sysmocom

sysmocom - s.f.m.c. GmbH

Osmocom ngff-cardem User Manual

by Harald Welte, Martin Schramm, and Stephan Skrodzki

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME
v1	March 2022	Initial version, covering ngff-cardem hardware v1	HW
v2	December 2022	Hardware v2 pictures added, smaller typos	SK
v2	February 2023	Host Software and Application examples.	SK
v3	October 2023	osmo-remsim Example Setup	SK

Contents

1 Introduction

This manual describes the Osmocom ngff-cardem, a NGFF/M.2 cellular modem carrier board with integrated SIM card tracing, switching and remote SIM forwarding capabilities.

The target audience are test lab engineers or system integrators who use the ngff-cardem to build their own products, such as remote nodes for cellular network quality monitoring or roaming testing.

If you are familiar with the related Osmocom ngff-breakout and SIMtrace2 products: The ngff-cardem board is basically a combination of those two.

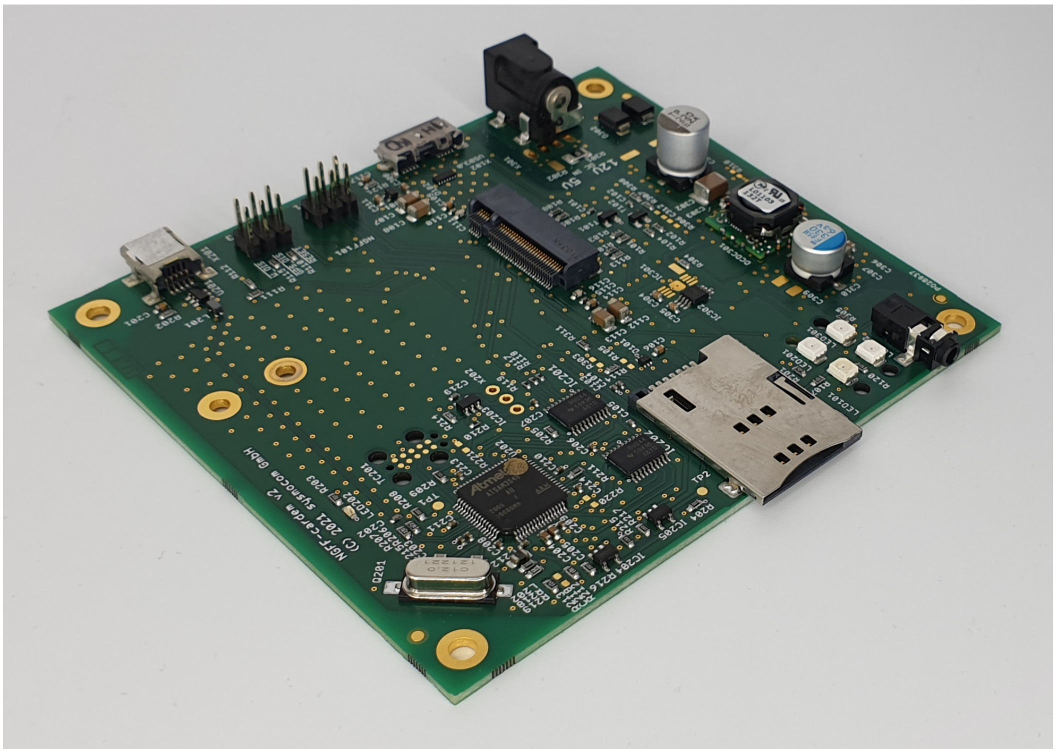


Figure 1: ngff-cardem PCBA

1.1 Purpose

The purpose of the ngff-cardem is to host a cellular (WWAN) modem in M.2 form factor, sometimes allso called NGFF form-factor. Such modems are available from a variety of suppliers, such as Sierra Wireless, SIMcom, Quectel, Ericsson, Huawei and others.

The host-facing USB 3 super-speed (and high-speed) signals of the modem are exposed on a micro-USB-3 connector, from where they can be attached to any USB host controller, whether a desktop PC, laptop or embedded system at the choice of the user.

The unique feature of the ngff-cardem board over other modem carrier boards is that it has built-in microcontroller that can operate firmware from the SIMtrace2 universe, which can be used to

- perform passive tracing of the SIM card protocol beteween the local SIM card inserted into the on-board SIM slot and the modem
- switch between the locally-inserted SIM card and a remote SIM card
- switch the local SIM card to the SIMtrace2 processor and directly access the card from custom host software

1.2 Designated Use

The designated use of the ngff-cardem is to be used as a carrier board for one to four mPCIe compliant cellular (WWAN) modems, integrated into a larger customer-specific device/appliance.

It is the customer's responsibility to

- ensure proper integration with the cellular modems he selected
- mount the product in a suitable enclosure providing
  - protection from environmental influences
  - protection from ESD (Electrostatic Discharge) exposure to the bare circuit board assembly
  - EMC (Electromagnetic Compatibility) compliance
  - providing sufficient heat dissipation capability for the product and modems
- connect a suitable compatible power supply
- separately obtain and install the modems and SIM cards intended to be used in the given application
- connect cabling, adapters and antennas compatible with the chosen cellular modems

1.3 Intended Audience

The intended audience of this manual is the technical staff of the systems integrator who integrates the ngff-cardem into a customer-specific product/appliance within the designated use stated above.

1.4 Regulatory compliance

The product is designed to be conforming with all applicable harmonized standards in the EU. As such, the series-produced units will be accompanied with a declaration of conformity for the European market.

However, only a given reference configuration of the product is submitted to related conformance testing. This reference configuration includes

- a CE compliant cellular modem
- a typical shielded metal enclosure
- a CE compliant AC power supply for supplying 5 .. 12V DC
- a set of U.FL to SMA pigtails
- a set of antennas compatible with the requirements of the modem
- a CE compliant personal computer connected to the mini USB port and the mini USB3 port

Due to the many variable parameters of any customer-specific appliance built from the ntff-cardem, it is the responsibility of said system integrator to test and declare conformity with all applicable norms and standards on his final product.

2 Specifications

- 90x100mm four-layer PCB assembly with one-sided component placement
- mounting holes (M3) for mounting on PCB spacers/stands
- M.2 slot for cellular / WWAN Modems
- SIM/UICC slot for cards in ETSI/3GPP 2FF form-factor
- USB 3 device port on USB3 micro-B connector (Modem)
- USB 1 device port on USB mini-B connector (SIMtrace2/SAM3S)
- Atmel SAM3 microcontrollers for monitoring and control
  - temperature monitoring
  - reset of modem
  - power cycling of modem
  - SIM card forwarding / emulation
  - SIM card protocol tracing
  - remote WWAN LED reading
- on-board WWAN LED
- on-board programmable LED

2.1 Electrical

Table 1: Electrical Specifications

Parameter	Min	Typ	Max	Unit
Supply Voltage	5	12	14	Vdc
Supply Current			5	Adc

The current rating is determined almost exclusively by the type of modem used and above figure is the worst-case peak consumption with the modem transmitting a GSM burst at 2W RF output power. The board itself doesn't draw a significant amount of power, typically 100-150mA only.

2.2 Environmental Specifications

The ngff-cardem has been designed exclusively from parts specified for the **full industrial temperature range from -40 to 85 centigrade**.

Note
The actual usable temperature range might be limited by system integration. Care must be taken to ensure sufficient heat dissipation.

Please also observe the environmental specification of the M.2 modems you intend to use. They might have a more limited range than the ngff-cardem board itself.

3 ngff-cardem Hardware

The ngff-cardem hardware consists of a printed circuit board assembly (PCBA), sized 90 x 100 mm.

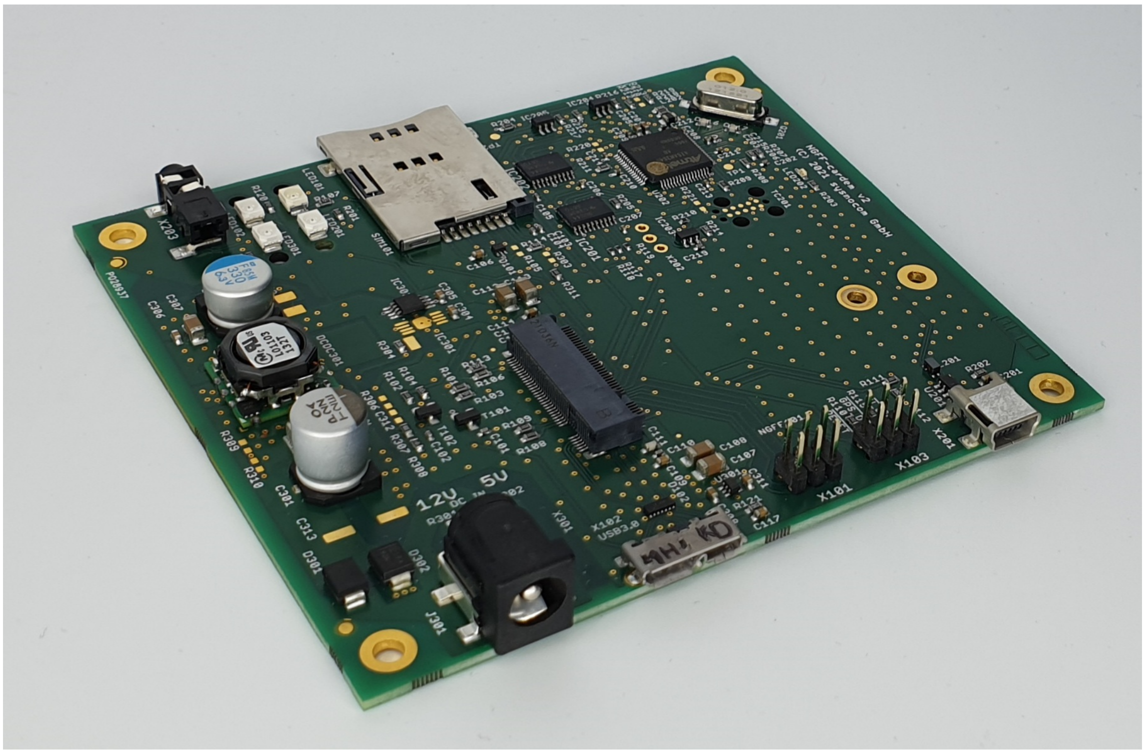


Figure 2: ngff-cardem PCBA

3.1 Power Supply

The ngff-cardem has one DC power input with a nominal input voltage of 5 .. 12V, which is used to power all on-board circuits. This 12V DC input can be supplied via *either* one of the following options:

- barrel-type power jack **J301** (center positive)
- The 5V pin of the floppy-style power connector **X301**
- The 12V pin of the floppy-style power connector **X301**

The power input has on-board protection diodes to prevent polarity reversal (D301) as well as an over-voltage zener (D302) diode. However, there **is no internal on-board fuse**, so the power supply should have reasonable current limits in place, or an external fuse shall be used.

