other hand, a smart card will typically lock itself up after some low number of consecutive bad PIN attempts, for example 10. Thus, the dictionary attack is no longer a feasible way to access the private key if it has been securely stored on a smartcard.

6. Non Repudiation: The ability to deny, after the fact, that your private key performed a digital signature is called repudiation. If, however, your private signing key exists only on a single smart card and only you know the PIN to that smart card, it is very difficult for others to impersonate your digital signature by using your private key.

Many digital signature systems require "hardware strength Non Repudiation", meaning that the private key is always protected within the security perimeter of a hardware token and can't be used without the knowledge of the proper PIN. Smart cards can provide hardware strength Non Repudiation.

7. Counting the Number of Private Key Usages: So many of the important things in our lives are authorized by our handwritten signature. Smart card based digital signatures provide benefits over handwritten signatures because they are much more difficult to forge and they can enforce the integrity of the document through technologies such as hashing. Also, because the signature is based in a device that is actually a computer; many new benefits can be conceived of. For example, a smart card could count the number of times that your private key was used, thus giving you an accurate measure of how many times you utilized your digital signature over a given period of time.

3.2 Smart Card Security

There are many reasons to use a smart card, but as we said earlier one of the main reasons is the built-in security features of a smart card. The microprocessor of the smart card has encryption keys and encryption algorithms built-in for performing ciphering/deciphering of data inside the card. The operating system file structure prevents the secret keys from being read from outside the smart card.

If multiple applications reside on the same smart card, they are protected from each other by a firewall between them. In addition to the smart card itself, a smart card solution needs to address total system security, which includes readers, terminals, network, and back-end processing systems. In other words, to ensure overall security it is necessary to do a total system design, which covers all the subjects that can be attacked by criminals.

During the design of a smart card; the risks involved versus the rewards of establishing strong security features must be evaluated, the expenses of implementing the solution against the exposure of suffering a security breach.

Smart cards are used primarily in applications requiring high security, such as facilities access or in applications handling sensitive information such as financial applications. Before I describe the security features of smart cards, I will briefly talk about magnetic stripe cards. It will give us a better perspective of what we gain in terms of security when we move from magnetic stripe cards to smart cards.

3.2.1 Magnetic Stripe Card Security

The data in the magnetic stripe is usually coded using two or three tracks. The standard covering this area is ISO 7811. The technique for writing to the tracks is known as F/2F. We can read from time to time in the news that some criminal has counterfeited some of these cards. The reason is that it is not that difficult and/or expensive to have the equipment to encode magnetic stripes. For this reason you can make as many copies as you want from a magnetic stripe.

As these cards are so widely used by financial institutions, a new way of encoding the stripe was developed, where it uses a magnetic material called high-coercivity (HiCo), as opposed to the low-coercivity (LoCo) material used before.

The HiCo material requires stronger magnetic fields to encode in it. Any card reader can read any one of these materials, since the encoding technique (F/2F) is the same. The security resides in the fact that not many encoding machines in the market can handle the HiCo material, and are definitely more expensive than those to encode LoCo material. The manufacturers of these encoders will certainly want to know why someone may be interested in purchasing such a device. Another good reason for using the HiCo material is that it is better suited to avoid local disturbances on the stripe due to magnetic fields and heat. Even if it very difficult to counterfeit a magnetic stripe card, it is far from impossible.

3.2.2 Smart Card Security Features

Some components that play a role in smart card security:

1· Human-readable security features

2· Security features of the smart card chip

3· Security features of the operating system

4· Security features of the network

5· Security features of the application

The fifth component will not be discussed in this document because the features selected are very dependent on the application program itself. The total system security is strengthened when all these components work in combination with each other. There should not be a "weak link" in the chain of security.

3.2.2.1 Human Readable Security Features of Smart Cards

There is often a need to include human-readable security identifiers on smart cards, where these features try to prevent smart card falsification. These features, of course, do not protect the data in the card. They prevent the misuse of the card as a badge identificator.

You may find some of these features in your credit card. These features are more important for the magnetic stripe cards than for the smart cards, since it is easier to alter the content of a magnetic stripe than the memory of a smart card. However, since many smart cards also have a magnetic stripe in the back, these features are also valuable for these cards. Here are a few of these features:

1. **Photo Lamination:** The smart card is personalized when issued to the cardholder with a passport-sized photograph of the cardholder. The photo would be laminated to the card. The security is embodied in the procedure followed before the photo is laminated. The cardholder must present the photo in person to a certified representative so that the cardholder's identity can be confirmed before the smart card is issued.

2. **Signature strip:** This is a very familiar feature on credit cards. A signature strip is bonded onto the card at manufacture. The cardholder must sign the strip using indelible ink when the smart card is issued. The signature cannot be modified nor the strip replaced without being obvious to the naked eye. Some credit card companies have electronic images of their customers' signatures on record and these signature images are indelibly printed onto the card when a new card is issued.

3. **Holograms:** This is another common feature found on credit cards. The holograms are bonded to the card at manufacture and cannot be separated from the card without destroying the substrate. The security feature of the hologram is based on the limited number of firms who can manufacture the hologram itself as holograms are expensive and complicated to be easily manufactured, and the difficulty in reproducing the hologram.

4. **Micro-printing:** This feature is ultra-fine printing that appears as a line to the naked eye but is visible under magnification. The printing itself is difficult to reproduce.

5. Embossing: This is another familiar feature of credit cards. The card number is pressed into the card, sometimes over the hologram for additional security, so that the numbers are raised above the surface of the card. An impression of the number can be transferred to paper using a machine. Unfortunately, as fate would have it, the position of the embossing marks called "domain 1" in the ISO 7811 specification can interfere with the smart card chip position defined in ISO 7816 specification

The domain 1 position is very familiar to credit card users because this is the location where the credit card number is normally embossed. There is no overlap between the domain 1 position and the smart card chip position but the stamping process can sometimes fracture electrical connections to the chip if care is not taken. Qualified smart card manufacturers have reliable embossing processes in place and there is no risk with embossing if such a manufacturer is chosen.

6. Security Patterns: This expensive process is otherwise known as "guilloche". It is the printing of very fine, interwoven lines onto the card substrate. This is a typical security feature on paper currency. The security feature is similar to holograms; they are difficult to reproduce and only a limited number of companies can perform this procedure. Printing of credit card company logos is a variation on this security mechanism. An additional requirement for credit card company logos is that the smart card laminating and printing process can only be performed by a limited number of registered and licensed firms. These firms must conform to very strict rules regarding the manufacture and shipping of the card substrates and the processes are certified by the credit card company regularly.

7. Laser-gravure: Using a laser, it is possible to burn images into the card substrate. The burning is indelible and very personal because it can be done when the smart card is issued to the cardholder. Examples of items that can be laser-gravured are cardholder name, cardholder photograph and card number. This technology is limited to black and white text or images.

3.2.2.2 Security Features of the Smart Card Chip

It is necessary during production for the smart card chip to test the microcircuit. After the chip has been tested, the chip must be irreversibly converted to a mode where it is impossible to access the internal chip circuit, for example directly accessing memory from the outside.

One of the last processes in the chip fabrication is to apply an electric current to the selected chip to blow a fusible link on the chip. Sometimes, in concert with blowing this fusible link, some manufacturers modify a location in EEPROM that logically changes the chip.

The card operating system detects the blown link and/or reads this memory location to determine the current mode. Once changed at the factory, it is impossible to change the operating mode back to "service mode".

Other on-chip security features include burying componentry deep inside the chip in inaccessible locations. For example, the ROM is buried in the lower layers of silicon to prevent reverse engineering of the card operating system.

The internal address and data buses that connect the major components on the chip together are scrambled. That is to say, the individual conductors are interchanged to make it more difficult for the attacker to deduce their function. Communication between on-chip components are encrypted on some smart card chips.

To prevent electrical signals emitted by the memory cells from being monitored externally, the area of the chip around the EEPROM is coated in a metal shield. Removing this shield will destroy the chip and it will no longer function.

The chip is also coated with a passivation layer to stop ultraviolet light from erasing the memory on the chip. Smart cards have circuits to detect external tampering with the chip. There are circuits to detect too high or too low supply voltage, too high or too low external clock frequency or sometimes too low an operating temperature.

3.2.2.3 Security Features of the Card Operating System

One of the enormous strengths of smart cards is the card operating system. All memory accesses must flow through the CPU so the design of the card operating system is critical for implementing security at a logical level. The logical organization of the dedicated files in EEPROM memory forms a security barrier. For example, when a dedicated file (DF) is selected, the card operating system prevents access to data in other DFs.

3.2.2.4 Security Features of the Network

The system design should take into account the accessibility of data in transit and protect it accordingly or design the transport protocol such that tampering will not affect the overall system security. One easy access point in the network is at the smart card contact pads. An attacker can insert the smart card into a hostile smart card reader whose purpose is to exercise the smart card and intercept the data stream flowing between the smart card and the smart card reader. Encrypting all sensitive data that will exit the smart card through the contact pads is one way to thwart and to prevent this attack.

If the card terminal can be physically secured by building it into a wall for example, then equipping the card terminal with a motorized smart card reader with shutter will enhance the network security. The motorized smart card reader will draw the smart card into the machine when the card is inserted and seal the smart card in the smart card reader while it is in use. People who have used an automated teller machine are familiar with this security method. The card remains inaccessible until the transaction is complete. The card could be retained if the system determines it is being misused.

