Battery Operated Smart Card Reader

Notes compiled by :
Asst. Prof. Melina Maria Afonso
Department of Computer Engineering
Goa College of Engineering,Farmagudi

Course: Embedded System Design
Semester: VI
TE Computer Engineering

Introduction:

These notes are divided into two parts. The first part will cover a basic study of smart cards which will include the classification, types and architecture of smart cards.

The second part will be about the design of a Battery Operated Smart Card Reader. We will list the various Tasks involved in reading a smart card, discuss an example hardware configuration of a smart card reader and the details of how each task is carried out.

Though this is a study the smart card reader we need to understand that we have to study smart cards as we will be designing the reader based on the type of smart card. Also a smart card is a good application of a microcontroller. Hence the emphasis on basic study of smart cards too.

Smart Cards

- A smartcard is a credit card sized plastic card containing a memory or a 'CPU and memory' which is commonly used by us all
- A Smartcard contains memory in the order of a few bytes to a few kilo bytes.
- For this card to be useful it should be read. A smart card is connected to the host computer or controller via a card reader. Reader gets information from the smart card and accordingly passes the information to the host computer or controller.
- For a card or any device to be able to work it has to have some source of power. The card itself does not have a power source but is powered up by the card reader.
- A few examples are Credit card, debit card, medical insurance card, license etc
- Smartcard follows a specific command sequence for data read/write operations.

Generalized Smart Card System

Figure 1 is a pictorial depiction of a Smart Card system. As you can see there is an owner of the smart card. This smart card will be read by a reader and the data will be passed on to the host system for processing.

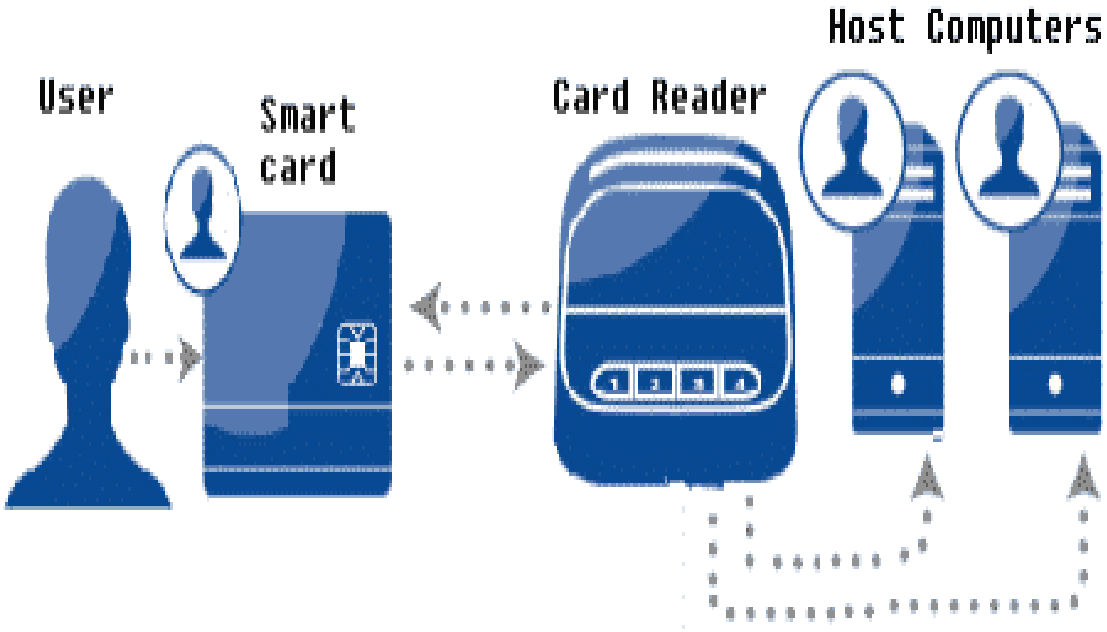

Figure 1: Generalized Smart Card System

The chip on a smart card can be either, a microcontroller/ microprocessor or an embedded memory chip depending on the application of the card. Those cards with microcontroller chips can perform on-card processing functions and can manipulate information in the chip's memory; they can perform read- write- delete operations.

