

SCP03 Authentication Issue Descriptive

MW: SE Plug and Trust – 03.03.00 – latest version in NXP website

Host: Embedded Linux environment, running in a BeagleBone Black with OpenSSL Engine to work with SE050.

MW Compilation Configuration: My C-Make configuration is attached to a file “cmake_options.txt”.

HW Configuration: The communication is established through T=1 Protocol over I2C.

Environment: I have built the “libsss_engine.so” and linked it to OpenSSL Engine following the Plug and Trust Manual, by modifying “openssl.cnf” to work with SSS Library.

Tests:

1 – Firstly, I tested OpenSSL Engine without SCP03 Authentication and it worked.

It was configured as following:

-DSCP=None

-DSE05X_Auth=None

And the result is shown below:

Running: Get Info

```
root@am335x-evm:~# ./se05x_GetInfo
```

```
App :INFO :PlugAndTrust_v03.03.00_20210528
```

```
App :INFO :Running ./se05x_GetInfo
```

```
App :INFO :If you want to over-ride the selection, use ENV=EX_SSS_BOOT_SSS_PORT or pass in command line arguments.
```

```
smCom :DEBUG:phPalEse_i2c_open_and_configure Opening port
```

```
smCom :DEBUG:I2CInit: opening /dev/i2c-2
```

```
smCom :DEBUG:I2C driver: PEC flag cleared
```

```
smCom :DEBUG:I2C driver supports plain i2c-level commands.
```

```
smCom :DEBUG:I2C driver Initialized :: fd = [12]
```

smCom :DEBUG:phNxpEseProto7816_Open: First open completed

smCom :DEBUG:phNxpEse_clearReadBuffer Enter ..

smCom :DEBUG:phPalEse_i2c_read Read Requested 260 bytes

smCom :DEBUG:Done with rv = 0d

smCom :DEBUG:TX (axI2CRead): (Len=260)

F7 20 01 00 70 99 37 49 00 00 00 00 54 E8 D3 BE
F4 E7 D3 BE FC E7 D3 BE B3 76 35 49 FC E7 D3 BE
D0 9A 37 49 04 00 00 00 78 FE F1 B6 01 00 00 00
00 00 00 00 01 00 00 00 70 99 37 49 00 00 00 00
2C 9B 37 49 2C 9B 37 49 00 00 00 00 01 80 AD FB
00 E9 D3 BE 00 E9 D3 BE 00 E9 D3 BE 00 E9 D3 BE
FF FF FF FF FE E9 D3 BE 40 A3 38 49 20 F8 F1 B6
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 05 00 00 00 01 00 00 00 00 71 05 00
10 D0 F1 B6 D0 D4 F1 B6 00 00 00 00 01 00 00 00
00 90 37 49 00 00 00 00 DF B0 35 49 78 FE F1 B6
01 00 00 00 01 00 00 00 00 00 00 00 10 D0 F1 B6
40 A3 38 49 E8 E8 D3 BE 00 70 05 00 90 E8 D3 BE
57 4C 3F 49 88 13 00 00 E8 03 00 00 40 42 0F 00
39 46 41 49 00 00 00 00 40 4B 4C 00 00 70 05 00
22 EB D3 BE 00 00 00 00 B3 95 03 00 A4 E8 D3 BE
05 00 00 00

smCom :DEBUG:_i2c_read() error : 13

smCom :DEBUG:TransceiveProcess nextTransceiveState 4

smCom :DEBUG:S-Frame PCB: c0

smCom :DEBUG:phNxpEse_WriteFrame Enter ..

smCom :DEBUG:TX (axI2CWrite) > (Len=5)

5A C0 00 FF FC

smCom :DEBUG:Done with rv = 0c

smCom :DEBUG:RAW Tx> (Len=5)

5A C0 00 FF FC

```
smCom :DEBUG:phNxpEse_read Enter ..
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
    A5 E0
smCom :DEBUG:phNxpEse_readPacket Read HDR
smCom :DEBUG:phNxpEse_readPacket SOF FOUND
smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=1)
    00
smCom :DEBUG:poll_sof_chained_delay value is 0
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
    3F 19
smCom :DEBUG:RAW Rx< (Len=5)
    A5 E0 00 3F  19
smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x5bc88 len ----> 0x5
smCom :DEBUG:Received CRC:0x3f19 Calculated CRC:0x3f19
smCom :DEBUG:Retry Counter = 0
smCom :DEBUG:phNxpEseProto7816_DecodeFrame S-Frame Received
smCom :DEBUG:TransceiveProcess nextTransceiveState 7
smCom :DEBUG:S-Frame PCB: c7
smCom :DEBUG:phNxpEse_WriteFrame Enter ..
smCom :DEBUG:TX (axI2CWrite) > (Len=5)
    5A C7 00 F7  B1
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:RAW Tx> (Len=5)
    5A C7 00 F7  B1
smCom :DEBUG:phNxpEse_read Enter ..
```

```
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
    A5 E7
smCom :DEBUG:phNxpEse_readPacket Read HDR
smCom :DEBUG:phNxpEse_readPacket SOF FOUND
smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=1)
    23
smCom :DEBUG:poll_sof_chained_delay value is 0
smCom :DEBUG:phPalEse_i2c_read Read Requested 37 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=37)
    00 A0 00 00  03 96 04 03  E8 00 FE 02  0B 03 E8 08
    01 00 00 00  00 64 00 00  0A 4A 43 4F  50 34 20 41
    54 50 4F 2A  8D
smCom :DEBUG:RAW Rx< (Len=40)
    A5 E7 23 00  A0 00 00 03  96 04 03 E8  00 FE 02 0B
    03 E8 08 01  00 00 00 00  64 00 00 0A  4A 43 4F 50
    34 20 41 54  50 4F 2A 8D
smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x5bc88 len ----> 0x28
smCom :DEBUG:Received CRC:0x2a8d Calculated CRC:0x2a8d
smCom :DEBUG:Retry Counter = 0
smCom :DEBUG:phNxpEseProto7816_DecodeFrame S-Frame Received
smCom :DEBUG:phNxpEseProto7816_DecodeSFrameData frameoffset=3 value=0x0
smCom :DEBUG:Data[0]=0x0 len=35 Data[34]=0x50 Data[79]=0x23
sss :INFO :atr (Len=35)
    00 A0 00 00  03 96 04 03  E8 00 FE 02  0B 03 E8 08
    01 00 00 00  00 64 00 00  0A 4A 43 4F  50 34 20 41
    54 50 4F
```

```
smCom :DEBUG:Trying to Acquire Lock thread: -1225666544
smCom :DEBUG:LOCK Acquired by thread: -1225666544
smCom :DEBUG:APDU Tx> (Len=22)
    00 A4 04 00 10 A0 00 00 03 96 54 53 00 00 00 01
    03 30 00 00 00 00
smCom :DEBUG:Enter phNxpEseProto7816_Transceive
smCom :DEBUG:Transceive data ptr 0x0xbed3eb7c len:22
smCom :DEBUG:I-Frame Data Len: 22 Seq. no:0
smCom :DEBUG:TransceiveProcess nextTransceiveState 1
smCom :DEBUG:phNxpEse_WriteFrame Enter ..
smCom :DEBUG:TX (axI2CWrite) > (Len=27)
    5A 00 16 00 A4 04 00 10 A0 00 00 03 96 54 53 00
    00 00 01 03 30 00 00 00 00 79 1C
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:RAW Tx> (Len=27)
    5A 00 16 00 A4 04 00 10 A0 00 00 03 96 54 53 00
    00 00 01 03 30 00 00 00 00 79 1C
smCom :DEBUG:phNxpEse_read Enter ..
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
    00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
    A5 00
smCom :DEBUG:phNxpEse_readPacket Read HDR
smCom :DEBUG:phNxpEse_readPacket SOF FOUND
```

smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=1)
02
smCom :DEBUG:poll_sof_chained_delay value is 0
smCom :DEBUG:phPalEse_i2c_read Read Requested 4 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=4)
6E 00 1A 49
smCom :DEBUG:RAW Rx< (Len=7)
A5 00 02 6E 00 1A 49
smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x5bc88 len ----> 0x7
smCom :DEBUG:Received CRC:0x1a49 Calculated CRC:0x1a49
smCom :DEBUG:Retry Counter = 0
smCom :DEBUG:phNxpEseProto7816_DecodeFrame I-Frame Received
smCom :DEBUG:phNxpEseProto7816_DecodeFrame I-Frame lastRcvdIframeInfo.seqNo:0x0
smCom :DEBUG:Data[0]=0x6e len=2 Data[1]=0x6e Data[0]=0x2
smCom :DEBUG: phNxpEse_Transceive Exit status 0x0
smCom :DEBUG:APDU Rx< (Len=2)
6E 00
smCom :DEBUG:Trying to Released Lock by thread: -1225666544
smCom :DEBUG:LOCK Released by thread: -1225666544
App :WARN :No SemsLite Applet Available.
hostLib:DEBUG:CloseSession command is sent only if valid Session exists!!!
smCom :DEBUG:TransceiveProcess nextTransceiveState 6
smCom :DEBUG:S-Frame PCB: c5
smCom :DEBUG:phNxpEse_WriteFrame Enter ..
smCom :DEBUG:TX (axI2CWrite) > (Len=5)
5A C5 00 47 82
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:RAW Tx> (Len=5)

5A C5 00 47 82

smCom :DEBUG:phNxpEse_read Enter ..

smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes

smCom :DEBUG:Done with rv = 0c

smCom :DEBUG:TX (axI2CRead): (Len=2)

