

sysmocom

sysmocom - systems for mobile communications GmbH

sysmoEUICC1 User Manual

by Harald Welte

Copyright © 2016-2024 sysmocom - systems for mobile communications GmbH

All rights reserved.

| REVISION HISTORY | | | |
|------------------|-----------|--|------|
| NUMBER | DATE | DESCRIPTION | NAME |
| v1.2 | Oct 2024 | sysmoEUICC1-CMG now in webshop | hw |
| v1.1 | June 2024 | Describe the ARA-M clash problem | hw |
| v1 | May 2024 | Updated version for sysmoEUICC1 v2 mass production | hw |
| v0 | Jan 2024 | Initial version for sysmoEUICC1 v1 samples | hw |

Contents

| | | |
|----------|--|----------|
| 1 | Preface | 1 |
| 2 | eSIM / eUICC Introduction | 1 |
| 2.1 | Historical Evolution: from SIM via UICC to eUICC | 1 |
| 2.2 | The eUICC and its function in the eSIM system | 1 |
| 2.3 | Consumer eSIM System | 2 |
| 2.4 | Further Reading / Information sources | 2 |
| 2.4.1 | Recorded Technical Presentations | 2 |
| 2.4.2 | Written Information | 3 |
| 3 | The sysmocom eUICC family | 3 |
| 3.1 | sysmoEUICC variants | 3 |
| 3.2 | sysmoEUICC form-factors | 3 |
| 3.2.1 | 2FF/3FF/4FF seamless-cut form-factor | 3 |
| 3.2.2 | MFF2 solder-type form-factor | 3 |
| 3.3 | sysmoEUICC certificates / key materials | 4 |
| 3.3.1 | GSMA certificates | 4 |
| 3.3.2 | Test certificates | 4 |
| 3.3.3 | Private (alternate root) certificates | 4 |
| 4 | sysmoEUICC1 specifications | 5 |
| 4.1 | Physical Specification | 5 |
| 4.2 | Logical Specification | 5 |
| 4.2.1 | GSMA Specification Compliance | 5 |
| 4.2.2 | Interoperable Profile Support | 6 |
| 4.2.3 | ETSI/3GPP/GP Specification Compliance | 6 |
| 4.3 | Supported Features | 7 |
| 4.3.1 | Authentication Algorithms | 7 |
| 4.4 | Product Form-Factor Variants | 7 |
| 4.5 | Java API Packages | 8 |
| 5 | Pre-installed TS.48 test profile | 8 |
| 5.1 | eSIM profile metadata | 9 |
| 5.2 | eSIM profile parameters | 9 |
| 5.3 | eSIM profile RFM parameters | 9 |
| 5.4 | eSIM profile OTA keys | 9 |

| | | |
|-----------|--|-----------|
| 6 | Smart Card Readers | 9 |
| 6.1 | Verifying your smart card reader + software stack | 10 |
| 6.2 | Verifying your smart card reader + software stack | 10 |
| 6.3 | Mechanical Card Adapters | 11 |
| 7 | Using the 1pac implementation of the LPA | 12 |
| 7.1 | downloading an eSIM profile | 12 |
| 7.2 | Notifications | 12 |
| 7.2.1 | Listing notifications | 13 |
| 7.2.2 | Processing notifications | 13 |
| 7.2.3 | Removing notifications | 13 |
| 7.3 | Listing, Enabling, Disabling and Deleting of Profiles | 14 |
| 7.3.1 | Listing installed profiles | 14 |
| 7.3.2 | Enabling a profile | 14 |
| | Error iccid or aid not found | 15 |
| | Error wrong profile reenabling | 15 |
| 7.3.3 | Disabling a profile | 15 |
| 7.3.4 | Deleting a profile | 15 |
| 8 | Using the EasyEUICC implementation of the LPA for Android | 16 |
| 8.1 | Main screen | 16 |
| 8.2 | Settings menu | 17 |
| 8.3 | Downloading an eSIM profile | 18 |
| 8.4 | Managing notifications | 20 |
| 8.4.1 | Enabling (switching) a profile | 21 |
| 8.4.2 | Deleting a profile | 22 |
| 8.5 | Troubleshooting | 23 |
| 8.5.1 | Compatibility Check | 23 |
| 8.5.2 | EUICC not recognized | 24 |
| 9 | Using pySim-shell with eUICCs | 25 |
| 10 | osmo-smdpp as a proof-of-concept SM-DP+ | 25 |
| 11 | sysmocom SGP.26 test SM-DP+ for Consumer eSIM | 26 |
| 12 | The unsolved ARA-M problem in the case of eUICCs | 26 |
| 12.1 | Affected eSIM profiles | 26 |
| 12.2 | Further Reading | 27 |
| 12.3 | Solutions | 27 |
| 12.4 | Workarounds | 27 |
| 12.4.1 | eUICCs without ARA-M in ISD-R | 27 |
| 12.4.2 | eSIM profile with non-mandatory ARA-M | 27 |

13 sysmoEUICC1 changelog **27**

13.1 sysmoEUICC1-C2G v0 (November 2023) 27

13.2 sysmoEUICC1-C2G v1 (May 2024) 27

14 Acknowledgements **28**

15 Glossary **28**

A Osmocom TCP/UDP Port Numbers **36**

B Bibliography / References **38**

References 38

1 Preface

sysmocom is a small German company providing primarily research, development and consulting in cellular network technologies from 2G to 5G, from RAN to CN, with a specific focus on Open Source in mobile communications. As part of our R&D activities, we often are in need of tools that are difficult to impossible to acquire on the open market, and hence we build them ourselves for internal use, but then also sell those products to the world wide community of parties interested in research into cellular technology.

For more than a decade we've now been very successful at providing highly flexible, configurable and programmable SIM, UICC/USIM/ISIM cards to thousands of customers world wide. The success of the product has shown a clear need for this kind of product, which did not exist before, at the very least not as accessible, documented and available to anyone.

As part of our activities we discovered that the eSIM / eUICC universe was even more difficult than the domain of physical UICC/USIM/ISIM cards, which lead us to the development of the new sysmoEUICC product line.

With these products, we aim to make eUICC and eSIM technology more accessible. This should enable hands-on training, exploration, research and understanding of eSIM protocols for any interested parties.

Working with eUICCs locked into the GSMA root-of-trust are mostly useful in practical usage applications within existing commercial cellular network operators that offer consumer eSIM profiles.

Much more exotic and interesting is however, in our belief, the use of eUICCs with certificates and key materials under the control of our customers. Combining such eUICCs with the open source proof-of-concept SM-DP+ `osmo-smdpp` developed and published by sysmocom founder Harald Welte, anyone is able to operate a complete eSIM system end-to-end. That means using your own certificates, running your own self-hosted SM-DP+, creating your own eSIM profiles and downloading them into your own test/private eUICCs.

— Harald Welte, Osmocom.org and sysmocom founder, January 2024.

2 eSIM / eUICC Introduction

2.1 Historical Evolution: from SIM via UICC to eUICC

When 2G GSM networks were first introduced in the early 1990s, the GSM SIM (*Subscriber Identity Module*) was introduced to de-couple the subscribers' subscription identity from the phone they were using. This meant that multiple subscribers could share a (back then ridiculously expensive) phone, and they could migrate from one phone to the other, for example when renting a car with car-installed mobile phone. The SIM was a single-application smart card.

Over time, this concept has been generalized into the ETSI UICC (Universal Integrated Circuit Card), which is a platform for multi-application smart cards. When 3G (UMTS) came around, its subscriber identity was specified as the USIM (Universal Subscriber Identity Module) Application running on an UICC. That USIM application has subsequently been extended for 4G (LTE) and 5G (NR). With the advent of IMS (VoLTE, VoWiFi), an optional ISIM Application has been specified.

Up to this point, a given subscriber identity was always bound to a given physical chip card. The identity (specifically, the cryptographic authentication key material) would be *personalize* on the card during card manufacturing.

With the eSIM system, this changed fundamentally. The subscriber identity (comprising typically of an USIM and optionally an ISIM application with associated filesystem data and key materials) was virtualized and de-coupled from the underlying chip card. That virtualized subscriber identity is called an *eSIM profile* and the underlying chip (most often no longer a "card") is called the *eUICC*.

2.2 The eUICC and its function in the eSIM system

The eUICC (embedded Universal Integrated Chip Card) is the hardware component typically soldered onto the circuit board of a UE (User Equipment, the term 3GPP uses for a phone/modem). It is the physical component onto which the purely logical/virtual eSIM [profiles] are installed.

You can liken an eUICC conceptually with so-called *secure element* or *trusted platform module* used in other industries.

In order for cellular operators to trust such a virtualized SIM system with their most valuable cryptographic key materials, comprehensive security mechanisms had to be introduced into the eSIM system: Virtually any part of it is authenticated by cryptographic certificates, which can all be verified and traced back to a root-of-trust, the GSMA Certificate Authority (CA). This CA in turn has a very stringent policy about whom it will issue certificates under which circumstances. Those are detailed requirements on IT security, physical access security, certification levels of Hardware Security Modules, protection profiles for the CardOS of an eUICC, etc. which any certificate holder must be independently audited for at least every two years.

GSMA has specified three different eSIM systems. Those are technically relate to some degree by using similar building blocks, but there are *significant* differences between those systems, and specifically the eUICC are different between M2M, Consumer and IoT. They *can not be mixed/matched*.

| System | Specifications | Description |
|---------------|----------------|--|
| M2M eSIM | SGP.01, SGP.02 | requires special M2M eSIM subscriptions offered by M2M providers/MVNOs, typically with regional or global coverage; intended for large fleets of devices |
| Consumer eSIM | SGP.21, SGP.22 | permits eSIM profiles that are individually purchased from a variety of providers in MOQ-1 |
| IoT eSIM | SGP.31, SGP.32 | combines the advantages of M2M and consumer (especially for smaller customers): Ability to install consumer profiles, but centrally managed for a fleet of devices |

As of early 2024, the M2M and Consumer systems are in production, while products for the new IoT scheme are still under development and not expected before end of 2024 (soonest).

2.3 Consumer eSIM System

The consumer eSIM system is - at its minimum - comprised of the following elements:

- the **eUICC** as described above
- the **LPA** (Local Profile Assistant); a piece of software running on the UE (phone, cellular modem) which interfaces locally with the eUICC and remotely with the SM-DP+.
- the **SM-DP+** (Subscription Manager Data Preparation; Enhanced); a server component which prepares, protects and *binds* eSIM profiles so they can be downloaded (via the LPA) into the eUICC

The eUICC contains a set of certificate and private key, signed by the eUICC manufacturers certificate, which in turn is signed by the GSMA CA.

The SM-DP+ has a set of certificates and private keys (for TLS, Authentication and Data Preparation), signed by the GSMA CA.

The LPA acts mostly as some kind of relay between the smart card interface and the (usually https based) interface to the SM-DP+.

2.4 Further Reading / Information sources

For more information about eSIM and eUICC technology, we recommend the following resources:

2.4.1 Recorded Technical Presentations

- [Demystifying eSIM Technology](#) (video recording of talk at CCCCamp2023)
- [Exploring eUICCs and eSIMs using pySim, lpac and osmo-smdpp](#) (video recording of talk at OsmoDevCall)
- [GlobalPlatform in USIM and eUICC](#) (video recording of talk at OsmoDevCon2024)
- [Anatomy of the eSIM profile](#) (video recording of talk at OsmoDevCon2024)

2.4.2 Written Information

- [GSMA eSIM whitepaper](#)
- [Osmocom eUICC and eSIM Developer Manual](#)

3 The sysmocom eUICC family

This manual describes the sysmoEUICC1 state-of-the-art eUICC for use with the Consumer eSIM Remote SIM Provisioning. The target audience are developers, researchers and operators of cellular equipment who use the sysmoEUICC1 in order to identify the subscribers to their network.

3.1 sysmoEUICC variants

sysmoEUICC are available in a number of different variants in terms of

- the mechanical form factor (removable plastic card vs. solder-type)
- the certificates and key materials used

| SKU | System | Form-Factor | Certificates |
|-----------------|----------|-------------|---------------|
| sysmoEUICC1-C2G | Consumer | 2FF/3FF/4FF | GSMA |
| sysmoEUICC1-C2T | Consumer | 2FF/3FF/4FF | Test (SGP.26) |
| sysmoEUICC1-C2P | Consumer | 2FF/3FF/4FF | Private |
| sysmoEUICC1-CMG | Consumer | MFF2 | GSMA |
| sysmoEUICC1-CMT | Consumer | MFF2 | Test (SGP.26) |
| sysmoEUICC1-CMP | Consumer | MFF2 | Private |

Assuming related quantity purchases, sysmocom is also able to provide M2M eUICC as part of project business.

IoT eUICC are expected to become available as soon as the system becomes production-ready.

3.2 sysmoEUICC form-factors

3.2.1 2FF/3FF/4FF seamless-cut form-factor

The sysmoEUICC is available in the traditional plastic card form factor of SIM/UICC cards. It is a so-called *seamless cut*, allowing for a single card to be used in full (credit card) size, as well as 2FF (mini-SIM), 3FF (micro-SIM) or 4FF (nano-SIM).

