Using osdp-sc to Configure the OSM-1000

osdp-sc is a command line tool created by Cypress Computer Systems to configure and test OSDP compliant devices.

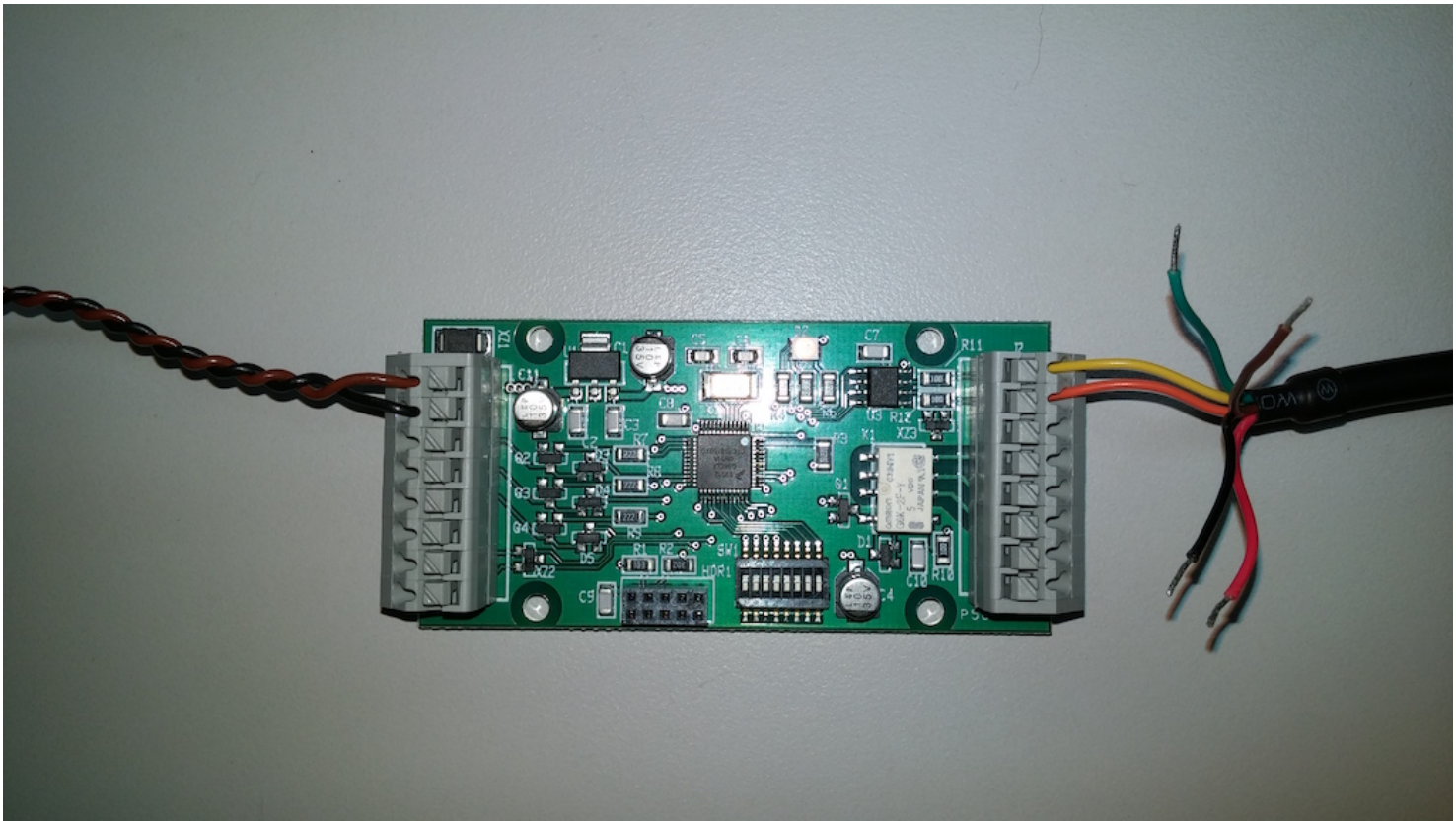
To use osdp-sc, the following items are needed:

+ USB to RS-485 adapter
+ External power supply
+ OSDP compliant device
+ Computer running a supported operating system (OS X)

This document will provide a step-by-step guide to connecting a Cypress OSM-1000, and changing it's SCBK (Secure Channel Base Key)

PRELIMINARY

Step 1: Connect the Device



Ensure all DIP switches on the OSM-1000 are off. The device must be a Peripheral Device (PD), and the default polling address is 0.

Connect the device to an external power supply (+12 VDC in this case), and to the RS-485 Adapter. The adapter used in this guide is the USB-RS485-WE-1800-BT.

The OSM-1000's Status LED should cycle through red, blue, green, off, and white during its startup sequence. The LED should then slowly pulse red.