3.2 Connectors

The ngff-cardem has the following physical connections:

- Power
  - J301: Barrel-type DC input
  - X301: floppy-style DC input

- Modem
  - X102: USB 3 micro-B connector for interfacing modem with external USB host
  - SIM101: SIM card slot (2FF form factor)
- SIMtrace2
  - X201: USB mini-B connector for interfacing SIMtrace2 firmware with external USB host
  - X202: Debug UART on THT pin header
  - X203: Debug UART of SIMtrace2 on Osmocom-style 3-pin 2.5mm jack

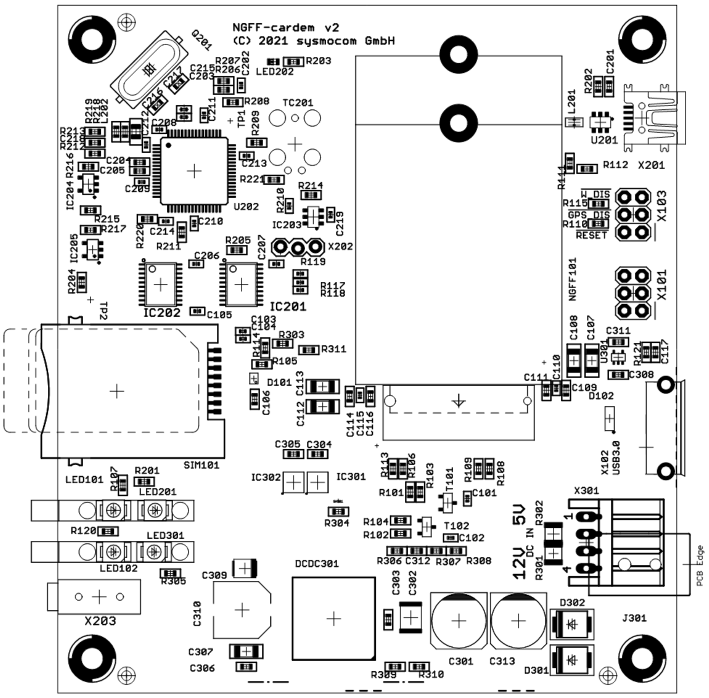


Figure 3: Board Layout

3.2.1 J301: Barrel-type DC Input

This is a 5.5mm diameter barrel-type DC input connector with 2.5mm pin diameter and the following pin-out:

Table 2: J301 DC Pinout

Pin	Function	Type
Center	+VIN	5V-12V DC Input (positive)
Outer	-VIN	5V-12V DC Input (ground, **not chassis ground**)

3.2.2 X102: USB 3 micro-B connector towards USB host (PC)

This is a standard USB-B type connector, exposing the USB device port of the on-board USB hub towards an external USB host (PC).

Table 3: X102 USB 3 micro-B Pinout

Pin	Function	Type
1	VBUS	Input / V_BUS detection
2	D-	Bi-Directional / Negative USB LS/FS/HS Data
3	D+	Bi-Directional / Positive USB LS/FS/HS Data
4	ID	NC
5	GND	Reference
6	SSTX-	Negative USB SS Transmit
7	SSTX+	Positive USB SS Transmit
8	GND	Reference
9	SSRX-	Negative USB SS Receive
10	SSRX+	Positive USB SS Receive

VBUS is only used for detecting the presence of a USB host, it is not used to power the ngff-cardem board.

3.2.3 TC201: JTAG + SWD connector for SAM3 microcontrollers

This is a 10-pin TagConnect connector, compatible with the TC2050 plug. Using this connector has the advantage of having zero cost impact on the PCB side, as the "connector" is just a PCB footprint.

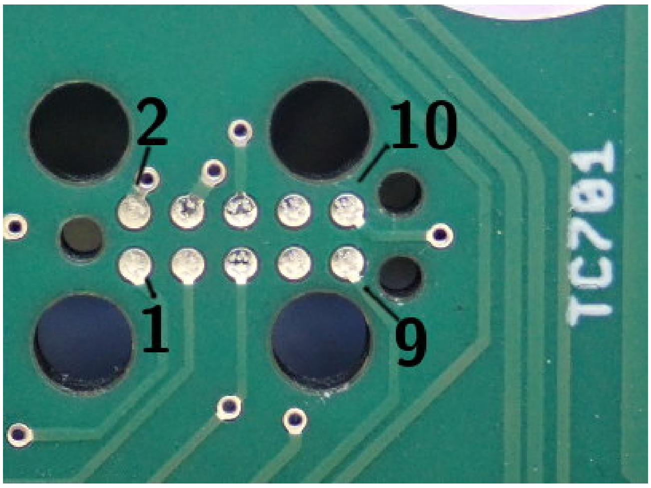


Figure 4: pin assignment TC601 and TC701 (shown TC701)

The pin-out is as follows:

Table 4: TC201 Pinout

Pin	Function	Type
1	TCK	Input
2	GND	Reference

Table 4: (continued)

Pin	Function	Type
3	TDO	Output
4	VCC	Reference
5	TMS	Input
6	!RESET	Input
7	NC	
8	NC	
9	TDI	Input
10	GND	Reference

JTAG can be used for flash programming, factory testing and firmware development/debugging of the SAM3 microcontroller.

3.2.4 X202, X203: 3.3V Serial Console of SAM3 microcontroller

This connector exposes the serial debug UART of the respective SAM3 microcontroller. During development and testing, this can be used for debugging and firmware updates.

Table 5: X203 Pinout

Pin	Function	Type
tip	RXD	input of SAM3
center	TXD	output of SAM3
ring	GND	Reference

Table 6: X202 Pinout

Pin	Function	Type
1	RXD	input of SAM3
2	TXD	output of SAM3
3	GND	Reference

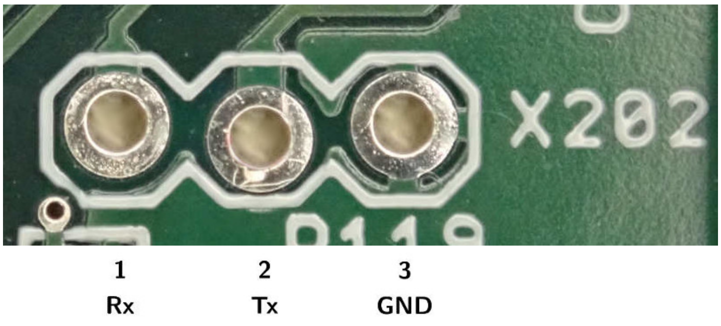


Figure 5: pin assignment X202

Note
As X202 (3 pos. THT pin header) also serves as 3.3V serial console connector of SAM3 microcontroller, only one of X202 or X203 can be used at a time. If both connectors are used at the same time, you know what you are doing or expect side effects.

3.2.5 SIM101: SIM Card Slot

This is a standard SIM card holder for a SIM card in ETSI 2FF form-factor.

For the pin-out, please refer to the ETSI/3GPP specifications on SIM/UICC cards.

3.2.6 X101: PCM interface

Some select M.2F modules make available the digital audio interface (PCM bus) on non-standard pins of the M.2 socket. This connector exposes pins 20, 22, 24 and 28 of the respective M.2 socket. It is intended to be attached to some external peripheral capable of interfacing the PCM bus.

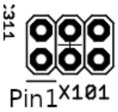


Figure 6: X101 Header

Table 7: X101: PCM interface pinout

Pin	M.2 Pin	Function
1	20	PCM_CLK/I2S_CLK
2	24	PCM_DOUT/I2S_DOUT
3	22	PCM_DIN/I2S_DIN
4	28	PCM_SYNC/I2S_WS
5	-	VCC_1V8
6	-	GND

3.2.7 NGFF101: M.2 / NGFF connector

This is a M.2 connector suitable for interfacing cellular modems (sometimes called WWAN modems) in M.2 form-factor. It provides supply power on the 3.3V rail, as well as the electrical USB (FS/LS/HS + SS) interface and the SIM card slot and SAM3 for SIM emulation.

For the pin-out, please refer to the relevant M.2 specification of the PCI SIG.

Note
For different reasons, not all modem manufacturer decided to comply electrically to PCI-SIG standardized specification. System integrators shall run own testing for usability of a particular modem prior to purchase.

3.2.8 Installing M.2 modems

M.2 card modem are mounted with M2 screws in a threaded SMT standoff, Two large-head M2 screws (PH1, 3mm) are included in the delivery of the ngff-cardem, as well as a SMT standoff.

In order to facilitate M.2 cards of different lengths (42mm and 52mm), the SMT standoff is not soldered to the board, but can be moved to the desired location and fixed using one of the two screws from the bottom side.

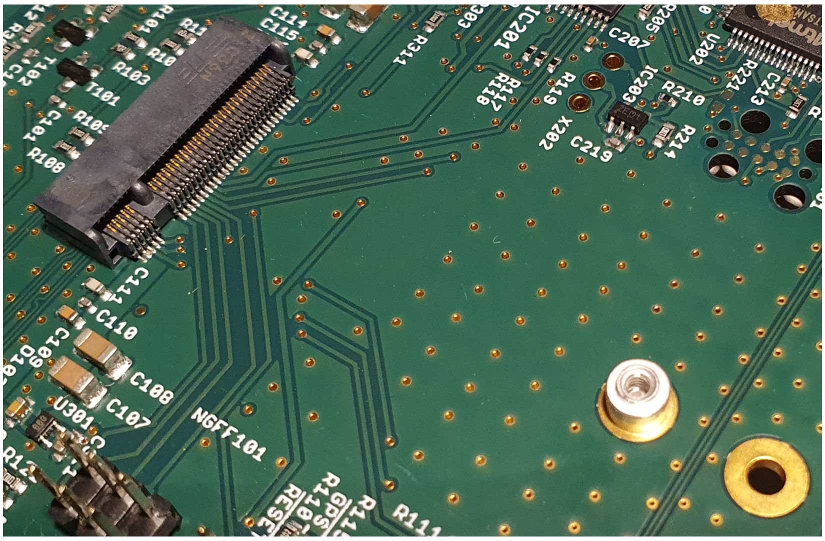


Figure 7: Empty Modem Mount

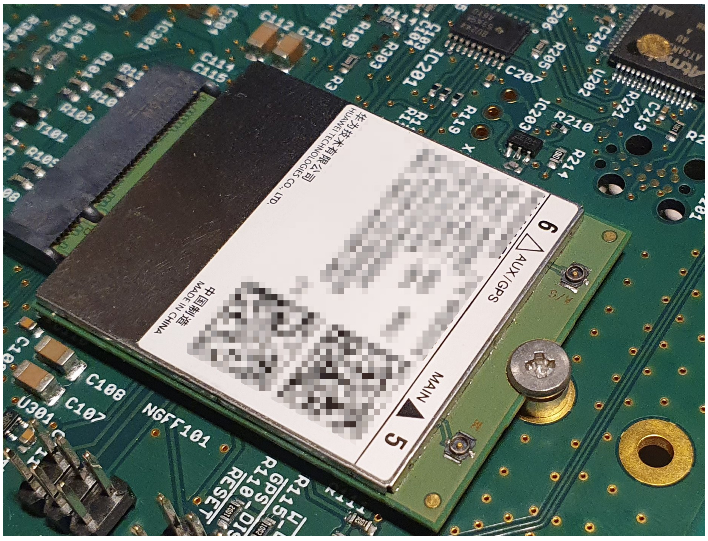


Figure 8: Modem Mounted

Note

Some modem manufacturers decided to deviate from the mechanical sizes of cards as stated in the M.2 Electromechanical Specification by the PCI-SIG. Such modems may be difficult to mount due to their non-standard location of the mounting hole for the SMT standoff. We have designed the board to respect the standard, an we have no influence on what kind of non-standard-compatible products other vendors build.

3.3 Modem Monitoring / Control via SAM3

The on-board SAM3 microcontroller has some capability to monitor and control the on-board modem. This ensures the option of a full remote recovery from any kind of stuck states, which is important in long-term remote deployments without the need for "remote hands" to power cycle equipment.

Specifically, the following features are implemented:

Table 8: Modem Monitoring/Control Capabilities

Signal Name	Description
MODEM_EN	Enable/Disable modem supply voltage via IC301 load switch IC
PWR_ON	Enable/Disable the PWR_ON_OFF pin of the M.2 slot.
PERST	Assert/De-Assert the !RESET signal of the M.2 slot.
WWAN	Read the Modem LED status as per the WWAN_LED of the modem. This can be used to remotely replicate the LED status and blinking pattern by software in the SAM3.