This form-factor is useful primarily in that:

- it can be used to eSIM-enable devices that have a traditional SIM card slot, and no built-in/on-board eUICC
- it can be used during research, development and testing; for example by inserting it into a smart-card reader that is attached to a computer

3.2.2 MFF2 solder-type form-factor

The sysmoEUICC is available in the ETSI MFF2 form-factor. This is the oldest and most standard solder-type package for an eUICC.

The MFF2 package is mostly useful if you are building some kind of embedded / IoT device to which you would like to add the capability for downloading eSIM profiles.

Compared to an eUICC in the removable plastic card form-factor, the advantages are mostly:

- better contact, especially in case of vibration-intensive applications like automotive
- reduction of BOM cost (no card slot required)
- ability to manufacture sealed / waterproof devices (no more removable parts)

The recommended footprint, reflow/moisture profile etc. can be found in the ETSI MFF2 specification ETSI TS 102 671 [\[etsi-ts102671\]](#).

Associated with a related volume purchase, sysmocom is also able to provide other (e.g. smaller) solder-type packages than MFF2.

3.3 sysmoEUICC certificates / key materials

3.3.1 GSMA certificates

The most common use case for eUICCs is within the GSMA *root-of-trust*, i.e. with certificates issued under the GSMA CA. This is the only way to permit interoperability with the vast majority of eSIM profiles that are for sale by hundreds of mobile operators around the world.

The disadvantage of an eUICC with GSMA certificates is that it will **only** accept eSIM profiles issued by a GSMA SAS-SM accredited SM-DP+. This makes it relatively unattractive for laboratory and research use, or even some use cases of private cellular networks.

Specifically, you can not autonomously create and install your own eSIM profile on an eUICC that contains [only] GSMA certificates. This is a significant step back from the prior situation with physical SIM/USIM, where anyone could autonomously create whatever SIM they like and insert it into any device of their choosing.

3.3.2 Test certificates

In order to facilitate R&D of eSIM related products, GSMA has specified and released a set of *test certificates* together with the associated *key materials* in GSMA SGP.26.

The advantage of those test certificate/keys is that contrary to the GSMA certificates, you can create, sign and encrypt your own eSIM profiles and download/install them on an eUICC.

The disadvantage of the test certificates is that the CA root certificate and private key are public, meaning that *anyone* can impersonate any element of the eSIM system, and hence there is no security whatsoever. This reduces the usage entirely to R&D of eSIM systems

3.3.3 Private (alternate root) certificates

An eUICC can also be equipped with *private* (alternate root) certificates. This means that another entity operates as Certificate Authority, and can hence issue certificates to SM-DP+ and eUICCs.

The use case for this is somewhere in between the GSMA certificates and the test certificates:

- entities without GSMA-SAS accreditation can issue certificates for eUICCs and SM-DP+ and hence eSIM profiles
- the private key materials are not publicly available (like in the test certificates), meaning that impersonation is not possible, at least not to any random third party.

Such an alternate root configuration might, for example, make sense in case of private cellular networks, where there is no need for fulfilling the expensive and cumbersome GSMA-SAS requirements, and/or where a higher degree of autonomy and sovereignty without dependencies to third parties is desired or even required.

4 sysmoEUICC1 specifications




sysmocom
systems for mobile communications GmbH

EUICC1-C2G

- Expertise in protocol R&D from 2G to 5G, RAN to CN
- Support and development for Osmocom + open5gs
- small-cell cellular base station hardware
- GSM, UMTS and LTE networks in the box (NITB)
- SIM cards, accessories, tracers, remote SIM, eUICC

Please support <https://osmocom.org/>
a community creating projects related to Open source mobile communications including (among many other things) the **pySim** software you can use to work with this eUICC and its eSIMs. Osmocom relies on contributions, whether by code, documentation improvements or financially.

sysmoEUICC1-C2G



sysmocom
systems for mobile communications GmbH

EUICC1-C2T

- Expertise in protocol R&D from 2G to 5G, RAN to CN
- Support and development for Osmocom + open5gs
- small-cell cellular base station hardware
- GSM, UMTS and LTE networks in the box (NITB)
- SIM cards, accessories, tracers, remote SIM, eUICC

Please support <https://osmocom.org/>
a community creating projects related to Open source mobile communications including (among many other things) the **pySim** software you can use to work with this eUICC and its eSIMs. Osmocom relies on contributions, whether by code, documentation improvements or financially.

sysmoEUICC1-C2T

The sysmoEUICC1-C are eUICC for consumer eSIM with the following specifications and features:

4.1 Physical Specification

- Available mechanical form factor
 - 2FF + 3FF + 4FF seamless triple cut (either full-size or half-size plastic)
 - MFF2 (solder-type) chip
- 800 kBytes flash memory (about 300kBytes available)
 - 3.200.000 write operations per page
 - 200.000 erase operations per page
 - Data Retention: typical 10 years @ 25 centigrade
- Temperature Range: -40 to +105 Centigrade chip temperature
- 1.8V, 3V and 5V compliant (absolute range: 1.62V to 5.5V)
- ESD protection > 4 kv (HBM)
- external clock frequency: 1 to 10 MHz
- max. sleep mode current (typical) < 100 uA in clock-off mode

4.2 Logical Specification

4.2.1 GSMA Specification Compliance

- GSMA SGP.22 V2.3.0
- Maximum number of profiles: 10

4.2.2 Interoperable Profile Support

- eUICC Profile Package Version: 2.3.1
- UICC capability: 067f36f3c0
 - usimSupport, isimSupport, csimSupport,
 - akaMilenage, akaCave, akaTuak128, akaTuak256,
 - gbaAuthenUsim, gbaAuthenIsim,
 - eapClient, javacard,
 - multipleUsimSupport, multipleIsimSupport, multipleCsimSupport, berTlvFileSupport,
 - getIdentity, profile-a-x25519, profile-b-p256, suciCalculatorApi

4.2.3 ETSI/3GPP/GP Specification Compliance

The sysmoEUICC1-C adheres to the following specifications / spec versions:

- USIM and ISIM application
 - ETSI TS 102 221; [[etsi-ts102221](#)]
 - ETSI TS 102 225; [?]
 - 3GPP TS 51.011 (R17); [[3gpp-ts-51-011](#)]
 - 3GPP TS 31.101 (R17); [[3gpp-ts-31-101](#)]
 - 3GPP TS 31.102 (R17); [[3gpp-ts-31-102](#)]
 - 3GPP TS 31.103 (R17); [[3gpp-ts-31-103](#)]
- Java Card v3.0.5
 - SIM API (3GPP TS 43.019)
 - UICC API (ETSI TS 102 241 15.1.0)
 - UICC Remote File Update Event (ETSI TS 102 241)
 - USIM API (3GPP TS 31.130)
 - GlobalPlatform API
 - Connection API (ETSI TS 102 267)
 - Algorithms: DES/2DES/3DES, AES128/192/256, CRC16/32, SHA1/224/256, MD5, HMAC, ECC
- Global Platform v2.1.1 (SCP02, SCP03, SCP80)
 - GlobalPlatform v2.2 Amendments A, B, D, E
- UICC / USIM Toolkit Support
- OTA (Over-The-Air) Support
- Remote File Management / Remote App Management
 - 3GPP TS 23.048 (R4); [[3gpp-ts-23-048](#)]
 - 3GPP TS 31.115 (R6); [[3gpp-ts-31-115](#)]
 - 3GPP TS 31.116 (R6); [[3gpp-ts-31-116](#)]

4.3 Supported Features

- Total number of logical channels: 8
- Maximum number of applets: 90
- Maximum number of user packages: 39
- Suspend and Resume
- BER-TLV files
- GBA network authentication
- EAP-SIM and EAP-AKA (no support for RFC5448 EAP-AKA')
- SUCI-computation-by-ME
- SUCI-computation-on-card
- RAM (Remote Applet Management) + RFM (Remote File Management)
 - Proactive Commands
 - Expanded Format
 - Script chaining
 - Concatenated response
 - CAT-TP
 - HTTPS
 - TLS 1.0, 1.1 and 1.2

4.3.1 Authentication Algorithms

- 3G (UMTS AKA) Authentication, also used by 4G/5G/IMS
 - Default 3G Authentication Algorithm: MILENAGE [3gpp-ts-35-206]
 - Supported: MILENAGE, TUAK, XOR-3G

The algorithm can be changed when authenticated using ADM1 PIN.

4.4 Product Form-Factor Variants

The cards are sold by sysmocom in the following different product variants, depending on your needs.

| SKU | Form-Factor | certificates | Link to sysmocom webshop |
|-----------------|-----------------------|--------------|---|
| sysmoEUICC1-C2G | 1FF + 2FF + 3FF + 4FF | GSMA | https://shop.sysmocom.de/sysmoEUICC1-eUICC-for-consumer-eSIM-RSP/-sysmoEUICC1-C2G |
| sysmoEUICC1-C2T | 1FF + 2FF + 3FF + 4FF | Test | https://shop.sysmocom.de/eUICC-for-consumer-eSIM-RSP-with-SGP.26-Test-Certificates/sysmoEUICC1-C2T |
| sysmoEUICC1-CMG | MFF2 | GSMA | https://shop.sysmocom.de/sysmoEUICC1-eUICC-for-consumer-eSIM-RSP-in-MFF2-10-pack/sysmoEUICC1-CMG-10p |
| sysmoEUICC1-CMT | MFF2 | Test | bulk / made-to-order only |

4.5 Java API Packages

| Package | Version | AID |
|--------------------------------|---------|------------------------------------|
| java.lang | 1.0 | 0xA0000000620001 |
| java.io | 1.0 | 0xA0000000620002 |
| java.rmi | 1.0 | 0xA0000000620003 |
| javacard.framework | 1.5 | 0xA0000000620101 |
| javacard.framework.service | 1.0 | 0xA000000062010101 |
| javacard.security | 1.5 | 0xA0000000620102 |
| javacardx.crypto | 1.5 | 0xA0000000620201 |
| javacardx.framework.util | 1.0 | 0xA000000062020801 |
| javacardx.framework.util.intx | 1.0 | 0xA00000006202080101 |
| sim.access | 2.2 | 0xA000000090003FFFFFFFF8910710001 |
| sim.toolkit | 2.6 | 0xA000000090003FFFFFFFF8910710002 |
| uicc.access | 1.2 | 0xA000000090005FFFFFFFF8911000000 |
| uicc.access.fileadministration | 1.0 | 0xA000000090005FFFFFFFF8911010000 |
| uicc.access.bertlvfile | 1.0 | 0xA000000090005FFFFFFFF8911010000 |
| uicc.system | 1.2 | 0xA000000090005FFFFFFFF8913000000 |
| uicc.toolkit | 1.12 | 0xA000000090005FFFFFFFF8912000000 |
| uicc.suspendresume | 1.0 | 0xA000000090005FFFFFFFF8917000000 |
| uicc.usim.access | 1.4 | 0xA0000000871005FFFFFFFF891310000 |
| uicc.usim.toolkit | 1.9 | 0xA0000000871005FFFFFFFF8913200000 |
| uicc.usim.geolocation | 1.0 | 0xA0000000871005FFFFFFFF8913200000 |
| uicc.usim.suci | 1.0 | 0xA0000000871005FFFFFFFF8913400000 |
| uicc.connection | 2.0 | 0xA000000090005FFFFFFFF8915000000 |
| org.globalplatform | 1.6 | 0xA00000015100 |

5 Pre-installed TS.48 test profile

NOTE

This section only applies to sysmoEUICC1-C2G and not to other product variants!

The sysmoEUICC1-C2G has a pre-installed and enabled *TS.48 GSMA test profile*.

GSMA TS.48 is a specification of eSIM profiles to be used in testing and type approval purposes.

The idea of the pre-installed profile has the following rationale:

- to make the eUICC usable straight away for some test use cases, without having to install a commercial operator eSIM profile
- to make sure EasyEUICC can work with the sysmoEUICC, as EasyEUICC will only talk to eUICC with an active profile

As this profile is clearly marked as *test* profile, it behaves slightly different than normal (*operational*) profiles that are downloaded. One such difference is that a number of LPA software will not even show those test profiles in their listings.

NOTE

As required by SGP.22 section 3.2.1, **a test profile must not be implicitly disabled when a production profile is enabled!** This means, in order to activate a normal (operational) profile that you downloaded from a SM-DP+, you must first **explicitly disable** the factory-enabled test profile. You can use any standards-compliant LPA software to do so; see the Section 7 section for one such example.

