Secure Element Processor (SEP)
Lollipop STM32 Board



1 SEP BOARDS 4

2 SERIAL COMMANDS 6

2.1 A, SEND APDU T=0 7

2.2 A, SEND APDU T=1 7

2.3 Note: JAVACARD APDU Processing 7

2.4 Starting T=0, with nopts 7

2.5 Starting T=1 8

2.6 Starting T=0, with pts=2 (TA=0x12) 8

2.7 Starting T=1 pts=2 (TA=0x12) 9

2.8 Command test, with T=0 9

2.9 Command test, with T=1 10

2.10 Testing, T=1 Case 4, no LE 12

2.11 Testing, T=1 with LE 12

2.12 Testing T=0, P3=0 13

2.13 Testing, T=1 P3=0 14

2.14 Command edump, dump EEPROM 15

2.15 Command BINARY x/X SERIAL 16

2.15.1 Request 16

2.15.2 Response 16

3 MODE I²C 16

3.1 Frame format 16

3.2 NAD 16

3.3 PCB 16

3.3.1 SN, sequence number 16

3.3.2 RESET 16

3.3.3 OFF 16

3.3.4 Retry 17

3.3.5 Send APDU with NS 17

3.3.6 Send APDU, no Sequence Number 17

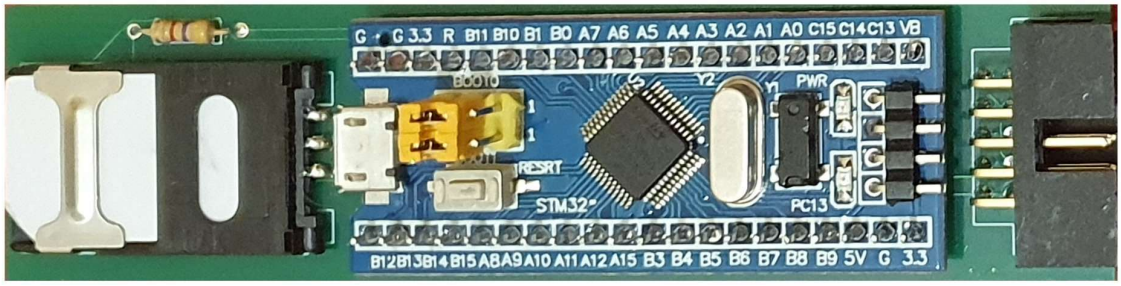
3.3.7 Echo 17

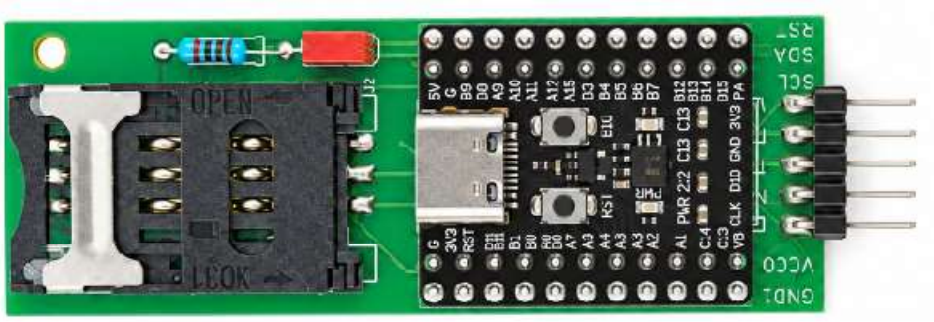
3.4 CRC 17

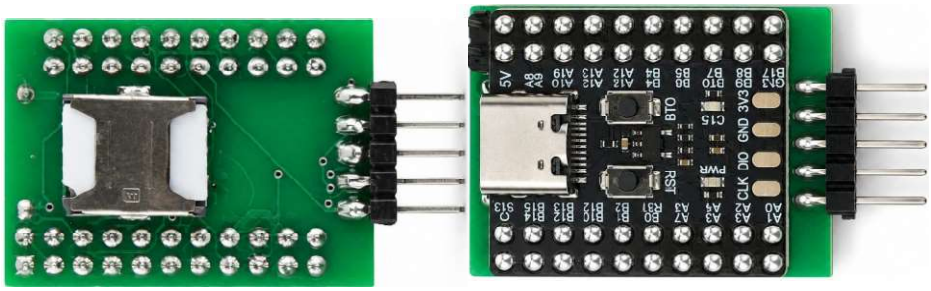
3.5 I²C protocol 17
3.5.1 Write I²C 17
3.5.2 Read I²C 18

