TWN4

Description PC/SC

DocRev2, May 13, 2016

Elatec GmbH

Contents

1 PC/SC Specification Overview

TWN4 is the name of a powerful and versatile series of RFID readers and writers. PC/SC (short for “Personal Computer/Smart Card”) is a specification for smart card integration into computing environments.

This document describes how to setup a PC/SC environment with TWN4 and different kinds of Integrated Circuit Cards.

1.1 PC/SC Components

1.2 Integrated Circuit Card (ICC)

The ICC (commonly called a “smart card”) is a credit card sized plastic case with an embedded microprocessor chip.

1.3 Interface Device (IFD)

The IFD (commonly called a “smart card reader”) is the physical interface through which ICCs communicate with a PC. The IFD provides DC power to the microprocessor chip (DC = direct current, as opposed to alternating current). Also, the IFD provides a clock signal, which is used to step the program counter of the microprocessor, as well as an I/O line through which digital information may be passed between the IFD and the ICC.

1.4 IO Device Driver

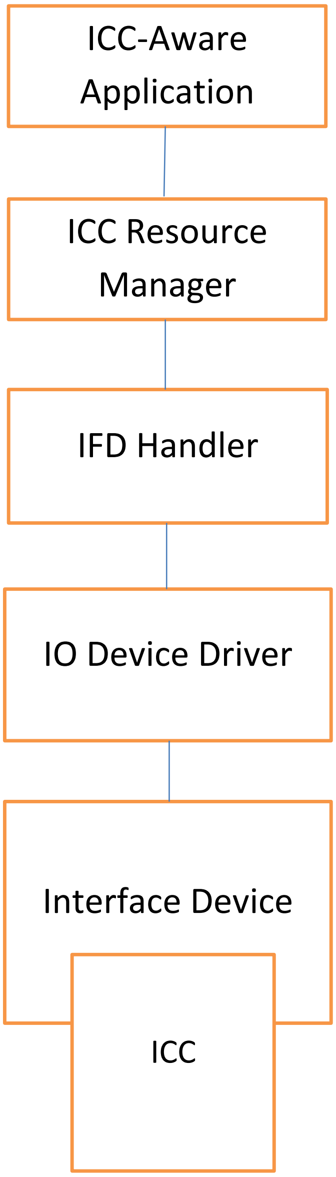
The IO Device Driver implements the low level communication between the IFD and the Host. A USB document[3] describes proposed requirements and specifications for Universal Serial Bus (USB) devices that interface with Integrated Circuit Cards or act as interfaces with Integrated Circuit Cards.

1.5 Interface Device Handler (IFD Handler)

The IFD Handler encompasses the PC software necessary to map the native capabilities of the IFD to the IFD Handler interface defined in Part 3 of this specification.

Under Linux, the corresponding software component can be for example libccid.

Figure 1.1: PC/SC Components



1.6 ICC-Aware Application

The ICC-Aware Application (“Application”) is an arbitrary software program within the PC operating environment, which wants to make use of the functionality provided by one or more ICCs.

Under Linux, the corresponding software component can be for example opensc-tool.

1.7 Resource Manager

The ICC Resource Manager is a key component of the PC/SC Workgroup's architecture. It is responsible for managing the other ICC-relevant resources within the system and for supporting controlled access to IFDs and, through them, individual ICCs.

Under Linux, the corresponding software component can be for example pcscd.

2 Typical ICC-Aware Application Workflow

Typically, an ICC-aware application that the user implements should distinguish the type of the ICC, because different ICCs have different APDUs supported. This can be done by reading the Answer to Reset (ATR) of the ICC.

Once the ATR is read, the ICC-aware application can send APDU commands to TWN4, in order to read or write data saved on ICC.

2.1 Distinguish the Type of ICC

2.1.1 Answer to Reset (ATR)

An Answer To Reset (ATR) is a message output by a contact card conforming to ISO/IEC 7816 standards, following electrical reset of the card's chip by a card reader. The ATR conveys information about the communication parameters proposed by the card, and the card's nature and state.

How an ATR is constructed and how to parse an ATR is beyond the range of this document. Please refer to ISO 7816-3 [1] for more information.