NOTE

If you want to manage (show, disable, enable, delete) test profiles using EasyEUICC, you need to check the **Show unfiltered profile list** box within the developer options. To enable the developer options you must first enable the developer options by pressing a few times on the App version number you find on in the Info section of the menu. (similar activation style to the general Android developer options)

5.1 eSIM profile metadata

| Parameter | Value |
|-----------------------|--------------------------------|
| Profile Type | Test |
| Profile Name | Operational Profile Name 1 |
| Service Provider Name | SP Name 1 |
| ISD-P AID | a0000005591010ffffff8900001000 |

5.2 eSIM profile parameters

The pre-installed profile has the following key parameters:

| | |
|---------------|----------------------------------|
| ICCID | 89000123456789012341 |
| IMSI | 001010123456063 |
| PIN1 | 0000 |
| PUK1 | 11111111 |
| PIN2 | 9999 |
| PUK2 | 22222222 |
| ADM1 | 55555555 |
| ADM2 | 66666666 |
| K | 000102030405060708090A0B0C0D0E0F |
| AKA Algorithm | XOR-3G |

5.3 eSIM profile RFM parameters

The pre-installed eSIM profile has the following RFM (Remote File Management) configuration:

| Instance AID | TAR | MSL | ADF Access |
|--------------------|--------|------|---------------------------------|
| a00000055910100001 | b00120 | 0x06 | |
| a00000055910100002 | b00140 | 0x06 | a0000000871002ff49ff0589 (USIM) |
| a00000055910100003 | b00141 | 0x06 | a0000000871004ff49ff0589 (ISIM) |

5.4 eSIM profile OTA keys

The pre-installed eSIM profile has the following OTA keys:

| KID | KVN | Value |
|------|------|----------------------------------|
| 0x01 | 0x01 | 66778899aabbccdd1122334455eeff10 |
| 0x02 | 0x01 | 112233445566778899aabbccddeeff10 |
| 0x03 | 0x01 | 99aabbccddeeff101122334455667788 |
| 0x01 | 0x02 | 66778899aabbccdd1122334455eeff10 |
| 0x02 | 0x02 | 112233445566778899aabbccddeeff10 |
| 0x03 | 0x02 | 99aabbccddeeff101122334455667788 |

6 Smart Card Readers

SIM/UICC/USIM/ISIM cards are smart cards compliant to the electrical parameters of ISO 7816-3, both in terms of voltage but also in terms of signal / timing. This is the same standard as used by many other smart cards, including all kinds of identification cards, debit/credit cards, cryptographic smart cards, etc.

In order to interface a SIM/UICC/USIM/ISIM to a computer, you thus need a smart card interface device (colloquially called "card reader") compliant to ISO 7816-3.

In order to support maximum compatibility with software programs, the reader should inter-operate with the pcsc-lite software stack on your GNU/Linux based operating system.

The easiest type of readers in recent years have proven to be USB attached smart card readers compliant to the USB CCID specification.

Compliance to USB CCID ensures that a variety of vendor-neutral/independent drivers will work on virtually any operating system.

sysmocom offers suitable USB CCID compliant card readers at <https://shop.sysmocom.de/SIM/Card-Readers-Writers/>



Figure 1: Omnikey CardMan 3121 USB CCID Smart Card Reader

6.1 Verifying your smart card reader + software stack

For details on how to configure your smart card reader / driver stack, please consult related documentation. In the case of USB CCID readers and pcsc-lite, any modern GNU/Linux distribution should have everything pre-configured without any manual intervention required.

In case of Ubuntu or Debian GNU/Linux, you only need to install the pcscd and libccid packages, e.g. using **apt-get install pcscd libccid**

6.2 Verifying your smart card reader + software stack

Every smart card returns a so-called ATR (Answer-To-Reset) as soon as it is first interrogated by the card reader.

You can use the **pcsc_scan** utility in order to read the status of your card reader and obtain the ATR of the currently-inserted card.

Example output of pcsc_scan with a sysmoUSIM-SJS1 inserted

```
$ pcsc_scan
PC/SC device scanner
V 1.4.26 (c) 2001-2011, Ludovic Rousseau <ludovic.rousseau@free.fr>
Compiled with PC/SC lite version: 1.8.15
Using reader plug'n play mechanism
Scanning present readers...
0: Alcor Micro AU9560 00 00

Sat May 21 21:38:31 2016
Reader 0: Alcor Micro AU9560 00 00
Card state: Card inserted,
```

```

ATR: 3B 9F 96 80 1F C7 80 31 A0 73 BE 21 13 67 43 20 07 18 00 00 01 A5
ATR: 3B 9F 96 80 1F C7 80 31 A0 73 BE 21 13 67 43 20 07 18 00 00 01 A5
+ TS = 3B --> Direct Convention
+ T0 = 9F, Y(1): 1001, K: 15 (historical bytes)
  TA(1) = 96 --> Fi=512, Di=32, 16 cycles/ETU
    250000 bits/s at 4 MHz, fMax for Fi = 5 MHz => 312500 bits/s
  TD(1) = 80 --> Y(i+1) = 1000, Protocol T = 0
---
  TD(2) = 1F --> Y(i+1) = 0001, Protocol T = 15 - Global interface bytes following
---
  TA(3) = C7 --> Clock stop: no preference - Class accepted by the card: (3G) A 5V B 3V C ↔ 1.8V
+ Historical bytes: 80 31 A0 73 BE 21 13 67 43 20 07 18 00 00 01
  Category indicator byte: 80 (compact TLV data object)
    Tag: 3, len: 1 (card service data byte)
      Card service data byte: A0
        - Application selection: by full DF name
        - BER-TLV data objects available in EF.DIR
        - EF.DIR and EF.ATR access services: by GET RECORD(s) command
        - Card with MF
    Tag: 7, len: 3 (card capabilities)
      Selection methods: BE
        - DF selection by full DF name
        - DF selection by path
        - DF selection by file identifier
        - Implicit DF selection
        - Short EF identifier supported
        - Record number supported
      Data coding byte: 21
        - Behaviour of write functions: proprietary
        - Value 'FF' for the first byte of BER-TLV tag fields: invalid
        - Data unit in quartets: 2
      Command chaining, length fields and logical channels: 13
        - Logical channel number assignment: by the card
        - Maximum number of logical channels: 4
    Tag: 6, len: 7 (pre-issuing data)
      Data: 43 20 07 18 00 00 01
+ TCK = A5 (correct checksum)

Possibly identified card (using /home/laforge/.cache/smartcard_list.txt):
3B 9F 96 80 1F C7 80 31 A0 73 BE 21 13 67 43 20 07 18 00 00 01 A5
    sysmoUSIM-SJS1 (Telecommunication)
    http://www.sysmocom.de/products/sysmousim-sjs1-sim-usim

```

6.3 Mechanical Card Adapters

Smart card readers most often only are available for insertion of full-size (credit-card sized) smart cards.

Thus, you may need a mechanical adapter that converts the physical size of your SIM card to the full-sized card as supported by the smart card reader. The adapter is not required, if your SIM is still in full size (credit card size), but generally required if the card is already broken out and now has the 2FF, 3FF or 4FF form-factor

sysmocom offers a suitable low-cost, reliable adapter at <https://shop.sysmocom.de/Professional-SIM-card-adapter-plug-in-micro-nano-SIM-to-full-size/sim-adapter-pcb>

We also sell a number of other adapters suitable for different use cases, for example for interfacing

- MFF2-packaged UICC / eUICC with a card reader (solder type)
- MFF2-packaged UICC / eUICC with a card reader (ZIF socket type)

- half-sized cards with card readers whose slot is deeper than the card
- Flex-PCB (FPC) adapters to use MFF2 or full-sized cards in 2FF/3FF/4FF slots

The full range of adapter products is available from <https://shop.sysmocom.de/SIM/Adapters/>

7 Using the `lpac` implementation of the LPA

DISCLAIMER

`lpac` is an independent open source software package which is not part of the sysmoEUICC product delivered to you. sysmocom suggests using it for education, research and development purposes, but is not able to provide free support or bug fixing for this third-party program. We are very happy to do so under a separate support services agreement.

`lpac` is an open source implementation of the eSIM LPA (Local Profile Assistant) function for consumer eSIM. It is available in from <https://github.com/estkme-group/lpac> and supports Linux, MacOS and Windows.

You can use it to download, activate, deactivate and delete ESIM profiles onto a consumer eUICC, assuming you have a smart card interface (*smart card reader*) matching the form-factor of your eUICC.

If you have an eUICC with GSMA certificates, then you can only download eSIM profiles from a GSMA accredited SM-DP+.

Conversely, if you have an eUICC with test certificates (or private certificates), then you can only download eSIM profiles from a SM-DP+ with certificates of that same test (or private) certificate authority.

7.1 downloading an eSIM profile

Example output of a typical `lpac` session for profile download

```
$ ./lpac profile download -s testsmplus1.example.com -m 1234
{"type":"progress","payload":{"code":0,"message":"es10b_get_euicc_challenge","data":null}}
{"type":"progress","payload":{"code":0,"message":"es10b_get_euicc_info","data":null}}
{"type":"progress","payload":{"code":0,"message":"es9p_initiate_authentication","data":null ←
}}
{"type":"progress","payload":{"code":0,"message":"es10b_authenticate_server","data":null}}
{"type":"progress","payload":{"code":0,"message":"es9p_authenticate_client","data":null}}
{"type":"progress","payload":{"code":0,"message":"es10b_prepare_download","data":null}}
{"type":"progress","payload":{"code":0,"message":"es9p_get_bound_profile_package","data": ←
null}}
{"type":"progress","payload":{"code":0,"message":"es10b_load_bound_profile_package","data": ←
null}}
{"type":"lpa","payload":{"code":0,"message":"success","data":null}}
```

Note that there can be significant delay (up to a minute) until the final states message can appear on the screen, as eUICC might take quite some time to install a new eSIM profile.

If the download procedure fails during any stage *before* `es9p_get_bound_profile_package`, you will see related error messages in the `lpac` console output. Any later errors are not reported immediately, as the ES9+ interface is specified in a way that the result of the profile installation operation on the eUICC is not reported synchronously, but it is stored in a *notification* on the eUICC. Notifications must be read, processed and removed explicitly (see below).

If the eUICC now hosts a new profile, you should see it in the list. Note that new profiles are not enabled by default, but need to be enabled explicitly.

7.2 Notifications

Notifications are created by the eUICC on the eUICC itself. The LPA is expected to periodically list them, and if there are any, process and remove them.

7.2.1 Listing notifications

The below `lpac` command can be used to list all notifications stored on the eUICC (i.e. those not yet successfully sent to the respective SM-DP+):

Example of listing the notifications

```
$ ./lpac notification list
{"type":"lpa","payload":{"code":0,"message":"success","data":[{"seqNumber":59,"profileManagementOperation":128,"notificationAddress":"testsmdpplus1.example.com","iccid":"89000123456789012358"}]}}
```

If you would like a better decode of the JSON output, you can for example use the `json_pp` utility, or any other such utility that you might have available:

Example of listing the notifications via `json_pp`

```
$ ./lpac notification list | json_pp
{
  "payload" : {
    "code" : 0,
    "data" : [
      {
        "iccid" : "89000123456789012358",
        "notificationAddress" : "testsmdpplus1.example.com",
        "profileManagementOperation" : 128,
        "seqNumber" : 59
      }
    ],
    "message" : "success"
  },
  "type" : "lpa"
}
```

So we can see there is one notification available, and that the notification number is 59.

Notifications can also be listed from `pySim-shell list_notification` command in the ADF.ISD-R.

7.2.2 Processing notifications

The below `lpac` command can be used to *process* a notification (send it to the respective SM-DP+), identified by its number:

Example of processing a notification (sending it to the SM-DP+)

```
$ ./lpac notification process 59
{"type":"progress","payload":{"code":0,"message":"es9p_handle_notification","data":null}}
{"type":"lpa","payload":{"code":0,"message":"success","data":null}}
```

If that operation was successful (see the `"message": "success"` part above, and the exit status 0 of the process), the notification should be removed from the eUICC.

7.2.3 Removing notifications

The below `lpac` command can be used to remove a given notification (identified by its number) from the eUICC:

Example of removing a notification (local operation on eUICC)

```
$ ./lpac notification remove 59
{"type":"lpa","payload":{"code":0,"message":"success","data":null}}
```

Notifications can also be removed using `pySim-shell remove_notification_from_list` command in the ADF.ISD-R

7.3 Listing, Enabling, Disabling and Deleting of Profiles

Note that those operations can also be performed by `pySim-shell`, which provides slightly better usability due to decoding numerical values like `profileState` into human-readable strings.

7.3.1 Listing installed profiles

Listing installed profiles

```
./lpac profile list | json_pp
{
  "payload" : {
    "code" : 0,
    "data" : [
      {
        "iccid" : "89000123456789012341",
        "isdpAid" : "A0000005591010FFFFFFFFF8900001100",
        "profileClass" : 2,
        "profileName" : "GSMA Generic eUICC Test Profile 1A",
        "profileState" : 0,
        "serviceProviderName" : "GSMA Test 1A"
      },
      {
        "iccid" : "89000123456789012358",
        "isdpAid" : "A0000005591010FFFFFFFFF8900001200",
        "profileClass" : 2,
        "profileName" : "OsmocomProfile",
        "profileState" : 0,
        "serviceProviderName" : "OsmocomSPN"
      }
    ],
    "message" : "success"
  },
  "type" : "lpa"
}
```

Profiles can also be listed using `pySim-shell get_profiles_info` command in the ADF.ISD-R.

7.3.2 Enabling a profile

```
$ ./lpac profile enable 89000123456789012358
{"type":"lpa","payload":{"code":0,"message":"success","data":null}}
```

You can verify the status modification by listing profiles. The enabled profile now has its *profileState* set to 1.

```
./lpac profile list | json_pp
{
  "payload" : {
    "code" : 0,
    "data" : [
      {
        "iccid" : "89000123456789012341",
        "isdpAid" : "A0000005591010FFFFFFFFF8900001100",
        "profileClass" : 2,
        "profileName" : "GSMA Generic eUICC Test Profile 1A",
        "profileState" : 0,
        "serviceProviderName" : "GSMA Test 1A"
      },
      {
        "iccid" : "89000123456789012358",
        "isdpAid" : "A0000005591010FFFFFFFFF8900001200",
        "profileClass" : 2,
        "profileName" : "OsmocomProfile",
        "profileState" : 1,
        "serviceProviderName" : "OsmocomSPN"
      }
    ],
    "message" : "success"
  },
  "type" : "lpa"
}
```

```

        "iccid" : "89000123456789012358",
        "isdpaId" : "A0000005591010FFFFFFFF8900001200",
        "profileClass" : 2,
        "profileName" : "OsmocomProfile",
        "profileState" : 1,
        "serviceProviderName" : "OsmocomSPN"
    },
    ],
    "message" : "success"
},
"type" : "lpa"
}

```

Profiles can also be enabled using `pySim-shell enable_profile` command in the ADF.ISD-R.

