Smart Card Training
from Wolfgang Rankl

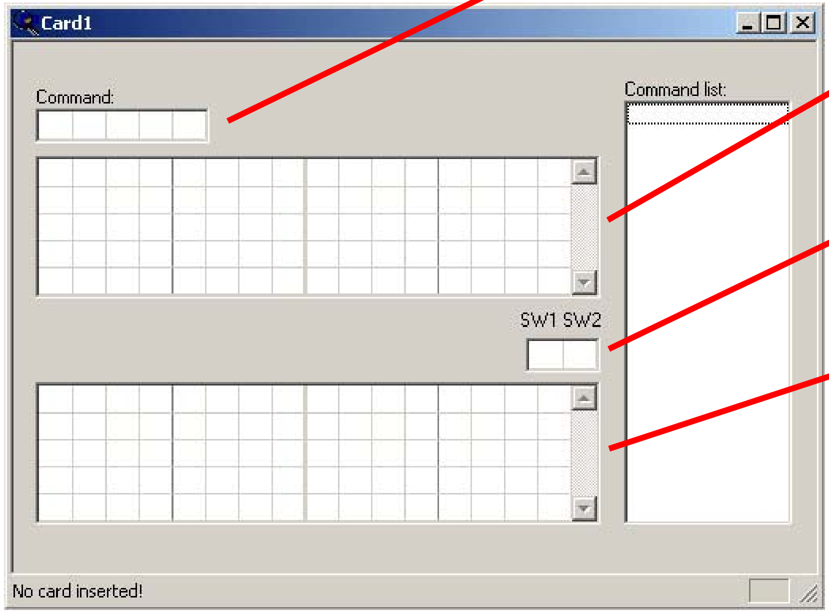
Some Basics about the SIM

Description

- These examples show some **transactions with a SIM** (subscriber identity module). The SIM is the smart card used in GSM mobile phones.
- **Overview** about the transactions: In the first step the ATR will be received after the reset of the SIM. In the next step the PIN will be verified and some DFs and EFs will be selected. In the the next steps some data will be read out from EFs with different file structures.
- The intension of this examples is to give people without tools and smart cards an **understanding about the basics of communication** and **data elements** from typical smart cards.
- For a better understanding of the examples it is recommendable to read the corresponding chapters from the **Smart Card Handbook** or **Handbuch der Chipkarten** from Wolfgang Rankl (www.wrankl.de) and Wolfgang Effing and the corresponding ETSI specification **GSM 11.11** available from www.etsi.org.

User Interface

This is a short description of the user interface of a PC based communication tool. The communication with the smart card is done with a PC tool which is able to send commands and receive responses to and from a smart card. For the following command response sequences the transport protocol T=0 is used.



This is the field for the command header with CLASS || INSTRUCTION || P1 || P2 || P3.

This is the field for the command body with DATA 1 || DATA 2 || ...

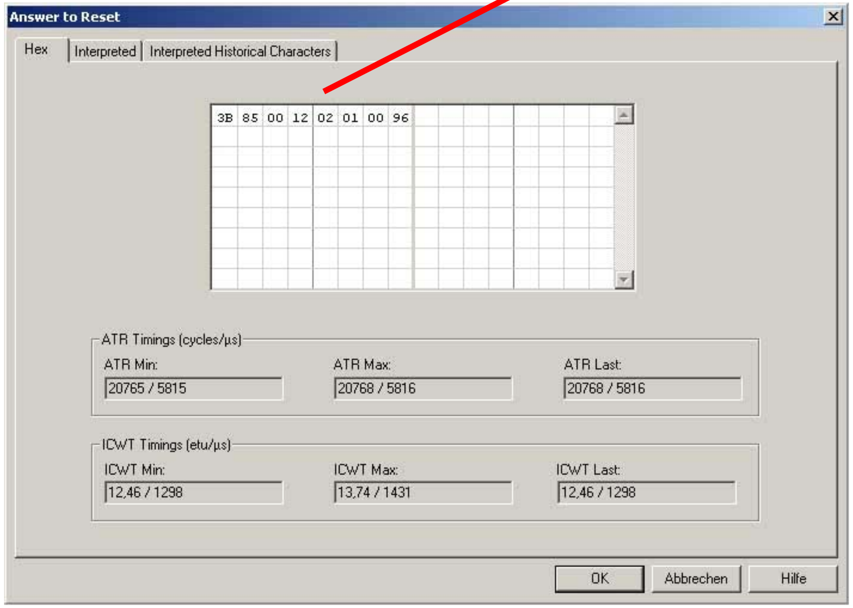
This is the field for the response returncode with SW1 || SW2.

This is the field for the response data with DATA 1 || DATA 2 || ...

ATR – hexadecimal notation

Step 1: A reset of the card is executed and the ATR will be received.

