APPLICATION NOTE

DEMONSTRATION BOARD
CAKE 8020_06-D
FOR DUAL SMART CARD INTERFACE TDA8020HL

AN00058

Philips
Semiconductors

PHILIPS

Abstract

This report describes the demonstration board CAKE 8020_06-D that has been developed in order to demonstrate the dual smart card interface TDA8020HL.

APPLICATION NOTE

DEMONSTRATION BOARD
CAKE 8020_06-D
FOR DUAL SMART CARD INTERFACE TDA8020HL

Author:
Christophe CHAUSSET

Systems and Applications - Caen
France

Keywords
TDA8020HL
Dual smart card interface
ISO7816-3
Protocols T=0, T=1
Security Access Modules

Date: December 2000

CONTENTS

1 INTRODUCTION

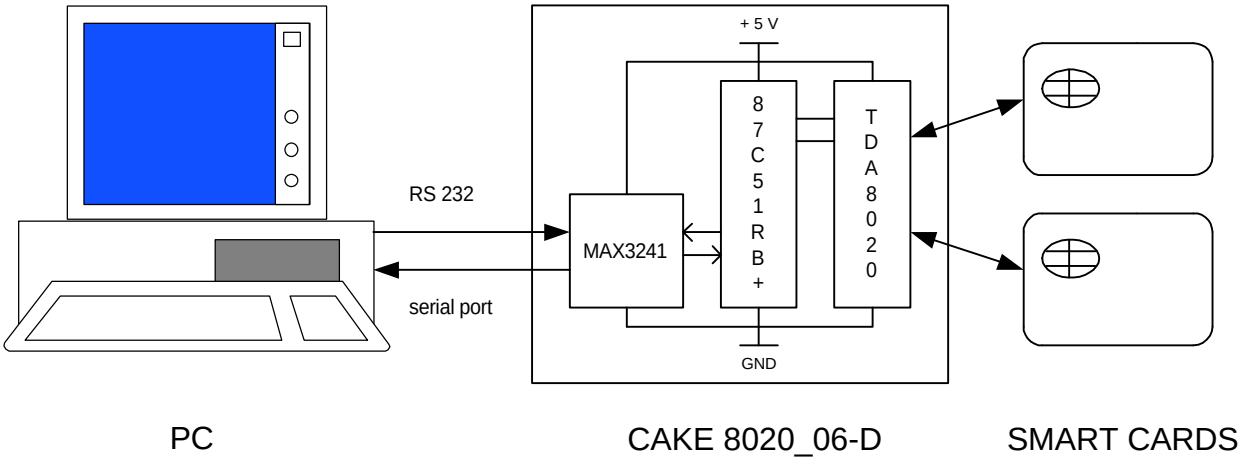
The TDA8020HL is a dual smart card interface providing all analogue electrical interface signals to two smart cards. This interface, mainly for asynchronous cards, should be placed between the smart card connectors and a microcontroller. It performs all supply protection and control functions and is directly compatible with ISO7816-3[1] specification.

A board has been built in order to demonstrate a communication between two smart cards and a host system which is here a PC; this board is driven from the PC by means of a software called “Alid.exe” through a serial link.

This demonstration tool allows to communicate with asynchronous cards (T=0 and T=1 protocols) respecting the ISO7816-3 standards.

A specific protocol called « ALPAR » has been defined on the serial interface between the dual smart card reader and the host system; it uses the APDUs frame types to convey the asynchronous card commands.

The following diagram illustrates this application.



[1] It is assumed that the reader of this application note is aware of ISO7816 terminology.

2 HARDWARE DESCRIPTION

The complete hardware information for the demo board CAKE 8020_06-D is available in appendix: Hardware Information.

2.1 Power Supply

This demonstration board requires a voltage supply from + 3.0 to 5.5 V.

2.2 Microcontroller

The microcontroller used is a P87C51RB+. It includes 16 Kbytes ROM and 512 bytes RAM. The microcontroller software is about 10 Kbytes in ROM, and a complete 256-byte page in RAM is dedicated to the card data. A complete 256-byte message can be exchanged with the smart card, thus respecting the EMV standards.

2.3 Interface with the PC

The communication between the PC and the board microcontroller is achieved according to a serial interface at 38400 bauds.
An interface circuit MAX3241ECAI is placed between the microcontroller 87C51RB+ and the serial port of the PC. This circuit allows to separate ingoing and outgoing signals.
The board may be connected to a PC via a serial SUB-D connector.

2.4 Clock Frequencies

On the demo board, a 14.74 MHz clock is delivered to the microcontroller and to the TDA8020 CLKIN1 and CLKIN2 pins. An asynchronous card, when activated, receives a clock equal to ¼ of the main clock, that is 3.68 MHz, fixed by CLKSEL1 and CLKSEL2 bits of TDA8020 control byte.

3 MICROCONTROLLER SOFTWARE

The TDA8020 I2C bus is controlled by software through the microcontroller pins P1.6 (SCL) and P1.7 (SDA).

The interrupt line IRQN is connected to the external interrupt P3.3 (INT1). Each time IRQN goes to low level, the 87C51RB+ reads the 2 TDA8020 status cards, and reacts accordingly to the happening event.

As there is a single software ISO UART, which handles the communication with the smart card, both I/OUC lines (I/O1UC and I/O2UC) are connected to the external interrupt P3.2 (INT0). In this case, before an APDU command is sent to card 1, card 1 I/OEN bit is set to logic 1 and card 2 I/OEN bit is set to logic 0.

CLKIN1 and CLKIN2 are connected together and driven from the same signal (XTAL2).