3.6 I²C Error processing 18

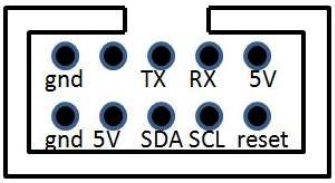
1 SEP BOARDs

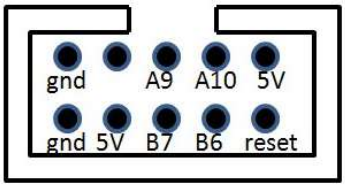


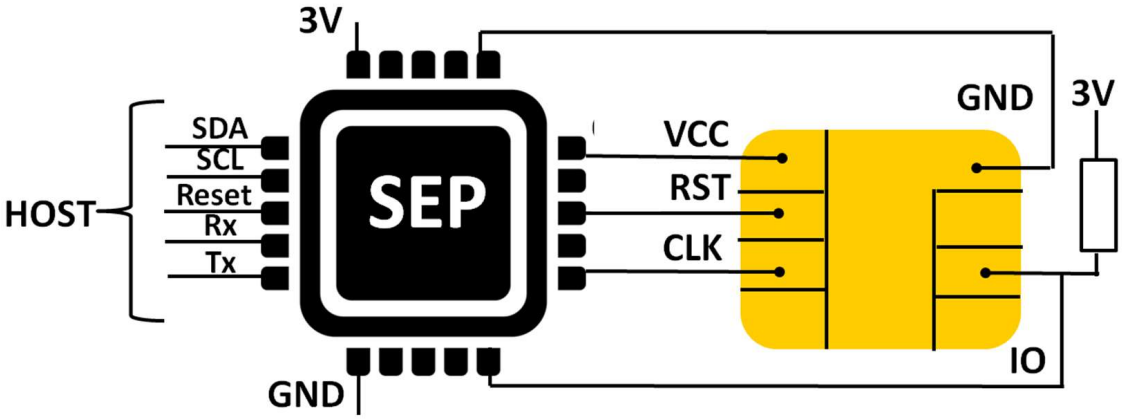




Pin B4 to GROUND + RESET => Start in SERIAL MODE 19200 bauds







	VCC	RST	CLK	IO
Blue Pill STM32	C14	C15	A6	B5
Mini Blue Pill STM32	B19	B11	A6	B5

2 SERIAL COMMANDS

Command	Parameter	Response
Empty		Ready
Wrong command	Anything	ERROR
test	N time	Select PIN Clear Curve Genkey N x Sign
eclear		Clear configuration
eread		Read & Set configuration
ewrite		Write configuration
edump		Dump configuration (debug mode)
local		Serial mode ASCII command only
nolocal		Serial mode Binary+ASCII command
eserial	Optional mode (1,2,3)	COM mode 1=I2C 2=SERIAL 3=BOTH
delay	Optional delay ms	Delay (ms)
adr	Optional address (decimal)	I2C address (1…127)
baud	Optional baudrate (decimal)	Baudrate 19200…115200 (9600*n)
nodebug		No Debug
debug		Debug
F	Optional frequency decimal (Hz)	Frequency: 1000 to 12000 Hz, divisor of 72000
ifs	Optional value (decimal)	IFS value, maximum254
ta	Optional TA byte value (hexa)	TA byte, hexadecimal value (11,12)
pts	Optional pts value (decimal)	TA= 0x10 + pts, return pts=TA-0x10 in decimal Set PTS mode
nopts		Cancel PTS mode
t0		Set protocol to T=0
t1		Set protocol to T=1
ptcol		Return protocol, 0 or 1
on	Optional TA value (decimal)	Cold Start with pts if TA present
w	Optional TA value (decimal)	Warm Start with PTS if TA present
off		Power off smartcard
A	Hexadecimal string	Send APDU
S	Hexadecimal string	Send APDU (5 bytes), LE=0, 256 bytes expected
hist		Return historical bytes (hexadecimal)