Error iccid or aid not found

```

{"type":"lpa","payload":{"code":-1,"message":"es10c_enable_profile","data":"iccid or aid ↵
not found"}}

```

This error is signaled when you try to enable a profile that does not exist (wrong ICCID or AID value).

Error wrong profile reenabling

```

{"type":"lpa","payload":{"code":-1,"message":"es10c_enable_profile","data":"wrong profile ↵
reenabling"}}

```

This error is signalled if you try to enable a non-test (operational) profile while a test profile is still enabled. As per GSMA SGP.22Section 3.2.1 this is not permitted; the test profile must be disabled explicitly and not implicitly in this case. Use the `lpac profile disable` command described below.

7.3.3 Disabling a profile

```

$ ./lpac profile disable 89000123456789012358
{"type":"lpa","payload":{"code":0,"message":"success","data":null}}

```

You can verify the status modification by listing profiles. The enabled profile now has its *profileState* set to 0.

Profiles can also be enabled using `pySim-shell disable_profile` command in the ADF.ISD-R.

7.3.4 Deleting a profile

Note: Deleting profiles is permanent. It is not possible to undo or recover a profile after it has been deleted!

You can delete a given profile (identified by its ICCID) using the `lpac profile delete` command:

```

$ ./lpac profile delete 89000123456789012358
{"type":"lpa","payload":{"code":0,"message":"success","data":null}}

```

You can verify the deletion by listing profiles. The deleted profile is no longer listed among the profiles:

```

$ ./lpac profile list | json_pp
{
  "payload" : {
    "code" : 0,
    "data" : [
      {

```

```
        "iccid" : "89000123456789012341",
        "isdpaId" : "A0000005591010FFFFFFFF8900001100",
        "profileClass" : 2,
        "profileName" : "GSMA Generic eUICC Test Profile 1A",
        "profileState" : 0,
        "serviceProviderName" : "GSMA Test 1A"
    }
},
    "message" : "success"
},
    "type" : "lpa"
}
```

Profiles can also be deleted using pySim-shell `delete_profile` command in the ADF.ISD-R.

8 Using the EasyEUICC implementation of the LPA for Android

DISCLAIMER

EasyEUICC is an independent open source software package which is not part of the sysmoEUICC1 product delivered to you. sysmocom suggests using it for education, research and development purposes, but is not able to provide free support or bug fixing for this third-party program. We are very happy to do so under a separate support services agreement.

EasyEUICC is an open source implementation of the eSIM LPA (Local Profile Assistant) function for consumer eSIM. It is available from [1] and runs on Android devices. Pre-built APK binaries are available from [2].

[1] <https://gitea.angry.im/PeterCxy/OpenEUICC>

[2] <https://gitea.angry.im/PeterCxy/OpenEUICC/releases>

If you have an eUICC (e.g. sysmoEUICC1-C2G) with GSMA certificates, then you can only download eSIM profiles from a GSMA accredited SM-DP+.

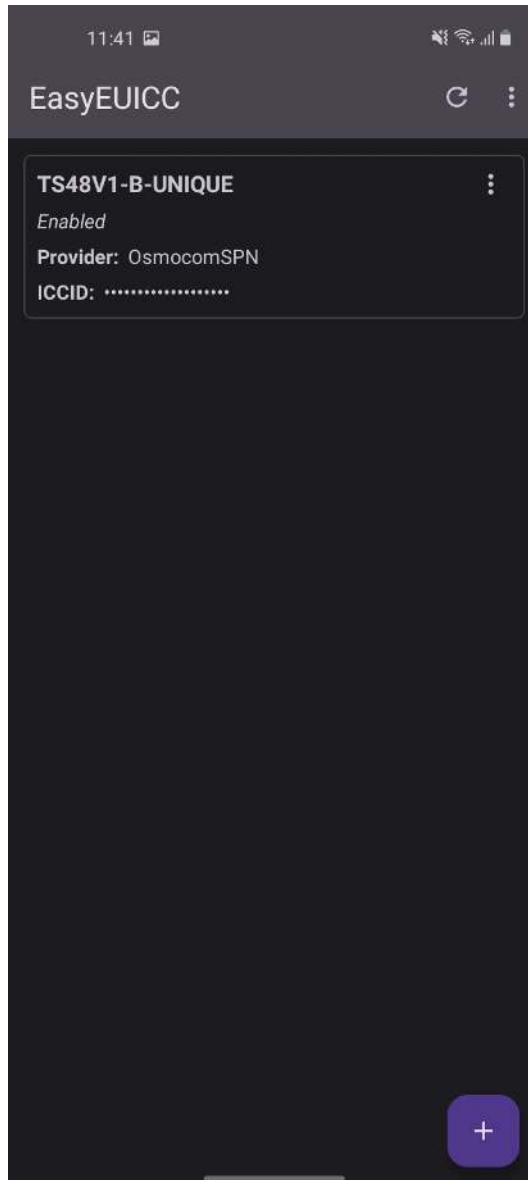
Conversely, if you have an eUICC (e.g. sysmoEUICC1-C2T) with test certificates (or private certificates), then you can only download eSIM profiles from a SM-DP+ with certificates of that same test (or private) certificate authority.

CAUTION

'EasyEUICC' will check the SSL/TLS certificates of the SM-DP+ server to make sure profiles are only downloaded from GSMA accredited SM-DP+ servers. If you use an sysmoEUICC1-C2T on a test SM-DP+ (e.g. `smdpp.test.rsp.sysmocom.de`) which uses GSMA SGP.26 test (or private certificates), then you must ensure that the checkbox 'Ignore SM-DP+ TLS certificate' in the Developer Options (see below) is checked.

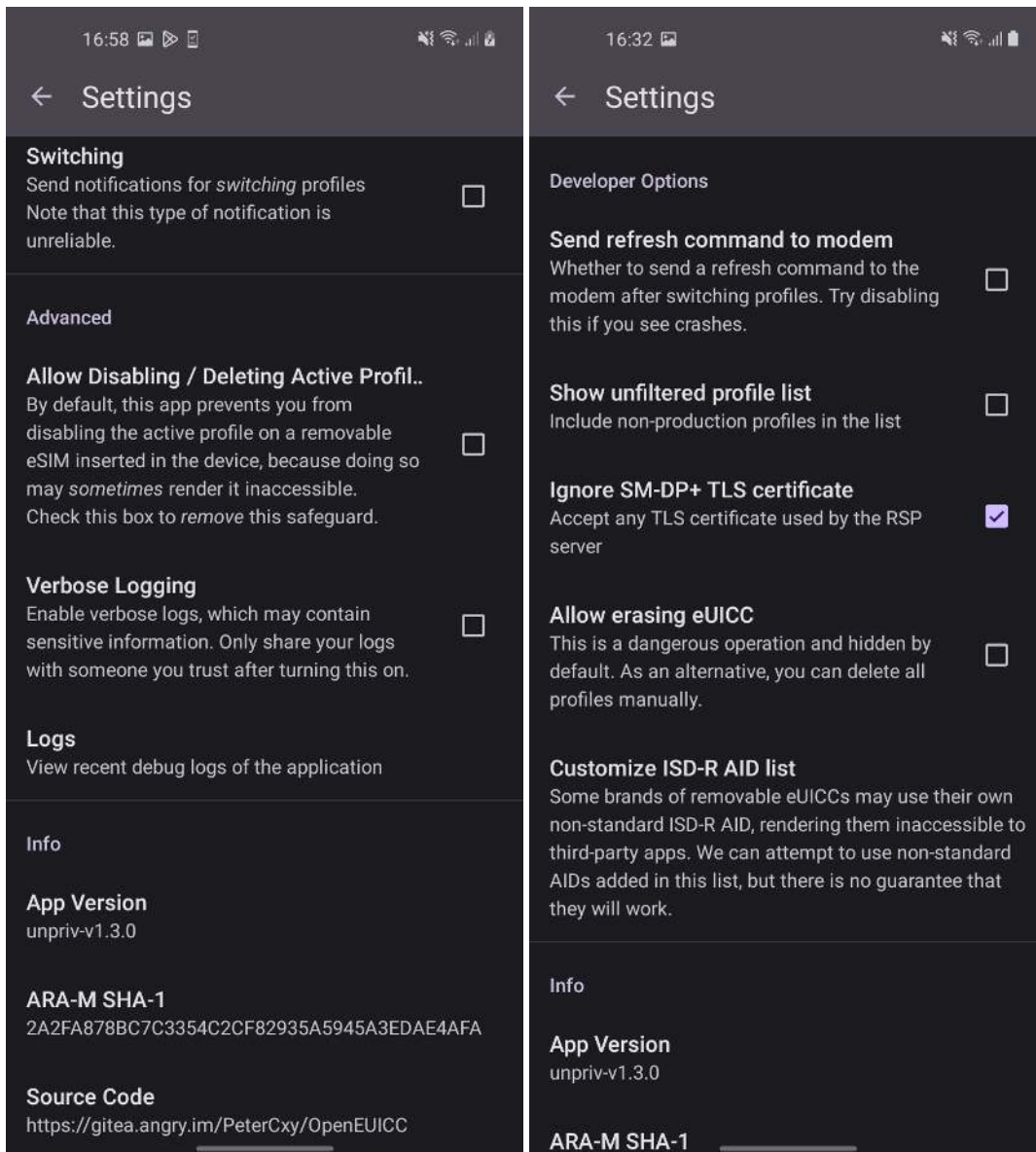
8.1 Main screen

The main screen of EasyEUICC will show you a list of installed eSIM profiles. From there you can enable (switch), rename and delete profiles. On the top right corner, next to the app title, you find the button for the main menu. Also each item in the profile list has its dedicated menu. This menu is reachable through the menu button next to the profile name.



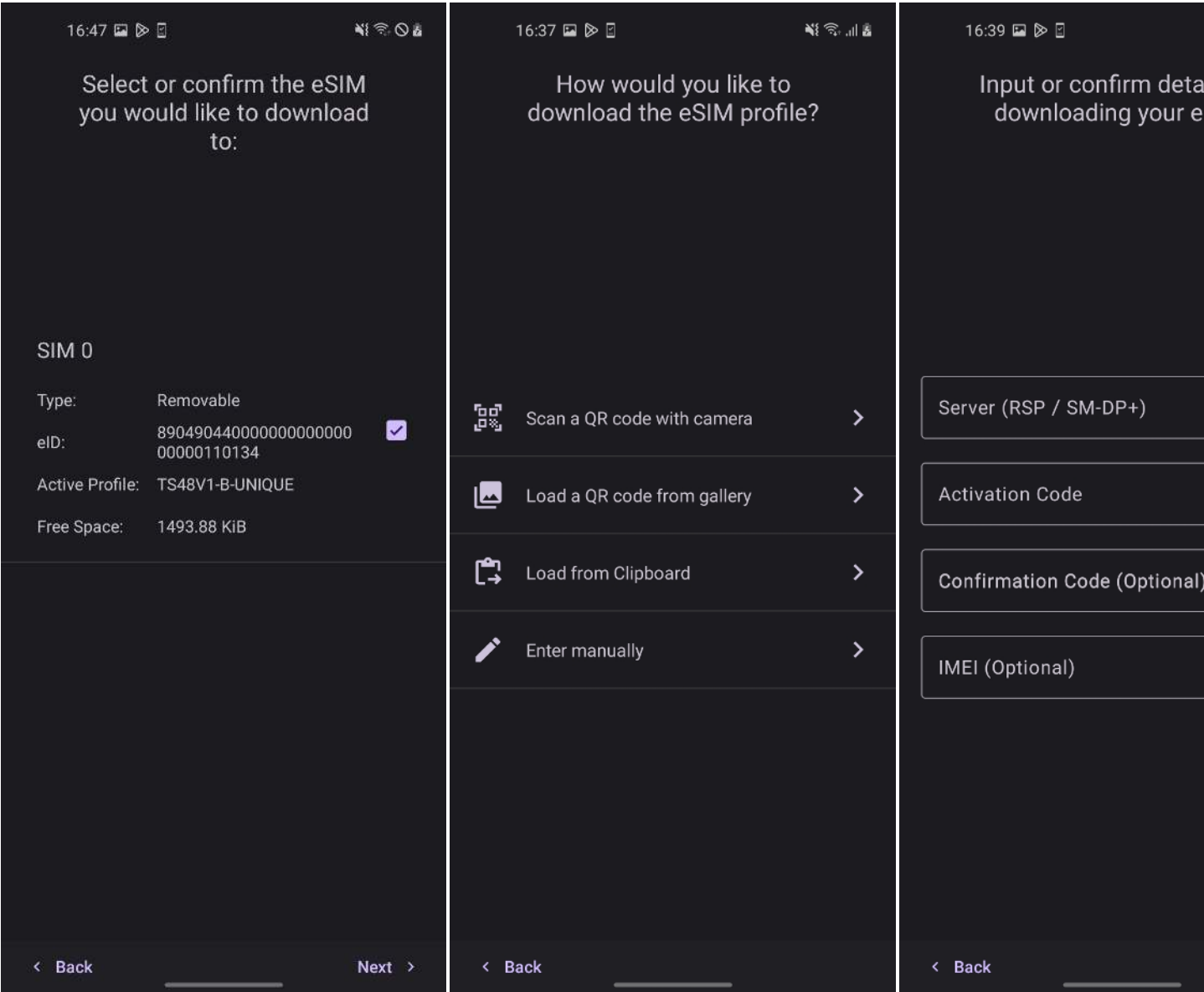
8.2 Settings menu

The settings menu is reachable through the main menu. The standard settings menu only has very few options. To get more options you must enable the developer options by pressing a few times on the App version number you find on in the `Info` section of the menu. (similar to the android developer options)