Modern card terminals are just a part of a larger, more complex network of communications links between computers. These communications links must be physically protected from tampering if data integrity is to be maintained. The smart card reader and any communications links can be physically protected by lacing them in a secured environment where personnel or monitoring equipment continuously observe the use of the smart card reader and prevent tampering.

3.3 Cryptography and Security Principles

Current state of the art smartcards have sufficient cryptographic capabilities to support popular security applications and protocols. In spite of the increased cost, the benefits to computer and network security of including the cryptographic coprocessor are great, for it allows the private key never to leave the smartcard. As we'll see in the following sections, this becomes a critical factor for operations such as digital signatures, authentication, and non-repudiation. Eventually, though, the need for a cryptographic coprocessor and its associated cost will likely go away.

The basic processors could become powerful enough to perform the math-intensive operations, or other algorithms such as those based on elliptic curve technology could become popular. Elliptic curve algorithms provide strong security without the need for large integer math, and it has found its way into widespread use.

3.3.1 What is Cryptography?

Data that can be read and understood without any special measures is called plaintext or cleartext. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called ciphertext. You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called decryption.

When trying to better define cryptography, it's reasonable to say that cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography is best known as a way to keep certain information private, which is accomplished by encryption and decryption sensitive information (however, cryptography is nowadays also used for authentication).

Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication.

Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

Cryptography can be strong or weak; there are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files.

Cryptographic strength is measured in the time and resources it would require to recover the plaintext. The result of strong cryptography is ciphertext that is very difficult to decipher without possession of the appropriate decoding tool. How difficult? Given all of today's computing power and available time even a billion computers doing a billion checks a second it is not possible to decipher the result of strong cryptography before the end of the universe.

One would think, then, that strong cryptography would hold up rather well against even an extremely determined cryptanalyst. Who's really to say? No one has proven that the strongest encryption obtainable today will hold up under tomorrow's computing power. However, the strong cryptography employed by Pretty Good Privacy (PGP) is the best available today. Vigilance and conservatism will protect you better, however, than claims of impenetrability.

A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key—a word, number, or phrase to encrypt the plaintext. The same plaintext encrypts to different ciphertext with different keys.

The security of encrypted data is entirely dependent on two things: where the strength of the cryptographic algorithm and the secrecy of the key. A cryptographic algorithm, plus all possible keys and all the protocols that make it work comprise a cryptosystem. PGP is a cryptosystem.

3.3.2 Secret Key Cryptography - Conventional Cryptography

The traditional cryptography, also called Secret-Key or Symmetric-Key encryption, and conventional cryptography, is based on the mechanism that both the sender and the receiver of a message share the same secret key. One key is used both for encryption and decryption.

A simple symmetric key could be a pass phrase, PIN, or password that the trusted parties know. For simplicity, we'll use two trusted parties in this example. With symmetric key, both parties assume that they each have the key. When one of the parties starts a secure channel or session, the other one has to know the key or the session does not start.

However, this does not take into account how the key exchange even happens. Keys may be passed directly from person to person without any third-party involvement, making less likely the possibility of an attack. Most experts will tell you that it is usually better to exchange the key "out of band" or through a different channel than the one used by the cryptographic session. In other words, you wouldn't email your key if you thought that your network was insecure enough to warrant encryption. Also, if you use the same channel as the session, a lurker could snatch your key.

Another way that symmetric key exchange may happen is that a trusted third party may be used to exchange keys. This third party could be either another person or another computer that is trusted to handle the keys. This function is very similar to how a notary public works.

After the keys are exchanged, this third party is now partly responsible for the keys. However, if this entity is compromised, then we must destroy the symmetric keys and replace them with new ones, as well as replace the third party, because it is now also corrupt. Keep in mind that the participants can still compromise the keys and do so without the knowledge of the trusted third party. This process ensures that only trusted participants receive keys.

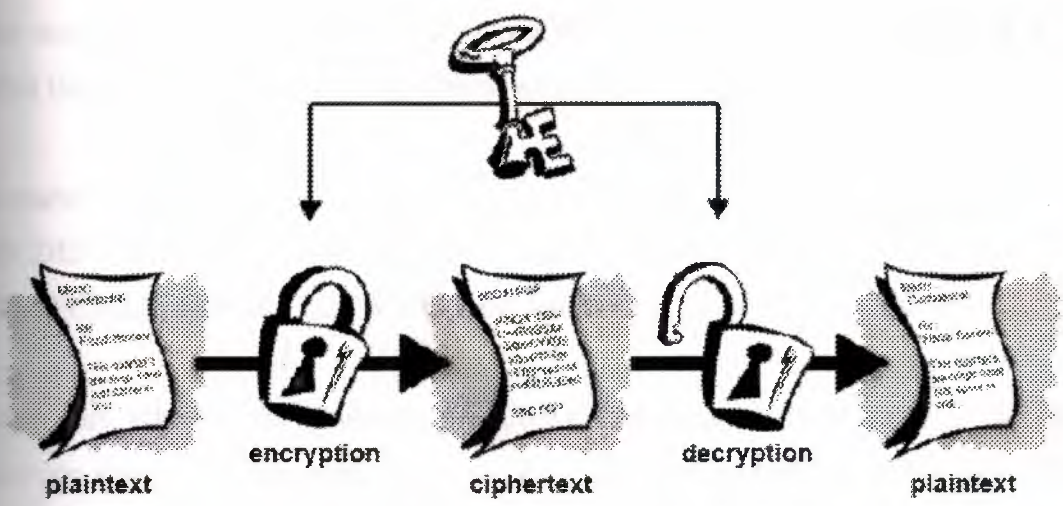


Figure 2.1, Data Transfer with Symmetric Keys

The biggest weakness with symmetric key cryptography is the key exchange itself. If the keys are exchanged out in the open, then the keys are at risk of being discovered. Another problem with the key exchange is the trusted third-party involvement. If that third party is compromised, then the established trust is gone.

The other problem is to have someone masquerade as a trusted party. If a nefarious participant becomes the trusted third party for key exchange-be it either a "trusted" computer system or a person-the key is then compromised.

As you can see, symmetric key encryption has a fundamental flaw: the key exchange. However, if the symmetric key is used in conjunction with public key algorithm, then the key exchange can be made more secure.

An extremely simple example of conventional cryptography is a substitution cipher. A substitution cipher substitutes one piece of information for another. This is most frequently done by offsetting letters of the alphabet. Two examples are Captain Midnight's Secret Decoder Ring, which you may have owned when you were a kid, and Julius Caesar's cipher. In both cases, the algorithm is to offset the alphabet and the key is the number of characters to offset it.

For example, if we encode the word "SECRET" using Caesar's key value of 3, we offset the alphabet so that the 3rd letter down (D) begins the alphabet.

So starting with
ABCDEFGHIJKLMNOPQRSTUVWXYZ and sliding everything up by 3, you get
DEFGHIJKLMNOPQRSTUVWXYZABC where D=A, E=B, F=C, and so on.

Using this scheme, the plaintext, "SECRET" encrypts as "VHFUHW." To allow someone else to read the ciphertext, you tell them that the key is 3. Obviously, this is exceedingly weak cryptography by today's standards, but hey, it worked for Caesar, and it also illustrates how conventional cryptography works.

3.3.3 Public Key Cryptography

The problems of key distribution are solved by public key cryptography, the concept of which was introduced by Whitfield Diffie and Martin Hellman in 1975. (There is now evidence that the British Secret Service invented it a few years before Diffie and Hellman, but kept it a military secret and did nothing with it.)

Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private, or secret key for decryption.

You publish your public key to the world while keeping your private key secret. Anyone with a copy of your public key can then encrypt information that only you can read. Even people you have never met. It is computationally infeasible to deduce the private key from the public key.

Anyone who has a public key can encrypt information but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information.

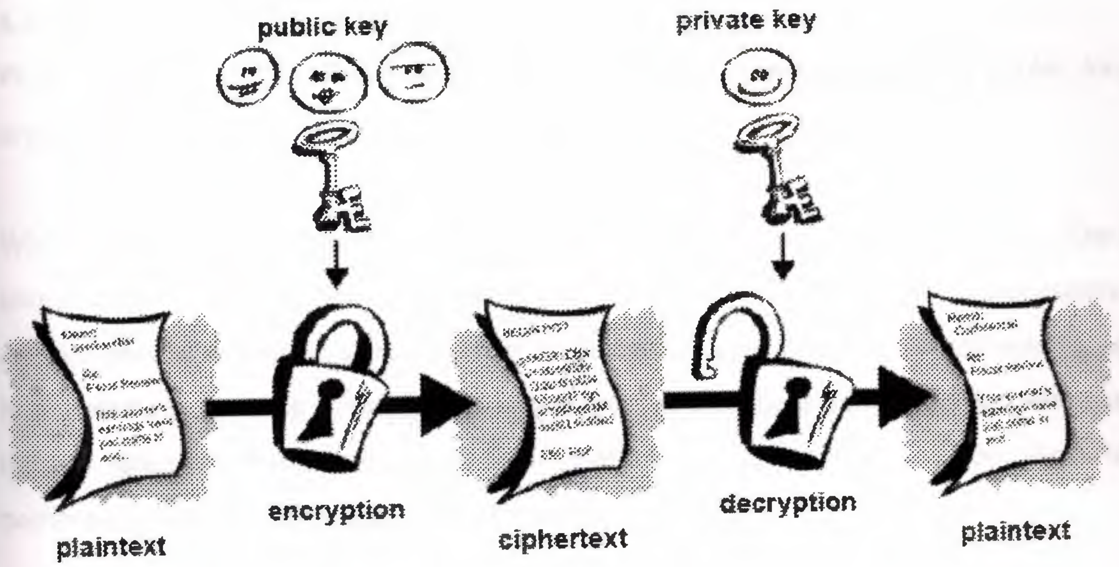


Figure 3.2, Public Key Encryption

The primary benefit of public key cryptography is that it allows people who have no preexisting security arrangement to exchange messages securely. The need for sender and receiver to share secret keys via some secure channel is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared.

