CHAPTER 1

SMART CARDS
A smart card is a type of chip card, is a plastic card embedded with a computer chip that stores and transacts data between users. This data is associated with either value or information or both and is stored and processed within the card’s chip, either a memory or microprocessor. The card data is transacted via a reader that is part of a computing system [1]. Smart card-enhanced systems are in use today throughout several key applications, including healthcare, banking, entertainment and transportation.

Even the name Smart Card captures the imagination, however such a term is ambiguous and is used in many different ways. ISO uses the term, Integrated Circuit Card (ICC) to encompass all those devices where an integrated circuit is contained within an ISO1 identification card piece of plastic. The card is 85.6mm x 53.98mm x 0.76mm and is the same as the ubiquitous bankcard with its magnetic stripe that is used
as the payment instrument for numerous financial schemes. Integrated Circuit Cards come in two forms, contact and contact less. The former is easy to identify because of its gold connector plate. Although the ISO Standard (7816-2) defined eight contacts, only 6 are actually used to communicate with the outside World. The Contact less card may contain its own battery, particularly in the case of a "Super Smart Card" which has an integrated keyboard and LCD display. In general however the operating power is supplied to the contact less card electronics by an inductive loop using low frequency electronic magnetic radiation. The communications signal may be transmitted in a similar way or can use capacitive coupling or even an optical connection.

The Contact Card is the most commonly seen ICC to date largely because of its use in France and now other parts of Europe as a telephone prepayment card. Most contact cards contain a simple integrated circuit although various experiments have taken place using two chips. The chip itself varies considerably between different manufacturers.

1.2. Types of Smart Cards

Integrated circuit cards come in two forms, contact and contact less. These shown in fig1.1. The former is easy to identify because of its gold connector plate. The ISO standard (7816-2) defined eight contacts only 6 are actually used to communicate with the outside world. The contact less card may contain its own battery, particularly in the case of a "super Smart Card" which has an integrated keyboard and LCD display. In general however the operating power is supplied to the contact less card electronics by an inductive loop using low frequency electro magnetic radiation.
The contact card is the most commonly seen ICC to date largely. Most contact cards contain a simple integrated circuit along various experiments have taken place using two chips. The chip itself varies considerably between different manufacturers. Smart cards are defined according to the type of chip implanted in the card and its capabilities. There is a wide range of options to choose from when designing your system.

Vcc is the supply voltage that drives the chips and is generally 5 volts. It should be noted however that in the future we are likely to see a move towards 3 volts taking advantage of advanced semiconductor technology and allowing much lower current levels to be consumed by the integrated circuit.

Vss, ground reference voltage against which the Vcc potential is measured.

Reset is the signal line that is used to initiate the state of the integrated circuit after power on. This is in itself an integral and complex process that we shall describe later in more detail.

The clock signal is used drive the logic of the IC and is also used as the reference for the serial communications link. There are two commonly used clock speeds 3.57 MHZ and 4.92 MHZ. The lower speed is most commonly used, may change in the future.

Vpp connector is used for the high voltage signal that is necessary to program the EPROM memory.

The serial input/output (SIO) is the signal line by which the chip receives commands and interchanges data with the outside world.
Increased levels of processing power, flexibility and memory add cost. Single function cards are often the most cost-effective solution.

Memory Cards

Memory cards have no sophisticated processing power and cannot manage files dynamically. All memories communicate to readers through synchronous protocols. Smart card electrical contacts are shown in fig1.2. There are three primary types memory cards:

![Diagram of Memory Cards and Microprocessor Cards](image-url)
Straight Memory Cards

These cards just store data and have no data processing capabilities. These cards are the lowest cost per bit for user memory.

Protected / Segmented Memory Cards

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

Stored Value Memory Cards

These cards are designed for the specific purpose of storing value or tokens. The cards are either disposable or rechargeable. Most cards of this type incorporate permanent security measures at the point of manufacture. These measures can include password keys and logic that are hard-coded into the chip by the manufacturer. 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.
Fig 2. Smart Card ELECTRICAL CONTACTS

CPU/MPU Microprocessor Multifunction Cards

These cards have on-card dynamic data processing capabilities. Multifunction smart cards allocate card memory into independent sections assigned to a specific function or application. Within the card is a microprocessor or microcontroller chip that manages this memory allocation and file access. This type of chip is similar to those found inside all personal computers and when implanted in a smart card, manages data in organized file structures, via a card operating system (COS). Unlike other operating systems, this software controls access to the on-card user memory. This capability permits different and multiple functions and/or different applications to reside on the card, allowing businesses to issue and maintain a diversity of ‘products’ through the card. One example of this is a debit card that also enables building access on a college campus.

