Application Note

EUICC PROVISIONING FOR CONSUMER AND M2M DEVICES

Joint test solutions of R&S® and COMPRION®

Products:

- R&S® CMX500
- R&S® CMW290
- R&S® CMW500
- R&S® CMW-Z10
- R&S® CMW-Z11
- COMPRION® eUICC Profile Manager
- COMPRION® eSIM Test Profile Service

Yong Shi | GFM342 | Version 4e | 02.2023

http://www.rohde-schwarz.com/appnote/GFM342

ROHDE&SCHWARZ

Make ideas real

Contents

Abstract

The GSMA[1] specified a global standard for remote provisioning and management of the embedded Universal Integrated Circuit Card (eUICC) in the machine-to-machine (M2M) environment as well as the consumer devices via Over the Air (OTA) methodology.

This application note describes GSMA compliant remote eUICC provisioning test solution based on R&S® CMW500/CMW290/CMX500 and COMPRION® eUICC Profile Manager software tool. Moreover, an eUICC provisioning method for GSMA Security Accreditation Scheme (SAS) compliant consumer devices by adopting COMPRION® eSIM Test Profile Service is introduced which is essential for RF, protocol testing on R&S®CMW500/CMW290/CMX500 for eSIM capable consumer devices.

1 General

eUICCs have long replaced the traditional SIM cards used in the mobile industry. They are integrated into mobile devices, for instance in car telematics units, in machine-to-machine (M2M) devices such as industrial sensors or in consumer devices such as mobile phones, wearables and tablets. Vendors can use eUICCs to optimize their hardware design. This results in much smaller form factor thanks to replacing the SIM card slot with a small chip.

A great advantage of eUICC over the traditional SIM card is the ability to remotely change eUICC profile – in particular the operator subscription – without physically changing the eUICC itself. This is extremely important for the M2M market since device vendors can store multiple operator profiles simultaneously on one device and remotely switch between them by OTA method – although only one can be used at a time. This is necessary because changing the SIM cards in remote locations has been problematic for many industrial applications. In addition, soldering an eUICC to an M2M device or a car telematics unit poses new challenges. Once permanently installed or soldered into the device, changing or updating the card profile requires new methods.

GSMA introduced an initiative to define specifications for eUICC cards. The aim is to provide global standards for remote provisioning and management of eUICC profiles that include OTA provisioning of an initial operator subscription and subsequent switching of subscriptions from one operator to another. Core specifications [1] (SGP.02) and test specifications (SGP.11) ensure that eUICC cards deliver robust, secure and ubiquitous connectivity after field adaptation for M2M devices. The similar framework for consumer devices is defined by GSMA in the technical specification [2] (SGP.22).

SAS framework was also specified by GSMA to ensure secure provisioning of the eUICC/eSIM profile irrespective of M2M or consumer device. A market-ready M2M or consumer device should fulfill the mandatory GSMA SAS requirement (SAS-compliant) that requires the GSMA operational live certificate to connect to the remote eSIM provision service. However, it is sufficient to use a GSMA test certificate to establish the connection to the remote eSIM provision service for a non-SAS compliant device which typically refers to the device that is still in R&D or prototyping phase.

The remainder of this document is structured in the following way:

Chapter 2 gives an overview of eUICC test solutions that cover the test requirements over the device product life cycle.

[1] https://www.gsma.com/

Chapter 3 describes the eUICC profile handling for non-SAS compliant M2M devices based on R&S® CMW500/CMX500 wideband radio communication tester and COMPRION® eUICC Profile Manager (ePM) software tool.

Chapter 4 provides complementary information of eUICC profile handling for non-SAS compliant consumer devices.

Chapter 5 highlights the procedure to show how to provision the R&S® Test eSIM profile on a SAS compliant consumer devices by using COMPRION eSIM Test Profile Service.

The following abbreviations are used in this application note:

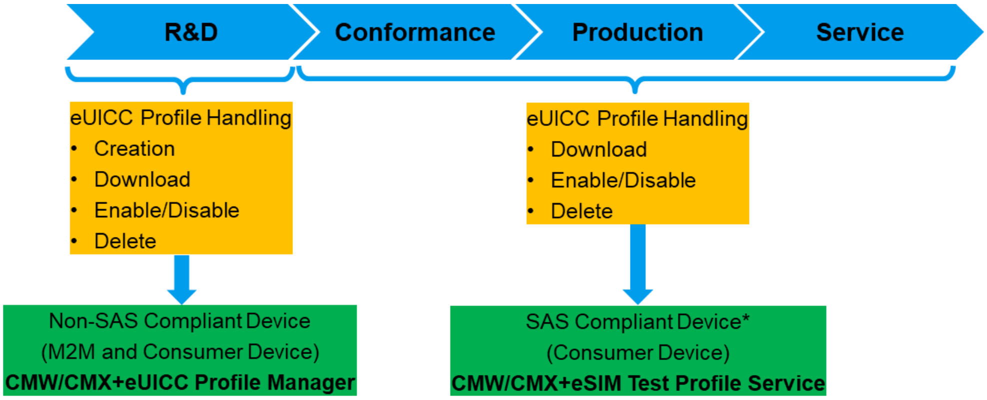
- The R&S®CMW500 or R&S®CMW290 wideband radio communication tester is referred to as CMW
- The R&S®CMX500 wideband radio communication tester is referred to as CMX
- The R&S®CMW-Z10 universal RF shield box is referred to as Z10
- The R&S®CMW-Z11 antenna coupler is referred to as Z11
- COMPRION® eUICC Profile Manager is referred to ePM

The readers are assumed to have a basic knowledge about CMW and CMX.