2.1 A, SEND APDU T=0

T= 0, A APDU

Case1**:** CLA INS P1 P2 00, return SW1 W2
Case2**:** CLA INS P1 P2 LE (LE#0), return LE-bytes SW1 SW2
Case 3: CLA INS P1 P2 LC [LC-bytes], return SW1,SW2
Case 4: CLA INS P1 P2 LC [LC-bytes] LE, return LE-bytes SW1 SW2, if present LE bytes is ignored

T=0, S APDU (obsolete)
Case 2: CLA INS P1 P2 00 [LE=256], return up 256 bytes plus SW1 SW2

2.2 A, SEND APDU T=1

T=1, A APDU

Case1: CLA INS P1 P2 (or CLA INS P1 P2 00), return SW1 SW2
Case2: CLA INS P1 P2 LE, return LE-bytes SW1 SW2
Case3: CLA INS P1 P2 LC [LC-bytes], return SW1,SW2
Case 4: CLA INS P1 P2 LC [LC-bytes] LE (or CLA INS P1 P2 LC LC-bytes), return LE-bytes SW1 SW2

2.3 Note: JAVACARD APDU Processing

For javacard API APDU processing

- A null byte is always append for Case1
- If present the LE bytes is removed for Case4

2.4 Starting T=0, with nopts

```
nopts
OK
t0
OK
on
T0 {T0 }
TA1= 95
Fi=9 Di=5
SC Frequency = 6000 KHz
TCK = 0
00|3B 98 95 00 6B 65 79 31 2E 63 6F 6D             ';...key1.com....'
F= 372 D= 1
etu =62
102240us
OK
```

2.5 Starting T=1

```
t1
OK
On
T0 {T0 }
TA1= 95
Fi=9 Di=5
SC Frequency = 6000 KHz
TCK = 0
00|FF 11 11 FF                                          '................'
00|FF 11 11 FF                                          '................'
PTS OK
00|3B 94 95 00 46 54 56 01                              ';...FTV........'
F= 372 D= 1
etu =62
TxT1: 5
00C101FE3E
RxT1: 5
00E101FE1E
200686us
OK
```

2.6 Starting T=0, with pts=2 (TA=0x12)

```
off
OK
t0
OK
pts 2
OK
ta
12
on

T0 {T0 }
TA1= 95
Fi=9 Di=5
SC Frequency = 6000 KHz
TCK = 0
00|FF 10 12 FD                                          '................'
00|FF 10 12 FD                                          '................'
PTS OK
00|3B 98 95 00 6B 65 79 31 2E 63 6F 6D                  ';...key1.com....'
F= 372 D= 2
etu =31
180385us
OK
```

2.7 Starting T=1 pts=2 (TA=0x12)

```
off
OK
t1
OK
pts 2
OK
ta
12
on

T0 {T0 }
TA1= 95
Fi=9 Di=5
SC Frequency = 6000 KHz
TCK = 0
00|FF 11 12 FC                                          '................'
00|FF 11 12 FC                                          '................'
PTS OK
00|3B 98 95 00 6B 65 79 31 2E 63 6F 6D                  ';...key1.com....'
F= 372 D= 2
etu =31
TxT1: 5
00C101FE3E
RxT1: 5
00E101FE1E
202986us
OK
```

