# sysmocom

sysmocom - s.f.m.c. GmbH



# osmo-remsim User Manual

by Harald Welte

DRAFT

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with the Invariant Sections being just 'Foreword', 'Acknowledgements' and 'Preface', with no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

| HISTORY | | | |
|---|---|---|---|
| NUMBER | DATE | DESCRIPTION | NAME |
| 1 | March 2019 | Initial version. | HW |
| 2 | December 2021 | Update manual to osmo-remsim v1.0.0 (logging, command line arguments) | HW |

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

# Contents

**1 Overview** **1**

1.1 About this manual . . . 1
1.2 About osmo-remsim . . . 1
1.3 Credits . . . 1
1.4 osmo-remsim-server . . . 1
1.5 osmo-remsim-client . . . 1
1.6 osmo-remsim-bankd . . . 2
1.7 osmo-remsim-apitool . . . 2
1.8 RSPRO . . . 2
1.9 RSRES . . . 2
1.10 Security . . . 2

**2 osmo-remsim-server** **3**

2.1 Running . . . 3
2.1.1 SYNOPSIS . . . 3
2.1.2 OPTIONS . . . 3
2.2 Logging . . . 3
2.3 RESTful/JSON Web API . . . 3
2.3.1 /api/backend/v1/clients . . . 3
2.3.2 /api/backend/v1/clients/:client_id . . . 4
2.3.3 /api/backend/v1/banks . . . 4
2.3.4 /api/backend/v1/banks/:bank_id . . . 4
2.3.5 /api/backend/v1/slotmaps . . . 4
2.3.6 /api/backend/v1/slotmaps/:slotmap_id . . . 4
2.3.7 /api/backend/v1/global-reset . . . 4
2.3.8 Examples . . . 4

**3 osmo-remsim-apitool** **5**

3.1 Usage . . . 5
3.1.1 Listing connected clients . . . 5
3.1.2 Listing connected bankds . . . 5
3.1.3 Listing installed slotmaps . . . 5
3.1.4 Listing all information . . . 5
3.1.5 Creating a slotmap . . . 6
3.1.6 Deleting a slotmap . . . 6
3.1.7 Reset all state . . . 6

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

**4 osmo-remsim-client-st2** **6**
4.1 Running . . . 7
4.1.1 SYNOPSIS . . . 7
4.1.2 OPTIONS . . . 7
4.1.3 Examples . . . 8
4.2 Logging . . . 8
4.3 Helper Script . . . 8
4.3.1 Script Environment Variables . . . 8
4.3.2 REMSIM_CAUSE values . . . 9

**5 osmo-remsim-client-shell** **9**
5.1 Running . . . 9
5.1.1 SYNOPSIS . . . 9
5.1.2 OPTIONS . . . 10
5.1.3 Examples . . . 10

**6 libifd_remsim_client** **11**
6.1 Configuration . . . 11

**7 osmo-remsim-bankd** **12**
7.1 Running . . . 13
7.1.1 SYNOPSIS . . . 13
7.1.2 OPTIONS . . . 13
7.1.3 Examples . . . 14
7.2 Logging . . . 14
7.3 `bankd_pcsc_slots.csv` CSV file . . . 14

**8 osmo-remsim logging** **15**
8.1 `-d` command line argument . . . 15
8.2 Example . . . 16

**9 RSPRO** **16**
9.1 Underlying Transport Layer . . . 17
9.2 RSPRO PDU . . . 17
9.3 RSPRO Operations . . . 17
9.3.1 ConnectBank . . . 17
9.3.2 ConnectClient . . . 17
9.3.3 CreateMapping . . . 17
9.3.4 RemoveMapping . . . 17
9.3.5 ConfigClientId . . . 17
9.3.6 ConfigClientBank . . . 17

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

9.3.7 ErrorInd . . . 18
9.3.8 SetAtr . . . 18
9.3.9 TpduModemToCard . . . 18
9.3.10 TpduCardToModem . . . 18
9.3.11 ClientSlotStatusInd . . . 18
9.3.12 BankSlotStatusInd . . . 18

**10 Glossary** **18**

**A Bibliography / References** **27**
A.0.0.0.1 References . . . 27

**B GNU Free Documentation License** **31**
B.1 PREAMBLE . . . 31
B.2 APPLICABILITY AND DEFINITIONS . . . 31
B.3 VERBATIM COPYING . . . 32
B.4 COPYING IN QUANTITY . . . 32
B.5 MODIFICATIONS . . . 33
B.6 COMBINING DOCUMENTS . . . 34
B.7 COLLECTIONS OF DOCUMENTS . . . 34
B.8 AGGREGATION WITH INDEPENDENT WORKS . . . 34
B.9 TRANSLATION . . . 35
B.10 TERMINATION . . . 35
B.11 FUTURE REVISIONS OF THIS LICENSE . . . 35
B.12 RELICENSING . . . 35
B.13 ADDENDUM: How to use this License for your documents . . . 36

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

# 1 Overview

## 1.1 About this manual

This manual should help you getting started with the osmo-remsim software.

It will cover aspects of configuration and running osmo-remsim as well as some introduction about its internal architecture and external interfaces.

## 1.2 About osmo-remsim

osmo-remsim is a suite of software programs enabling physical/geographic separation of a cellular phone (or modem) on the one hand side and the SIM/USIM/ISIM card on the other side.

Using osmo-remsim, you can operate an entire fleet of modems/phones, as well as banks of SIM cards and dynamically establish or remove the connections between modems/phones and cards.

So in technical terms, it behaves like a proxy for the ISO 7816 smart card interface between the MS/UE and the UICC/SIM/USIM/ISIM.

While originally designed to be used in context of cellular networks, there is nothing cellular specific in the system. It can therefore also be used with other systems that use contact based smart cards according to ISO 7816. Currently only the T=0 protocol with standard (non-extended) APDUs is supported. Both T=1 and extended APDU support can easily be added as a pure software update, should it be required at some future point.

## 1.3 Credits

osmo-remsim was originally developed by Harald Welte with contributions by Kevin Redon. It builds on top of pre-existing infrastructure of the Osmocom project, including the Osmocom SIMtrace project.

Development of osmo-remsim software was funded by GSMK and sysmocom.