For contactless ICCs, the IFD subsystem must construct an ATR from the fixed elements that identify the cards. Please refer to Interoperability Specification for ICCs and Personal Computer Systems Part 3 [4] for more information.

2.2 Exchange Data to ICC

2.2.1 APDU

An Application Protocol Data Unit (APDU) is the communication unit between a smart card reader and a smart card. The structure of the APDU is defined by ISO/IEC 7816-4 [2].

2.2.2 Structure of an APDU

There are two categories of APDUs: command APDUs and response APDUs. A command APDU is sent by the reader to the card. It contains a mandatory 4-byte header (CLA, INS, P1, P2) 0 to 65534 bytes of data.

A response APDU is sent by the card to the reader. It contains from 0 to 65 535 bytes of data, and 2 mandatory status bytes (SW1, SW2).

ISO 7816-4 defines interindustry commands for interchange as well as the responses for the commands. Please refer to it for more information.

Command APDU		
Field name	**Lenth(bytes)**	**Description**
CLA	1	Instruction class - indicates the type of command, e.g. interindustry or proprietary
INS	1	Instruction code - indicates the specific command, e.g. “write data”
P1-P2	2	Instruction parameters for the command, e.g. offset into file at which to write the data
Lc	0, 1 or 3	Encodes the number (Nc) of bytes of command data to follow
Command data	Nc	Nc bytes of data
Le	Ne	Encodes the maximum number (Ne) of response bytes expected
Response APDU		
Field name	**Lenth(bytes)**	**Description**
Response Data	X	Payload of the response.
SW1-SW2	2	Command processing status. For instance 0x9000 indicates success

3 Overview of ICCs and TWN4 Family

This chapter helps the user to understand different TWN4 products and different ICC types. It also helps the user to choose a suitable TWN4, depending on the ICC they want to use.

3.1 TWN4 Family

3.1.1 TWN4 SmartCard

The TWN4 SmartCard Reader includes both a contactless RFID interface as well as a slot to read contact-based cards. This exciting combination allows its users to add an additional higher level of security where required for certain applications dealing with extremely sensitive information.

It is worthy of being mentioned that the contactless RFID interface and the contact slot have the same logical slot. Contact-based ICC has priority against the contactless ICC. When a contact-based ICC is inserted, TWN4 SmartCard will close its RFID interface.

3.1.2 TWN4 Desktop

TWN4 Desktop has the same performance like a TWN4 SmartCard, when it needs to exchange data with a transponder. It has no contact slots, where the user can insert its own contact-based cards.

3.2 Overview of ICCs

Depending on the physical connection of an ICC, an ICC can be contact-based or contactless.

3.2.1 Contact-Based ICCs

Contact-based ICCs have a contact area, which provides electrical connection between ICC and TWN4. Please contact the manufacturer of the ICCs concerning ATRs and/or APDUs of an ICC.

TWN4 SmartCard is able to support the most of the contact-based ICCs.

3.2.2 Contactless ICCs

3.2.2.1 Micro Processor Cards

Some RFID transponder can also behave like a ICC, which is able to send APDUs natively. TWN4 supports most of them.

3.2.3 Storage Cards

A normal RFID transponder can also work like an ICC in PC/SC specification. In this case, TWN4 must translate the transponder as an ICC.

3.2.4 List of supported Contactless ICCs

ICC Class	ICC Type
Calypso	Micro processor card
EM4102	Storage card
Hitag1	Storage card
Hitag2	Storage card
HitagS	Storage card
Legic Prime	Storage card
Legic Advant	Storage card
MIFARE Classic 1K	Storage card
MIFARE Classic 4K	Storage card
MIFARE DESFire EV1	Micro processor card
MIFARE Ultralight	Storage card
SmartMX	Micro processor card

3.3 How to Select a Suitable TWN4

This section lists different ICCs which are supported by TWN4 SmartCard or by TWN4 Desktop.

For detailed information concerning supported APDUs please refer to section 6.3.

	Contact-based ICCs	Micro Processor Cards	Storage Cards
TWN4 SmartCard	$\surd$	$\surd$	$\surd$
TWN4 Desktop		$\surd$	$\surd$

4 Contact-Based Card

In general, TWN4 works with ISO 7816-3 and ISO 7816-4 conformed cards.

