2.1. Introduction

A smart card is a portable, hand-held card, usually the size of a credit card, containing an embedded computer microchip. Smart card technology [1] provides the greatest degree of flexibility for future applications. In the modern day society, smart cards have proven to be convenient tokens for identification and authentication in day-to-day activities. Most of the people carry a collection of such cards with them whenever they leave home, be it credit cards, identification cards or perhaps a grocery store club card and a library card. Smart cards are small and convenient to carry and make certain information easily available. It makes sense that the progression of technology and the idea of technology would involve extending the idea of having small convenient data holding security. The smart cards will be as important as computers are today. There are more than million point-of-sale terminals and half a million ATM machines [2]. The most common method of identification is based on an Integrated chip card system.

A Smart Card is like an "Electronic Wallet"[3]. It is a standard credit card-sized plastic intelligent token within which a microchip has been embedded within its body and which makes it 'smart'. It provides not only memory capacity, but computational capability as well and thus the chip is capable of processing data. It has gold contacts that allow other devices to communicate with it. This chip holds a variety of information, from stored (monetary) value used for retail and vending machines to secure information and applications for higher-end operations such as medical/healthcare records. New information and applications can be added. Smart Cards can store several hundred times more data than a
conventional card with a magnetic stripe and can be programmed to reveal only the relevant information. The card may embed a hologram to avoid counterfeiting.

The integrated circuit also known as IC, microcircuit, microchip, silicon chip, or chip is a miniaturized electronic circuit consisting mainly of semiconductor devices, as well as passive components such as resistors, capacitors, microprocessors, or transistors, that has been manufactured in the surface of a thin substrate of semiconductor material. The sample smart cards are look like as shown in fig 2.1

![Smart Cards](image)

Fig 2.1: smart cards

"Key to the global village" that is how the Smart Card has been described. Smart Cards bring big changes to the way people provide and receive information and the way they spend money. The marriage between a convenient plastic card and a microprocessor allows information to be stored, accessed and processed either online or offline. Therefore, unlike the read-only plastic card, the processing power of Smart Cards gives them the versatility needed to make payments, to configure cell phones, TVs and video players and to connect to computers via telephone, satellite or the Internet anytime, anywhere in the world.

"The chip card is self-sufficient. Incorporating internal processing capabilities, the chip can follow its own programs and organize its own memory independent from network systems. This allows a consumer to have free reign to a myriad of functions and applications, Ex: Personal health and identification information, and communication access."[4].
Smart cards are indeed tiny computers; they provide the variety of applications that will be possible with them in the future. It's quite possible that smart cards will follow the same trend of rapid increases in processing power that computers have, following "Moore’s Law" and doubling in performance while halving in cost every eighteen months.

"With chip cards, people will be able to receive additional value in many areas outside the financial payments. These cards used for example, to store important health care information; function as a personal ID card with on-board passport to reduce the wait in customs lines at airports; store driver's license and other information; access a library or health club; control a company's inventory; or even - as has been suggested - be a person's key to the information superhighway".

The need for security and enhanced privacy in systems increasing the electronic forms of identification replace face-to-face and paper-based ones. The emergence of the global Internet and the expansion of the corporate network to include access by customers and suppliers from outside the firewall have accelerated the demand for solutions based on smart card technology. Some kinds of services that smart card technology enables are secure channel communications, digital signatures to ensure image integrity and confidentiality, authentication of a client to a server (and vice versa), and for strong authentication. Smart card systems are the best and most cost-effective computing systems for developing and deploying smart card solutions.

Smart cards use the same methods as a computer to secure information and authenticate encryption, public key cryptography, and challenge and response authentication. Smart card-based device is so secure that it can use its own on-board computer and software independently from the PC, mobile phone or other device to which it is attached. Secrets, like private keys, passwords and PINs, never leave the smart card, so spy ware or a person with
access to the PC cannot steal them. Other devices that want to communicate must first pass muster with the smart card, and it will only send secret information like passwords to a legitimate host system. Even then, any data exchanges will be encrypted so that any attempt at eavesdropping will fail as the information passes through the Internet.

Today, leaders in information security in large global industries such as government, oil, and pharmaceutical and information technology all use smart cards as part of a digital security strategy. The Defense Department has issued more than 10 million Common Access Cards. These are smart cards used for both physical access control and online identity authentication. Smart cards greatly improve the convenience and security of any transaction. They provide tamper-proof storage of user and account identity and also provide a system security for the exchange of data with practically any type of network. They protect against a full range of security threats, from slipshod storage of user passwords to experienced system hackers.

Smart cards will protect both privacy and provide the convenience of the networked world of the card or "application." Smart cards are diverse, ranging from simple single function cards like credit cards to cards serving multiple functions such as a student ID on a university campus, which allows access into buildings, pays for meals and serves as a library card. While diverse all share a common basic function: authentication. A driver's license, e-cash and even a door key are simply tools that authenticate or certify different things about the individual: a driver's license — their ability to drive and identity; e-cash — their ability to pay for goods; door key — their authority to enter a building.

Smart Card technology provides very safe and convenient way of controlling and restricting the access of individuals to the critical infrastructure for an organization. Based on the sensitivity, a building or infrastructure can be categorized into multi levels of desired security, and divided into security zones. Access to these zones is regulated through Smart
Card Reader controlled electronic/electromagnetic door locks. Smart Card and the Card holder is authenticated by these readers and the access privileges written on the card are read by the readers to control the release of lock.