## 1.4 osmo-remsim-server

The `osmo-remsim-server` is the central element of the osmo-remsim architecture. All other elements connect to it. It maintains the inventory of other network elements, as well as the list of slot-mappings, i.e. the relationship between each given physical card in a bank and each card emulator attached to a phone/modem.

The tasks of `osmo-remsim-server` include:

- accepting incoming TCP control connections from `osmo-remsim-client` and `osmo-remsim-bankd` instances
- providing a RESTful JSON interface for external application logic to

For more information, please see Section 2.

## 1.5 osmo-remsim-client

The `osmo-remsim-client` software is co-located next to the *user of the card* which traditionally is a phone or modem. However, there are other flavors of clients available, too. This is for example useful if existing software wants to interface remote smart cards, rather than those physically inserted into a local reader next to the PC running that application.

In the classic phone / modem use case, osmo-remsim-client typically runs on an [embedded] computer next to the phone/modem.

The tasks of `osmo-remsim-client` include:

- interaction with the user application. For phone/modem, that's over USB with a device supported by the *SIMtrace2 cardem* firmware, which provides the physical interface to the phone/modem SIM interface (ISO 7816-3).

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

- establishing a TCP connection with the osmo-remsim-server, in order to enable the server to issue control commands
- under control of osmo-remsim-server, establishing a TCP connection to a osmo-remsim-bankd in order to connect a card physically located at the bankd.

osmo-remsim-client supports at this point only one phone/modem. If you have multiple phones/modems at one location, you can simply run multiple instances of osmo-remsim-client on the same system, one for each phone/modem.

For more information, please see [?].

### 1.6 osmo-remsim-bankd

The osmo-remsim-bankd software is co-located next to a bank of SIM cards.

The tasks of osmo-remsim-bankd include:

- interaction with the actual card reader hardware. At this point, only PC/SC based readers are supported, with 1 to 255 slots per reader.
- establishing a TCP connection with the osmo-remsim-server, in order to enable the server to issue control commands
- running a TCP server where TCP connections from osmo-remsim-client instances are accepted and handled.

For more information, please see Section 7.

### 1.7 osmo-remsim-apitool

The osmo-remsim-apitool utility is an optional tool that can be used to manually interface with the RSRES interface of osmo-remsim-server in absence of a back-end system managing this.

For more information, please see Section 3.

### 1.8 RSPRO

RSPRO is the *R*emote *S*IM *PRO*tocol. It is a binary protocol specified in ASN.1 which is spoken on any of the internal connections between osmo-remsim-client, osmo-remsim-bankd and osmo-remsim-server.

You can find more information about RSPRO in Section 9.

### 1.9 RSRES

RSRES is the *R*emote *S*IM *RES*T protocol. It is an interface offered by osmo-remsim-server towards external back-end application logic of the operator of an osmo-remsim network.

You can find more information about RSRES in Section 2.3.

### 1.10 Security



**Warning**
RSPRO, RSRES and their underlying transport layer both operate in plain-text, There is no authentication or encryption built into the protocol. It is assumed that the protocols are only spoken over trusted, controlled IP networks, such as inside a VPN or a closed / private corporate network.

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

# 2 osmo-remsim-server

## 2.1 Running

`osmo-remsim-server` currently has no command-line arguments. It will bind to INADDR_ANY and offer the following TCP ports:

- Port 9998 for the inbound control connections from `osmo-remsim-client` and `osmo-remsim-bankd`
- Port 9997 for the RESTful/JSON Web API (role: HTTP server)

It is intended to make these settings (IP addresses, ports) configurable in future versions.

### 2.1.1 SYNOPSIS

**osmo-remsim-server** [-h] [-V] [-d LOGOPT]

### 2.1.2 OPTIONS

**-h, --help**
Print a short help message about the supported options

**-V, --version**
Print the software version number

**-d, --debug LOGOPT**
Configure the logging verbosity, see Section 8.

## 2.2 Logging

`osmo-remsim-server` currently logs to stderr only; the logging verbosity is configurable via command line argument only. However, as the libosmocore logging framework is used, extending this is an easy modification.

## 2.3 RESTful/JSON Web API

`osmo-remsim-server` provides a RESTful/JSON WEB API for application logic integration. The purpose of the API is to allow run-time configuration and monitoring of the entire osmo-remsim system.

The API currently has version 1, and the URL prefix is /api/backend/v1



**Warning**
The RESTful/JSON Web API operates in plain-text, There is no authentication or encryption built into the protocol. It is assumed that the protocol is only spoken over trusted, controlled IP networks, such as inside a VPN or a closed / private corporate network.

### 2.3.1 /api/backend/v1/clients

**GET** obtains a JSON list where each element represents one currently connected `osmo-remsim-client`.

No other HTTP operation is implemented.

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

#### 2.3.2 /api/backend/v1/clients/:client_id

**GET** obtains a single JSON object representing one specific currently connected `osmo-remsim-client`.

No other HTTP operation is implemented.

#### 2.3.3 /api/backend/v1/banks

**GET** obtains a JSON list where each element represents one currently connected `osmo-remsim-bankd`.

No other HTTP operation is implemented.

#### 2.3.4 /api/backend/v1/banks/:bank_id

**GET** obtains a single JSON object representing one specific currently connected `osmo-remsim-bankd`.

No other HTTP operation is implemented.

#### 2.3.5 /api/backend/v1/slotmaps

**GET** obtains a JSON list where each element represents one provisioned slot mapping.

**POST** creates a new slot mapping as specified in the JSON syntax contained in the HTTP body.

No other HTTP operation is implemented.

#### 2.3.6 /api/backend/v1/slotmaps/:slotmap_id

**DELETE** deletes a slot mapping by its identifier. If the mapping is currently in use, the related bankd is instructed to disconnect the client from the card.

No other HTTP operation is implemented.