3.4 SIM Card Interface Emulation

The SIM Card interface emulation feature is implemented by two main components:

- three sets of SPDT switches between modem, SIM card and SIM slot
- a SAM3 microcontroller with specific firmware to emulate the card-side ISO7816-1/-2/-3 interface

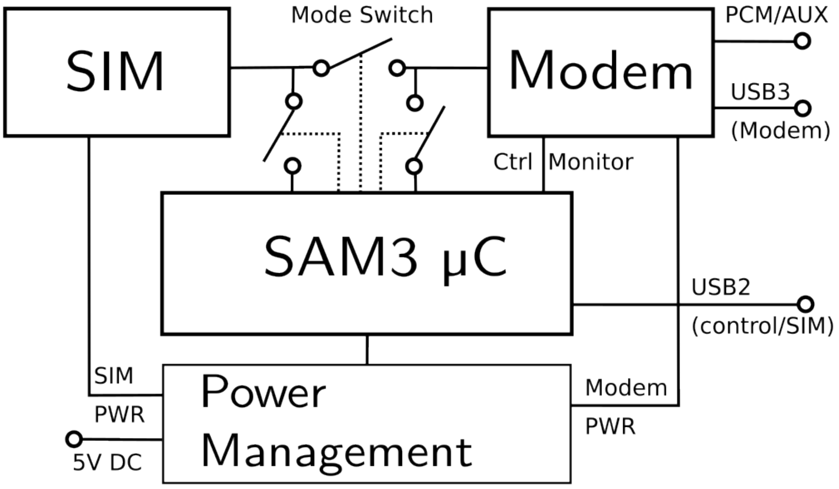


Figure 9: SIM Switching

Note
The remote SIM functionality depends on a proper implementation of the `PERST#` signal by the modem manufacturer. Many modems have this, but there is also a number of known modems which don't. Systems integrators should run own tests on specific modems to ensure usability for remote SIM function in terms of proper `PERST#` signal implementation for asserting a warm reset on the modem card.

3.5 Hardware Options

The hardware can be built with some options, among them are

- Barrel-type or Floppy-type DC input (Default: Barrel-type, J301)
- PCM header can be present/soldered or not (X101) (Default: present)
- Debug UART header can be present/soldered or not (X203 default: present; X202 default: no pinheader soldered)

If not stated otherwise at ordering, the default options will be used.

3.6 LEDs

There are four LEDs on the board.

3.6.1 User-visible LEDs

Table 9: User-visible LEDs

LED Number	Connected to	Color	Description
LED101	Modem WWAN LED	Yellow	WWAN LED of Modem 1, under Modem control
LED102	USB3 VBUS	Green	Indicates presence of VBUS supply from USB host
LED201	SAM3S	Green	Under SIMtrace2 firmware control
LED301	VCC_3V3	Green	Indicates presence of main 3V3 supply voltage

3.6.2 Non-User-visible LEDs

These LEDs are primarily for diagnostic purposes and are not normally exposed to the end user.

Table 10: Non-User-visible LEDs

LED Number	Color	Description
LED202	SAM3S	Red

4 Host connection

The connection to the host is accomplished via two separata USB connections:

- USB2 mini-B connector for access to SIM card and SAM3
- USB 3 micro-B connector for interfacing modem

To verify the correct recognition of the SAM3 and SIM card access, after connecting the USB2 cable, the syslog of the host should contain lines similar to this:

```
[Mo Jan 30 17:54:33 2023] usb 1-3.2.2: new full-speed USB device number 69 using xhci_hcd
[Mo Jan 30 17:54:33 2023] usb 1-3.2.2: New USB device found, idVendor=1d50, idProduct=616e, ↩
     bcdDevice= 0.02
[Mo Jan 30 17:54:33 2023] usb 1-3.2.2: New USB device strings: Mfr=1, Product=2,  ↩
    SerialNumber=11
[Mo Jan 30 17:54:33 2023] usb 1-3.2.2: Product: ngff-cardem
[Mo Jan 30 17:54:33 2023] usb 1-3.2.2: Manufacturer: sysmocom - s.f.m.c. GmbH
[Mo Jan 30 17:54:33 2023] usb 1-3.2.2: SerialNumber: 512032205433315233303420333303035
```

The recognition of the modem is done via the dedicated USB 3 micro-B connector. This manual contains no information how to access and control different modems, as there are a lot of different models and firmwares on the market.

5 SAM3 Firmware

In general, the firmware consists of two parts:

- the DFU bootloader, used for in-the-field updates of he SAM3 microcontrollers over USB
- the application program, installed and updated by the DFU bootloader, containing actual code for SIM card forwarding or emulation.

Note
When communicating to the firmware via the serial port, the speed on these ports is **115200** bps for firmware versions up to **0.5.1**, and it is **921600** bps for versions from **0.5.1.1** onwards. - Usage of these ports is not needed for normal operation of ngff-cardem.

5.1 Updating the firmware via DFU

At sysmocom factory programming time, the SAM3 controllers are loaded with a DFU bootloader. It occupies the first 16kBytes of flash in the SAM3.

DFU is the official standard of the USB Implementers Forum for **Device Firmware Upgrades**. It is used by many USB devices of various manufacturers.

For more information about DFU, please see the USB DFU specification, which can be obtained from http://www.usb.org/sites/default/files/DFU_1.1.pdf

5.1.1 DFU Basics

A DFU-capable device advertises its DFU capabilities via a DFU runtime descriptor which is exported during normal operation of the device (SAM3 application code is running). By sending special requests via USB, the device can be switched from application (runtime) mode into DFU (bootloader) mode.

Once the device enumerates in DFU mode, other DFU-specific requests on the control endpoint can be used to read (upload) and write (download) firmware from/to the device.

A device can export multiple **alternate settings**, and thereby export different memory types, flash partitions or the like. The DFU bootloader of the ngff-cardem supports

- downloading of application code into volatile RAM (alternate setting 0)
- downloading of application code into the flash (alternate setting 1)

Note
In almost all cases, you will want to install firmware images into the flash. Loading code into RAM is only used during development. You cannot use images linked for the flash in RAM (no relocation) or vice versa!

5.1.2 Entering DFU mode from the runtime

The DFU mode can be entered in the following ways:

- by sending a DFU_DETACH request from the host PC, or
- by placing a jumper across the RxD and TxD lines of the debug UART (X202) during boot of the controller, or
- by erased/implausible flash content at the start of the application partition (offset 16k = 0x4000)

If either of those three conditions is fulfilled, the SAM3 will boot the DFU bootloader and thus expose DFU-mode USB interfaces, rather than the regular application program.

5.1.3 Updating the application using `dfu-util`

`dfu-util` is an open source implementation of the USB DFU protocol using libusb, running on Linux and other operating systems.

It can interact with DFU-capable devices and perform operations such as

- listing DFU-capable devices attached to the system
- switching devices from Runtime to DFU mode
- uploading firmware from the device to a file on the Linux host
- downloading firmware from a file ont he Linux host to the device
- resetting a device to return from DFU mode to runtime mode

Firmware files for the ngff-cardem have the naming convention `ngff_cardem-<appname>-dfu.bin`

Existing applications are:

- Card Emulation (cardem): ngff_cardem-cardem-dfu
- (SIM)Trace: ngff_cardem-trace-dfu

At delivery, the latest ngff_cardem-cardem-dfu firmware is installed.

Note
Retrieving the firmware version of a firmware file is easily possible with the Linux `string` command: e.g. `strings ngff_cardem-trace-dfu-latest.bin` contains: `SIMtrace2 firmware 0.8.1.58-773d, BOARD=ngff_cardem, APP=trace`

You can use a command like

```
$ dfu-util -d 1d50:616e -p 1-4.4.1.1 -a 1 -D bin/ngff_cardem-cardem-dfu.bin -R
```

from the USB host to install the firmware. 1-4.4.1.1 is the path at which the respective processor is attached, which is seen in `dmesg` output

```
[79086.696291] usb 1-4.4.1.1: New USB device found, idVendor=1d50, idProduct=616e
```

The output of dfu-util while flahsing looks like this:

```
$ dfu-util -d 1d50:616e -p 1-4.4.1.1 -a 1 -D bin/ngff_cardem-cardem-dfu.bin -R
dfu-util 0.9

Copyright 2005-2009 Weston Schmidt, Harald Welte and OpenMoko Inc.
Copyright 2010-2016 Tormod Volden and Stefan Schmidt
This program is Free Software and has ABSOLUTELY NO WARRANTY
Please report bugs to http://sourceforge.net/p/dfu-util/tickets/

dfu-util: Invalid DFU suffix signature
dfu-util: A valid DFU suffix will be required in a future dfu-util release!!!
Opening DFU capable USB device...
ID 1d50:616e
Run-time device DFU version 0100
Claiming USB DFU Runtime Interface...
Determining device status: state = appIDLE, status = 0
Device really in Runtime Mode, send DFU detach request...
Resetting USB...
Opening DFU USB Device...
Claiming USB DFU Interface...
Setting Alternate Setting #1 ...
Determining device status: state = dfuIDLE, status = 0
dfuIDLE, continuing
DFU mode device DFU version 0100
Device returned transfer size 512
Copying data from PC to DFU device
Download        [=========================] 100%        28320 bytes
Download done.
state(7) = dfuMANIFEST, status(0) = No error condition is present
state(2) = dfuIDLE, status(0) = No error condition is present
Done!
dfu-util: can't detach
Resetting USB to switch back to runtime mode
```

5.2 Emergency recovery using SAM-BA

The SAM3 contains a mask-ROM boot loader called SAM-BA (SAM Boot Assist). When erasing the complete flash, this SAM-BA can be activated to perform an emergency recovery and/or to update the DFU bootloader.

Note
It is recommended to only use this SAM-BA method as a last resort, if DFU based flashing as described above has failed, or if you need to update the DFU bootloader itself.

The complete flash can be erased the following ways:

- by activating the ERASE signal of the SAM3 while it starts (release from RESET), or
- by JTAG

On the ngff-cardem, the ERASE signal of the SAM3 can be controlled via test pad TP1. In case of severe malfunction or the requirement to update the DFU bootloader, this signal can be brought to high (3.3V) level to erase the SAM3, and then recover it usign the SAM-BA ROM-loader.

5.2.1 Using `bossac` for flashing

`bossac` is an open source command-line utility program that can be used to talk to the SAM-BA loader inside Atmel SAM controllers such as the SAM3 on the ngff-cardem.

Once a SAM3 has been placed into SAM-BA mode, you can use `bossac` over the Debug UART or over USB.

To program the SAM3 over the UART, you need to connect a 3.3V USB-UART cable (sysmocom CP2102) to the respective SAM3 UART jack (X202 or X203).

DFU bootloader firmware files have the naming convention `ngff_cardem-dfu-flash.bin`. Do not attempt to flash any application images, only the DFU bootloader image shall be flashed via SAM-BA!

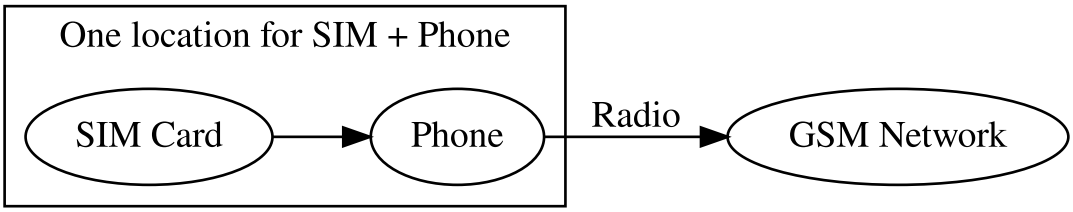
Example of `bossac` usage to flash the DFU bootloader into a chip:

```
$ bossac -e -w -v -b ngff_cardem-dfu-flash.bin -p ttyUSB0
Erase flash
Write 14748 bytes to flash
[==============================] 100% (58/58 pages)
Verify 14748 bytes of flash
[==============================] 100% (58/58 pages)
Verify successful
Set boot flash true
$
```

6 Remote SIM functionality

Normally, the SIM/USIM/RUIM card is physically co-located with the phone or cellular modem. The interconnection between SIM card and the cellular baseband processor is just a few centimeters of printed circuit trace. Replacing the SIM card requires physical access to the Phone, and swapping the cards frequently requires lots of manual interaction and associated system downtime.