Smart Card technology offers most promising way of storing digital data and conveniently transacting it for small business transactions. For security reasons, current credit card payment systems have made on-line connectivity mandatory for business transactions. This hugely increases the operational cost for the systems where amount of money per transaction is relatively smaller. This concept of e-Purse transaction can also be successfully applied in automatic vending machines, like milk vending, tea/coffee vending machines etc where seller’s card can be fixed inside the vending machines, and accumulated digital money collected in a desired frequency.

2.2. **Smart card-Micro Module**

Smart card is a single silicon integrated circuit chip with memory and microprocessor. The smart card gold connector plate is shown in fig 2.2 and its micro module in fig 2.3.

Fig 2.2: Smart card gold connector plate  
Fig 2.3: Smart card micro module

In general any micro module has eight metallic pads on its surface, each designed to international standards for
<table>
<thead>
<tr>
<th>Contact Name</th>
<th>Contact Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cl</td>
<td>VCC</td>
</tr>
<tr>
<td>C2</td>
<td>RST</td>
</tr>
<tr>
<td>C3</td>
<td>CLK</td>
</tr>
<tr>
<td>C5</td>
<td>GND</td>
</tr>
<tr>
<td>C6</td>
<td>VPP</td>
</tr>
<tr>
<td>C7</td>
<td>I/O</td>
</tr>
<tr>
<td>C4, C8</td>
<td>RFU</td>
</tr>
</tbody>
</table>

**VCC- Power supply voltage**

The power supply to the IC is defined to be between 4.75 volts and 5.25 volts with a maximum current consumption of 200mA. Newer chip fabrication technologies are moving to operate with a supply voltage of 3 volts which results in lower current consumption, by taking advantage of advanced semiconductor technology and allowing lower current levels to be consumed by the integrated circuit. Most card acceptor devices (CAD) operate at 5 volts as specified in the ISO standard. Whilst a 3 volt IC may be designed to operate between 3 volts and 5volts. Most 3-volt IC cards have a power consumption of between 10mA and 20mA (at 3.58MHz).

**RST-Reset**

Reset is the signal line that is used to initiate the state of the integrated circuit after power on. The reset signal is asserted by the interface device and is used to start up the program contained in the IC ROM. The ISO standard defines three reset modes, internal reset, active low reset and synchronous high active reset. Most microprocessor ICs are operated using the active low reset mode where the IC transfers control to the entry address for the program when the reset signal returns to the high voltage level. The sequence of operations for activating and deactivating the IC is defined in order to minimize the damage to the IC. In particular the inadvertent corruption of the non-volatile memory (EPROM or EEPROM) must be avoided.
The **IC Activation sequence** for the interface device as follows,

- Take RST low
- Apply VCC
- Put I/O in receive mode
- Put VPP in idle mode
- Apply clock
- Take RST high (active low reset)

The **IC Deactivation sequence** for the interface device is as follows,

- Take RST low
- Take clock low
- Deactivate VPP
- Put I/O in the low state
- Deactivate VCC

**CLK -Clock signal**

The **clock signal** is used drive the logic of the IC and is also used as the reference for the serial communications link. Although the integrated circuit could contain its own clock circuit for driving the internal logic, in practice most IC chips are supplied with an external clock by the interface device. It should be noted that the speed of the serial communications on the I/O line is effectively defined by the frequency of this clock. The ISO standard aligns with the use of two widely used external clock frequencies, 3.579545 MHz and 4.91522 MHz.

**GND (Vss)-Ground**

**Vss** is the substrate or ground reference voltage against which the Vcc potential is measured.
VPP-Programming or write voltage

The Vpp connector is used for the high voltage signal that is necessary to program the EPROM memory. This signal is designed to provide the high voltage required to enable writing to the non volatile memory. The more popular IC’s use EEPROM memory where the high voltage is generated by a charge pump on chip. However the EPROM memory type needs the high voltage to be externally provided on the IC connector. There have been problems in the past with terminals supplying the wrong programming voltage with somewhat drastic effects. Because of this and the significant advantages of having a rewriteable memory the EEPROM memory is by far the most popular for IC card applications, hence the role of VPP is rapidly diminishing.

I/O -Serial input/output line

The input/output (I/O) signal line which the chip receives commands and interchanges data with the outside world. The ISO standard defines a single line for the interchange of data between the IC and the interface device. This means that the line must change direction depending on whether the IC is transmitting or receiving. In practice this cannot be instantaneous and the expression 'line turn around time' is commonly encountered in the modem world. The transmission protocol must take account of this need to turn the line around. The transmission characteristics operated by most microprocessor IC cards are based on an asynchronous half duplex mode of operation.

In the T=0 communication protocol this involves the transmission of bytes

The T=1 protocol defines a block mode of operation.

RFU

The RFU two pads are reserved for future purpose
2.3. Smart card - Micro module Components and architecture

Memory cards [5] contain only non-volatile memory storage components, and perhaps some specific security logic. Microprocessor cards contain volatile memory and microprocessor components. The micro module on board the smart card [6] is made up of certain key components that allow it to execute instructions supporting the card’s functionality. The smart card micro module components are shown in fig 2.4.

![Smart card micro module components diagram](image)

**Fig 2.4: smart card micro module components**

The Microprocessor Unit (MPU) executes programmed instructions. Older version smart cards [7] are based on relatively slow, 8-bit embedded microcontrollers. The trend during the 1990s has been toward using customized controllers with a 32-bit Reduced Instruction Set Computing (RISC) processor [8] running at 25 to 32 MHz.

The I/O Controller manages the flow of data between the Card Acceptance Device (CAD) and the microprocessor.