Due to processing time reasons, the software UART is only supporting two configurations with the external clock input frequency at 14.74 MHz:

- F = 372, D = 1: card clock = 3.68 MHz bit rate = 9906 Bauds
- F = 372, D = 2: card clock = 3.68 MHz bit rate = 19812 Bauds

Any asynchronous protocol (T=0, T=1) can be used because TDA8020 is protocol transparent on the I/O lines. The protocol management is made by software in the system controller.

4 SERIAL INTERFACE

4.1 Physical lines

The serial link between the demo board and the host controller is made by using the 2 lines Rx and Tx; Rx is used to receive data from the system controller and Tx is used to transmit data to the system controller.

A security feature has been implemented on the microcontroller receiving procedure in order to avoid any blocking of the serial interface.

4.2 Data link layer

Serial data format

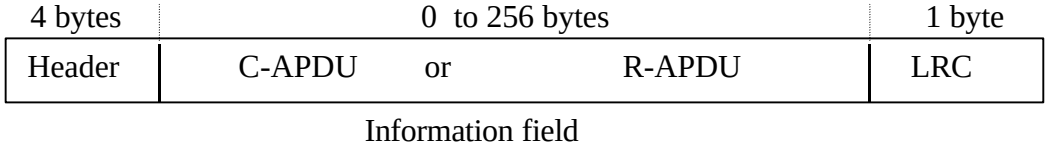
1 start bit
8 data bits
1 stop bit, no parity

Baud rate 38400 bauds

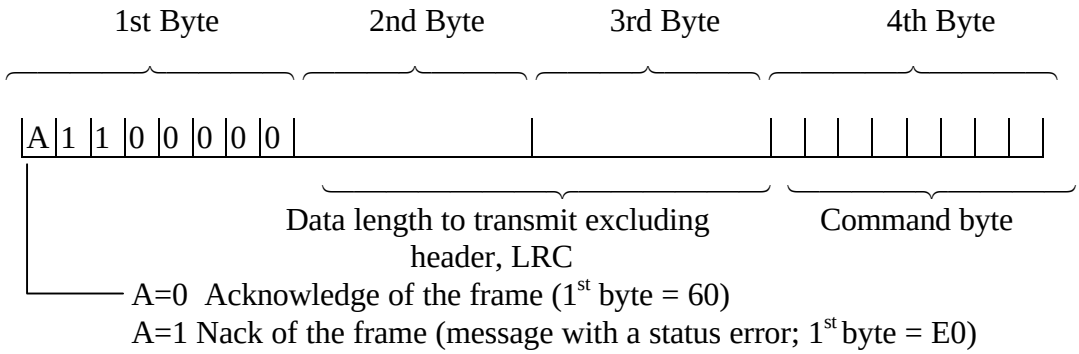
Data is exchanged between the system controller and the microcontroller in blocks, each block made up of binary characters on one byte:

4 header characters
0 to 256 data characters (C-APDU or R-APDU)
1 LRC character

Frame structure:



The 4 bytes header includes:



LRC byte:

The LRC (Longitudinal Redundancy Check) byte is such that the exclusive-oring of all bytes including LRC is null.

4.3 Dialog structure

The system controller is the master for the transmission; each command from the master is followed by an answer from the dual smart card reader including the same command byte as the input command. The only commands which are outgoing commands from the dual smart card reader are those related to a card insertion or extraction or a time out command on Rx line.

The dual smart card reader (TDA8020 and P87C51RB+) will be called Interface Device (**IFD**) in the following document.

4.3.1 Successful command

System to IFD:	60	XX XX	YY	nnnnnnnnnnnnnnnnnnnn	ZZ
	ACK	length	code	data (C-APDU)	LRC
IFD to System:	60	UU UU	YY	mmmmmmmmmmmm	TT
	ACK	length	code	data (R-APDU)	LRC

The same command byte YY is returned in the answer from IFD.

4.3.2 Unsuccessful command

System to IFD:	60	XX XX	YY	nnnnnnnnnnnnnnnnnnnn		ZZ
	ACK	length	code	data (C-APDU)		LRC
IFD to System:	E0	UU UU	YY	SS	TT	
	NACK	length	code	STATUS	LRC	

The status gives the error code information (see error list).

4.3.3 Card removal

IFD to System:	60	00 01	A0	10	ZZ
	ACK	length	code	param	LRC

4.3.4 Card insertion

IFD to System:	60	00 01	A0	11	ZZ
	ACK	length	code	param	LRC

4.3.5 Answer with an acknowledge (power_off)

System to IFD:	60	00 00	4D	ZZ	
	ACK	length	code	LRC	
IFD to System:	60	00 00	4D	ZZ	
	ACK	length	code	LRC	

When the answer is an acknowledge of the command, the IFD sends a frame back with the same content of the command.

5 COMMAND BYTES

The following command bytes are available:

Incoming command	*Code*	*Answer from reader*
power_on_3V	$6D_H$	ATR from card or error message
power_on_5V	$6E_H$	ATR from card or error message
power_off	$4D_H$	acknowledge or error message
card_command (APDU)	00_H	card command (APDU) or error message
ifsd_request	$0C_H$	acknowledge or error message
select_card	$6A_H$	acknowledge or error message
check_pres_card	09_H	card presence information

5.1 Outgoing commands (only)

Outgoing command	*Code*	*Parameter/Description*
Card1_extraction	$A0_H$	10_H
Card1_insertion	$A0_H$	11_H
Card2_extraction	$A0_H$	20_H
Card2_insertion	$A0_H$	21_H

These commands are sent as soon as a card is inserted or extracted without any command coming from the system. These commands are using the same operating code with a parameter giving the additional information.

Card1_deactivated	$E5_H$	The card is deactivated due to a hardware problem (short circuit on Vcc, overcurrent)
Card2_deactivated	$E6_H$	Idem

These outgoing commands are sent only when the host is either waiting for a reply or in stand by; when the card is extracted whereas the host is sending a frame to the IFD, the card_extraction message will be sent from the IFD only when it has received the complete frame coming from the host controller. This system avoids any conflict on the serial line.