2 Overview of eUICC Test Solutions

Illustrated in Fig. 2-1, to cope with the different landscape of the eUICC handlings throughout the entire device lifecycle from initial product R&D way to the final service stage, two COMPRION tools are deployed, namely, eUICC Profile Manager (ePM) and eSIM Test Profile Service. Both tools are operated in conjunction with R&S mobile radio tester CMX or CMW.

The focus of the testing in R&D phase is to ensure the functional eUICC provisioning (downloading, enabling, disabling and deletion of a profile) with debugging capability. CMW/CMX together with ePM is the best choice for such use case. Whereas in the rest of the device lifecycle (conformance, production and service) stages, the market-ready device or so-called SAS compliant device has to fulfill the stringent SAS requirements. The digitized eSIM profile, R&S Test eSIM profile in particular which was formerly a physical test SIM, has to be downloaded within the SAS framework to allow the device under test (DUT) to be registered on the cellular network simulated by CMW/CMX. This enables RF, protocol testing in cellular network in question, e.g, 2G, 3G, LTE or NR. A tandem solution consists of CMW/CMX and COMPRION eSIM Test Profile Service provides the proper test environment for this test requirement.



* Only consumer devices are supported at the release of this document.

Fig. 2-1 Device life cycle and landscape of eUICC test solutions

Fig. 2-2 outlines the eUICC test solution for testing non-SAS compliant M2M and consumer device based on CMX and ePM.

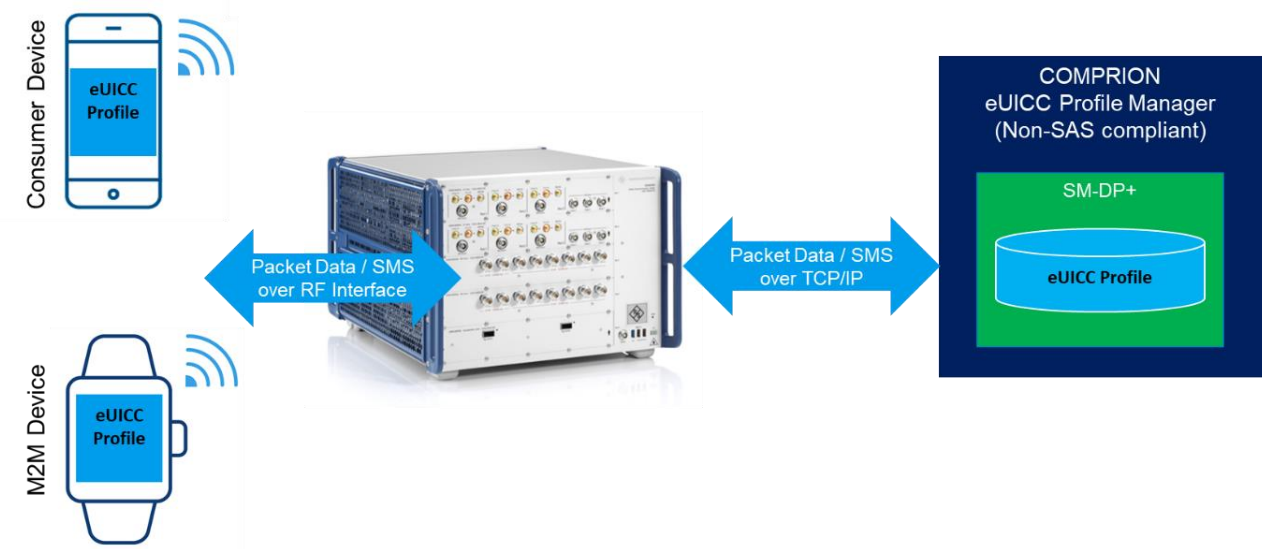

Consumer Device
eUICC Profile
M2M Device
eUICC Profile
Packet Data / SMS over RF Interface
Packet Data / SMS over TCP/IP
COMPRION eUICC Profile Manager (Non-SAS compliant)
SM-DP+
eUICC Profile