This is the ATR in hexadecimal notation



```
3B 85 00 12 02 01 00 96
```

ATR Timings (cycles/µs)

ATR Min: 20765 / 5815

ATR Max: 20768 / 5816

ATR Last: 20768 / 5816

ICWT Timings (etu/µs)

ICWT Min: 12,46 / 1298

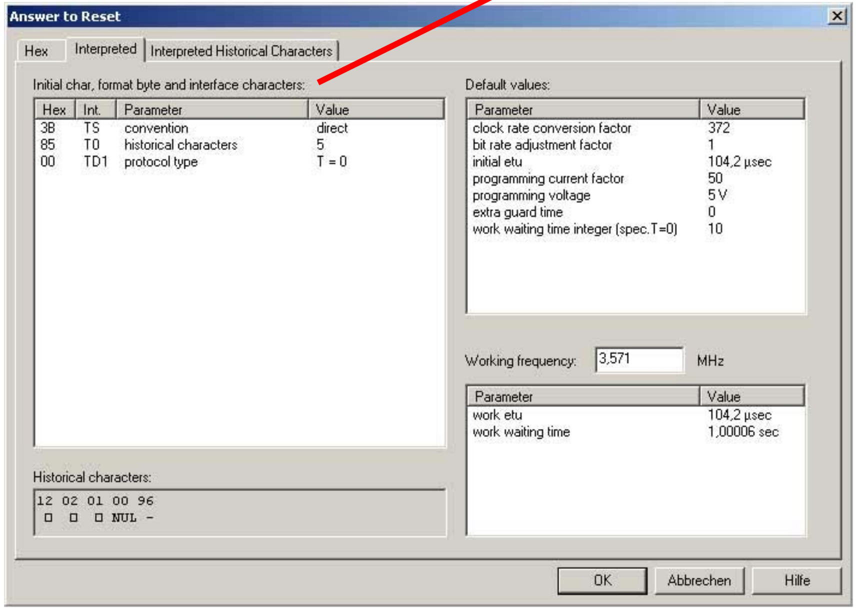
ICWT Max: 13,74 / 1431

ICWT Last: 12,46 / 1298

ATR - decoded

Step 1: A reset of the card is executed and the ATR will be received.

This is the ATR in decodet notation. It is a quite simple ATR which informs the terminal. that direct convention (‘3B‘) and T=0 is used. There are 5 historical characters.



Answer to Reset

Initial char, format byte and interface characters:

Hex	Int.	Parameter	Value
3B	TS	convention	direct
85	T0	historical characters	5
00	TD1	protocol type	T = 0

Default values:

Parameter	Value
clock rate conversion factor	372
bit rate adjustment factor	1
initial etu	104,2 µsec
programming current factor	50
programming voltage	5 V
extra guard time	0
work waiting time integer (spec.T=0)	10

Working frequency: 3,571 MHz

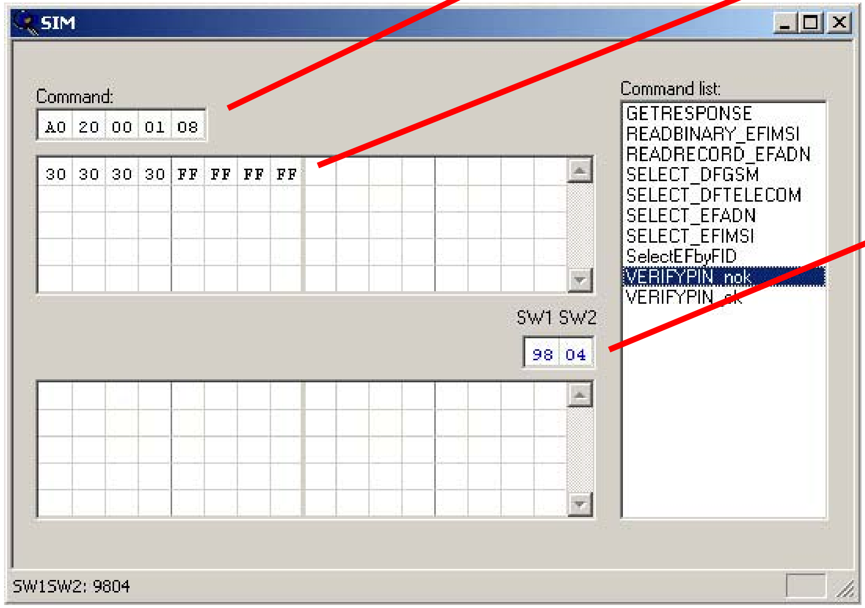
Parameter	Value
work etu	104,2 µsec
work waiting time	1,00006 sec

Historical characters:

```
12 02 01 00 96
 □  □  □ NUL -
```

VERIFY PIN – bad case

Step 2: Now the user enter a false 4 digit PIN („0000“) and the terminal send it to the SIM. The SIM verifies the PIN and send the answer back.