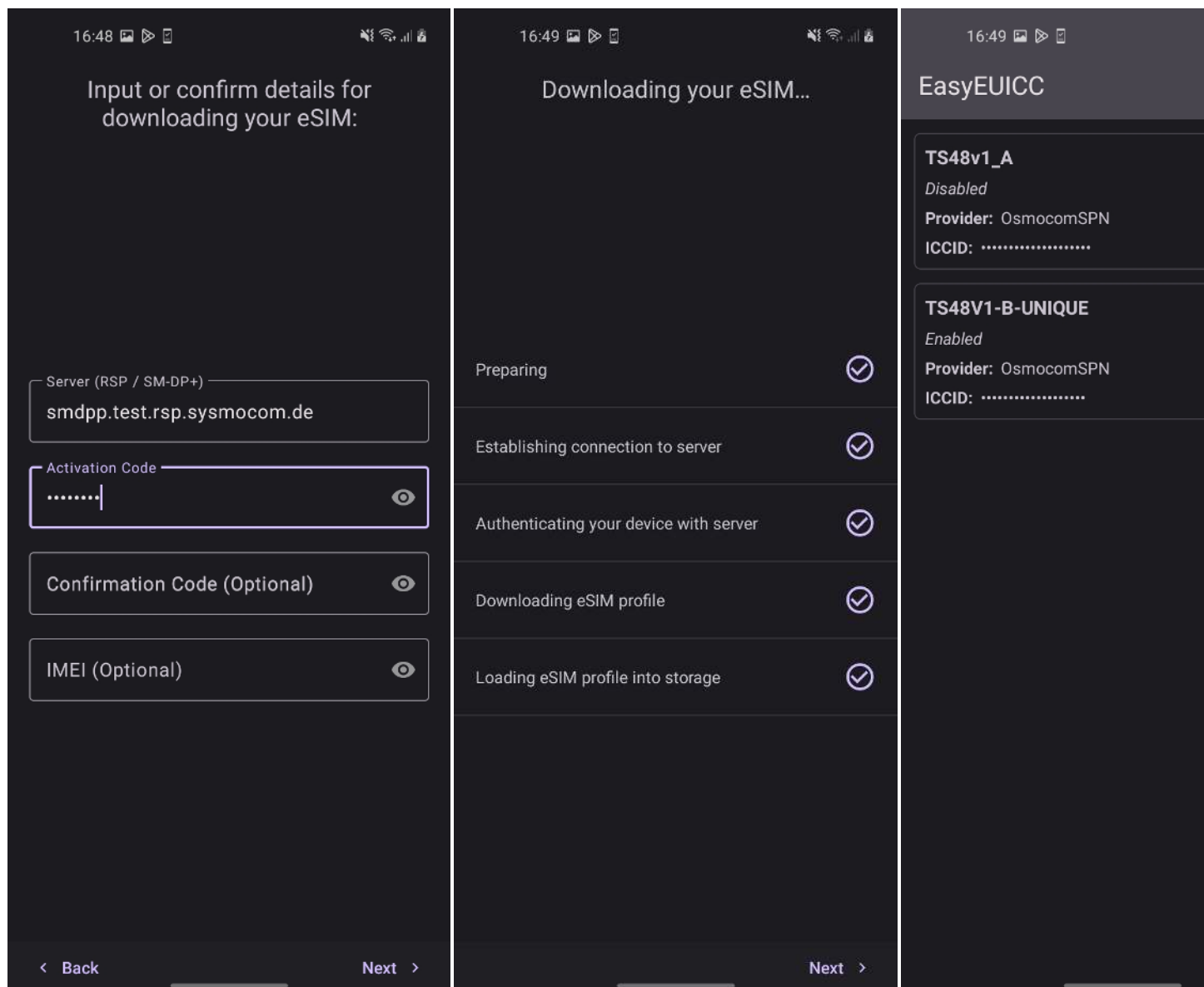


8.3 Downloading an eSIM profile

While in the main screen (list of installed profiles), click on the "+" button in the lower right corner. This will open a dialog that first prompts you to select the eUICC on which the profile should be installed. Then you can select a method to enter the activation code.



If you have a QR-code ready you can use that. Alternatively you can also load the activation code from the clip board or enter it manually.



The download starts when you press the **Next** button in the lower right corner. The application will show you the progress of the individual download steps. When each step has completed, press **Next** again and you should see the installed profile displayed on the main screen. The profile is still in the disabled state. To use it you must enable it first.

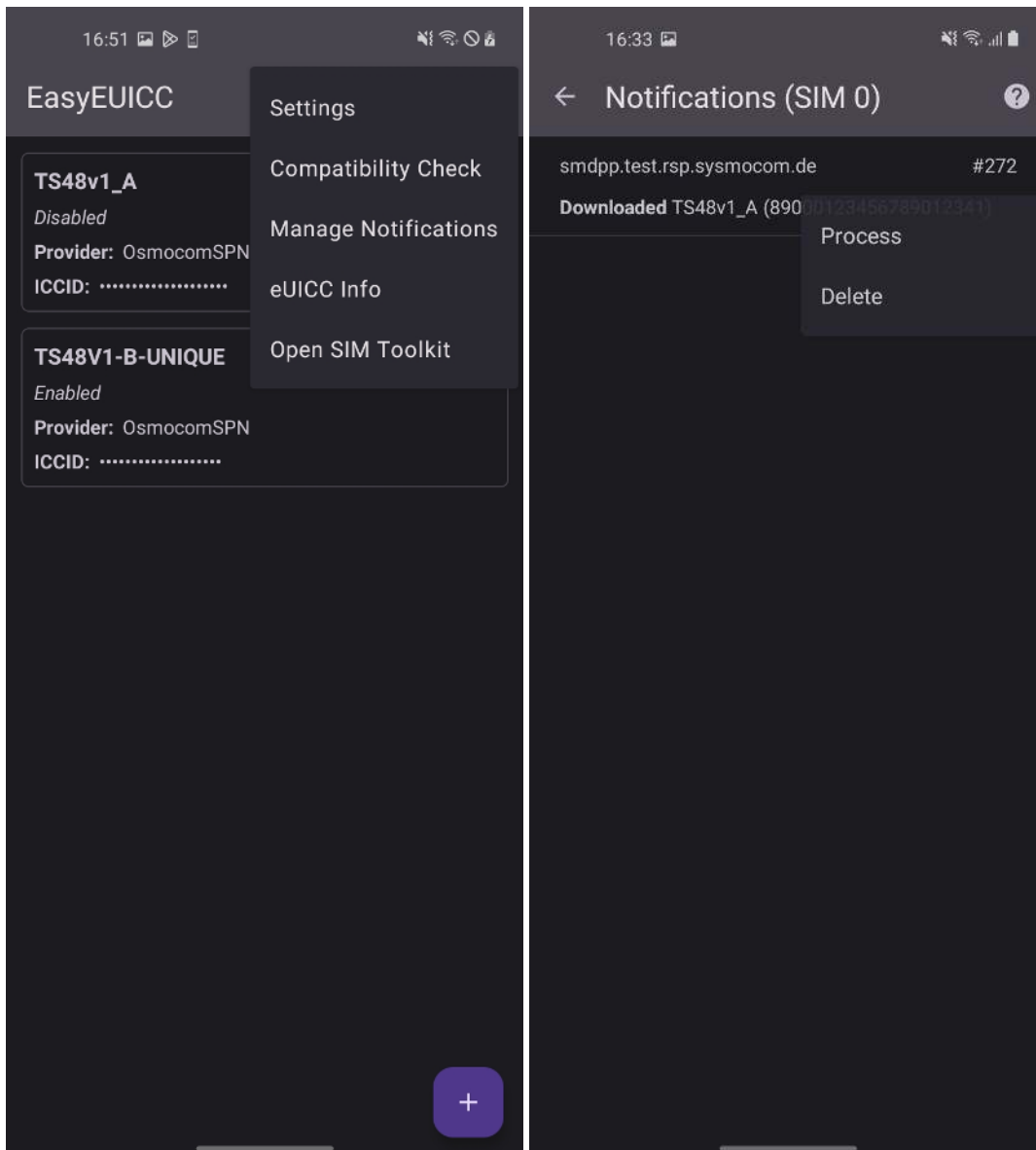
Once the download has completed, a notification will be added to the notification queue on the eUICC (needs manual processing, see below)

NOTE

In case any of the download steps fails a log will be shown. Common failures are problems when reaching the download server or SSL/TLS certificate issues.

8.4 Managing notifications

EasyEUICC, like *lpac*, does not automatically delete notifications generated by the card. Also the processing (forwarding of the notifications to the SMDP+ server) may not be done automatically unless you have configured EasyEUICC to do so (see settings menu).



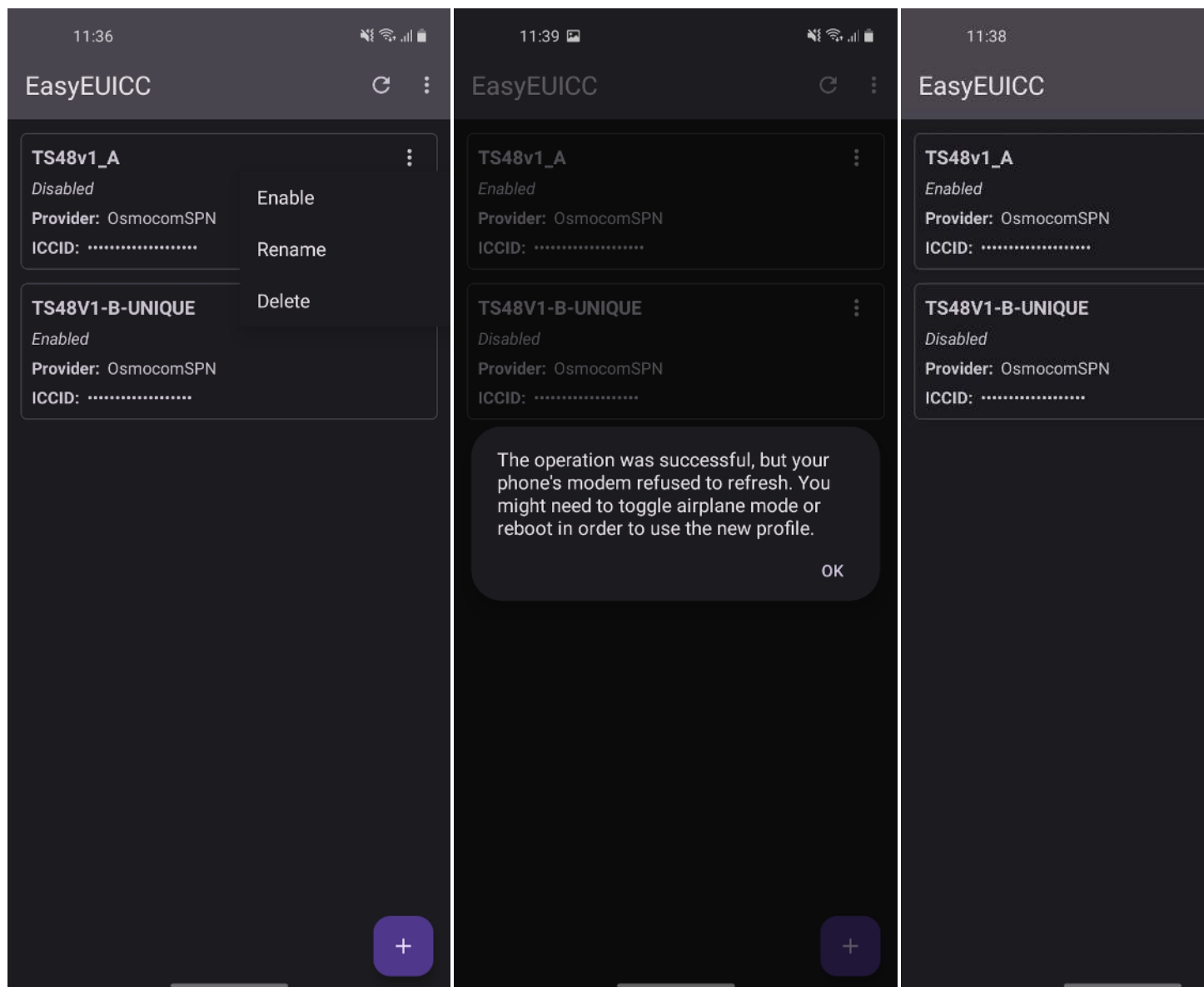
Select *Manage Notifications* from the main menu to get to the list of notifications. Then you can long-press on one of the notifications and select either to *Process* the notification or to *Delete* it. *Process* will send the notification to the SM-DP+. *Delete* will delete the notification.

