Smart Card Reader Meeting ISO 7816-3 and EMV Level 1 Specifications using PIC24F Microcontroller

Abhay A. D., Ganesh Krishna, Channabasappa Baligar

Abstract*— A smart card is a pocket-sized card containing an embedded intelligent integrated circuit (i.e., intelligence to respond to a request from an external device). Smart cards contain a microprocessor chip that serves the dual functions of communication and extensive data storage. These cards are user friendly and have the capacity to retain, and protect the critical information stored in an electronic form. Smart cards are being deployed in most public and private sectors. Typically, a smart card reader is used for data transactions with the smart card. The smart card can be divided into two types: 1) Contact type 2) Contactless type. In contact type smart cards, the card communicates with the reader through a direct physical contact. In contactless type smart cards, the card communicates with the reader through a remote radio frequency interface. This paper shows the design of smart card reader meeting ISO 7816-3 & EMV Level 1 specifications using PIC24F microcontroller.

***Index Terms*— Block wait time, Character wait time, Character guard time, EMV Level 1 Reader, IFD ,ISO 7816-2, ISO 7816-3, T=1, T=0**

I. INTRODUCTION

Although the ISO 7816-2 standard defines eight contacts for the smart card, normally six pins are used for communication.

VCC is used to supply power to the smart card. RST is used to reset the smart card. CLK provides the clock input to the smart card. VPP provides the programming voltage input to the smart card. I/O line is used for serial data communication between the smart card and the smart card reader. This is a half-duplex communication. GND is a Ground pin. C4 and C8 pins are reserved for future use. Currently these pins are used for USB interface.

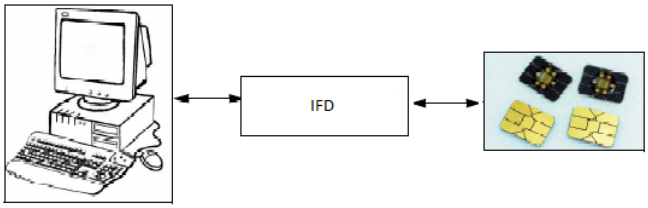
Most of the smart cards used in the market are ISO 7816-3 and EMV (Europay, MasterCard and Visa) compliant. Typically, an interfacing device (IFD) i.e. smart card reader is used for data transactions with the smart card.

Revised Manuscript Received on February 06, 2013.

Abhay A D, M.Tech in VLSI Design and Embedded System, VTU Extension Center, UTL Technologies, Bangalore, India.

Ganesh Krishna, Project Manager, MCU 16, Microchip Technology Private Ltd,Bangalore,India.

Channabasappa Baligar, VLSI Design and Embedded System, Visiting Faculty,VTU Extension Center, UTL Technologies,Bangalore, India.



A card communication session with the IFD (Interfacing Device) is comprised of the following stages: 1) Insertion of the smart card into the IFD and activation of the contacts. 2) Reset of the smart card and establishment of communication between the terminal and the smart card. 3) Execution of the transaction(s). 4) Deactivation of the contacts and removal of the smart card.

ISO 7816 is an International Standard specifications document that describes the interfacing requirements to communicate with the contact type smart cards. Whereas the EMV Level 1 document specifies the tests that need to be passed by the IFD to communicate with EMV certified cards. Other than electrical and mechanical tests, EMV Level 1 comprises the following firmware level tests: 1) Card Session tests: These tests are related to activation and deactivation sequence of the card. 2) Answer to Reset tests: These tests are related to ATR bytes received from the card. 3) T = 0 tests: These tests are related to T = 0 protocol specifications. 4) T = 1 tests: These tests are related to T = 1 protocol specifications

II. PROTOCOL DESCRIPTION

After the detection of a smart card in the appropriate slot through a mechanical contact, the IFD has to perform a cold reset of the smart card using the following steps: 1) Pull the RST line to low state. 2) Pull the VCC line to high state. 3) Set UART module in Reception mode. 4) Provide the clock signal at CLK line of the smart card. 5) The RST line has to be in the low state for at least 400 clock cycles after the clock signal is applied at CLK pin. Therefore, give a delay for atleast 400 clock cycles after providing the clock at CLK pin of the smart card. 6) Pull the RST line to high state.

If the ATR (Answer to Reset) received following a cold reset does not conform to the EMV specifications, the terminal shall initiate a warm reset and obtain an ATR from the smart card using the following steps: 1) Pull the RST line to low state. 2) Provide the VCC and CLK signal to the card. 3) Within a maximum of 200 clock cycles following T0', the smart card and IFD shall set their I/O line drivers to reception mode. 4) The terminal shall maintain RST in low state from time T0' for a period of between 40,000 and 45,000 clock cycles following time T0' to time T1', when it shall set RST to high state. 5) The answer to

reset on I/O from the smart card shall begin between 400 and 40,000 clock cycles after time T1'. 6) The IFD shall have a reception window which is opened no later than 380 clock cycles after time T1' and closed no earlier than 42,000 clock cycles after time T1'. If no answer to reset is received from the smart card, the terminal shall initiate the deactivation sequence.