Command: A0 20 00 01 08

30 30 30 30 FF FF FF FF

SW1 SW2: 98 04

SW1SW2: 9804

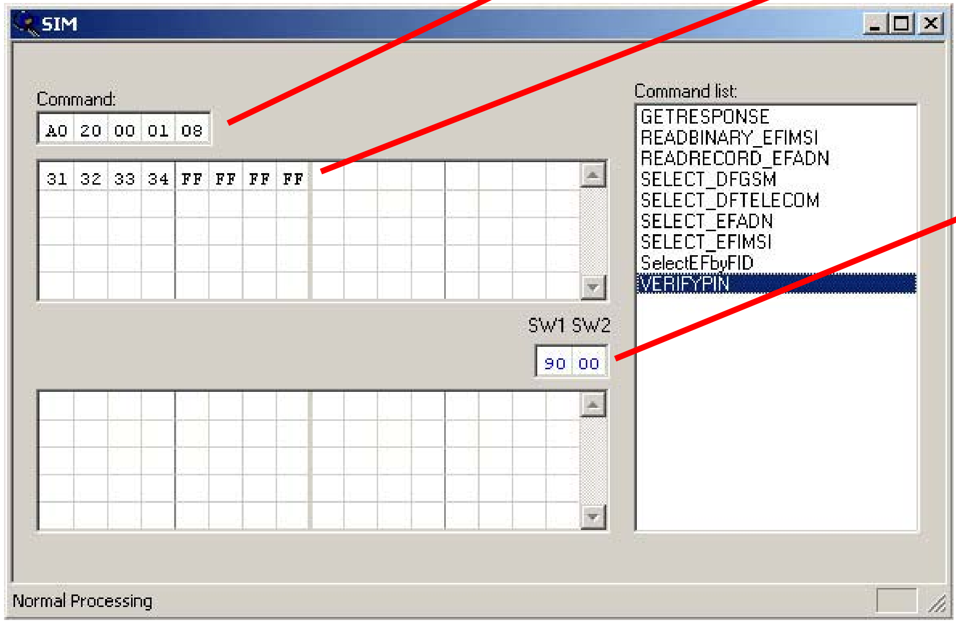
This is the VERIFY PIN command header.

This is the command body with a 4 digit false PIN „0000“. The PIN is coded in ASCII, left adjusted and filled up to 8 byte with ‘FF‘.

This is the returncode SW1 SW2 of the card. ‘9804‘ means that the PIN verification was not successful.

VERIFY PIN – good case

Step 3: Now the user enter his correct 4 digit PIN („1234“) and the terminal send it to the SIM. The SIM verifies the PIN and send the answer back.



Command: A0 20 00 01 08

Data: 31 32 33 34 FF FF FF FF

SW1 SW2: 90 00

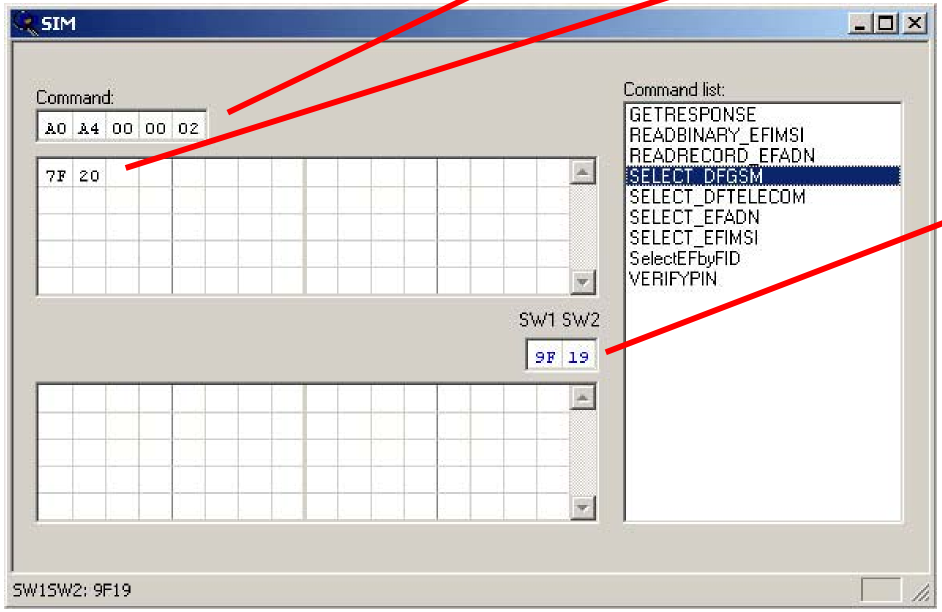
This is the VERIFY PIN command header.

This is the command body with the 4 digit PIN „1234“. The PIN is coded in ASCII, left adjusted and filled up to 8 byte with ‘FF‘.

This is the returncode SW1 SW2 of the card. ‘9000‘ means that the PIN verification was successful and the error counter of the PIN is set to zero.

SELECT DF GSM – part 1 of 2

Now the DF GSM will be selected.