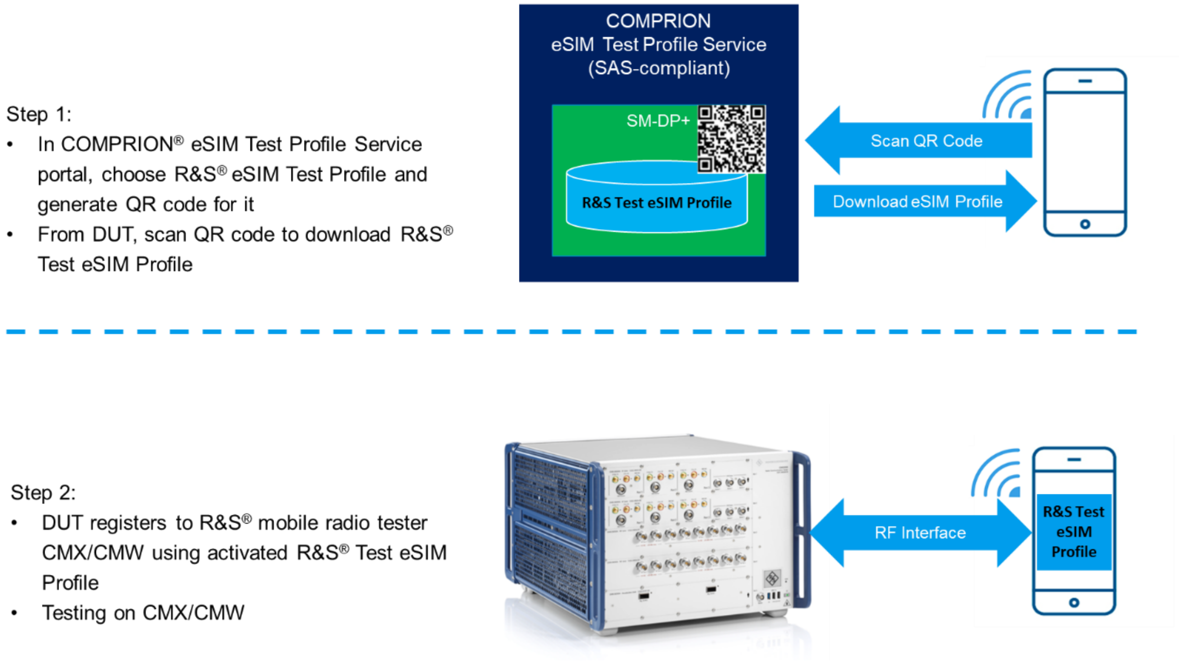
Fig. 2-2 eUICC test solution for non-SAS compliant M2M and consumer device with R&S® CMX and COMPRION® eUICC Profile Manager

In this test approach,

- CMX simulates the cellular network and takes care of the eUICC profile transfer and the profile management commands conveyance from ePM to the DUT over the air interface in form of either packet data or SMS. Alternatively, the mobile radio tester CMW can be deployed and holds the same function as the CMX does.
- COMPRION® eUICC Profile Manger (ePM) is responsible for the profile management, i.e. creation, download, installation, edit, read, write, deletion, activation of the eUICC profile with compliance to the eUICC remote provisioning architecture specified by GSMA technical specification [1] and [2] for M2M and consumer device, respectively.

More detailed information about this test approach can be found in Chapter 3 (for M2M device) and 4 (for consumer device).

As mentioned earlier in this chapter, testing SAS compliant device on CMX or CMW requires SAS compliant remote provisioning service to obtain its desired R&S test eSIM profile. A solution illustrated in Fig. 2-3 shows the consumer device downloads the R&S test eSIM profile by scanning a QR code generated by the COMPRION's eSIM Test Profile Service as a first step. With the proper test eSIM profile installed and activated, device under test (DUT) can then be registered to mobile radio tester CMX or CMW to conduct the further tests, such as classical RF, protocol tests etc. A guideline of using eSIM Test Profile Service is described in Chapter 5.



Step 1:

- In COMPRION® eSIM Test Profile Service portal, choose R&S® eSIM Test Profile and generate QR code for it
- From DUT, scan QR code to download R&S® Test eSIM Profile

Step 2:

- DUT registers to R&S® mobile radio tester CMX/CMW using activated R&S® Test eSIM Profile
- Testing on CMX/CMW

Fig. 2-3 eUICC test solution for SAS compliant consumer device with R&S® CMX and COMPRION® eSIM Test Profile Service

3 eUICC Handling of Non-SAS Compliant M2M Devices[2]

3.1 eUICC Basics

3.1.1 GSMA Provisioning Architecture for M2M Devices

GSMA SGP.02 [1] specified the eUICC remote provisioning architecture for M2M devices as shown in Fig. 3-1 from the system perspective. In this chapter, the functions of each entity and eUICC interfaces are explained.

[2] In this chapter, CMW is primarily used as the mobile radio tester. Therefore, screenshots and texts are all based on CMW. In principle, the same test concept can be adopted for CMX as well.

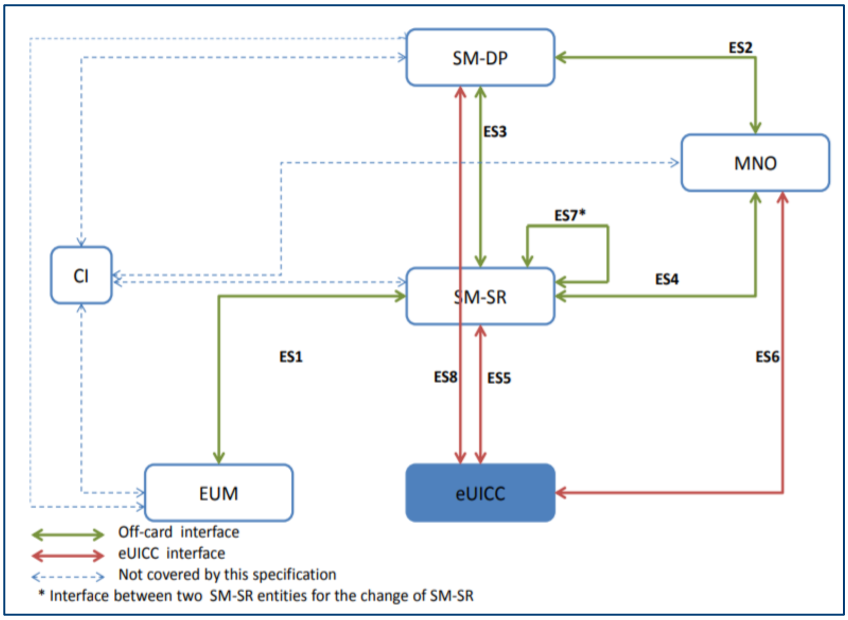

SM-DP
ES2
ES3
MNO
ES7*
CI
SM-SR
ES4
ES1
ES8
ES5
ES6
EUM
eUICC
Off-card interface
eUICC interface
Not covered by this specification
* Interface between two SM-SR entities for the change of SM-SR

Fig. 3-1: Remote M2M provisioning architecture (Source: GSMA SGP.02)

Subscription Manager Secure Routing (SM-SR) is the main entity communicating with the eUICC. It ensures the secure transport of eUICC profile management commands in order to enable, disable or delete the profile on the eUICC. Additionally, it secures the communications link between the eUICC and Subscription Manager Data Preparation (SM-DP) for the delivery of operator profiles.