An Answer To Reset (ATR) is a message output by a contact card conforming to ISO/IEC 7816 standards, following electrical reset of the card's chip by a card reader. The ATR conveys information about the communication parameters proposed by the card, and the card's nature and state.

ATRs cannot be used for user identification.

The APDUs used by contact-based card are defined in ISO 7816-4. Manufacturers may also define proprietary APDUs. Please refer to the relative documents and/or the manufacturers for more information.

5 Micro Processor Cards

The information about ATR of a micro processor card can be found in PC/SC specification Part 3 Requirements for PC-Connected Interface Devices [4]. Please refer to the document for more information.

ATRs cannot be used for user identification.

In general, TWN4 SmartCard and TWN4 Desktop support ISO 14443-4 conformed cards. The following ICCs have been tested by Elatec:

- MIFARE® DESFire®[1] EV1
- Calypso® [2]
- SmartMX™[3]

Users may also use APDUs defined in PC/SC specification Part 3 [4], PC/SC specification Part 3 Supplemental Document 2 - Contactless ICCs [5] and Amendment 1: Requirements for PC-Connected Interface Devices [6] to get information of a micro processor card. Please refer to the corresponding documents for more information.

Manufacturers may also have defined proprietary APDUs. Please refer to the relative documents and/or the manufacturers for more information.

In general, one can use Get Data command to retrieve the UID of a micro processor card.

Command	CLA	INS	P1	P2	Lc	Le
Get Data	FF	CA	00	00	-	00

Response data	SW1-SW2
UID of the transponder	90 00

[1] MIFARE and MIFARE DESFire are registered trademarks of NXP B.V. and are used under license.
[2] Calypso is a registered trademark of Calypso Technology.
[3] SmartMX is a trademark of NXP Semiconductors N.V.

6 Storage Cards

The following storage cards are tested, which can be translated as an ICC by TWN4.

- MIFARE Classic 1K
- MIFARE Classic 4K
- MIFARE Ultralight
- EM4102
- Hitag1
- Hitag2
- HitagS

The information about ATR of a storage card can be found in PC/SC specification Part 3 Supplemental Document 1 - Storage Card ATR [7]. Please refer to the document for more information.

This chapter lists the ATRs and APDUs to read/write information of storage cards. If not explicitly noted, all the values are in hex format.

The following examples show only successful APDU commands. In case SW1 and SW2 are not 0x90 and 0x00, please refer to PC/SC document [4] for more information.

6.1 List of Transponders

ATRs cannot be used for user identification.

6.1.1 HF Transponders

6.1.1.1 MIFARE Classic 1K

ATR	3B 8F 80 01 80 4F 0C A0 00 00 03 06 03 00 01 00 00 00 00 6A

6.1.1.2 MIFARE Classic 4K

ATR	3B 8F 80 01 80 4F 0C A0 00 00 03 06 03 00 02 00 00 00 00 69

6.1.1.3 MIFARE Ultralight

ATR	3B 8F 80 01 80 4F 0C A0 00 00 03 06 03 00 03 00 00 00 00 68

6.1.2 LF Transponders

6.1.2.1 EM4102, Hitag

ATR	3B 8F 80 01 80 4F 0C A0 00 00 03 06 40 00 00 00 00 00 00 28

6.2 List of APDUs

The APDUs in this section are defined in Interoperability Specification for ICCs and Personal Computer Systems Part 3 [4].

6.2.1 Get Data

The Get Data command can be used to retrieve the UID of a transponder.

6.2.1.1 Command

Command	CLA	INS	P1	P2	Lc	Le
Get Data	FF	CA	00	00	-	00

6.2.1.2 Response

Response data	SW1-SW2
UID of the transponder	90 00

6.2.2 Load Keys

6.2.2.1 Command

The reader is able to store up to 16 keys in its volatile memory.

Command	CLA	INS	P1	P2	Lc	Data	Le
Load Key	FF	82	00	Key number	Key Length	Key	-

6.2.2.2 Response

SW1 and SW2 will be returned.