Command: A0 A4 00 00 02

7F 20

SW1 SW2: 9F 19

Command list:
- GETRESPONSE
- READBINARY_EFIMSI
- READRECORD_EFADN
- SELECT_DFGSM
- SELECT_DFTELECOM
- SELECT_EFADN
- SELECT_EFIMSI
- SelectEFbyFID
- VERIFYPIN

SW1SW2: 9F19

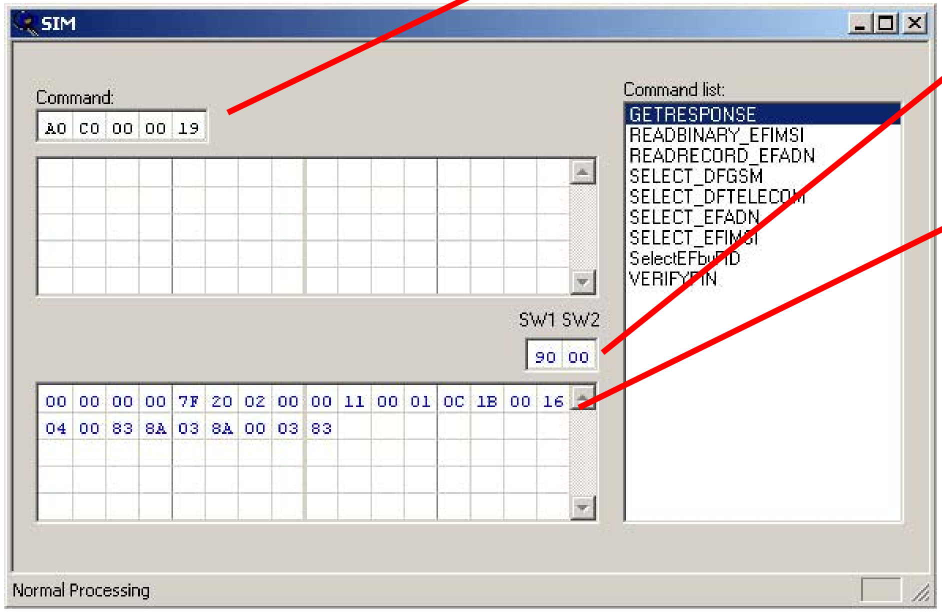
This is the SELECT command header. The body have a length of 2 byte.

This is the command body with the 2 byte FID ‘7F20‘ for the DF GSM.

This is the returncode SW1 SW2 of the card. ‘9F19‘ means SELECT command successful executed and ,’19‘ byte (= 25 byte decimal) additional information can be optional fechted by a GET RESPONSE command.

SELECT DF GSM – part 2 of 2

Step 5:The additional information about the previous selected file will be fetched by a GET RESPONSE command. GET RESPONSE is a typical command within the T=0 protocoll.



Command:

```
A0 C0 00 00 19
```

SW1 SW2

```
90 00
```

```
00 00 00 00 7F 20 02 00 00 11 00 01 0C 1B 00 16
04 00 83 8A 03 8A 00 03 83
```

Normal Processing

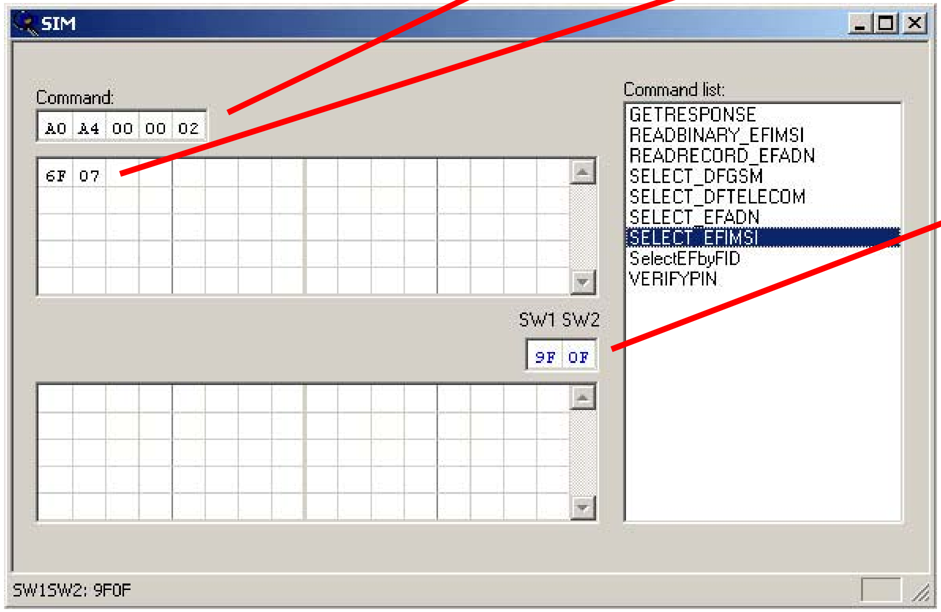
This is the GET RESPONSE command header. ’19‘ byte (= 25 byte decimal) will be fetched from the card.

This is the returncode SW1 SW2 of the card. ‘9000‘ means GET RESPONSE successful executed.

This is the response body with informations about the DF GSM.

SELECT EF IMSI – part 1 of 2

Step 6: The EF IMSI (international mobile subscriber information) will be selected.



Command:
A0 A4 00 00 02

6F 07

SW1 SW2
9F 0F

SW1SW2: 9F0F

This is the SELECT command header. The body have a length of 2 byte.

This is the command body with the 2 byte FID ‘6F07‘ for the EF IMSI.

This is the returncode SW1 SW2 of the card. ‘9F0F‘ means SELECT command successful executed and ’0F‘ byte (= 15 byte decimal) additional information can be optional fechted by a GET RESPONSE command.