Categorization of Smart Cards

Smart cards can be broadly classified based on the following areas: (Figure 2)

1) The way they interface with the card reader(Mechanism)
2) The type of chip(Configuration- memory or Processing unit)

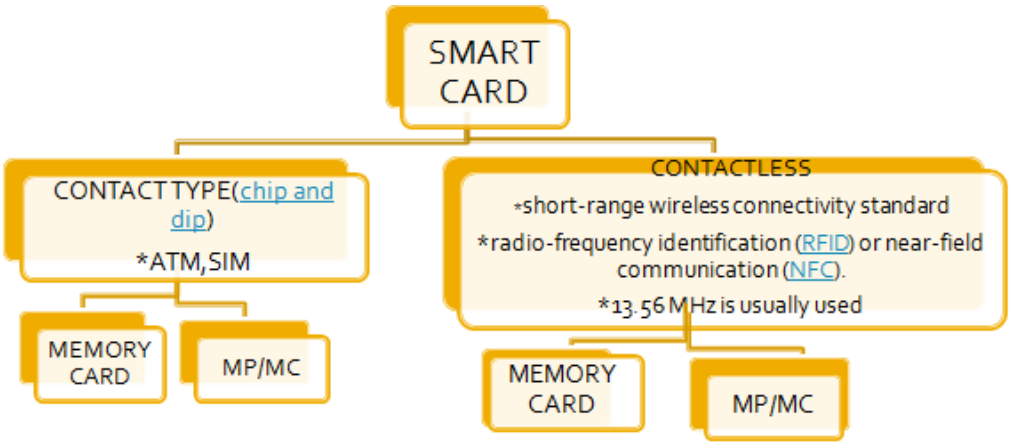

Figure 2: Categorization of Smart Cards

1) The way they interface with the card reader:
   - Contact type

     The Contact type smartcard requires physical contact between the reader and the smartcard. The contact type smartcard follows the ISO-7816 standard and its physical contact looks exactly the same as that of the contacts of a GSM cell phone's SIM card.
   - Contactless

     The contactless smartcard doesn't require a physical contact between the reader and the smartcard for data communication. The data communication for a contactless smartcard happens over air interface and it uses radio frequency waves for data transmission. 13.56 MHz is the commonly used radio frequency for smartcard operation. 13.56 MHz is the commonly used radio frequency for smartcard operation.

2) The type of chip
   - Memory cards
   - Processing Unit

Types of Smart Cards

This is a list of smart cards based on their areas of classification and their application:

- Contact Smart Cards
- Contactless Smart Cards
- Dual- Interface Cards
- Hybrid Cards
- Cash Card
- Debit Card
- Control Access Card

- Contact type

  The Contact type smartcard requires physical contact between the reader and the smartcard. The contact type smartcard follows the ISO-7816 standard and its physical contact looks exactly the same as that of the contacts of a GSM cell phone's SIM card.
- Contactless

  The contactless smartcard doesn't require a physical contact between the reader and the smartcard for data communication. The data communication for a contactless smartcard happens over air interface and it uses radio frequency waves for data transmission. 13.56 MHz is the commonly used radio frequency for smartcard operation. 13.56 MHz is the commonly used radio frequency for smartcard operation.
- Dual Interface Smart Card

  Also called the combi card that provides greater payment processing convenience as they can be used with both contact and contactless payment terminals. So there is a single chip with two modes of reading the card.

- A hybrid smart card, or hybrid card

Contains more than one card technology. A good example of a hybrid smart card is a card that contains an embedded microprocessor smart card chip in addition to a contactless RFID proximity chip. So there are multiple chips on a single card space.

- Cash and debit cards

Both allow you allow you to make ATM withdrawals. However a debit card also allow you to pay directly for goods and services in any place where your card's payment network is accepted.

- Access Control Cards

Also there are cards which give you access to a certain area. Smart cards contain a computer chip programmed with personal information about the cardholder and the access point or points the individual is allowed to enter.