NOTE

Notifications may be important to properly manage the state of your subscription on the MNO side. Be sure notifications are forwarded properly.

8.4.1 Enabling (switching) a profile

To enable a profile, use the menu next to the profile item. Then press *Enable*. EasyEUICC will then disable the currently enabled profile and enables the profile you chose.

**NOTE**

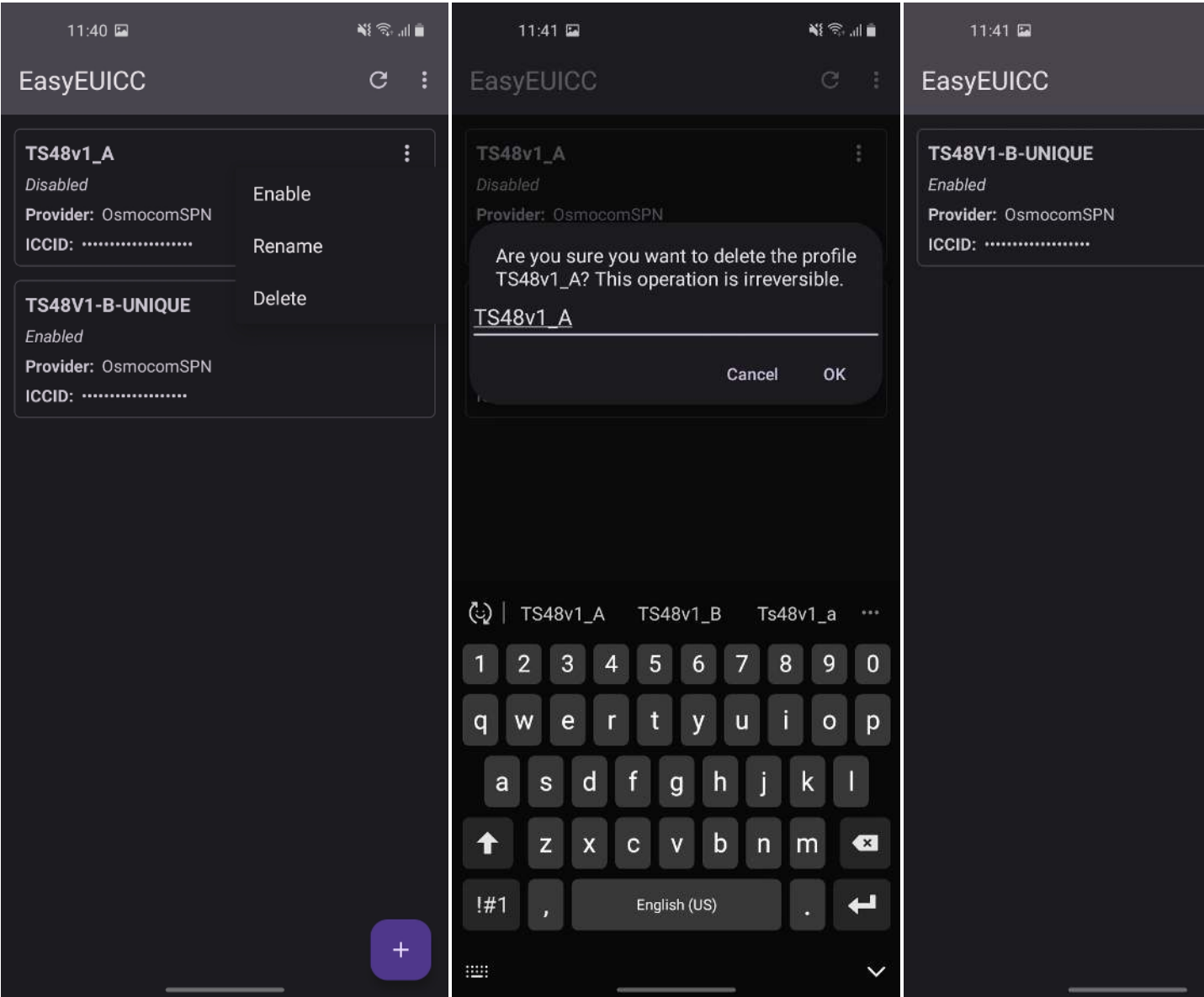
On some phone models there may be problems with sending the refresh signal to the modem. This may cause EasyEUICC to hang and you will have to force-stop the app through the app menu. When you restart EasyEUICC after this, your chosen profile should show up as *Enabled* on the main-screen. To prevent such crashes, uncheck the `Send refresh command to modem` checkbox in the Developer Options (see above).

NOTE

By default, EasyEUICC will not allow you to disable all profiles at once. At least one profile must stay activated. The reason for this is that EasyEUICC might no longer detect your eUICC after a restart without any profile active. If you card has no profile activated for some reason, you can plug the card in a PCSC card-reader and use pySim-shell or lpac to re-enable a profile before re-inserting the card into the phone.

8.4.2 Deleting a profile

Deleting a profile is permanent. There is no way to restore a deleted profile once it has been deleted. To delete a profile, use the menu next to the profile item. Then press `Delete`. EasyEUICC will prompt you to enter the profile name to make sure that you have consciously chosen the correct profile. When the deletion has been successful, the chosen profile will vanish from the profile list.

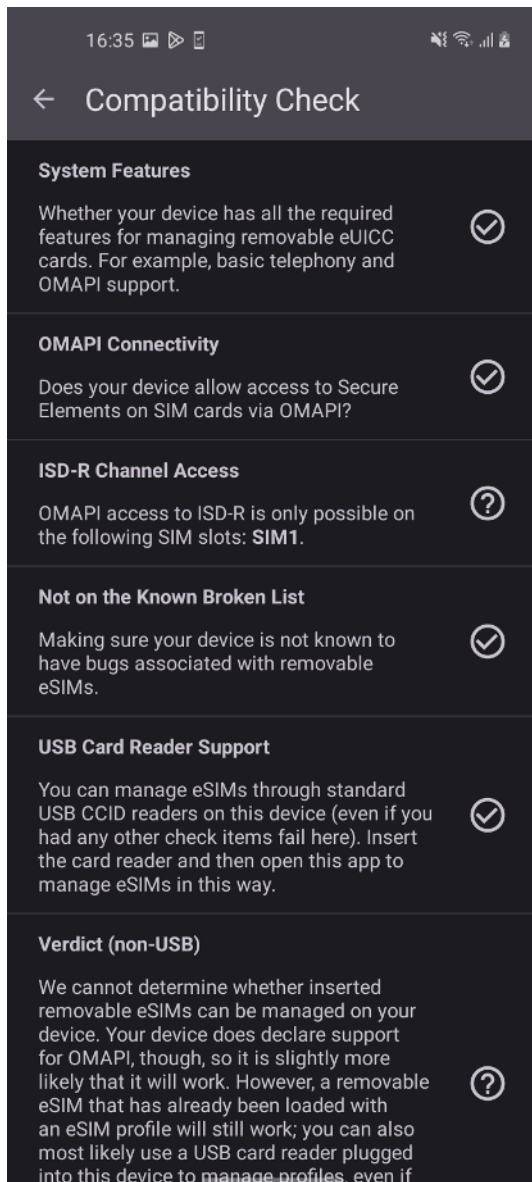


NOTE
EasyEUICC will not let you delete profiles when they are enabled. You must disable the profile first. This can only be done by enabling a different profile. This is to ensure that there is always one active profile installed on your eUICC.

8.5 Troubleshooting

8.5.1 Compatibility Check

EasyEUICC contains a **Compatibility Check** function that can be reached from the main menu.



Usually all items in the checklist should show a check mark. A question mark indicates that a check has detected a problem. In case check marks are missing, this likely means an incompatibility between EasyEUICC and your specific device. Try another phone/device.

However, not in all cases a missing check mark indicates a serious problem. In particular the `ISD-R Channel Access` check may show a check mark in case the phone has multiple sim slots but only one of those slots actually contains an eUICC. In this case one must look carefully on which slot the check has failed. The screenshot (above) was taken on a phone where the eUICC is plugged into slot 0 (SIM0) while slot 1 (SIM1) has been left unpopulated.

8.5.2 EUICC not recognized

If your eUICC is not recognized /listed by EasyEUICC, this usually means that either

- your eUICC is not inserted
- your eUICC is still empty and does not even contain one profile. If this is the case, use another LPA like Section 7 to install a first profile, and then re-try.
- your eUICC does not contain the certificate hash value of the signing key of the EasyEUICC application. The way how Android works, only apps whose APK signing keys hash value is stored on the EUICC will get access. The `sysmoEUICC1-C2T`

samples (from EID value ≥ 13) and sysmoEUICC1-C2G mass produced cards (sysmocom artwork) contain the hash value of the signing key of sysmocom and PeterCxy, meaning official EasyEUICC builds and sysmocom builds should get the required privileges.

9 Using pySim-shell with eUICCs

DISCLAIMER

pySim-shell is an independent open source software package which is not part of the sysmoEUICC delivered to you. sysmocom suggests using it for education, research and development purposes, but is not able to provide free support or bug fixing for this third-party program. We are very happy to help you under a separate support services agreement.

pySim-shell is part off the pySim open source project, a general *swiss army knife* for working with any kind of SIM/USIM/ISIM/HPSIM/CSIM/RUIM/UICC/eUICC cards. It provides an interactive command line interface (the *shell*) to navigate around the the card filesystem, applications, etc.

pySim-shell was primarily designed for use with classic SIM/USIM/ISIM/HPSIM/CSIM/RUIM/UICC cards, but has meanwhile been extended with some eUICC related functionality. Specifically, it implements parts of the ES10a, ES10b and ES10c interfaces by which normally the LPA (or IPA in case of SGP.32 IoT) interfaces with the eUICC.

At time of writing, the main pySim-shell functionalities regarding eUICCs were

- reading out the EID
- listing available profiles
- enabling profiles
- disabling profiles
- deleting profiles
- listing notifications
- deleting notifications

As an eUICC with an *enabled eSIM profile* will just look to the outside like a traditional USIM (possibly with ISIM), you can of course also use all the normal USIM/ISIM features of pySim-shell, such as reading/decoding and or writing/editing the contents of the various files - within the access control rules defined of the respective eSIM profile and your access level (e.g. ADM1 PIN or the like).

The pySim-shell user manual can be found online at <https://downloads.osmocom.org/docs/pysim/master/html/shell.html> and the commands specific for the eUICC ISD-R application are described at <https://downloads.osmocom.org/docs/pysim/master/html/shell.html#eucc-isd-r-commands>

10 osmo-smdpp as a proof-of-concept SM-DP+

DISCLAIMER

osmo-smdpp is an independent open source software package which is not part of the sysmoEUICC delivered to you. sysmocom suggests using it for education, research and development purposes, but is not able to provide free support or bug fixing for this third-party program. We are very happy to help you under a separate support services agreement.

osmo-smdpp is a very new part off the pySim open source project, a general *swiss army knife* for working with any kind of SIM/USIM/ISIM/HPSIM/CSIM/RUIM/UICC/eUICC cards.

The osmo-smdpp user manual can be found at <https://downloads.osmocom.org/docs/pysim/master/html/osmo-smdpp.html>

11 sysmocom SGP.26 test SM-DP+ for Consumer eSIM

sysmocom operates an instance of `osmo-smdpp` using SGP.26 test certificates which is reachable via the public internet, operating at `smdpp.test.rsp.sysmocom.de`.

You can use this hosted test SM-DP+ to download eSIM profiles to eUICCs with SGP.26 test certificates, such as the sysmoEUICC1-C2T. Using the hosted service means you don't need to build/install/setup your own self-hosted `osmo-smdpp`.

You can find more information about this SM-DP+ at <https://test.rsp.sysmocom.de/>

At time of this writing, all SGP.48 test profiles (v1 through v5 of SGP.48) are available for download via the https based ES9+ interface. The related activation codes in text and QR code format are stated on <https://test.rsp.sysmocom.de/>

12 The unsolved ARA-M problem in the case of eUICCs

The sysmoEUICC1 by default installs a so-called ARA-M in the ISD-R. The purpose of this is to authorize apps like EasyEUICC to act as LPA by means of the Android UICC Carrier Privileges mechanism.

Without an ARA-M in the ISD-R, it is not possible to authorize a regular android user application for low-level access to the eUICC, and hence it's impossible to manage (install/activate/deactivate) eSIM profiles from such a user-level application.

A serious problem now arises if you want to download an eSIM profile into the eUICC, and that eSIM profile itself *also contains an ARA-M applet*. In this case, the eUICC will refuse the installation of the eSIM profile. The reason for this is:

- The ARA-M is specified to have a single, well-known AID (without the spec permitting to use suffixes and prefix matching, as it is normally done on many other cases)
- In GlobalPlatform, each AID can only exist once on a card
- Neither the GSMA eSIM specifications nor the GlobalPlatform specifications state whether ISD-R or ISD-P are permitted to bring their own ARA-M.