Time_out	FF_H	Time out problem on (IFD) Rx line

This command is used in order to warn the host controller that the last communication has broken down so that the Rx line of the IFD does not remain blocked.

6 ERROR LIST

The error list gives the status code identification and a brief explanation of the status error code.

Status code	*Meaning*
01_H	One byte in ATR have a 'Reserved for Future Use' value
02_H	The card may need a VPP of 5 V to process certain commands
04_H	The card may need a VPP > 5 V to process certain commands
08_H	TS is neither 0x3B nor 0x3F
$0A_H$	3 consecutive errors from the card in T=1 protocol
20_H	Too long APDU
21_H	Too short APDU
22_H	Card mute during T=1 exchange
23_H	Procedure byte error
24_H	Bad NAD value
25_H	Bad LRC value
26_H	Resynchronised
27_H	Chain aborted
28_H	Bad PCB value
$2A_H$	4 parity errors in transmission
$2B_H$	4 parity errors in reception
$3B_H$	Early answer during power on
40_H	Overflow from card (258 bytes max.)
55_H	Unknown command
80_H	Card mute after power on
82_H	ATR not supported (bad ATR mapping)
84_H	Wrong TCK value in the ATR
88_H	Bad FiDi (parameters Fi or Di not supported)
90_H	Protocol is neither T=0 nor T=1
99_H	IFSD is not accepted
$9A_H$	Not a T=0 card
$9B_H$	Not a T=1 card

$A0_H$	CRC code in T=1 not supported
$C0_H$	Card absent
$E5_H$	Card 1 deactivated
$E6_H$	Card 2 deactivated
$F0_H$	Serial LRC error
FF_H	Serial time out

7 COMMANDS DESCRIPTION

7.1 Power_on commands

The power up command (3V or 5V) has to be followed by a parameter;
00_H indicates that all the parameters of the ATR of the card compliant with ISO7816-3 will be taken into account.
01_H indicates that an automatic IFSD request is sent if a T=1 protocol card is active.

7.2 Power_on_3V

This command allows to activate the card at a VCC of 3V. Every signal going to the card will be referenced to this VCC=3V.

An activation sequence is processed following the ISO7816-3 normalisation (VCC is rising, I/O is enabled, CLK is started and RST is processed). If the card answers to this command, the answer will contain all the ATR parameters; these parameters are memorised in IFD and will be taken into account during all the card session (until the card is deactivated or until a warm reset is processed). The structure of the answer is the following:

System to IFD:	60	00	01	6D	00	0F	
				code	ISO	LRC	
IFD to System:	60	XX	XX	6D	nnnnnnnnnnnnnnnnnnnn		ZZ
	ACK	length		code	ATR parameters		LRC

If the card is in specific mode, IFD will process the next command directly using the new interface parameters of this specific mode.
If the card does not answer to the reset, an error code is returned to the application.
This command can be used to generate a warm reset if the card is already activated.

7.3 Power_on_5V

This command allows to activate the card at a VCC of 5V. All the signals going to the card will be referenced to this VCC=5V.
See power_on_3V for the other characteristics.

System to IFD:	60	00	01	6E	00	0F	
				code	ISO	LRC	
IFD to System:	60	XX	XX	6E	nnnnnnnnnnnnnnnnnnnn		ZZ
	ACK	length		code	ATR parameters		LRC

7.4 Power_off

This command is used to deactivate the card whatever it has been activated for 3V or 5V operation. A deactivation sequence is processed in about 100µs following the ISO 7816-3 normalisation.

System to IFD: 60 00 00 4D 2D
IFD to System: 60 00 00 4D 2D

7.5 Card_command (APDU)

This command is used to transmit card commands under APDU format from system to IFD. An answer to such a command is also made in APDU format from IFD to the system.

Example:
System to IFD: 60 00 07 00 00 A4 00 00 02 4F 00 LRC (Select File 4F 00)
IFD to System: 60 00 02 00 90 00 LRC

7.6 IFSD_request

This command is sent from the host controller to the card in order to negotiate the size of the interface device buffer (IFSD). In ISO mode, the default value is 32 bytes; it can be negotiated up to 254 bytes.

One parameter has to be sent to the card: the IFSD value.

Example:

System to IFD:	60 00 01 0C FE LRC	FE is the IFSD value
IFD to System:	60 00 00 0C 6C	

7.7 Select_card

This command is used to select card 1 or card 2. Parameter 01_H is used for selecting card 1 and parameter 02_H for selecting card 2.

When calling this function, several operations are executed:

1. All current card parameters are saved.
   - parameter FiDi
   - parameter Protocol
   - for T=0 protocol : WI
   - for T=1 protocol : CWI, BWI, ifsc.
2. The new card is selected.
3. All new card parameters are restored.

Example:

System to IFD:	60 00 01 6A 01 LRC	Card 1 selected
IFD to System:	60 00 01 6A 01 LRC	
System to IFD:	60 00 01 6A 02 LRC	Card 2 selected
IFD to System:	60 00 01 6A 02 LRC	

7.8 Card movement (card insertion, card extraction)

This command is sent directly to the system processor as soon as a card extraction or insertion has occurred.

Example:

IFD to System:	60 00 01 A0 10 LRC	(card 1 extracted)
or		
IFD to System:	60 00 01 A0 21 LRC	(card 2 inserted)

7.9 Time_out

This command is sent from IFD to the host controller if, during a transmission from the host controller to IFD, the time difference between 2 characters exceeds 10 ms. This timing is calculated between each character of a frame and starts after the first character. It is disabled after the last character of the frame. This feature has been implemented in order to avoid any blocking of the transmission line between the host controller and IFD.