SM-DP is responsible for preparing, storing and protecting operator profiles. It also downloads and installs profile onto the eUICC.

Certificate Issuer (CI) issues certificates for eUICC remote provisioning system. It contains SM-DP and eUICC (ECASD) certificate and acts as a trusted third party for the purpose of mutual authentication of the SM-DP and ECASD.

eUICC Manufacturer (EUM) provision an initial profile which allows the device to connect to the network at the starting of its lifecycle.

Mobile Network Operator (MNO) is the owner of the profiles.

As shown in Fig. 3-1, there are three eUICC interfaces defined by SGP.02 [1]. Each of the connection between off-card entities (SM-SR, SM-DP and MNO) and on-card security domains (ISD-R, ISD-P and MNO-DP, will be explained in Chapter 3.1.2) has its individual defined interface, namely ES5, ES8 and ES6. The interface makes the access control of backend servers to the eUICC possible.

ES5 (see Fig. 3-2) ensures that the communication between the SM-SR and ISD-R. It is protected by secure communication protocol SCP80 (SMS or CAT_TP) or SCP81 (HTTPs). The interface itself allows the creation or deletion of the profile container ISD-P on eUICC and enable or disable of the given profile.

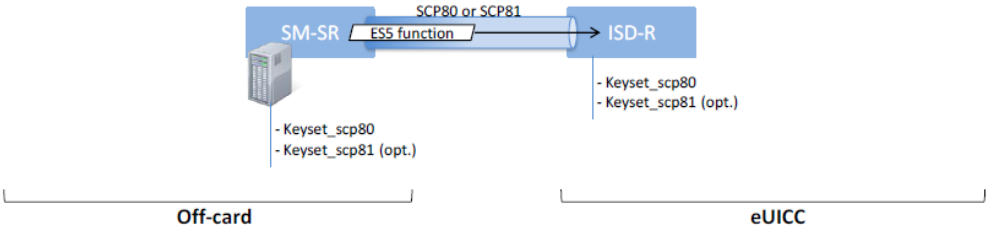


Fig. 3-2: ES5 Interface (Source: GSMA SGP.02)

ES6 interface (see Fig. 3-3) enables the MNO to access the MNO-SD by either SCP80 or SCP81. This function allows the MNO to update the operator's policy rules within the profile (POL1), as well as the connectivity parameters on eUICC.

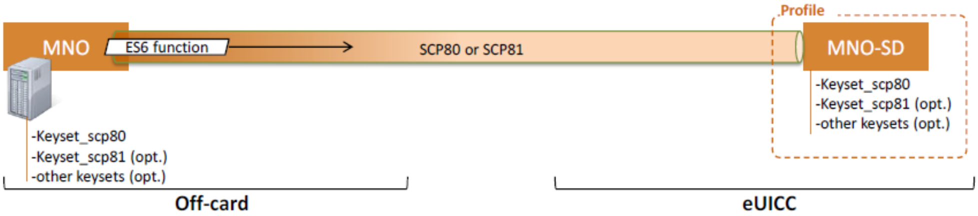


Fig. 3-3: ES6 Interface (Source: GSMA SGP.02)

The interface ES8 (see Fig. 3-4) is responsible for delivering the new profiles data to ISD-P on the eUICC and protects the key propagation from the SM-DP to the ISD-P through SM-SR. The interface facilitates a confidential data transmission protocol SCP03 or SCP03t which is then encapsulated in SM-SR with SCP80 or SCP81.

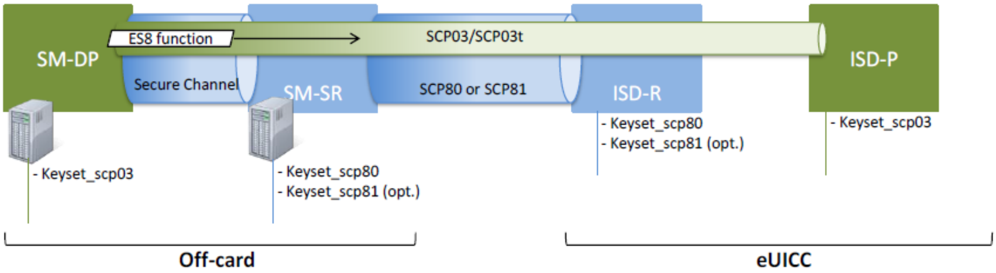


Fig. 3-4: ES8 Interface (Source: GSMA SGP.02)

For details of ES5, ES6 and ES8 functions, please refer to SGP.02 [1].

The eUICC test solution described in this application note contains the COMPRION's implementation of ES5, ES6 and ES8 functions, as well as associated entities SM-SR, MNO and SM-DP.