2.8 Command test, with T=0

```
test 1

Tx: 00A4040006010203040500
APDU Error = 0
A49000
Rx[30ms]:
9000

Tx: 00200001083030303030303030
APDU Error = 0
209000
Rx[23ms]:
9000

Tx: 0081000000
APDU Error = 0
9000
Rx[65ms]:
9000

Tx: 0089000000
APDU Error = 0
9000
Rx[173ms]:
9000
```

```
Tx: 0082000000
APDU Error = 0
9000
Rx[215ms]:
9000

Tx: 008000002012345678900ABCDEF123456
    7890ABCDEF1234567890ABCDEF123456
    7890ABCDEF
APDU Error = 0
806148
Rx[71ms]:
6148

Tx: 00C0000048
APDU Error = 0
C09000
Rx[30ms]:
    004630440220399BD6492871D1CBF50F
    0E4FB19E08DEF9B2BC77C252141A94A3
    029289B1DFE90220139140705BFDA020
    8C6339405B4E1EC81D546604FAD11235
    8E72087951FDF287
    9000

004630440220399BD6492871D1CBF50F0E4FB19E08DEF9B2BC77C252141A94A3029289B1DFE
90220139140705BFDA0208C6339405B4E1EC81D546604FAD112358E72087951FDF2879000
```

2.9 Command test, with T=1

```
test 1

Tx: 00A4040006010203040500
TxT1: 4
00000BAC
RxT1: 6
000002900092
APDU Error = 0
Rx[41ms]:
9000

Tx: 00200001083030303030303030
TxT1: 4
00400D64
RxT1: 6
0040029000D2
APDU Error = 0
Rx[44ms]:
9000

Tx: 0081000000
TxT1: 4
00000584
RxT1: 6
000002900092
APDU Error = 0
Rx[84ms]:
9000
```

```
Tx: 0089000000
TxT1: 4
004005CC
RxT1: 6
0040029000D2
APDU Error = 0
Rx[192ms]:
9000

Tx: 0082000000
TxT1: 4
00000587
RxT1: 6
000002900092
APDU Error = 0
Rx[235ms]:
9000

Tx: 008000002012345678 90ABCDEF123456
    7890ABCDEF1234567890ABCDEF123456
    7890ABCDEF
TxT1: 4
004025C5
RxT1: 80
00404C00483046022100D305516DB17F5786B17571FCE8B72584553D28786A6D
17BF49D65E5D4C629A3802210086072B4886EFF8EF8A41EB3770A9A13250FD6F
5AD5C60140B5799AB11CEA82D8900027
APDU Error = 0
Rx[213ms]:
    00483046022100D305516DB17F5786B1
    7571FCE8B72584553D28786A6D17BF49
    D65E5D4C629A3802210086072B4886EF
    F8EF8A41EB3770A9A13250FD6F5AD5C6
    0140B5799AB11CEA82D8
    9000

00483046022100D305516DB17F5786B17571FCE8B72584553D28786A6D17BF49D65E5D4C629
A3802210086072B4886EFF8EF8A41EB3770A9A13250FD6F5AD5C60140B5799AB11CEA82D890
00
```

2.10 Testing, T=1 Case 4, no LE

```
t=1 Case 4, no LE

A 008000002012345678900ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF
Tx: 008000002012345678900ABCDEF123456
    7890ABCDEF1234567890ABCDEF123456
    7890ABCDEF
TxT1: 4
00002585
RxT1: 78
00004A0046304402204A2C3FF63CE69FCA1326A1C689E772B6CDEDFDCD6920FB
9E4EF5D164CC41F0E5022046B29E145929F3ABD876FF8A19A38340A08D456F24
D2522BBAE697FFB6960A549000AC
APDU Error = 0
Rx[210ms]:
    0046304402204A2C3FF63CE69FCA1326
    A1C689E772B6CDEDFDCD6920FB9E4EF5
    D164CC41F0E5022046B29E145929F3AB
    D876FF8A19A38340A08D456F24D2522B
    BAE697FFB6960A54
    9000

0046304402204A2C3FF63CE69FCA1326A1C689E772B6CDEDFDCD6920FB9E4EF5D164CC41F0E
5022046B29E145929F3ABD876FF8A19A38340A08D456F24D2522BBAE697FFB6960A549000
```