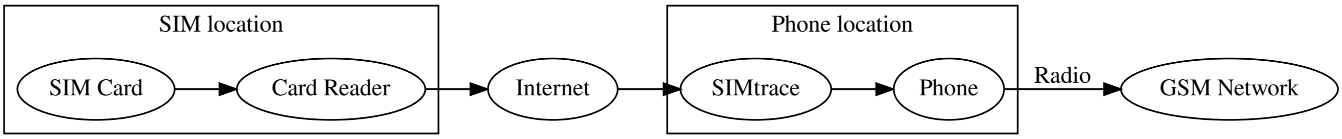
This system is fine for the normal use case where a human is carrying a cellphone, and the cellphone contains the SIM card of a cellular subscription which is changed only infrequently (every few weeks to months to year).



In some applications, it is useful to have a different set-up, where the SIM card is located remotely from the modem/phone.

This is the case in many remotely deployed systems, where a physical SIM card replacement would be very costly due to the logistics of sending the card there and having a human operator replace the card.

The **remote SIM** functionality solves this problem by forwarding the communication between phone and SIM virtually anywhere using TCP/IP transport protocol.



The **SIM side** and the **Radio side** can subsequently be at completely different physical/geographical locations, just as long as there is a transport channel between them.

6.1 Remote SIM Transport Channel

This transport channel can be high-latency and low-speed. It must only be capable of forwarding either all APDU data (simplistic implementation), or only the GSM/UMTS Authentication messages (optimized implementation with partial SIM card emulation on **Radio side**).

In fact, the transport channel in practise has shown to be able to use technologies like

- VSAT satellite links
- another set of physical SIM Card + Modem, so that the expensive roaming SIM is only used to tunnel the authentication data of a virtual other (e.g. non-roaming)SIM which is virtually provisioned in a dynamic way to that remote modem

6.2 Remote SIM Use Cases

There are many use case for such a setup, including

- Roaming / IREG testing systems
- Voice Quality testing systems
- Least Cost Routing of cellular data back-haul for vessels close to shore (e.g. using VSAT as transport channel)
- Interoperability testing to test different SIM cards with different modems

6.3 Host Software for Cardem Application

Caution
Please verify, that your ngff-cardem board is loaded with the Cardem Application.

There are two different options available in terms of software:

- `simtrace2-cardem-pcsc` as the most simple proof-of-concept. This is useful if you just want to quickly verify the correct operation of the ngff-cardem product and/or its built-in card-emulation firmware
- `osmo-remsim` as a fully open source software suite to manage populations of remote SIM cards and card emulators. This is more geared towards production operation.

The reference software consists of command-line tools to be used on GNU/Linux based systems. Those programs are provided as C language source code and require the libraries **libosmocore** as well as **libusb** to operate.

The software components are provided as Free / Open Source Software.

`simtrace2-list` and `simtrace2-cardem-pcsc` can be found as part of the https://git.osmocom.org/simtrace2 repository in the *host* subdirectory.

`osmo-remsim` can be found at https://git.osmocom.org/osmo-remsim

All related software is also provided as binary packages for Debian GNU/Linux, Ubuntu as well as Raspbian within the Osmocom binary package feeds, see https://osmocom.org/projects/cellular-infrastructure/wiki/Binary_Packages

6.3.1 simtrace2-list

The `simtrace2-list` utility is used to list the physical SIM card interfaces present on the system, to which a program like simtrace2-remsim could attach.

There is one line being printed for each interface. In the case of the ngff-cardem product, you should see one such line, as there is only one modem.

```
# simtrace2-list
USB matches: 2
        1d50:616e Addr=32, Path=1-3.2.2, Cfg=1, Intf=0, Alt=0: 255/2/0 (CardEmulator Modem  ↩
            1)
        1d50:616e Addr=32, Path=1-3.2.2, Cfg=2, Intf=0, Alt=0: 255/255/0 (0.8.1.20-8680)
```

The output lists two matches: while the first match (Configuration 1) is the CardEmulator, the second match (Configuration 2) is the bootloader of the ngff-cardem.

6.3.2 simtrace2-cardem-pcsc

The `simtrace2-cardem-pcsc` program is a simple proof-of-concept to demonstrate the remote SIM functionality. In order to use this, you will need

- a simtrace2-compatible device attached to your Linux PC and which shows up in simtrace2-list (such as the ngff-cardem)
- a smart card reader attached to your Linux PC, supported and exposed by pcsc-lite. We recommend USB-CCID compliant smart card readers, such as the Omnikey CardMan 3121 and 6121 series.

When you have the required hardware set-up and connected, you can start `simtrace2-cardem-pcsc`. After start, it will

- open the first available PC/SC reader on the system
- open the specified USB interface (see -V, -P, -C, -I, -S command line options)
- instruct the SIMTRACE2 compatible device to switch from local SIM to remote SIM mode
- instruct the SIMTRACE2 compatible device to perform a PERST (power enable reset) of the modem module, which causes implicit re-enumeration on the USB as well as re-reading of the SIM card during boot of the modem
- forward any APDUs between the modem and the SIM card inserted into the PC/SC reader

Caution
`simtrace2-cardem-pcsc` is not recommended for regular operation, but for evaluation and testing.

```
$ ./simtrace2-cardem-pcsc -V 0x1d50 -P 0x616e -C 1 -I 0 -H 1-3.2.2w -n 0
simtrace2-cardem-pcsc - Remote SIM card forwarding
(C) 2010-2017 by Harald Welte <laforge@gnumonks.org>

SCardEstablishContext: OK

SCardListReaders: OK

SCardConnect: OK

<- 01 05 00 00 00 00 09 00 01
<- 02 02 00 00 00 00 09 00 01
```

```
<= cardem_request_set_atr(3b 9f 96 80 1f c7 80 31 a0 73 be 21 13 67 43 20 07 18 00 00 01 a5 ↩
    )
<- 01 02 00 00 00 00 1f 00 16 3b 9f 00 80 1f c7 80 31 a0 73 be 21 13 67 43 20 07 18 00 00  ↩
    01 a5
<- 02 01 00 00 00 00 0b 00 02 2c 01
Entering main loop
```

The following command-line options are relevant:

- -V to specify the USB vendor ID (0x1d50)
- -P to specify the USB product ID (0x616e for ngff-cardem)
- -H to specify the USB path (1-4.4.1.1 here)
- -C to specify the USB configuration number (1)
- -I to specify the USB interface number (0 for first slot; 1 for second)
- -n to specify the PC/SC reader number (0 for first reader)

In a typical ngff-cardem, you will have:

- -H x-xxx.x for the controller serving the modem
- -I 0 for the first and only modem of a given controller

The program will automatically switch the SPDT switches from local SIM to remote SIM, and will issue a reset pulse to the modem. You should then see follow-up message exchanges like given below:

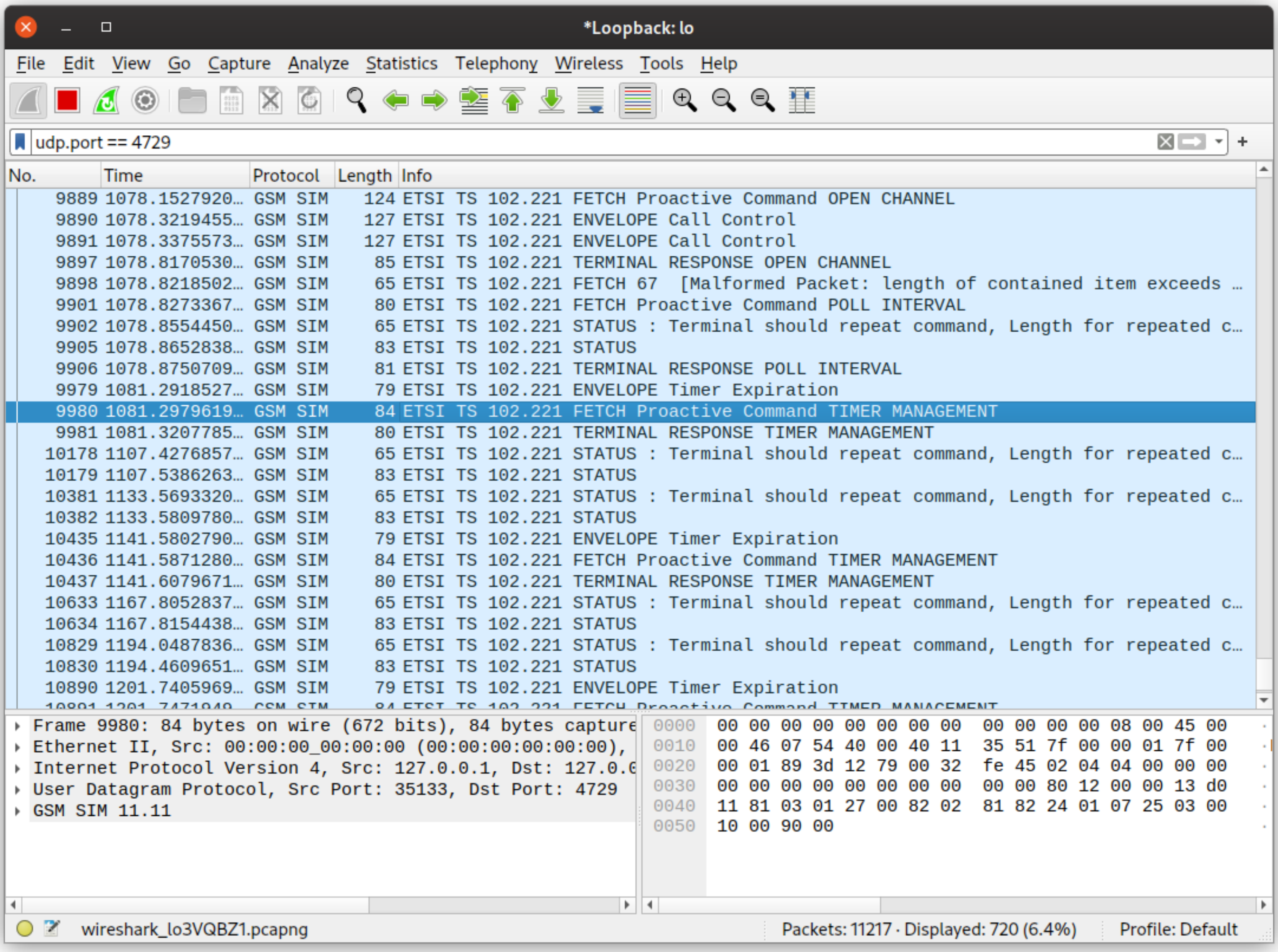
```
URB:
-> 01 06 00 00 00 00 13 00 01 00 00 00 05 00 00 a4 00 04 02
=> DATA: flags=1, 00 a4 00 04 02 : CLA=00 INS=a4 P1=00 P2=04 P3=02; case=4, lc=2(0), le ↩
    =0(0)
<= cardem_request_pb_and_rx(a4, 2)
<- 01 01 00 00 00 00 0f 00 08 00 00 00 01 00 a4
URB:
-> 01 06 00 00 00 00 10 00 02 00 00 00 02 00 3f 00
=> DATA: flags=2, 3f 00 : CLA=00 INS=a4 P1=00 P2=04 P3=02; case=4, lc=2(2), le=0(0)
TX: 00 a4 00 04 02 3f 00
SCardEndTransaction: OK
```

Once there are no more messages exchanged for some time, the modem has read all relevant information from the SIM, and the modem should show you the IMSI of the card when issuing "AT+CIMI".