So the eUICC is **technically correct** to refuse the installation of an eSIM profile containing an ARA-M profile. Even if it were to permit that installation: What should happen at this point when the ARA-M is selected by the UE?

- Should it select the one from the ISD-R? Then only the access rules related to the LPA are active, but not the access rules of the ISD-P, which is what authorizes Android apps of the eSIM-issuing MNO/MVNO to perform operations guarded by UICC Carrier Privileges.
- Or should it select the ARA-M of the ISD-P (eSIM profile)? Then the situation is the opposite: Then only the access rules of the eSIM-issuing MNO/MVNO would be active, but not those of the ISD-R. That in fact means that the LPA software (such as EasyEUICC) can no longer access the eUICC, and you could never enable/disable the eSIM or download any other eSIM profile.

The eUICC is also technically correct if it brings its own ARA-M: There's nothing in the eUICC/eSIM specs that forbid this, and the *GlobalPlatform Secure Element Access Control* spec just states the ARA-M shall be in the *Issuer SD* with nobody defining whether that means ISD-R or ISD-P in an eUICC.

12.1 Affected eSIM profiles

We so far know of eSIM profiles of the following operators that contain an ARA-M applet and hence run into the above-mentioned clash:

- AT&T US
- Vodafone DE
- Vodafone UK

An updated list is kept in the *eSIM profile database wiki page* in the Osmocom wiki at https://osmocom.org/projects/sim-card-related/wiki/ESIM_profile_database

If you know or suspect of any other affected eSIM profiles, please do report them to the contact address stated on that wiki page.

12.2 Further Reading

See <https://discourse.osmocom.org/t/conflict-between-euicc-access-rules-ara-and-esim-profile-access-rules/395>

12.3 Solutions

Real solutions are hard and will likely take years to materialise, until the standards organizations (GSMA, Trusted Connectivity Alliance and/or GlobalPlatform) have managed to settle this conflict and come up with an interoperable solution.

12.4 Workarounds

12.4.1 eUICCs without ARA-M in ISD-R

If you prefer your eUICCs without an ARA-M in the ISD-R, sysmocom is capable to remove it from cards. This is best done prior to shipping, but in theory can also be done remotely *once we developed software supporting such remote modification*.

Obviously, you can not use the EasyEUICC LPA on a normal, non-rooted Android anymore at that point.

Please reach out to support@sysmocom.de if you required cards without ARA-M.

12.4.2 eSIM profile with non-mandatory ARA-M

If you have a good technical contact to your eSIM-profile-issuing MNO/MVNO, you can ask them to provide you with an eSIM profile that does not set the *mandated* flag for the *application Profile Element* of the ARA-M.

This basically makes an installation failure of the ARA-M in the eSIM profile non-fatal:

- If the eUICC doesn't have an ARA-M in its ISD-R, the ARA-M of the eSIM profile will become active.
- If the eUICC has an ARA-M in its ISD-R, the one in the profile will fail, but the eSIM can still be installed.

13 sysmoEUICC1 changelog

This chapter documents the changes to the sysmoEUICC1 product over time.

13.1 sysmoEUICC1-C2G v0 (November 2023)

- initial product release
- white plastic card

13.2 sysmoEUICC1-C2G v1 (May 2024)

- plastic card with pink sysmocom artwork
- Add ARA applet to ISD-R
- Enable SCP03 to ECASD
- Enable SCP03 to ISD-R
- Attempt to enable SCP80 + SCP81 to ISD-R (untested)
- Add ISD-A security domain with SCP03 enabled
- Pre-install a TS.48 eSIM test profile

14 Acknowledgements

sysmocom would like to thank a number of individuals in the context of improving the availability of freely available programmable SIM cards and related tools

- **Sylvain Munaut** for developing the original `pySim` tool
- **Philipp Maier** for developing the `sysmo-usim-tool`
- **Benoit Michau** for the python `card` abstraction library
- **Kevin Redon** for `Osmocom SIMtrace`
- **Eric Butler** and **Karl Koscher** of shadyltel for their hello world Java cardlet and the `sim-tools` for OTA installation
- **Supreeth Herle** for all of his research on the role of SIM cards in VoLTE/IMS, CarrierPrivileges and many related contributions to `pySim`
- **Bertrand Martel** for his open source implementation `ARA-M` applet, which we also pre-install on the `sysmoISIM-SJA2`
- **Martin Paljak** for his work on `GlobalPlatformPro`

15 Glossary

2FF

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

3FF

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

3GPP

3rd Generation Partnership Project

4FF

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

A Interface

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

A3/A8

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

A5

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

Abis Interface

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

ACC

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

AGCH

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

AGPL

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

AQPSK

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

ARFCN

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

AUC

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

BCCH

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

BCC

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

BTS

Base Transceiver Station

BSC

Base Station Controller

BSIC

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

BSSGP

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

BVCI

BSSGP Virtual Circuit Identifier

CBC

Cell Broadcast Centre; central entity of Cell Broadcast service

CBCH

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

CBS

Cell Broadcast Service

CBSP

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

CC

Call Control; Part of the GSM Layer 3 Protocol

CCCH

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

Cell

A cell in a cellular network, served by a BTS

CEPT

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

CGI

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

CSFB

Circuit-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

dnxload

Tool to program UBL and the Bootloader on a sysmoBTS

EDGE

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

EGPRS

Enhanced GPRS; the part of EDGE relating to GPRS services

EIR

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

ESME

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

ETSI

European Telecommunications Standardization Institute

FPGA

Field Programmable Gate Array; programmable digital logic hardware

Gb

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

GERAN

GPRS/EDGE Radio Access Network

GGSN

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

GMSK

Gaussian Minimum Shift Keying; modulation used for GSM and GPRS

GPL

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

Gp

Gp interface between SGSN and GGSN; uses GTP protocol

GPRS

General Packet Radio Service; the packet switched 2G technology

GPS

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

GSM

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

GSMTAP

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

GSUP

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

GT

Global Title; an address in SCCP

GTP

GPRS Tunnel Protocol; used between SGSN and GGSN

HLR

Home Location Register; central subscriber database of a GSM network

HNB-GW

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

HPLMN

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

IE

Information Element

IMEI

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

IMEISV

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

IMSI

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

IP

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

IPA

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

Iu

Interface in 3G/UMTS between RAN and CN

IuCS

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

IuPS

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

LAC

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

LAPD

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

LAPDm

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

LLC

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

Location Area

Location Area; a geographic area containing multiple BTS

LU

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

M2PA

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

M2UA

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

M3UA

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

MCC

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

MMF

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

MGW

Media Gateway

MM

Mobility Management; part of the GSM Layer 3 Protocol

MNC

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

MNCC

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

MNO

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

MO

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

MS

Mobile Station; a mobile phone / GSM Modem

MSC

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

MSC pool

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

MSISDN

Mobile Subscriber ISDN Number; telephone number of the subscriber

MT

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

MTP

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

MVNO

Mobile Virtual Network Operator; Operator without physical radio network

NCC

Network Color Code; assigned by national regulator

NITB

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

NRI

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

NSEI

NS Entity Identifier

NVCI

NS Virtual Circuit Identifier

NWL

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

NS

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

OCXO

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

OML

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

OpenBSC

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

OpenGGSN

Open Source implementation of a GPRS Packet Control Unit

OpenVPN

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

Osmocom

Open Source MOBILE COMMUNICATIONS; collaborative community for implementing communications protocols and systems, including GSM, GPRS, TETRA, DECT, GMR and others

OsmoBSC

Open Source implementation of a GSM Base Station Controller

OsmoNITB

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

OsmoSGSN

Open Source implementation of a Serving GPRS Support Node

OsmoPCU

Open Source implementation of a GPRS Packet Control Unit

OTA

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

PC

Point Code; an address in MTP

PCH

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

PCP

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

PCU

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

PDCH

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

PIN

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

PLMN

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

PUK

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

RAC

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

RACH

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

RAM

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

RF

Radio Frequency

RFM

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

Roaming

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

Routing Area

Routing Area; GPRS specific sub-division of Location Area

RR

Radio Resources; Part of the GSM Layer 3 Protocol

RSL

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

RTP

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

SACCH

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

SCCP

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

SDCCH

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

SDK

Software Development Kit

SGs

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

SGSN

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

SIGTRAN

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

SIM

Subscriber Identity Module; small chip card storing subscriber identity

Site

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

SMPP

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

SMSC

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

SS7

Signaling System No. 7; Classic digital telephony signaling system

SS

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

SSH

Secure Shell; *IETF RFC 4250* [\[ietf-rfc4251\]](#) to 4254

SSN

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

STP

Signaling Transfer Point; A Router in SS7 Networks

SUA

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

syslog

System logging service of UNIX-like operating systems

System Information

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

TCH

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

TCP

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

TFTP

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

TOS

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

TRX

Transceiver; element of a BTS serving a single carrier

TS

Technical Specification

u-Boot

Boot loader used in various embedded systems

UBI

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

UBL

Initial bootloader loaded by the TI Davinci SoC

UDP

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

UICC

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

Um interface

U mobile; Radio interface between MS and BTS

uplink

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

USIM

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

USSD

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

VAMOS

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

VCTCXO

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

VLAN

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

VLR

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

VPLMN

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

VTY

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

A Osmocom TCP/UDP Port Numbers

The Osmocom GSM system utilizes a variety of TCP/IP based protocols. The table below provides a reference as to which port numbers are used by which protocol / interface.

Table 1: TCP/UDP port numbers

| L4 Protocol | Port Number | Purpose | Software |
|-------------|-------------|---------|-------------------------|
| UDP | 1984 | Osmux | osmo-mgw, osmo-bts |
| UDP | 2427 | MGCP GW | osmo-bsc_mgcp, osmo-mgw |

Table 1: (continued)

| L4 Protocol | Port Number | Purpose | Software |
|-------------|-------------|--|-----------------------------------|
| TCP | 2775 | SMPP (SMS interface for external programs) | osmo-nitb |
| TCP | 3002 | A-bis/IP OML | osmo-bts, osmo-bsc, osmo-nitb |
| TCP | 3003 | A-bis/IP RSL | osmo-bts, osmo-bsc, osmo-nitb |
| TCP | 4227 | telnet (VTY) | osmo-pcap-client |
| TCP | 4228 | telnet (VTY) | osmo-pcap-server |
| TCP | 4236 | Control Interface | osmo-trx |
| TCP | 4237 | telnet (VTY) | osmo-trx |
| TCP | 4238 | Control Interface | osmo-bts |
| TCP | 4239 | telnet (VTY) | osmo-stp |
| TCP | 4240 | telnet (VTY) | osmo-pcu |
| TCP | 4241 | telnet (VTY) | osmo-bts |
| TCP | 4242 | telnet (VTY) | osmo-nitb, osmo-bsc, cellmgr-ng |
| TCP | 4243 | telnet (VTY) | osmo-bsc_mgcp, osmo-mgw |
| TCP | 4244 | telnet (VTY) | osmo-bsc_nat |
| TCP | 4245 | telnet (VTY) | osmo-sgsn |
| TCP | 4246 | telnet (VTY) | osmo-gbproxy |
| TCP | 4247 | telnet (VTY) | OsmocomBB |
| TCP | 4249 | Control Interface | osmo-nitb, osmo-bsc |
| TCP | 4250 | Control Interface | osmo-bsc_nat |
| TCP | 4251 | Control Interface | osmo-sgsn |
| TCP | 4252 | telnet (VTY) | sysmobts-mgr |
| TCP | 4253 | telnet (VTY) | osmo-gtphub |
| TCP | 4254 | telnet (VTY) | osmo-msc |
| TCP | 4255 | Control Interface | osmo-msc |
| TCP | 4256 | telnet (VTY) | osmo-sip-connector |
| TCP | 4257 | Control Interface | osmo-ggsn, ggsn (OpenGGSN) |
| TCP | 4258 | telnet (VTY) | osmo-hlr |
| TCP | 4259 | Control Interface | osmo-hlr |
| TCP | 4260 | telnet (VTY) | osmo-ggsn |
| TCP | 4261 | telnet (VTY) | osmo-hnbgw |
| TCP | 4262 | Control Interface | osmo-hnbgw |
| TCP | 4263 | Control Interface | osmo-gbproxy |
| TCP | 4264 | telnet (VTY) | osmo-cbc |
| TCP | 4265 | Control Interface | osmo-cbc |
| TCP | 4266 | D-GSM MS Lookup: mDNS serve | osmo-hlr |
| TCP | 4267 | Control Interface | osmo-mgw |
| TCP | 4268 | telnet (VTY) | osmo-uecups |
| SCTP | 4268 | UECUPS | osmo-uecups |
| TCP | 4269 | telnet (VTY) | osmo-e1d |
| TCP | 4270 | telnet (VTY) | osmo-isdntap |
| TCP | 4271 | telnet (VTY) | osmo-smlc |
| TCP | 4272 | Control Interface | osmo-smlc |
| TCP | 4273 | telnet (VTY) | osmo-hnodeb |
| TCP | 4274 | Control Interface | osmo-hnodeb |
| TCP | 4275 | telnet (VTY) | osmo-upf |
| TCP | 4276 | Control Interface | osmo-upf |
| TCP | 4277 | telnet (VTY) | osmo-pfcp-tool |
| TCP | 4278 | Control Interface | osmo-pfcp-tool |
| UDP | 4729 | GSMTAP | Almost every osmocom project |
| TCP | 5000 | A/IP | osmo-bsc, osmo-bsc_nat |
| UDP | 23000 | GPRS-NS over IP default port | osmo-pcu, osmo-sgsn, osmo-gbproxy |
| TCP | 48049 | BSC-CBC (CBSP) default port | osmo-bsc, osmo-cbc |

