AN1370

Smart Card Communication Using PIC® MCUs

Author: Abhay Deshmukh
Microchip Technology Inc.

INTRODUCTION

This application note describes the fundamentals of the contact type smart cards and how they are communicated using an interfacing device (PIC® microcontrollers).

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. The major application areas of the smart card includes: information security, physical access security, banking, communications, transportation, retail and loyalty, healthcare, government programs, university identification, etc.

The smart card is more reliable, highly secured, with larger data storage capacity, multifunctional and has a longer life-span when compared to the magnetic strip cards.

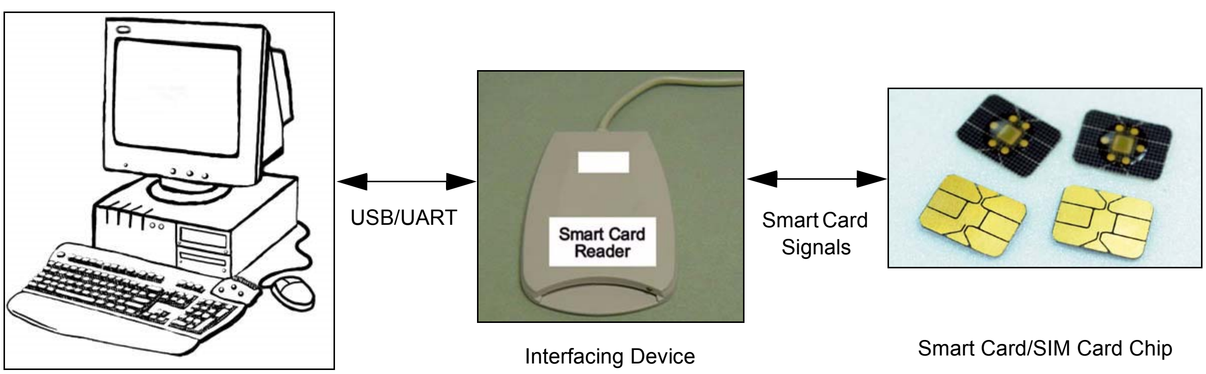
Typically, a smart card reader is used for data transactions with the smart card. Based on the connection type with the smart card reader, the smart card can be divided into two types:

- Contact type
- 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.

Generally, a personal computer (PC) application is used to communicate with the smart card through an interfacing device (i.e., smart card reader), as shown in Figure 1.

FIGURE 1: SMART CARD COMMUNICATION USING PC APPLICATION



© 2011 Microchip Technology Inc.

ISO 7816 is an International Standard specifications document that describes the interfacing requirements to communicate with the contact type smart cards. ISO 7816 has multiple parts.

The high level information of some of the ISO 7816 parts are as follows:

- ISO 7816-1 specifies the physical characteristics of the card
- ISO 7816-2 specifies the dimension and the location of the chip contacts of the card
- ISO 7816-3 specifies the electronic signals and transmission protocols of the card
- ISO 7816-4 specifies the organization, security and commands for interchange

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

FIGURE 2: SMART CARD

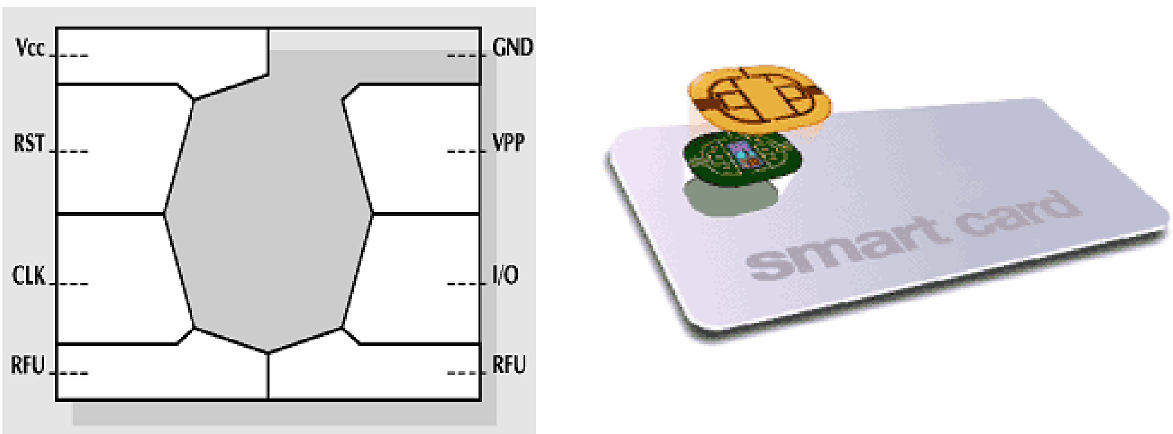


Table 1 lists the signal descriptions of each of the contacts.

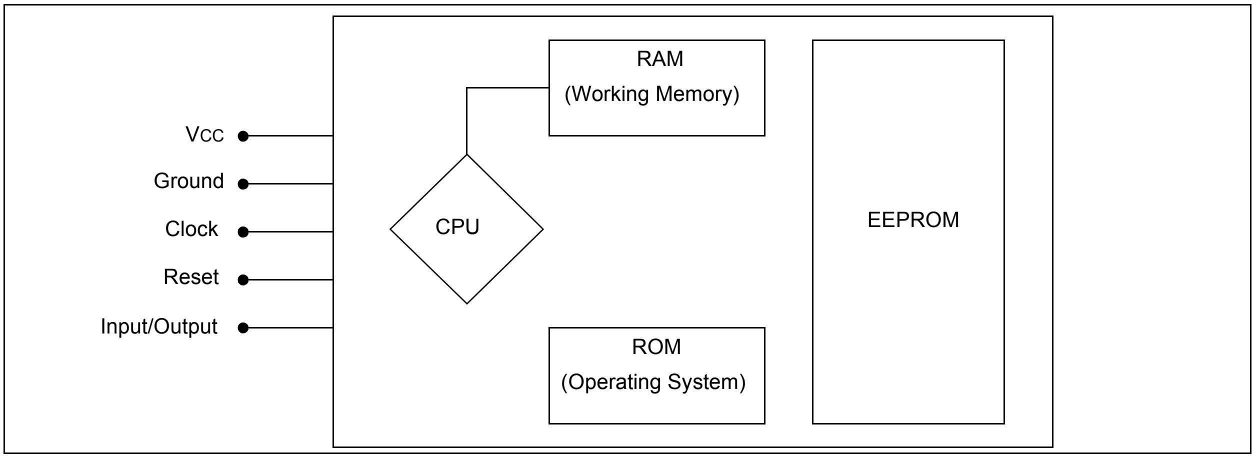
TABLE 1: SIGNAL DESCRIPTIONS

Signal	Description
VCC	This signal is used to supply power to the smart card
RST	This signal is used to reset the smart card
CLK	This signal provides the clock input to the smart card
GND	Ground
VPP	This signal provides the Programming Voltage Input to the smart card
I/O	Input/Output line is used for serial data communication between the smart card and the interfacing device. This is a half-duplex communication (The TX and RX lines of Universal Asynchronous Receiver and Transmitter (UART) in the Interfacing Device (IFD) is to be shorted and connected to the I/O line of the smart card).
RFU	Reserved for Future Use. Currently, used for Universal Serial Bus (USB) interface.