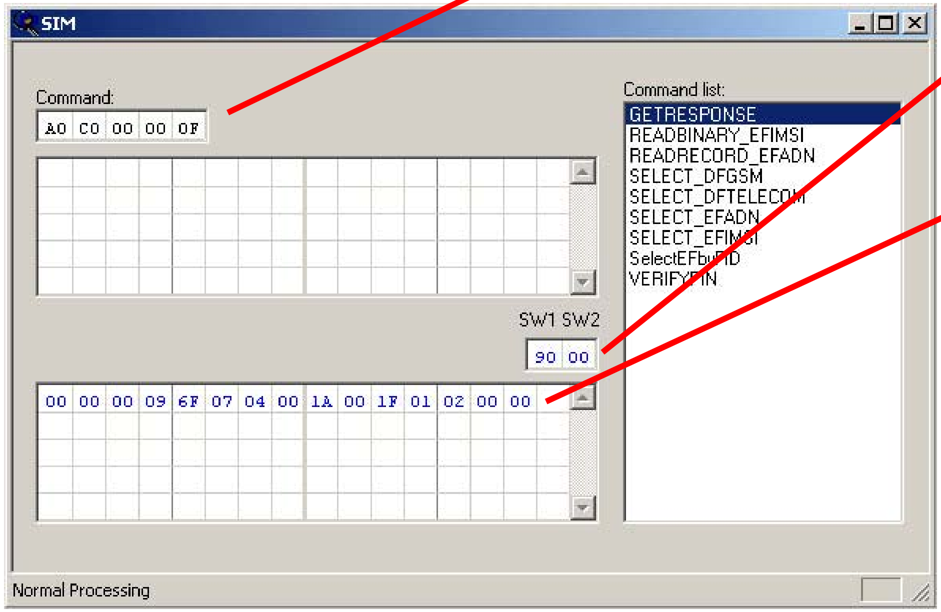
SELECT EF IMSI – part 2 of 2

Additional information about the previous selected file will be fetched by a GET RESPONSE command. GET RESPONSE is a typical command within the T=0 protocol.

This is the GET RESPONSE command header. ’0F‘ byte (= 15 byte decimal) will be fetched from the card.

This is the returncode SW1 SW2 of the card. ‘9000‘ means GET RESPONSE successful executed.

This is the response body with informations about the EF IMSI.



SIM

Command:

```
A0 C0 00 00 0F
```

SW1 SW2

```
90 00
```

```
00 00 00 09 6F 07 04 00 1A 00 1F 01 02 00 00
```

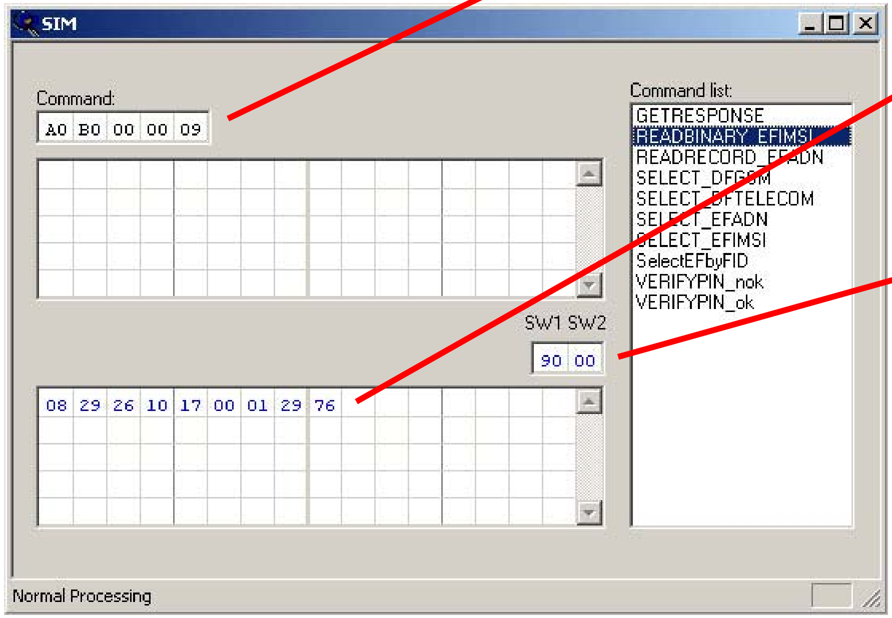
Command list:

- GETRESPONSE
- READBINARY_EFIMSI
- READRECORD_EFADN
- SELECT_DFGSM
- SELECT_DFTELECOM
- SELECT_EFADN
- SELECT_EFIMSI
- SelectEFbyFID
- VERIFYPIN

Normal Processing

READ BINARY EF IMSI

The data of the transparent structured EF IMSI (international mobile subscriber information) are read from the SIM by a READ BINARY command.