**Memories**

Three types of memory are present on the smart card chip:

- **ROM.**
- **RAM** and
- Non-volatile memory like **EEPROM** or **Flash EEPROM** [9].

**Read Only Memory (ROM)** or Program Memory is where the instructions are permanently burned into memory by the silicon manufacturer. These instructions (such as when the power supply is activated and the program that manages the password) are the fundamentals of the Chip Operating System. The ROM [10] is programmed by mask during device fabrication.
Random Access Memory (RAM) or Working Memory serves as a temporary storage of results from calculations or input/output communications. RAM [11] is a volatile memory and loses information immediately when the power supply is switched off. The RAM of smart cards is currently Static RAM (SRAM). The main reason is the possibility to use a power-saving mode: when the CPU stays in sleep mode, the clock is fixed to the high or the low level permanently. Whereas a Dynamic RAM (DRAM) needs to be periodically refreshed, the SRAM doesn’t need this and the presence of the supply voltage is sufficient to retain the information. A SRAM cell occupies more die area than a DRAM cell (6 transistors vs. one transistor and a tiny capacitor), but this is compensated by the absence of refresh circuit for small memories (36...256 bytes). Several manufacturers master well the fabrication of SRAM [12], [13] and DRAM for some years now, with speed and power performances superior to conventional bulk silicon memories.

EE-PROM (Electrically Erasable Programmable Read-Only Memory), which is almost Application Memory, can be erased electronically and rewritten. By international standards, this memory should retain data for up to 10 years without electrical power and should support at least 10,000 read-write actions during the life of the card. Application memory [14] is used by an executing application to store information on the card. Most of the chip cards carry their user-specific information in an EEPROM or Flash EEPROM memory.

2.4. Smart card- Dimensions

In particular the standard defines more precisely the physical dimensions of the card as follows,

- **Width** 85.47mm - 85.72mm
- **Height** 53.92mm - 54.03mm
- **Thickness** 0.76mm ± 0.08mm
2.5. Types of Chip Cards

Smart cards are defined according to how the smart card data is read and written, and the type of chip [15] implanted within the card and its capabilities. There is a wide range of options to choose from when designing a system. The cards contain from one to three different types of embedded chip technologies: contact smart chip, Contactless smart chip and cards that contain two or more chip technologies are referred to as hybrid cards or combi cards. The types of smart cards are as shown in fig 2.6.
2.5.1. Contact Cards

This is the most common type of smart card. Electrical contacts located on the outside of the card connect to a card reader when the card is inserted. Cards the size of a conventional credit or debit card with a single embedded integrated circuit chip that contains just memory or memory plus a microprocessor. Contact Smart Card [16] shown in Fig 2.7 and are classified into two types. They are

1. Memory Cards

2. CPU/MPU Microprocessor Multifunction Cards

![Contact Smart Card](image1)

Fig 2.7: Contact Smart Card
Popular Uses of contact smart card:

- Network security
- Vending
- Meal plans
- Loyalty
- Electronic cash
- Government IDs
- Campus IDs
- e-commerce
- Health cards

2.5.1.1. Memory Cards

Memory cards have no sophisticated processing power and cannot manage files dynamically. All memory cards communicate to readers through synchronous protocols. In all memory cards they are used to read and write to a fixed address on the card. There are three primary types of memory cards:

1). Straight,
2). Protected, and
3). Stored Value.

2.5.1.1.1. Straight Memory Cards

These straight memory cards just store data and have no data processing capabilities. These cards cannot identify themselves to the reader, so the host system has to know what type of card is being inserted into a reader. These cards are easily duplicated and cannot be tracked by on-card identifiers. These cards are the lowest cost per bit for user memory.
2.5.1.1.2. Protected / Segmented Memory Cards

These cards have built-in logic to control the access to the memory of the card. Sometimes referred to as Intelligent Memory cards, these devices can be set to write protect some or the entire memory array. Some of these cards can be configured to restrict access to both reading and writing. This is usually done through a password or system key. Segmented memory cards can be divided into logical sections for planned multi-functionality. These cards are not easily duplicated but can possibly be impersonated by hackers. They typically can be tracked by an on-card identifier.

2.5.1.1.3. Stored Value Memory Cards

These cards are designed for the specific purpose of storing value or tokens. The cards are either disposable or rechargeable. Most cards of this type incorporate permanent security measures at the point of manufacture. These measures can include password keys and logic that are hard-coded into the chip by the manufacturer. The memory arrays on these devices are set-up as decrements or counters. There is little or no memory left for any other function. For simple applications such as a telephone card the chip has 60 or 12 memory cells, one for each telephone unit. A memory cell is cleared each time a telephone unit is used. Once all the memory units are used, the card becomes useless and is thrown away. This process can be reversed in the case of rechargeable cards.

2.5.1.2. CPU/MPU Microprocessor Multifunction Cards

A Microprocessor card [17] is a card with a micro controller chip, which contains a Processing Unit, volatile memory and non-volatile memory. Microprocessor cards, or smart cards, contain an entire computer with a processor (CPU), RAM, ROM and EEPROM. Smart cards offer a high storage capacity. Microprocessor cards are especially ideal for use where the very best security and protection mechanisms for sensitive data are demanded. Smart cards offer the very highest security and protection and ensure maximum authenticity and
confidentiality. As a result, the data can be secured against unwanted access and manipulation, for example. They enable identification and authorization, as well as optimum continuity, integrity and reliability.