© 2011 Microchip Technology Inc.

A high-level view of a typical smart card chip is as shown in Figure 3.

FIGURE 3: HIGH-LEVEL VIEW OF SMART CARD CHIP



The interfacing device (such as a PIC® microcontroller) controls the CLK, RST and VCC signals given to the smart card.

Based on the nominal supply voltage provided by the interfacing device through VCC, the smart card can be classified into three types:

- **Class A** – 4.5V ≤ VCC ≤ 5.5V at ICC ≤ 60 mA
- **Class B** – 2.70V ≤ VCC ≤ 3.3V at ICC ≤ 50 mA
- **Class C** – 1.62V ≤ VCC ≤ 1.98V at ICC ≤ 30 mA

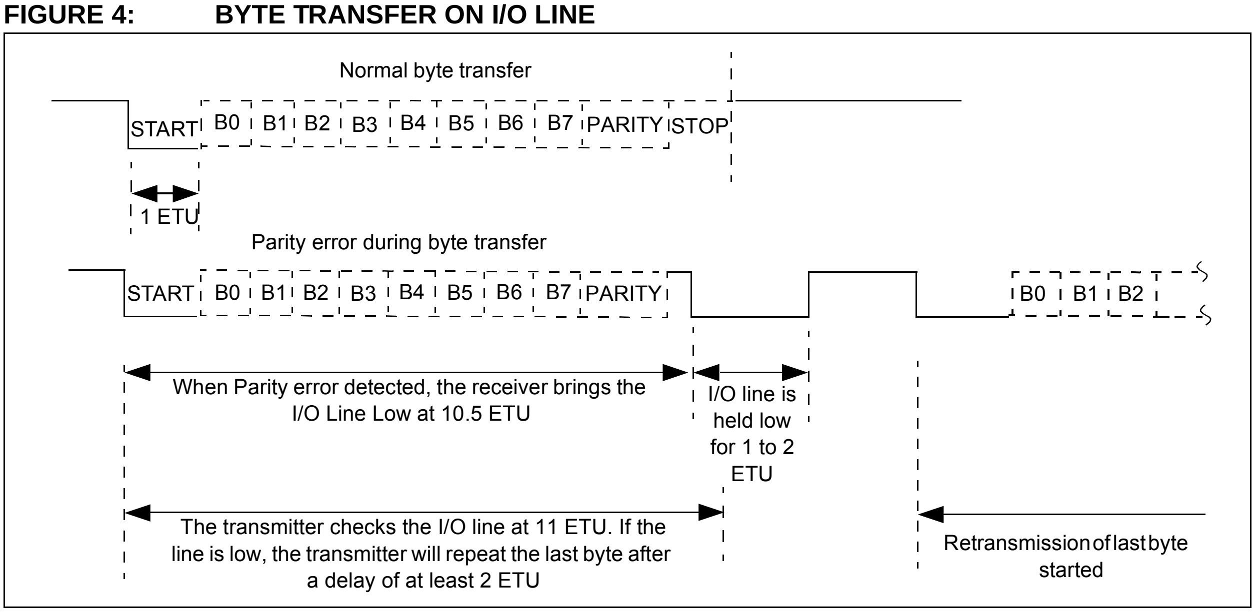
Each byte transfer in the smart card communication on the I/O line consists of ten bits as shown in Figure 4. The first bit of a character is a Start bit, which is always low. Preceding the Start bit, the I/O line is kept in its default high state. The Start bit is followed by a 8-bit data byte. The last bit of the character is the parity bit, which is either high or low as determined by the source.

After the ten bits of information, there is a Stop bit. If there is any error in the reception of the data, then the receiving device has to pull the I/O line low before the middle of the Stop bit (i.e.,10.5-bit time from start edge). The receiver pulls the line low for 1 to 2 ETU. Elementary Time Unit (ETU) is one bit time on the I/O line.

The transmitter checks the I/O line at the end of the Stop bit (11 ETU). If the transmitter detects the line as low, it retransmits the previous data byte after at least 2 ETU. The UART peripheral in the PIC microcontrollers sets the Receiver Ready and Transmitter Empty flags to true at 0.5 Stop bit. This allows the implementation of the ISO 7816-3 error detection and the possible retransmission protocol using the PIC microcontrollers.

> **Note:** For more information on electrical characteristics of the smart card, refer to the ISO 7816-3 document.

FIGURE 4: BYTE TRANSFER ON I/O LINE



OPERATING PROCEDURE

The communication between the smart card and the interfacing devices involves the following steps:

1. Insertion of the smart card in the slot.
2. Detection of the smart card insertion by the interfacing device (i.e., microcontroller).
3. Cold reset of the smart card by the interfacing device.
4. Answer to Reset (ATR) response by the card to the microcontroller.
5. Protocol and Parameter Selection (PPS) exchange between the smart card and the microcontroller (if the smart card supports PPS).
6. Execution of the command(s) between the smart card and the interfacing device.
7. Removal of the smart card from the slot.
8. Detection of the smart card removal by the microcontroller.
9. Deactivation of the smart card contacts by the microcontroller.

After the detection of a smart card in the appropriate slot through a mechanical contact, the interfacing device 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. The UART module in the interfacing device should be in the Reception mode in the software.
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 at least 400 clock cycles after providing the clock at CLK pin of the smart card.
6. Pull the RST line to high state.

ATR is a series of characters responded to by the card reader after the successful Cold Reset operation. The ATR response on the I/O line starts between 400 to 40,000 clock cycles after the RST line is set to high state. ATR characters determine the initial communication parameters, bit timing, and the data transfer details between the card and the interfacing device. If the ATR response does not come from the card after the Cold Reset routine, then the card is deactivated by the microcontroller. By issuing the PPS command, the interfacing device can modify certain communication parameters in the card.

The bit timing of the characters during the ATR is called the "Initial ETU". Equation 1 provides the formula for the computation of the Initial ETU.

EQUATION 1: INITIAL ETU

Initial ETU = $372/f$ seconds

UART Baud Rate in PIC® Microcontroller = 1/Initial ETU

Where,

f = Clock fed to the smart card (in hertz)

If the card supports PPS, then the ETU value can be modified by the interfacing device after receiving the ATR from the card. The modified ETU is called "Current ETU". Equation 2 provides the formula for the computation of the Current ETU. Only the interfacing device is permitted to start the PPS exchange.