IFD to System: E0 00 01 00 FF LRC

7.10 Check_pres_card

This command is used to check the card presence of the current selected card.

System to IFD: 60 00 00 09 69
IFD to System: 60 00 01 09 PAR LRC

PAR = 00_H for card absent
PAR = 01_H for card present

8 INFORMATION FIELD FOR ASYNCHRONOUS CARDS

The information field that can include up to 256 bytes is composed of APDUs (Application Protocol Data Unit) according to the ISO7816-4 normalisation definition.

Different examples are given according to Annex A of the EMV'96 in T = 0.

Case 1 command

TAL (System)		TTL (IFD)
{60, 00, 04, 00, CLA, INS, P1, P2, LRC}	⇒	
4 header bytes	⇐	{60, 00, 02, 00, 90, 00, LRC}

Case 2 command

TAL		TTL
{60, 00, 05, 00, CLA, INS, P1, P2, 00, LRC}	⇒	
4 header bytes	⇐	{60, Licc+2, 00, [Data (Licc)], 90, 00, LRC}

Case 3 command

TAL		TTL
{60, 00, Lc+5, 00, CLA, INS, P1, P2, Lc, [data Lc], LRC}	⇒	
4 header bytes	⇐	{60, 00, 02, 00, 90, 00, LRC}

Case 4 command

TAL TTL

{60, 00, Lc+5+1, 00, CLA, INS, P1, P2, Lc, [data Lc], 00, LRC} ⇒

4 header bytes ⇐ {60, Licc+2, 00, [data Licc], 90, 00, LRC}

Case 2 command using the 61 and 6C procedure byte

TAL TTL

{60, 00, 05, 00, CLA, INS, P1, P2, 00, LRC} ⇒

4 header bytes ⇐{60, D1+D2+Dn+2, 00, [data D1+D2+Dn], 90, 00, LRC}

9 CONCLUSION

This demo board is a typical example of a dual smart card reader for a set top box or an application with security access modules.

Some applications, such as banking applications, require that a smart card having some security features concerning the application, be permanently inserted in the smart card reader. These Security Access Modules are characterising the application and the terminal. Depending on the number of applications that is supported by the terminal, there can be more than one SAM in the terminal. For each type of payment operator (e.g. GIE), a specific security module is included in the terminal in order to validate the transactions.

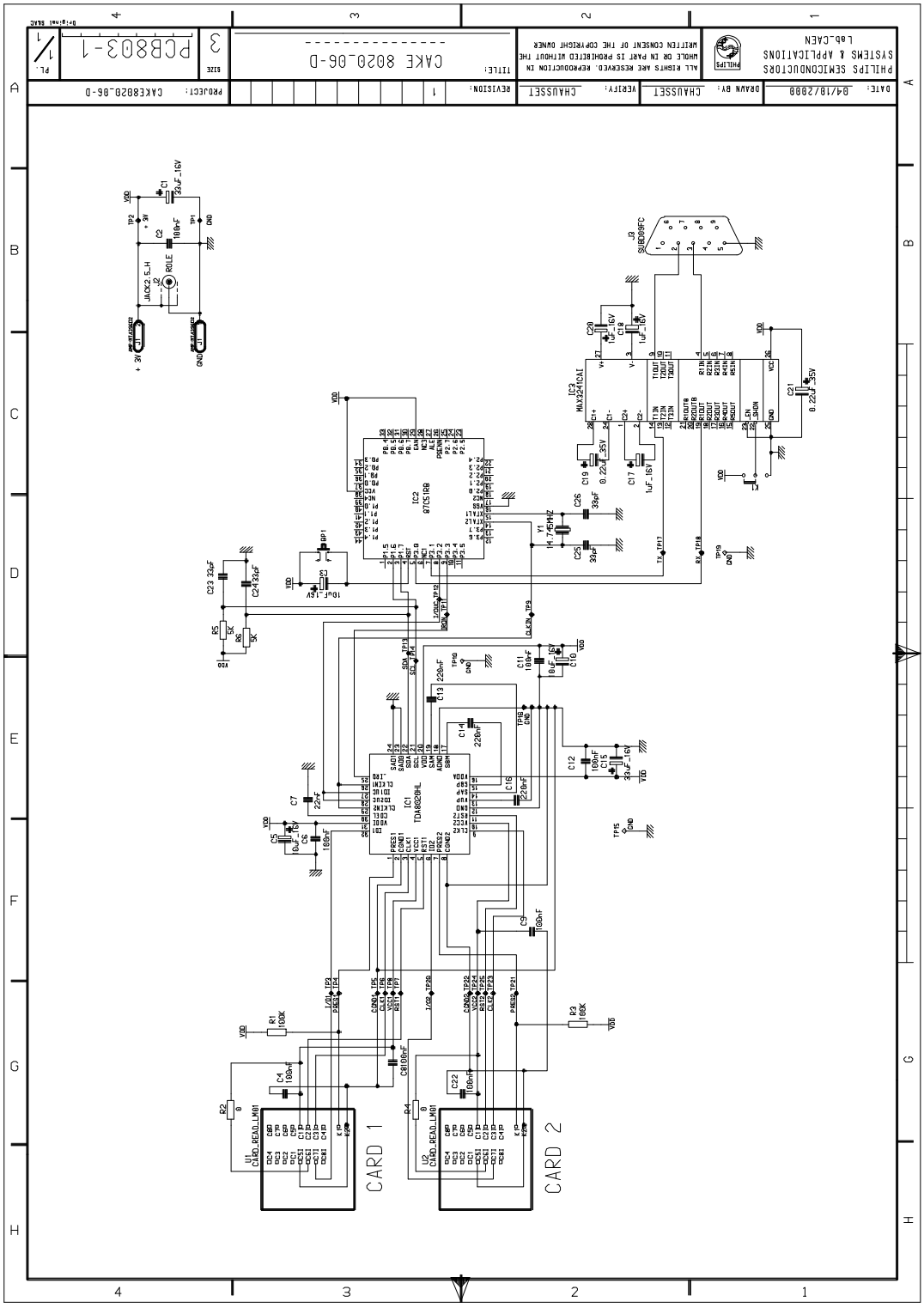
In this application, any card supporting an asynchronous protocol (T=0, T=1) can be used as TDA8020 is protocol transparent on the I/O lines. The protocol is managed by software in the system controller.