#### 2.3.7 /api/backend/v1/global-reset

**POST** performs a global reset of the `osmo-remsim-server` state. This means all mappings are removed.

#### 2.3.8 Examples

**remsim-server is on 10.2.3.4, one simbank with 5 cards: http://10.2.3.4:9997/api/backend/v1/banks**


```
{"banks":[{"peer":"B1","state":"CONNECTED_BANKD","component_id":{"type_":"remsimBankd"," ↩
    name":"fixme-name","software":"remsim-bankd","swVersion":"0.1.0.17-6d8a"},"bankId":1," ↩
    numberOfSlots":5}]}
```


**remsim-server is on 10.2.3.4, 4 clients: http://10.2.3.4:9997/api/backend/v1/clients**


```
{"clients":[{"peer":"C0:2","state":"CONNECTED_CLIENT","component_id":{"type_":"remsimClient ↩
    ","name":"simtrace2-remsim-client","software":"remsim-client","swVersion":"0.1.0.17-6d8a ↩
    "}},{"peer":"C0:0","state":"CONNECTED_CLIENT","component_id":{"type_":"remsimClient"," ↩
    name":"simtrace2-remsim-client","software":"remsim-client","swVersion":"0.1.0.17-6d8a ↩
    "}},{"peer":"C0:3","state":"CONNECTED_CLIENT","component_id":{"type_":"remsimClient"," ↩
    name":"simtrace2-remsim-client","software":"remsim-client","swVersion":"0.1.0.17-6d8a ↩
    "}},{"peer":"C0:1","state":"CONNECTED_CLIENT","component_id":{"type_":"remsimClient"," ↩
    name":"simtrace2-remsim-client","software":"remsim-client","swVersion":"0.1.0.17-6d8a ↩
    "}}]}
```


Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

# 3 osmo-remsim-apitool

`osmo-remsim-apitool` is a small python script whic can be used to manually control `osmo-remsim-server` via its RESTful interface in setups where no external back-end application is controlling this interface.

For more information about The RESTful inteface, see [?].

## 3.1 Usage

Common command line arguments that can be used with any of the commands below:

**-H, --host HOST**
Specify the hostname / IP of the `osmo-remsim-server` to connect to. Default: localhost

**-P, --port PORT**
Specify the remote TCP port of the RSRES interface of `osmo-remsim-server`. Default: 9997 **-v, --verbose** Increase verbosity of output: Show the GET request generated, not just the response.

### 3.1.1 Listing connected clients

The command `osmo-remsim-apitool -c` can be used to list all currently connected clients.

```
$ osmo-remsim-apitool -c
/clients: {'clients': [{'peer': 'C23:0', 'state': 'CONNECTED_CLIENT', 'component_id': {' ↩
    type_': 'remsimClient', 'name': 'nataraja', 'software': 'remsim-client', 'swVersion':  ↩
    '0.2.2.63-844b'}}]}
```

### 3.1.2 Listing connected bankds

The command `osmo-remsim-apitool -b` can be used to list all currently connected bankds.

```
$ osmo-remsim-apitool -b
/banks: {'banks': [{'peer': 'B1', 'state': 'CONNECTED_BANKD', 'component_id': {'type_': ' ↩
    remsimBankd', 'name': 'fixme-name', 'software': 'remsim-bankd', 'swVersion':  ↩
    '0.2.2.46-3598'}, 'bankId': 1, 'numberOfSlots': 5}]}
```

### 3.1.3 Listing installed slotmaps

The command `osmo-remsim-apitool -s` can be used to list all currently installed slotmaps.

```
$ osmo-remsim-apitool -s
/slotmaps: {'slotmaps': [{'bank': {'bankId': 1, 'slotNr': 1}, 'client': {'clientId': 23, ' ↩
    slotNr': 0}, 'state': 'ACTIVE'}]}
```

### 3.1.4 Listing all information

The command `osmo-remsim-apitool -a` can be used to list all information (clients, bankds, slotmaps).

```
$ osmo-remsim-apitool -a
/clients: {'clients': [{'peer': 'C23:0', 'state': 'CONNECTED_CLIENT', 'component_id': {' ↩
    type_': 'remsimClient', 'name': 'nataraja', 'software': 'remsim-client', 'swVersion':  ↩
    '0.2.2.63-844b'}}]}
/banks: {'banks': [{'peer': 'B1', 'state': 'CONNECTED_BANKD', 'component_id': {'type_': ' ↩
    remsimBankd', 'name': 'fixme-name', 'software': 'remsim-bankd', 'swVersion':  ↩
    '0.2.2.46-3598'}, 'bankId': 1, 'numberOfSlots': 5}]}
/slotmaps: {'slotmaps': [{'bank': {'bankId': 1, 'slotNr': 1}, 'client': {'clientId': 23, ' ↩
    slotNr': 0}, 'state': 'ACTIVE'}]}
```

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

### 3.1.5 Creating a slotmap

The command `osmo-remsim-apitool -m bank_id bankd_slot client_id client_slot` can be used to create a new slotmap.

**Create a slotmap between Bankd 1 Slot a (B1:1) and Client 23 Slot 0 (C23:0)**

```
$ osmo-remsim-apitool -m 1 1 23 0
```

### 3.1.6 Deleting a slotmap

The command `osmo-remsim-apitool -d bank_id bank_slot` can be used to create a new slotmap.

**Remove a slotmap for Bankd 1 Slot a (B1:1)**

```
$ osmo-remsim-apitool -m 1 1
```

### 3.1.7 Reset all state

The command `osmo-remsim-apitool -r` can be used to reset all state in bankd, including all slotmaps.

```
$ osmo-remsim-apitool -r
```



**Warning**
Use with extreme caution, particularly in production environments.

# 4 osmo-remsim-client-st2

The client interfaces with GSM phones / modems via dedicated "Card Emulation" devices such as the Osmocom SIMtrace2 or sysmocom sysmoQMOD board + firmware. This hardware implements the ISO7816-3 electrical interface and protocol handling and passes any TPDU headers received from the phone/modem to `osmo-remsim-client` for further processing of the TPDUs associated to the given APDU transfer.

`osmo-remsim-client` connects via a RSPRO control connection to `osmo-remsim-server` at startup and registers itself. It will receive configuration data such as the `osmo-remsim-bankd` IP+Port and the ClientId from `osmo-remsim-server`.

After receiving the configuration, `osmo-remsim-client` will establish a RSPRO data connection to the `osmo-remsim-bankd` IP:Port.

As the USB interface for remote SIM in simtrace2.git uses one interface per slot, we can implement the client in blocking mode, i.e. use blocking I/O on the TCP/RSPRO side. This simplifies the code compared to a more complex async implementation.