EQUATION 2: CURRENT ETU

Current ETU = $F/(D*f)$ seconds

UART Baud Rate in PIC® Microcontroller = 1/Current ETU

Where,

F = Clock-rate conversion factor

D = Bit-rate adjustment factor

f = Clock fed to the smart card (in hertz)

The parameters F and D are explained in the **Section "TA1 Interface Character"**.

© 2011 Microchip Technology Inc.

ANSWER TO RESET

The ATR characters provide information to the interfacing device about how to communicate with the smart card for the remainder of the session.

The ATR message, which can be up to 33 characters, (including the initial character (TS)) consists of these fields:

- Initial Character (TS) (mandatory)
- Format Character (T0) (mandatory)
- Interface Characters (TA1,TB1,TC1 and TD1) (optional)
- Historical Characters (T1,T2,...TK) (optional)
- Check Character (TCK) (conditional)

Initial Character (TS)

The TS character synchronizes the information and defines the communication pattern for all the subsequent characters. The first four bits of TS are used for timing synchronization. The next three bits are either all high to indicate “Direct convention”, or all low to indicate the “Inverse convention”. In direct convention, a high state on the I/O line is equivalent to logic 1, and the Least Significant bit (LSb) is transmitted first. In the inverse convention, a low state on the I/O line is equivalent to logic 1, and the Most Significant bit (MSb) is transmitted first.

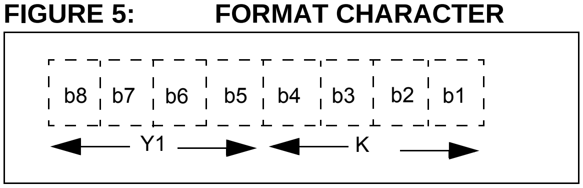
Format Character (T0)

The T0 byte is made up of Y1 and K nibbles as shown in Figure 5. Y1 is the higher nibble and K is the lower nibble.

Y1 indicates the presence or absence of TA1, TB1, TC1 and TD1 in the ATR.

- TA1 is transmitted when bit 5 = 1
- TB1 is transmitted when bit 6 = 1
- TC1 is transmitted when bit 7 = 1
- TD1 is transmitted when bit 8 (MSb) = 1

FIGURE 5: FORMAT CHARACTER



K nibble indicates the number (0 to 15) of historical characters present in the remaining ATR sequence.

TA1 Interface Character

The TA1 character is divided into upper and lower nibbles. The upper nibble determines the clock rate conversion factor (F), which is used to modify the frequency of the clock signal (see Table 2). The lower nibble determines the bit rate adjustment factor (D), which is used to adjust the bit duration subsequent to the ATR (see Table 3). The default values (F = 372 and D = 1) are used for the calculation of the “Initial ETU” value and will continue to be used during the subsequent exchanges, unless changed during the PPS operation.

TABLE 2: UPPER NIBBLE

Bits 8 to 5	F	*f*(max) MHz
0000	372	4
0001	372	5
0010	558	6
0011	744	8
0100	1116	12
0101	1488	16
0110	1860	20
0111	RFU	—
1000	RFU	—
1001	512	5
1010	768	7,5
1011	1024	10
1100	1536	15
1101	2048	20
1110	RFU	—
1111	RFU	—

TABLE 3: LOWER NIBBLE

Bits 4 to 1	D
0000	RFU
0001	1
0010	2
0011	4
0100	8
0101	16
0110	32
0111	64
1000	12
1001	20
1010	RFU
1011	RFU
1100	RFU
1101	RFU
1110	RFU
1111	RFU

© 2011 Microchip Technology Inc.

TB1 Interface Character

The TB1 character conveys the programming voltage requirements of the smart card. TB1 = 0x00 indicates that the VPP pin is not connected in the smart card.

TC1 Interface Character

The TC1 character is used to calculate the guard time in the smart card communication protocol. The minimum delay between the leading edges of two consecutive characters is named as “Guard Time” (GT).

TD1 Interface Character

The TD1 character contains a bit map that indicates:

- The presence or absence of TA2, TB2, TC2 and TD2 interfacing bytes
- The type of smart card communication protocol supported

TA2 Interface Character

The presence of TA2 in the ATR indicates the specific operative mode, and the absence of TA2 indicates the negotiable operative mode. The PPS exchange can be done in the negotiable mode, but cannot be done in the specific mode of smart card operation.

TB2 Interface Character

The character TB2 conveys programming voltage required by the smart card.

TC2 Interface Character

The TC2 character is specific to T = 0 protocol. TC2 conveys the work Waiting-Time Integer (WI). The WI determines the maximum interval between the leading edge of the Start bit of any character sent by the smart card, and the leading edge of the Start bit of the previous character sent either by the card or by the interfacing device.

TD2 Interface Character

The TD2 character has the same function as the TD1 character.

TA3 Interface Character

The TA3 character conveys the Information Field Size Integer (IFSI) for the smart card, which is used for T = 1 protocol. For an ATR not containing TA3, the interfacing device will assume a default value of 0x20.

TB3 Interface Character

The TB3 character indicates the value of the Character Waiting Time Integer (CWI) and the Block Waiting Time Integer (BWI), which are used to compute the Character Waiting Time (CWT) and Block Waiting Time (BWT), respectively. The CWT is the maximum delay between the leading edges of the two consecutive characters in the block. 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.

TC3 Interface Character

When TC3 is present, it indicates the type of block error detection to be used (LRC or CRC). When TC3 is absent, the default Longitudinal Redundancy Check (LRC) is used. LRC/CRC is applicable only for T = 1 protocol.

TD3 Interface Character

The TD3 indicates the interface bytes similar to that of TD1 and TD2.

Historical Characters (T1,T2,...TK)

The historical bytes indicate the operating characteristics of the card. They are the optional bytes in the ATR response, which convey the general information of the card (such as the card manufacturer, the chip in the card, the masked ROM in the chip, the card’s state of life, etc.).

Check Character (TCK)

If only T = 0 is indicated, then TCK shall be absent. If T = 0 and T = 15 are present and in all the other cases, TCK shall be present. When TCK is present, exclusive-ORing of all the bytes from T0 to TCK should result as 0x00. Any other value is invalid.

For more information on ATR, refer to the ISO 7816-3 document.

© 2011 Microchip Technology Inc.

PPS REQUEST AND RESPONSE

The PPS request and response consists of an initial byte, PPSS. The PPSS is followed by a format byte, PPS0, three optional parameter bytes, PPS1, PPS2, PPS3, and a check byte, PCK, as the last byte.

- PPSS is set to 0xFF
- In PPS0 byte, bit 8 is reserved for future use. Each bit 5, bit 6 or bit 7 is set to '1', to indicate the presence of optional bytes, PPS1, PPS2 and PPS3, respectively. Bit 4 to bit 1 encode the protocol type T (i.e., T = 0 or T = 1 or T = 2, etc.)
- PPS1 is same as TA1
- PPS2 is same as first TB byte for T = 15
- PPS3 is reserved for future use
- Exclusive-ORing for all the bytes from PPSS to PCK should result as 0x00

In common, the PPS response is identical to the PPS request.