A5 E5

smCom :DEBUG:phNxpEse_readPacket Read HDR

smCom :DEBUG:phNxpEse_readPacket SOF FOUND

smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes

smCom :DEBUG:Done with rv = 0c

smCom :DEBUG:TX (axI2CRead): (Len=1)

00

smCom :DEBUG:poll_sof_chained_delay value is 0

smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes

smCom :DEBUG:Done with rv = 0c

smCom :DEBUG:TX (axI2CRead): (Len=2)

87 67

smCom :DEBUG:RAW Rx< (Len=5)

A5 E5 00 87 67

smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x5bc88 len ----> 0x5

smCom :DEBUG:Received CRC:0x8767 Calculated CRC:0x8767

smCom :DEBUG:Retry Counter = 0

smCom :DEBUG:phNxpEseProto7816_DecodeFrame S-Frame Received

smCom :DEBUG:Close i2c device 3.

smCom :DEBUG:phNxpEse_close - ESE Context deinit completed

App :INFO :Running ./se05x_GetInfo

App :INFO :If you want to over-ride the selection, use ENV=EX_SSS_BOOT_SSS_PORT or pass in command line arguments.

smCom :DEBUG:phPalEse_i2c_open_and_configure Opening port

smCom :DEBUG:I2CInit: opening /dev/i2c-2

smCom :DEBUG:I2C driver: PEC flag cleared

smCom :DEBUG:I2C driver supports plain i2c-level commands.

smCom :DEBUG:I2C driver Initialized :: fd = [12]

smCom :DEBUG:phNxpEseProto7816_Open: First open completed

smCom :DEBUG:phNxpEse_clearReadBuffer Enter ..

smCom :DEBUG:phPalEse_i2c_read Read Requested 260 bytes

smCom :DEBUG:Done with rv = 0d

smCom :DEBUG:TX (axI2CRead): (Len=260)

```
70 45 73 65 50 72 6F 74 6F 37 38 31 36 5F 4F 70
65 6E 3A 20 46 69 72 73 74 20 6F 70 65 6E 20 63
6F 6D 70 6C 65 74 65 64 00 E8 D3 BE 00 00 00 00
F0 52 04 00 E4 E9 D3 BE 58 E8 D3 BE 00 00 00 00
9B E1 3C 49 00 00 00 00 FF FF FF FF 01 80 AD FB
D0 E8 D3 BE D0 E8 D3 BE D0 E8 D3 BE D0 E8 D3 BE
F4 E8 D3 BE CE E9 D3 BE D0 E8 D3 BE CE E9 D3 BE
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 05 00 00 00 00 00 00 00 49 03 3D 49
00 00 47 49 00 00 00 00 98 04 00 00 90 81 05 00
C1 F9 3C 49 40 E8 D3 BE FF FF FF FF 00 00 00 00
00 00 00 00 A8 E8 D3 BE FF FF FF FF 10 D0 F1 B6
00 55 00 00 B8 E8 D3 BE 75 2F 41 49 60 E8 D3 BE
57 4C 3F 49 88 13 00 00 E8 03 00 00 40 42 0F 00
39 46 41 49 00 00 00 00 40 4B 4C 00 00 70 05 00
F2 EA D3 BE 00 00 00 00 B3 95 03 00 74 E8 D3 BE
05 00 00 00
```

smCom :DEBUG:_i2c_read() error : 13

smCom :DEBUG:TransceiveProcess nextTransceiveState 4

smCom :DEBUG:S-Frame PCB: c0


```
smCom :DEBUG:phNxpEse_WriteFrame Enter ..
smCom :DEBUG:TX (axI2CWrite) > (Len=5)
    5A C0 00 FF  FC
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:RAW Tx> (Len=5)
    5A C0 00 FF  FC
smCom :DEBUG:phNxpEse_read Enter ..
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
    A5 E0
smCom :DEBUG:phNxpEse_readPacket Read HDR
smCom :DEBUG:phNxpEse_readPacket SOF FOUND
smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=1)
    00
smCom :DEBUG:poll_sof_chained_delay value is 0
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
    3F 19
smCom :DEBUG:RAW Rx< (Len=5)
    A5 E0 00 3F  19
smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x5bc88 len ----> 0x5
smCom :DEBUG:Received CRC:0x3f19 Calculated CRC:0x3f19
smCom :DEBUG:Retry Counter = 0
smCom :DEBUG:phNxpEseProto7816_DecodeFrame S-Frame Received
smCom :DEBUG:TransceiveProcess nextTransceiveState 7
smCom :DEBUG:S-Frame PCB: c7
smCom :DEBUG:phNxpEse_WriteFrame Enter ..
```

```
smCom :DEBUG:TX (axI2CWrite) > (Len=5)
    5A C7 00 F7 B1
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:RAW Tx> (Len=5)
    5A C7 00 F7 B1
smCom :DEBUG:phNxpEse_read Enter ..
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
    A5 E7
smCom :DEBUG:phNxpEse_readPacket Read HDR
smCom :DEBUG:phNxpEse_readPacket SOF FOUND
smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=1)
    23
smCom :DEBUG:poll_sof_chained_delay value is 0
smCom :DEBUG:phPalEse_i2c_read Read Requested 37 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=37)
    00 A0 00 00 03 96 04 03 E8 00 FE 02 0B 03 E8 08
    01 00 00 00 00 64 00 00 0A 4A 43 4F 50 34 20 41
    54 50 4F 2A 8D
smCom :DEBUG:RAW Rx< (Len=40)
    A5 E7 23 00 A0 00 00 03 96 04 03 E8 00 FE 02 0B
    03 E8 08 01 00 00 00 00 64 00 00 0A 4A 43 4F 50
    34 20 41 54 50 4F 2A 8D
smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x5bc88 len ----> 0x28
smCom :DEBUG:Received CRC:0x2a8d Calculated CRC:0x2a8d
smCom :DEBUG:Retry Counter = 0
smCom :DEBUG:phNxpEseProto7816_DecodeFrame S-Frame Received
```

smCom :DEBUG:phNxpEseProto7816_DecodeSFrameData frameoffset=3 value=0x0

smCom :DEBUG:Data[0]=0x0 len=35 Data[34]=0x50 Data[79]=0x23

smCom :DEBUG:Trying to Acquire Lock thread: -1225666544

smCom :DEBUG:LOCK Acquired by thread: -1225666544

smCom :DEBUG:APDU Tx> (Len=22)

00 A4 04 00 10 A0 00 00 03 96 54 53 00 00 00 01

03 00 00 00 00 00

smCom :DEBUG:Enter phNxpEseProto7816_Transceive

smCom :DEBUG:Transceive data ptr 0x0xbed3e3e8 len:22

smCom :DEBUG:I-Frame Data Len: 22 Seq. no:0

smCom :DEBUG:TransceiveProcess nextTransceiveState 1

smCom :DEBUG:phNxpEse_WriteFrame Enter ..

smCom :DEBUG:TX (axI2CWrite) > (Len=27)

5A 00 16 00 A4 04 00 10 A0 00 00 03 96 54 53 00

00 00 01 03 00 00 00 00 00 A8 C8

smCom :DEBUG:Done with rv = 0c

smCom :DEBUG:RAW Tx> (Len=27)

5A 00 16 00 A4 04 00 10 A0 00 00 03 96 54 53 00

00 00 01 03 00 00 00 00 00 A8 C8

smCom :DEBUG:phNxpEse_read Enter ..

smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes

smCom :DEBUG:Done with rv = 0d

smCom :DEBUG:TX (axI2CRead): (Len=2)

00 00

smCom :DEBUG:_i2c_read() error : 13

smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF

smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms

smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes

smCom :DEBUG:Done with rv = 0d

smCom :DEBUG:TX (axI2CRead): (Len=2)

00 00

```
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
    A5 00
smCom :DEBUG:phNxpEse_readPacket Read HDR
smCom :DEBUG:phNxpEse_readPacket SOF FOUND
smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=1)
    09
smCom :DEBUG:poll_sof_chained_delay value is 0
smCom :DEBUG:phPalEse_i2c_read Read Requested 11 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=11)
    03 06 00 61 D2 01 0B 90 00 50 AD
smCom :DEBUG:RAW Rx< (Len=14)
    A5 00 09 03 06 00 61 D2 01 0B 90 00 50 AD
smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x5bc88 len ----> 0xe
smCom :DEBUG:Received CRC:0x50ad Calculated CRC:0x50ad
smCom :DEBUG:Retry Counter = 0
smCom :DEBUG:phNxpEseProto7816_DecodeFrame I-Frame Received
smCom :DEBUG:phNxpEseProto7816_DecodeFrame I-Frame lastRcvdIframeInfo.seqNo:0x0
smCom :DEBUG:Data[0]=0x3 len=9 Data[8]=0x90 Data[0]=0x9
smCom :DEBUG: phNxpEse_Transceive Exit status 0x0
smCom :DEBUG:APDU Rx< (Len=9)
    03 06 00 61 D2 01 0B 90 00
smCom :DEBUG:Trying to Released Lock by thread: -1225666544
smCom :DEBUG:LOCK Released by thread: -1225666544
```

```
sss :INFO :atr (Len=35)
    00 A0 00 00 03 96 04 03 E8 00 FE 02 0B 03 E8 08
    01 00 00 00 00 64 00 00 0A 4A 43 4F 50 34 20 41
    54 50 4F
sss :INFO :Newer version of Applet Found
sss :INFO :Compiled for 0x30100. Got newer 0x30600
sss :WARN :Communication channel is Plain.
sss :WARN :!!!Not recommended for production use.!!!
smCom :DEBUG:Trying to Acquire Lock thread: -1225666544
smCom :DEBUG:LOCK Acquired by thread: -1225666544
smCom :DEBUG:APDU Tx> (Len=11)
    80 04 00 27 06 41 04 7F FF 02 06
smCom :DEBUG:Enter phNxpEseProto7816_Transceive
smCom :DEBUG:Transceive data ptr 0x0xbed3dc4c len:11
smCom :DEBUG:I-Frame Data Len: 11 Seq. no:1
smCom :DEBUG:TransceiveProcess nextTransceiveState 1
smCom :DEBUG:phNxpEse_WriteFrame Enter ..
smCom :DEBUG:TX (axI2CWrite) > (Len=16)
    5A 40 0B 80 04 00 27 06 41 04 7F FF 02 06 A1 C3
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:RAW Tx> (Len=16)
    5A 40 0B 80 04 00 27 06 41 04 7F FF 02 06 A1 C3
smCom :DEBUG:phNxpEse_read Enter ..
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
    00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
```

smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
A5 40
smCom :DEBUG:phNxpEse_readPacket Read HDR
smCom :DEBUG:phNxpEse_readPacket SOF FOUND
smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=1)
02
smCom :DEBUG:poll_sof_chained_delay value is 0
smCom :DEBUG:phPalEse_i2c_read Read Requested 4 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=4)
69 85 00 C1
smCom :DEBUG:RAW Rx< (Len=7)
A5 40 02 69 85 00 C1
smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x5bc88 len ----> 0x7
smCom :DEBUG:Received CRC:0xc1 Calculated CRC:0xc1
smCom :DEBUG:Retry Counter = 0
smCom :DEBUG:phNxpEseProto7816_DecomposeFrame I-Frame Received
smCom :DEBUG:phNxpEseProto7816_DecomposeFrame I-Frame lastRcvdIframeInfo.seqNo:0x1
smCom :DEBUG:Data[0]=0x69 len=2 Data[1]=0x69 Data[133]=0x2
smCom :DEBUG: phNxpEse_Transceive Exit status 0x0
smCom :DEBUG:APDU Rx< (Len=2)
69 85
smCom :DEBUG:Trying to Released Lock by thread: -1225666544
smCom :DEBUG:LOCK Released by thread: -1225666544
sss :WARN :nxEnsure:'ret == SM_OK' failed. At Line:6291 Function:sss_se05x_TXn
App :ERROR:Failed Se05x_API_CheckObjectExists
App :INFO :Error in lot_Applet_Identify
smCom :DEBUG:Trying to Acquire Lock thread: -1225666544

```
smCom :DEBUG:LOCK Acquired by thread: -1225666544
smCom :DEBUG:APDU Tx> (Len=5)
    00 A4 04 00  00
smCom :DEBUG:Enter phNxpEseProto7816_Transceive
smCom :DEBUG:Transceive data ptr 0x0xbed3e608 len:5
smCom :DEBUG:I-Frame Data Len: 5 Seq. no:0
smCom :DEBUG:TransceiveProcess nextTransceiveState 1
smCom :DEBUG:phNxpEse_WriteFrame Enter ..
smCom :DEBUG:TX (axI2CWrite) > (Len=10)
    5A 00 05 00  A4 04 00 00  1E 3C
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:RAW Tx> (Len=10)
    5A 00 05 00  A4 04 00 00  1E 3C
smCom :DEBUG:phNxpEse_read Enter ..
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
    00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
    00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
```

A5 00

smCom :DEBUG:phNxpEse_readPacket Read HDR

smCom :DEBUG:phNxpEse_readPacket SOF FOUND

smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes

smCom :DEBUG:Done with rv = 0c

smCom :DEBUG:TX (axI2CRead): (Len=1)

14

smCom :DEBUG:poll_sof_chained_delay value is 0

smCom :DEBUG:phPalEse_i2c_read Read Requested 22 bytes

smCom :DEBUG:Done with rv = 0c

smCom :DEBUG:TX (axI2CRead): (Len=22)

6F 10 84 08 A0 00 00 01 51 00 00 00 A5 04 9F 65

01 FF 90 00 95 F6

smCom :DEBUG:RAW Rx< (Len=25)

A5 00 14 6F 10 84 08 A0 00 00 01 51 00 00 00 A5

04 9F 65 01 FF 90 00 95 F6

smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x5bc88 len ----> 0x19

smCom :DEBUG:Received CRC:0x95f6 Calculated CRC:0x95f6

smCom :DEBUG:Retry Counter = 0

smCom :DEBUG:phNxpEseProto7816_DecompileFrame I-Frame Received

smCom :DEBUG:phNxpEseProto7816_DecompileFrame I-Frame lastRcvdIframeInfo.seqNo:0x0

smCom :DEBUG:Data[0]=0x6f len=20 Data[19]=0x90 Data[0]=0x14

smCom :DEBUG: phNxpEse_Transceive Exit status 0x0

smCom :DEBUG:APDU Rx< (Len=20)

6F 10 84 08 A0 00 00 01 51 00 00 00 A5 04 9F 65

01 FF 90 00

smCom :DEBUG:Trying to Released Lock by thread: -1225666544

smCom :DEBUG:LOCK Released by thread: -1225666544

smCom :DEBUG:Trying to Acquire Lock thread: -1225666544

smCom :DEBUG:LOCK Acquired by thread: -1225666544

smCom :DEBUG:APDU Tx> (Len=8)


```
80 CA 00 FE 02 DF 28 00
smCom :DEBUG:Enter phNxpEseProto7816_Transceive
smCom :DEBUG:Transceive data ptr 0x0xbed3eb84 len:8
smCom :DEBUG:I-Frame Data Len: 8 Seq. no:1
smCom :DEBUG:TransceiveProcess nextTransceiveState 1
smCom :DEBUG:phNxpEse_WriteFrame Enter ..
smCom :DEBUG:TX (axI2CWrite) > (Len=13)
5A 40 08 80 CA 00 FE 02 DF 28 00 50 06
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:RAW Tx> (Len=13)
5A 40 08 80 CA 00 FE 02 DF 28 00 50 06
smCom :DEBUG:phNxpEse_read Enter ..
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
A5 40
smCom :DEBUG:phNxpEse_readPacket Read HDR
```

```
smCom :DEBUG:phNxpEse_readPacket SOF FOUND
smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=1)
    49
smCom :DEBUG:poll_sof_chained_delay value is 0
smCom :DEBUG:phPalEse_i2c_read Read Requested 75 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=75)
    FE 45 DF 28  42 01 0C 00  01 A7 7E B8  DD 1E EE 56
    49 10 76 02  08 00 00 00  00 00 00 00  01 03 18 4A
    33 52 33 35  31 30 32 36  34 35 37 31  31 30 30 03
    4D 67 74 0B  E1 42 19 05  01 01 07 01  00 08 08 2E
    5A D8 84 09  C9 BA DB 90  00 57 64
smCom :DEBUG:RAW Rx< (Len=78)
    A5 40 49 FE  45 DF 28 42  01 0C 00 01  A7 7E B8 DD
    1E EE 56 49  10 76 02 08  00 00 00 00  00 00 00 01
    03 18 4A 33  52 33 35 31  30 32 36 34  35 37 31 31
    30 30 03 4D  67 74 0B E1  42 19 05 01  01 07 01 00
    08 08 2E 5A  D8 84 09 C9  BA DB 90 00  57 64
smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x5bc88 len ----> 0x4e
smCom :DEBUG:Received CRC:0x5764 Calculated CRC:0x5764
smCom :DEBUG:Retry Counter = 0
smCom :DEBUG:phNxpEseProto7816_Decompile I-Frame Received
smCom :DEBUG:phNxpEseProto7816_Decompile I-Frame lastRcvdIframeInfo.seqNo:0x1
smCom :DEBUG:Data[0]=0xfe len=73 Data[72]=0x90 Data[0]=0x49
smCom :DEBUG: phNxpEse_Transceive Exit status 0x0
smCom :DEBUG:APDU Rx< (Len=73)
    FE 45 DF 28  42 01 0C 00  01 A7 7E B8  DD 1E EE 56
    49 10 76 02  08 00 00 00  00 00 00 00  01 03 18 4A
    33 52 33 35  31 30 32 36  34 35 37 31  31 30 30 03
```

4D 67 74 0B E1 42 19 05 01 01 07 01 00 08 08 2E

5A D8 84 09 C9 BA DB 90 00

smCom :DEBUG:Trying to Released Lock by thread: -1225666544

smCom :DEBUG:LOCK Released by thread: -1225666544

App :WARN :#####

App :INFO :Tag value - proprietary data 0xFE = 0xFE

App :INFO :Length of following data 0x45 = 0x45

App :INFO :Tag card identification data (Len=2)

DF 28

App :INFO :Length of card identification data = 0x42

App :INFO :Tag configuration ID (Must be 0x01) = 0x01

App :DEBUG:Length configuration ID 0x0C = 0x0C

App :INFO :Configuration ID (Len=12)

00 01 A7 7E B8 DD 1E EE 56 49 10 76

App :INFO :OEF ID (Len=2)

A7 7E

App :INFO :Tag patch ID (Must be 0x02) = 0x02

App :DEBUG:Length patch ID 0x08 = 0x08

App :INFO :Patch ID (Len=8)

00 00 00 00 00 00 00 01

App :INFO :Tag platform build ID1 (Must be 0x03) = 0x03

App :DEBUG:Length platform build ID 0x18 = 0x18

App :INFO :Platform build ID (Len=24)