The ATR characters provide information to the IFD about how to communicate with the smart card for the remainder of the session. The ATR message, which can be up to 33 characters, consists of fields: 1) Initial Character (TS) 2) Format Character (T0) 3) Interface Characters (TA1,TB1, TC1 and TD1) (optional) 4) Historical Characters (optional) 5) Check Character (TCK) (conditional)

By issuing the PPS (Protocol Parameter Selection) command, the IFD can modify certain communication parameters in the smart card.

After the ATR and PPS exchange between the card and the IFD, the next step is to execute the commands between the card and the IFD. There are two protocols, which are widely used for smart card communications: T = 0 and T = 1.

A. T = 0

The T = 0 protocol is a byte-oriented protocol, which means that the smallest unit processed by this protocol is a single byte. The interfacing device always initiates the command. The smart card performs the requested operation(s), and communicates the result as a response from the smart card. This command response message pair is known as an Application Protocol Data Unit (APDU). The below table lists the codes of the APDU command header for T = 0 protocol.

Code	Description	Bytes
CLA	Instruction class	1
INS	Instruction code	1
P1	Instruction code qualifier	1
P2	Additional INS code qualifier	1
P3	Length of data block	0 or 1

The CLA, INS, P1 and P2 are mandatory fields in the APDU command header, whereas P3 is an optional field. P3 encodes either the number of bytes present in the APDU command data field or the maximum number of data bytes expected in the data field of the APDU response.

There are two status bytes: SW1 and SW2. These bytes are sent from the smart card to the interface device on completion of the APDU command to indicate the status of the current card. The normal response is: SW1 = 0x90 and SW2 = 0x00.

B. T = 1

The T = 1 protocol is a block oriented protocol, which means that one block is the smallest data unit that can be transmitted between the smart card and the interfacing device. There are three types of blocks in T = 1 protocol: 1) Information Blocks (I-blocks) – They are used to exchange the application layer data. 2) Receive Ready Blocks (R-blocks) – They are used to convey a positive or negative acknowledgment. 3) Supervisory Blocks (S-blocks) – They are used to exchange control information between the IFD and the card.

The three fields involved in the each of these block frames are: 1) Prologue field 2) Information field 3) Epilogue field.

The prologue and epilogue fields are mandatory for all three types of blocks, whereas the information field is mandatory for I blocks and optional for S blocks. R-blocks do not have any information field.

Prologue Field			Information Field	Epilogue Field
NAD	PCB	LEN	Optional	LRC or CRC
1 byte	1 byte	1 byte	0 – 254 bytes	1/ 2 bytes

The Node address (NAD) contains the destination and the source addresses for the block. It also has a VPP control bit, which is usually not used in the current smart card controllers. Protocol Control Byte (PCB) helps to control and supervise the transmission protocol.

LEN indicates the length of the information field in hexadecimal form. The value 0x00 indicates the absence of the information field.

C. Timings for T = 0 and T = 1 protocol

The interfacing device (i.e., smart card reader) has to follow the timing regulations for the transmission and the reception of data bytes from the smart card. These definitions apply for both the smart card and the interfacing device.

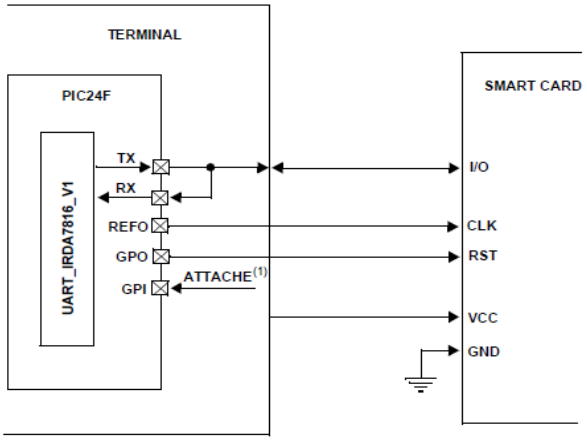
The minimum delay between the leading edges of two consecutive characters in the same direction of transmission is named as"Guard Time" (GT).

The maximum delay allowed between two consecutive characters transmitted by the card or a IFD is named as "Waiting Time" (WT). Waiting Time is useful in detecting unresponsive cards.

The Block Waiting Time(BWT) is the maximum delay between the leading edge of the last character of the block received by the card, and the leading edge of the first character of the next block transmitted by the card. BWT is applicable only for T = 1 protocol.