B Bibliography / References

References

- [1] [userman-ice1usb] Osmocom Project: icE1usb User Manual.
- [2] [userman-ogt] Pau Espin: osmo-gsm-tester User Manual.
- [3] [userman-remsim] Harald Welte: osmo-remsim User Manual.
- [4] [osmobts-abis-spec] Neels Hofmeyr & Harald Welte. OsmoBTS Abis Protocol Specification. <https://ftp.osmocom.org/docs/latest/osmobts-abis.pdf>
- [5] [userman-osmobsc] Osmocom Project: OsmoBSC User Manual. <https://ftp.osmocom.org/docs/latest/osmobsc-usermanual.pdf>
- [6] [vty-ref-osmobsc] Osmocom Project: OsmoBSC VTY Reference Manual. <https://ftp.osmocom.org/docs/latest/osmobsc-vty-reference.pdf>
- [7] [userman-osmobts] Osmocom Project: OsmoBTS User Manual. <https://ftp.osmocom.org/docs/latest/osmobts-usermanual.pdf>
- [8] [vty-ref-osmobts] Osmocom Project: OsmoBTS VTY Reference Manual. <https://ftp.osmocom.org/docs/latest/osmobts-trx-vty-reference.pdf> <https://ftp.osmocom.org/docs/latest/osmobts-sysmo-vty-reference.pdf> <https://ftp.osmocom.org/docs/latest/osmobts-lc15-vty-reference.pdf> <https://ftp.osmocom.org/docs/latest/osmobts-oc2g-vty-reference.pdf> <https://ftp.osmocom.org/docs/latest/osmobts-octphy-vty-reference.pdf> <https://ftp.osmocom.org/docs/latest/osmobts-virtual-vty-reference.pdf>
- [9] [userman-osmocbc] Osmocom Project: OsmoCBC User Manual. <https://ftp.osmocom.org/docs/latest/osmocbc-usermanual.pdf>
- [10] [vty-ref-osmocbc] Osmocom Project: OsmoCBC VTY Reference Manual. <https://ftp.osmocom.org/docs/latest/osmocbc-vty-reference.pdf>
- [11] [userman-osmogbproxy] Osmocom Project: OsmoGBProxy User Manual. <https://ftp.osmocom.org/docs/latest/osmogbproxy-usermanual.pdf>
- [12] [vty-ref-osmogbproxy] Osmocom Project: OsmoGBPROxy VTY Reference Manual. <https://ftp.osmocom.org/docs/latest/osmogbproxy-vty-reference.pdf>
- [13] [userman-osmoggsn] Osmocom Project: OpenGGSN User Manual. <https://ftp.osmocom.org/docs/latest/osmoggsn-usermanual.pdf>
- [14] [vty-ref-osmoggsn] Osmocom Project: OsmoGGSN VTY Reference Manual. <https://ftp.osmocom.org/docs/latest/osmoggsn-vty-reference.pdf>
- [15] [userman-osmohlr] Osmocom Project: OsmoHLR User Manual. <https://ftp.osmocom.org/docs/latest/osmohlr-usermanual.pdf>
- [16] [vty-ref-osmohlr] Osmocom Project: OsmoHLR VTY Reference Manual. <https://ftp.osmocom.org/docs/latest/osmohlr-vty-reference.pdf>
- [17] [userman-osmohnbgw] Osmocom Project: OsmoHNBGW User Manual. <https://ftp.osmocom.org/docs/latest/osmohnbgw-usermanual.pdf>
- [18] [vty-ref-osmohnbgw] Osmocom Project: OsmoHNBGW VTY Reference Manual. <https://ftp.osmocom.org/docs/latest/osmohnbgw-vty-reference.pdf>
- [19] [userman-osmomgw] Osmocom Project: OsmoMGW User Manual. <https://ftp.osmocom.org/docs/latest/osmomgw-usermanual.pdf>

- [20] [vty-ref-osmongw] Osmocom Project: OsmoMGW VTY Reference Manual. <https://ftp.osmocom.org/docs/latest/osmongw-vty-reference.pdf>
- [21] [userman-osmomsc] Osmocom Project: OsmoMSC User Manual. <https://ftp.osmocom.org/docs/latest/osmomsc-usermanual.pdf>
- [22] [vty-ref-osmomsc] Osmocom Project: OsmoMSC VTY Reference Manual. <https://ftp.osmocom.org/docs/latest/osmomsc-vty-reference.pdf>
- [23] [userman-osmonitb] Osmocom Project: OsmoNITB User Manual. <https://ftp.osmocom.org/docs/latest/osmonitb-usermanual.pdf>
- [24] [vty-ref-osmonitb] Osmocom Project: OsmoNITB VTY Reference Manual. <https://ftp.osmocom.org/docs/latest/osmonitb-vty-reference.pdf>
- [25] [userman-osmopcu] Osmocom Project: OsmoPCU User Manual. <https://ftp.osmocom.org/docs/latest/osmopcu-usermanual.pdf>
- [26] [vty-ref-osmopcu] Osmocom Project: OsmoPCU VTY Reference Manual. <https://ftp.osmocom.org/docs/latest/osmopcu-vty-reference.pdf>
- [27] [userman-osmosgsn] Osmocom Project: OsmoSGSN User Manual. <https://ftp.osmocom.org/docs/latest/osmosgsn-usermanual.pdf>
- [28] [vty-ref-osmosgsn] Osmocom Project: OsmoSGSN VTY Reference Manual. <https://ftp.osmocom.org/docs/latest/osmosgsn-vty-reference.pdf>
- [29] [userman-osmosipconnector] Osmocom Project: OsmoSIPconnector User Manual. <https://ftp.osmocom.org/docs/latest/osmosipconnector-usermanual.pdf>
- [30] [vty-ref-osmosipconnector] Osmocom Project: OsmoSIPconnector VTY Reference Manual. <https://ftp.osmocom.org/docs/latest/osmosipconnector-vty-reference.pdf>
- [31] [userman-osmosmlc] Osmocom Project: OsmoSMMLC User Manual. <https://ftp.osmocom.org/docs/latest/osmosmlc-usermanual.pdf>
- [32] [vty-ref-osmosmlc] Osmocom Project: OsmoSMMLC VTY Reference Manual. <https://ftp.osmocom.org/docs/latest/osmosmlc-vty-reference.pdf>
- [33] [userman-osmostp] Osmocom Project: OsmoSTP User Manual. <https://ftp.osmocom.org/docs/latest/osmostp-usermanual.pdf>
- [34] [vty-ref-osmostp] Osmocom Project: OsmoSTP VTY Reference Manual. <https://ftp.osmocom.org/docs/latest/osmostp-vty-reference.pdf>
- [35] [userman-osmotrx] Osmocom Project: OsmoTRX User Manual. <https://ftp.osmocom.org/docs/latest/osmotrx-usermanual.pdf>
- [36] [vty-ref-osmotrx] Osmocom Project: OsmoTRX VTY Reference Manual. <https://ftp.osmocom.org/docs/latest/osmotrx-uhd-vty-reference.pdf> <https://ftp.osmocom.org/docs/latest/osmotrx-lms-vty-reference.pdf> <https://ftp.osmocom.org/docs/latest/osmotrx-ipc-vty-reference.pdf> <https://ftp.osmocom.org/docs/latest/osmotrx-usrp1-vty-reference.pdf>
- [37] [3gpp-ts-23-041] 3GPP TS 23.041: Technical realization of Cell Broadcast Service (CBS)
- [38] [3gpp-ts-23-048] 3GPP TS 23.048: Security mechanisms for the (U)SIM application toolkit; Stage 2 <https://www.3gpp.org/DynaReport/23048.htm>
- [39] [3gpp-ts-23-236] 3GPP TS 23.236: Intra-domain connection of Radio Access Network (RAN) nodes to multiple Core Network (CN) nodes <https://www.3gpp.org/DynaReport/23236.htm>
- [40] [3gpp-ts-24-007] 3GPP TS 24.007: Mobile radio interface signalling layer 3; General Aspects <https://www.3gpp.org/DynaReport/24007.htm>

- [41] [3gpp-ts-24-008] 3GPP TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols; Stage 3. <https://www.3gpp.org/dynareport/24008.htm>
- [42] [3gpp-ts-31-101] 3GPP TS 31.101: UICC-terminal interface; Physical and logical characteristics <https://www.3gpp.org/DynaReport/31101.htm>
- [43] [3gpp-ts-31-102] 3GPP TS 31.102: Characteristics of the Universal Subscriber Identity Module (USIM) application <https://www.3gpp.org/DynaReport/31102.htm>
- [44] [3gpp-ts-31-103] 3GPP TS 31.103: Characteristics of the IMS Subscriber Identity Module (ISIM) application <https://www.3gpp.org/DynaReport/31103.htm>
- [45] [3gpp-ts-31-111] 3GPP TS 31.111: Universal Subscriber Identity Module (USIM) Application Toolkit (USAT) <https://www.3gpp.org/DynaReport/31111.htm>
- [46] [3gpp-ts-31-115] 3GPP TS 31.115: Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications <https://www.3gpp.org/DynaReport/31115.htm>
- [47] [3gpp-ts-31-116] 3GPP TS 31.116: Remote APDU Structure for (U)SIM Toolkit applications <https://www.3gpp.org/DynaReport/31116.htm>
- [48] [3gpp-ts-35-205] 3GPP TS 35.205: 3G Security; Specification of the MILENAGE algorithm set: General
- [49] [3gpp-ts-35-206] 3GPP TS 35.206: 3G Security; Specification of the MILENAGE algorithm set: Algorithm specification <https://www.3gpp.org/DynaReport/35206.htm>
- [50] [3gpp-ts-44-006] 3GPP TS 44.006: Mobile Station - Base Station System (MS - BSS) interface; Data Link (DL) layer specification <https://www.3gpp.org/DynaReport/44006.htm>
- [51] [3gpp-ts-44-018] 3GPP TS 44.018: Mobile radio interface layer 3 specification; Radio Resource Control (RRC) protocol <https://www.3gpp.org/DynaReport/44018.htm>
- [52] [3gpp-ts-44-064] 3GPP TS 44.064: Mobile Station - Serving GPRS Support Node (MS-SGSN); Logical Link Control (LLC) Layer Specification <https://www.3gpp.org/DynaReport/44064.htm>
- [53] [3gpp-ts-45-002] 3GPP TS 45.002: Digital cellular telecommunications system (Phase 2+) (GSM); GSM/EDGE Multiplexing and multiple access on the radio path <https://www.3gpp.org/DynaReport/45002.htm>
- [54] [3gpp-ts-48-008] 3GPP TS 48.008: Mobile Switching Centre - Base Station system (MSC-BSS) interface; Layer 3 specification <https://www.3gpp.org/DynaReport/48008.htm>
- [55] [3gpp-ts-48-016] 3GPP TS 48.016: General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN) interface; Network service <https://www.3gpp.org/DynaReport/48016.htm>
- [56] [3gpp-ts-48-018] 3GPP TS 48.018: General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN); BSS GPRS protocol (BSSGP) <https://www.3gpp.org/DynaReport/48018.htm>
- [57] [3gpp-ts-48-049] 3GPP TS 48.049: Digital cellular communications system; Base Station Controller - Cell Broadcast Centre (BSC-CBC) interface specification; Cell Broadcast Service Protocol (CBSP) <https://www.3gpp.org/DynaReport/48049.htm>
- [58] [3gpp-ts-48-056] 3GPP TS 48.056: Base Station Controller - Base Transceiver Station (BSC - BTS) interface; Layer 2 specification <https://www.3gpp.org/DynaReport/48056.htm>
- [59] [3gpp-ts-48-058] 3GPP TS 48.058: Base Station Controller - Base Transceiver Station (BSC - BTS) Interface; Layer 3 specification <https://www.3gpp.org/DynaReport/48058.htm>
- [60] [3gpp-ts-51-011] 3GPP TS 51.011: Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface
- [61] [3gpp-ts-51-014] 3GPP TS 51.014: Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface <https://www.3gpp.org/DynaReport/51014.htm>
- [62] [3gpp-ts-52-021] 3GPP TS 52.021: Network Management (NM) procedures and messages on the A-bis interface <https://www.3gpp.org/DynaReport/52021.htm>

- [63] [etsi-tr102216] ETSI TR 102 216: Smart cards https://www.etsi.org/deliver/etsi_tr/102200_102299/102216/-03.00.00_60/tr_102216v030000p.pdf
- [64] [etsi-ts102221] ETSI TS 102 221: Smart Cards; UICC-Terminal interface; Physical and logical characteristics https://www.etsi.org/deliver/etsi_ts/102200_102299/102221/13.01.00_60/ts_102221v130100p.pdf
- [65] [etsi-ts101220] ETSI TS 101 220: Smart Cards; ETSI numbering system for telecommunication application providers https://www.etsi.org/deliver/etsi_ts/101200_101299/101220/12.00.00_60/ts_101220v120000p.pdf
- [66] [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 IPv4 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>
- [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>