Using osdp-sc to Upgrade the OSM-1000

CYPRESS
INTEGRATION SOLUTIONS

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

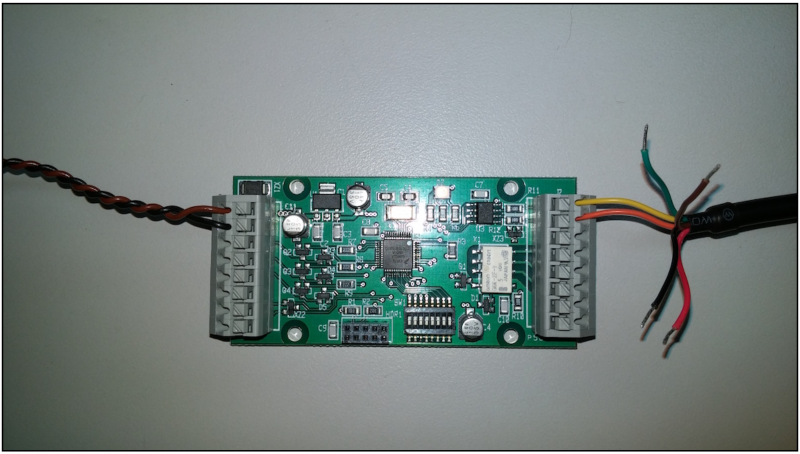
To use osdp-sc, the following items are needed:

- 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 upgrading its Firmware

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, ensure osdp-sc and the firmware file to be uploaded are in the same directory.

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:
```

If the device is configured to use a user SCBK, Choose menu option 15. Otherwise, if the device is configured to use the default SCBK (SCBK_D), continue with the instructions on the next page.

```
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 device's SCBK and press enter. Enter the SCBK as 32 hexadecimal digits (numbers 0-9, and letters A-F), without any spaces or other characters. It is important remember these keys, and to keep them secret.

```
Enter Key[16] in HEX (no spaces '.' to cancel) :31313233343536373839З3A3B3C3D3E3F
Host's Key[16]: 31 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

< 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 Firmware Upload Command

Choose menu option 99 to return to the Main Menu:

```
Choose Command: 99

< 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:
```

Choose menu option 7:

```
Choose Command: 7

< 1 > Upload Firmware
< 2 > Write Serial Number
< 3 >
< 4 >
< 5 >
< 6 >
< 7 >
< 8 >
< 9 > Test Multi-Decrypt
< 99 > Main Menu
Choose Command:
```

Choose menu option 1:

```
Choose Command: 1

Select Firmware File...
 1.) OSM1000_1_2_3.s19
Enter :




Data Field[n*16]:
CA 44 6C 01 80 00 00 00 00 00 00 00 00 00 00 00
00
CV[16] = CD E8 67 F1 19 4B CF 57 A2 27 6E CC 62 88 E3 DA
Multi-Block MAC derivation
POLL[ 0] (32 Bytes):  FF 53 00 1F 00 0F 02 17 80 CE 92 CE BB 09 81 81
                      14 73 AB 4E 8D 0D 54 AE 08 00 44 55 E7 E1 DD F3

RESP[ 0] (31 Bytes):  FF 53 80 1E 00 0F 02 18 90 0A 50 2B 82 46 26 D4
                      C2 0E 4E A8 E5 01 B4 D3 9E 13 DE 50 40 0B 81
sync = 1, ctrl = 0F, response = 90
Len = 28  RXcrc = 810B CRC = 810B  CRC OK

...

sync = 1, ctrl = 0D, response = 90
Len = 28  RXcrc = 64E6 CRC = 64E6  CRC OK

...
```

At this point, the selected firmware image will begin to upload into the device. Packets will be transmitted about twice a second, and the upload will take about one and a half minutes for a 45 KB file.

Once the upload is complete, the device will automatically reboot. osdp-sc should send a final poll and, because the device is rebooting, should not receive a response. The final output might look like the following:

```
...

MFGREP - RMAC[4] =
DF9C4A7F
Multi-Block MAC derivation
DeCrypting Data Field... Reply[16] = CA446C03303030318000000000000000
Vendor CA:44:6C = 13255788  ... Cypress Computer Systems, Inc.
Data Field[n*16]:
CA 44 6C 03 80 00 00 00 00 00 00 00 00 00 00 00
00
CV[16] = DF 9C 4A 7F CF F0 89 A0 44 51 3F 9F AB 09 81 10
Multi-Block MAC derivation
POLL[ 0] (32 Bytes):  FF 53 00 1F 00 0F 02 17 80 70 10 A8 AA 58 F6 90
                      88 44 77 5E 98 C7 9D FF C4 00 67 30 1A 06 B4 A9
```

```
RESP[ 0] ( 0 Bytes):
sync = 0, ctrl = 00, response = 0E
Checksum ****** BAD ******
Unknown Command: $0E
BAD RESPONSE - 0E
ERROR = 1

< 1 > Upload Firmware
< 2 > Write Serial Number
< 3 >
< 4 >
< 5 >
< 6 >
< 7 >
< 8 >
< 9 > Test Multi-Decrypt
< 99 > Main Menu
Choose Command:
```

After a firmware upload, it may be pertainent to test communication. Reinitiate secure channel communications as described above.