Some examples of public-key cryptosystems are Elgamal (named for its inventor, Taher Elgamal), RSA (named for its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman), Diffie-Hellman (named, you guessed it, for its inventors), and DSA, the Digital Signature Algorithm (invented by David Kravitz).

Because conventional cryptography was once the only available means for relaying secret information, the expense of secure channels and key distribution relegated its use only to those who could afford it, such as governments and large banks (or small children with secret decoder rings).

Public key encryption is the technological revolution that provides strong cryptography to the adult masses. Remember the courier with the locked briefcase handcuffed to his wrist? Public-key encryption puts him out of business (probably to his relief).

3.3.4 Pretty Good Privacy (PGP)

PGP combines some of the best features of both conventional and public key cryptography. PGP is a hybrid cryptosystem.

When a user encrypts plaintext with PGP, PGP first compresses the plaintext. Data compression saves modem transmission time and disk space and, more importantly, strengthens cryptographic security. Most cryptanalysis techniques exploit patterns found in the plaintext to crack the cipher. Compression reduces these patterns in the plaintext, thereby greatly enhancing resistance to cryptanalysis. (Files that are too short to compress or which don't compress well aren't compressed.)

PGP then creates a session key, which is a one-time-only secret key. This key is a random number generated from the random movements of your mouse and the keystrokes you type. This session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key. This public key-encrypted session key is transmitted along with the ciphertext to the recipient.

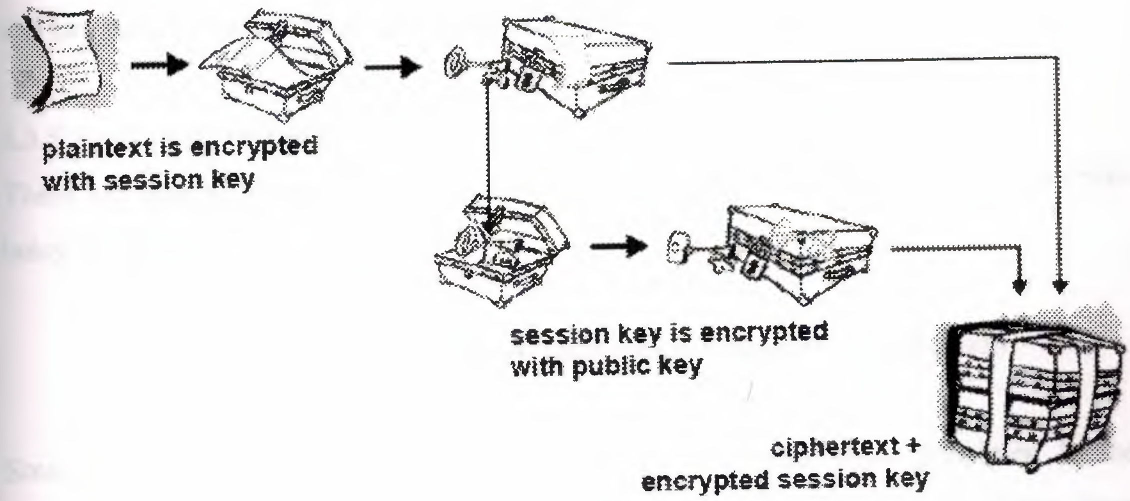

plaintext is encrypted with session key
session key is encrypted with public key
ciphertext + encrypted session key

Figure 3.3 The way PGP Encryption works

Decryption works in the reverse. The recipient's copy of PGP uses his or her private key to recover the temporary session key, which PGP then uses to decrypt the conventionally-encrypted ciphertext.

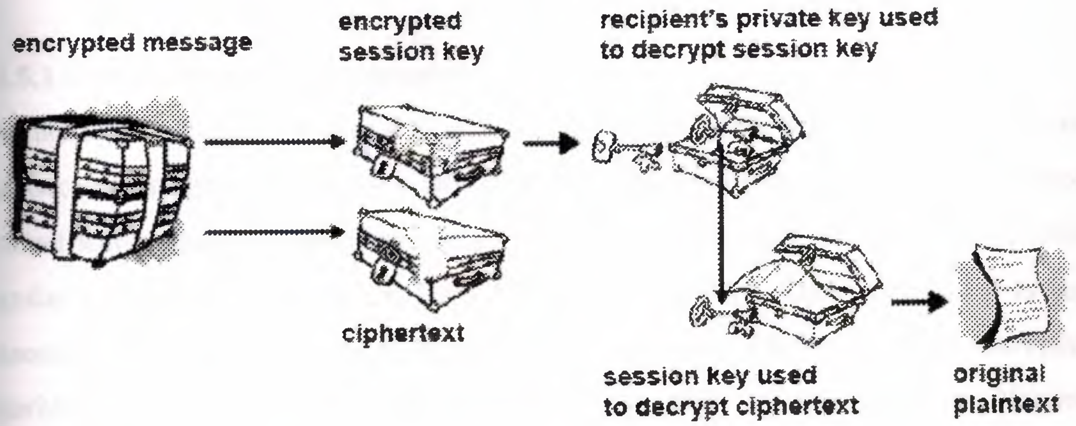

encrypted message
encrypted session key
recipient's private key used to decrypt session key
ciphertext
session key used to decrypt ciphertext
original plaintext

Figure 3.4 The way PGP Decryption works

The combination of the two encryption methods combines the convenience public key encryption with the speed of conventional encryption. Conventional encryption is about 1,000 times faster than public key encryption. Public key encryption in turn provides a solution to key distribution and data transmission issues. Used together, performance and key distribution are improved without any sacrifice in security.

3.3.5 Security Principles

There are several reasons one requires security in a smart card system. The principles being enforced are:

· Privacy · Non-repudiation · Authentication · Integrity · Verification

Smart cards use different encryption algorithms to implement these principles. In the following sections, I will describe the mechanisms use in smart cards to enforce these principles.

3.3.5.1 Privacy

Privacy is the act of ensuring the nondisclosure of information between two parties from casual third-party intrusion. There are two cryptographic techniques used to assure privacy symmetrical cryptography and asymmetrical cryptography and each cryptographic technique have different application areas in smart cards.

3.3.5.1.1 Symmetrical Cryptography

Symmetrical cryptography uses a single key to encrypt plain text into enciphered text and decrypt enciphered text back into plain text. Symmetrical cryptography is termed symmetrical because the same key is used to encrypt and decrypt the message. The most popular symmetrical algorithm is Data Encryption Standard (DES) because it is fast, reasonably secure and simple to implement in hardware. DES is a block-encryption algorithm developed by IBM and standardized in 1977 by the American National Standards Institute (ANSI) as Federal Information Processing Standard (FIPS) 46-2, otherwise known as the Data Encryption Algorithm (DEA).

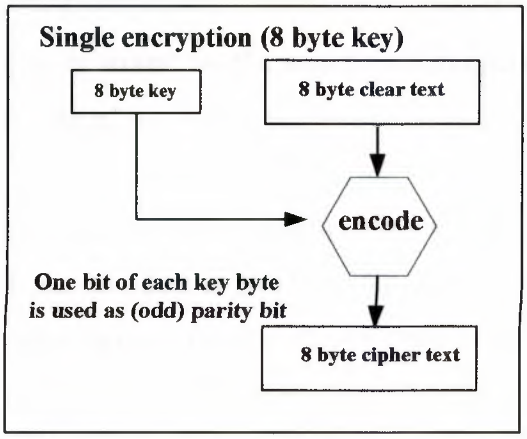

Single encryption (8 byte key)
8 byte key
8 byte clear text
encode
One bit of each key byte is used as (odd) parity bit
8 byte cipher text

Figure 3.5, Symmetric Encryption using DES

DES can use different key lengths. The longer the key, the more difficult is to break it. A 40 bits key can be broken with a few CPU hours, while a 56 bits key would take considerably longer.

These brute force attacks are benefiting from the dramatic increase of the processing power of the CPUs, so this "considerable longer time" that we mentioned is a relative term.

Data is encrypted in blocks of 8 bytes and results in cipher text of the same size. This is a "noiseless" algorithm because the enciphered text size and encryption time is constant and independent of size of the supplied plain text.

A noiseless encryption algorithm is more difficult to attack because it is not possible to deduce the encryption mechanics based upon the time differences between encrypting large quantities of plain text input and small quantities.

DES can be implemented on smart card software, as it is a relatively fast algorithm. The time it takes to encrypt one 8-byte block of plain text is in the order of 10 milliseconds. As a comparison, the same text could be encrypted in about 60 nanoseconds with specialized DES hardware.

The majority of data on a smart card is stored in EEPROM in clear-text form. However, certain confidential data is stored on the smart card in encrypted form. DES is used to generate that encrypted data.

In cases requiring greater security, for example in the transmission of encryption keys, Triple-DES is used. Plain text data in blocks of 8 bytes is enciphered three times using a 16-byte key (which, after accounting for the 16 parity bits, results in an effective key length of 112 bits). Needless to say, this is strong encryption.