Command:

```
A0 B0 00 00 09
```

SW1 SW2

```
90 00
```

```
08 29 26 10 17 00 01 29 76
```

Command list:

- GETRESPONSE
- READBINARY_EFIMSI
- READRECORD_EFADN
- SELECT_DFGSM
- SELECT_DFTELECOM
- SELECT_EFADN
- SELECT_EFIMSI
- SelectEFbyFID
- VERIFYPIN_nok
- VERIFYPIN_ok

Normal Processing

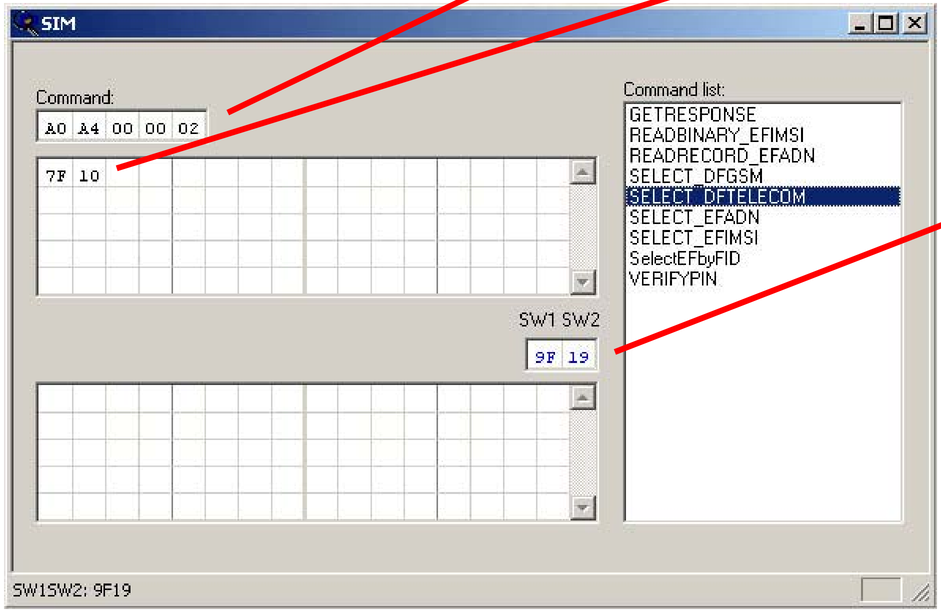
This is the READ BINARY command header. The whole (= 9 byte) transparend structured EF IMSI will be read.

This is the response body with the 9 byte file content of EF IMSI.
D1: length of the IMSI
D2 ... D9: IMSI

This is the returncode SW1 SW2 of the card. ‘9000‘ means READ BINARY successfully executed.

SELECT DF Telekom – part 1 of 2

The DF Telekom is selected and the card signalized that 25 byte file information could be fetched by a following GET RESPONSE command.



SIM

Command:

```
A0 A4 00 00 02
7F 10
```

SW1 SW2

```
9F 19
```

Command list:

- GETRESPONSE
- READBINARY_EFIMSI
- READRECORD_EFADN
- SELECT_DFGSM
- SELECT_DFTELECOM
- SELECT_EFADN
- SELECT_EFIMSI
- SelectEFbyFID
- VERIFYPIN

SW1SW2: 9F19

This is the SELECT command header. The body have a length of 2 byte.

This is the command body with the 2 byte FID ‘7F10‘ for the DF Telekom.

This is the returncode SW1 SW2 of the card. ‘9F19‘ means SELECT command successful executed and ’19‘ byte (= 25 byte decimal) additional information can be optional fechted by a GET RESPONSE command.

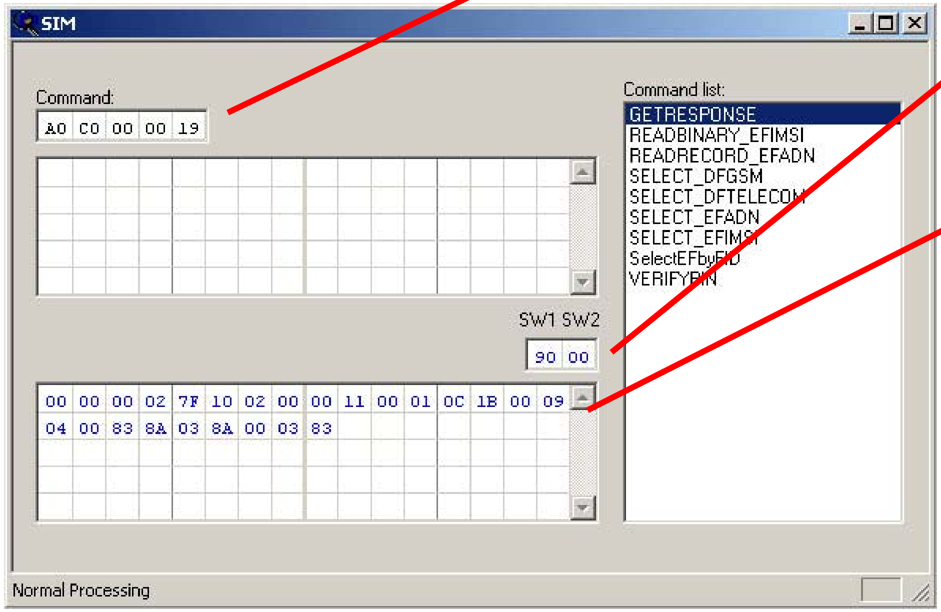
SELECT DF Telekom – part 2 of 2

Additional information about the previous selected file will be fetched by a GET RESPONSE command. GET RESPONSE is a typical command within the T=0 protocol.