EX: CardLogix operating system
1.3. READER AND TERMINAL BASICS

The term "Reader" is 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.

Both terminals and readers read and write to smart cards. Readers come in many form factors and in a wide variety of 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.

1.4. STANDARDS

Smart card standards govern physical properties and communication characteristics of the embedded chip and are covered through the ISO 7816-1,2,3.

The International Standards Organization (ISO) 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 (commonly known as smart cards) that use electrical contacts.

ISO 7816 Summary This is a quick overview of what the 7816 specifications cover. Some of these are frozen and some are in revision; ISO 7816 has six parts. Some have been completed others are currently in draft stage.

Part I

Physical characteristics-ISO 7816-1:1987 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.

Part 2

Dimensions and Location of Contacts- ISO 7816-2: 1988 defines the location, purpose and electrical characteristics of the card’s metallic contacts

Part 3


Part 4

Inter-industry Commands for Interchange- ISO 7816-4 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.

Part 5

Numbering System and Registration Procedure for Application Identifiers- ISO 7816-5:1994 establishes standards for Application Identifiers (AIDs). 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.

Part 6

Inter-industry data elements- ISO 7816-6 Details the 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. (Note: Some card
manufacturers adhere to neither of these protocols. The transmission protocols for such
cards are described as T=14).

1.5. EARLIER LITERATURE OF SMART CARD SYSTEMS

A smart card is a credit card in size and shape, but inside it is completely
different. First of all it has, inside -- a normal credit card is a simple piece of plastic. The
inside of a smart card usually contains an embedded 8-bit microprocessor [2]. The
microprocessor is under a gold contact pad on one side of the card. Think of the
microprocessor as replacing the usual magnetic stripe on a credit card or debit card.

Smart cards are much more popular in Europe than in the U.S. In Europe the
health insurance and banking industries use smart cards extensively. Every German
Citizen has a smart card for health insurance. Even though smart cards have been
around in their modern form for at least a decade, they are just starting to take off in the
U.S.

Magnetic stripe technology remains in wide use in the U.S. However, the data on
the stripe can easily be read, written, deleted or changed with off-the-shelf equipment.
Therefore, the stripe is really not the best place to store sensitive information. To protect the consumer, businesses in the U.S. have invested in extensive online mainframe-based Computer networks for verification and processing. In Europe, such an infrastructure did not develop and instead the card carries the intelligence. There are advantages and disadvantages to both systems.

The microprocessor on the smart card is there for security. The host computer and card reader actually "talk" to the microprocessor. The microprocessor enforces access to the data on the card. If the host computer read and wrote the smart card's random access memory (RAM), it would be no different than a diskette. Smarts cards may have up to 1 Kbytes of RAM, 16 Kbytes of programmable read only memory, 24 Kbytes of read only memory (ROM), with an 8-bit microprocessor running at 5 MHz. The smart card uses a serial interface and receives its power from external sources like a Card Reader [3]. The processor uses a limited instruction set for applications such as Cryptography.

Smart cards can be used with a smart card reader attachment to a personal Computer to authenticate a user. Web browsers too, can use smart card technology to Supplement Secure Sockets Layer (SSL) for improved security of Internet transactions. The recent American Express Online Wallet shows how online purchases work using a Smart card and a PC equipped with a smart card reader. Smart card readers can also be found in mobile phones and vending Machines.
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.

Today, there are three categories of smart cards, all of which are evolving rapidly into new markets and applications:

1. Integrated Circuit (IC) Microprocessor Cards.
2. Integrated Circuit (IC) Memory Cards.
3. Optical Memory Cards.

**Integrated Circuit (IC) Microprocessor Cards.**

Microprocessor cards (also generally referred to by the industry as "chip cards" or "IC cards") offer greater memory storage and security of data than a traditional Magnetic stripe card. Smart cards that are chip cards or IC cards also can process data on the card. The current generation of chip cards has an eight-bit processor, 16KB read-only memory, and 512 bytes of random-access memory. This gives them the equivalent processing power of the original IBM-XT computer, albeit with slightly less memory capacity [4].

These smart cards are used for variety applications, especially those that have Cryptography built in, which require manipulation of large numbers. Thus, chip cards have been the main platform for cards that hold a secure digital identity. Some examples of these cards are:

- Cards that hold money ("stored value cards")
- Card that hold money equivalents (for example, "affinity cards")
Cards that provide secure access to a network

- Cards that secure cellular phones from fraud
- Cards that allow set-top boxes on televisions to remain secure from piracy

Integrated Circuit (IC) Memory Cards.