At the present time, nearly all smart cards perform DES encryption in software. The disadvantage of symmetrical encryption is that both partners need to know the key. The transfer of the key from one partner to the other can compromise the security that otherwise the encryption provides.

Writing a DES key at card personalization time is the typical method of safely transferring keys to cardholders. If this is not possible, asymmetrical cryptography must be used, which is described below.

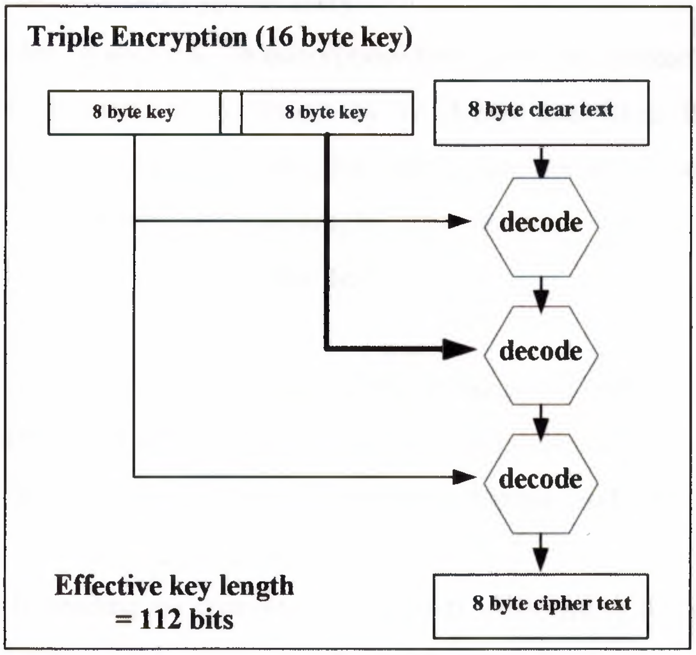


Figure 3.6, Symmetric Encryption using Triple DES

3.3.5.1.2 Asymmetrical Cryptography

In 1976, the idea of splitting the encryption/decryption key instead of sharing a common key was first proposed in an article by W. Diffie and M.E. Hellman entitled New Directions in Cryptography. This idea has since become known as asymmetrical cryptography. Asymmetrical cryptography uses two keys: one to encrypt the plain text and another to decrypt the enciphered text.

The keys are mathematically related. Only messages encrypted with one key can be decrypted with the other key. The best-known asymmetrical cryptographic algorithm is RSA which was named after its inventors Rivest, Shamir, and Adleman.

Assume Bob is sending an encrypted message to Alice using RSA. The two RSA keys are called the private key and public key. Alice would distribute her RSA public key and keep her RSA private key private.

To start the process, Bob would first obtain Alice's public key. Bob would encrypt the plain text using Alice's public key and send the enciphered text to Alice. Alice would use her private key to decrypt the enciphered text. Because of the relationship between the public and private keys, Bob can be assured that only Alice can decrypt the message.

It is not necessary for Bob or Alice to share any secret between them and thus there is no risk of inadvertently disclosing such a secret to a third person.

Asymmetrical cryptography is used in smart cards but rarely to perform general data encryption. Symmetrical cryptography such as DES is used for that purpose. Instead, asymmetrical cryptography is used in smart cards for authentication purposes such as digital signatures. The private key of the key pair of a digital certificate is normally stored on the smart card for example. This is because it can be safely protected by the card operating system and not disclosed outside the smart card.

As in the case of symmetrical encryption, the keys can have different lengths. The three most common values are 512, 768 and 1024 bits. The last two values are considered strong encryption.

The disadvantage of the RSA algorithm is that it is slow, much slower than the DES algorithm. Due to the limited speed of the smart card CPU, it is not practical to implement the key generation algorithm in software. There are special smart cards that have crypto-processors for that purpose. The symmetrical and asymmetrical encryptions usually complement each other.

The asymmetrical encryption is often used to send the DES key safely from one partner to the other. Once both partners know the DES key, the data is transmitted symmetrically encrypted, which significantly improves the performance.

3.3.5.2 Integrity

Electronic communications links are prone to errors and data tampering. Cryptographic techniques are used to ensure that data content does not change while it is being transmitted from the originator to the recipient. This is called data integrity.

3.3.5.2.1 Message Authentication Code (MAC)

A message authentication code (MAC) is an 8-byte value generated for a message that is unique to that message because a one-way cryptographic algorithm is used to generate the value. A one-way cryptographic algorithm is special because it cannot be reversed (that is, the original plain text cannot be recovered from the cipher text) and the enciphered text is guaranteed always unique.

The MAC used in smart cards is calculated with DES using a key which is shared by both the smart card and the smart card reader. The MAC is appended to the end of the plain text message before being sent.

When the message is received, the recipient calculates a MAC value from the contents of the message and compares the result to the MAC that accompanied the message.

Because changing even one character in the message changes the MAC in an unpredictable way, the recipient can be sure that the message was not changed after the MAC was generated. A MAC is a guarantee of integrity, a guarantee that the message has not been tampered. All messages that are exchanged between the smart card and the smart card reader must be protected with a MAC for example.

3.3.5.3 Non-Repudiation

Cryptography can also provide authentication of the engaged parties and ensure non-repudiation of the transaction. Non-repudiation is proof of the integrity and origin of data exchanged in the transaction. It is forgery prevention.

3.3.5.3.1 Digital Signature

When Bob sent an encrypted message to Alice, he used Alice's public key to encrypt the message and Alice would use her private key to decrypt the message. One of the properties of asymmetrical cryptography would allow Alice to check that Bob actually originated the message. This property forms the basis for digital signatures.

A digital signature results from the process of encrypting a message authentication value with the originator's private RSA key. The main property of a signature is that only one person can generate one (that is to say a digital signature is unique for each person) but anyone can check the digital signature. In general, it would take too much time to sign a full clear-text message so instead only the message authentication value of the message is signed. Instead of using the MAC algorithm described above to create the message authentication value, the message is passed through a one-way cryptographic process called a hashing algorithm. One popular hashing algorithm used on smart cards is the Secure Hash Algorithm (SHA-1).

Hashing the plain text message with SHA-1 and then encrypting the hash with a person's RSA private key creates the digital signature. The signature can be verified with the originator's RSA public key.

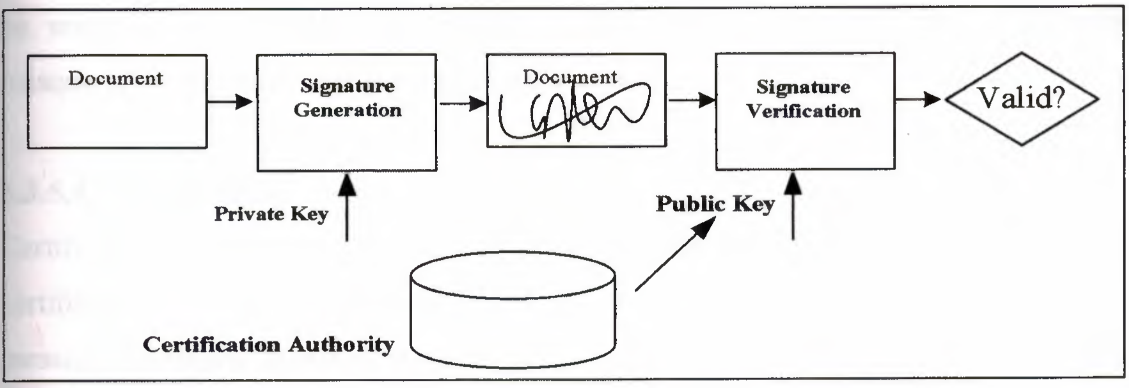


Figure 3.7, a simplified signature signing and verification process

Let's take an example. Let's assume Bob wishes to sign a message and send it to Alice. First, he runs the plain text through the SHA-1 hashing process and produces a fixed length hash of the message. Then, Bob encrypts the hash using his private RSA key to create the unique signature for that particular message. Bob then sends the plain text message and the digital signature to Alice. Alice can use Bob's public key to decrypt the digital signature and recover the hash, then generate a hash for the received plain text message and finally compare the two hashes.

Again, because of the mathematical relationship between the keys, if the hash decrypts and verifies properly, Alice can be assured that only Bob could have created the message in the first place and neither the message nor the hash changed during transmission.

Digital signatures also serve as proof of the origin of a message. RSA asymmetrical encryption is not the only mechanism for creating digital signatures. The Digital Signature Algorithm (DSA) is a specification for a process that creates signatures from message content.

The advantage of DSA over RSA is that DSA is designed to use technology that is freely exportable worldwide. DSA signatures are as unambiguous as signatures created with RSA. However, DSA does not do general-purpose encryption and decryption as does RSA.

3.3.5.4 Authentication

Before two parties conduct business, each wants to be sure that the other party is authenticated. For example, before Bob accepts a message with Alice's digital signature, he wants to be sure that the public key belongs to Alice and not to someone masquerading as Alice. This is what certificates do.

3.3.5.4.1 Certificates

Certificates are guarantees by the authority issuing the certificate that the holder of the certificate is who he/she claims to be. In short, a certificate is just a digitally signed message containing information about the certificate holder plus a copy of the holder's public key.

Anyone receiving the certificate has assurance that the key contained in the certificate is authentic because it is signed by the issuing authority, which is a trusted entity.