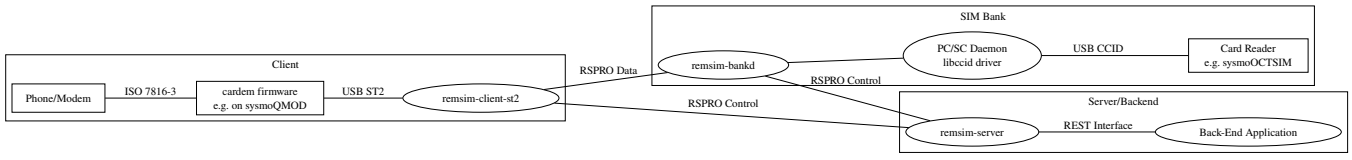



Figure 1: Overall osmo-remsim architecture using osmo-remsim-client-st2

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

## 4.1 Running

osmo-remsim-client-st2 currently has the following command-line options:

### 4.1.1 SYNOPSIS

**osmo-remsim-client-st2** [. . . ]

### 4.1.2 OPTIONS

**-h, --help**
Print a short help message about the supported options

**-V, --version**
Print the software version number

**-d, --debug LOGOPT**
Configure the logging verbosity, see Section 8.

**-i, --server-ip A.B.C.D**
Specify the remote IP address / hostname of the `osmo-remsim-server` to which this client shall establish its RSPRO control connection

**-p, --server-port <1-65535>**
Specify the remote TCP port number of the `osmo-remsim-server` to which this client shall establish its RSPRO control connection

**-c, --client-id <1-1023>**
Specify the numeric client identifier of the SIM bank this bankd instance operates. The tuple of client-id and client-slot must be unique among all clients connecting to the same `osmo-remsim-server`.

**-n, --client-slot <0-1023>**
Specify the slot number served within this client. The tuple of client-id and client-slot must be unique among all clients connecting to the same `osmo-remsim-server`.

**-a, --atr HEXSTRING**
Specify the initial ATR to be communicated to the modem/phone. Can and will later be overridden by the ATR as specified by `osmo-remsim-bankd` once a card has been mapped to this client, unless the `--atr-ignore-rspro` option is also specified.

**-r, --atr-ignore-rspro**
Ignore any incoming RSPRO setAtrReq and always only use the locally-specified ATR when communicating with the UE/modem/phone. This can be used to constrain the capabilities advertised. This way, for example, the baud rate can be constrained, or the use of logical channels prevented.

**-e, --event-script COMMAND**
Specify the shell command to be execute when the client wants to call its helper script

**-V, --usb-vendor**
Specify the USB Vendor ID of the USB device served by this client, use e.g. 0x1d50 for SIMtrace2, sysmoQMOD and OWHW.

**-P, --usb-product**
Specify the USB Product ID of the USB device served by this client, use e.g. 0x4004 for sysmoQMOD.

**-C, --usb-config**
Specify the USB Cofiguration number of the USB device served by this client. Default will use current configuration of the device.

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

**-I, --usb-interface**
Specify the USB Interface number (within active configuration) of the USB device served by this client. Default will use FIXME.

**-S, --usb-altsetting**
Specify the USB Alternate Setting to be used within the USB Interface of the USB device served by this client. Default will use FIXME.

**-A, --usb-address <0-255>**
Specify the USB Address of the USB device served by this client. This is useful in case multiple identical USB devices are attached to the same host. However, the address changed at every re-enumeration and it's therefor recommended to use the USB path (see below).

**-H, --usb-path**
Specify the USB path of the USB device served by this client. This is usefule to disambiguate between multiple identical USB devices attached to the same host. You don't need this if you have only one SIM emulation device attached to your system.

#### 4.1.3 Examples

**remsim-server is on 10.2.3.4, sysmoQMOD on usb bus, all 4 modems:**

```
osmo-remsim-client-st2 -s 10.2.3.4 -V 1d50 -P 4004 -C 1 -I 0 -H 2-1.1 -c 0 -n 0
osmo-remsim-client-st2 -s 10.2.3.4 -V 1d50 -P 4004 -C 1 -I 1 -H 2-1.1 -c 0 -n 1
osmo-remsim-client-st2 -s 10.2.3.4 -V 1d50 -P 4004 -C 1 -I 0 -H 2-1.4 -c 0 -n 2
osmo-remsim-client-st2 -s 10.2.3.4 -V 1d50 -P 4004 -C 1 -I 1 -H 2-1.4 -c 0 -n 3
```

### 4.2 Logging

`osmo-remsim-client` currently logs to stdout only, and the logging verbosity is not yet configurable. However, as the libosmocore logging framework is used, extending this is an easy modification.

### 4.3 Helper Script

`osmo-remsim-client` can call an external shell command / script / program at specific instances of time. This serves two purposes:

- To keep external system integration posted about the overall status of remsim-client, such as whether or not it is connected to a server and/or bankd.
- To request the external system to perform specific actions, such as triggering the reset of the modem - in case the hardware doesn't allow the simtrace2 firmware to do that itself.

#### 4.3.1 Script Environment Variables

The environment passed to the helper script contains a number of variables to provide inormation to the external script:

Table 2: Environment Variables

| Name | Example Value | Description |
|---|---|---|
| REMSIM_CLIENT_VERSION | 0.2.2.37-5406a | Compile version of the software |
| REMSIM_SERVER_ADDR | 1.2.3.4:1234 | Address and port of the remsim-server |
| REMSIM_SERVER_STATE | CONNECTED | FSM state of the connection to remsim-server |
| REMSIM_BANKD_ADDR | 1.2.3.4:1234 | Address and port of the remsim-bankd |

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

Table 2: (continued)

| Name | Example Value | Description |
|---|---|---|
| REMSIM_BANKD_STATE | CONNECTED | FSM state of the connection to remsim-bankd |
| REMSIM_CLIENT_SLOT | 23:42 | Client ID and Client Slot Number |
| REMSIM_BANKD_SLOT | 55:33 | Bank ID and Bank Slot Number |
| REMSIM_USB_PATH | 2-1.1 | USB path of the USB device with simtrace2 cardem firmware |
| REMSIM_USB_INTERFACE | 1 | Interface number of the USB device with simtrace2 cardem firmware |
| REMSIM_SIM_VCC | 1 | Whether or not the modem currently applies SIM VCC (0/1) |
| REMSIM_SIM_RST | 1 | Whether or not the modem currently asserts SIM RST (0=inactive, 1=active) |
| REMSIM_CAUSE | request-card-insert | The cause why this script has been called |