For more information on PPS exchange, refer to the ISO 7816-3 document.

SMART CARD COMMUNICATION PROTOCOL

After the ATR and PPS exchange between the card and the interfacing device, the next step is to execute the command(s) between the card and the interfacing device.

Currently, there are two protocols, which are widely used for smart card communication:

- T = 0 (asynchronous half-duplex character transmission protocol)
- T= 1 (asynchronous half-duplex block transmission protocol)

T = 0 Protocol

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 in T = 0 communication protocol. The transactions are accomplished by issuing the commands from the interfacing device to the smart card.

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). A specific command message sent by the interfacing device (C-APDU) will have a specific response message from the card (R-APDU). These messages are referred to as APDU command response pairs.

Table 4 lists the codes of the APDU command header for T = 0 protocol.

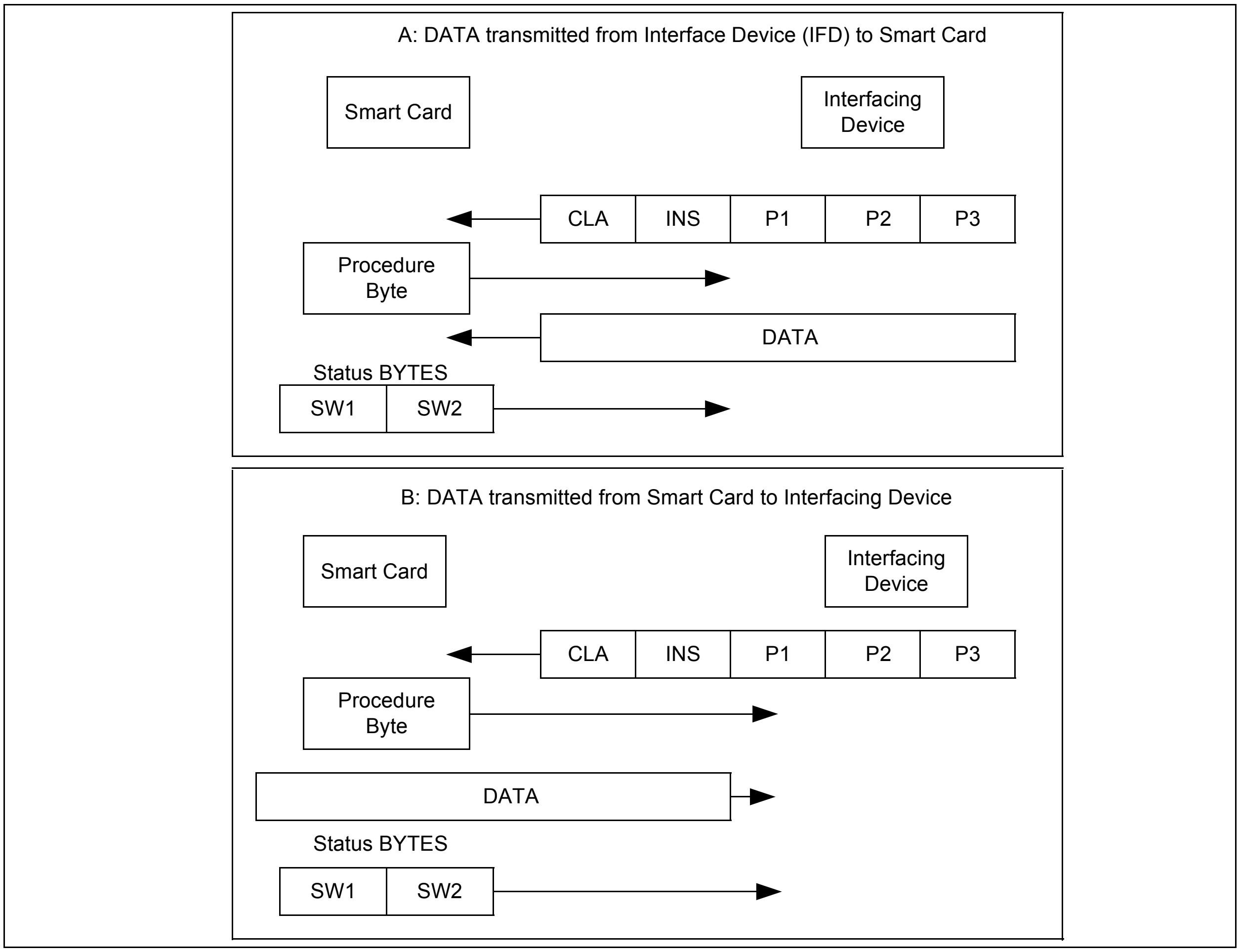
The CLA, INS, P1 and P2 are mandatory fields in the APDU command header, where as P3 is an optional field. P3 encodes either the number of bytes present in the APDU command data field or the maximum number of data bytes expected in the data field of the APDU response. See Figure 6 for a pictorial understanding of the smart card communication using T = 0 protocol.

The APDU command message is sent by the interfacing device to the smart card. The smart card then replies with a procedure byte, after which either data is sent to the smart card or data is received from the smart card, depending upon the command transmitted to the smart card.

TABLE 4: CODES OF 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	The Length of the 'Data' Block	0 or 1

FIGURE 6: SMART CARD COMMUNICATION USING T = 0 PROTOCOL



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
- SW2 = 0x00

The card reports the error condition by transmitting SW1 = 6X or 9X (where ‘X’ has any value from 1 to F). ISO 7816-3 defines five such error conditions:

- SW1:
  - 6E – Card does not support instruction class
  - 6D – Invalid INS code
  - 6B – Incorrect reference
  - 67 – Incorrect length
  - 6F – No particular diagnosis

The T = 0 protocol also includes an error detection and correction mechanism. After detecting the parity error, the receiver pulls the I/O line to low logic level for a minimum of 1 ETU and maximum of 2 ETU in the middle of the Stop bit transmission (10.5 ± 0.2 ETU). The transmitter checks for this condition and retransmits the corrupt character.

T = 1 Protocol

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:

- Information Blocks (I-blocks) – They are used to exchange the application layer data.
- Receive Ready Blocks (R-blocks) – They are used to convey a positive or negative acknowledgment.
- Supervisory Blocks (S-blocks) – They are used to exchange control information between the interfacing device and the card.

The three fields involved in the block frames are:

- Prologue field
- Information field
- Epilogue field

Table 5 lists the block frame fields of T = 1 protocol.

 © 2011 Microchip Technology Inc.