On the World Wide Web, Secure Sockets Layer (SSL) uses certificates for example. The Web browser will obtain the certificate of the Web server and use the public key within the certificate to encipher the initial encryption key. Similarly, when the smart card sends data to a card terminal's Security Access Module, the smart card will construct an encrypted channel, like SSL does, using the card terminal's public key.

The information fields in a certificate are extendible; however some fields are mandatory. A certificate issuer, known as a certificate authority, can add as many fields as it likes so it becomes a flexible way to associate personal information with a particular individual and maintain the integrity of the information. For example, a certificate can hold the person's name and address, the person's employment start date, their employee number, their security access level, and so on.

Before a certificate is issued to a person, depending on the grade of certificate, the issuing authority will require legally binding proof as to the identity of the person. Application for a low grade certificate would only require a passport or driver's license as proof of identity, for example.

A higher grade certificate would possibly need a document certified by an attorney. The higher the grade of certificate issued, the greater the assurance the recipient has that the person truly is who he/she claims to be.

Certificate chains are only based on trust. The receiver must trust that the authority has verified the authenticity of the certificate holder and has not tampered with the information before signing the certificate. If the recipient does not trust the issuing authority, then the certificate will have no value.

3.3.5.5 Verification

It is to the benefit of both a smart card owner and a smart card issuer that the identity of the cardholder is confirmed before the card is used. Before both parties transact business, they must be assured of the identity of the other party. When we meet in person, we use visual and verbal clues to help us to recognize the other party. With electronic communication, we use encryption technology to unambiguously verify that the other person is who they may claim to be.

3.3.5.5.1 PIN Codes

A Personal Identification Code (PIN) is usually a four or five-digit number that accompanies a smart card and must be memorized by the cardholder. The PIN is stored securely within the smart card in a way that can never be read from the external world. Data and functions on the smart card can be protected in a way that access from the external world is allowed only after the correct PIN code is presented. The IBM MFC can store up to two PIN codes per application but normally only one PIN code is required.

This simplifies the user interface. It is possible to program the second PIN code as an administrator PIN code. For example, this would be used to unblock the card in case the user either forgot the first PIN code or entered the code incorrectly too many times in sequence. The PIN can be assigned and stored in the card during personalization. The application program can supply the PIN code in two different ways.

If the user has an intelligent smart card reader attached (for example a smart card reader with a keyboard and display), then the application can ask the smart card reader to display the password prompt and accept the user's input. If the user has a simple smart card reader attached, then the PIN code can be entered from within the application program it and send to the smart card reader.

With the profusion of smart card applications, people are required to remember more and more PIN numbers. This puts a strain on the user's memory. After all, who can remember 15 or 20 different PIN codes? Sometimes, people jot down the PIN number on the card itself as a means to jog their memory. This is dangerous as it nullifies the advantage of having the PIN in the first place.

That is why recent emphasis on security measures has revolved around biometric measurement techniques as a means of identifying a person.

3.3.5.5.2 Biometrics

Biometrics is the science and technology of measuring human biological features to unambiguously identify an individual within a group of people. One of the driving forces behind the development of biometric identification technology is the reluctance within the user community to memorize passwords and PIN numbers for identification. Also, a PIN number does not uniquely identify an individual because PIN numbers can be shared among different people (sometimes inadvertently when people write their PIN numbers on the card itself and then lose the card). Biometrics identifies the actual person and not the person's knowledge of a shared secret.

Some of the biological features that are both unique to an individual and that can be measured are:

1· Signature
2· Fingerprint
3· Voiceprint
4· Hand geometry
5· Eye retina
6· Facial recognition

Signatures and fingerprints are two techniques that have been known for hundreds of years. Both techniques are in popular use, the latter most often associated with police identification. Using machines to automate the analysis is relatively new.

Fingerprint analysis is based on mathematical relationships in the direction of cutpoints through the minutia, the lines in your finger. The set of minutia vectors (that is, the number and direction of cutpoints) for an individual are unique for each and every individual. A precompiled minutia vector database can be stored on the smart card because the data takes up very little space, approximately 300-800 bytes. The fingerprint scanned at the biometric station can be mathematically compared to the reference and a statistically good match will be accepted as that individual.

Hand geometry is a biometric technique that uses features of the size and shape of the person's hand to uniquely single out a person from a group. The recognition speed is relatively fast. Also, the size of the reference pattern is small, normally 10-30 bytes, so it can easily be stored onto a smart card. The main limitation of hand geometry recognition is that the group size must be small.

This technique is usually employed for facilities access where the total number of people to be allowed access is relatively small, a few dozen at the most. The pattern of blood vessels on the back of the eye retina is also, like a fingerprint, unique in each person. A low-power laser can scan the retina and record the pattern. Like a fingerprint analysis system, the pattern of the retina can be compared to a statically stored pattern on the card and a match will authenticate the individual.

Today, smart cards contain reference data that will be used by the biometric station. The biometric station will compare the dynamic data obtained from the biological feature to the reference data stored in the smart card. The comparison is done on the biometric station and not within the smart card itself. Thus, the security of the system is dependent on the security of the biometric station itself. For example, if a fingerprint sensor is built into a computer station keyboard, the security of the system is no better than the preventative measures in place to prevent tampering with the keyboard and its connecting wires.

3.4 Biometrics and Smart Cards

Secure access, whether to buildings, information, bank funds, or other resources, has long been based on a combination of two concepts: what you have and what you know. Basic bank debit card security is based upon what you have the debit card and what you know – the PIN. This type of security is considered insufficient for securing access to areas of high value since PINs can be recorded, lost or stolen. In situations requiring higher security, the requirements expand to include “what you are” which can be substantiated by the use of a biometric. Biometric technology involves the measurement of a distinctive biological feature to verify the claimed identity of an individual through automated means.

A biometric is a measurable physiological or behavioral trait of a living person, especially one that can be used to identify a person or verify a claimed identity. As a biometric is uniquely bound to a person, it can provide the strongest single factor for user authentication. A biometric can be used in conjunction with a password or a token (such as a smart card) to provide strong, two-factor authentication. Although biometric systems have been commercially available since 1968, the commercial use of biometrics has experienced significant growth only in the last five years. Biometrics are increasingly used in time and attendance systems, customs and immigration, physical access control systems, ATMs and point-of-sale (POS) systems, and information system access control.

A physiological biometric (also called physical biometric, static biometric) is a biometric based on data derived from measurement of a part of a person's anatomy. Examples of physiological biometrics include fingerprint, hand, face, iris and retina.

A behavioral biometric (also called dynamic biometric) is a biometric based on data derived from measurements of an action performed by a person and, distinctively, incorporating time as a metric; that is, the measured action has a beginning, middle, and end. Examples of behavioral biometrics include voice and signature.

Physiological biometrics are unchanging (barring severe physical injury) and unalterable without significant duress, but are perceived as more invasive and raise privacy concerns more quickly. Behavioral biometrics are less stable than physiological traits, changing with stress and sickness and, generally, are less secure.

This section describes different types of biometrics that can be used with a smart identification card, including information about biometric uniqueness, image capture method and template definition and size.

<u>1. Fingerprint Scan</u>: The fingerprint is one of the most widely used biometrics in the government today. It is currently the only authorized biometric for the Department of Defense, and then only for specific purposes disclosed to the individual.

Fingerprint scanners have been commercially successful biometric devices over the last several years, accounting for nearly 50 percent of the 2001 worldwide biometrics market (according to the International Biometric Group). A wide variety of devices are available. Because of the association of fingerprints with criminal forensics, these biometric technologies are also called fingertip or finger scan technologies.

Distinctiveness: It has been estimated that the chance of two people having the same fingerprint is less than one in a hundred billion (even for monozygotic siblings "identical" twins or triplets). While this is difficult to prove empirically, in over a century of the use of fingerprinting, no two fingerprints have ever been found to be identical. In addition, it is now known that fingerprints form in the womb at around five months and remain constant even after death. Fingerprints have even been successfully taken from well-preserved mummies more than 2,000 years after their death.

Image capture: A fingerprint image can be captured using one of four technologies: optical, capacitive (silicon), thermal (silicon), and ultrasonic. The majority of companies use optical technology, but the trend is toward silicon.

Over the past decade, optical scanners have been the most widely implemented fingerprint technology. Optical fingerprint technology is proven but is relatively expensive and not always reliable due to environmental conditions.

To operate, a user places a finger on a platen of glass or hard plastic (proprietary to each company). The fingerprint is illuminated by an internal light source and a charge-coupled device (CCD) converts the image of the fingerprint into a digital signal.

Capacitive (silicon) technology has gained considerable acceptance since its introduction in the late 1990s. Most silicon, or chip, technology is based on direct current (DC) capacitance: the silicon sensor acts as one plate of a capacitor and the user's finger is the other. The capacitance between platen and the finger is converted into an eight-bit grayscale digital image. An exception to this is a technology, which employs alternating current (AC) capacitance and reads to the live layer of skin. Capacitive imaging generally produces better image quality from a smaller surface area than optical.

The chips have a resolution of about 0.05 millimeters (0.002 inches) and are small enough to be integrated into many devices that cannot accommodate optical technology. Many major companies have recently moved into the silicon field.

Using thermal (silicon) technology, the finger is swept across a rectangular array of pixels, which are sensitive to heat transfer due to the application of a pyroelectric layer above the silicon. A slice of the fingerprint is captured, and multiple slices are reconstructed into a full fingerprint image. This technology has a thick surface coating, providing high levels of mechanical robustness (e.g., resistance to abrasion and corrosion) and electrostatic discharge (EDS) protection. Power consumption is low.