#### 4.3.2 REMSIM_CAUSE values

The REMSIM_CAUSE environment variable (as well as the first argument) passed to the helper script indicated why the script has been called.

| Name | Description |
|---|---|
| event-modem-status | The SIM card interface status has changed (e.g. VCC/RST change) |
| event-bankd-connect | A logical RSPRO connection to a bankd has been established |
| event-server-connect | A logical RSPRO connection to a server has been established |
| event-config-bankd | The server has instructed the client of the bankd address |
| request-card-insert | The client asks the system to simulate SIM card insertion to the modem |
| request-card-remove | The client asks the system to simulate SIM card removal from the modem |
| request-sim-remote | The client asks the system to switch to remote SIM |
| request-sim-local | The client asks the system to switch to local SIM |
| request-modem-reset | The client asks the system to perform a modem reset |

# 5 osmo-remsim-client-shell

This is a remsim-client that's mostly useful for manual debugging/testing or automatic testing.

Instead of using hardware like the SIMtrace with cardem firmware to interface a virtual SIM card to a real phone or modem, it simply offers and interactive way to exchange APDUs with a remote SIM card via STDIO of the process.

This allows testing of large parts of the osmo-remsim-client code as well as the integration with the overall osmo-remsim network including osmo-remsim-server, osmo-remsim-bankd and any external backend application driving the REST interface.

## 5.1 Running

osmo-remsim-client-shell currently has the following command-line options:

#### 5.1.1 SYNOPSIS

**osmo-remsim-client-shell** [. . . ]

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

#### 5.1.2 OPTIONS

**-h, --help**
Print a short help message about the supported options

**-v, --version**
Print the compile-time version information

**-d, --debug LOGOPT**
Configure the logging verbosity, see Section 8.

**-i, --server-ip A.B.C.D**
Specify the remote IP address / hostname of the `osmo-remsim-server` to which this client shall establish its RSPRO control connection

**-p, --server-port <1-65535>**
Specify the remote TCP port number of the `osmo-remsim-server` to which this client shall establish its RSPRO control connection

**-c, --client-id <1-1023>**
Specify the numeric client identifier of the SIM bank this bankd instance operates. The tuple of client-id and client-slot must be unique among all clients connecting to the same `osmo-remsim-server`.

**-n, --client-slot <0-1023>**
Specify the slot number served within this client. The tuple of client-id and client-slot must be unique among all clients connecting to the same `osmo-remsim-server`. `osmo-remsim-bankd` once a card has been mapped to this client.

**-e, --event-script COMMAND**
Specify the shell command to be execute when the client wants to call its helper script

#### 5.1.3 Examples

The below example uses stderr-redirection to avoid the log output cluttering the console.

**remsim-server is at 192.168.11.10; we are client 23 slot 0**

```
./osmo-remsim-client-shell -i 192.168.11.10 -c 23  2>/dev/null
SET_ATR: 3b 00
SET_ATR: 3b 7d 94 00 00 55 55 53 0a 74 86 93 0b 24 7c 4d 54 68
a0a40000023f00
R-APDU: 9f 17
```

- The first SET_ATR is performed by osmo-remsim-client locally using a default ATR
- The second SET_ATR is performed by osmo-remsim-bankd to inform us about the ATR of the real remote card
- The `a0a40000023f00` is a command TPDU entered on STDIN by the suer
- The `9f17` is a response TPDU provided by the remote card in response to the command

The program continues in this loop (read command APDU as hex-dump from stdin; provide response on stdout) until it is terminated by Ctrl+C or by other means.

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

# 6 libifd_remsim_client

This is a remsim-client implemented as so-called `ifd_handler`, i.e. a card reader driver that plugs into the bottom side of the PC/SC daemon of pcsc-lite.

Using this library, you can use normal smart card application programs with remote smart cards managed by osmo-remsim. The setup looks like this:

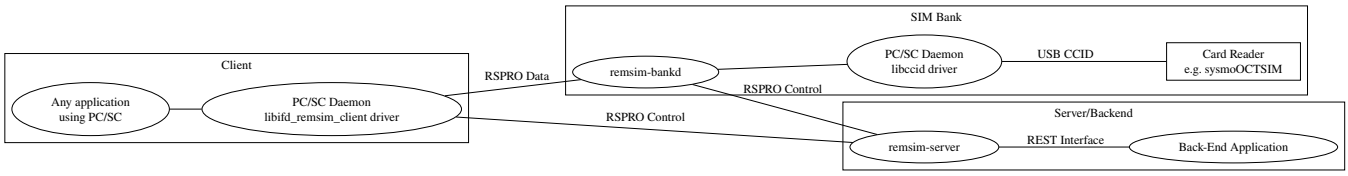



Figure 2: Overall osmo-remsim architecture using libifd_remsim_client

## 6.1 Configuration

Like all non-USB PC/SC reader drivers, this is happening in `/etc/reader.conf` or, at least on Debian GNU/Linux based systems via files in `/etc/reader.conf.d`. The osmo-remsim software includes an example configuration file and installs it as `osmo-remsim-client-reader_conf` in that directory.

**contents of the configuration example provided by osmo-remsim-client**

```
#FRIENDLYNAME "osmo-remsim-client"
#DEVICENAME   0:0:192.168.11.10:9998
#LIBPATH /usr/lib/pcsc/drivers/libifd-osmo-remsim-client.bundle/Contents/Linux/ ↩
    libifd_remsim_client.so
```

As you can see, all lines are commented out by default. In order to enable the remsim-client virtual reader, you need to

- remove the # character on all three lines
- configure the DEVICNAME according to your local configuration. It is a string with fields separated by colons, in the form of CLIENT_ID:CLIENT_SLOT:SERVER_IP:SERVER_PORRT
  - First part is the Client ID (default: 0)
  - Second part is the Client SlotNumbera (default: 0)
  - Third part is the IP address of the `osmo-resim-server` (default: localhost)
  - Last part is the RSPRO TCP port of the `osmo-remsim-server` (default: 9998)

Once the configuration file has been updated, you should re-start pcscd by issuing `systemctl restart pcscd` or whatever command your Linux distribution uses for restarting services.