This is a compilation of various cards and card readers in Figure 3. There is a commonly seen reader which you see at a petrol pump or a mall or a shop. There are slightly different versions. Then we have card readers in our laptops as well. There is a contactless card which using some wireless technology to read it.

Figure 3: Various cards and card

Physical Components of a Contact less Smart Card

Let us get into a few more details about the Physical Components of a Contact less Smart Card

So if you have a look at figure 4 you understand better. There is a contact pad beneath which here is the smart card. The plastic layer on the top and below sandwich the layer having the antenna. This antenna coils around the card.

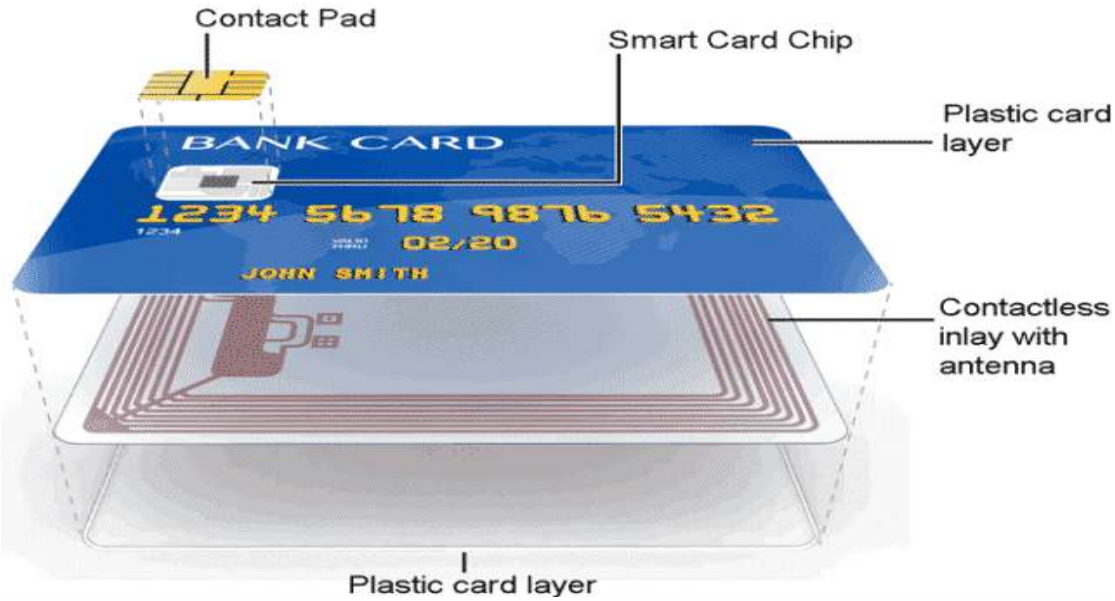

Figure 4: Physical Components of a Contact less Smart Card

Chip Module on Smart Card

This is a more detailed contact pad layout. You can recognize the various connections. This circuit diagram can also be seen on your SIM if you have noticed.

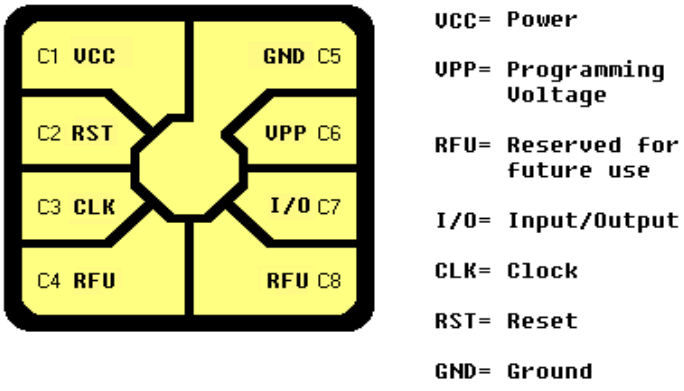

Figure 5: Chip Module on Smart Card

Example Configuration Of a smart card

As we have discussed the smart card could have a processing unit. If so it will have to have a microcontroller/ microprocessor to manage its operations. Here is an example of an 8051 based Smart card unit.