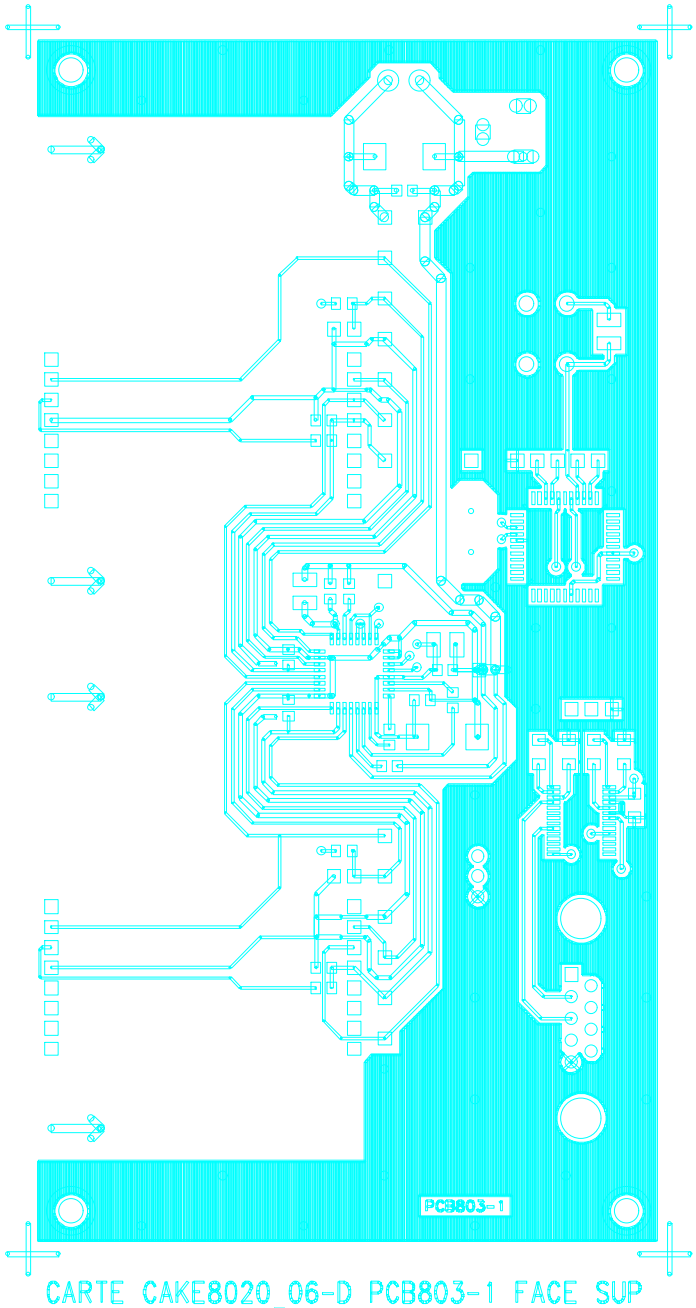
TDA8020 requires a few external components but also a few microcontroller interface signals (SCL, SDA, I/O1UC, I/O2UC and IRQN).

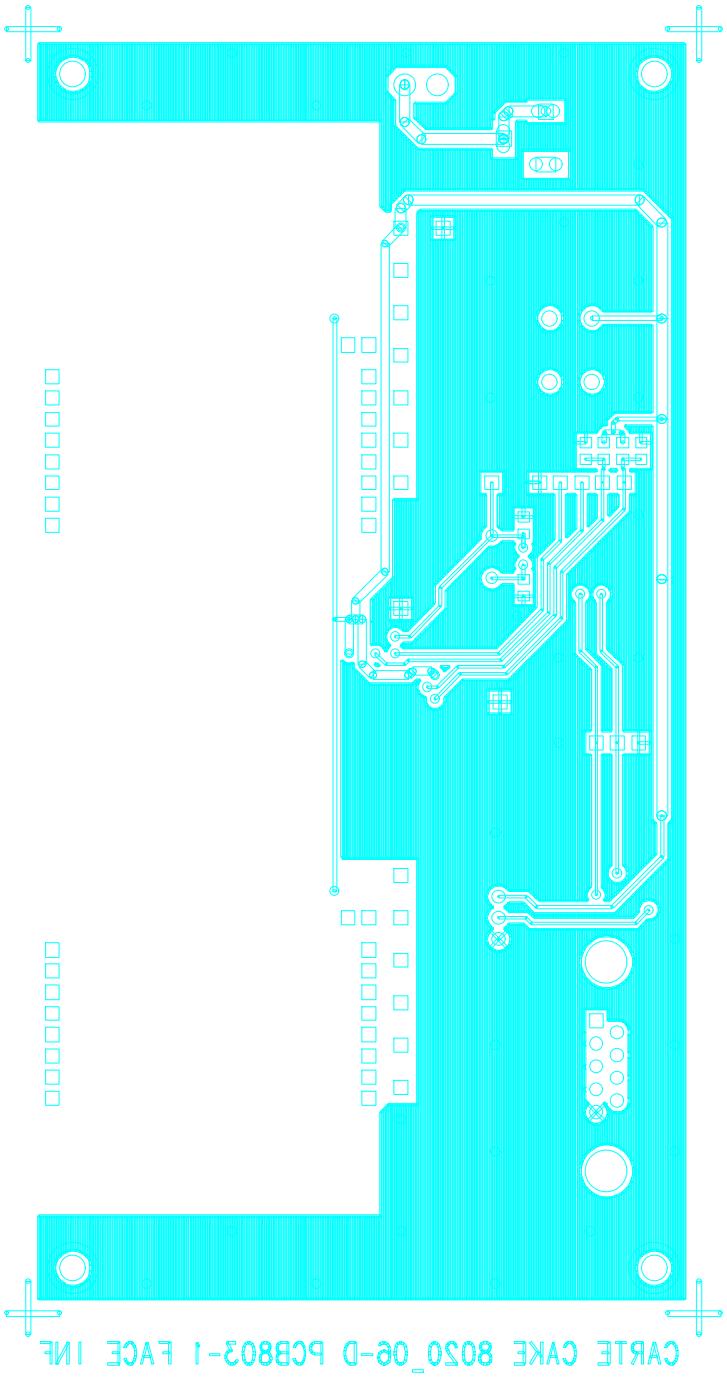
The general characteristics of this reader are:

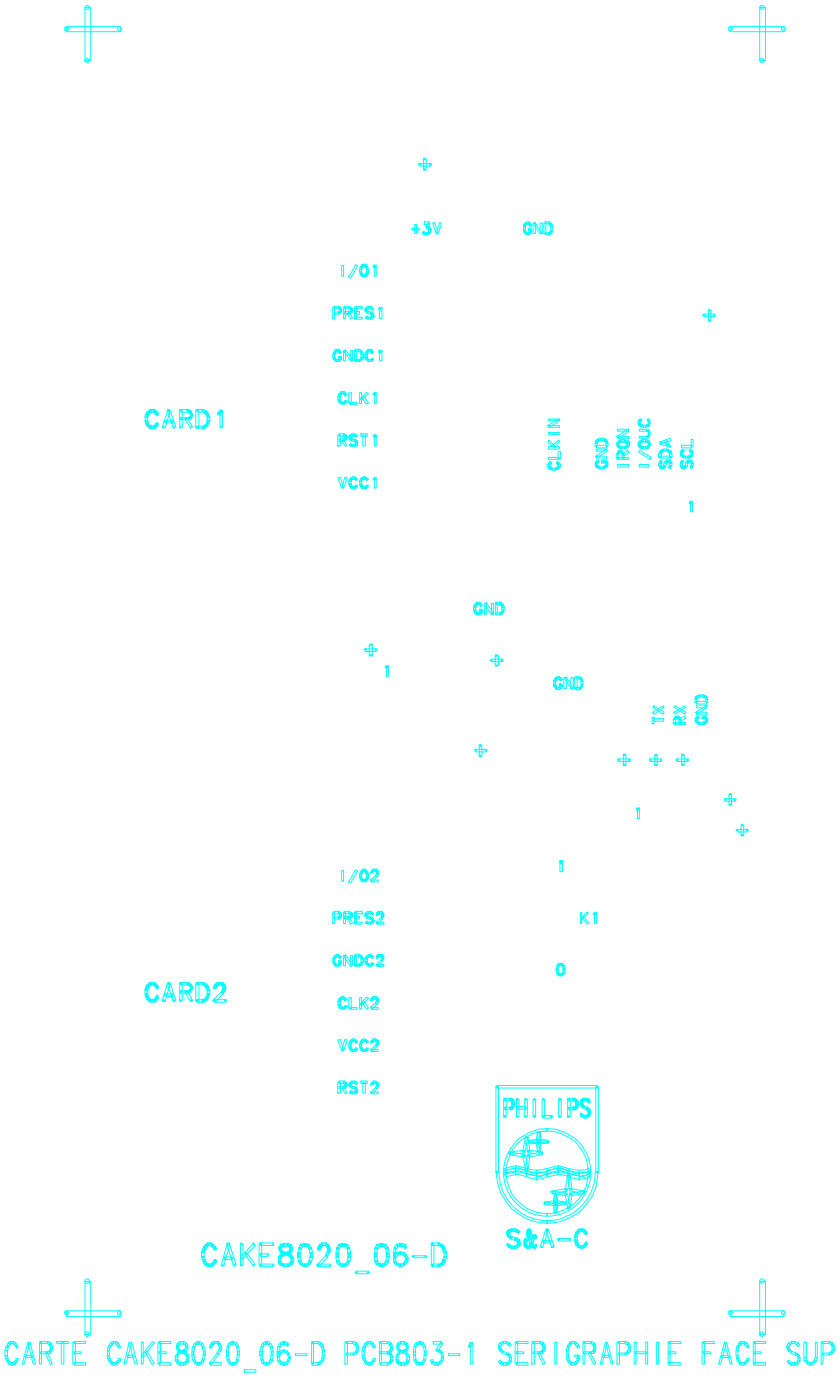
- Dual slot reader with card selection
- Two cards supported at the same time whatever the protocol and the VCC value are
- 3V and 5V cards supported
- ISO 7816-3 supported
- Asynchronous protocols (T=0 and T=1) supported
- Control and communication with the host through a serial interface at 38400 bauds
- Automatic hardware protections in the event of card take off, supply voltage dropout, short circuit or overheating
- Communication with the host made at the APDU level
- Supply voltage from 2.5V up to 6.5V for TDA8020