You can check if the driver is loaded by using the `pcsc_scan` tool included with `pcscd`:

```
$ pcsc_scan
Using reader plug'n play mechanism
Scanning present readers...
0: osmo-remsim-client 00 00

Wed Mar  4 13:31:42 2020
 Reader 0: osmo-remsim-client 00 00
  Event number: 0
  Card state: Card removed,
 -
```

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

Once a proper slotmap to an existing SIM card in a remote bank daemon has been installed in the server, you should see something like this:

```
$ pcsc_scan
Using reader plug'n play mechanism
Scanning present readers...
0: osmo-remsim-client 00 00

Wed Mar  4 13:35:18 2020
 Reader 0: osmo-remsim-client 00 00
  Event number: 1
  Card state: Card inserted,
  ATR: 3B 7D 94 00 00 55 55 53 0A 74 86 93 0B 24 7C 4D 54 68

ATR: 3B 7D 94 00 00 55 55 53 0A 74 86 93 0B 24 7C 4D 54 68
+ TS = 3B --> Direct Convention
+ T0 = 7D, Y(1): 0111, K: 13 (historical bytes)
  TA(1) = 94 --> Fi=512, Di=8, 64 cycles/ETU
    62500 bits/s at 4 MHz, fMax for Fi = 5 MHz => 78125 bits/s
  TB(1) = 00 --> VPP is not electrically connected
  TC(1) = 00 --> Extra guard time: 0
+ Historical bytes: 55 55 53 0A 74 86 93 0B 24 7C 4D 54 68
  Category indicator byte: 55 (proprietary format)

Possibly identified card (using /home/laforge/.cache/smartcard_list.txt):
        NONE
```

From now on, you can use any application using PC/SC, whether C, Python or Java with a remote SIM card managed by osmo-remsim.

# 7 osmo-remsim-bankd

The `osmo-remsim-bankd` (SIM Bank Daemon) manages one given SIM bank. The initial implementation supports a PC/SC driver to expose any PC/SC compatible card readers as SIM bank.

`osmo-remsim-bankd` initially connects via a RSPRO control connection to `osmo-remsim-server` at startup, and will in turn receive a set of initial [client,slot]:[bankd,slot] mappings. These mappings determine which slot on the client (corresponding to a modem) is mapped to which slot on the SIM bank. Mappings can be updated by `osmo-remsim-server` at any given point in time.

`osmo-remsim-bankd` implements a RSPRO server, where it listens to connections from `osmo-remsim-clients`.

As PC/SC only offers a blocking API, there is one thread per PC/SC slot. This thread will perform blocking I/O on the socket towards the client, and blocking API calls on PC/SC.

In terms of thread handling, we do:

- accept() handling in [spare] worker threads
  - this means blocking I/O can be used, as each worker thread only has one TCP connection
  - client identifies itself with client:slot
  - lookup mapping based on client:slot (using mutex for protection)
  - open the reader based on the lookup result

The worker threads initially don't have any mapping to a specific reader, and that mapping is only established at a later point after the client has identified itself. The advantage is that the entire bankd can live without any non-blocking I/O.

The main thread handles the connection to `osmo-remsim-server`, where it can also use non-blocking I/O. However, re-connection would be required, to avoid stalling all banks/cards in the event of a connection loss to the server.

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

worker threads have the following states: * INIT (just started) * ACCEPTING (they're blocking in the accept() call on the server socket fd) * CONNECTED_WAIT_ID (TCP established, but peer not yet identified itself) * CONNECTED_CLIENT (TCP established, client has identified itself, no mapping) * CONNECTED_CLIENT_MAPPED (TCP established, client has identified itself, mapping exists) * CONNECTED_CLIENT_MAPPED_CARD (TCP established, client identified, mapping exists, card opened) * CONNECTED_SERVER (TCP established, server has identified itself)

Once the client disconnects, or any other error occurs (such as card I/O errors), the worker thread either returns to INIT state (closing client socket and reader), or it terminates. Termination would mean that the main thread would have to do non-blocking join to detect client termination and then re-spawn clients, so the "return to INIT state" approach seems to make more sense.

## 7.1 Running

`osmo-remsim-bankd` currently has the following command-line options:

### 7.1.1 SYNOPSIS

**osmo-remsim-bankd** [-h] [-V] [-d LOGOPT] -i A.B.C.D [-p <1-65535>] [-b <1-1023>] [-n <1-1023>] [-I A.B.C.D] [-P <1-65535> ]

### 7.1.2 OPTIONS

**-h, --help**
Print a short help message about the supported options

**-V, --version**
Print the software version number

**-d, --debug LOGOPT**
Configure the logging verbosity, see Section 8.

**-i, --server-host A.B.C.D**
Specify the remote IP address/hostname of the `osmo-remsim-server` to which this bankd shall establish its RSPRO control connection. Do not specify a loopback address or localhost, as this would in most cases result in a broken configuration where a [usually remote] remsim-client attempts to reach the bankd via loopback, which doesn't work.

**-p, --server-port <1-65535>**
Specify the remote TCP port number of the `osmo-remsim-server` to which this bankd shall establish its RSPRO control connection

**-b, --bank-id <1-1023>**
Specify the numeric bank identifier of the SIM bank this bankd instance operates. Must be unique among all banks connecting to the same `osmo-remsim-server`.

**-n, --num-slots <1-1023>**
Specify the number of slots that this bankd handles.

**-I, --bind-IP A.B.C.D**
Specify the local IP address to which the socket for incoming connections from `osmo-remsim-clients` is bound to.

**-P, --bind-port <1-65535>**
Specify the local TCP port to which the socket for incoming connections from `osmo-remsim-client`s is bound to.

**-s, --permit-shared-pcsc**
Specify whether the PC/SC readers should be accessed in SCARD_SHARE_SHARED mode, instead of the default (SCARD_SHARE_EXCLUSIVE). Shared mode would permit multiple application programs to access a single reader/slot/card concurrently. This is potentially dangerous as the two programs operate without knowledge of each other, and either of them might modify the card state (such as the currently selected file, validated PIN, etc.) in a way not expected by the other application.