- **Central Processing Unit:**8 bit to 16-bit CPU. 8051 based designs are common.
- **Memory System: few bites to few kilobytes**
  - RAM : 1 - 8 kilobytes of RAM
  - EEPROM: Between 1 to 24K
  - ROM: Between 8 to 24K
- **Input/Output**
- **Serial I/O Interface**
- **Operating Systems**
- **File Systems**
- **Software**

The complexity and size of the operating system depends on the application of the card. Just like any other device which uses a microcontroller the Operating system could comprise of a full fledged operating system to a few basic set of instructions.

Smart Card Architecture

Based on the above configuration we can now represent the architecture in the Figure 6.

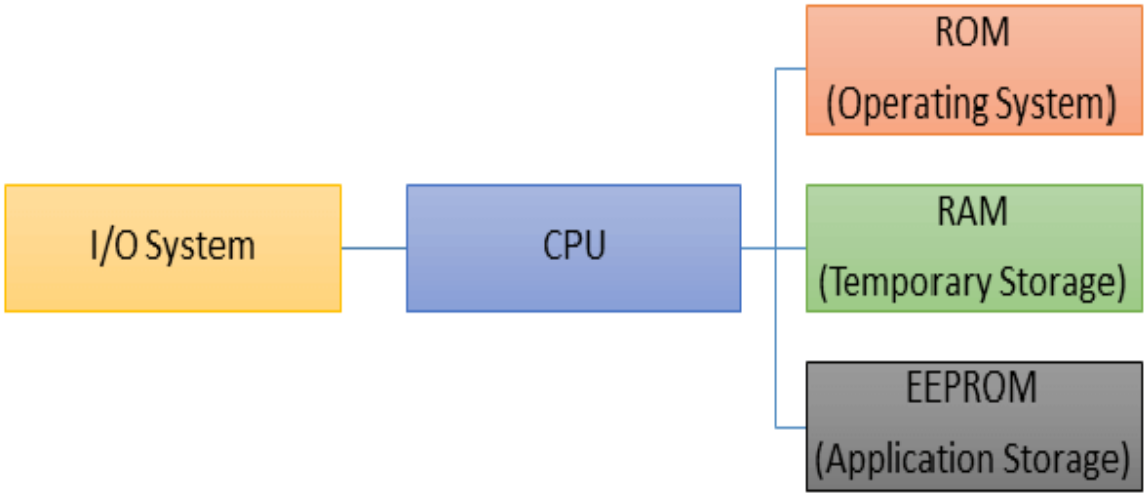

Figure 6: Smart Card Architecture

The design of these smart cards follow the **International Standards Organization (ISO) /International Electrotechnical Commission (IEC) Standards**

- ISO/IEC is one of the worldwide standard-setting bodies for technology, including plastic cards.
- The primary standards for smart cards are ISO/IEC 7816, ISO/IEC 14443, ISO/IEC 15693 and ISO/IEC 7501.

Design of a battery operated contactless smartcard reader (Handheld Reader)

A card reader is a data input device that reads data from a card-shaped storage medium (Figure 7). It will have a processing unit in order to read the cards.

Figure 7: Contactless Smart Card Reader

In order for this card reader to work you can now think of the tasks if would have to do from the time it is turned on. So think in terms of the study of the microcontroller.

Tasks

The firmware requirements for building the handheld smartcard reader can be divided into the following tasks.

1. Startup task
2. Battery monitoring and Charge controlling task
3. Card read/write operation task
4. Communication Task
5. Keyboard scanning task
6. LCD update task
7. Watchdog timer expire event

The details of each are discussed later.

In order to perform these tasks supporting hardware will be needed for this design which will be the host processor and additional processing units not inbuilt in the host processor. These will be interfaced with the host processor.

Hardware

The following are the hardware components:

- **BATTERY: rechargeable Li-Io battery** (Say 7V with capacity lOOOmAh) is used as the power source for the handheld.

- **Battery monitor and charge control IC**:The batteiy parameter (capacity and
- voltage) monitoring and charging is controlled using a battery monitor and charge control IC (Like DS2770 from Maxim Dallas Semiconductor).

- **The host processor**:The host processor can be an 8 or 16bit microcontroller (Like 8051 or PIC family of controller).