2.11 Testing, T=1 with LE

```
T=1, Case 4 with LE

A 008000002012345678900ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF00
Tx: 008000002012345678900ABCDEF123456
    7890ABCDEF1234567890ABCDEF123456
    7890ABCDEF00
TxT1: 4
004026C6
RxT1: 78
00404A00463044022001979087C67D857F2AEF830133EAE710E969CB014FE2CB
F09E9D42537DC4FAC90220522676F7611020358D72FF29CA8457A95BBA40C63D
12620B007E9F2637CE91D6900015
APDU Error = 0
Rx[210ms]:
    00463044022001979087C67D857F2AEF
    830133EAE710E969CB014FE2CBF09E9D
    42537DC4FAC90220522676F761102035
    8D72FF29CA8457A95BBA40C63D12620B
    007E9F2637CE91D6
    9000

00463044022001979087C67D857F2AEF830133EAE710E969CB014FE2CBF09E9D42537DC4FAC
90220522676F7611020358D72FF29CA8457A95BBA40C63D12620B007E9F2637CE91D69000
```

2.12 Testing T=0, P3=0

```
A 00B0000000
Tx: 00B0000000
APDU Error = 0
B09000
Rx[101ms]:
    00000000000000000000000000000000
    00000000000000000000000000000000
    00000000000000000000000000000000
    00000000000000000000000000000000
    00000000000000000000000000000000
    00000000000000000000000000000000
    00000000000000000000000000000000
    00000000000000000000000000000000
    00000000000000000000000000000000
    00000000000000000000000000000000
    00000000000000000000000000000000
    00000000000000000000000000000000
    00000000000000000000000000000000
    00000000000000000000000000000000
    00000000000000000000000000000000
    9000

000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000009000
```

2.13 Testing, T=1 P3=0

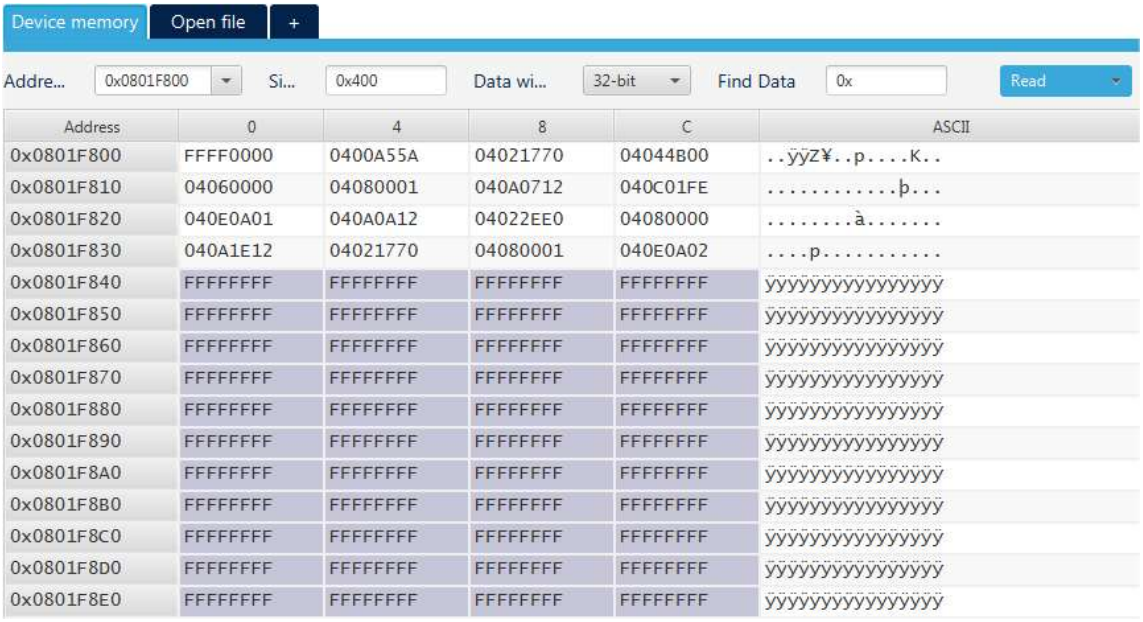
```
A 00B0000000
Tx: 00B0000000
TxT1: 4
004005F5
RxT1: 258
0060FE0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
009E
453ms
RxT1: 8
0000040000900094
APDU Error = 0
Rx[471ms]:
9000

0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000009000
```