This is the GET RESPONSE command header. ’19‘ byte (= 25 byte decimal) will be fetched from the card.

This is the returncode SW1 SW2 of the card. ‘9000‘ means GET RESPONSE successful executed.

This is the response body with informations about the DF GSM.



Command: A0 C0 00 00 19

SW1 SW2: 90 00

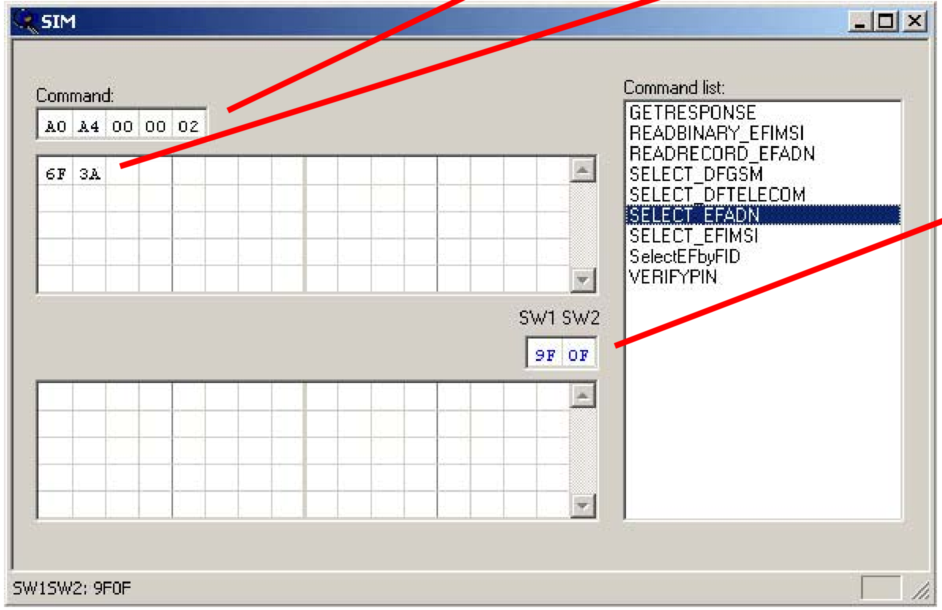
```
00 00 00 02 7F 10 02 00 00 11 00 01 0C 1B 00 09
04 00 83 8A 03 8A 00 03 83
```

Normal Processing

3. June 2004 - Version 4

SELECT EF ADN – part 1 of 2

The EF ADN (abbreviated dialing numbers) with the file structure linear fixed is selected and the card signalized that 15 byte file information could be fetched by a following GET RESPONSE command.



Command:

A0 A4 00 00 02

6F 3A

SW1 SW2

9F 0F

SW1SW2: 9F0F

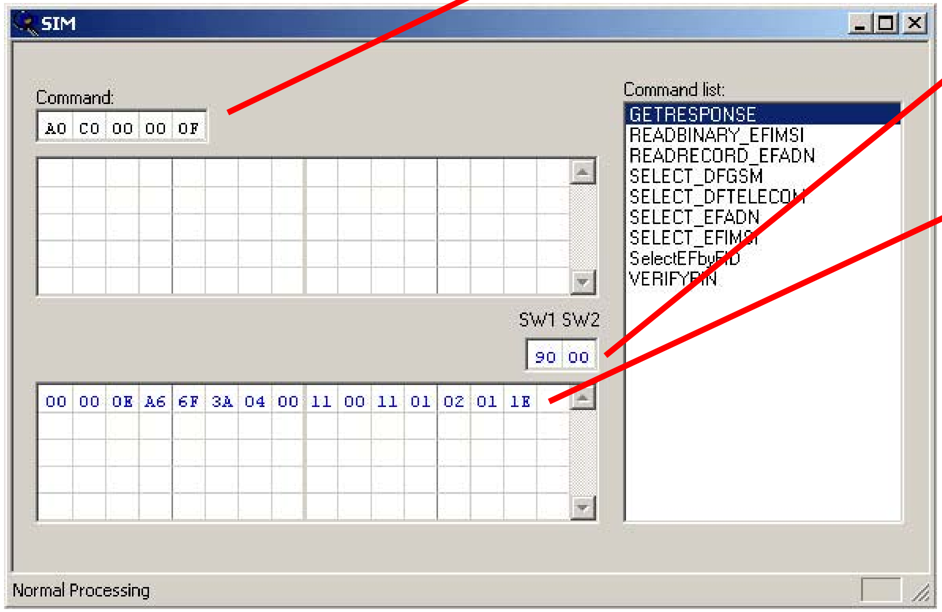
This is the SELECT command header. The body have a length of 2 byte.

This is the command body with the 2 byte FID ,'6F3A' for the EF ADN.