III. DESIGN, IMPLEMENTATION AND RESULTS

The below figure shows a smart card sub-system using a UART-ISO 7816 module of PIC24F microcontroller for smart card communication.

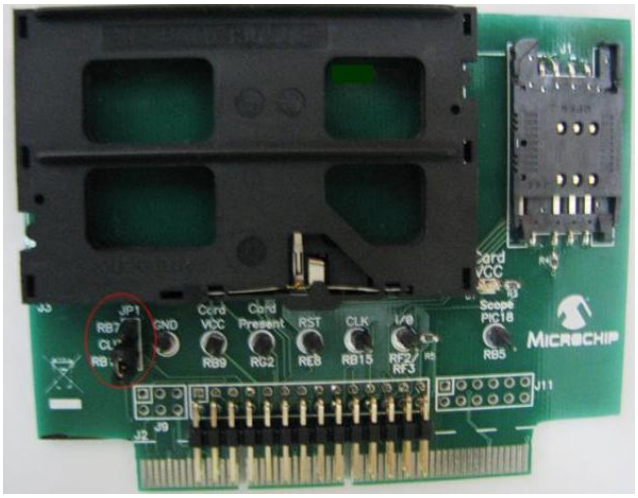


The 4 MHz external clock signal is fed to the smart card by reference clock output (REFO) pin of PIC24FJ128GB204 microcontroller. Since the smart card protocols (T = 0 and T = 1) communicate in half duplexed mode, the TX and RX pins of the microcontroller are shorted and given to I/O pin of the smart card.

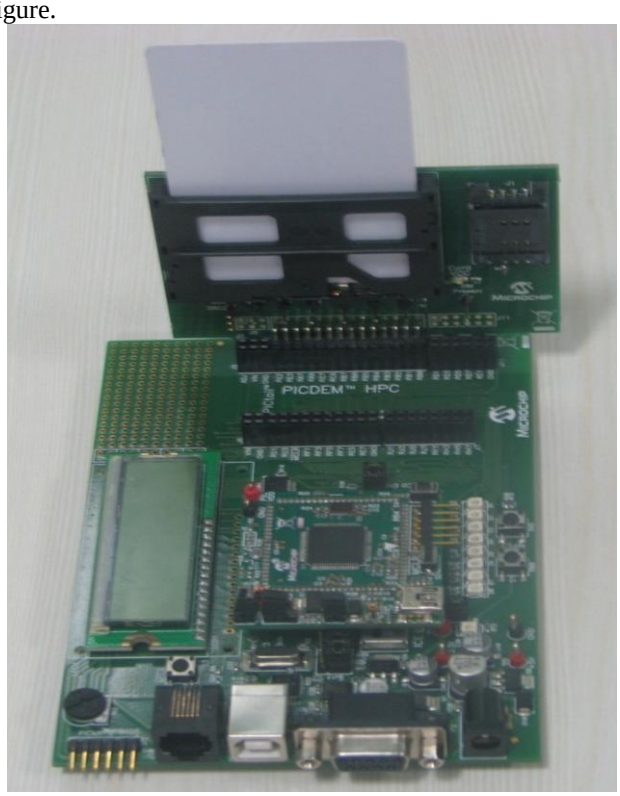
The firmware is written in the layered architecture for efficient software development life and improved maintainability of the source code.

Smart Card Stack (ISO 7816 -3 and EMV Level 1 Spec)
PIC24F UART Driver
Hardware Layer(Register Configurations)

A smart card daughter board is designed to communicate between the smart card reader and the smart card. The smart card or sim card can be inserted in the slot provided by daughter board.

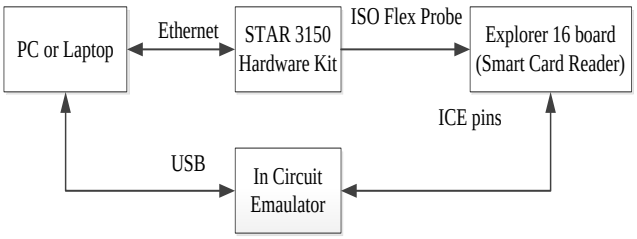


The designed daughter board sits on the Explorer 16 evaluation board provided by Microchip Technologies Inc. The combination of explorer 16 mother board and the daughter board works as a smart card reader as shown in figure.