6.2.2.3 Example

Load key FF FF FF FF FF FF to key number 1:

Command	FF 82 00 01 06 FF FF FF FF FF FF
Answer	90 00

6.2.3 General Authenticate

6.2.3.1 Command

Command	CLA	INS	P1	P2	Lc	Data	Le
General Authenticate	FF	86	00	00	5	See table 6.1	-

Byte1	Byte2	Byte3	Byte4	Byte5
Version 01	Block Address MSB	Block Address LSB	Key type	Key Nr.

Table 6.1: General Authenticate data bytes

6.2.3.2 Response

SW1 and SW2 will be returned.

6.2.3.3 Example

Authenticate at MIFARE block 02 with key number 1, keytype A.

Command	FF 86 00 00 05 01 00 02 60 01
Answer	90 00

6.2.4 Read Binary

6.2.4.1 Command

Command	CLA	INS	P1	P2	Lc	Data	Le
Read Binary	FF	B0	00	Block Address	-	-	XX

6.2.4.2 Response

Response data	SW1-SW2
Binary Data	90 00

6.2.4.3 Example

Read block number 4

Command	FF B0 00 04 00

6.2.5 Update Binary

6.2.5.1 Command

This command always updates entire blocks, this means i.e. in case of Mifare Classic 16 bytes of payload data is required.

Command	CLA	INS	P1	P2	Lc	Data	Le
Update Binary	FF	D6	00	Block Address	XX	Data	-

6.2.5.2 Response

SW1 and SW2 will be returned.

6.2.5.3 Example

Write data block number 4

Command	FF D6 00 04 10 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF

6.3 Supported APDUs by Different Transponders

EM4102 only supports Get Data Command, since it contains only the UID.

MIFARE Ultralight has no keys saved, therefore it cannot run Load Keys and General Authenticate command.

	MIFARE Classic 1K	MIFARE Classic 4K	MIFARE Ultralight	EM4102
Get Data	√	√	√	√
Load Keys	√	√		
General Authenticate	√	√		
Read Binary	√	√	√	
Update Binary	√	√	√	

7 Legic Cards

When a Legic transponder is presented, the IFD emulates an ISO7816-4 compatible MF/DF/EF file structure. This means every accessible data segment located on the transponder is mapped as a DF (Directory File) under the MF (Master File), the respective DF ID is a 16 bit number starting from 0001. The respective segment stamp becomes the DF name, so each segment can be accessed either by its DF ID or the stamp. As a DF cannot contain any payload data, each DF has an EF (Elementary File), containing the segment data.

In order to grant access to the segment data, TWN4 provides the necessary ISO7816-4 interindustry commands.

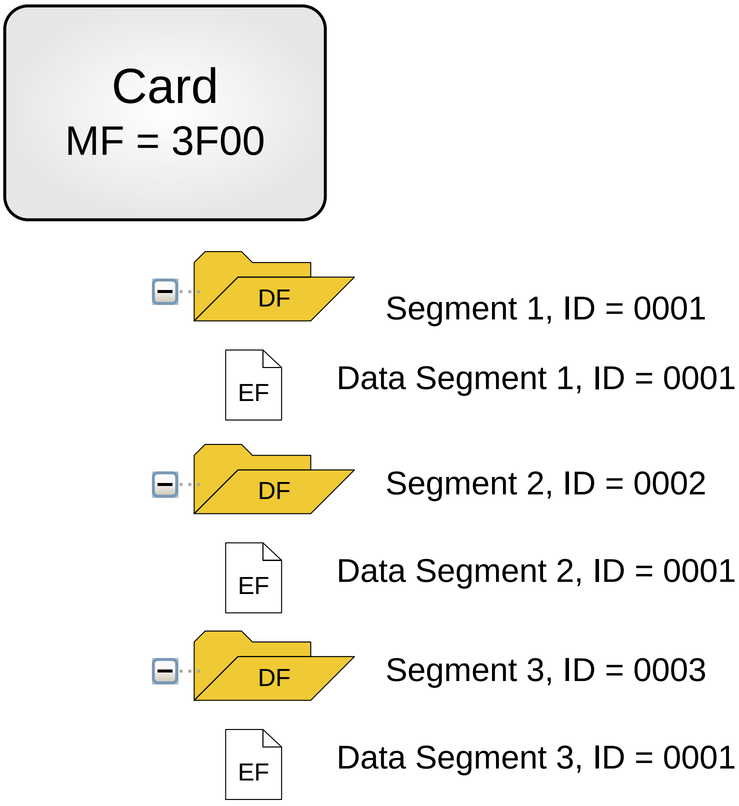


Figure 7.1: MF/DF/EF Structure

Example:

Data Segment 3 (Stamp 2700010203) can either be accessed by specifying the file IDs 3F00/0003/0001 or by specifying the DF name 3F00/2700010203/0001.