Step 2: Start osdp-sc

In OS X, open Terminal.app

Navigate to the directory containing osdp-sc

```
$ cd ~/Downloads/
```

Run osdp-sc

```
$ ./osdp-sc
```

Note: If a permission error occurs, you may need to enable the file's execution flag and try again.

```
$ chmod +x osdp-sc
```

A message should appear such as:

```
Usage ./osdp-sc -a <deviceID> -s < IP or serial port  >  -p <Port>   -v  -f <filename>
./osdp-sc           0..127       1.2.3.4:123  or ttyS0   dflt 10001
 verbose  none
==================  OSDP Secure Channel Simulator/Tester ==================
Here are the available serial ports...
Choose by entering the number or type (cut/paste) name
 1.) cu.usbserial-FTY507ZN
 2.) Simulator
Enter :
```

Type the number of the virtual com port to which the OSM-1000 is connected, and then hit enter.

Input your OSDP device's polling address after the following prompt:

```
Select initial OSDP Device Polling Address:
```

A message should appear, along with a menu of options:

```
Select initial OSDP Device Polling Address: 0
Opening Serial Port cu.usbserial-FTY507ZN to OSDP Device
Opening Serial Port [ /dev/cu.usbserial-FTY507ZN ]
Port Open OK
Setting Attributes
                       0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
                     +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
POLL[ 1] ( 8 Bytes):  FF 53 00 07 00 00 60 46
RESP[ 1] ( 8 Bytes):  FF 53 80 07 00 00 40 E6
sync = 1, ctrl = 00, response = 40
Checksum  OK

< 1 > Host Config
< 2 > Device Config
< 3 > Device Polling
< 4 > Device Reports
< 5 > Device I/O
< 6 > Secure Channel
< 7 > Manufacturer Specific
< 8 > Test Functions
< 99 > Quit
Choose Command:
```

Step 3: Initiate Secure Channel Communication

Choose menu option 6, and the following menu should appear:

```
Choose Command: 6

< 1 > Start Session
< 2 > CHLNG
< 3 > SCRYPT
< 4 > KEYSET
< 5 > Generate Session Keys
< 6 > Generate Cryptograms
< 7 > Clear Session Keys
< 8 > Display Session Keys
< 9 > Poll Current ID once
< 10 > Send Special Packet with Bad CRC
< 11 > Resend Special Packet w/ Good CRC
< 12 > Terminate with BAD MAC
< 13 > Change Current Device
< 14 > Use SCBK
< 15 > Change Host SCBK
< 16 > Randomize
< 99 > Main Menu
Choose Command:
```

Choose menu option 1:

```
Choose Command: 1
ID = 0
CRC = 7731
POLL[ 0] (20 Bytes):  FF 53 00 13 00 0D 03 11 00 76 B0 B1 B2 B3 B4 B5
                      B6 B7 31 77
RESP[ 0] (44 Bytes):  FF 53 80 2B 00 0D 03 12 00 76 CA 44 6C 00 00 FF
                      FF FF 4F BE F8 70 E0 20 44 88 9E BD A9 A4 48 60
                      C5 37 F1 EB 6D 09 D2 30 2A D0 A5 A2
sync = 1, ctrl = 0D, response = 76
Len = 41  RXcrc = A2A5 CRC = A2A5  CRC OK
CCRYPT
    UID: CA446C0000FFFFFF
   RndB: 4FBEF870E0204488
 CCrypt: 9EBDA9A44860C537F1EB6D09D2302AD0
Key    [ 0]: 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
Key    [ 0]: 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
Key    [ 0]: 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
CRC = E752
POLL[ 0] (28 Bytes):  FF 53 00 1B 00 0E 03 13 00 77 F0 66 03 63 B5 C3
                      DD AA B2 07 D6 CC 92 FE A9 6A 52 E7
RESP[ 0] (28 Bytes):  FF 53 80 1B 00 0E 03 14 01 78 7D CB 74 4F CD 6F
                      99 B3 9E 11 8F 1E 7E 77 88 90 02 90
sync = 1, ctrl = 0E, response = 78
Len = 25  RXcrc = 9002 CRC = 9002  CRC OK
Secure Session Started...
    RMAC_I: 7DCB744FCD6F99B39E118F1E7E778890
```

Step 4: Issue the KEYSET command

Choose menu option 4:

```
Choose Command: 4
ID = 0
Enter Key[16]:
```

Enter a new SCBK, and enter "y" when propmted:

```
Enter Key[16]: 313132333435363738393A3B3C3D3E3F
New Key: 31313233 34353637 38393A3B 3C3D3E3F do you want to update PD?(y/n)
y
CV[16] = 7D CB 74 4F CD 6F 99 B3 9E 11 8F 1E 7E 77 88 90
Data Field: 01 20 31 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 80 00 00 00 00 00 00 00
00 00 00 00 00 00
Multi-Block MAC derivation
POLL[ 0] (47 Bytes):  FF 53 00 2E 00 0F 02 17 75 5B F4 E2 52 D2 9F 32
                      ED 01 60 82 24 98 51 AD 9A F4 97 0C E2 41 B8 C6
                      EA 68 60 18 E5 DE 06 87 17 9E A2 2E 28 5B F6
RESP[ 0] (15 Bytes):  FF 53 80 0E 00 0F 02 16 40 BE D1 7A 3A 33 B8
sync = 1, ctrl = 0F, response = 40
Len = 12  RXcrc = B833 CRC = B833  CRC OK
POLL - RMAC[4] = BED17A3A
         CV[16]= 9EA22E280351BF2BE13B0E16A70D09A9
Single Block MAC derivation
       RMAC[16]= BED17A3A3EF34DC2A7B34CBCD991C947
RMAC[4] OK Copying RV[16] -> CV[16]
```