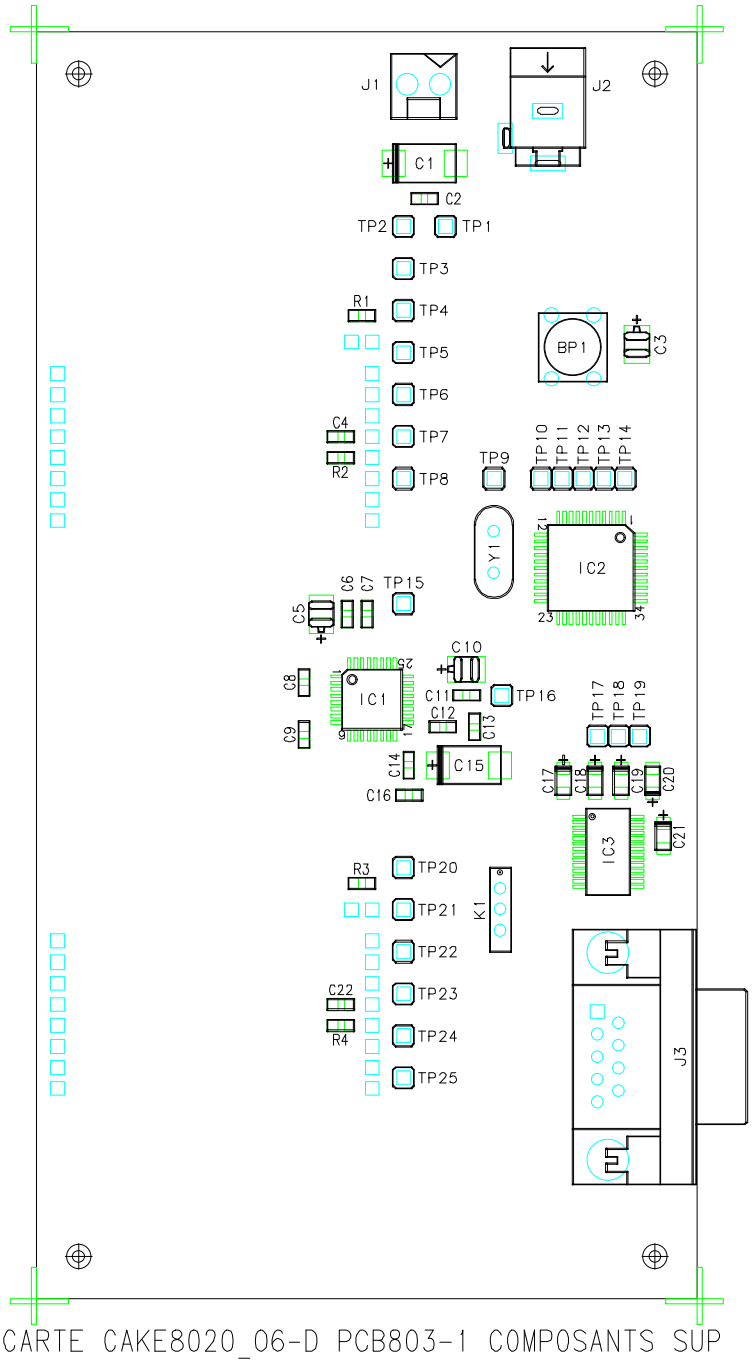
10 APPENDIX: Hardware Information

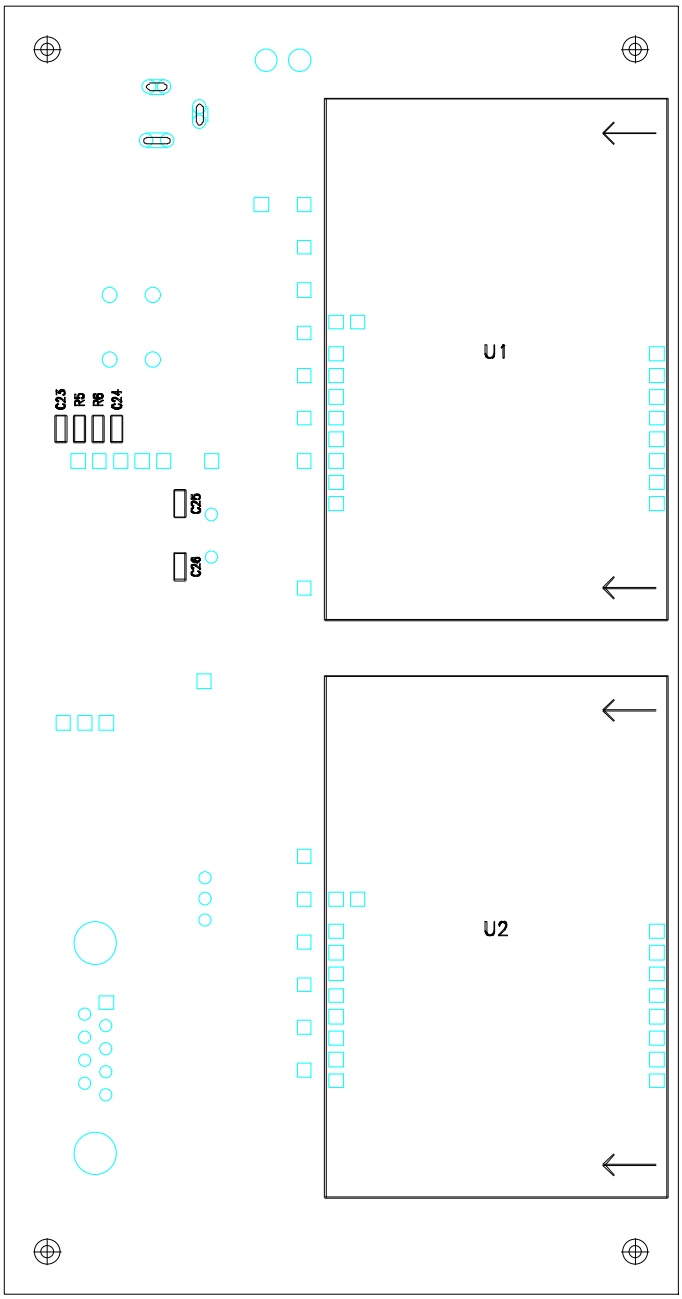

PHILIPS SEMICONDUCTORS
SYSTEMS & APPLICATIONS
Lab_CAEN
ALL RIGHTS ARE RESERVED. REPRODUCTION IN WHOLE OR IN PART IS PROHIBITED WITHOUT THE WRITTEN CONSENT OF THE COPYRIGHT OWNER
TITLE: CAKE 8020_06-D
SIZE: 3
PCB803-1
DRAWN BY: CHAUSSET
VERIFY: CHAUSSET
REVISION: 1
PRODUCT: CAKE8020_06-D
DATE: 04/10/2000
CARD 1
CARD 2
IC1 TDA8020HL
IC2 87C51RB
IC3 MAX241CAI
J3 SUB9PC
Y1 4.745MHZ


PCB803-1
CARTE CAKE8020_06-D PCB803-1 FACE SUP


CARTE CAKE 8020_06-D PCB803-1 FACE INF


+3V
GND
I/O1
PRES1
GNDC1
CLK1
RST1
VCC1
CARD1
CLK IN
GND
IRQN
I/OUC
SDA
SCL
GND
GND
TX
RX
GND
I/O2
PRES2
GNDC2
CLK2
VCC2
RST2
CARD2
K1
PHILIPS
S&A-C
CAKE8020_06-D
CARTE CAKE8020_06-D PCB803-1 SERIGRAPHIE FACE SUP


J1
J2
C1
C2
TP2
TP1
TP3
R1
TP4
TP5
BP1
C3
TP6
C4
TP7
R2
TP8
TP9
TP10
TP11
TP12
TP13
TP14
Y1
IC2
C5
C6
C7
TP15
C10
C8
IC1
C11
TP16
C12
C13
TP17
TP18
TP19
C9
C14
IC15
C17
C18
C19
C20
C16
IC3
C21
R3
TP20
TP21
K1
TP22
C22
TP23
R4
TP24
TP25
J3
CARTE CAKE8020_06-D PCB803-1 COMPOSANTS SUP



CARTE CAKE8020_06-D PCB803-1 COMPOSANTS INF

```
# date : Tuesday October 10, 2000; 15:42:30

        **** NOMENCLATURE ****

CARTE CAKE8020_06-D  PCB803-1

     REFERENCE           GEOMETRY             DESCRIPTION

        BP1             microcosmos    poussoir2, MICROCOSMOS
         C1               c293d_d      capa_pol, 33uF_16V
         C2                c0805       capa, 100nF
         C3               c595d_b      capa_pol, 10uF_16V
         C4                c0805       capa, 100nF
         C5               c595d_b      capa_pol, 10uF_16V
         C6                c0805       capa, 100nF
         C7                c0805       capa, 22nF
         C8                c0805       capa, 100nF
         C9                c0805       capa, 100nF
        C10               c595d_b      capa_pol, 10uF_16V
        C11                c0805       capa, 100nF
        C12                c0805       capa, 100nF
        C13                c0805       capa, 220nF
        C14                c0805       capa, 220nF
        C15               c293d_d      capa_pol, 33uF_16V
        C16                c0805       capa, 220nF
        C17               c293d_a      capa_pol, 1uF_16V
        C18               c293d_a      capa_pol, 1uF_16V
        C19               c293d_a      capa_pol, 0.22uF_35V