The Over the Air (OTA) communication of the eUICC remote provisioning and management system on the ES5 interface is exclusively handled by SM-SR and together with the communication over ES6 interface handled by MNO OTA platform. The OTA utilizes SMS, Card Application Toolkit Transport Protocol (CAT_TP) or HTTPs as one of the transport protocols. See more in details about OTA communication in Chapter 3.1.3

3.1.2 eUICC Architecture

eUICC is the secure computing device that contains memory and provides identification services which can handle multiple profiles. Each profile contains the data related to subscriptions including the operator's credential, security algorithm, IMSI, ICCID or third-party SIM based applications. Only one profile shall be activated on eUICC at any point in time. The structure and content of the profiles stored on eUICC are similar to those installed on conventional SIMs.

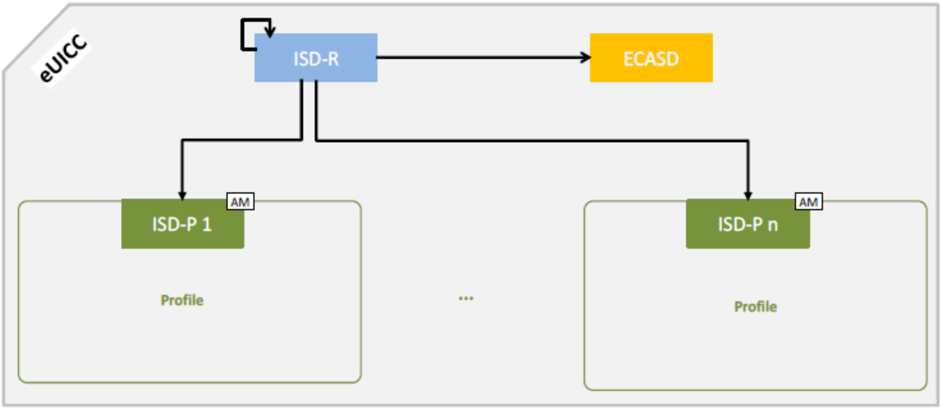


Fig. 3-5: eUICC Security Domain Architecture (Source: GSMA SGP.02)

Fig. 3-5 illustrates the eUICC's architecture as per GSMA SGP.02 definition [1]. On-card security domains like Issuer Security Domain Profile (ISD-P), Issuer Security Domain Root (ISD-R) and eUICC Controlling Authority Security Domain (ECASD) should be presented. They are the representative of the off-card entities SM-DP, SM-SR and CI.

ISD-R facilitates an interface for OTA communication with SM-SR. It is the highest privileged security domain on the eUICC. Remote commands sent to eUICC are received and processed by the ISD-R and then relayed to the target application, e.g. ISD-P.

The ISD-R is involved in the following functions

- ISD-P Creation (during the creation, an association between the ISD-R and an ISD-P is generated)
- ISD-P Deletion and Master Delete
- Profile Enabling and Disabling
- Fall-Back Attribute setting
- The association that allows the connection establishment between the SM-DP and the ISD-P

An eUICC can contain more than one ISD-P. Each ISD-P represents an installed profile and is associated to ISD-R of the eUICC.

Profile associated to each ISD-P is the key part of the eUICC. As an example shown in Fig. 3-6, it consists of following mandatory components

- MNO-SD (Secure Domain)
- At least one NAA (Network Access Application)
- POL1 (Policy Rules within the Profile)
- File systems
- Connectivity parameters of the profile

Optionally, it may contain

- Several Applications
- One CASD

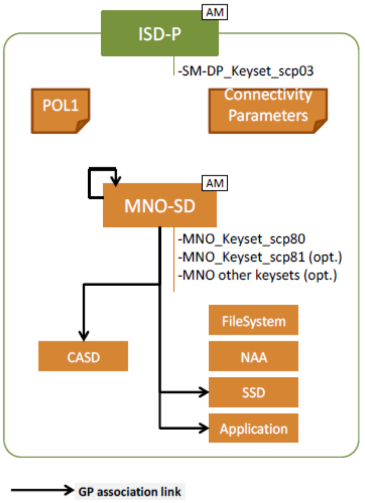


Fig. 3-6: Profile structure (Source: GSMA SGP.02)

ECASD on eUICC takes care of

- SM-DP key set establishment for Profile Download and Installation
- SM-SR key set establishment for SM-SR Change

For function details of the eUICC, please refer to [1]

3.1.3 OTA Communication

OTA communication is essential for the remote provisioning and management between the backend servers (SM-SR and MNO OTA platform) and eUICC. It occurs on ES5 and ES6 interface as illustrated in Fig. 3-1 and is triggered or handled directly by SMS. The SMS has one of the following functions:

- It serves as an administration session trigger (push SMS) to open a HTTPs session addressed to ISD-R on the eUICC. The typical sequence for HTTPs session triggering as defined in [1] is shown in Fig. 3-7.
- Similar to HTTPs session trigger, it serves as an administration session trigger (push SMS) to open a Card Application Toolkit Transport Protocol (CAT_TP) session addressed to ISD-R on the eUICC.
- It conveys directly the remote management commands to eUICC, if the commands to be sent fit into a few SMSs.

The security aspect of the OTA communication on ES5 and ES6 is ensured by either secure channel protocol SCP80 or SCP81. It is mandatory for eUICC to support SCP80, optionally SCP81 may be supported too.

SCP80 secures the SMS defined in [5] and [6], as well as the secured packets exchanged during CAT_TP session.

SCP81 secures the HTTPs communication [3]. The security for data exchange over TCP is provided by Pre-Shared Key TLS (PSK-TLS) protocol.