Thermal technology provides a high quality image and is able to capture poor fingerprints (i.e., those with little topography) very well. The swiping method is self-cleaning and, combined with the thermal technology, enables the sensor to operate in challenging environmental conditions. Resolution is 0.05 millimeters (500 dots per inch). Due to the swiping method and the resulting small silicon area, thermal technology offers a small and low cost solution.

Ultrasound technology is not yet widely used. The sensor transmits acoustic waves and measures the distance based on the impedance of the finger, platen, and air. Preliminary uses of the products indicate that this technology promises to be the most accurate fingerprint technology.

Templates: Systematic approaches to matching fingerprints to certain individuals were introduced in the 19th century. One such approach, the Henry Classification System, is based on patterns such as loops, whorls and arches and is still used today to organize fingerprint card files. The most common method of generating a template emulates the traditional police method of matching minutiae (literally, “small details”): bifurcations, divergences, enclosures, endings and valleys in the ridge pattern.

Each minutia is described by a set of numeric variables. A typical fingerprint image can show between 30 and 40 minutiae. Approximately 80 percent of biometric fingerprint sensors use minutiae in some fashion. Other methods include “traditional” pattern matching techniques and moiré fringe patterns.

The fingerprint has one of the largest biometric templates, ranging from 250 bytes (minutiae) to over 1,000 bytes (pattern matching). Note that, as with any other biometric technology, the template holds only particular data about the features, not the image of the fingerprint itself, and the image cannot be reconstructed from the template.

2. Hand Geometry: Hand geometry is currently being used in several government agencies including the Department of Energy and the Department of State. Hand geometry systems use optical technology to map key geometrical features of hand topography to verify an individual's identity. Hand geometry technology uses a number of different measurements to create the template.

These readings may include measuring finger length, skin translucency, hand thickness, and palm shape. Different products use diverse methodologies to construct the hand geometry template, so there is currently no standard template that can be used for smart cards. Live scans of the hand are compared against the template to verify a person's identity.

Distinctiveness: Virtually every person's hands are shaped differently, and the shape does not significantly change over time. A biometric template can be built from measurements of geometrical characteristics of a person's hand.

Image capture: Hand geometry scanning devices use either mechanical or image-edge detection. In either case, a charge-coupled device is used to record the hand's three-dimensional shape. One variant uses the shape and characteristics of just the index and middle fingers.

Templates: Over 90 measurements of the length, width, thickness, and surface area of a person's hand and/or fingers are used to generate the template. This is one of the smallest templates, generally 10 to 20 bytes.

3. Facial Recognition: Several state motor vehicle departments are currently using facial recognition to provide identity authentication in issuing driver's licenses. Facial recognition is based on comparing the characteristics of a live scan of a face against a stored template of facial characteristics.

Various technologies may be used to perform facial recognition. Some products use off-the-shelf video/digital cameras. Such products employ algorithms to create a set of numbers related to the face rather than the facial image itself. One method uses spatial measurement, recording such distances as the center of the eye to the bottom of the ear, to the tip of the chin, and to the high cheek feature.

Another method uses two cameras to record a stereo view of the face. This method evaluates the entire face, not just key features. Other products use infrared technology. Because the technology for creating facial templates varies from product to product, there is no standard facial recognition template.

Distinctiveness: An obvious limitation of face verification is that, because it generally disregards changeable characteristics like hair color and style, it cannot differentiate between monozygotic siblings.

Image capture: The system locates the human face within an image captured by a video camera, isolating it from the other objects captured within the image. Software then analyzes the captured images for general facial structures (such as eyes and nose) and measures and determines the rest of the face. Other imaging methods include three-dimensional mapping (using a laser range scanner, instead of a camera) and thermal imaging of blood vessels under the skin.

Templates: Templates may be generated by one of several methods:

3. Eigenfaces: Eigenface (from the German eigen, 'own') is an MIT-patented technology that uses two-dimensional, global grayscale images representing distinctive characteristics of a facial image. Variations of eigenface are frequently used as the basis of other face recognition methods.

Eigenfeatures: The system combines facial metrics—measurements of the distance between specific facial features, such as the eyes, nose and mouth—with the eigenface approach.

Local feature analysis: In this derivative of the eigenface method, the system selects sets of blocks, or features, in each face that differ from other faces in the database. The most common points used are the nose, eyes, mouth, and areas of definite bone curvature differences, such as the cheeks.

4. Neural Networking Technology: This system employs artificial intelligence and "learns" from experience. Features from both faces—the enrollment and trial face—"vote" on whether there is a match.

5. Curvature Measurement: This method is used with three-dimensional mapping.

Thermogram: This method is used with thermal imaging.

6. Iris Scan: The iris consists of a trabecular meshwork of connective tissue, collagenous stromal fibers, ciliary's processes, contraction furrows, rings, and coloration. In the 1960s ophthalmologists proposed that the iris might be used as a kind of "optical fingerprint," based on clinical results that showed that every iris is unique and unchanging. John Daugman, Ph.D., O.B.E., an academic at the Computer Laboratory, University of Cambridge, U.K., developed the mathematical algorithms behind iris recognition (Internet: www.cl.cam.ac.uk/users/jgd1000/).

Distinctiveness: The uniqueness of eye identification is well-established. The iris is a robust biometric as it remains unchanged throughout a person's life and is not subject to wear and injury, although damage to the cornea or disease might obscure the iris.

The iris has 6 times as many distinct, identifiable features as a fingerprint. Like fingerprints, no two iris patterns are alike, even among monozygotic siblings.

Image capture: The iris presents a number of challenges. It is a small target (one centimeter or half an inch) that must be acquired from a distance (one meter or one yard), and is often prone to movement. Moreover, the iris is located behind a curved, wet, reflecting surface, is obscured by eyelashes, lenses, and reflections, and is partially occluded by eyelids that are often drooping.

This accounts for the higher capture device cost as compared to some other biometric systems. Iris image capture can be passive or active. With active iris image capture, the user must be between 15 and 35 centimeters (6 and 14 inches) from the camera lens. Passive iris image capture incorporates a wide-angle lens, automatically determines the position of the eye, and zooms in on the eye to capture the image. The user can be between 30 and 100 centimeters (1 and 3 feet) away from the cameras. This method is more user-friendly, but also more costly.

Templates: The template or "IrisCode" is constructed by "demodulation" of the iris pattern. This mathematical process is unchanged by the size of the iris (and hence unaffected by the imaging distance and the optical magnification factor) and by the dilation diameter of the pupil within the iris. It is also insensitive to contrast, camera gain and illumination level. The description is very compact, requiring only 256 bytes to represent each iris pattern. (The other 256 bytes of a 512 byte IrisCode control the comparison process.) The recognition of irises by their IrisCodes is based on the "failure of a test of statistical independence." Any given IrisCode is statistically guaranteed to pass a test of independence against any IrisCode computed from a different eye; however, it will uniquely fail this same test against the eye from which it was computed.

7. Retina: Research into eye recognition technology began in 1935 when an article appearing in the New York State Journal of Medicine suggested that the pattern of blood vessels on the retina were unique from person to person and so could be used to identify an individual. The first commercial product to use retinal scans, EyeDentify 7.5, appeared in 1985. Today, the retina segment of the biometrics market comprises a very small market share.

Distinctiveness: Along with iris recognition technology, retina scan is perhaps the most accurate and reliable biometric technology. Research has shown that retinal patterns, even between monozygotic siblings, are unique. With the exception of some types of degenerative eye diseases, severe head trauma, damage to the cornea, glaucoma, cataracts, and other factors that might obscure the retina, retinal patterns can be used throughout a person's life.

Image capture: Retina scan devices read through the pupil, with the user putting his or her eye within 1 to 2 centimeters (approximately 0.5 to 0.8 inches) of the device and holding still while the image is captured. The user looks at a rotating green light as a low-intensity infrared light is projected through the eye and onto the retina.

Template: The patterns of the retinal blood vessels are measured at over 400 points to generate a 96-byte template.

8. Voice Recognition: Voice identification technology was pioneered in the 1960s. Voice identification has since undergone aggressive research and development to bring it into the mainstream. Voice verification is possible because every person has a unique set of voice characteristics and speech patterns. Voice verification extracts specific and unique features from a person's speech, such as pitch, tone, cadence, harmonic level and vibrations in the larynx, and stores and uses them to differentiate that person's voice from other voices. All voice recognition systems require speech samples from each user to associate with the user's profile or account. A person using a voice verification system begins by claiming to be an enrolled user.

This is generally accomplished by speaking or otherwise inputting an identification code. The spoken input is compared with a stored sample of the enrolled user's speech. This stored sample is called a voiceprint. If the voiceprint and spoken input samples match, then the person is accepted. If they do not match, the person is rejected and denied access. Voice is a very convenient verification system for use in telephonic transactions. Voice verification can greatly enhance security for dial-up computer links and terminal access, so it is particularly popular for logical access control applications.

Distinctiveness: Voice is less accurate than other biometrics. Its main attraction is its suitability for telephone applications and interactive voice response (IVR) systems, where it can be deployed with no additional user hardware costs.

Image capture: Voice "images" can be captured with conventional microphones used in telephones and PCs.

Templates: There are different methods or processes to analyze a person's speech pattern, but all systems are developed using broader-based speech processing technology. Voice systems incorporate several variables or parameters in the recognition of the voice or speech pattern, including pitch, dynamics, and waveform. Voice scan templates commonly require 1,500 to 3,000 bytes.