4A 33 52 33 35 31 30 32 36 34 35 37 31 31 30 30

03 4D 67 74 0B E1 42 19

App :INFO :JCOP Platform ID = J3R3510264571100

App :INFO :Tag FIPS mode (Must be 0x05) = 0x05

App :DEBUG:Length FIPS mode 0x01 = 0x01

App :INFO :FIPS mode var = 0x01

App :INFO :Tag pre-perso state (Must be 0x07) = 0x07

App :DEBUG:Length pre-perso state 0x01 = 0x01

```
App :INFO :Bit mask of pre-perso state var = 0x00
App :INFO :Tag ROM ID (Must be 0x08) = 0x08
App :DEBUG:Length ROM ID 0x08 = 0x08
App :INFO :ROM ID (Len=8)
    2E 5A D8 84 09 C9 BA DB
App :INFO :Status Word (SW) (Len=2)
    90 00
App :INFO :se05x_GetInfoPlainApplet Example Success !!!...
smCom :DEBUG:Trying to Acquire Lock thread: -1225666544
smCom :DEBUG:LOCK Acquired by thread: -1225666544
smCom :DEBUG:APDU Tx> (Len=5)
    80 CA 9F 7F 00
smCom :DEBUG:Enter phNxpEseProto7816_Transceive
smCom :DEBUG:Transceive data ptr 0x0xbed3eb98 len:5
smCom :DEBUG:I-Frame Data Len: 5 Seq. no:0
smCom :DEBUG:TransceiveProcess nextTransceiveState 1
smCom :DEBUG:phNxpEse_WriteFrame Enter ..
smCom :DEBUG:TX (axI2CWrite) > (Len=10)
    5A 00 05 80 CA 9F 7F 00 3E 52
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:RAW Tx> (Len=10)
    5A 00 05 80 CA 9F 7F 00 3E 52
smCom :DEBUG:phNxpEse_read Enter ..
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
    00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
```

```
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
    00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
    A5 00
smCom :DEBUG:phNxpEse_readPacket Read HDR
smCom :DEBUG:phNxpEse_readPacket SOF FOUND
smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=1)
    2F
smCom :DEBUG:poll_sof_chained_delay value is 0
smCom :DEBUG:phPalEse_i2c_read Read Requested 49 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=49)
    9F 7F 2A 47  90 D3 21 47  00 00 00 00  00 12 10 00
    00 49 95 55  95 00 00 00  00 00 00 00  00 01 39 04
    30 30 30 34  39 00 00 00  00 00 00 00  00 90 00 91
    9F
smCom :DEBUG:RAW Rx< (Len=52)
    A5 00 2F 9F  7F 2A 47 90  D3 21 47 00  00 00 00 00
    12 10 00 00  49 95 55 95  00 00 00 00  00 00 00 00
    01 39 04 30  30 30 34 39  00 00 00 00  00 00 00 00
    90 00 91 9F
smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x5bc88 len ----> 0x34
smCom :DEBUG:Received CRC:0x919f Calculated CRC:0x919f
```

smCom :DEBUG:Retry Counter = 0
smCom :DEBUG:phNxpEseProto7816_DecodeFrame I-Frame Received
smCom :DEBUG:phNxpEseProto7816_DecodeFrame I-Frame lastRcvdIframeInfo.seqNo:0x0
smCom :DEBUG:Data[0]=0x9f len=47 Data[46]=0x90 Data[0]=0x2f
smCom :DEBUG: phNxpEse_Transceive Exit status 0x0
smCom :DEBUG:APDU Rx< (Len=47)
 9F 7F 2A 47 90 D3 21 47 00 00 00 00 00 12 10 00
 00 49 95 55 95 00 00 00 00 00 00 00 00 01 39 04
 30 30 30 34 39 00 00 00 00 00 00 00 00 90 00
smCom :DEBUG:Trying to Released Lock by thread: -1225666544
smCom :DEBUG:LOCK Released by thread: -1225666544
App :WARN :#####
App :INFO :cplc_data.IC_fabricator (Len=2)
 47 90
App :INFO :cplc_data.IC_type1 (Len=2)
 D3 21
App :INFO :cplc_data.Operating_system_identifier (Len=2)
 47 00
App :INFO :cplc_data.Operating_system_release_date (Len=2)
 00 00
App :INFO :cplc_data.Operating_system_release_level (Len=2)
 00 00
App :INFO :cplc_data.IC_fabrication_date (Len=2)
 12 10
App :INFO :cplc_data.IC_Serial_number (Len=4)
 00 00 49 95
App :INFO :cplc_data.IC_Batch_identifier (Len=2)
 55 95
App :INFO :cplc_data.IC_module_fabricator (Len=2)
 00 00
App :INFO :cplc_data.IC_module_packaging_date (Len=2)

00 00
App :INFO :cplc_data.ICC_manufacturer (Len=2)
00 00
App :INFO :cplc_data.IC_embedding_date (Len=2)
00 00
App :INFO :cplc_data.IC_OS_initializer (Len=2)
01 39
App :INFO :cplc_data.IC_OS_initialization_date (Len=2)
04 30
App :INFO :cplc_data.IC_OS_initialization_equipment (Len=4)
30 30 34 39
App :INFO :cplc_data.IC_personalizer (Len=2)
00 00
App :INFO :cplc_data.IC_personalization_date (Len=2)
00 00
App :INFO :cplc_data.IC_personalization_equipment_ID (Len=4)
00 00 00 00
App :INFO :cplc_data.SW (Len=2)
90 00
App :INFO :ex_sss Finished
hostLib:DEBUG:CloseSession command is sent only if valid Session exists!!!
smCom :DEBUG:TransceiveProcess nextTransceiveState 6
smCom :DEBUG:S-Frame PCB: c5
smCom :DEBUG:phNxpEse_WriteFrame Enter ..
smCom :DEBUG:TX (axI2CWrite) > (Len=5)
5A C5 00 47 82
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:RAW Tx> (Len=5)
5A C5 00 47 82
smCom :DEBUG:phNxpEse_read Enter ..
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes

```
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
    A5 E5
smCom :DEBUG:phNxpEse_readPacket Read HDR
smCom :DEBUG:phNxpEse_readPacket SOF FOUND
smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=1)
    00
smCom :DEBUG:poll_sof_chained_delay value is 0
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
    87 67
smCom :DEBUG:RAW Rx< (Len=5)
    A5 E5 00 87 67
smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x5bc88 len ----> 0x5
smCom :DEBUG:Received CRC:0x8767 Calculated CRC:0x8767
smCom :DEBUG:Retry Counter = 0
smCom :DEBUG:phNxpEseProto7816_DecomposeFrame S-Frame Received
smCom :DEBUG:Close i2c device 3.

smCom :DEBUG:phNxpEse_close - ESE Context deinit completed
```

2 – Later, I tested OpenSSL Engine with SCP03 Authentication and it did not work.

It was configured as following:

-DSCP=SCP03_SSS

-DSE05X_Auth=PlatfSCP03

And the result is shown below:


```
root@am335x-evm:~# ./se05x_GetInfo
App :INFO :PlugAndTrust_v03.03.00_20210528
App :INFO :Running ./se05x_GetInfo
App :INFO :If you want to over-ride the selection, use ENV=EX_SSS_BOOT_SSS_PORT or pass
in command line arguments.
App :DEBUG:Using File: /home/root/plain_scp.txt
App :WARN :Using SCP03 keys from:'/home/root/plain_scp.txt'
(FILE=/home/root/plain_scp.txt)
smCom :DEBUG:phPalEse_i2c_open_and_configure Opening port
smCom :DEBUG:I2CInit: opening /dev/i2c-2

smCom :DEBUG:I2C driver: PEC flag cleared

smCom :DEBUG:I2C driver supports plain i2c-level commands.

smCom :DEBUG:I2C driver Initialized :: fd = [12]
smCom :DEBUG:phNxpEseProto7816_Open: First open completed
smCom :DEBUG:phNxpEse_clearReadBuffer Enter ..
smCom :DEBUG:phPalEse_i2c_read Read Requested 260 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=260)
    5B 21 01 00  70 99 37 49  00 00 00 00  54 D8 FA BE
    F4 D7 FA BE  FC D7 FA BE  B3 76 35 49  FC D7 FA BE
    D0 9A 37 49  04 00 00 00  78 1E FC B6  01 00 00 00
    00 00 00 00  01 00 00 00  70 99 37 49  00 00 00 00
    2C 9B 37 49  2C 9B 37 49  00 00 00 00  01 80 AD FB
    00 D9 FA BE  00 D9 FA BE  00 D9 FA BE  00 D9 FA BE
    FF FF FF FF  FE D9 FA BE  40 A3 38 49  20 18 FC B6
    00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
    00 00 00 00  05 00 00 00  01 00 00 00  04 D1 05 00
    10 F0 FB B6  D0 F4 FB B6  00 00 00 00  01 00 00 00
    00 90 37 49  00 00 00 00  DF B0 35 49  78 1E FC B6
```

01 00 00 00 01 00 00 00 00 00 00 00 10 F0 FB B6
40 A3 38 49 E8 D8 FA BE 00 D0 05 00 90 D8 FA BE
57 4C 3F 49 88 13 00 00 E8 03 00 00 40 42 0F 00
39 46 41 49 00 00 00 00 40 4B 4C 00 00 D0 05 00
22 DB FA BE 00 00 00 00 47 E7 03 00 A4 D8 FA BE
05 00 00 00

smCom :DEBUG:_i2c_read() error : 13

smCom :DEBUG:TransceiveProcess nextTransceiveState 4

smCom :DEBUG:S-Frame PCB: c0

smCom :DEBUG:phNxpEse_WriteFrame Enter ..

smCom :DEBUG:TX (axI2CWrite) > (Len=5)