TABLE 5: BLOCK FRAME FIELDS

Prologue Field			Information Field	Epilogue Field
Node Address (NAD)	Protocol Control Byte (PCB)	Data Length (LEN)	Optional (INF)	Error Detection LRC or CRC (EDC)
1 Byte	1 Byte	1 Byte	0-254 Bytes	1/2 Bytes

The prologue and epilogue fields are mandatory for all three types of blocks, whereas the information field has the following scenarios:

- I-blocks contain an information field
- R-blocks do not have an information field
- S-blocks may or may not have an information field depending on its controlling function

PROLOGUE FIELD

The prologue field consists of three bytes:

- Node Address (NAD)
- Protocol Control Byte (PCB)
- Data Length (LEN)

Node address (NAD)

The Node address 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.

The bit fields of the NAD byte for all the three types of blocks are shown in Table 6.

Protocol Control Byte (PCB)

As the name suggests, the PCB helps to control and supervise the transmission protocol.

PCB of I-Block

Table 7 lists the PCB fields for an I-block. Every I-block carries the send sequence number N(S). The I-blocks transmitted by the interfacing device, and those transmitted by the smart card are counted independently from each other. N(S) is counted as modulo 2 and encoded by one bit. At the beginning of the transmission protocol or after resynchronization, the initial value is N(S) = `0`, then the value alternates after transmitting each I-block.

The “M” bit in PCB controls the chaining of I-blocks. The value of the “M” bit indicates the state of the I-block.

- If M = `1`, then an I-block is chained to the next block, which shall be an I-block.
- If M = `0`, then an I-block is not chained to the next block.

TABLE 6: BIT FIELDS OF NAD BYTE

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
VPP control 1	Destination Address (DAD)			VPP control 2	Source Address (SAD)		

TABLE 7: PCB FIELD FOR I-BLOCK

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
`0` (I-block identifier)	Send sequence number N(S)	Sequence data bit (M)	Reserved				

PCB of R-Block

Table 8 lists the PCB fields for the R-block. N(R) is the send sequence number of the expected I-block.

The R-blocks are used to convey the positive or negative acknowledgment for the I-blocks.

TABLE 8: PCB FIELDS FOR R-BLOCK

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Meaning
1	0	—	—	—	—	—	—	R-block Identifier
—	—	0	N(R)	0	0	0	0	No Error
—	—	0	N(R)	0	0	0	1	EDC or Parity Error
—	—	0	N(R)	0	0	1	0	Other Error

PCB of S-Block

Table 9 lists the PCB fields for the S-block. The "Resync" request is used by the interfacing device to reset the block transmission parameters to their initial values.

An "Abort" request can be used by an interfacing device or a smart card to abort an ongoing transaction between the smart card and the interfacing device.

Each T = 1 smart card has an Information Field Size value (IFS). The IFS defines the maximum size of the information field block that it can receive from the interfacing device. The default value is 32. Similarly, the interfacing device has an IFS value that defines the maximum size of the information field block that it can receive from the smart card. The IFS value can be adjusted by the "Information Field Size" request where the information field consists of one byte of new IFS value. This request can be initiated either by the smart card or by an interfacing device.

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. If the card requires more than one BWT to process the previously received I-block, it transmits the waiting time extension request to the interfacing device. In this waiting time extension request, the information field has one byte encoding an integer multiplier of the BWT value. The interfacing device shall acknowledge the smart card by the waiting time extension response. The waiting time extension response should have the same information field value, which the card had transmitted in its waiting time extension request.

TABLE 9: PCB FIELD FOR S-BLOCK

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Meaning
1	1	—	—	—	—	—	—	S-block Identifier
—	—	0	0	0	0	0	0	Resync Request (only from Terminal)
—	—	1	0	0	0	0	0	Resync Response (only from Smart Card)
—	—	0	0	0	0	0	1	Request Change to Information Field Size
—	—	1	0	0	0	0	1	Response to Request Change to the Information Field Size
—	—	0	0	0	0	1	0	Request Abort
—	—	1	0	0	0	1	0	Response to Abort Request
—	—	0	0	0	0	1	1	Request Waiting Time Extension (only from Smart Card)
—	—	1	0	0	0	1	1	Response to Waiting Time Extension (only from Terminal)
—	—	1	0	0	1	0	0	VPP Error Response (only from Smart Card)

© 2011 Microchip Technology Inc.

Data length (LEN)

This field indicates the length of the information field in hexadecimal form for all three types of blocks.

- The value 0x00 indicates the absence of the information field.
- The values from 0x01 to 0xFE indicates the length of the information field.
- The value 0xFF is reserved for future use.

INFORMATION FIELD

The information field in an I-block transmitted by the interfacing device to the smart card includes the following bytes, as shown in Table 10. The information field in the I-block is same as the APDU command used in the T = 0 protocol.

TABLE 10: INFORMATION FIELD OF I-BLOCK COMMAND

Code	Description	Bytes
CLA	Instruction Class	1
INS	Instruction Code	1
P1	Instruction Code Qualifier	1
P2	Additional INS Code Qualifier	1
P3	The Length of the 'Data' Block	0 or 1
Data	String of Data Bytes sent in Command	P3
LE	Maximum Number of Data Bytes expected in Data Field of Response	0 or 1

The information field in an I-block response transmitted by the smart card for an I-block request is shown in Table 11.

TABLE 11: INFORMATION FIELD OF I-BLOCK RESPONSE

Code	Description	Bytes
Data	String of Data bytes sent in Command	LE
SW1	Status Byte 1	1
SW2	Status Byte 2	1

EPILOGUE FIELD

The epilogue field is transmitted at the end of the block, and it contains an error detection code computed from all the previous bytes of the block. The computation employs either a Longitudinal Redundancy Check (LRC) or a Cyclic Redundancy Check (CRC). The method used must be specified in the interface characters of the ATR. If it is not specified, the LRC method is implicitly used. The LRC is calculated by exclusive-ORing all the previous bytes in the block, where as, CRC is calculated by using the polynomial:

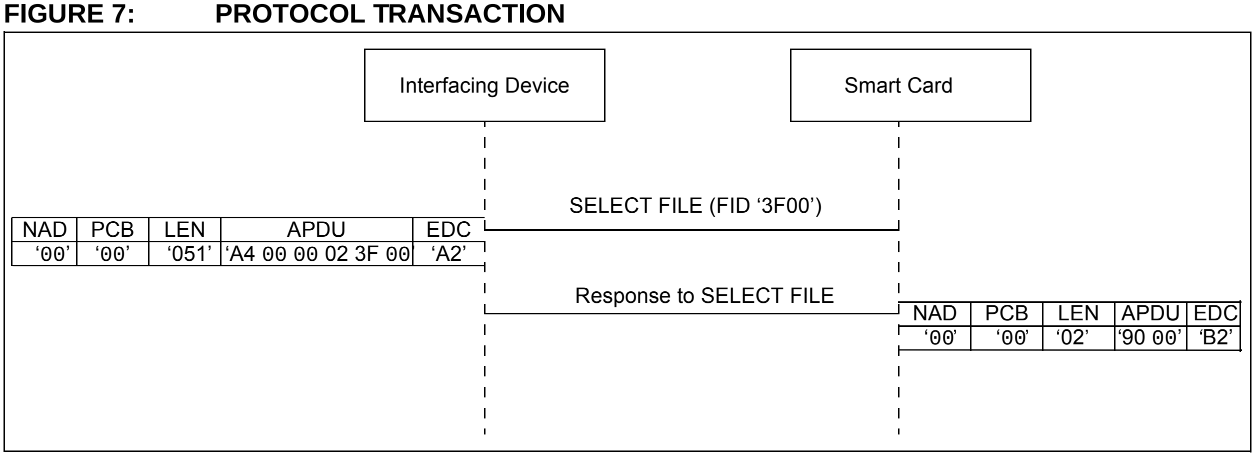
EQUATION 3: CRC

$$G(x) = x^{16} + x^{12} + x^5 + 1$$

Figure 7 shows an example of T = 1 protocol transaction.