9. Signature: Signature-based authentication, also known as dynamic signature verification (DSV), is another instinctive biometric as authentication by signature occurs during many everyday transactions. It is popular in document authentication applications that have traditionally used written signatures.

Distinctiveness: Signature identification systems analyze two different areas of a person's signature: the specific features of the signature itself (the visual image) and the specific features of the process of signing. Features that are taken into account and measured include speed, pen pressure, directions, stroke length, and the points in time when the pen is lifted from the paper. With sufficient practice, a person might be able to duplicate the visual image of someone else's signature, but it is difficult, if not impossible, to duplicate the dynamics.

Image capture: Signature identification is an inexpensive biometric solution. Tablet-based systems that operate using off-the-shelf digitizers cost as little as US$99, but suffer from limited accuracy.

Templates: The major technological hurdle for signature identification involves the method of trying to differentiate between the parts of the signature that are habitual (consistent) and those that vary from time to time. Systems must also be able to adapt to any slight variations over time.

3.4.1 Biometric Systems

Although biometric technologies differ in what and how they measure, all biometric systems work in a similar way. The user submits a sample that is, an identifiable, unprocessed image or recording of the physiological or behavioral biometric via an acquisition device (for example, a scanner or camera).

This biometric is processed to extract information about distinctive features to create a trial template (or verification template). Templates are essentially large number sequences; it's impossible to reconstruct the sample from the template. The trial template is the equivalent of the user's "password."

Verifying a memorized password or a one-time password (such as a password that is generated by an authentication token) is a yes/no decision. However, verifying a trial template is not. A trial template is compared against a reference template (or enrollment template) that was created from multiple images when the person enrolled in the biometric system. No two templates are ever exactly alike, so the biometric system must judge whether or not there is a "close enough" match: i.e., the matching score must exceed a configurable threshold.

Thus, biometric systems can err. A trial template might be matched incorrectly against another person's reference template, or it might not be matched even though the user is enrolled. The accuracy of a biometric system is measured by:

False match rate (FMR), also known as Type I error or false acceptance rate (FAR), and False non-match rate (FNMR), also known as Type II error or false rejection rate (FRR).Both methods focus on the system's ability to limit entry to authorized users. The lower a system's FMR, the better its security. The lower a system's FNMR, the easier it is to use. In general, for a given system and as the threshold is varied, the lower the FMR, the greater the FNMR. Therefore, there is often a trade-off between security and ease of use when using biometric systems.

3.4.2 The Role of Smart Cards with Biometrics

The role of smart cards with biometrics is as a powerful one-to-one verification-authentication technique for cardholder identity. Depending on the biometric system, the role of the smart card can be quite varied.

Two main uses for the smart card are discussed below. Match off-card. For this type of implementation, the enrolled template is initially loaded onto the smart card and then dispensed from the smart card via either contact or contactless interface when requested by the external biometric system.

The external equipment then compares a new live scan template of the biometric with the one being presented from the smart card. This implementation clearly has some security risks associated with transmitting the enrolled template off the smart card for every biometric challenge.

Appropriate security measures should be implemented to ensure the confidentiality and integrity of the released template. With this technique, the smart card is storing a template (or multiple templates), but has no significant knowledge of the type of biometric information, nor the ability to process it in any way. This implementation method is appropriate for all types of smart cards; this technique will work with memory, wired logic or microcontroller-based smart cards.

Match on-card. This implementation technique initially stores the enrollment template into the smart card's secure memory. When a biometric match is requested, the external equipment submits a new live scan template to the smart card. The smart card then performs the matching operation within its secure processor and securely communicates the result to the external equipment.

This method protects the initial enrollment template since it is maintained within the smart card and never transmitted off-card. Cardholder privacy is also maintained with this technique since the cardholder's biometric template information is not readable from the smart card. With this technique, the smart card must be a microcontroller-based device and be capable of computing the one-to-one match. One such implementation of match-on-card for fingerprint patterns is commercially available and has been implemented on several smart cards.

It is also important to note that Java Card API V2.2 supports the notion of a Biometric Manager that can use the on-card API to facilitate the secure match-on-card functionality.

3.4.3 Biometric Technology Benefits

Increased Security: Biometric information cannot be lost, stolen, or forgotten. It cannot be written down or discovered by social engineering. It cannot be shared with other users. In some biometric systems, it cannot, without duress, be used by anyone other than the individual.

By installing biometrics, organizations can positively verify users' identities, improving personal accountability (through positive identification of users in audit trails) and allowing high-value transactions to be offered at remote terminals and over the Internet.

In conjunction with smart cards, biometrics can provide strong security for PKI credentials held on the cards, thus providing greater trust in PKI services, especially digital signatures for non-repudiation.

A user is not required to present a card or remember a password or PIN. Since biometric information cannot be lost, stolen or forgotten, it is always available to the individual.

Organizations can eliminate the overhead of password management and improve customer service.

Organizations can implement recognition systems rather than simple authentication systems, so that users no longer have to manually logon to information systems.

3.4.4 Biometric Technology Risks

Privacy Concerns: Users, especially consumers rather than corporate users are concerned about the storage and distribution of biometric data. If an organization holds a central repository of templates, users have no control over the distribution of this data and are wary of: Misuse of the data (for example, illicit exchange with other organizations).

In the European Union, established data protection legislation might apply to biometric data as it does for other personal data for a living person. In the U.S. and elsewhere, regulatory statutes are required to provide safeguards.

Holding the user's reference template on a smart card is a way of mitigating this concern, but may give rise to manageability issues.

Other privacy concerns include fears about the ability to search records about a person and to monitor a person in real-time. This is a particular concern for consumer applications; however, corporate users also may see the specter of "Big Brother" if, for example, an organization places a video camera on every desk to implement iris or face recognition biometric systems.

When considering using smart cards with biometric systems, the smart card should be viewed as a privacy-enhancing technology. The smart card is able to augment the identity/biometric system, providing a secure container for the biometric template and having the ability to compute the biometric match within the card rather than on external equipment. The smart card can be viewed as the "local security officer" of the issuer for the day-to-day use of the ID by the cardholder.

Suitability for All Users: Between 1 and 3 percent of the general public do not have the feature required for mapping any one biometric. Users who are mute cannot use voice systems. Users lacking fingers or hands from congenital disease, surgery or injury cannot use fingerprint or hand systems. A biometric system that is, or is seen to be, socially regressive, in that it excludes the disabled and the old, may meet with principled resistance. A biometric system might be defeated by legal challenges on a number of grounds and may also be vulnerable to attackers who are or pretend to be disabled.

Any organization that wants to employ a biometric system must address this issue by providing a "fallback" system, not necessarily using another biometric. If these are less secure, then their use may yield an attack.

3.5 Smart Card Application

Applications of smart cards spread out over a wide scope. Their use in our 21st century day-to-day life is established, and most people in Western countries will have contact with a smart card in one way or another. This section aims to look at these applications, and present problems encountered, as well as advantages of the smart card.

3.5.1 Telephony and Broadcasting

Smart cards are used in these industries for three main applications:

1. Telephone cards for public (fixed) telephones
2. *Subscriber Identity Modules (SIMs) in mobiles*
3. Conditional Access (CA) modules in cable and satellite-broadcast networks

3.5.2 Telephone cards for public (fixed) telephones

Telephone cards were introduced as an answer to the problems that cash public phones entailed, such as being expensive to build, and to operate. The first card was made up of simple memory cards, and this has been improved upon giving us what we are now familiar with, the so-called third generation of telephone cards. This is based on the Infineon Euro-chip and other companies' variants. It has a dynamic challenge and response authentication method, which makes counterfeiting more difficult.

The traditional idea of a disposable card has now been replaced by a re-usable card that can be securely reloaded (topped up) from a linked account or a debit or credit card.

3.5.3 Subscriber Identity Modules (SIMs) in Mobiles

SIMs are smart cards used in GSM (global system for mobile telephony) phones, which was developed in response to the problems of the early mobile phones, where eavesdropping and fraudulent charges to accounts were carried out. GSM security aims to:

1. Authenticate the user
2. Protect the confidentiality of calls and call-related data

Mobile services have evolved to, but by no means replaced by, WAP services (Wireless Application Protocol), which allows telephones to display a subset of the HTML

(Hypertext Markup Language) used for Internet pages. This subset is known as the Wireless Markup Language (WML).

3.5.4 Conditional Access (CA) Modules in Cable and Satellite Networks

Subscription services to the cable and satellite channels are transmitted in an encrypted form, and the decryption is carried out in a set-top box, which is fitted with a smart card. The move to digital media means that a more extensive range of encryption can now be used but there are calls for a public key infrastructure to be developed for DVB (digital video broadcast) data applications.

3.5.5 Network Security

Traditionally access to a network involved a user inputting a password and using a username to gain access. The accompanying security threats accompanied by this system have prompted for smart card access, where it is an intelligent token used in conjunction with a password, usually a PIN.

Smart cards are one of the easiest forms of tokens to use. The card can check the password or PIN, which subsequently doesn't need to be stored in the system. The system authenticates the card, and the card authenticates the user. Indeed a smart card based sign-on mechanism of this type has been built into the NT operating system since 1998, and now forms a standard operation in Windows 2000.

3.5.6 Confidentiality of Data and Programs

Smart cards are used for the storage of keys needed to access stored data, and can enforce access control. They are also used for storage and loading of keys onto encrypting modems and other hardware devices used for encrypting data during transmission from one system to another.