Microprocessor cards contain a microprocessor, an operating system, and read/write memory that can be updated many times. The microprocessor card is like a miniature PC that can be carried in a wallet. The microprocessor card is the normally referred to as a smart card. These cards have on-card data processing capabilities. This type of smart card is the CPU/MPU Microprocessor Multifunction Card [18]. Multifunction smart cards [19] allocate card memory into independent sections, with each assigned to a specific task. Within the card is a microprocessor or micro controller chip that manages the memory allocation and file access. It has the ability to manage and access data in organized file structures by using card operating system.

2.5.2. Contactless Cards

The term **Contactless smart card** that does not need to make contact with the reader to be read, or swiped in a special slot. This capability is implemented using a tiny RFID tag [20] in the card. By the Contactless smart cards provide the user with greater convenience by speeding checkout or authentication processes.

Cards containing an embedded antenna instead of contact pads attached to the chip for to the chip for reading and writing information contained in the chip’s memory. These are the smart cards that employ a radio frequency (RFID) [21] between card and reader without physical insertion of the card. Instead the card is passed along the exterior of the reader and read. Types include proximity cards, which are implemented as a read-only technology for building access. These cards function with a limited memory and communicate at 125 MHz. True read & write contactless cards were first used in transportation for quick decrementing and re-loading of fare values where their lower security was not an issue. They communicate
at 13.56 MHz, and conform to the ISO14443 standard. These cards are often straight memory types. They are also gaining popularity in retail stored value, since they can speed-up transactions and not lower transaction processing revenues (i.e. VISA and MasterCard), like traditional smart cards. **Contactless Smart Card** shown in Fig 2.8.

**Fig 2.8: Contactless Smart Card**

Variations of the ISO14443 specification include A, B, and C, which specify chips from either specific or various manufacturers. Contactless card drawbacks include the limits of cryptographic functions and user memory versus microprocessor cards and the limited distance between card and reader required for operation.

The Internal Architecture of Contactless smart cards as have shown in Fig 2.9 use an antenna with approximately a 10- centimeter (cm) range to communicate with the reader. These credit card sized memory chip devices derive their power from an RF field generated by the card reader. The RF field also transfers information to and from the card and card reader. Employee identification badges issued by the organizations for building access are typically contactless smart cards.

**Fig 2.9: Internal architecture of Contactless Smart Card**
Popular Uses of Contactless Cards:

- Student identification
- Electronic passport
- Vending
- Parking
- Tolls
- IDs

2.5.3. Combination Cards

Cards containing one smart chip that can be accessed through either contact pads or an embedded antenna. These are hybrids that employ both contact and contactless technology in one card. Combi-cards can also contain two different types of chips in contrast to a Dual-Interface card where a single chip manages both functions. This diagram shows the top and bottom card layers which sandwich the antenna/chip module shown fig 2.10. This shows both the contact and contactless elements of the card.

Popular Uses:

- Vending
- Meal plans
- Loyalty

Fig 2.10: CombiCard
2.6. Evaluation-History and Earlier literature of Smart cards

The first plastic based card was issued by Diners Club. The roots of the current day smart card can be traced back to the United States, in the early 1950s, when Diner’s Club produced the first all plastic card to be used for payment applications. The use of the synthetic material PVC allowed for longer lasting cards than the previous conventional paper-based cards. The ancestor of data storage cards is most probably the calling card. In this system, a Diner’s Club card allowed you to pay with your name rather than cash. The card identified you as a member of a select group, and was accepted by certain restaurants and hotels that recognized this group.

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. However, these early cards were only capable of 'storing' embossed identification items (names, numbers, codes etc). VISA and MasterCard then entered the market, but eventually the cost pressures of fraud, tampering, merchant handling, and bank charges necessitated a machine-readable card. Interbank launched another system called MasterCard.

There are currently three main technologies in card technologies. These are magnetic stripe, smart cards, and optical cards. Other technologies can be put on cards as well (such as bar codes, touch memory, etc.).

**Magnetic stripe card**

The subsequent introduction of the magnetic stripe allowed additional digitized data to be stored on the cards in a machine-readable format. This type of embossed card with a magnetic stripe is still the most commonly used method of payment. The first use of magnetic stripes on cards was in the early 1960’s. London Transit Authority installed a magnetic stripe system in the London Underground (UK). By the late 1960’s BART (Bay Area Rapid...
Transit) (USA) had installed a paper-based ticket the same size as the credit cards we use today. Magnetic stripes were developed by the International Air Transportation Association (IATA) in the 1970's. This system used a stored value on the magnetic stripe, which was read and rewritten every time the card was used. Magnetic stripe card is shown in fig 2.11.

Fig 2.11: Magnetic stripe card

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.)

Magnetic stripe technology suffers from a critical weakness, however, in that anyone with access to the appropriate device can read, re-write, or delete the data. Thus a magnetic stripe card is unsuitable for storing sensitive data and, as such, requires an extensive online, centralized, back-end infrastructure for verification and processing.

Optical Memory Card

Optical memory cards use a technology similar to the one used for music CDs or CD ROMs. A panel of the "gold colored" laser sensitive material is laminated in the card and is used to store the information. Optical memory card can be seen in fig 2.12.
The material is comprised of several layers that react when a laser light is directed at them. The laser burns a tiny hole (2.25 microns in diameter) in the material, which can then be sensed by a low power laser during the read cycle. The presence or absence of the burn spot indicates a "one" or a "zero". Because the material is actually burned during the write cycle, the media is a write once read many (WORM) media and the data is non-volatile (not lost when power is removed). The optical card can currently store between 4 and 6.6 MB of data which gives the ability to store graphical images such as photographs, logos, fingerprints, x-rays, etc. The data is encoded in a linear x-y format and ISO/IEC 11693 and 11694 standards cover the details.