5A C0 00 FF FC

smCom :DEBUG:Done with rv = 0c

smCom :DEBUG:RAW Tx> (Len=5)

5A C0 00 FF FC

smCom :DEBUG:phNxpEse_read Enter ..

smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes

smCom :DEBUG:Done with rv = 0c

smCom :DEBUG:TX (axI2CRead): (Len=2)

A5 E0

smCom :DEBUG:phNxpEse_readPacket Read HDR

smCom :DEBUG:phNxpEse_readPacket SOF FOUND

smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes

smCom :DEBUG:Done with rv = 0c

smCom :DEBUG:TX (axI2CRead): (Len=1)

00

smCom :DEBUG:poll_sof_chained_delay value is 0

smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes

smCom :DEBUG:Done with rv = 0c

smCom :DEBUG:TX (axI2CRead): (Len=2)

3F 19

```
smCom :DEBUG:RAW Rx< (Len=5)
    A5 E0 00 3F  19
smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x61dd8 len ----> 0x5
smCom :DEBUG:Received CRC:0x3f19 Calculated CRC:0x3f19
smCom :DEBUG:Retry Counter = 0
smCom :DEBUG:phNxpEseProto7816_DecodeFrame S-Frame Received
smCom :DEBUG:TransceiveProcess nextTransceiveState 7
smCom :DEBUG:S-Frame PCB: c7
smCom :DEBUG:phNxpEse_WriteFrame Enter ..
smCom :DEBUG:TX (axI2CWrite) > (Len=5)
    5A C7 00 F7  B1
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:RAW Tx> (Len=5)
    5A C7 00 F7  B1
smCom :DEBUG:phNxpEse_read Enter ..
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
    A5 E7
smCom :DEBUG:phNxpEse_readPacket Read HDR
smCom :DEBUG:phNxpEse_readPacket SOF FOUND
smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=1)
    23
smCom :DEBUG:poll_sof_chained_delay value is 0
smCom :DEBUG:phPalEse_i2c_read Read Requested 37 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=37)
    00 A0 00 00  03 96 04 03  E8 00 FE 02  0B 03 E8 08
    01 00 00 00  00 64 00 00  0A 4A 43 4F  50 34 20 41
```

```
54 50 4F 2A 8D
smCom :DEBUG:RAW Rx< (Len=40)
    A5 E7 23 00 A0 00 00 03 96 04 03 E8 00 FE 02 0B
    03 E8 08 01 00 00 00 00 64 00 00 0A 4A 43 4F 50
    34 20 41 54 50 4F 2A 8D
smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x61dd8 len ----> 0x28
smCom :DEBUG:Received CRC:0x2a8d Calculated CRC:0x2a8d
smCom :DEBUG:Retry Counter = 0
smCom :DEBUG:phNxpEseProto7816_DecodeFrame S-Frame Received
smCom :DEBUG:phNxpEseProto7816_DecodeSFrameData frameoffset=3 value=0x0
smCom :DEBUG:Data[0]=0x0 len=35 Data[34]=0x50 Data[79]=0x23
smCom :DEBUG:Trying to Acquire Lock thread: -1225002992
smCom :DEBUG:LOCK Acquired by thread: -1225002992
smCom :DEBUG:APDU Tx> (Len=17)
    00 A4 04 00 0B D2 76 00 00 85 30 4A 43 4F 90 03
    00
smCom :DEBUG:Enter phNxpEseProto7816_Transceive
smCom :DEBUG:Transceive data ptr 0x0xbefad418 len:17
smCom :DEBUG:I-Frame Data Len: 17 Seq. no:0
smCom :DEBUG:TransceiveProcess nextTransceiveState 1
smCom :DEBUG:phNxpEse_WriteFrame Enter ..
smCom :DEBUG:TX (axl2CWrite) > (Len=22)
    5A 00 11 00 A4 04 00 0B D2 76 00 00 85 30 4A 43
    4F 90 03 00 71 18
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:RAW Tx> (Len=22)
    5A 00 11 00 A4 04 00 0B D2 76 00 00 85 30 4A 43
    4F 90 03 00 71 18
smCom :DEBUG:phNxpEse_read Enter ..
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
```

```
smCom :DEBUG:TX (axI2CRead): (Len=2)
    00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
    00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
    A5 00
smCom :DEBUG:phNxpEse_readPacket Read HDR
smCom :DEBUG:phNxpEse_readPacket SOF FOUND
smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=1)
    17
smCom :DEBUG:poll_sof_chained_delay value is 0
smCom :DEBUG:phPalEse_i2c_read Read Requested 25 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=25)
    6F 13 84 0B  D2 76 00 00  85 30 4A 43  4F 90 03 A5
    04 9F 65 01  FF 90 00 F2  5C
smCom :DEBUG:RAW Rx< (Len=28)
    A5 00 17 6F  13 84 0B D2  76 00 00 85  30 4A 43 4F
    90 03 A5 04  9F 65 01 FF  90 00 F2 5C
```

smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x61dd8 len ----> 0x1c
smCom :DEBUG:Received CRC:0xf25c Calculated CRC:0xf25c
smCom :DEBUG:Retry Counter = 0
smCom :DEBUG:phNxpEseProto7816_DecodeFrame I-Frame Received
smCom :DEBUG:phNxpEseProto7816_DecodeFrame I-Frame lastRcvdIframeInfo.seqNo:0x0
smCom :DEBUG:Data[0]=0x6f len=23 Data[22]=0x90 Data[0]=0x17
smCom :DEBUG: phNxpEse_Transceive Exit status 0x0
smCom :DEBUG:APDU Rx< (Len=23)
 6F 13 84 0B D2 76 00 00 85 30 4A 43 4F 90 03 A5
 04 9F 65 01 FF 90 00
smCom :DEBUG:Trying to Released Lock by thread: -1225002992
smCom :DEBUG:LOCK Released by thread: -1225002992
sss :INFO :atr (Len=35)
 00 A0 00 00 03 96 04 03 E8 00 FE 02 0B 03 E8 08
 01 00 00 00 00 64 00 00 0A 4A 43 4F 50 34 20 41
 54 50 4F
scp :DEBUG:FN: nxScp03_AuthenticateChannel
scp :DEBUG: Output: hostChallenge (Len=8)
 96 AC C2 96 37 D8 51 14
scp :DEBUG:FN: nxScp03_GP_InitializeUpdate
scp :DEBUG:Input:keyVersion 0b
scp :DEBUG: Input: hostChallenge (Len=8)
 96 AC C2 96 37 D8 51 14
scp :DEBUG:Sending GP Initialize Update Command !!!
smCom :DEBUG:Trying to Acquire Lock thread: -1225002992
smCom :DEBUG:LOCK Acquired by thread: -1225002992
smCom :DEBUG:APDU Tx> (Len=13)
 80 50 0B 00 08 96 AC C2 96 37 D8 51 14
smCom :DEBUG:Enter phNxpEseProto7816_Transceive
smCom :DEBUG:Transceive data ptr 0x0xbefad144 len:13
smCom :DEBUG:I-Frame Data Len: 13 Seq. no:1

```
smCom :DEBUG:TransceiveProcess nextTransceiveState 1
smCom :DEBUG:phNxpEse_WriteFrame Enter ..
smCom :DEBUG:TX (axI2CWrite) > (Len=18)
    5A 40 0D 80  50 0B 00 08  96 AC C2 96  37 D8 51 14
    8E 81
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:RAW Tx> (Len=18)
    5A 40 0D 80  50 0B 00 08  96 AC C2 96  37 D8 51 14
    8E 81
smCom :DEBUG:phNxpEse_read Enter ..
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
    00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
    00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
    00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
```

smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)

A5 40

smCom :DEBUG:phNxpEse_readPacket Read HDR

smCom :DEBUG:phNxpEse_readPacket SOF FOUND

smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes

smCom :DEBUG:Done with rv = 0c

smCom :DEBUG:TX (axI2CRead): (Len=1)

1F

smCom :DEBUG:poll_sof_chained_delay value is 0

smCom :DEBUG:phPalEse_i2c_read Read Requested 33 bytes

smCom :DEBUG:Done with rv = 0c

smCom :DEBUG:TX (axI2CRead): (Len=33)

90 03 12 10 00 00 49 95 55 95 0B 03 00 85 84 27

C3 F3 90 38 DD EB 36 BF 17 21 26 4E 4C 90 00 D1

9F

smCom :DEBUG:RAW Rx< (Len=36)

A5 40 1F 90 03 12 10 00 00 49 95 55 95 0B 03 00

85 84 27 C3 F3 90 38 DD EB 36 BF 17 21 26 4E 4C

90 00 D1 9F

smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x61dd8 len ----> 0x24

smCom :DEBUG:Received CRC:0xd19f Calculated CRC:0xd19f

smCom :DEBUG:Retry Counter = 0

smCom :DEBUG:phNxpEseProto7816_DecodeFrame I-Frame Received

smCom :DEBUG:phNxpEseProto7816_DecodeFrame I-Frame lastRcvdIframeInfo.seqNo:0x1

smCom :DEBUG:Data[0]=0x90 len=31 Data[30]=0x90 Data[0]=0x1f

smCom :DEBUG: phNxpEse_Transceive Exit status 0x0

smCom :DEBUG:APDU Rx< (Len=31)

90 03 12 10 00 00 49 95 55 95 0B 03 00 85 84 27

C3 F3 90 38 DD EB 36 BF 17 21 26 4E 4C 90 00

smCom :DEBUG:Trying to Released Lock by thread: -1225002992

smCom :DEBUG:LOCK Released by thread: -1225002992

scp :DEBUG: Output: keyDivData (Len=10)