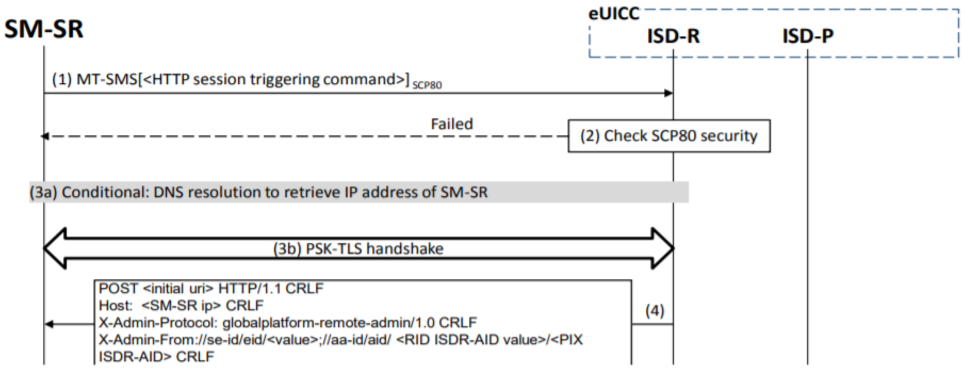

SM-SR
eUICC
ISD-R
ISD-P
(1) MT-SMS[<HTTP session triggering command>] SCP80
Failed
(2) Check SCP80 security
(3a) Conditional: DNS resolution to retrieve IP address of SM-SR
(3b) PSK-TLS handshake
(4)
POST <initial uri> HTTP/1.1 CRLF
Host: <SM-SR ip> CRLF
X-Admin-Protocol: globalplatform-remote-admin/1.0 CRLF
X-Admin-From://se-id/eid/<value>;//aa-id/aid/ <RID ISDR-AID value>/<PIX ISDR-AID> CRLF

Fig. 3-7: Sequence for HTTPs session triggering (Source: GSMA SGP.02)

As per GSMA SGP.02 specification [1], Fig. 3-7 shows the sequence of HTTPs session triggered by an SMS and the description of the flow is given as follows:

1. SM-SR sends a Mobile Terminated (MT)-SMS to ISD-R containing the necessary Toolkit Application Reference (TAR) information defined by [1].
2. ISD-R checks the security of the MT-SMS. The procedure continues if the check is successful
3. Optionally, DNS request of resolving the SM-SR IP address is sent. Otherwise, the secure TLS socket is opened with PSK-TLS handshake procedure
4. The HTTP POST request is sent from ISD-R to SM-SR to fetch the remote Application Protocol Data Unit (APDU) strings

3.2 eUICC Test Setup

3.2.1 System Overview

The entire eUICC test solution comprises following components:

- R&S® CMX500 or CMW500 or CMW290 (incl. hardware and associated software)
- Test PC with COMPRION® eUICC Profile Manager (ePM) featuring ePM profile loader for M2M and profile explorer, see Table 3-2 for the required ePM options.
- Accessories
  - Ethernet Switch
  - (Optional) Z10 or Z11 (required when DUT is tested over the air with CMW/CMX)

A brief description of the main entities is given as follows:

- CMW/CMX handles all the OTA communication. It transfers or receives the SMS between the backend servers and DUT (eUICC) via the air interface over the cellular technology in question.
- ePM Profile Loader for M2M

  It handles OTA communication occurs on ES5 which is responsible for profile download/install, enable, disable, delete and setting fallback attribute of eUICC. It also features the ES3 and ES8 function and simulates SM-SR and SM-DP.
- ePM Profile Explorer

  It facilitates the ES6 function by applying the standard remote Application Protocol Data Unit (APDU) structure for eUICC based applications which is the same application as UICC. This interface provides the possibility to update already provisioned profile including remote file management (RFM) and remote application management (RAM).

Fig. 3-8 and Fig. 3-9 illustrate the system cabling of both CMW rear panel and front panel, respectively.

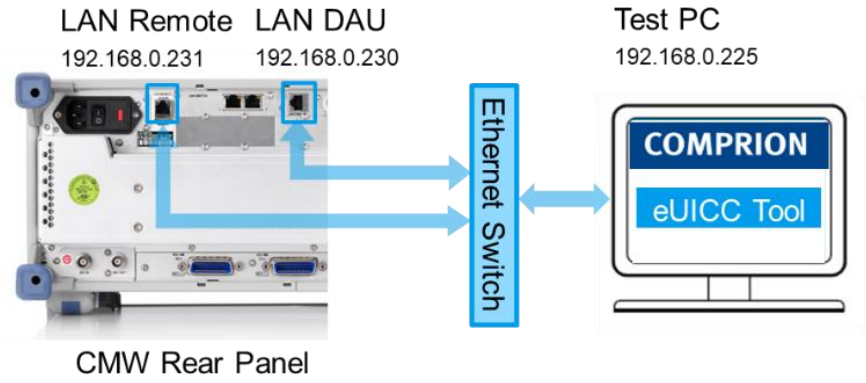


Fig. 3-8: Connection between CMW Rear Panel and Test PC

Fig. 3-8 shows the connections between CMW rear panel and test PC. Three LAN patch cables are required and interconnected via an Ethernet Switch. Two of them are connected to LAN remote and LAN DAU port of the CMW rear panel, respectively. The third one is connected to test PC where COMPRION® ePM is installed. The details of IP settings of all three network interfaces are explained in Chapter 3.2.4. Table 3-1 gives an example of the system IP settings. In principle, the arbitrary IP addresses can be applied given that all the IPs should be assigned in the same subnet.