This is the returncode SW1 SW2 of the card. '9F0F' means SELECT command successful executed and '0F' byte (= 15 byte decimal) additional information can be optional fechted by a GET RESPONSE command.

SELECT EF ADN – part 2 of 2

Additional information about the previous selected file will be fetched by a GET RESPONSE command. GET RESPONSE is a typical command within the T=0 protocol.



Command:

```
A0 C0 00 00 0F
```

Command list:

- GETRESPONSE
- READBINARY_EFIMSI
- READRECORD_EFADN
- SELECT_DFGSM
- SELECT_DFTELECOM
- SELECT_EFADN
- SELECT_EFIMSI
- SelectEFbyFID
- VERIFYPIN

SW1 SW2

```
90 00
```

```
00 00 0E A6 6F 3A 04 00 11 00 11 01 02 01 1E
```

Normal Processing

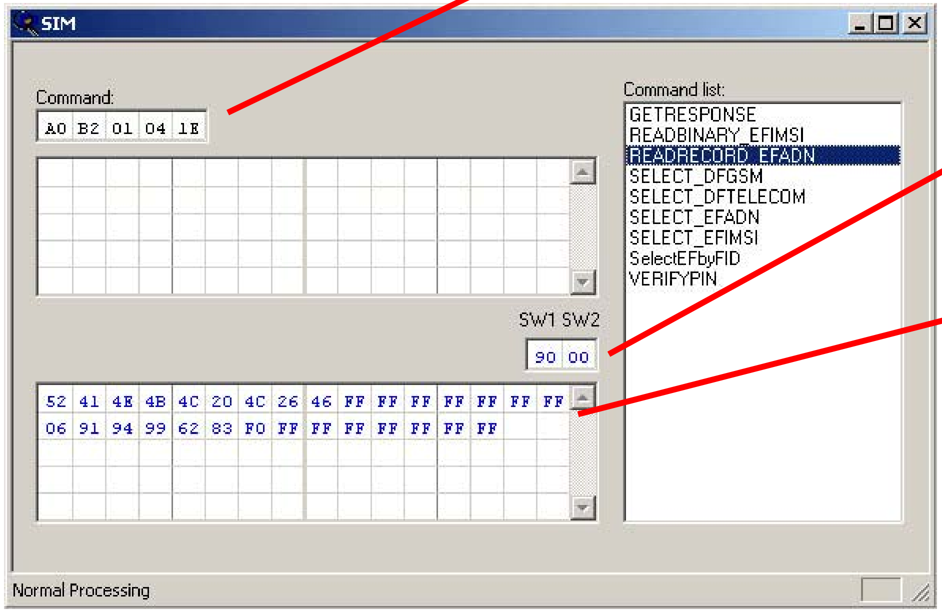
This is the GET RESPONSE command header. ’0F‘ byte (= 15 byte decimal) will be fetched from the card.

This is the returncode SW1 SW2 of the card. ‘9000‘ means GET RESPONSE successful executed.

This is the response body with informations about the EF IMSI.

READ RECORD in EF ADN

The first record of the linear fixed structured EF ADN (abbreviated dialling numbers) is read from the SIM by a READ RECORD command.



Command:

```
A0 B2 01 04 1E
```

SW1 SW2

```
90 00
```

```
52 41 4E 4B 4C 20 4C 26 46 FF FF FF FF FF FF FF
06 91 94 99 62 83 F0 FF FF FF FF FF FF FF
```

Normal Processing

This is the READ RECORD command header. The record will be addressed absolutely (P2=‘04‘). The record with the record number 1 (=P1) and the length 30 byte (=‘1E‘) will be read .

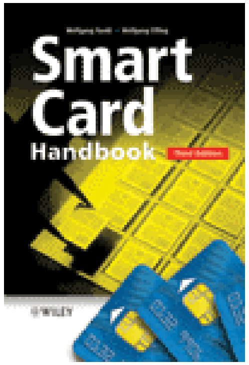
This is the returncode SW1 SW2 of the card. ‘9000‘ means READ RECORD successfully executed.

This is the command body with the content of record number 1.

End of this training

- This document can be **copied without restriction** as long as it's **content does not be changed**. It can be printed without problems in DIN A4 and US letter size.
- **Suggestions for improvements** are always welcome and can be send to the email address of Wolfgang Rankl.
- The **primary version** of this document is available on Wolfgang Rankl's Homepage "**www.WRankl.de**". This is also an additional source of informations about smart cards.
- For a better understanding of the examples it is recommendable to read the corresponding chapters from the **Smart Card Handbook** or **Handbuch der Chipkarten** from Wolfgang Rankl and Wolfgang Effing and the corresponding ETSI specification **GSM 11.11** available from www.etsi.org.
- The authors have carefully compiled the content of this document, but do not take any responsibility for the correctness. In case of doubt the respective standard or specification is to be considered.

Handbuch der Chipkarten
Wolfgang Rankl und Wolfgang Effing
4. Auflage 2002. Hanser
ISBN 3-446-22036-4



Smart Card Handbook
Wolfgang Rankl and Wolfgang Effing
3rd ed. 2003. John Wiley & Sons
ISBN 0-471-85668-8