90 03 12 10 00 00 49 95 55 95
scp :DEBUG: Output: keyInfo (Len=3)
0B 03 00
scp :DEBUG: Output: cardChallenge (Len=8)
85 84 27 C3 F3 90 38 DD
scp :DEBUG: Output: cardCryptoGram (Len=8)
EB 36 BF 17 21 26 4E 4C
scp :DEBUG:FN: nxScp03_HostLocal_CalculateSessionKeys
scp :DEBUG: Input:hostChallenge (Len=8)
96 AC C2 96 37 D8 51 14
scp :DEBUG: Input:cardChallenge (Len=8)
85 84 27 C3 F3 90 38 DD
scp :DEBUG:Set the Derivation data to generate Session ENC key
scp :DEBUG:FN: nxScp03_setDerivationData
scp :DEBUG:Input:ddConstant 04
scp :DEBUG:Input:ddl 80
scp :DEBUG:Input:iCounter 01
scp :DEBUG: Input: keyInfo (Len=16)
96 AC C2 96 37 D8 51 14 85 84 27 C3 F3 90 38 DD
scp :DEBUG:Output: KeyDivData (Len=32)
00 00 00 00 00 00 00 00 00 00 04 00 00 80 01
96 AC C2 96 37 D8 51 14 85 84 27 C3 F3 90 38 DD
scp :DEBUG:FN: nxScp03_Generate_SessionKey
scp :DEBUG: Input: inData (Len=32)
00 00 00 00 00 00 00 00 00 00 04 00 00 80 01
96 AC C2 96 37 D8 51 14 85 84 27 C3 F3 90 38 DD
scp :DEBUG: Output:outSignature (Len=16)
57 03 84 B3 76 D1 EF F1 55 4F 48 95 A5 AC 7B DF
scp :DEBUG: Output:sessionEncKey (Len=16)
57 03 84 B3 76 D1 EF F1 55 4F 48 95 A5 AC 7B DF
scp :DEBUG:Set the Derivation data to generate Session MAC key

```
scp :DEBUG:FN: nxScp03_setDerivationData
scp :DEBUG:Input:ddConstant 06
scp :DEBUG:Input:ddl 80
scp :DEBUG:Input:iCounter 01
scp :DEBUG: Input: keyInfo (Len=16)
    96 AC C2 96 37 D8 51 14 85 84 27 C3 F3 90 38 DD
scp :DEBUG:Output: KeyDivData (Len=32)
    00 00 00 00 00 00 00 00 00 06 00 00 80 01
    96 AC C2 96 37 D8 51 14 85 84 27 C3 F3 90 38 DD
scp :DEBUG:FN: nxScp03_Generate_SessionKey
scp :DEBUG: Input: inData (Len=32)
    00 00 00 00 00 00 00 00 00 06 00 00 80 01
    96 AC C2 96 37 D8 51 14 85 84 27 C3 F3 90 38 DD
scp :DEBUG: Output:outSignature (Len=16)
    3C 76 10 9E 17 9F 4C 5E 17 8C F5 42 6B 18 43 B5
scp :DEBUG: Output:sessionMacKey (Len=16)
    3C 76 10 9E 17 9F 4C 5E 17 8C F5 42 6B 18 43 B5
scp :DEBUG:Set the Derivation data to generate Session RMAC key
scp :DEBUG:FN: nxScp03_setDerivationData
scp :DEBUG:Input:ddConstant 07
scp :DEBUG:Input:ddl 80
scp :DEBUG:Input:iCounter 01
scp :DEBUG: Input: keyInfo (Len=16)
    96 AC C2 96 37 D8 51 14 85 84 27 C3 F3 90 38 DD
scp :DEBUG:Output: KeyDivData (Len=32)
    00 00 00 00 00 00 00 00 00 07 00 00 80 01
    96 AC C2 96 37 D8 51 14 85 84 27 C3 F3 90 38 DD
scp :DEBUG:FN: nxScp03_Generate_SessionKey
scp :DEBUG: Input: inData (Len=32)
    00 00 00 00 00 00 00 00 00 07 00 00 80 01
    96 AC C2 96 37 D8 51 14 85 84 27 C3 F3 90 38 DD
```

```
scp :DEBUG: Output:outSignature (Len=16)
    72 F4 4B 0D  F0 D9 65 2A  23 55 54 6A  F6 84 15 DA
scp :DEBUG: Output:sessionRmacKey (Len=16)
    72 F4 4B 0D  F0 D9 65 2A  23 55 54 6A  F6 84 15 DA
scp :DEBUG:FN: nxScp03_HostLocal_VerifyCardCryptogram
scp :DEBUG: Input:hostChallenge (Len=8)
    96 AC C2 96  37 D8 51 14
scp :DEBUG: Input:cardChallenge (Len=8)
    85 84 27 C3  F3 90 38 DD
scp :DEBUG:FN: nxScp03_setDerivationData
scp :DEBUG:Input:ddConstant 00
scp :DEBUG:Input:ddl 40
scp :DEBUG:Input:iCounter 01
scp :DEBUG: Input: keyInfo (Len=16)
    96 AC C2 96  37 D8 51 14  85 84 27 C3  F3 90 38 DD
scp :DEBUG:Output: KeyDivData (Len=32)
    00 00 00 00  00 00 00 00  00 00 00 00  00 00 40 01
    96 AC C2 96  37 D8 51 14  85 84 27 C3  F3 90 38 DD
scp :DEBUG:FN: nxScp03_Generate_SessionKey
scp :DEBUG: Input: inData (Len=32)
    00 00 00 00  00 00 00 00  00 00 00 00  00 00 40 01
    96 AC C2 96  37 D8 51 14  85 84 27 C3  F3 90 38 DD
scp :DEBUG: Output:outSignature (Len=16)
    31 A5 52 75  E5 B4 FD 82  7B 2A 37 08  DA 44 9E 0A
scp :DEBUG: Output:cardCryptogram (Len=16)
    31 A5 52 75  E5 B4 FD 82  7B 2A 37 08  DA 44 9E 0A
scp :WARN :nxEnsure:'status == kStatus_SSS_Success' failed. At Line:145
Function:nxScp03_AuthenticateChannel
sss :ERROR:Could not set SCP03 Secure Channel
smCom :DEBUG:Trying to Acquire Lock thread: -1225002992
smCom :DEBUG:LOCK Acquired by thread: -1225002992
```

```
smCom :DEBUG:APDU Tx> (Len=22)
    00 A4 04 00 10 A0 00 00 03 96 54 53 00 00 00 01
    03 30 00 00 00 00
smCom :DEBUG:Enter phNxpEseProto7816_Transceive
smCom :DEBUG:Transceive data ptr 0x0xbefadb7c len:22
smCom :DEBUG:I-Frame Data Len: 22 Seq. no:0
smCom :DEBUG:TransceiveProcess nextTransceiveState 1
smCom :DEBUG:phNxpEse_WriteFrame Enter ..
smCom :DEBUG:TX (axI2CWrite) > (Len=27)
    5A 00 16 00 A4 04 00 10 A0 00 00 03 96 54 53 00
    00 00 01 03 30 00 00 00 00 79 1C
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:RAW Tx> (Len=27)
    5A 00 16 00 A4 04 00 10 A0 00 00 03 96 54 53 00
    00 00 01 03 30 00 00 00 00 79 1C
smCom :DEBUG:phNxpEse_read Enter ..
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
    A5 00
smCom :DEBUG:phNxpEse_readPacket Read HDR
smCom :DEBUG:phNxpEse_readPacket SOF FOUND
smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=1)
    02
smCom :DEBUG:poll_sof_chained_delay value is 0
smCom :DEBUG:phPalEse_i2c_read Read Requested 4 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=4)
    6A 82 60 89
```