7.1 List of Transponders

The following Legic cards are tested, which can be translated as an ICC by TWN4.

- Legic Prime MIM256
- Legic Advant ATC4096

7.1.1 ATR

ATR	3B 88 80 01 45 53 43 4F 53 31 30 30 71

7.2 Command Set

7.2.1 Get Data

Use this APDU to retrieve either information about the emulated card operating system or the card UID.

7.2.1.1 Command

Command	CLA	INS	P1	P2	Lc	Le
Get Data OS	00	CA	01	See table 7.1	-	00
Get Data UID	FF	CA	00	00	-	00

P2 Value	Meaning
82	Query OS version
83	Query current lifecycle phase of current DF (0x10 is always returned, means "operational")

Table 7.1: Parameter P2

7.2.1.2 Response

Response data	SW1-SW2
Data	90 00

7.2.2 List Directory

Sending this APDU lists the content of the currently selected MF or DF.

7.2.2.1 Command

Command	CLA	INS	P1	P2	Lc	Le
List Directory	80	16	00	00	-	00

7.2.2.2 Response

Response data	SW1-SW2
TLV coded FCI	90 00

7.2.3 Select File

Use this APDU to select a MF, DF or EF for subsequent operations.

7.2.3.1 Command

Command	CLA	INS	P1	P2	Lc	Data	Le
Select File	00	A4	Selection Control See table 7.2	Selection Control See table 7.3	Empty or Length of data field		00

P1 Value	Meaning
00	Select DF or EF directly below the current DF using the file ID. If no file ID is transmitted, the MF 3F00 is selected.
04	Select a DF using its name.
08	Select DF or EF using the path starting from the MF.

Table 7.2: Parameter P1

P2 Value	Meaning
00	Send FCI data
0C	Only return SW1-SW2

Table 7.3: Parameter P2

7.2.4 Read Binary

Use this APDU to read binary data from a EF. The file must have been selected prior starting this operation. Please note that reading is limited to a maximum byte count of 200 bytes, if a larger amount is required, reading shall be done by issuing a sequence of Read Binary APDUs.

7.2.4.1 Command

Command	CLA	INS	P1	P2	Lc	Data	Le
Read Binary	00	B0	Address MSB	Address LSB	-	-	XX

7.2.4.2 Response

Response data	SW1-SW2
Binary Data	90 00

7.2.4.3 Example

Read 10 bytes starting from address 0x1234.

Command	00 B0 12 34 0A

7.2.5 Update Binary

7.2.5.1 Command

Use this APDU to write binary data to a EF. The file must have been selected prior starting this operation. Please note that writing is limited to a maximum byte count of 200 bytes, if a larger amount is required, writing shall be done by issuing a sequence of Update Binary APDUs.

Command	CLA	INS	P1	P2	Lc	Data	Le
Update Binary	FF	D6	Address MSB	Address LSB	Length of data field	Data	-

7.2.5.2 Response

SW1 and SW2 will be returned.

7.2.5.3 Example

Write 4 bytes 00 11 22 33 of binary data to address 0x1234.

Command	00 D6 12 34 04 00 11 22 33

8 Test PC/SC with TWN4 under Linux

8.1 Prepare the Hardware

In order to test PCSC under Linux with TWN4, it is necessary to program a correct Firmware/App to TWN4. Please refer to Elatec support for the latest Firmware/App image.

8.2 Prepare the Software

8.2.1 Install the Software Packages

A complete PC/SC software solution contains an ICC-aware software(e.g. opensc), an ICC resource manager(e.g. pcscd) and an IFD handler(e.g. libccid). Under Debian they can be installed by:

```
$sudo apt-get install opensc
$sudo apt-get install pcscd
```

8.2.2 Setup the Driver

In order to make pcscd work under Linux, it is necessary to know the Vendor ID (VID) and Product ID (PID) of the reader.