Note
After stopping `simtrace2-cardem-pcsc`, the cardem is still in emulation mode and there is no access to the onboard SIM card. This could be reverted by power-cycling the ngff-cardem.

GSMTAP / wireshark APDU tracing

A protocol trace of the APDUs going back and forth between the SIM emulator hardware and the Card can be inspected in wireshark by means of GSMTAP encapsulated SIM Communication on UDP Port 4729 on the loopback device.


*Loopback: lo
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
udp.port == 4729
```

```
No.   Time          Protocol Length Info
 9889 1078.1527920… GSM SIM  124 ETSI TS 102.221 FETCH Proactive Command OPEN CHANNEL
 9890 1078.3219455… GSM SIM  127 ETSI TS 102.221 ENVELOPE Call Control
 9891 1078.3375573… GSM SIM  127 ETSI TS 102.221 ENVELOPE Call Control
 9897 1078.8170530… GSM SIM   85 ETSI TS 102.221 TERMINAL RESPONSE OPEN CHANNEL
 9898 1078.8218502… GSM SIM   65 ETSI TS 102.221 FETCH 67  [Malformed Packet: length of contained item exceeds …
 9901 1078.8273367… GSM SIM   80 ETSI TS 102.221 FETCH Proactive Command POLL INTERVAL
 9902 1078.8554450… GSM SIM   65 ETSI TS 102.221 STATUS : Terminal should repeat command, Length for repeated c…
 9905 1078.8652838… GSM SIM   83 ETSI TS 102.221 STATUS
 9906 1078.8750709… GSM SIM   81 ETSI TS 102.221 TERMINAL RESPONSE POLL INTERVAL
 9979 1081.2918527… GSM SIM   79 ETSI TS 102.221 ENVELOPE Timer Expiration
 9980 1081.2979619… GSM SIM   84 ETSI TS 102.221 FETCH Proactive Command TIMER MANAGEMENT
 9981 1081.3207785… GSM SIM   80 ETSI TS 102.221 TERMINAL RESPONSE TIMER MANAGEMENT
10178 1107.4276857… GSM SIM   65 ETSI TS 102.221 STATUS : Terminal should repeat command, Length for repeated c…
10179 1107.5386263… GSM SIM   83 ETSI TS 102.221 STATUS
10381 1133.5693320… GSM SIM   65 ETSI TS 102.221 STATUS : Terminal should repeat command, Length for repeated c…
10382 1133.5809780… GSM SIM   83 ETSI TS 102.221 STATUS
10435 1141.5802790… GSM SIM   79 ETSI TS 102.221 ENVELOPE Timer Expiration
10436 1141.5871280… GSM SIM   84 ETSI TS 102.221 FETCH Proactive Command TIMER MANAGEMENT
10437 1141.6079671… GSM SIM   80 ETSI TS 102.221 TERMINAL RESPONSE TIMER MANAGEMENT
10633 1167.8052837… GSM SIM   65 ETSI TS 102.221 STATUS : Terminal should repeat command, Length for repeated c…
10634 1167.8154438… GSM SIM   83 ETSI TS 102.221 STATUS
10829 1194.0487836… GSM SIM   65 ETSI TS 102.221 STATUS : Terminal should repeat command, Length for repeated c…
10830 1194.4609651… GSM SIM   83 ETSI TS 102.221 STATUS
10890 1201.7405969… GSM SIM   79 ETSI TS 102.221 ENVELOPE Timer Expiration
10891 1201.7471949… GSM SIM   84 ETSI TS 102.221 FETCH Proactive Command TIMER MANAGEMENT
```

```
▸ Frame 9980: 84 bytes on wire (672 bits), 84 bytes capture
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00),
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0
▸ User Datagram Protocol, Src Port: 35133, Dst Port: 4729
▸ GSM SIM 11.11
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00
0010  00 46 07 54 40 00 40 11  35 51 7f 00 00 01 7f 00
0020  00 01 89 3d 12 79 00 32  fe 45 02 04 04 00 00 00
0030  00 00 00 00 00 00 00 00  00 00 80 12 00 00 13 d0
0040  11 81 03 01 27 00 82 02  81 82 24 01 07 25 03 00
0050  10 00 90 00
```

wireshark_lo3VQBZ1.pcapng
Packets: 11217 · Displayed: 720 (6.4%)
Profile: Default

Figure 10: Wireshark SIM Communication

6.3.3 osmo-remsim

For more details on the osmo-remsim software, please see

- osmo-remsim project homepage at https://osmocom.org/projects/osmo-remsim/wiki
- osmo-remsim user manual at https://ftp.osmocom.org/docs/latest/osmo-remsim-usermanual.pdf
- osmo-remsim video presentation at https://media.ccc.de/v/osmocon2018-93-osmo-remsim-remote-sim-card-software

7 Trace Application

Caution

Please verify, that your ngff-cardem board is loaded with the Trace Application: `simtrace2-list` should output like: `1d50:616e Addr=50, Path=1-3.2.2, Cfg=1, Intf=0, Alt=0: 255/1/0 (SIMtrace Sniffer)`

With the trace application, the SAM3 controller on the ngff-cardem board is passively tracing the communication between the modem and the SIM card on board, providing the same functionality like the well-known and widely used SIMtrace2 boards (https://osmocom.org/projects/simtrace2/wiki)

7.1 Host Software for Trace

`simtrace2-sniff` is used to retrieve the sniffed Modem-SIM communication.

The activity will be shown on the console output:

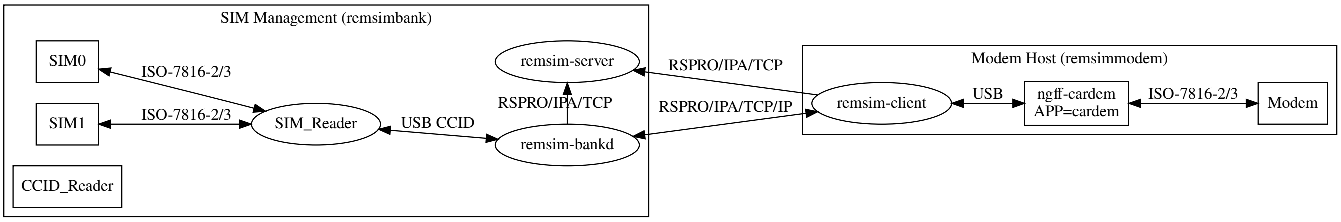
```
root# simtrace2-sniff
simtrace2-sniff - Phone-SIM card communication sniffer
(C) 2010-2017 by Harald Welte <laforge@gnumonks.org>
(C) 2018 by Kevin Redon <kredon@sysmocom.de>

Using USB device 1d50:616e Addr=50, Path=1-3.2.2, Cfg=1, Intf=0, Alt=0: 255/1/0 (SIMtrace  ←
    Sniffer)
Entering main loop
Card state change: reset de-asserted
TPDU: 80 c2 00 00 0e d7 0c 02 02 82 81 24 01 07 25 03 00 10 00 91 13
TPDU: 80 12 00 00 13 d0 11 81 03 01 27 00 82 02 81 82 24 01 07 25 03 00 10 00 90 00
TPDU: 80 14 00 00 0f 81 03 01 27 00 02 02 82 81 03 01 00 24 01 07 90 00
TPDU: 80 f2 00 01 00 6c 12
```

The TPDU will also be sent as GSMTAP frames to UDP/IPv4 localhost:4729. This also allows to analyze the communication in wireshark using the GSM SIM dissector.

8 osmo-remsim Example Setup

This chapter describes the setup and use of osmo-remsim in an exemplary environment of two Raspberry Pi 4: one with a ngff-cardem connected (this host is called remsimmodem and has IP 192.168.243.101) and the other one with a Omnikey CardMan 3121 USB CCID interface and a Omnikey CardMan 6121 USB CCID interface (this host is called remsimbank and has IP 192.168.243.100). Both devices are connected via ethernet.



8.1 Base installation on RPi 4 (both RPi)

Install raspios. For this document Raspberry Pi OS Lite 64bit as of 2023-10-10 was used.

Add osmocom nightly builds to your repos: https://osmocom.org/projects/cellular-infrastructure/wiki/Nightly_Builds

The next step is to install, configure and test the osmo-remsim components on the Raspberry Pis.

Note
while all services/components come with systemd service files, it may be easier to start them manually at the beginning to change commandline parameters faster and see issues immediately. Finally the services could be started via systemd.

8.2 remsimbank RPI4

To ease the understanding of this setup, the remsimbank holds both: the osmo-remsim-bankd and the osmo-remsim-server

8.2.1 Install and configure osmo-remsim-bankd

```
apt install osmo-remsim-bankd
```

To detect the connected ccid compatible readers, it is useful to install pcsc-tools:

```
apt install pcscd pcsc-tools
```

pcscn_scan detects in our case the following ccid devices:

```
root@remsimbank:~# pcsc_scan -r
0: HID Global OMNIKEY 6121 Smart Card Reader [OMNIKEY 6121 Smart Card Reader] 00 00
1: HID Global OMNIKEY 3x21 Smart Card Reader [OMNIKEY 3x21 Smart Card Reader] 01 00
```

As noted in the osmo-remsim-manual, escape regex relevant chars before adding these readers to the bankd slot configuration:

```
root@remsimbank:~# cat /etc/osmocom/bankd_pcsc_slots.csv
"1","0","HID Global OMNIKEY 6121 Smart Card Reader \[OMNIKEY 6121 Smart Card Reader\] 00  ↩
    00"
"1","1","HID Global OMNIKEY 3x21 Smart Card Reader \[OMNIKEY 3x21 Smart Card Reader\] 01  ↩
    00"
```

Caution
The non detection of a reader is reported only at the moment, when a client tries to access it.

osmo-remsim-bankd should be started with the following parameters (for this IP addresses):

```
osmo-remsim-bankd -i 192.168.243.100 -I 192.168.243.100 -n 2
```

Note
osmo-remsim-bankd looks in the same directory, where it is started, for the bankd_pcsc_slots.csv file, so for manual testing chdir to /etc/osmocom/ before starting.

These parameters should be set in `/etc/default/osmo-remsim-bankd` for the auto start of the service.

Note
Setting the bankd address to 127.0.0.1 does only work in a setup where the client is on the same host.

8.2.2 Install and configure osmo-remsim-server

```
apt install osmo-remsim-server
```

osmo-remsim-server does not need any parameters to start.

8.2.3 Check via API

Now it should be checked, if the server is reachable via it’s API. This could be done by issuing `osmo-remsim-apitool -H 192.168.243.100 -a` on any machine running Linux.

The output should contain:

```
/clients: {'clients': []}
/banks: {'banks': [{'peer': 'B1', 'state': 'CONNECTED_BANKD', 'component_id': {'type_': ' ↩
    remsimBankd', 'name': 'remsimbank', 'software': 'remsim-bankd', 'swVersion': '1.0.0.55- ↩
    bfcc.202310192026'}, 'bankId': 1, 'numberOfSlots': 2}]}
/slotmaps: {'slotmaps': []}
```

This shows, that the server is running, the bankd is connected to the server and provides two SIM-card slots.

8.3 remsimmodem RPi4

Connect the ngff-cardem with the two USB cables to the RPi 4. For bandwidth reasons use an USB3 port for the modem connection.

Depending on your modem, `lsusb` should contain two lines like:

```
root@remsimpi:~# lsusb
Bus 001 Device 005: ID 1d50:616e OpenMoko, Inc. ngff-cardem
Bus 001 Device 006: ID 03f0:581d HP, Inc lt4112 Gobi 4G Module Network Device
```

Install simtrace2-utils with `apt install simtrace2-utils`

Check with `simtrace2-list` if the cardem device is detected and it has loaded the right firmware (CardEmulator):

```
root@remsimpi:~# simtrace2-list
USB matches: 2
        1d50:616e Addr=8, Path=1-1.4, Cfg=1, Intf=0, Alt=0: 255/2/0 (CardEmulator Modem 1)
        1d50:616e Addr=8, Path=1-1.4, Cfg=2, Intf=0, Alt=0: 255/255/0 (0.8.1.58-773d ↩
            .202302240007)
```

This output provides you also with the parameters necessary for using osmo-remsim-client and osmo-remsim-tool e.g.

`simtrace2-tool -V 0x1d50 -P 0x616e -H 1-1.4 -I 0 -S 0 -C 1 modem reset cycle`

For the following installation of the modem, simtrace2-tool could also be used to switch between the onboard SIM card on the ngff-cardem PCB or the remote SIM.

8.3.1 Check modem funcionality

Note
This may differ depending on the modem of your choice. The complete setup a modem is not part of this document.

To have a working basis, it is recommended to first check the SIMcard you want to emulate with the SIM card slot directly connected to the modem.

After connecting to the modem via terminal, issuing an `at+cimi` command should return the IMSI of the SIM:

```
at+cimi
262034860345011
```

If you want to get the modem up and running e.g. to provide internet access, this is now the point to do so.

8.3.2 Install and configure osmo-remsim-client

```
apt install osmo-remsim-client-st2
```

Based on the above setup of the modem and the osmo-remsim-server, the osmo-remsim-client should be called with :

```
osmo-remsim-client-st2 -i 192.168.243.100 -V 0x1d50 -P 0x616e -H 1-1.4 -I 0 -S 0 -C 1
```

The output should show that the osmo-remsim-client is connected to the server.

This could be also checked via the API:

```
# osmo-remsim-apitool -H 192.168.243.100 -a
/clients: {'clients': [{'peer': 'C0:0', 'state': 'CONNECTED_CLIENT', 'component_id': {' ↩
    type_': 'remsimClient', 'name': 'remsimmodem', 'software': 'remsim-client', 'swVersion': ↩
     '1.0.0.55-bfcc.202310192026'}}]}
/banks: {'banks': [{'peer': 'B1', 'state': 'CONNECTED_BANKD', 'component_id': {'type_': ' ↩
    remsimBankd', 'name': 'remsimbank', 'software': 'remsim-bankd', 'swVersion': '1.0.0.55- ↩
    bfcc.202310192026'}, 'bankId': 1, 'numberOfSlots': 2}]}
/slotmaps: {'slotmaps': []}
```

Now, it is possible to map a SIM card to the osmo-remsim-client:

```
osmo-remsim-apitool -H 192.168.243.100 -m 1 0 0 0
```

If everything is setup correctly, `at+cimi` on the modem should show the IMSI of the mapped SIM card. If not, check the output of all programs above.

8.3.3 Finalize the setup

If everything is ok, the services can be started as systemd services. For osmo-remsim-bankd and osmo-remsim-server these services are already existing. For the osmo-remsim-client, the base service needs to be expanded:

```
systemctl enable osmo-remsim-client@0.service
```

9 Glossary

2FF
: 2nd Generation Form Factor; the so-called plug-in SIM form factor

3FF
: 3rd Generation Form Factor; the so-called microSIM form factor

3GPP
: 3rd Generation Partnership Project

4FF
: 4th Generation Form Factor; the so-called nanoSIM form factor

A Interface
: Interface between BTS and BSC, traditionally over E1 (*3GPP TS 48.008* [3gpp-ts-48-008])

A3/A8
: Algorithm 3 and 8; Authentication and key generation algorithm in GSM and GPRS, typically COMP128v1/v2/v3 or MILENAGE are typically used

A5
: Algorithm 5; Air-interface encryption of GSM; currently only A5/0 (no encryption), A5/1 and A5/3 are in use

Abis Interface
Interface between BTS and BSC, traditionally over E1 (*3GPP TS 48.058* [3gpp-ts-48-058] and *3GPP TS 52.021* [3gpp-ts-52-021])

ACC
Access Control Class; every BTS broadcasts a bit-mask of permitted ACC, and only subscribers with a SIM of matching ACC are permitted to use that BTS

AGCH
Access Grant Channel on Um interface; used to assign a dedicated channel in response to RACH request

AGPL
GNU Affero General Public License, a copyleft-style Free Software License

AQPSK
Adaptive QPSK, a modulation scheme used by VAMOS channels on Downlink

ARFCN
Absolute Radio Frequency Channel Number; specifies a tuple of uplink and downlink frequencies

AUC
Authentication Center; central database of authentication key material for each subscriber

BCCH
Broadcast Control Channel on Um interface; used to broadcast information about Cell and its neighbors

BCC
Base Station Color Code; short identifier of BTS, lower part of BSIC

BTS
Base Transceiver Station

BSC
Base Station Controller

BSIC
Base Station Identity Code; 16bit identifier of BTS within location area

BSSGP
Base Station Subsystem Gateway Protocol (*3GPP TS 48.018* [3gpp-ts-48-018])

BVCI
BSSGP Virtual Circuit Identifier

CBC
Cell Broadcast Centre; central entity of Cell Broadcast service

CBCH
Cell Broadcast Channel; used to transmit Cell Broadcast SMS (SMS-CB)

CBS
Cell Broadcast Service

CBSP
Cell Broadcast Service Protocol (*3GPP TS 48.049* [3gpp-ts-48-049])

CC
Call Control; Part of the GSM Layer 3 Protocol

CCCH
Common Control Channel on Um interface; consists of RACH (uplink), BCCH, PCH, AGCH (all downlink)

Cell
A cell in a cellular network, served by a BTS

CEPT
Conférence européenne des administrations des postes et des télécommunications; European Conference of Postal and Telecommunications Administrations.

CGI
Cell Global Identifier comprised of MCC, MNC, LAC and BSIC

CSFB
Circiut-Switched Fall Back; Mechanism for switching from LTE/EUTRAN to UTRAN/GERAN when circuit-switched services such as voice telephony are required.

dB
deci-Bel; relative logarithmic unit

dBm
deci-Bel (milliwatt); unit of measurement for signal strength of radio signals

DHCP
Dynamic Host Configuration Protocol (*IETF RFC 2131* [ietf-rfc2131])

downlink
Direction of messages / signals from the network core towards the mobile phone

DSCP
Differentiated Services Code Point (*IETF RFC 2474* [ietf-rfc2474])

DSP
Digital Signal Processor

dvnixload
Tool to program UBL and the Bootloader on a sysmoBTS

EDGE
Enhanced Data rates for GPRS Evolution; Higher-speed improvement of GPRS; introduces 8PSK

EGPRS
Enhanced GPRS; the part of EDGE relating to GPRS services

EIR
Equipment Identity Register; core network element that stores and manages IMEI numbers

ESME
External SMS Entity; an external application interfacing with a SMSC over SMPP

ETSI
European Telecommunications Standardization Institute

FPGA
Field Programmable Gate Array; programmable digital logic hardware

Gb
Interface between PCU and SGSN in GPRS/EDGE network; uses NS, BSSGP, LLC

GERAN
GPRS/EDGE Radio Access Network

GGSN
GPRS Gateway Support Node; gateway between GPRS and external (IP) network

GMSK
Gaussian Minimum Shift Keying; modulation used for GSM and GPRS

GPL
GNU General Public License, a copyleft-style Free Software License

Gp
Gp interface between SGSN and GGSN; uses GTP protocol

GPRS
General Packet Radio Service; the packet switched 2G technology

GPS
Global Positioning System; provides a highly accurate clock reference besides the global position

GSM
Global System for Mobile Communications. ETSI/3GPP Standard of a 2G digital cellular network

GSMTAP
GSM tap; pseudo standard for encapsulating GSM protocol layers over UDP/IP for analysis

GSUP
Generic Subscriber Update Protocol. Osmocom-specific alternative to TCAP/MAP

GT
Global Title; an address in SCCP

GTP
GPRS Tunnel Protocol; used between SGSN and GGSN

HLR
Home Location Register; central subscriber database of a GSM network

HNB-GW
Home NodeB Gateway. Entity between femtocells (Home NodeB) and CN in 3G/UMTS.

HPLMN
Home PLMN; the network that has issued the subscriber SIM and has his record in HLR

IE
Information Element

IMEI
International Mobile Equipment Identity; unique 14-digit decimal number to globally identify a mobile device, optionally with a 15th checksum digit

IMEISV
IMEI software version; unique 14-digit decimal number to globally identify a mobile device (same as IMEI) plus two software version digits (total digits: 16)

IMSI
International Mobile Subscriber Identity; 15-digit unique identifier for the subscriber/SIM; starts with MCC/MNC of issuing operator

IP
Internet Protocol (*IETF RFC 791* [ietf-rfc791])

IPA
ip.access GSM over IP protocol; used to multiplex a single TCP connection

Iu
Interface in 3G/UMTS between RAN and CN

IuCS
Iu interface for circuit-switched domain. Used in 3G/UMTS between RAN and MSC

IuPS
Iu interface for packet-switched domain. Used in 3G/UMTS between RAN and SGSN

LAC
Location Area Code; 16bit identifier of Location Area within network

LAPD
Link Access Protocol, D-Channel (*ITU-T Q.921* [itu-t-q921])

LAPDm
Link Access Protocol Mobile (*3GPP TS 44.006* [3gpp-ts-44-006])

LLC
Logical Link Control; GPRS protocol between MS and SGSN (*3GPP TS 44.064* [3gpp-ts-44-064])

Location Area
Location Area; a geographic area containing multiple BTS

LU
Location Updating; can be of type IMSI-Attach or Periodic. Procedure that indicates a subscriber's physical presence in a given radio cell.

M2PA
MTP2 Peer-to-Peer Adaptation; a SIGTRAN Variant (*RFC 4165* [ietf-rfc4165])

M2UA
MTP2 User Adaptation; a SIGTRAN Variant (*RFC 3331* [ietf-rfc3331])

M3UA
MTP3 User Adaptation; a SIGTRAN Variant (*RFC 4666* [ietf-rfc4666])

MCC
Mobile Country Code; unique identifier of a country, e.g. 262 for Germany

MFF
Machine-to-Machine Form Factor; a SIM chip package that is soldered permanently onto M2M device circuit boards.

MGW
Media Gateway

MM
Mobility Management; part of the GSM Layer 3 Protocol

MNC
Mobile Network Code; identifies network within a country; assigned by national regulator

MNCC
Mobile Network Call Control; Unix domain socket based Interface between MSC and external call control entity like osmo-sip-connector

MNO
Mobile Network Operator; operator with physical radio network under his MCC/MNC

MO
Mobile Originated. Direction from Mobile (MS/UE) to Network

MS
Mobile Station; a mobile phone / GSM Modem

MSC
Mobile Switching Center; network element in the circuit-switched core network

MSC pool
A number of redundant MSCs serving the same core network, which a BSC / RNC distributes load across; see also the "MSC Pooling" chapter in OsmoBSC's user manual [userman-osmobsc] and *3GPP TS 23.236* [3gpp-ts-23-236]

MSISDN
Mobile Subscriber ISDN Number; telephone number of the subscriber

MT
Mobile Terminated. Direction from Network to Mobile (MS/UE)

MTP
Message Transfer Part; SS7 signaling protocol (*ITU-T Q.701* [itu-t-q701])

MVNO
Mobile Virtual Network Operator; Operator without physical radio network

NCC
Network Color Code; assigned by national regulator

NITB
Network In The Box; combines functionality traditionally provided by BSC, MSC, VLR, HLR, SMSC functions; see OsmoNITB

NRI
Network Resource Indicator, typically 10 bits of a TMSI indicating which MSC of an MSC pool attached the subscriber; see also the "MSC Pooling" chapter in OsmoBSC's user manual [userman-osmobsc] and *3GPP TS 23.236* [3gpp-ts-23-236]

NSEI
NS Entity Identifier

NVCI
NS Virtual Circuit Identifier

NWL
Network Listen; ability of some BTS to receive downlink from other BTSs

NS
Network Service; protocol on Gb interface (*3GPP TS 48.016* [3gpp-ts-48-016])

OCXO
Oven Controlled Crystal Oscillator; very high precision oscillator, superior to a VCTCXO

OML
Operation & Maintenance Link (ETSI/*3GPP TS 52.021* [3gpp-ts-52-021])

OpenBSC
Open Source implementation of GSM network elements, specifically OsmoBSC, OsmoNITB, OsmoSGSN

OpenGGSN
Open Source implementation of a GPRS Packet Control Unit

OpenVPN
Open-Source Virtual Private Network; software employed to establish encrypted private networks over untrusted public networks

Osmocom
Open Source MObile COMmunications; collaborative community for implementing communications protocols and systems, including GSM, GPRS, TETRA, DECT, GMR and others

OsmoBSC
Open Source implementation of a GSM Base Station Controller

OsmoNITB
Open Source implementation of a GSM Network In The Box, combines functionality traditionally provided by BSC, MSC, VLR, HLR, AUC, SMSC

OsmoSGSN
Open Source implementation of a Serving GPRS Support Node

OsmoPCU
Open Source implementation of a GPRS Packet Control Unit

OTA
Over-The-Air; Capability of operators to remotely reconfigure/reprogram ISM/USIM cards

PC
Point Code; an address in MTP

PCH
Paging Channel on downlink Um interface; used by network to page an MS

PCP
Priority Code Point (*IEEE 802.1Q* [?])

PCU
Packet Control Unit; used to manage Layer 2 of the GPRS radio interface

PDCH
Packet Data Channel on Um interface; used for GPRS/EDGE signalling + user data

PIN
Personal Identification Number; a number by which the user authenticates to a SIM/USIM or other smart card

PLMN
Public Land Mobile Network; specification language for a single GSM network

PUK
PIN Unblocking Code; used to unblock a blocked PIN (after too many wrong PIN attempts)

RAC
Routing Area Code; 16bit identifier for a Routing Area within a Location Area

RACH
Random Access Channel on uplink Um interface; used by MS to request establishment of a dedicated channel

RAM
Remote Application Management; Ability to remotely manage (install, remove) Java Applications on SIM/USIM Card

RF
Radio Frequency

RFM
Remote File Management; Ability to remotely manage (write, read) files on a SIM/USIM card

Roaming
Procedure in which a subscriber of one network is using the radio network of another network, often in different countries; in some countries national roaming exists

Routing Area
Routing Area; GPRS specific sub-division of Location Area

RR
Radio Resources; Part of the GSM Layer 3 Protocol

RSL
Radio Signalling Link (*3GPP TS 48.058* [3gpp-ts-48-058])

RTP
Real-Time Transport Protocol (*IETF RFC 3550* [ietf-rfc3550]); Used to transport audio/video streams over UDP/IP

SACCH
Slow Associate Control Channel on Um interface; bundled to a TCH or SDCCH, used for signalling in parallel to active dedicated channel

SCCP
Signaling Connection Control Part; SS7 signaling protocol (*ITU-T Q.711* [itu-t-q711])

SDCCH
Slow Dedicated Control Channel on Um interface; used for signalling and SMS transport in GSM

SDK
Software Development Kit

SGs
Interface between MSC (GSM/UMTS) and MME (LTE/EPC) to facilitate CSFB and SMS.

SGSN
Serving GPRS Support Node; Core network element for packet-switched services in GSM and UMTS.

SIGTRAN
Signaling Transport over IP (*IETF RFC 2719* [ietf-rfc2719])

SIM
Subscriber Identity Module; small chip card storing subscriber identity

Site
A site is a location where one or more BTSs are installed, typically three BTSs for three sectors

SMPP
Short Message Peer-to-Peer; TCP based protocol to interface external entities with an SMSC

SMSC
Short Message Service Center; store-and-forward relay for short messages

SS7
Signaling System No. 7; Classic digital telephony signaling system

SS
Supplementary Services; query and set various service parameters between subscriber and core network (e.g. USSD, 3rd-party calls, hold/retrieve, advice-of-charge, call deflection)

SSH
Secure Shell; *IETF RFC 4250* [ietf-rfc4251] to 4254

SSN
Sub-System Number; identifies a given SCCP Service such as MSC, HLR

STP
Signaling Transfer Point; A Router in SS7 Networks

SUA
SCCP User Adaptation; a SIGTRAN Variant (*RFC 3868* [ietf-rfc3868])

syslog
System logging service of UNIX-like operating systems

System Information
A set of downlink messages on the BCCH and SACCH of the Um interface describing properties of the cell and network

TCH
Traffic Channel; used for circuit-switched user traffic (mostly voice) in GSM

TCP
Transmission Control Protocol; (*IETF RFC 793* [ietf-rfc793])

TFTP
Trivial File Transfer Protocol; (*IETF RFC 1350* [ietf-rfc1350])

TOS
Type Of Service; bit-field in IPv4 header, now re-used as DSCP (*IETF RFC 791* [ietf-rfc791])

TRX
Transceiver; element of a BTS serving a single carrier

TS
Technical Specification

u-Boot
Boot loader used in various embedded systems

UBI
An MTD wear leveling system to deal with NAND flash in Linux

UBL
Initial bootloader loaded by the TI Davinci SoC

UDP
User Datagram Protocol (*IETF RFC 768* [ietf-rfc768])

UICC
Universal Integrated Chip Card; A smart card according to *ETSI TR 102 216* [etsi-tr102216]

Um interface
U mobile; Radio interface between MS and BTS

uplink
Direction of messages: Signals from the mobile phone towards the network

USIM
Universal Subscriber Identity Module; application running on a UICC to provide subscriber identity for UMTS and GSM networks