- **ON/OFF BUTTON:** The device power ON is controlled through a push button switch.

- **Contactless smartcard read/write IC**: A single chip contactless smartcard read/write IC is used for data read write operation with the smartcard. The smartcard reader IC is interfaced to the host processor and the data communication will be under the control of the host processor. The smartcard read/write IC contains CPU (Or control logic implementation), read/write memory, analog circuits for data modulation and demodulation, transceiver unit for RF data transmission and reception, and antenna driver circuitry. For the handheld reader to communicate with a desktop machine, a communication channel using either USB or RS-232C is implemented in the reader.

- **The I/O unit:** The I/O unit of the system includes a
  - matrix keyboard for user inputs
  - a graphical/alpha-numeric LCD for visual indications
  - LEDs are used for various status indications like ‘Charging’, ‘Battery Low’, ‘Busy/Error’, etc.

- **The Oscillator and Reset circuitry**: The Oscillator and Reset circuitry generates the necessary clock and reset signals for the proper operation of the host processor and smartcard read/write IC.

- **The watchdog timer:** The watchdog timer unit provides the necessary reset to the system in case of system misbehaviour. Sometimes the watchdog timer hardware comes as part of the host processor; if not a separate watchdog timer IC is used. The watchdog interrupt is connected to one of the interrupt lines of the processor.

- **External Memory:** Most of the microcontrollers contain built in data memory and program memory. If the on-chip program and data memory are not sufficient

for the application, external data memory and program memory chips can be used in the design.

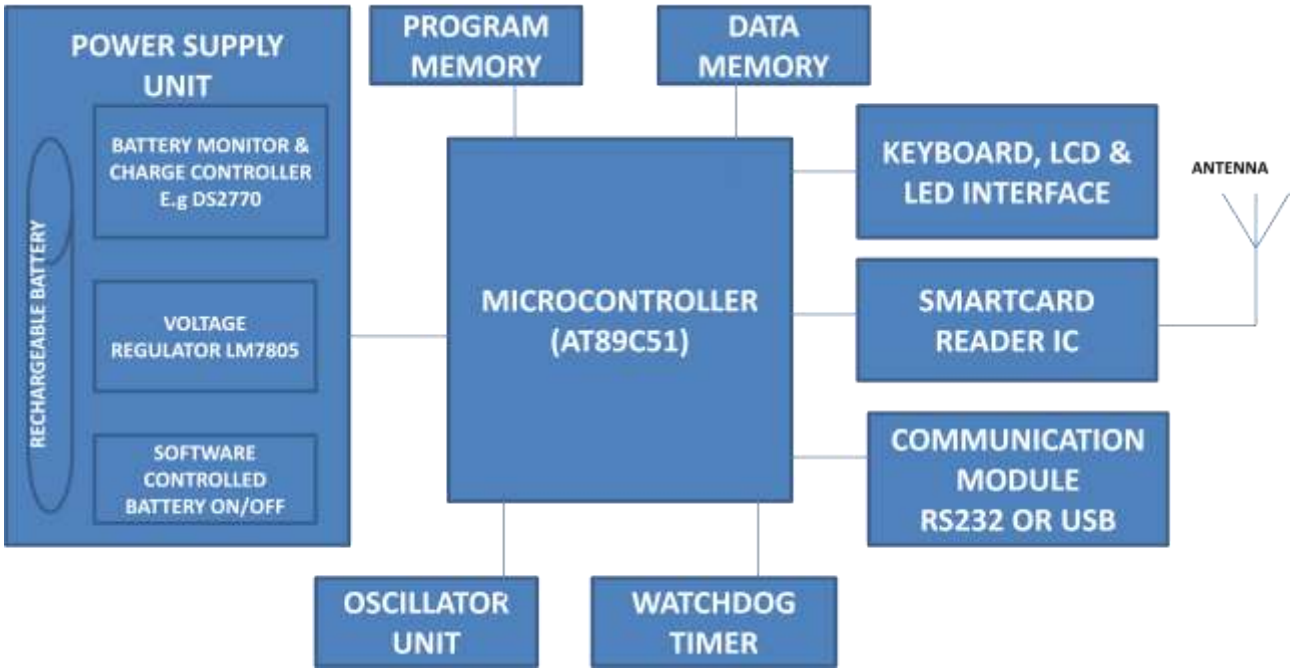

Figure 8: Block Diagram Of Handheld Contactless Smart Card Reader

The following are the activities of each task:

- **The communication task and keyboard scanning task** can be implemented either as a polling task or an interrupt driven task. The watchdog timer expiration event is captured as an interrupt.