A much higher amount of data can be stored on optical cards. In this case, 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. Optical cards are used mainly in the medical sector where storage of the patient’s medical records [22] and perhaps even of X-ray photographs is needed.

2.7. Smart card standards

Standards are key to ensuring interoperability and compatibility in an environment of multiple card and terminal vendors. Integrated circuit card standards have been underway since the early 1980’s 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 70 nations. The ISO 7816 series is the international standard for integrated circuit cards. Smart card standards govern physical properties, communication characteristics, and application identifiers of the embedded chip and data.

**ISO - International Standards Organization (ISO)**

ISO 7816 is the internationally accepted standard for smart cards. ISO 7816 is a family of standards primarily dealing with aspects of smart card interoperability regarding communication characteristics, physical properties, and application identifiers of the implanted chip and data. This organization facilitates the creation of voluntary standards through a process that is open to all parties. ISO 7816 is the international standard for integrated-circuit cards or smart cards that use electrical contacts on the card, as well as cards that communicate with readers and terminals without contacts, as with radio frequency (RF/Contactless) technology. The ISO 7816 family includes eleven parts which are in a constant state of flux as they are subject to revision and update.

**ISO 7816-1**

Physical Characteristics, 1987; defines the physical dimensions of contact smart cards and their resistance to static electricity, electromagnetic radiation and mechanical stress. It also describes the physical location of an IC card's magnetic stripe and embossing area.

**ISO 7816-2**

Dimensions and Location of Contacts, 1988; defines the location, purpose and electrical characteristics of the card's metallic contacts.

**ISO 7816-3**

Electronic Signals and Transmission Protocols, 1989; defines the voltage and current requirements for the electrical contacts as defined in part 2 and asynchronous half-duplex...
character transmission protocol (T=0). Amendment 1: 1992, Protocol type T=1, asynchronous half duplex block transmission protocol.

ISO 7816-4

Inter-industry Commands for Interchange; establishes a set of commands for CPU cards across all industries to provide access, security and transmission of card data. Within this basic kernel, for example, are commands to read, write and update records.

ISO 7816-5

Numbering System and Registration Procedure for Application Identifiers (AID); sets standards for Application Identifiers. An AID has two parts. The first is a Registered Application Provider Identifier (RID) of five bytes that is unique to the vendor. The second part is a variable length field of up to 11 bytes that RIDs can use to identify specific applications.

ISO 7816-6

Inter-industry data elements; physical transportation of device and transaction data, answer to reset and transmission protocols. The specifications permit two transmission protocols: character protocol (T=0) or block protocol (T=1). A card may support either but not both.

ISO 7816-7

Inter-industry command for Structured Card Query Language (SCQL); this document specifies the concept of a SCQL database (SCQL = Structured Card Query Language based on SQL, see MS ISO 9075), and the related inter-industry enhanced commands.

ISO 7816-8

Commands for Security Operation; this document codifies internal card commands for security operations.
ISO 7816-9

Commands for Card Management; specifies a description and coding of the life cycle of cards and related objects, a description and coding of security attributes of card related objects, functions and syntax of additional inter-industry commands, data elements associated with these commands, and a mechanism for initiating card-originated messages.

ISO 7816-10

Electrical signals and answer to reset for synchronous cards; this part of ISO 7816 specifies the power, signal structures, and the structure for the answer to reset between an integrated circuit card(s) with synchronous transmission and an interface device such as a terminal.

ISO 7816-11

Personal verification through biometric methods; currently a draft. See the Bio API for more info.

FIPS (Federal Information Processing Standards)

FIPS Developed by the Computer Security Division within National Institute of Standards and Technology (NIST). FIPS standards are designed to protect federal assets including computer and telecommunications systems. The following FIPS standards apply to smart card technology and pertain to digital signature standards, advanced encryption standards, and security requirements for cryptographic modules.

FIPS 140 (1-3):

The security requirements contained in FIPS 140 (1-3) pertain to the areas related to the secure design and implementation of a cryptographic module, specifically: cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic
key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

FIPS 201:

Currently a draft, this specification will cover all aspects of multifunction cards used in identity management systems throughout the U.S. government.

2.8. IDEAL smart card

Security was the main purpose of smart cards from the early day. In case of the ideal smart card tamper resistance has utmost priority. The card manufacturer provides the card’s physical and the OS’s logical security. This is necessary to preserve the applications logical security.

1. The ideal smart card has **large storage capacity**. It is in the region of megabytes. High storage capacity is also necessary to enable the use of more complex applications.

2. The ideal card is capable of **Real Time Speech and Video Encryption**. This requires 3 things are Fast computation, Fast communication with the outside world, fast Cryptographic function.

3. The ideal smart card has an own **power supply** and **Timer**. Equipping a security oriented micro computer with timers increases its cryptographic potential. The own power supply enables it to run without the support of a reader.

4. The ideal smart card has a **long lifetime** (measure in decades). This is the fact of storing previous information on the card gives robustness even more importance. To increase the number of smart card based applications will definitely increase the number of smart cards held by one person. To solve this problem the ideal smart card runs multiple applications. These may change dynamically so that new applications can be downloaded to the card and deleted when they are not used. By the storage of
multiple applications they can also interact with each other and share data. Ex: Cardholder name, even code.

5. The card is programmed in high level-independent programming language, so that the code can be easily transferred from one card to another

6. The card can easily programmed because its interface with the standard IT devices. The standard devices are PC and Mobile Phones and communication through the Internet.