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

**-g, --gsmtap-ip A.B.C.D**
Enable GSMTAP and send APDU traces to given IP.

**-G, --gsmtap-slot <0-1023>**
Limit tracing to given bank slot, only (default: all slots).

**-L, --disable-color**
Disable colors for logging to stderr.

**-T, --timestamp**
Prefix every log line with a timestamp.

**-e, --log-level number**
Set a global loglevel for all logging.

#### 7.1.3 Examples

**remsim-server is on 10.2.3.4, cardreader has 5 slots:**

```
osmo-remsim-bankd -i 10.2.3.4 -n 5
```

**remsim-server is on 10.2.3.4, cardreader has 4 slots, local ip is 10.5.4.3**

```
osmo-remsim-bankd -i 10.2.3.4 -n 4 -I 10.5.4.3
```

### 7.2 Logging

`osmo-remsim-bankd` currently logs to stdout only, and the logging verbosity is not yet configurable. However, as the libosmocore logging framework is used, extending this is an easy modification.

### 7.3 `bankd_pcsc_slots.csv` CSV file

bankd expects a CSV file `bankd_pcsc_slots.csv` in the current working directory at startup.

This CSV file specifies the mapping between the string names of the PCSC readers and the RSPRO bandk/slot numbers. The format is as follows:

- first column: bankd number
- second column: slot number within bankd
- third column: extended POSIX regular expression matching the slot

**Example: CSV file mapping bankd slots 0..4 to an ACS ACR33U-A1 reader slots**

```
"1","0","ACS ACR33 ICC Reader 00 00"
"1","1","ACS ACR33 ICC Reader 00 01"
"1","2","ACS ACR33 ICC Reader 00 02"
"1","3","ACS ACR33 ICC Reader 00 03"
"1","4","ACS ACR33 ICC Reader 00 04"
```

You can obtain the exact string to use as PC/SC reader name from the output of the `pcsc_scan` utility (part of pcsc-lite package). The tool will produce output like:

**Example: Output of pcsc_scan utility on a system with a single reader installed**

```
Scanning present readers...
0: Alcor Micro AU9560 00 00
```

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

In this example, there's only a single PC/SC reader available, and it has a string of "Alcor Micro AU9560 00 00" which needs to be used in the CSV file.

**NOTE**

If the reader name contains any special characters, they might need to be escaped according to the extended POSIX regular expression syntax. See `man 7 regex` for a reference.

**Example: CSV file mapping bankd slots 0..7 to a sysmoOCTSIM:**

```
"1","0","sysmocom sysmoOCTSIM \[CCID\] \(ab19180f3335355320202034463a15ff\) [0-9]{2} 00"
"1","1","sysmocom sysmoOCTSIM \[CCID\] \(ab19180f3335355320202034463a15ff\) [0-9]{2} 01"
"1","2","sysmocom sysmoOCTSIM \[CCID\] \(ab19180f3335355320202034463a15ff\) [0-9]{2} 02"
"1","3","sysmocom sysmoOCTSIM \[CCID\] \(ab19180f3335355320202034463a15ff\) [0-9]{2} 03"
"1","4","sysmocom sysmoOCTSIM \[CCID\] \(ab19180f3335355320202034463a15ff\) [0-9]{2} 04"
"1","5","sysmocom sysmoOCTSIM \[CCID\] \(ab19180f3335355320202034463a15ff\) [0-9]{2} 05"
"1","6","sysmocom sysmoOCTSIM \[CCID\] \(ab19180f3335355320202034463a15ff\) [0-9]{2} 06"
"1","7","sysmocom sysmoOCTSIM \[CCID\] \(ab19180f3335355320202034463a15ff\) [0-9]{2} 07"
```

In the above example, the `\[CCID\]` and the `\(serialnumber\)` both had to be escaped.

The `[0-9]{2}` construct exists to perform wildcard matching, no matter which particular two-digit number pcscd decides to use.

**Example: CSV file mapping bankd slot 0 to a OMNIKEY 3x21 Smart Card Reader:**

```
"1","0","HID Global OMNIKEY 3x21 Smart Card Reader \[OMNIKEY 3x21 Smart Card Reader\] 00 ↩
    00"
```

# 8 osmo-remsim logging

All programs within the osmo-remsim project use the logging sub-system of `libosmocore`.

Contrary to the larger Osmocom projects with their own VTY + configuration file, the logging configuration for osmo-remsim programs must happen via command line arguments.

Also, contrary to the larger Osmocom projects, only logging to `stderr` is supported; no direct logging to log files, syslog, systemd, etc. is supported at this point.

## 8.1 `-d` command line argument

Every osmo-remsim program like `osmo-remsim-bankd`, `osmo-remsim-server` or `osmo-remsim-client-st2` supports a `-d` command line argument. This argument takes one mandatory parameter configuring the log level for each log sub-system as follows:

```
-d SUBSYS,num_lvl[:SUBSYS,num_lvl[:...]]
```

So basically, a colon-separated list of tuples, where each tuple contains the sub-system name and the *numeric* log level.

Below is the list of sub-systems and a table of numerical levels:

Table 4: libosmocore log levels and their numeric values

| Level name | Numeric value |
|---|---|
| DEBUG | 1 |
| INFO | 3 |
| NOTICE | 5 |

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

Table 4: (continued)

| Level name | Numeric value |
|---|---|
| ERROR | 7 |
| FATAL | 8 |

Table 5: osmo-remsim log sub-system names and their description

| Sub-System Name | Description |
|---|---|
| DMAIN | respective main program code |
| DST2 | SIMtrace2 `cardem` firmware interaction via USB |
| DRSPRO | RSPRO protocol between bankd, server and client |
| DREST | REST interface of `osmo-remsim-server` |
| DSLOTMAP | slotmap code shared by `osmo-remsim-server` and `osmo-remsim-bankd` |
| DBANKDW | worker threads of `osmo-remsim-bankd` |

### 8.2 Example

Putting the above in a concrete example:

`-d DMAIN,5:DRSPRO,1`

would perform the following configuration:

- log only NOTICE (or higher) messages in the DMAIN subsystem (low verbosity)
- log DEBUG (or higher) messages in the DRSPRO subsystem (very high verbosity)

## 9 RSPRO

**RSPRO**, the **Remote SIM Protocol**, is an osmo-remsim specific, non-standard communications protocol used between the elements of the osmo-remsim system.