Choose menu option 12:

```
Choose Command: 12
                      0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
                    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
Single Block MAC derivation
POLL[ 1] (15 Bytes):  FF 53 00 0E 00 0E 02 15 60 C3 DC DF 67 6F E0
RESP[ 1] (10 Bytes):  FF 53 80 09 00 06 41 06 A0 BA
sync = 1, ctrl = 06, response = 41
Len = 7  RXcrc = BAA0 CRC = BAA0  CRC OK
NAK 06 - Encrypted Command Required
```

The device has now dropped out of secure channel mode using the default SCBK.
Now, if a CP attempts to initiate a secure channel using the default SCBK,
the device will respond with a NAK:

```
Choose Command: 1
ID = 0
CRC = FDF7
POLL[ 0] (20 Bytes):  FF 53 00 13 00 0F 03 11 00 76 B0 B1 B2 B3 B4 B5
                      B6 B7 F7 FD
RESP[ 0] (44 Bytes):  FF 53 80 2B 00 0F 03 12 00 76 CA 44 6C 00 00 FF
                      FF FF 5F 85 E9 54 C2 64 B3 BC D4 A1 A1 8E 64 52
                      40 BD C1 2F B6 BD 68 81 A6 BF 7E 62
sync = 1, ctrl = 0F, response = 76
Len = 41  RXcrc = 627E CRC = 627E  CRC OK
CCRYPT
    UID: CA446C0000FFFFFF
   RndB: 5F85E954C264B3BC
 CCrypt: D4A1A18E645240BDC12FB6BD6881A6BF
Key    [ 0]: 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
Key    [ 0]: 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
Key    [ 0]: 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
CRC = 68E7
POLL[ 0] (28 Bytes):  FF 53 00 1B 00 0D 03 13 00 77 8E CA D8 07 B3 14
                      28 30 26 75 48 0B 95 84 4D ED E7 68
RESP[ 0] (10 Bytes):  FF 53 80 09 00 05 41 06 F0 E3
sync = 1, ctrl = 05, response = 41
Len = 7  RXcrc = E3F0 CRC = E3F0  CRC OK
NAK 06 - Encrypted Command Required
```

Step 5: Change Host SCBK, and Test Communication

In order to resume secure channel communication with the device, we must change the program's SCBK.

```
Select menu option 15:
Choose Command: 15
Current key[16] is : 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
Enter Key[16] in HEX (no spaces '.' to cancel) :
```

Enter the same SCBK as above:

```
Enter Key[16] in HEX (no spaces '.' to cancel) :313132333435363738393A3B3C3D3E3F
Host's Key[16]: 31 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
```

Now a secure channel may be established using the new SCBK:

```
Choose Command: 1
ID = 0
CRC = B894
POLL[ 0] (20 Bytes):  FF 53 00 13 00 0E 03 11 00 76 B0 B1 B2 B3 B4 B5
                      B6 B7 94 B8
RESP[ 0] (44 Bytes):  FF 53 80 2B 00 0E 03 12 00 76 CA 44 6C 00 00 FF
                      FF FF AF F1 0A 11 53 C9 4D 9D F0 84 C6 82 76 11
                      FE 0D 7A EF 0D 6B 5B A8 A7 58 E3 34
sync = 1, ctrl = 0E, response = 76
Len = 41  RXcrc = 34E3 CRC = 34E3  CRC OK
CCRYPT
    UID: CA446C0000FFFFFF
   RndB: AFF10A1153C94D9D
 CCrypt: F084C6827611FE0D7AEF0D6B5BA8A758
Key    [ 0]: 31 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
Key    [ 0]: 31 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
Key    [ 0]: 31 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
CRC = FBC4
POLL[ 0] (28 Bytes):  FF 53 00 1B 00 0F 03 13 00 77 6A D8 3E B6 16 2A
                      35 0C 95 54 DE F4 40 18 F3 3F C4 FB
RESP[ 0] (28 Bytes):  FF 53 80 1B 00 0F 03 14 01 78 E6 B8 98 11 60 8C
                      20 29 DA 8F E6 A2 3B 9A D3 39 85 30
sync = 1, ctrl = 0F, response = 78
Len = 25  RXcrc = 3085 CRC = 3085  CRC OK
Secure Session Started...
    RMAC_I: E6B89811608C2029DA8FE6A23B9AD339
```