2.9. Smart cards in the future

The smart card can offer in abundance is security, honed over decades to deter hackers and counterfeitors. This is why financial institutions in much of the world have chosen smart cards for their payment cards and governments are relying on chips to safeguard information on electronic passports and many of their ID cards.

The smart cards have the same kind of protocols and interfaces as PCs and mobile phones. That would allow smart cards to communicate with these devices and enable a large pool of developers to write applications for them. That could change on the strength of another major technology.

The smart cards in future move to high-memory, high-speed smart cards in significant volumes are at least few years away, this other technology turn can be seen in future. And it promises to change the way issuers and cardholders use smart cards across all market segments. Governments are issuing the first passports equipped with contactless chips storing biometrics.

Flash can also replace the smart cards chips random-access memory in future, allowing issuers to avoid having the operating system burned into the chip. This greatly
speeds up the time it takes to get a new smart card onto the market. Flash is making greater inroads into smaller memory sizes, too, based on its time-to-market advantage.

"The identification market for smart cards will show tremendous growth in the near future," says Jason Halverson, an industry analyst for smart cards. From mini-Web server cards to contactless mobile phones and passports, smart card technology is transforming itself to play a major role in the convergence of the Internet and mobile networks, the development of new ways to pay, and the strengthening of security of national borders and corporate computer networks.

2.10. Smart card Reader

Smart Card Readers are also known as card programmers (because they can write to a card), card terminals, card acceptance device (CAD) or an interface device (IFD). There is a slight difference between the card reader and the terminal. The term 'reader' is generally used to describe a unit that interfaces with a PC for the majority of its processing requirements. In contrast, a 'terminal' is a self-contained processing device. Smart cards are portable data cards that must communicate with another device to gain access to a display device or a network. Cards can be plugged into a reader, commonly referred to as a card terminal, or they can operate using radio frequencies (RF).

Readers come in many forms, factors and capabilities. The easiest way to describe a reader is by the method of its interface to a PC. Smart card readers are available that interface to RS232 serial ports, USB ports, PCMCIA slots, floppy disk slots, parallel ports, infrared IRDA ports and keyboards and keyboard wedge readers. Card readers are used to read data from - and write data to - the smart card. Readers can easily be integrated into a PC utilizing Windows 98/Me, 2000, or XP platforms. Some card readers come with advanced security
features such as secure PIN entry, secure display and an integrated fingerprint scanner for the next-generation of multi-layer security.

When the smart card and the card reader come into contact, each identifies itself to the other by sending and receiving information. If the messages exchanged do not match, no further processing takes place. Communicating with a Smart Card Reader, the reader provides a path for an application to send and receive commands from the card. There are many types of readers available, such as serial, PCCard, and standard keyboard models. The manufacturer provides a different protocol for communication with the reader.

• First reader has to communicate with the reader.
• Second, the reader communicates with the card, acting as the intermediary before sending the data to the card.
• Third, communication with a smart card is based on the APDU format. The card will process the data and return it to the reader, which will then return the data to its originating source.

The following classes are used for communicating with the reader:

• ISO command classes for communicating with 7816 protocol
• Classes for communicating with the reader
• Classes for converting data to a manufacturer-specific format
• An application for testing and using the cards for an intended and specific purpose.
2.11. Applications and Advantages of Smart cards and smart card systems

Applications of a smart card are virtually limitless. A smart card, in conjunction with a card reader and suitable software, can store almost any type of information and there are several smart card applications in the market today.

A smart card is a portable computational device with data storage ability. As such, they can be a very reliable form of personal identification and a tamper-proof secure information repository. Smart cards are the self-containment and resistant to attack, as it does not need to depend upon potentially vulnerable external resources. Many of the applications of Smart Cards require sensitive data to be stored in the card, such as Identification, Security, Personal Medical history, Transportation, and Biometric applications, etc.

The first main advantage of smart cards is their flexibility. For example there is no need, to carry several cards. One card can simultaneously be an ID, a credit card, a stored-value cash card, and a repository of personal information such as telephone numbers or medical history. Therefore some smart card can store multi applications.

The second main advantage is security. Smart cards can be electronic key rings, giving the bearer ability to access information and physical places without need for online connections. They are encryption devices; so that the user can encrypt and decrypt information without rely.

Other general benefits of smart cards are Portability, Increasing data storage capacity, Reliability that is virtually unaffected by electrical and magnetic fields. Smart cards offer exciting possibilities for convenience, accuracy, customization, data security and cost reduction for individuals and organizations. The main possible applications of smart cards are the following explained below.
2.11.1. Financial Applications

The applications of smart cards include their use as credit or ATM cards, in a fuel card, SIMs for mobile phones, authorization cards for pay television, pre-pay utilities in household, high-security identification and access-control cards, and public transport and public phone payment cards.

Smart cards may also be used as electronic wallets. The smart card chip can be loaded with funds, which can be spent in parking meters and vending machines or at various merchants. Cryptographic protocols protect the exchange of money between the smart card and the accepting machine.

Banking & Retail

Smart banking cards can be used as credit, direct debit or stored value cards, offering a counterfeit- and tamper-proof device. The intelligent microchip on the card and the card readers use mutual authentication [26] procedures that protect users, merchants and banks from fraudulent use. Other services enabled by smart cards are advanced loyalty programs and electronic coupons.