For more information on I-block, R-block and S-block transactions, refer to the ISO 7816-3 specification.

FIGURE 7: PROTOCOL TRANSACTION



Waiting Time 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.

CHARACTER GUARD TIME (CGT)

The CGT is the minimum delay between the leading edges of the two consecutive characters in the same direction of transmission. During the ATR communication, CGT = 12 ETU. After the ATR communication, the value of CGT is calculated using the TC1 character, which is one of the ATR bytes received from the smart card. CGT is applicable for both T = 0 and T = 1 protocol.

WAIT TIME (WT)

The WT is the maximum delay allowed between two consecutive characters transmitted by the card or an interfacing device. For smart cards supporting only T = 0 protocol, WT also denotes the maximum time within which the APDU response has to be initiated by the smart card for the requested APDU command. WT is useful in detecting unresponsive cards. During the ATR communication, WT = 9600 ETU (for both T = 0 and T = 1 protocols). After the ATR communication, the value of WT is calculated using the TC2 character, which is one of the ATR bytes received from the smart card.

BLOCK GUARD TIME (BGT)

The BGT is defined as the minimum delay between the leading edges of the two consecutive characters in the opposite directions in a T =1 communication protocol. The BGT has a standard fixed value of 22 ETU.

CHARACTER WAIT TIME (CWT)

The CWT is the maximum delay between the leading edges of the two consecutive characters in the block as shown in Figure 8. The minimum delay is CGT. After the ATR communication, the value of CWT is calculated using the first TB for T = 1 protocol, which is one of the ATR bytes received from the smart card. CWT is applicable for T = 1 protocol.

BLOCK WAIT TIME (BWT)

The 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, as shown in Figure 9. BWT helps the interfacing device in detecting the unresponsive smart cards. The minimum delay is BGT. After the ATR communication, the value of BWT is calculated using the first TB for T = 1 protocol, which is one of the ATR bytes received from the smart card. BWT is applicable only for T = 1 protocol.

The descriptions and equations to calculate all of the above timing variables are explained in the ISO 7816-3 specification.

FIGURE 8: CHARACTER WAIT TIME

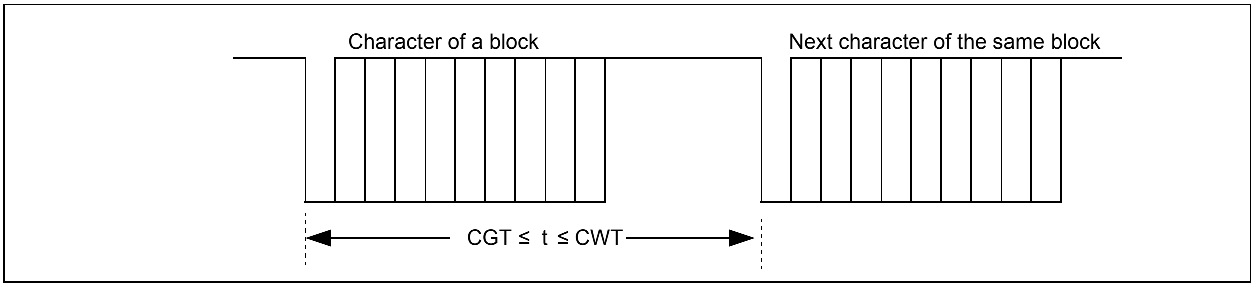
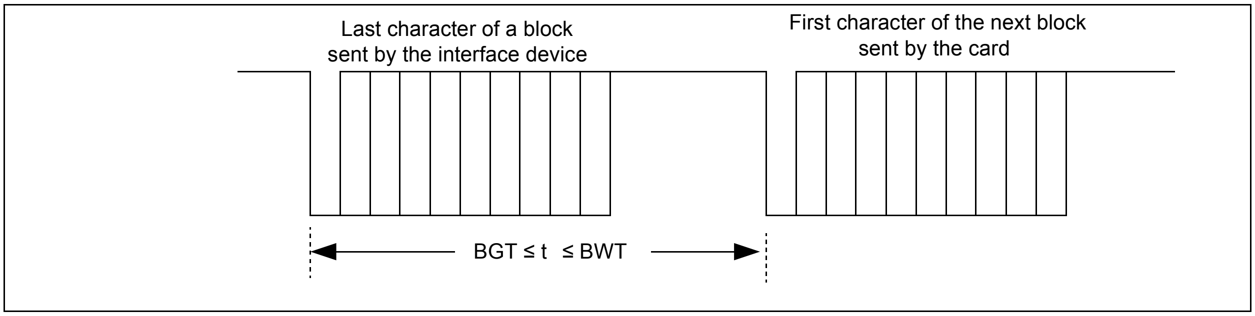


FIGURE 9: BLOCK WAIT TIME



© 2011 Microchip Technology Inc.

SYSTEM HARDWARE

The following hardware resources are used in the PIC microcontroller to develop a basic smart card communication demo:

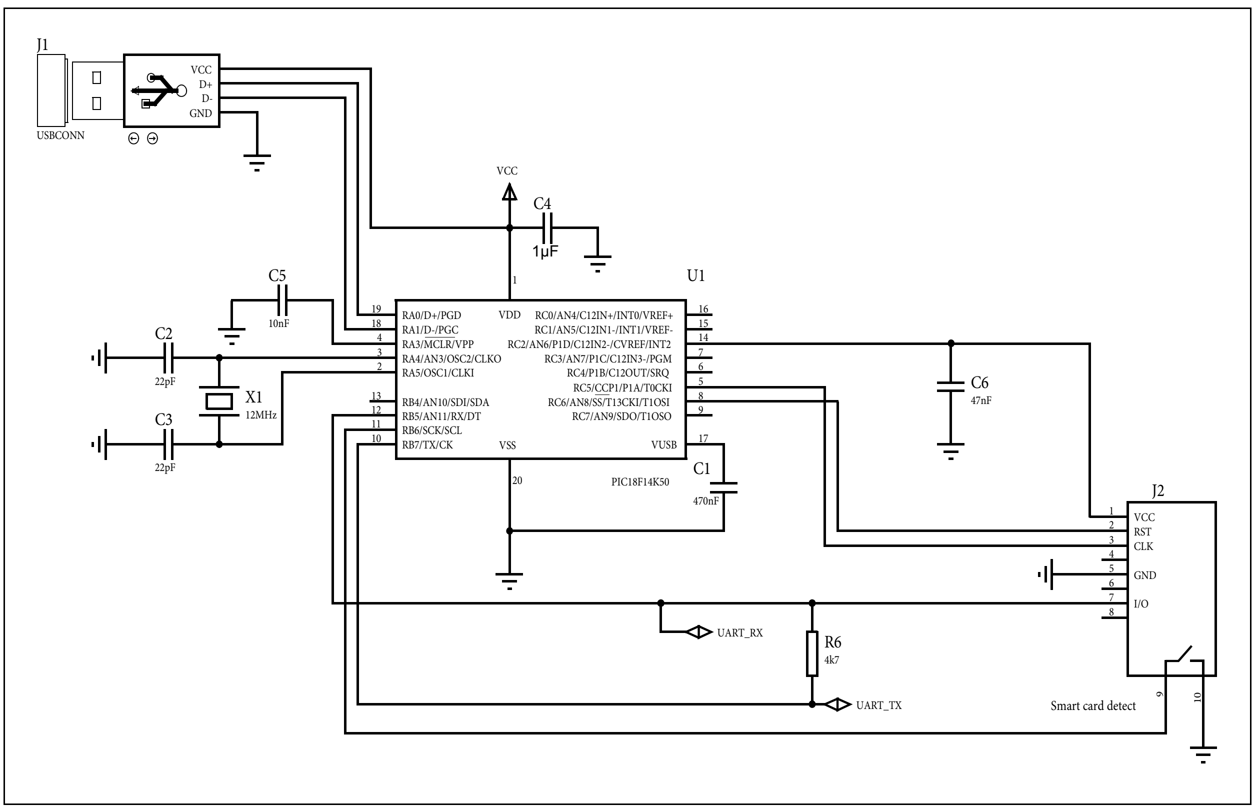
- One PWM Output or one Reference Clock Output
- One Timer
- One UART
- Six I/O pins

The smart card software library consists of UART driver, T = `0` and T = `1` protocol source code that meets the ISO 7816-3 standard. It allows the PIC microcontroller to communicate with the smart cards compatible with these protocols. For the latest version of the smart card software library, Help file, API header files and demo examples, refer to "www.microchip.com/MAL". Refer to the smart card software library help file for the details of possible demo boards for evaluation.

The microcontroller (interfacing device) has to be chosen based on the application and the electrical specifications of the smart card. Refer to Figure 10 as an example to develop your own smart card reader board. PIC18F14K50 provides VCC and Reset signal to the smart card. A PWM output is used as a reference clock for the smart card. The I/O signal from the card is sent to both UART_RX and UART_TX in order to manage bidirectional communication (half-duplex communication). Card presence is detected by the microcontroller using an internal pull-up input pin.

If the microcontroller is unable to provide enough current at the VCC pin of the smart card, then an op amp with suitable ratings can be used to supply the current to the smart card.

FIGURE 10: SMART CARD ADAPTER

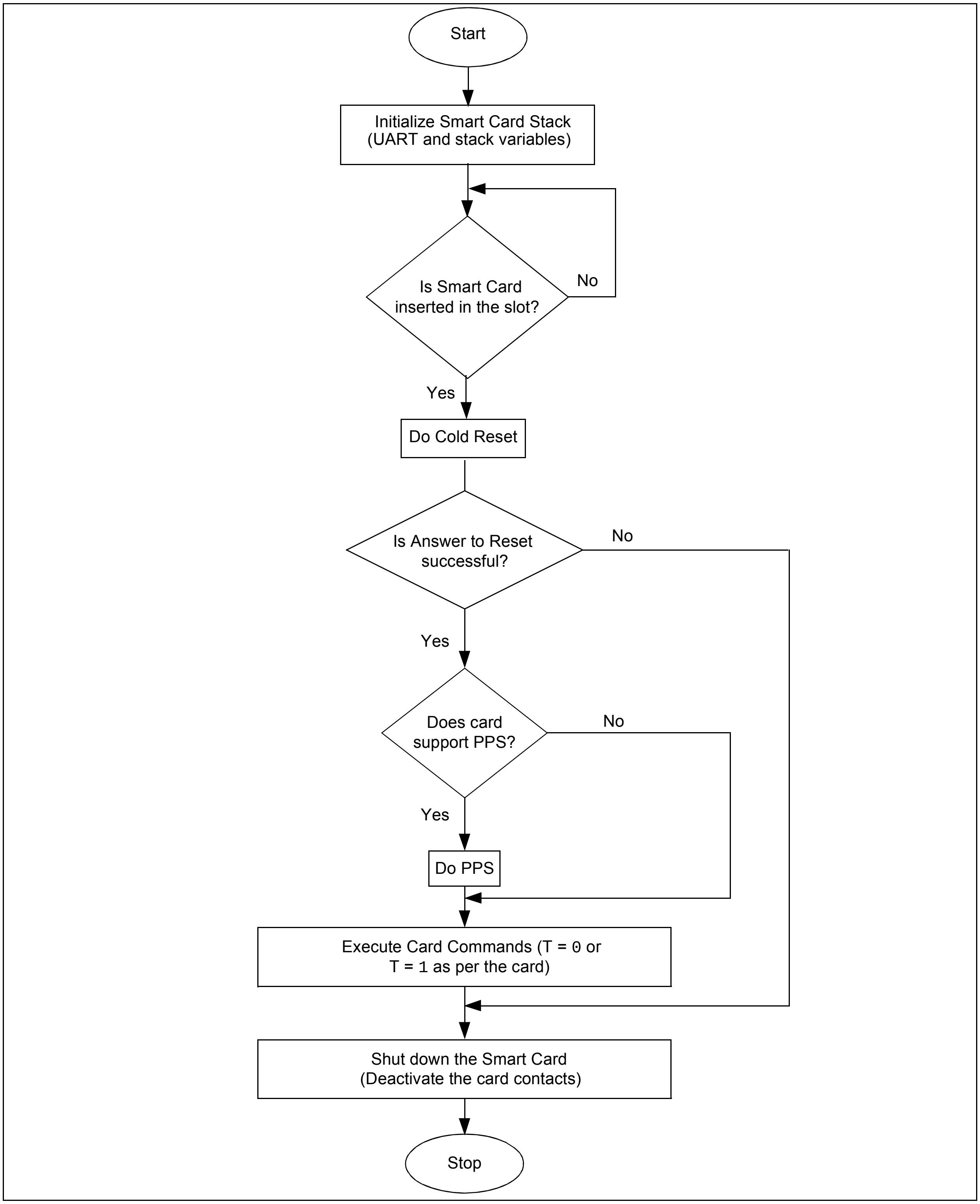


SOFTWARE FLOW

The smart card library provides the necessary APIs to communicate with the ISO 7816-3/4 compliant smart card.