IC memory cards can hold up to 1-64 KB of data, but have no processor on the Card with which to manipulate that data. Thus, they are dependent on the Smart Card Reader (also known as the card-accepting device) for their processing and are suitable for uses where the card performs a fixed operation.

Memory cards represent the bulk of the million smart cards sold, primarily for pre-paid, disposable-card applications like pre-paid phone cards. Memory cards are popular high-security alternatives to magnetic strip cards [5].

Optical Memory Cards.

Optical memory cards look like a card with a piece of a CD glued on top - which is basically what they are. Optical memory cards can store up to 4 MB of data. But once written, the data cannot be changed or removed. Thus, this type of card is ideal for record keeping - for example medical files, driving records, or travel histories. Today, these cards have no processor in them (although this is coming in the near future).

While the cards are comparable in price to chip cards, the card readers use non-standard protocols and are expensive.

The first smart card was developed in 1974, by independent inventor Roland Moreno. Smart card use in Europe and Asia is outpacing North America, but smart Card growth is expected to continue at a brisk pace.
By way of comparison, there are over 900 million credit cards in circulation today. Major uses will include providing enhanced financial services, increasing the security and flexibility of cellular phones, and securing satellite and cable transmissions in TV set-top boxes. Different types of smart cards are shown in Photograph 1.

Why Smart Cards

Smart cards greatly improve the convenience and security of any transaction. They provide tamper-proof storage of user and account identity. Smart cards also provide vital components of system security for the exchange of data throughout virtually any type of network. They protect against a full range of security threats, from careless storage of user passwords to sophisticated system hacks. Multifunction cards can also serve as network system access and store value and other data.

How the IC card is made

The manufacture of a smart card involves a large number of processes of which the embedding of the chip into the plastic card is key in achieving an overall quality product. The whole operation starts with the application requirements specification. From the requirements individual specifications can be prepared for the chip, card, mask ROM software and the application software. The ROM software is provided to the semiconductor supplier who manufactures the chips. The card fabricator embeds the chip in the plastic card. It is also quite normal for the fabricator to load the application software and personalization data. Security is a fundamental aspect in the manufacture of a smart card and is intrinsic to the total process.
Photograph 1: Different Types of Smart Cards
1.6. APPLICATIONS

First introduced in Europe over a decade ago, smart cards debuted as a stored value tool for pay phones to reduce theft. As smart cards and other chip-based cards advanced, people found new ways to use them, including charge cards for credit purchases and for record keeping in place of paper.

In the U.S., consumers have been using chip cards for everything from visiting libraries to buying groceries to attending movies, firmly integrating them into our everyday lives. Several states have chip card programs in progress for government applications [6] ranging from the Department of Motor Vehicles to Electronic Benefit Transfer (EBT).

Many industries have implemented the power of smart cards into their products such as the new GSM digital cellular phones to TV-satellite decoders. People worldwide are now using smart cards for a wide variety of daily tasks, these include:

**E-Commerce**

Smart cards make it easy for consumers to securely store information and cash for purchasing. The advantages they offer consumers are:

The card can carry personal account, credit and buying preference information that can be accessed with a mouse click instead of filling out forms.

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.
Health Care

The explosion of health care data brings up new challenges to the efficiency of patient care and privacy safeguards. Smart cards solve both challenges with secure storage and distribution of everything from emergency data to benefits status [7].

Rapid identification of patients; improved treatment

A convenient way to carry data between systems or to sites without systems.

Reduction of records maintenance costs.

Telecommuting And Corporate Network Security

Business to business Intranets and Virtual Private Networks “VPNs” are enhanced by the use of smart cards. Users can be authenticated and authorized to have access to specific information based on preset privileges. Additional applications range from secure email to electronic commerce.

Campus Barging and Access:

Businesses and universities of all types need simple identity cards for all employees and students. Most of these people are also granted access to certain data, equipment and departments according to their status. Multifunction, microprocessor-based smart cards [8] incorporate identity with access privileges and also store value for use in various locations, such as cafeterias and stores.
REFERENCES


2. Smart Card Tutorial, *Published in October 1992 BY David B Everett.*

3. Smart card detail from smart card supply.com

4. A technical overview of smart card technology is provided at the following IBM site: [http://www.chipcard.ibm.com/overview/sc_2.htm](http://www.chipcard.ibm.com/overview/sc_2.htm)

5. IBM provides information on its chip card at: [http://www.chipcard.ibm.com](http://www.chipcard.ibm.com)


7. The Open Card Framework site is accessible at: [http://www.opencard.org](http://www.opencard.org)

8. Gem plus offers a variety of smart card options: [http://www.gemplus.com](http://www.gemplus.com)