	LAN Remote	LAN DAU	Test PC
IP Address	192.168.0.231	192.168.0.230	192.168.0.225
Netmask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	0.0.0.0	192.168.0.225	192.168.0.230

Table 3-1: Example of System IP Configurations

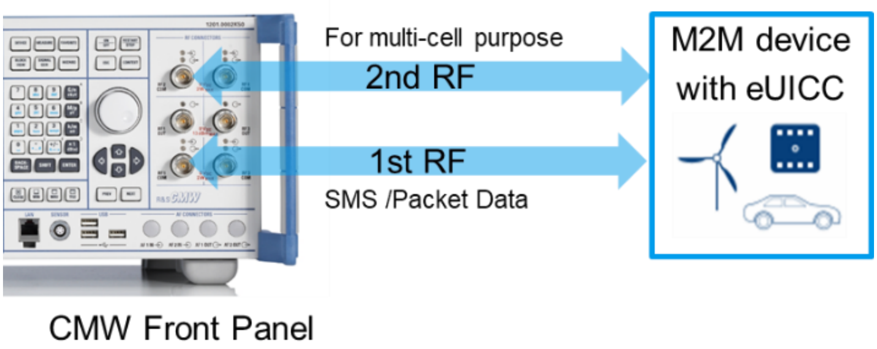


Fig. 3-9: Connection between CMW Front Panel and DUT (M2M device with eUICC)

Fig. 3-9 depicts the connections between CMW front panel and M2M DUT with eUICC. The primary RF connection is connected to CMW's RF1COM port. Optionally, the secondary RF connection mainly for the multi-cell test scenario can be connected to RF2COM port of the CMW front panel. In Chapter 3.3.1.1, it explains how to enable the multiple cells on CMW.

Please be noted that the described connection is based on a so-called conducted test mode where RF connector of the DUT is accessible and connected to CMW directly with the RF cable. Otherwise, a shielding box Z10 or antenna coupler Z11 from R&S® can be utilized here for RF signal coupling with CMW and the optional free space path loss (FSPL) has to be compensated roughly to ensure the stable RF connection between CMW and DUT, see Chapter 3.3.1.2 for details.

3.2.2 Preparation of Test PC

In this chapter, it gives the hardware and software configurations recommended by COMPRION®.

3.2.2.1 Hardware Requirements

The test PC should meet following requirements:

- CPU: at least 2 GHz (recommended: 2 × 1.5 GHz dual core or more)
- Hard disk: a minimum of 200 MB free space
- RAM: at least 1 GB RAM (recommended: 2 GB or more)
- Screen resolution: 1024 x 768 (recommended: 1280 x 1024 or higher)

3.2.2.2 Software Requirements

Operating System and Framework

- Windows 7, or
- Windows 8.1, or
- Windows 10
- .NET 4.6.1

Following software components need to be installed on test PC:

- COMPRION eUICC Profile Manager (ePM)
- National Instrument VISA runtime driver 17.0 or higher, recommended version 18.5. The VISA driver can be downloaded after registration from: http://www.ni.com/download/ni-visa-run-time-engine-18.5/7974/en/Table 3-2: COMPRION software options

A list of the software options of ePM is given in Table 3-2.

Item Nr.	eUICC Profile Manager Package
31000111	eUICC Profile Manager
31000112	eUICC Profile Manager Software
31000113	Profile Explorer
31000114	Profile Loader M2M
31000448	Sequence Diagram View
31000127	R&S CMW290/500 Signaling Control

Table 3-2: COMPRION software options

3.2.3 Preparation of CMW

In this chapter, it gives the hardware and software configurations recommended by R&S®.

3.2.3.1 Hardware Requirements

A minimum CMW hardware requirement is listed in Table 3-3.

Option	Order No.	Description	QTY
CMW-PS505	1208.8921.06	R&S®CMW500 Basic Assembly (Mainframe), 70MHz to 3.3GHz	1

Option	Order No.	Description	QTY
CMW-S100H	1202.4701.09	Baseband Measurement Unit with 1GByte digitizer memory	1
CMW-S550N	1202.4801.15	Baseband interconnection, flexible link	1
CMW-S570H	1202.5008.09	First RF Converter (TRX), BW160 MHz	1
CMW-S052S	1202.4201.20	Solid State Drive (SSD)	1
CMW-S590D	1202.5108.03	RF Frontend, advanced functionality	1
CMW-S600B	1201.0102.03	CMW500 front panel with display/keypad	1
CMW-B570H	1202.8659.09	Extra RF Converter (TRX), BW160 MHz (hardware option) (second TRX for second cell is required)	1
CMW-B690B	1202.6004.02	OCXO, high stability	1
CMW-B500I	1208.7954.10	Signaling Unit Advanced (SUA) for GSM, WCDMA, LTE, WLAN	1
CMW-B660H	1202.7000.09	Option Carrier	1
CMW-B661H	1202.7100.09	Ethernet switch	1
CMW-B450I	1202.8759.10	Data Application Unit, retrofittable in R&S service,(hardware option)	1
CMW-PK364	1208.7319.02	6GHz Flat Rate, for up to 4 RF converters (TRXs) (SL)	1

Table 3-3: Minimum CMW hardware requirement for eUICC testing

3.2.3.2 Software Requirements

The software license requirement is listed in Table 3-4.