The latest release of the smart card library supports both T = 0 and T = 1 protocols. The sequence of the function calls in the main application is shown in Figure 11.

FIGURE 11: SOFTWARE FLOW



 © 2011 Microchip Technology Inc.

CONCLUSION

This application note describes the fundamentals of the contact type smart cards, and how they are communicated using the PIC microcontroller. It also explains the `T = 0` and `T = 1` protocols, which are widely used in contact type smart card communications.

The software flow of a typical smart card reader and the hardware requirements of a basic smart card reader are described in this application note. Given the generic nature of the smart card software library, it can be easily ported to any PIC microcontroller (8-bit, 16-bit and 32-bit). For the latest version of the smart card software library, help file, API header files and demo examples, refer to "www.microchip.com/MAL".

REFERENCES

- ISO 7816-3 specifications available by license.
- www.microchip.com.

NOTES:

© 2011 Microchip Technology Inc.

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE**.** Microchip disclaims all liability arising from this information and its use. Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights.

Trademarks

The Microchip name and logo, the Microchip logo, dsPIC, KEELOQ, KEELOQ logo, MPLAB, PIC, PICmicro, PICSTART, PIC^{32} logo, rfPIC and UNI/O are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

FilterLab, Hampshire, HI-TECH C, Linear Active Thermistor, MXDEV, MXLAB, SEEVAL and The Embedded Control Solutions Company are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Analog-for-the-Digital Age, Application Maestro, CodeGuard, dsPICDEM, dsPICDEM.net, dsPICworks, dsSPEAK, ECAN, ECONOMONITOR, FanSense, HI-TIDE, In-Circuit Serial Programming, ICSP, Mindi, MiWi, MPASM, MPLAB Certified logo, MPLIB, MPLINK, mTouch, Octopus, Omniscient Code Generation, PICC, PICC-18, PICDEM, PICDEM.net, PICkit, PICtail, REAL ICE, rfLAB, Select Mode, Total Endurance, TSHARC, UniWinDriver, WiperLock and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

All other trademarks mentioned herein are property of their respective companies.

© 2011, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved.

Printed on recycled paper.

ISBN: 978-1-60932-957-0

QUALITY MANAGEMENT SYSTEM
CERTIFIED BY DNV
ISO/TS 16949:2002

Microchip received ISO/TS-16949:2002 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.

Worldwide Sales and Service

AMERICAS

Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
Technical Support:
http://www.microchip.com/support
Web Address:
www.microchip.com

Atlanta
Duluth, GA
Tel: 678-957-9614
Fax: 678-957-1455

Boston
Westborough, MA
Tel: 774-760-0087
Fax: 774-760-0088

Chicago
Itasca, IL
Tel: 630-285-0071
Fax: 630-285-0075

Cleveland
Independence, OH
Tel: 216-447-0464
Fax: 216-447-0643

Dallas
Addison, TX
Tel: 972-818-7423
Fax: 972-818-2924

Detroit
Farmington Hills, MI
Tel: 248-538-2250
Fax: 248-538-2260

Indianapolis
Noblesville, IN
Tel: 317-773-8323
Fax: 317-773-5453

Los Angeles
Mission Viejo, CA
Tel: 949-462-9523
Fax: 949-462-9608

Santa Clara
Santa Clara, CA
Tel: 408-961-6444
Fax: 408-961-6445

Toronto
Mississauga, Ontario,
Canada
Tel: 905-673-0699
Fax: 905-673-6509

ASIA/PACIFIC

Asia Pacific Office
Suites 3707-14, 37th Floor
Tower 6, The Gateway
Harbour City, Kowloon
Hong Kong
Tel: 852-2401-1200
Fax: 852-2401-3431

Australia - Sydney
Tel: 61-2-9868-6733
Fax: 61-2-9868-6755

China - Beijing
Tel: 86-10-8528-2100
Fax: 86-10-8528-2104

China - Chengdu
Tel: 86-28-8665-5511
Fax: 86-28-8665-7889

China - Chongqing
Tel: 86-23-8980-9588
Fax: 86-23-8980-9500

China - Hong Kong SAR
Tel: 852-2401-1200
Fax: 852-2401-3431

China - Nanjing
Tel: 86-25-8473-2460
Fax: 86-25-8473-2470

China - Qingdao
Tel: 86-532-8502-7355
Fax: 86-532-8502-7205

China - Shanghai
Tel: 86-21-5407-5533
Fax: 86-21-5407-5066

China - Shenyang
Tel: 86-24-2334-2829
Fax: 86-24-2334-2393

China - Shenzhen
Tel: 86-755-8203-2660
Fax: 86-755-8203-1760

China - Wuhan
Tel: 86-27-5980-5300
Fax: 86-27-5980-5118

China - Xian
Tel: 86-29-8833-7252
Fax: 86-29-8833-7256

China - Xiamen
Tel: 86-592-2388138
Fax: 86-592-2388130

China - Zhuhai
Tel: 86-756-3210040
Fax: 86-756-3210049

ASIA/PACIFIC

India - Bangalore
Tel: 91-80-3090-4444
Fax: 91-80-3090-4123

India - New Delhi
Tel: 91-11-4160-8631
Fax: 91-11-4160-8632

India - Pune
Tel: 91-20-2566-1512
Fax: 91-20-2566-1513

Japan - Yokohama
Tel: 81-45-471- 6166
Fax: 81-45-471-6122

Korea - Daegu
Tel: 82-53-744-4301
Fax: 82-53-744-4302

Korea - Seoul
Tel: 82-2-554-7200
Fax: 82-2-558-5932 or
82-2-558-5934

Malaysia - Kuala Lumpur
Tel: 60-3-6201-9857
Fax: 60-3-6201-9859

Malaysia - Penang
Tel: 60-4-227-8870
Fax: 60-4-227-4068

Philippines - Manila
Tel: 63-2-634-9065
Fax: 63-2-634-9069

Singapore
Tel: 65-6334-8870
Fax: 65-6334-8850

Taiwan - Hsin Chu
Tel: 886-3-6578-300
Fax: 886-3-6578-370

Taiwan - Kaohsiung
Tel: 886-7-213-7830
Fax: 886-7-330-9305

Taiwan - Taipei
Tel: 886-2-2500-6610
Fax: 886-2-2508-0102

Thailand - Bangkok
Tel: 66-2-694-1351
Fax: 66-2-694-1350

EUROPE

Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

Denmark - Copenhagen
Tel: 45-4450-2828
Fax: 45-4485-2829

France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

UK - Wokingham
Tel: 44-118-921-5869
Fax: 44-118-921-5820

02/18/11

© 2011 Microchip Technology Inc.