Electronic Purse

Smart cards can be used as an electronic purse, which can store a nominated cash value on the card. This can then be spent in the same way as cash, at participating retailers. A smart card can be used to store a monetary value for small purchases. Card readers retrieve the amount currently stored, and subtract the amount for the goods or services being purchased. Groceries, transportation tickets, parking, Laundromats, cafeterias, and taxis some of the purchases that often do not reach amounts to justify the hassle of using a credit card.
Electronic Purse to replace coins for small purchases in vending machines and over-the-counter transactions. Credit and/or Debit Accounts, replicating what is currently on the magnetic stripe bankcard, but in a more secure environment. Securing payment across the Internet as part of Electronic Commerce [27].

These Cards can manage and control expenditures with automatic limits and reporting. Internet loyalty programs can be deployed across multiple vendors with disparate POS systems and the card acts as a secure central depository for points or rewards.

"Micro Payments" - paying nominal costs without transaction fees associated with credit cards or for amounts too small for cash, like reprint charges.

2.11.2. Transportation

- Mass Transit Fare Collection Systems.
- Electronic Toll Collection Systems.
- Drivers Licenses.
- Parking

With billions of transport transactions occurring each day, Smart Cards have easily found a place in this rapidly growing market. A few of the numerous examples of Smart Cards in transportation are:

**Mass Transit Ticketing** - Using Contactless Smart Cards allows a passenger to ride several buses and trains during his daily commute to work while not having to worry about complex fare structures or carrying change.
Electronic Toll Collection - As you drive through the toll gate of a bridge, a Smart Card, inserted into an RF transponder within your car, electronically pays the toll; without you ever stopping!

Drivers Licenses- Using Contact Smart Cards allows drivers to ride several buses with driver license card. The first smart card driver's license system in the world was issued in 1995 in Mendoza, a province of Argentina. Mendoza has a high level of road accidents, driving offenses, and a poor record of recovering outstanding fines. The smart licenses keep an up-to-date record of driving offenses and unpaid fines. They also store personal information, license type and number, and a photograph of the holder. Emergency medical information like blood type, allergies, and biometrics (fingerprints) can be stored on the chip if the cardholder wishes.

Gujarat was the first state in India to introduce the smart card license system in 1999. To date the Gujarat Government has issued 5 million smart card driving licenses to its people. This card is basically a plastic card having ISO/IEC 7810 certification and integrated circuit, capable of storing and verifying information according to its programming.

Parking - we don't need to carry the correct change anymore... just a prepaid contact Smart Card in our pocket.

Airline Application - The frequent flyer miles are added onto our airline Smart Card as our ticket is removed from it at the gate, eliminating paperwork!

2.11.3. Communication

The secure initiation of calls and identification of caller (for billing purposes) on any Global System for Mobile Communications (GSM) phone.
Mobile Communications

Smart cards are used as identification device for GSM digital mobile phones. The card stores all the necessary information in order to properly identify and bill the user, so that any user can use any phone terminal.

Telephony

Smart Cards are found in many applications where coin operated machines have suffered from the increased costs and loss of service from vandalism, coin collection, and low reliability. Single-function cards are being used for payphone telephony and digital mobile telephony. They are already being used as a replacement for cash at:

- Toll booths.
- Pay Phones.
- Parking lots.
- Gas stations.
- Vending machines.

There are over 300,000,000 GSM mobile telephones with Smart Cards, which contain the mobile phone security and subscription information. The handset is personalized to the individual by inserting the card, which contains its phone number on the network, billing information, and frequently call numbers.

There are over 100 countries worldwide, which have reduced or eliminated coins from the pay phone system by issuing Smart Cards. Germany, France, UK, Brazil, Mexico, and China have major programs.
2.11.4. Internet

The role of the Internet has developed to include the support of electronic commerce. It was designed for the free exchange of information, and as such, it is a rich supply of academic, product and service information. But how does an Internet shopper go from looking at the product to actually buying it. The Smart Card is the ideal support for payment over the Internet, whether in cash or as credit. However, the Internet shopper needs to connect his smart payment card to his computer and through the computer to the Internet. Smart Card readers are inexpensive, low-power devices, which can be easily added to existing computers. The additional cost of building them into future computers or peripherals is extremely low.

The Internet is focusing on the need for online identification and authentication between parties who cannot otherwise know or trust each other, and Smart Cards are believed to be the most efficient way of enabling the new world of e-trade. Smart Cards can act as an identification card, which is used to prove the identity of the cardholder.

Besides using Smart Cards for payment over the Internet, the possibilities are endless like carrying your favorite addresses from your own Personal Computer to your friend's Network Computer and downloading your airline ticket and boarding passes, tele-payments of the goods purchased online and such others.

2.11.5 Health Care

Smart cards allow the information for a patient's history to be reliably and safely stored. Health care professionals can instantaneously access such information when needed, and update the content [28]. Instant patient verification allows immediate insurance processing and refund. Doctors and nurses themselves can carry smart card-based IDs that
allow secure, multi-level access to private information. Various countries with national health care programs have deployed Smart Card systems. The largest is the German solution, which deployed over 80,000,000 cards to every person in Germany and Austria.