        C20               c293d_a      capa_pol, 1uF_16V
        C21               c293d_a      capa_pol, 0.22uF_35V
        C22                c0805       capa, 100nF
        C23                c0805       capa, 33pF
        C24                c0805       capa, 33pF
        C25                c0805       capa, 33pF
        C26                c0805       capa, 33pF
        IC1               sot358_1     tda8020hl, TDA8020HL
        IC2               sot307_2     87c51rb, 87C51RB
        IC3               sot341_1     max3241, MAX3241CAI
         J1               mta396d2     edge, AMP:MTA396D2
         J2              jack2.5_h     cinch_h, JACK2.5_H
         J3              subd_09fc     subd_09, SUBD09FC
         K1               int_1k2      int_1k2, SECME:1K2
         R1                r0805       res, 100K
         R2                r0805       res, 0
         R3                r0805       res, 100K
         R4                r0805       res, 0
         R5                r0805       res, 5K
         R6                r0805       res, 5K
        TP1                 tp1        test, TEST_1MM
        TP2                 tp1        test, TEST_1MM
        TP3                 tp1        test, TEST_1MM
        TP4                 tp1        test, TEST_1MM
        TP5                 tp1        test, TEST_1MM
        TP6                 tp1        test, TEST_1MM
        TP7                 tp1        test, TEST_1MM
        TP8                 tp1        test, TEST_1MM
```

```
TP9                tp1         test, TEST_1MM
TP10               tp1         test, TEST_1MM
TP11               tp1         test, TEST_1MM
TP12               tp1         test, TEST_1MM
TP13               tp1         test, TEST_1MM
TP14               tp1         test, TEST_1MM
TP15               tp1         test, TEST_1MM
TP16               tp1         test, TEST_1MM
TP17               tp1         test, TEST_1MM
TP18               tp1         test, TEST_1MM
TP19               tp1         test, TEST_1MM
TP20               tp1         test, TEST_1MM
TP21               tp1         test, TEST_1MM
TP22               tp1         test, TEST_1MM
TP23               tp1         test, TEST_1MM
TP24               tp1         test, TEST_1MM
TP25               tp1         test, TEST_1MM
 U1          card_read_lm01  card_read_lm01, CARD_READ_LM01
 U2          card_read_lm01  card_read_lm01, CARD_READ_LM01
 Y1              hc49s       quartz, 14.745MHZ
```