To find the VID/PID of the connected TWN4, one can type

```
$lsusb
```

The output of lsusb is like:

```
Bus 001 Device 003: ID 09d8:0426
```

Depending on the USB stack running on TWN4, the Product ID (PID) is different. All TWN4 readers have Vendor ID (VID) 0x09d8.

USB Stack	Vendor ID	Product ID
CCID + HID	0x09D8	0x0425
CCID + CDC	0x09D8	0x0427
CCID	0x09D8	0x0428

By adding the VID, the PID and the name of the reader to Info.plist, one can make TWN4 work under Linux. The Info.plist file is located under for instance /usr/lib/pcsc/drivers/ifd-ccid.bundle/Contents/

8.3 Restart pcscd

In order to apply the modification has been done, it is necessary to kill the old pcscd process and restart it.

```
$sudo pcscd
```

To see the debug output of pcscd, one can type:

```
$sudo pcscd -afd
```

8.4 Work with opensc

After the resource manager and the IFD handler are ready, one can call opensc to start the normal operation. Note that slot 0 is reserved for either RFID transponder or contact-based ICC, reader 0 is selected in the following examples.

8.4.1 List the Readers

```
$opensc-tool -l
```

8.4.2 Read the ATR of an ICC

```
$opensc-tool -r 0 -a
```

8.4.3 Read the UID of a Card

```
$opensc-tool -r 0 -s FF:CA:00:00:00
```

8.4.4 Send APDU to the ICC

```
$opensc-tool -r 0 -s <APDU> # the bytes should be seperated with ':'
```

9 Disclaimer

Elatec reserves the right to change any information or data in this document without prior notice. The distribution and the update of this document is not controlled. Elatec declines all responsibility for the use of product with any other specifications but the ones mentioned above. Any additional requirement for a specific custom application has to be validated by the customer himself at his own responsibility. Where application information is given, it is only advisory and does not form part of the specification.

All referenced brands, product names, service names and trademarks mentioned in this document are the property of their respective owners.

Bibliography

[1] Cards with Contacts. Part 3: Electrical interface and transmission protocols. ISO/IEC 7816-3, 2002. http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816-3.aspx.

[2] Cards with Contacts. Part 4: Interindustry Commands for Interchange. ISO/IEC 7816-4, 2005. http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816-4.aspx.

[3] Specification for Integrated Circuit(s) Cards Interface Devices. Universal Serial Bus Device Class: Smart Card CCID. April 2005. http://www.usb.org/developers/docs/devclass_docs/DWG_Smart-Card_CCID_Rev110.pdf.

[4] PC/SC Work Group. Interoperability Specification for ICCs and Personal Computer Systems, Part 3 Requirements for PC-Connected Interface Devices. June 2007. http://www.pcscworkgroup.com/specifications/files/pcsc3_v2.01.09.pdf.

[5] PC/SC Work Group. Interoperability Specification for ICCs and Personal Computer Systems, Part 3. Supplemental Document 2 - Contactless ICCs. April 2010. http://www.pcscworkgroup.com/specifications/files/pcsc3_v2.02.00_sup2.pdf.

[6] PC/SC Work Group. Interoperability Specification for ICCs and Personal Computer Systems, Part 3. Amendment 1: Requirements for PC-Connected Interface Devices. August 2011. http://www.pcscworkgroup.com/specifications/files/pcsc3_v2.01.09_amd1.pdf.

[7] PC/SC Work Group. Interoperability Specification for ICCs and Personal Computer Systems, Part 3. Supplemental Document 1 - Storage Card ATR. June 2013. http://www.pcscworkgroup.com/specifications/files/pcsc3_v2.01.09_sup.pdf.

[8] Identification Cards – Contactless Integrated Circuit Cards – Proximity Cards. Part 4: Transmission protocol. ISO/IEC 14443-4, 2008. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50648.

[9] Identification Cards – Contactless Integrated Circuit Cards – Proximity Cards. Part 3: Initialization and Anticollision. ISO/IEC 14443-3, 2011. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50942.