smCom :DEBUG:RAW Rx< (Len=7)
A5 00 02 6A 82 60 89
smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x61dd8 len ----> 0x7
smCom :DEBUG:Received CRC:0x6089 Calculated CRC:0x6089
smCom :DEBUG:Retry Counter = 0
smCom :DEBUG:phNxpEseProto7816_DecodeFrame I-Frame Received
smCom :DEBUG:phNxpEseProto7816_DecodeFrame I-Frame lastRcvdIframeInfo.seqNo:0x0
smCom :DEBUG:Data[0]=0x6a len=2 Data[1]=0x6a Data[130]=0x2
smCom :DEBUG: phNxpEse_Transceive Exit status 0x0
smCom :DEBUG:APDU Rx< (Len=2)
6A 82
smCom :DEBUG:Trying to Released Lock by thread: -1225002992
smCom :DEBUG:LOCK Released by thread: -1225002992
App :WARN :No SemsLite Applet Available.
hostLib:DEBUG:CloseSession command is sent only if valid Session exists!!!
smCom :DEBUG:TransceiveProcess nextTransceiveState 6
smCom :DEBUG:S-Frame PCB: c5
smCom :DEBUG:phNxpEse_WriteFrame Enter ..
smCom :DEBUG:TX (axI2CWrite) > (Len=5)
5A C5 00 47 82
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:RAW Tx> (Len=5)
5A C5 00 47 82
smCom :DEBUG:phNxpEse_read Enter ..
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
A5 E5
smCom :DEBUG:phNxpEse_readPacket Read HDR
smCom :DEBUG:phNxpEse_readPacket SOF FOUND
smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes

```
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=1)
    00
smCom :DEBUG:poll_sof_chained_delay value is 0
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
    87 67
smCom :DEBUG:RAW Rx< (Len=5)
    A5 E5 00 87 67
smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x61dd8 len ----> 0x5
smCom :DEBUG:Received CRC:0x8767 Calculated CRC:0x8767
smCom :DEBUG:Retry Counter = 0
smCom :DEBUG:phNxpEseProto7816_DecodeFrame S-Frame Received
smCom :DEBUG:Close i2c device 3.

smCom :DEBUG:phNxpEse_close - ESE Context deinit completed
App :INFO :Running ./se05x_GetInfo
App :INFO :If you want to over-ride the selection, use ENV=EX_SSS_BOOT_SSS_PORT or pass
in command line arguments.
App :DEBUG:Using File: /home/root/plain_scp.txt
App :WARN :Using SCP03 keys from:'/home/root/plain_scp.txt'
(FILE=/home/root/plain_scp.txt)
smCom :DEBUG:phPalEse_i2c_open_and_configure Opening port
smCom :DEBUG:I2CInit: opening /dev/i2c-2

smCom :DEBUG:I2C driver: PEC flag cleared

smCom :DEBUG:I2C driver supports plain i2c-level commands.

smCom :DEBUG:I2C driver Initialized :: fd = [12]
smCom :DEBUG:phNxpEseProto7816_Open: First open completed
```

```
smCom :DEBUG:phNxpEse_clearReadBuffer Enter ..
smCom :DEBUG:phPalEse_i2c_read Read Requested 260 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=260)
    70 45 73 65  50 72 6F 74  6F 37 38 31  36 5F 4F 70
    65 6E 3A 20  46 69 72 73  74 20 6F 70  65 6E 20 63
    6F 6D 70 6C  65 74 65 64  00 D8 FA BE  00 00 00 00
    EC B8 04 00  E4 D9 FA BE  58 D8 FA BE  00 00 00 00
    9B E1 3C 49  00 00 00 00  00 00 00 00  01 80 AD FB
    D0 D8 FA BE  D0 D8 FA BE  D0 D8 FA BE  D0 D8 FA BE
    F4 D8 FA BE  CE D9 FA BE  D0 D8 FA BE  CE D9 FA BE
    00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
    00 00 00 00  05 00 00 00  00 00 00 00  49 03 3D 49
    00 00 47 49  00 00 00 00  98 04 00 00  90 E1 05 00
    C1 F9 3C 49  40 D8 FA BE  FF FF FF FF  00 00 00 00
    00 00 00 00  A8 D8 FA BE  FF FF FF FF  10 F0 FB B6
    00 55 00 00  B8 D8 FA BE  75 2F 41 49  60 D8 FA BE
    57 4C 3F 49  88 13 00 00  E8 03 00 00  40 42 0F 00
    39 46 41 49  00 00 00 00  40 4B 4C 00  00 D0 05 00
    F2 DA FA BE  00 00 00 00  47 E7 03 00  74 D8 FA BE
    05 00 00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:TransceiveProcess nextTransceiveState 4
smCom :DEBUG:S-Frame PCB: c0
smCom :DEBUG:phNxpEse_WriteFrame Enter ..
smCom :DEBUG:TX (axI2CWrite) > (Len=5)
    5A C0 00 FF  FC
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:RAW Tx> (Len=5)
    5A C0 00 FF  FC
smCom :DEBUG:phNxpEse_read Enter ..
```


smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
A5 E0
smCom :DEBUG:phNxpEse_readPacket Read HDR
smCom :DEBUG:phNxpEse_readPacket SOF FOUND
smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=1)
00
smCom :DEBUG:poll_sof_chained_delay value is 0
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
3F 19
smCom :DEBUG:RAW Rx< (Len=5)
A5 E0 00 3F 19
smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x61dd8 len ----> 0x5
smCom :DEBUG:Received CRC:0x3f19 Calculated CRC:0x3f19
smCom :DEBUG:Retry Counter = 0
smCom :DEBUG:phNxpEseProto7816_DecodeFrame S-Frame Received
smCom :DEBUG:TransceiveProcess nextTransceiveState 7
smCom :DEBUG:S-Frame PCB: c7
smCom :DEBUG:phNxpEse_WriteFrame Enter ..
smCom :DEBUG:TX (axI2CWrite) > (Len=5)
5A C7 00 F7 B1
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:RAW Tx> (Len=5)
5A C7 00 F7 B1
smCom :DEBUG:phNxpEse_read Enter ..
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes

```
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
    A5 E7
smCom :DEBUG:phNxpEse_readPacket Read HDR
smCom :DEBUG:phNxpEse_readPacket SOF FOUND
smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=1)
    23
smCom :DEBUG:poll_sof_chained_delay value is 0
smCom :DEBUG:phPalEse_i2c_read Read Requested 37 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=37)
    00 A0 00 00 03 96 04 03 E8 00 FE 02 0B 03 E8 08
    01 00 00 00 00 64 00 00 0A 4A 43 4F 50 34 20 41
    54 50 4F 2A 8D
smCom :DEBUG:RAW Rx< (Len=40)
    A5 E7 23 00 A0 00 00 03 96 04 03 E8 00 FE 02 0B
    03 E8 08 01 00 00 00 00 64 00 00 0A 4A 43 4F 50
    34 20 41 54 50 4F 2A 8D
smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x61dd8 len ----> 0x28
smCom :DEBUG:Received CRC:0x2a8d Calculated CRC:0x2a8d
smCom :DEBUG:Retry Counter = 0
smCom :DEBUG:phNxpEseProto7816_DecompileFrame S-Frame Received
smCom :DEBUG:phNxpEseProto7816_DecompileSFrameData frameoffset=3 value=0x0
smCom :DEBUG:Data[0]=0x0 len=35 Data[34]=0x50 Data[79]=0x23
smCom :DEBUG:Trying to Acquire Lock thread: -1225002992
smCom :DEBUG:LOCK Acquired by thread: -1225002992
smCom :DEBUG:APDU Tx> (Len=22)
    00 A4 04 00 10 A0 00 00 03 96 54 53 00 00 00 01
    03 00 00 00 00 00
```

```
smCom :DEBUG:Enter phNxpEseProto7816_Transceive
smCom :DEBUG:Transceive data ptr 0x0xbefad3e8 len:22
smCom :DEBUG:I-Frame Data Len: 22 Seq. no:0
smCom :DEBUG:TransceiveProcess nextTransceiveState 1
smCom :DEBUG:phNxpEse_WriteFrame Enter ..
smCom :DEBUG:TX (axI2CWrite) > (Len=27)
    5A 00 16 00  A4 04 00 10  A0 00 00 03  96 54 53 00
    00 00 01 03  00 00 00 00  00 A8 C8
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:RAW Tx> (Len=27)
    5A 00 16 00  A4 04 00 10  A0 00 00 03  96 54 53 00
    00 00 01 03  00 00 00 00  00 A8 C8
smCom :DEBUG:phNxpEse_read Enter ..
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
    00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
    00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
    00 00
```

smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)

00 00

smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)

00 00

smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)

00 00

smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)