3.5.7 Internet Browsing and E-mail

3.5.7.1 Public Key Infrastructures (PKI)

Most PKI packages include the option of using smart cards for carrying certificates and public keys, which gives a higher degree of security as well as portability.

3.5.7.2 E-mail

The standards that increase the security of some email typically recommend public key systems for authentication and transmission of a symmetric key, which is then used for the encryption of the body of the message. The private key for authentication can be stored on a smart card. This is relatively secure, and can be used on any computer fitted with a smart card reader.

3.5.7.3 E-Commerce

The recent surge in e-commerce means that there are a lot of companies out there that need security, as most of the transactions core to the business would be done over the unprotected Internet.

Indeed, e-commerce is one of the basic applications of smart cards. Here smart cards are used as electronic payment devices and also as enabling devices for wireless communication. Because they are linked to applications such as Internet e-commerce or pay-tv, e-payments can be seen as a meta-application. Another meta-application would be the use of smart cards for wireless communications, and this paves the way for mobile commerce (m-commerce). Payment methods and enabling methods on the Internet include:

1. Account payment and Open payments
2. Pre-registered card payments and virtual cards
3. Secured link (SSL connections) and the trusted third party (TTP)
4. Cash on delivery (where a signature is required to endorse credit card payments)
5. Digital cash
6. Electronic purse

3.5.8 Financial Applications

3.5.8.1 Bank Cards

So-called bank cards encompass account, ATM, debit, credit, and charge cards. The technology today allows bank cards to have a very high standard of interoperability. The Europay-MasterCard-Visa (EMV) standards are used by banks worldwide as a basis for smart debit and credit cards.

The implementation of EMV for credit and debit is being spearheaded by the UK, which expects to have 85% of its cards and 65% of transactions chip-based by 2003.

The smart card has been able to take the simple bank card to a higher level in the form of electronic purses. These are pre-paid cards, which are used in North America, sometimes called stored-value cards. The more modern electronic purses use public-key authentication. One of the first of these schemes was Mondex. This was unique in that it allowed card-to-card transactions, which do not pass through a merchant terminal but through a special wallet, which also contains a Mondex purse.

Mondex has been working with SmartAxis, a Netherlands-based firm that provides a payment service for companies selling goods over the Internet. They plan to provide e-purses for the growing market of 5-18 year olds who do not have access to credit cards. Although Mondex has had relative success with universities in the UK, in the open consumer market, it has failed to create a stir. Despite claims to have e-cash under development in 80 countries, it is a long way from breaking into the mainstream.

Other examples of electronic purses include vending machine cards. Indeed electronic purses in the form of smart card train tickets are being introduced onto London Transport under the direction of the ISG at Royal Holloway, University of London.

Electronic passbooks are also being planned, where records in an account (usually recorded by printing in a book) can be held by an account holder and a smart card authenticates the user.

3.5.8.2 A Closer Look

In 2000, HBSC Bank tested EMV payments on a MULTOS chip. This was to demonstrate that EMV smart card payments can be carried out on a MULTOS chip. This pilot was based in Northampton, which is the site of the first trials of UK banks smart cards. Those first trials were based on the UKIS chip (which Visa used), which has subsequently seen 8 million smart cards being issued with one in the UK. This is in contrast with 84 million of bank cards that need to be upgraded to smart cards in the UK.

In the HSBC pilot, the MULTOS chip carries the MasterCard version of the EMV standards. The pilot has demonstrated that MULTOS cards can be used in exactly the same way as UKIS cards.

3.5.9 Health Care

Using smart cards for healthcare applications is a highly political and controversial subject, and the level of use varies from country to country. However, it cannot be dismissed that the security and the storage advantages that smart cards bring will mean that in the future smart cards will be widely used in healthcare. The four most common uses for smart cards in healthcare are:

1. Insurance
2. Medical records
3. Prescriptions
4. Patient monitoring

3.5.9.1 Insurance

Smart cards used as insurance cards (without any medical application) control costs first and foremost. In France, the Sesame Vitale scheme has issued over 40 million cards to patients and 220,000 cards to doctors, pharmacists, and other health professionals.

3.5.9.2 Medical Records

The issue of storage that accompanies medical records cannot be solved by smart cards, at least at the standard of technology today.

However, smart cards can be used in combination with another card or storage medium to carry the data, control access to records, store important summary information, for specific applications, and so on.

3.5.9.3 Prescriptions

Because of the increasing need to control access to drugs, smart cards could be used for the operation of a simple prescription-handling system. This would not only prevent fraud, but it would form the basis for a control system with a double ended check on the issue and the dispensation of prescriptions.

Pilots of a smart card that hold individual patients' records are ongoing in the UK and India at the moment. The Royal Surrey County Hospital in Guildford, Surrey is just one of the hospitals involved. This smart card will run on the MULTOS operating system and will hold up to 40 pages of medical history.

Abroad, the Health Passport pilot in three Western US states is the largest multi-state, health-related smart card project of its kind in the US.

3.5.10 Transport

Smart cards can be used in various transportation applications. Contact-less cards are relatively cheap to use, and this has led to an explosion in chip-card based public transport schemes.

From local transportation to taxis, trains and air travel, smart cards can be used for a wide range of purposes. Road tolling is a classic example, as it uses RFID (radio frequency identification). Using a simple contact-less smart card could reduce the significant extra cost of fitting a sensor to each car.

Even parking system management can be improved with smart cards, as street furniture can be reduced simply by using a smart card that functions like a personal street meter.

A very good example of transport using smart cards in the UK is the London Underground and Transport, where several million contactless smart cards will be used for the Tube and bus journeys. This will be the first smart-card based mass transit system in the UK and is financed partly by the government's Private Finance Initiative.

Another sector to be updating to smart cards will be the long-haul transport vehicles on Europe's roads. In 2004, a system whereby all transport vehicles have to be fitted with a digital tachometer that reads smart cards will be introduced. This is mandated by the European Commission, and is expected to launch a new market for several million microprocessor smart cards a year.

3.5.11 Personal Identification

There are five main applications:

1. Identity card
2. Access control
3. Universities and schools
4. Government cards

Identity smart cards must be able to do two things: authenticate the user as well as the issuing organisation. Access control is widely needed for access to buildings. Here smart cards face competition from biometrics, bar code cards, and magnetic stripe cards.

Universities and schools use smart cards to record attendance, to pay for meals, to distinguish between students who pay more for meals, and those who don't, for instance.

3.5.12 Governments

A mixture of PKI and smart card technology is the solution of choice for eGovernment in Europe. National governments and private initiatives alike vouch their support for this powerful combination to deliver an essential layer of reliable electronic services and address identity requirements in a broad range of application areas.

The US federal government has also started developing MULTOS smart cards for its employees since 2000. The Smart Access Common ID card will provide building and systems access, electronic signature and authentication, and an e-purse.

Government cards could be used as smart passport cards, or national identity cards. Malaysia implemented a national smart card project which plans to issue a smart card to each citizen, who would then hold health details, be an e-purse, and an X.509 digital certificate for use in e-commerce transactions. Hong Kong has partnered with Australia's Keycorp to supply ID cards on the MULTOS operating system by mid-2004. Florida plans to incorporate MULTOS smart cards into their voting system in time for the next presidential election.

Conclusion

In today's world smart card play an increasingly important role in everyday life. If the main advantage of smart cards were to be summed up in one word, it would probably be "*Convenience*". We encounter them as credit cards, loyalty cards, electronic purse, health cards, and as a secure token for authentication or digital signature. Their small size and the compatibility of their form with the magnetic strip card make them the ideal carriers of personal information such as secret keys, passwords, and customization.

This project work, and through its all sections, has focused on the state of the art for smartcards and their use in computer and network security systems.

Obviously, special care was taken with "*Security features of Smart cards*". This is because smart cards have proven to be useful for transaction, authorization, and identification media. 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, smartcards could be used to voluntarily identify attributes of ourselves no matter where we are or to which computer network we are attached this is has to do with security principle of smart cards also.

An important characteristic of smart card is that the information on it cannot be copied. A credit card's magnetic stripe can easily be copied and then be misused. This could never happen with a smart card based credit card. Therefore, smart cards are recognized as the next generation financial transaction card.

Additionally, the Java Smart Card is under full development, various firms such as telecommunication operator which develop SIM card, firms which install advertisements in the street, or firms which install soft drink distributors firms plan to use Java Card technology. Within 10 years, Java Card is likely to become a systematically used standard. Java card development sets the tendency for the general use of Java in many fields

References

1- Schneier, B., "Applied Cryptography", John Wiley & Sons, 1996.

2- William Stallings, "Network security Essentials: applications and standards", Prentice Hall, Inc., 2000.

3- Schneier, B., “Secrets and Lies”, John Wiley & Sons, 2000.

4- Hendry, M. “Smart Card Security and Applications”, 2nd ed., Artech House Publishers, 2001.

5- Rankl W., Effing W., *Smart Card Handbook*, John Wiley & Sons, Inc., 2000.

6- Bright, Roy. "Smart Cards: Principles, Practices and Applications", Chichester: Ellis Horwood Limited, 1988.

7- Smart Cards: A Case Study (IBM SG24-5239), International Technical Support Organization, October 1998.

8- U.S. General Service General Administration, GOVERNMENT SMART CARD HANDBOOK, Feb. 2004, retrieved from:
, April 2004.