2.14 Command edump, dump EEPROM

edump

EEPROM: : 16
5AA57017004B00000100121EFE01020A
F= 6000
PTS= true
T= 0
TA= 0x12
SE_ADR= 30
IFS= 254
SERIAL (1:I2C 2:SERIAL 3:BOTH)= 2
BAUDRATE= 19200
LOCAL= true
LoopDelay= 10



Address	0	4	8	C	ASCII
0x0801F800	FFFF0000	0400A55A	04021770	04044B00	..ÿÿZ¥..p....K..
0x0801F810	04060000	04080001	040A0712	040C01FE	............þ...
0x0801F820	040E0A01	040A0A12	04022EE0	04080000	........à.......
0x0801F830	040A1E12	04021770	04080001	040E0A02	....p...........
0x0801F840	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x0801F850	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x0801F860	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x0801F870	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x0801F880	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x0801F890	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x0801F8A0	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x0801F8B0	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x0801F8C0	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x0801F8D0	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0x0801F8E0	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ

2.15 Command BINARY x/X SERIAL

2.15.1 Request

X/x LENmsb LENlsb [LEN-Bytes]
x => A command
X =>S command (case 2, T=0, obsolete)

2.15.2 Response

X/x LENmsb LENlsb [LEN bytes)
Error: FF 00 00

3 Mode I²C

3.1 Frame format

NAD PCB LEN payload CRC(2 bytes)
LEN is the payload length, LEN=0 for empty payload

3.2 NAD

NAD= 5A for request
NAD= A5 for response

3.3 PCB

3.3.1 SN, sequence number

PCB= 0x00/0x40: for SN (0/1)
ERROR SN: A5 81 00

3.3.2 RESET

PCB =CF =>reset board
Response:
A5 CF LEN HISTORICAL-BYTES CRC
ERROR   A5 82 00 CRC

3.3.3 OFF

PCB=C3, power-off Secure Element
Response:
A5 C3 00 CRC

3.3.4 Retry

PCB=83, request to re-send again (error CRC)

3.3.5 Send APDU with NS

PCB=0x00/0x40, 5A 0x40/0x00 LEN [request] CRC

Response:
A5 0x40/0x00 LEN [response] CRC
ERROR: A5 82 00 CRC

3.3.6 Send APDU, no Sequence Number

PCB=C1/C2 5A C1/C2 LEN [request] CRC
PCB= C1=>A command,
PCB=C2 =>S command (obsolete)

Response:
A5 C1/C2 LEN [response] CRC
Error: A5 82 00 CRC

3.3.7 Echo

PCB=C0, A5 C0 LEN PAYLOAD CRC

Response:
A5 C0 LEN PAYLOAD CRC
Error PCB: A5 81 00

3.4 CRC

CRC is ISO/IEC 3309

3.5 I²C protocol

3.5.1 Write I²C

Write one byte (NAD)
Write one byte (PCB)
Write one byte (LEN)
Write 32 bytes: PAYLOAD + CRC is segmented in 32 bytes records

3.5.2 Read I²C

I2C read & no data 1 byte 00 is returned
00= nodata

I2C read 1 byte (NAD))
I2C read 1 byte (PCB)
I2C read 1 byte (LEN)

I2C read 32 bytes: PAYLOAD + CRC is segmented in 32 bytes records

3.6 I²C Error processing