**Streamlining Healthcare Services**

In healthcare, Smart Cards may be used as Medical Cards [29] as Health Insurance Card or Medical File Access Card. This has the following advantages -

- Health Smart cards are small; they fit in every body’s pocket.
- Health Smart cards are very secure, can’t be read, copied, manipulated with, counterfeited, duplicated
- Health Smart card protect privacy where needed, Reduces routine paperwork.
- Health cards are re-writable
- Health Smart card can contain digital log with location, date, time, person’s stamp to record every transaction [30]
- Health Smart card can contain digital prescriptions, no mistakes with handwriting, quantity or quality of medications, Eliminates errors and fraud.
- Health Smart health card could be used anywhere, on the street by medical emergency crew to quickly learn about allergies and treatments, even if injured person is incapable to interact with anybody [31]
- Health Smart card can be set that certain profile of medical personnel can see only certain portion of card data, Speeds up payment and claim processes, Insurance, administrative and personal ID data are there
- Avoid long sign ups and clipboards at doctor’s offices, just insert card into the smart card reader
• Only after doctor presents his own medical professional smart card and his card and patient's card verify each other transactions can take place
• Inexpensive equipment setup.
• Patient controls doctors' access to information.
• Patient's medical history and data can be stored and becomes readily available using a card reader, Pharmacist has access to prescription information only.
• Small and inexpensive balance reader can read emergency data at any time anywhere
• Smart health cards speed up medical administration, put it in right format (HIPAA), process claims faster and more precisely
• Smart cards wherever implemented save hundreds of millions of administration, insurance, government money
• Smart health card [32] is actively fighting medical fraud and errors saving money and lives

Smart health care hardware is not expensive at all. Any PC can be set to read or read/write smart cards, there are portable readers, USB desktop readers, PIN pad readers, dual card readers...will not break you budget.

2.11.6. Identification

A quickly growing application is in digital identification cards. In this application, the cards are used for authentication of identity [33]. The computational power of smart cards allows running mutual authentication and public-key encryption software in order to reliably identify the bearer of the card. For higher security needs, a smart card is a tamper-proof device to store such information as a user's picture or fingerprints. Smart cards can be used also for network access: in addition or in alternative to user IDs and passwords, a networked computer equipped with a smart card reader can reliably identify the user.
A quickly growing application is in digital identification cards [34]. In this application, the cards are used for authentication of identity. The smart card will store an encrypted digital certificate issued along with any other relevant or needed information about the cardholder.

**Campus Badging and Access**

Businesses and universities of all types need simple identity cards for all employees and students [35]. Most of these people are also granted access to certain data, equipment and departments according to their status. Multifunction, microprocessor-based smart cards incorporate identity with access privileges and also store value for use in various locations, such as cafeterias and stores.

**2.11.7 Smart card -channel protocol TV satellite receiver**

Smart cards are widely used to protect digital television streams. Almost every small dish TV satellite receiver uses a Smart Card as its removable security element and subscription information. Subscriber activation of programming on Pay-TV.

**2.12. The scope of the Future**

The important thing about Smart Cards is that they are everyday objects that people can carry in their pockets, yet they have the capacity to retain and protect critical information stored in electronic form. The “smartness” of Smart Cards comes from the integrated circuit embedded in the plastic card. Embedding similar circuits in other everyday objects, such as key rings, watches, glasses, rings or earrings, could perform the same electronic function. The development of contactless card technology was the catalyst for what is known as tags. Tags function like contactless Smart Cards but are in the form of a coin, a ring or even a baggage label. They are generally attached to objects such as gas bottles, cars or animals and can hold
and protect information concerning that object. This allows the object to be managed by an information system without any manual data handling. The use of Biometrics will soon mean that his/her hand, fingerprint and the retina of the eye or the sound of the voice can reliably identify a person. Soon it will be possible to authorize the use of electronic information in Smart Cards by using a spoken word or the touch of a hand.

Also, Smart Card readers will be appearing on the PC and will enable the user to pay for goods purchased over the Internet. This will be especially useful for small value purchases, which are not really appropriate for credit card transactions. As a smart infrastructure for mobile computing, Smart Card technologies will prove to be the killer application for the networked economy. With all vast advantages if smart cards, an attempt has been made to design and develop a integrated Electronic Health Record System using contact and contact less (RFID) smart cards.
References:

1. Won Kim, He-Joon Kim, "Smart Cards: Status, Issues, and US Adoption", JOURNAL OF OBJECT TECHNOLOGY, Published by ETH Zurich, Vol. 3, No. 5, May-June 2004
2. Nalini K. Ratha and Ruud Bolle, "SMARTCARD BASED AUTHENTICATION", IBM T. J. Watson Research Center, Yorktown Heights, NY {ratha,bolle} @ Us. ibm. Com
3. Smart-card ICs secure secrets safe and sound, By Michael Ganzera, Marketing Manager, E-government & Smart Identity, Philips Semiconductors.
5. Smart card forum, www.smartcardforum.org, 26 Broadway suite 400 NEW YORK NY10004
6. The Government Smart Card Handbook by the General Services Administration Office of Government wide Policy and the Smart Card Interoperability Advisory Board (IAB) and was published in February 2004
16. John McCrindle, "Smart Cards", Published by IFS, 1990, Original from the University of Michigan, Digitized 11 Dec 2007
25. Rankl, Wolfgang “Smart Card Applications: Design models for using and programming smart cards”.


29. Health Cards '97, By L. Van den Broek, A. J. Sikkel, Published by IOS Press

30. Dr Jim Briggs, Dr Roger Beresford, “Smart cards in health”, Healthcare Computing Group, University of Portsmouth, Portsmouth, PO1 3AE


32. eEurope Smart Cards: “Smart cards Evolution in the Health Area” – A Requirements survey. TrailBlazer 11 Health white Paper v 0.55 2002.


35. Arami, Mitra, Vienna, Vienna, Krimmer, Robert, “USER ACCEPTANCE OF MULTIFUNCTIONAL SMART CARDS” Vienna University, Vienna, Austria

*****