- **The startup task** implements the necessary startup operations like setting up the interrupts, configuring the ports of the host processor, initialising the LCD, initialising the battery monitor and charge control IC, initialising the smart card reader IC, etc.

- **The battery monitoring and charge controlling task** reads the various registers (Voltage, capacity registers etc) of the battery monitor IC, checks the presence of a charger and initiates a charge command, terminates the charging when the battery is full, produces warning signal when the battery voltage is below a threshold value and switch off the unit if the battery voltage falls below the critical threshold value. This task is assigned highest priority to avoid data corruption in case of a power down.

- **The card read/write operation task** is responsible for implementing the communication sequence for data read/write operation with the card. The smartcard read/write operation follows a specific sequence of operation. The sequence varies with the standards (Like ISO/IEC 14443 A/B, ISO/IEC 15693, etc.) supported by the read write IC.
- A typical read write operation follows the sequence:

    - Reader initiates a 'Request' command for checking the presence of cards in the vicinity of the reader. If a card is present in the field it responds to the reader with Answer To Request (ATR).

    - Upon receiving the ATR, the reader sends a command to capture the serial number of all cards present in the field.
    - Most of the reader ICs implement special algorithms to decode and capture the serial number of all cards present in the field.

    - Reader selects the serial number of a card from the list of serial numbers received and sends a command to select the specified card. The card whose serial number matches with the one sent by the reader responds to the reader and all other cards in the field enters sleep state. Now the communication channel is established exclusively between the reader and a card.

    - The Reader authenticates the card with an encrypted key. If the key matches with the key stored in the card, the authentication succeeds. Different security mechanisms are used by different family of cards and readers for implementing authentication.

    - The reader sends a read/write command to the card along with the details of the memory area which the reader wants to read/write and the data to write in case of a write operation. The memory of the card is segmented into different sectors and each sector may be further divided into blocks. Each block holds a fixed number of data bytes. Each memory segment contains a key for authentication. The memory organisation of the card is manufacturer specific.

- **The keyboard scanning task** scans the keyboard and identifies a key press and performs the operation corresponding to the key press. This can be implemented as a task or an Interrupt Service Routine if the keyboard hardware supports interrupt generation on a key press.

- **The LCD update task** updates the LCD with new data. This task can be invoked by other tasks like keyboard scanning task, battery monitoring task, card read/write task and communication task for displaying the various nformation.

- **The communication** task handles reader communication with the host PC. The communication interface can be either USB or RS-232. This task can also be

implemented as Interrupt Service Routine. Most of the processors support Serial Interrupt for handling Serial data transmission using UART and RS-232. If USB is used as the interface, the interrupt line of the USB chip can be connected to the Interrupt line of the processor and communication can be controlled in the ISR.

- **The watchdog timer** expiration ISR handles the actions corresponding to a watchdog timer event.

The firmware for controlling the handheld reader can be implemented in either a 'Super loop' model where the tasks are executed in sequence in a super loop with interrupts running in the background or using an RTOS scheduler like uC/OS-II or RTX-51 or VxWorks for scheduling the tasks.

References:

- **Introduction to Embedded Systems by Shibu KV**
- **https://electricalfundablog.com/smart-card-works-specifications-types**
- http://www.smartcardbasics.com
- https://www.plugandplaytechcenter.com
- https://www.slideshare.net
- https://electricalfundablog.com/smart-card-works-specifications-types/
- https://people.cs.uchicago.edu/~dinoj/smartcard/arch-1.html
- https://www.securetechalliance.org/smart-cards-intro-standards/
- https://www.alldatasheet.com