USSD
Unstructured Supplementary Service Data; textual dialog between subscriber and core network, e.g. **100 → Your extension is 1234*

VAMOS
Voice services over Adaptive Multi-user channels on One Slot; an optional extension for GSM specified in Release 9 of 3GPP GERAN specifications (*3GPP TS 48.018* [3gpp-ts-48-018]) allowing two independent UEs to transmit and receive simultaneously on traffic channels

VCTCXO
Voltage Controlled, Temperature Compensated Crystal Oscillator; a precision oscillator, superior to a classic crystal oscillator, but inferior to an OCXO

VLAN
Virtual LAN in the context of Ethernet (*IEEE 802.1Q* [ieee-802.1q])

VLR
Visitor Location Register; volatile storage of attached subscribers in the MSC

VPLMN
Visited PLMN; the network in which the subscriber is currently registered; may differ from HPLMN when on roaming

VTY
Virtual TeletYpe; a textual command-line interface for configuration and introspection, e.g. the OsmoBSC configuration file as well as its telnet link on port 4242

A Bibliography / References

References

[1] [userman-ice1usb] Osmocom Project: icE1usb User Manual.

[2] [userman-ogt] Pau Espin: osmo-gsm-tester User Manual.

[3] [userman-remsim] Harald Welte: osmo-remsim User Manual.

[4] [osmobts-abis-spec] Neels Hofmeyr & Harald Welte. OsmoBTS Abis Protocol Specification. https://ftp.osmocom.org/docs/latest/osmobts-abis.pdf

[5] [userman-osmobsc] Osmocom Project: OsmoBSC User Manual. https://ftp.osmocom.org/docs/latest/osmobsc-usermanual.pdf

[6] [vty-ref-osmobsc] Osmocom Project: OsmoBSC VTY Reference Manual. https://ftp.osmocom.org/docs/-latest/osmobsc-vty-reference.pdf

[7] [userman-osmobts] Osmocom Project: OsmoBTS User Manual. https://ftp.osmocom.org/docs/latest/osmobts-usermanual.pdf

[8] [vty-ref-osmobts] Osmocom Project: OsmoBTS VTY Reference Manual. https://ftp.osmocom.org/docs/-latest/osmobts-trx-vty-reference.pdf https://ftp.osmocom.org/docs/latest/osmobts-sysmo-vty-reference.pdf https://ftp.osmocom.org/docs/latest/osmobts-lc15-vty-reference.pdf https://ftp.osmocom.org/docs/latest/-osmobts-oc2g-vty-reference.pdf https://ftp.osmocom.org/docs/latest/osmobts-octphy-vty-reference.pdf https://ftp.osmocom.org/docs/latest/osmobts-virtual-vty-reference.pdf

[9] [userman-osmocbc] Osmocom Project: OsmoCBC User Manual. https://ftp.osmocom.org/docs/latest/-osmocbc-usermanual.pdf

[10] [vty-ref-osmocbc] Osmocom Project: OsmoCBC VTY Reference Manual. https://ftp.osmocom.org/docs/-latest/osmocbc-vty-reference.pdf

[11] [userman-osmogbproxy] Osmocom Project: OsmoGBProxy User Manual. https://ftp.osmocom.org/docs/-latest/osmogbproxy-usermanual.pdf

[12] [vty-ref-osmogbproxy] Osmocom Project: OsmoGBPRoxy VTY Reference Manual. https://ftp.osmocom.org/-docs/latest/osmogbproxy-vty-reference.pdf

[13] [userman-osmoggsn] Osmocom Project: OpenGGSN User Manual. https://ftp.osmocom.org/docs/latest/-osmoggsn-usermanual.pdf

[14] [vty-ref-osmoggsn] Osmocom Project: OsmoGGSN VTY Reference Manual. https://ftp.osmocom.org/docs/-latest/osmoggsn-vty-reference.pdf

[15] [userman-osmohlr] Osmocom Project: OsmoHLR User Manual. https://ftp.osmocom.org/docs/latest/osmohlr-usermanual.pdf

[16] [vty-ref-osmohlr] Osmocom Project: OsmoHLR VTY Reference Manual. https://ftp.osmocom.org/docs/latest/-osmohlr-vty-reference.pdf

[17] [userman-osmohnbgw] Osmocom Project: OsmoHNBGW User Manual. https://ftp.osmocom.org/docs/latest/-osmohnbgw-usermanual.pdf

[18] [vty-ref-osmohnbgw] Osmocom Project: OsmoHNBGW VTY Reference Manual. https://ftp.osmocom.org/-docs/latest/osmohnbgw-vty-reference.pdf

[19] [userman-osmomgw] Osmocom Project: OsmoMGW User Manual. https://ftp.osmocom.org/docs/latest/-osmomgw-usermanual.pdf

[20] [vty-ref-osmomgw] Osmocom Project: OsmoMGW VTY Reference Manual. https://ftp.osmocom.org/docs/-latest/osmomgw-vty-reference.pdf

[21] [userman-osmomsc] Osmocom Project: OsmoMSC User Manual. https://ftp.osmocom.org/docs/latest/osmomsc-usermanual.pdf

[22] [vty-ref-osmomsc] Osmocom Project: OsmoMSC VTY Reference Manual. https://ftp.osmocom.org/docs/latest/osmomsc-vty-reference.pdf

[23] [userman-osmonitb] Osmocom Project: OsmoNITB User Manual. https://ftp.osmocom.org/docs/latest/osmonitb-usermanual.pdf

[24] [vty-ref-osmonitb] Osmocom Project: OsmoNITB VTY Reference Manual. https://ftp.osmocom.org/docs/latest/osmonitb-vty-reference.pdf

[25] [userman-osmopcu] Osmocom Project: OsmoPCU User Manual. https://ftp.osmocom.org/docs/latest/osmopcu-usermanual.pdf

[26] [vty-ref-osmopcu] Osmocom Project: OsmoPCU VTY Reference Manual. https://ftp.osmocom.org/docs/latest/osmopcu-vty-reference.pdf

[27] [userman-osmosgsn] Osmocom Project: OsmoSGSN User Manual. https://ftp.osmocom.org/docs/latest/osmosgsn-usermanual.pdf

[28] [vty-ref-osmosgsn] Osmocom Project: OsmoSGSN VTY Reference Manual. https://ftp.osmocom.org/docs/latest/osmosgsn-vty-reference.pdf

[29] [userman-osmosipconnector] Osmocom Project: OsmoSIPconnector User Manual. https://ftp.osmocom.org/docs/latest/osmosipconnector-usermanual.pdf

[30] [vty-ref-osmosipconnector] Osmocom Project: OsmoSIPconnector VTY Reference Manual. https://ftp.osmocom.org/docs/latest/osmosipconnector-vty-reference.pdf

[31] [userman-osmosmlc] Osmocom Project: OsmoSMLC User Manual. https://ftp.osmocom.org/docs/latest/osmosmlc-usermanual.pdf

[32] [vty-ref-osmosmlc] Osmocom Project: OsmoSMLC VTY Reference Manual. https://ftp.osmocom.org/docs/latest/osmosmlc-vty-reference.pdf

[33] [userman-osmostp] Osmocom Project: OsmoSTP User Manual. https://ftp.osmocom.org/docs/latest/osmostp-usermanual.pdf

[34] [vty-ref-osmostp] Osmocom Project: OsmoSTP VTY Reference Manual. https://ftp.osmocom.org/docs/latest/osmostp-vty-reference.pdf

[35] [userman-osmotrx] Osmocom Project: OsmoTRX User Manual. https://ftp.osmocom.org/docs/latest/osmotrx-usermanual.pdf

[36] [vty-ref-osmotrx] Osmocom Project: OsmoTRX VTY Reference Manual. https://ftp.osmocom.org/docs/latest/osmotrx-uhd-vty-reference.pdf https://ftp.osmocom.org/docs/latest/osmotrx-lms-vty-reference.pdf https://ftp.osmocom.org/docs/latest/osmotrx-ipc-vty-reference.pdf https://ftp.osmocom.org/docs/latest/osmotrx-usrp1-vty-reference.pdf

[37] [3gpp-ts-23-041] 3GPP TS 23.041: Technical realization of Cell Broadcast Service (CBS)

[38] [3gpp-ts-23-048] 3GPP TS 23.048: Security mechanisms for the (U)SIM application toolkit; Stage 2 https://www.3gpp.org/DynaReport/23048.htm

[39] [3gpp-ts-23-236] 3GPP TS 23.236: Intra-domain connection of Radio Access Network (RAN) nodes to multiple Core Network (CN) nodes https://www.3gpp.org/DynaReport/23236.htm

[40] [3gpp-ts-24-007] 3GPP TS 24.007: Mobile radio interface signalling layer 3; General Aspects https://www.3gpp.org/DynaReport/24007.htm

[41] [3gpp-ts-24-008] 3GPP TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols; Stage 3. https://www.3gpp.org/dynareport/24008.htm

[42] [3gpp-ts-31-101] 3GPP TS 31.101: UICC-terminal interface; Physical and logical characteristics https://www.3gpp.org/DynaReport/31101.htm

[43] [3gpp-ts-31-102] 3GPP TS 31.102: Characteristics of the Universal Subscriber Identity Module (USIM) application https://www.3gpp.org/DynaReport/31102.htm

[44] [3gpp-ts-31-103] 3GPP TS 31.103: Characteristics of the IMS Subscriber Identity Module (ISIM) application https://www.3gpp.org/DynaReport/31103.htm

[45] [3gpp-ts-31-111] 3GPP TS 31.111: Universal Subscriber Identity Module (USIM) Application Toolkit (USAT) https://www.3gpp.org/DynaReport/31111.htm

[46] [3gpp-ts-31-115] 3GPP TS 31.115: Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications https://www.3gpp.org/DynaReport/31115.htm

[47] [3gpp-ts-31-116] 3GPP TS 31.116: Remote APDU Structure for (U)SIM Toolkit applications https://www.3gpp.org/DynaReport/31116.htm

[48] [3gpp-ts-35-205] 3GPP TS 35.205: 3G Security; Specification of the MILENAGE algorithm set: General

[49] [3gpp-ts-35-206] 3GPP TS 35.206: 3G Security; Specification of the MILENAGE algorithm set: Algorithm specification https://www.3gpp.org/DynaReport/35206.htm

[50] [3gpp-ts-44-006] 3GPP TS 44.006: Mobile Station - Base Station System (MS - BSS) interface; Data Link (DL) layer specification https://www.3gpp.org/DynaReport/44006.htm

[51] [3gpp-ts-44-018] 3GPP TS 44.018: Mobile radio interface layer 3 specification; Radio Resource Control (RRC) protocol https://www.3gpp.org/DynaReport/44018.htm

[52] [3gpp-ts-44-064] 3GPP TS 44.064: Mobile Station - Serving GPRS Support Node (MS-SGSN); Logical Link Control (LLC) Layer Specification https://www.3gpp.org/DynaReport/44064.htm

[53] [3gpp-ts-45-002] 3GPP TS 45.002: Digital cellular telecommunications system (Phase 2+) (GSM); GSM/EDGE Multiplexing and multiple access on the radio path https://www.3gpp.org/DynaReport/45002.htm

[54] [3gpp-ts-48-008] 3GPP TS 48.008: Mobile Switching Centre - Base Station system (MSC-BSS) interface; Layer 3 specification https://www.3gpp.org/DynaReport/48008.htm

[55] [3gpp-ts-48-016] 3GPP TS 48.016: General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN) interface; Network service https://www.3gpp.org/DynaReport/48016.htm

[56] [3gpp-ts-48-018] 3GPP TS 48.018: General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN); BSS GPRS protocol (BSSGP) https://www.3gpp.org/DynaReport/48018.htm

[57] [3gpp-ts-48-049] 3GPP TS 48.049: Digital cellular communications system; Base Station Controller - Cell Broadcast Centre (BSC-CBC) interface specification; Cell Broadcast Service Protocol (CBSP) https://www.3gpp.org/DynaReport/48049.htm

[58] [3gpp-ts-48-056] 3GPP TS 48.056: Base Station Controller - Base Transceiver Station (BSC - BTS) interface; Layer 2 specification https://www.3gpp.org/DynaReport/48056.htm

[59] [3gpp-ts-48-058] 3GPP TS 48.058: Base Station Controller - Base Transceiver Station (BSC - BTS) Interface; Layer 3 specification https://www.3gpp.org/DynaReport/48058.htm

[60] [3gpp-ts-51-011] 3GPP TS 51.011: Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface

[61] [3gpp-ts-51-014] 3GPP TS 51.014: Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface https://www.3gpp.org/DynaReport/51014.htm

[62] [3gpp-ts-52-021] 3GPP TS 52.021: Network Management (NM) procedures and messages on the A-bis interface https://www.3gpp.org/DynaReport/52021.htm

[63] [etsi-tr102216] ETSI TR 102 216: Smart cards https://www.etsi.org/deliver/etsi_tr/102200_102299/102216/03.00.00_60/tr_102216v030000p.pdf

[64] [etsi-ts102221] ETSI TS 102 221: Smart Cards; UICC-Terminal interface; Physical and logical characteristics https://www.etsi.org/deliver/etsi_ts/102200_102299/102221/13.01.00_60/ts_102221v130100p.pdf

[65] [etsi-ts101220] ETSI TS 101 220: Smart Cards; ETSI numbering system for telecommunication application providers https://www.etsi.org/deliver/etsi_ts/101200_101299/101220/12.00.00_60/ts_101220v120000p.pdf

[66] [ieee-802.1q] IEEE 802.1Q: Bridges and Bridged Networks https://ieeexplore.ieee.org/document/6991462

[67] [ietf-rfc768] IETF RFC 768: User Datagram Protocol https://tools.ietf.org/html/rfc768

[68] [ietf-rfc791] IETF RFC 791: Internet Protocol https://tools.ietf.org/html/rfc791

[69] [ietf-rfc793] IETF RFC 793: Transmission Control Protocol https://tools.ietf.org/html/rfc793

[70] [ietf-rfc1035] IETF RFC 1035: Domain Names - Implementation and Specification https://tools.ietf.org/html/-rfc1035

[71] [ietf-rfc1350] IETF RFC 1350: Trivial File Transfer Protool https://tools.ietf.org/html/rfc1350

[72] [ietf-rfc2131] IETF RFC 2131: Dynamic Host Configuration Protocol https://tools.ietf.org/html/rfc2131

[73] [ietf-rfc2474] IETF RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv44 and IPv6 Headers https://tools.ietf.org/html/rfc2474

[74] [ietf-rfc2719] IETF RFC 2719: Signal Transport over IP https://tools.ietf.org/html/rfc2719

[75] [ietf-rfc3331] IETF RFC 3331: Message Transfer Part 2 User Adaptation Layer https://tools.ietf.org/html/-rfc3331

[76] [ietf-rfc3550] IETF RFC 3550: RTP: A Transport protocol for Real-Time Applications https://tools.ietf.org/-html/rfc3550

[77] [ietf-rfc3596] IETF RFC 3596: DNS Extensions to Support IP Version 6 https://tools.ietf.org/html/rfc3596

[78] [ietf-rfc3868] IETF RFC 3868: SCCP User Adaptation Layer https://tools.ietf.org/html/rfc3868

[79] [ietf-rfc4165] IETF RFC 4165: Message Transfer Part 2 Peer-to-Peeer Adaptation Layer https://tools.ietf.org/-html/rfc4165

[80] [ietf-rfc4251] IETF RFC 4251: The Secure Shell (SSH) Protocol Architecture https://tools.ietf.org/html/-rfc4251

[81] [ietf-rfc4666] IETF RFC 4666: Message Transfer Part 3 User Adaptation Layer https://tools.ietf.org/html/-rfc4666

[82] [ietf-rfc5771] IETF RFC 5771: IANA Guidelines for IPv4 Multicast Address Assignments https://tools.ietf.org/html/rfc5771

[83] [itu-t-q701] ITU-T Q.701: Functional Description of the Message Transfer Part (MTP) https://www.itu.int/rec/-T-REC-Q.701/en/

[84] [itu-t-q711] ITU-T Q.711: Functional Description of the Signalling Connection Control Part https://www.itu.int/rec/T-REC-Q.711/en/

[85] [itu-t-q713] ITU-T Q.713: Signalling connection control part formats and codes https://www.itu.int/rec/T-REC-Q.713/en/

[86] [itu-t-q714] ITU-T Q.714: Signalling connection control part procedures https://www.itu.int/rec/T-REC-Q.714/en/

[87] [itu-t-q921] ITU-T Q.921: ISDN user-network interface - Data link layer specification https://www.itu.int/rec/-T-REC-Q.921/en

[88] [smpp-34] SMPP Develoepers Forum. Short Message Peer-to-Peer Protocol Specification v3.4 https://docs.nimta.com/SMPP_v3_4_Issue1_2.pdf

[89] [gnu-agplv3] Free Software Foundation. GNU Affero General Public License. https://www.gnu.org/licenses/agpl-3.0.en.html

[90] [freeswitch_pbx] FreeSWITCH SIP PBX https://freeswitch.org