A. *Test setup*

The smart card stack is tested using **Micropros STAR 3150** kit and **CardSim** software GUI provided by **LBI Informatique**. The bench setup is made as shown in the below block diagram:

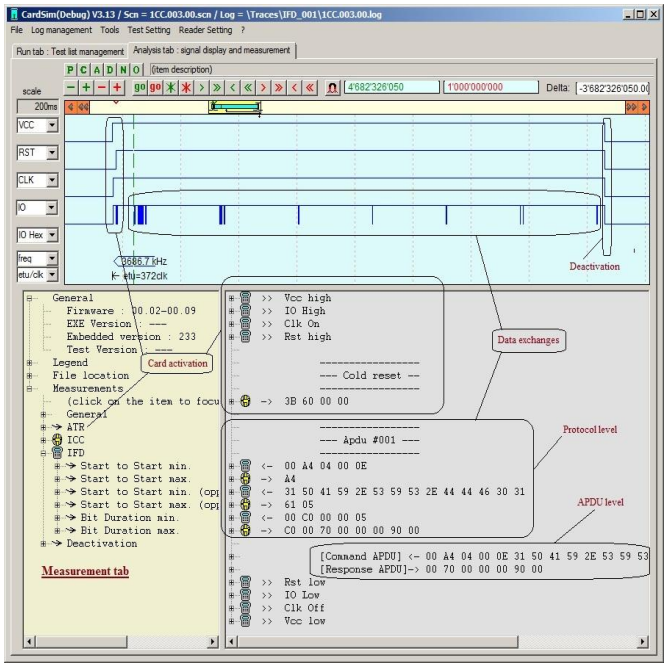


The **STAR 3150** (Smart Tester And Reader) is a tool for testing smart card readers. It allows the simulation of card functionality and recording all the changes of state occurring on the card pins as well as every character conveying between the reader and the card. **CardSim** provides the visual interface to test the smart card reader by modifying the smart card parameters of STAR 3150 flex probe.

B. *Results and Discussion*

CardSim GUI displays the result file, also called log file, which are binary files produced by an internal Star 3150 sampling module for each of the test case/test script. This sampler catches Signal transitions, Clock information and bytes in and out, with a 50 ns precision.

The Analysis tab in the CardSim GUI, displays the test result using a mixed graphical/textual display.



The display shows the commands transmitted by the IFD and the responses given by the smart card along with the relevant timing information.

The final result of all the test cases is also consolidated in a single pdf file.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

IV. CONCLUSIONS

This project has demonstrated the implementation of smart card reader meeting ISO 7816-3 and EMV Level 1 specifications using PIC24F microcontroller. The software developed is ISO 7816-3 and EMV level 1 compliant. This is a cost effective solution as the ISO 7816 hardware module is built in the microcontroller itself thus saving the cost of an external ISO 7816 smart card chip. This is a low power solution as well because the deep sleep current is extremely low in nA for PIC24F microcontrollers. The smart card reader can be made to wake up by an external interrupt, only when the smart card is inserted in the slot. During all other times the microcontroller can be put in the deep sleep state.

ACKNOWLEDGMENT

The authors would like to thank Srikhanth Nagaraj, Senior Applications Manager, Microchip Technologies Inc. Bangalore and Amardeep Gupta, Applications Manager, Microchip Technologies Inc. Bangalore.

REFERENCES

1. Matanovic G and Mikuc M, “Implementing Certificate -based Authentication Protocol on Smart Cards” IEEE Proceedings of the 35th International Convention, pp.1514-1519, May 2012.
2. de Koning Gans G and de Ruiter J, “The SmartLogic Tool: Analysing and Testing Smart Card Protocols”, IEEE Fifth International Conference, pp.864-871, April 2012.
3. “Cards with contacts — Electrical interface and transmission protocols” ISO 7816-3 Specifications, third edition, pp. 1−58, Nov 2006.
4. “Application Independent ICC to Terminal Interface Requirements” EMVCo, LLC, v4.3, pp. 1−189, Nov. 2011.
5. “Cards with contacts — Electrical interface and transmission protocols” EMVCo, LLC, v2.1,pp. 1−158, July. 2009.
6. “Specification for Integrated Circuit Cards Interface Devices” USB CCID Specifications,v1.1, pp. 1−123, Apr 2005.
7. “Organization, Security & Commands for Interchange” ISO 7816-4 Specifications, second edition, pp. 1−90, Jan 2005.

AUTHORS PROFILE

Abhay A D is studying M.Tech 6th semester in VLSI Design and Embedded Systems in VTU Extension Center, UTL Technologies Bangalore. He has around 11.5 years of experience in embedded domain in various mulitnational companies like Delphi Electronics and Safety, Honeywell Technologies and Microchip Technology(India) Private Ltd.

Ganesh Krishna completed B.E in Electronics and Communication from Sri Jayachamarajendra College of Engineering Mysore in the year 2002. He has around 11 years of experience in embedded domain in various MNCs and is currently project manager in MCU16 division of Microchip Technolgy (India) Pvt Ltd.

Channabasappa Baligar has completed M.Tech in VLSI Design and Embedded Systems in VTU Extension Center, UTL Technologies Bangalore. He is currently working in DRDO and is a visiting faculty at UTL Technologies Bangalore. He has vast experience in RTOS and various embedded domains.