00 00

smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms

```
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
    00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
    A5 00
smCom :DEBUG:phNxpEse_readPacket Read HDR
smCom :DEBUG:phNxpEse_readPacket SOF FOUND
smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=1)
    09
smCom :DEBUG:poll_sof_chained_delay value is 0
smCom :DEBUG:phPalEse_i2c_read Read Requested 11 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=11)
    03 06 00 61 D2 01 0B 90 00 50 AD
smCom :DEBUG:RAW Rx< (Len=14)
    A5 00 09 03 06 00 61 D2 01 0B 90 00 50 AD
smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x61dd8 len ----> 0xe
smCom :DEBUG:Received CRC:0x50ad Calculated CRC:0x50ad
smCom :DEBUG:Retry Counter = 0
smCom :DEBUG:phNxpEseProto7816_DecodeFrame I-Frame Received
smCom :DEBUG:phNxpEseProto7816_DecodeFrame I-Frame lastRcvdIframeInfo.seqNo:0x0
smCom :DEBUG:Data[0]=0x3 len=9 Data[8]=0x90 Data[0]=0x9
smCom :DEBUG: phNxpEse_Transceive Exit status 0x0
```

```
smCom :DEBUG:APDU Rx< (Len=9)
    03 06 00 61  D2 01 0B 90  00
smCom :DEBUG:Trying to Released Lock by thread: -1225002992
smCom :DEBUG:LOCK Released by thread: -1225002992
sss :INFO :atr (Len=35)
    00 A0 00 00  03 96 04 03  E8 00 FE 02  0B 03 E8 08
    01 00 00 00  00 64 00 00  0A 4A 43 4F  50 34 20 41
    54 50 4F
sss :INFO :Newer version of Applet Found
sss :INFO :Compiled for 0x30100. Got newer 0x30600
scp :DEBUG:FN: nxScp03_AuthenticateChannel
scp :DEBUG: Output: hostChallenge (Len=8)
    05 BE 7D 11  3D F6 AF B8
scp :DEBUG:FN: nxScp03_GP_InitializeUpdate
scp :DEBUG:Input:keyVersion 0b
scp :DEBUG: Input: hostChallenge (Len=8)
    05 BE 7D 11  3D F6 AF B8
scp :DEBUG:Sending GP Initialize Update Command !!!
smCom :DEBUG:Trying to Acquire Lock thread: -1225002992
smCom :DEBUG:LOCK Acquired by thread: -1225002992
smCom :DEBUG:APDU Tx> (Len=13)
    80 50 0B 00  08 05 BE 7D  11 3D F6 AF  B8
smCom :DEBUG:Enter phNxpEseProto7816_Transceive
smCom :DEBUG:Transceive data ptr 0x0xbefad114 len:13
smCom :DEBUG:I-Frame Data Len: 13 Seq. no:1
smCom :DEBUG:TransceiveProcess nextTransceiveState 1
smCom :DEBUG:phNxpEse_WriteFrame Enter ..
smCom :DEBUG:TX (axI2CWrite) > (Len=18)
    5A 40 0D 80  50 0B 00 08  05 BE 7D 11  3D F6 AF B8
    34 1A
smCom :DEBUG:Done with rv = 0c
```

```
smCom :DEBUG:RAW Tx> (Len=18)
    5A 40 0D 80  50 0B 00 08  05 BE 7D 11  3D F6 AF B8
    34 1A
smCom :DEBUG:phNxpEse_read Enter ..
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
    00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
    00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0d
smCom :DEBUG:TX (axI2CRead): (Len=2)
    00 00
smCom :DEBUG:_i2c_read() error : 13
smCom :DEBUG:_i2c_read() [HDR]errno : 79 ret : FFFFFFFF
smCom :DEBUG:phNxpEse_readPacket Normal Pkt, delay read 1ms
smCom :DEBUG:phPalEse_i2c_read Read Requested 2 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=2)
    A5 40
smCom :DEBUG:phNxpEse_readPacket Read HDR
smCom :DEBUG:phNxpEse_readPacket SOF FOUND
```

```
smCom :DEBUG:phPalEse_i2c_read Read Requested 1 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=1)
    1F
smCom :DEBUG:poll_sof_chained_delay value is 0
smCom :DEBUG:phPalEse_i2c_read Read Requested 33 bytes
smCom :DEBUG:Done with rv = 0c
smCom :DEBUG:TX (axI2CRead): (Len=33)
    90 03 12 10  00 00 49 95  55 95 0B 03  00 54 6A F5
    AB B2 5E A8  15 E9 4D BD  70 6E 76 F8  72 90 00 70
    BB
smCom :DEBUG:RAW Rx< (Len=36)
    A5 40 1F 90  03 12 10 00  00 49 95 55  95 0B 03 00
    54 6A F5 AB  B2 5E A8 15  E9 4D BD 70  6E 76 F8 72
    90 00 70 BB
smCom :DEBUG:phNxpEseProto7816_ProcessResponse p_data ----> 0x61dd8 len ----> 0x24
smCom :DEBUG:Received CRC:0x70bb Calculated CRC:0x70bb
smCom :DEBUG:Retry Counter = 0
smCom :DEBUG:phNxpEseProto7816_DecomposeFrame I-Frame Received
smCom :DEBUG:phNxpEseProto7816_DecomposeFrame I-Frame lastRcvdIframeInfo.seqNo:0x1
smCom :DEBUG:Data[0]=0x90 len=31 Data[30]=0x90 Data[0]=0x1f
smCom :DEBUG: phNxpEse_Transceive Exit status 0x0
smCom :DEBUG:APDU Rx< (Len=31)
    90 03 12 10  00 00 49 95  55 95 0B 03  00 54 6A F5
    AB B2 5E A8  15 E9 4D BD  70 6E 76 F8  72 90 00
smCom :DEBUG:Trying to Released Lock by thread: -1225002992
smCom :DEBUG:LOCK Released by thread: -1225002992
scp :DEBUG: Output: keyDivData (Len=10)
    90 03 12 10  00 00 49 95  55 95
scp :DEBUG: Output: keyInfo (Len=3)
    0B 03 00
```


scp :DEBUG: Output: cardChallenge (Len=8)
54 6A F5 AB B2 5E A8 15

scp :DEBUG: Output: cardCryptoGram (Len=8)
E9 4D BD 70 6E 76 F8 72

scp :DEBUG:FN: nxScp03_HostLocal_CalculateSessionKeys

scp :DEBUG: Input:hostChallenge (Len=8)
05 BE 7D 11 3D F6 AF B8

scp :DEBUG: Input:cardChallenge (Len=8)
54 6A F5 AB B2 5E A8 15

scp :DEBUG:Set the Derivation data to generate Session ENC key

scp :DEBUG:FN: nxScp03_setDerivationData

scp :DEBUG:Input:ddConstant 04

scp :DEBUG:Input:ddl 80

scp :DEBUG:Input:iCounter 01

scp :DEBUG: Input: keyInfo (Len=16)
05 BE 7D 11 3D F6 AF B8 54 6A F5 AB B2 5E A8 15

scp :DEBUG:Output: KeyDivData (Len=32)
00 00 00 00 00 00 00 00 00 00 00 04 00 00 80 01
05 BE 7D 11 3D F6 AF B8 54 6A F5 AB B2 5E A8 15

scp :DEBUG:FN: nxScp03_Generate_SessionKey

scp :DEBUG: Input: inData (Len=32)
00 00 00 00 00 00 00 00 00 00 00 04 00 00 80 01
05 BE 7D 11 3D F6 AF B8 54 6A F5 AB B2 5E A8 15

scp :DEBUG: Output:outSignature (Len=16)
44 E7 6C 49 A1 1E 20 CA 7C 49 E5 66 F6 01 8E 6D

scp :DEBUG: Output:sessionEncKey (Len=16)
44 E7 6C 49 A1 1E 20 CA 7C 49 E5 66 F6 01 8E 6D

scp :DEBUG:Set the Derivation data to generate Session MAC key

scp :DEBUG:FN: nxScp03_setDerivationData

scp :DEBUG:Input:ddConstant 06

scp :DEBUG:Input:ddl 80

```
scp :DEBUG:Input:iCounter 01
scp :DEBUG: Input: keyInfo (Len=16)
    05 BE 7D 11  3D F6 AF B8  54 6A F5 AB  B2 5E A8 15
scp :DEBUG:Output: KeyDivData (Len=32)
    00 00 00 00  00 00 00 00  00 00 00 06  00 00 80 01
    05 BE 7D 11  3D F6 AF B8  54 6A F5 AB  B2 5E A8 15
scp :DEBUG:FN: nxScp03_Generate_SessionKey
scp :DEBUG: Input: inData (Len=32)
    00 00 00 00  00 00 00 00  00 00 00 06  00 00 80 01
    05 BE 7D 11  3D F6 AF B8  54 6A F5 AB  B2 5E A8 15
scp :DEBUG: Output:outSignature (Len=16)
    93 F2 74 30  46 93 10 BD  16 55 58 33  83 99 E9 FA
scp :DEBUG: Output:sessionMacKey (Len=16)
    93 F2 74 30  46 93 10 BD  16 55 58 33  83 99 E9 FA
scp :DEBUG:Set the Derivation data to generate Session RMAC key
scp :DEBUG:FN: nxScp03_setDerivationData
scp :DEBUG:Input:ddConstant 07
scp :DEBUG:Input:ddl 80
scp :DEBUG:Input:iCounter 01
scp :DEBUG: Input: keyInfo (Len=16)
    05 BE 7D 11  3D F6 AF B8  54 6A F5 AB  B2 5E A8 15
scp :DEBUG:Output: KeyDivData (Len=32)
    00 00 00 00  00 00 00 00  00 00 00 07  00 00 80 01
    05 BE 7D 11  3D F6 AF B8  54 6A F5 AB  B2 5E A8 15
scp :DEBUG:FN: nxScp03_Generate_SessionKey
scp :DEBUG: Input: inData (Len=32)
    00 00 00 00  00 00 00 00  00 00 00 07  00 00 80 01
    05 BE 7D 11  3D F6 AF B8  54 6A F5 AB  B2 5E A8 15
scp :DEBUG: Output:outSignature (Len=16)
    22 EF A1 76  A2 B6 11 B3  34 AA 13 53  E6 C8 6B 31
scp :DEBUG: Output:sessionRmacKey (Len=16)
```

```
22 EF A1 76 A2 B6 11 B3 34 AA 13 53 E6 C8 6B 31
scp :DEBUG:FN: nxScp03_HostLocal_VerifyCardCryptogram
scp :DEBUG: Input:hostChallenge (Len=8)
05 BE 7D 11 3D F6 AF B8
scp :DEBUG: Input:cardChallenge (Len=8)
54 6A F5 AB B2 5E A8 15
scp :DEBUG:FN: nxScp03_setDerivationData
scp :DEBUG:Input:ddConstant 00
scp :DEBUG:Input:ddl 40
scp :DEBUG:Input:iCounter 01
scp :DEBUG: Input: keyInfo (Len=16)
05 BE 7D 11 3D F6 AF B8 54 6A F5 AB B2 5E A8 15
scp :DEBUG:Output: KeyDivData (Len=32)
00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 01
05 BE 7D 11 3D F6 AF B8 54 6A F5 AB B2 5E A8 15
scp :DEBUG:FN: nxScp03_Generate_SessionKey
scp :DEBUG: Input: inData (Len=32)
00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 01
05 BE 7D 11 3D F6 AF B8 54 6A F5 AB B2 5E A8 15
scp :DEBUG: Output:outSignature (Len=16)
E0 F0 29 E5 73 19 8F 81 0A FB EF 16 EF 94 8E F0
scp :DEBUG: Output:cardCryptogram (Len=16)
E0 F0 29 E5 73 19 8F 81 0A FB EF 16 EF 94 8E F0
scp :WARN :nxEnsure:'status == kStatus_SSS_Success' failed. At Line:145
Function:nxScp03_AuthenticateChannel
sss :ERROR:Could not set SCP03 Secure Channel
App :ERROR:sss_session_open failed
App :ERROR:ex_sss_session_open Failed
App :ERROR:se05x_GetInfoPlainApplet Example Failed !!!...
App :INFO :ex_sss Finished
App :ERROR:ex_sss_entry Failed
```

App :ERROR:!ERROR! ret != 0.