It is specified in ASN.1 syntax (see `asn1/RSPRO.asn` in the `osmo-remsim` source code) and uses BER (Basic Encoding Rules) on the transport level.



**Warning**
RSPRO and its underlying transport layer both operate in plain-text, There is no authentication or encryption built into the protocol. It is assumed that the protocol is only spoken over trusted, controlled IP networks, such as inside a VPN or a closed / private corporate network.

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

## 9.1 Underlying Transport Layer

RSPRO uses TCP as an underlying transport protocol. As TCP doesn't preserve message boundaries, the IPA multiplex is used as intermediate layer between TCP and the BER-encoded RSPRO PDU.

For more information about the IPA multiplex, see the related chapter in http://ftp.osmocom.org/docs/latest/osmobts-abis.pdf

RSPRO uses the IPA CCM PING/PONG messages for keep-alive and detection of dead/stale connections. The compiled-in defaults transmits one IPA PING every 30s and waits 10s for a response from the peer before declaring the connection as dead.

## 9.2 RSPRO PDU

An RsproPDU consists of:

- **version** of the protocol (v2 is current)
- **tag** specified by the sender, echoed back by the receiver in its response so the server can map responses back to a specific request
- **msg** the actual RSPRO Message (union/choice)

## 9.3 RSPRO Operations

Each RSPRO Operation typically (unless specified othewise) consists of a Request and Response pair.

### 9.3.1 ConnectBank

This is used by `remsim-bankd` to identify itself to `remsim-server` and to establish a logical connection between the two elements.

### 9.3.2 ConnectClient

This is used by `remsim-client` to identify itself to `remsim-server` and to establish a logical connection between the two elements.

### 9.3.3 CreateMapping

This is used by `remsim-server` to install a slot mapping in a `remsim-bankd`.

### 9.3.4 RemoveMapping

This is used by `remsim-server` to remove a slot mapping from a `remsim-bankd`.

### 9.3.5 ConfigClientId

This is used by `remsim-server` to dynamically configure a ClientID in a `remsim-client`. This mode is currently not supported yet, each client must have a locally-configured ClientID.

### 9.3.6 ConfigClientBank

This is used by `remsim-server` to inform a `remsim-client` about the details (bankd ID, slot number, IP address, TCP port) of a the `remsim-bankd` to which it shall connect.

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

#### 9.3.7 ErrorInd

This is a generic error indication that can be sent by any RSRPO entity.

#### 9.3.8 SetAtr

This is used by `remsim-bankd` to inform the `remsim-client` about the ATR of the card, so that `remsim-client` can replicate that ATR when answering to the reset of the SIM card interface of the phone/modem.

#### 9.3.9 TpduModemToCard

This is used by `remsim-client` to transfer a command TPDU/APDU from the phone/modem to the SIM card in `remsim-bankd`

#### 9.3.10 TpduCardToModem

This is used by `remsim-bankd` to transfer a response TPDU/APDU from the SIM card back to the phone/modem at `remsim-client`

#### 9.3.11 ClientSlotStatusInd

This is used by `remsim-client` to report the status of a given slot.

#### 9.3.12 BankSlotStatusInd

This is used by `remsim-bankd` to report the status of a given slot.

## 10 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])

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

**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.

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

**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

**GFDL**
GNU Free Documentation License; a copyleft-style Documentation License

**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

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

**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

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

**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]

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

**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

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

**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

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

**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])

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

**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

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

# A Bibliography / References

#### A.0.0.0.1 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


Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

[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

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

[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

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

[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] [etsi-ts102671] ETSI TS 102 671: Smart Cards; Machine to Machine UICC; Physical and logical characteristics https://www.etsi.org/deliver/etsi_ts/102600_102699/102671/18.01.00_60/ts_102671v180100p.pdf

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

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

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

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

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

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

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

[74] [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

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

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

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

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

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

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

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

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

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

[84] [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/

[85] [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/

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

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

[88] [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

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

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

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

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

[92] [tw-ts-001] TW-TS-001: Enhanced RTP transport of FR and EFR codec frames in an IP-based GSM RAN https://www.freecalypso.org/specs/tw-ts-001-v010100.txt

[93] [tw-ts-002] TW-TS-002: Enhanced RTP transport of HRv1 codec frames in an IP-based GSM RAN https://www.freecalypso.org/specs/tw-ts-002-v010100.txt

[94] [tw-ts-003] TW-TS-003: BSSMAP extension for selection of enhanced RTP transport formats https://www.freecalypso.org/specs/tw-ts-003-v010002.txt

# B GNU Free Documentation License

Version 1.3, 3 November 2008

Copyright © 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc. http://fsf.org/

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

## B.1 PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

## B.2 APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Section whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then

it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The “Cover Texts” are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A “Transparent” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not Transparent is called “Opaque”.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The “Title Page” means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, Title Page means the text near the most prominent appearance of the work’s title, preceding the beginning of the body of the text.

The “publisher” means any person or entity that distributes copies of the Document to the public.

A section “Entitled XYZ” means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as “Acknowledgements”, “Dedications”, “Endorsements”, or “History”.) To “Preserve the Title” of such a section when you modify the Document means that it remains a section “Entitled XYZ” according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

## B.3 VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section Section B.4.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

## B.4 COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document’s license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

### B.5 MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

a. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

b. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

c. State on the Title Page the name of the publisher of the Modified Version, as the publisher.

d. Preserve all the copyright notices of the Document.

e. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

f. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

g. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

h. Include an unaltered copy of this License.

i. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

j. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

k. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

l. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

m. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

n. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Sections.

o. Preserve any Warranty Disclaimers.

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Section and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

## B.6 COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

## B.7 COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

## B.8 AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

### B.9 TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

### B.10 TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

### B.11 FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

### B.12 RELICENSING

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

### B.13 ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

```
Copyright (c)  YEAR  YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.3
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled ``GNU
Free Documentation License''.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with…Texts." line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

Copyright © 2019-2021 sysmocom - s.f.m.c. GmbH 