Option	Order No.	Description	QTY
CMW-KS200	1203.0600.02	GSM GPRS EDGE R6, basic signaling	1
CMW-KS400	1203.0751.02	WCDMA Release 99,signaling/network emulation,	1
CMW-KS500	1203.6108.02	LTE FDD Release 8, SISO, signaling/network emulation, basic functionality (software license)	1
CMW-KA100	1207.2607.02	Enabling of IP-Data interface for IPV4 (software license)	1
CMW-KM050	1203.9359.02	IP based measurements, in combination with technology specific IP data enabling (software license)	1

Table 3-4: CMW software license

The required CMW firmware version is listed in Table 3-5:

Firmware	Version
CMW-Base	3.7.41 or higher
CMW-DAU	3.7.20 or higher
CMW-LTE-Sig	3.7.50 or higher
CMW-WCDMA-Sig	3.7.21 or higher
CMW-GSM-Sig	3.7.27 or higher

Table 3-5: CMW firmware version requirement

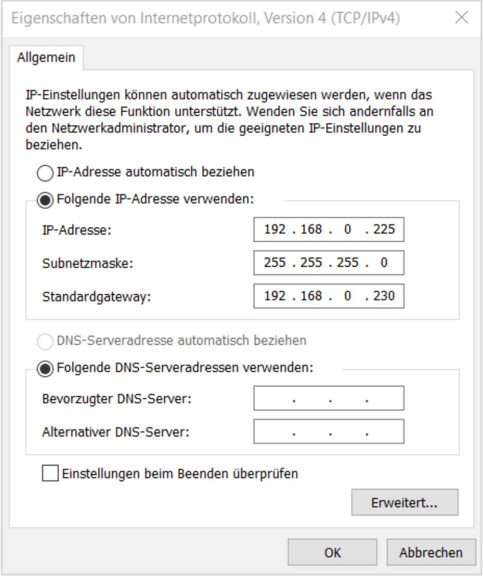
3.2.4 System IP Configurations

3.2.4.1 Test PC LAN IP Configuration

To properly setup the test environment, the network adapter of the test PC needs to be configured so that the IP addresses of the test PC, LAN remote and LAN DAU port of the CMW are on the same IP subnet.

Furthermore, Windows firewall shall allow connections and ICMP echoes (Ping tests) from the CMW.

As an example, the IP settings of the network adapter of the test PC is given in Fig. 3-10



Eigenschaften von Internetprotokoll, Version 4 (TCP/IPv4)

Allgemein

IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.

○ IP-Adresse automatisch beziehen

● Folgende IP-Adresse verwenden:

IP-Adresse: 192 . 168 . 0 . 225

Subnetzmaske: 255 . 255 . 255 . 0

Standardgateway: 192 . 168 . 0 . 230

○ DNS-Serveradresse automatisch beziehen

● Folgende DNS-Serveradressen verwenden:

Bevorzugter DNS-Server: . . .

Alternativer DNS-Server: . . .

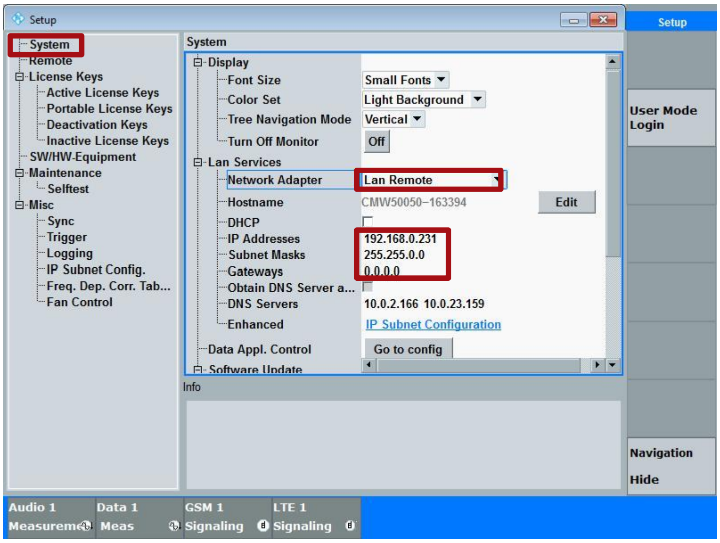
□ Einstellungen beim Beenden überprüfen

Fig. 3-10: Example IP settings of the network adapter of the test PC

3.2.4.2 LAN Remote IP Configuration

As shown in Fig. 3-8, the LAN remote port on the rear panel of the CMW is connected with the test PC. This allows the ePM on the test PC remotely control the CMW by SCPI commands that configure cell parameters, start the cellular network, set the SMS Center (SMSC) parameters etc.

The IP settings of the LAN remote port on CMW are shown in Fig. 3-11. This is done by pressing "Setup" hard key on the front panel of the CMW, clicking on "System">"Network Adapter", selecting "Lan Remote". In that section, IP addresses can be entered. If IP address setting is greyed out, uncheck the DHCP beforehand.



System

Display

Font Size: Small Fonts

Color Set: Light Background

Tree Navigation Mode: Vertical

Turn Off Monitor: Off

Lan Services

Network Adapter: Lan Remote

Hostname: CMW50050–163394 Edit

DHCP: □

IP Addresses: 192.168.0.231

Subnet Masks: 255.255.0.0

Gateways: 0.0.0.0

Obtain DNS Server a...: □

DNS Servers: 10.0.2.166 10.0.23.159

Enhanced: IP Subnet Configuration

Data Appl. Control: Go to config

Software Update

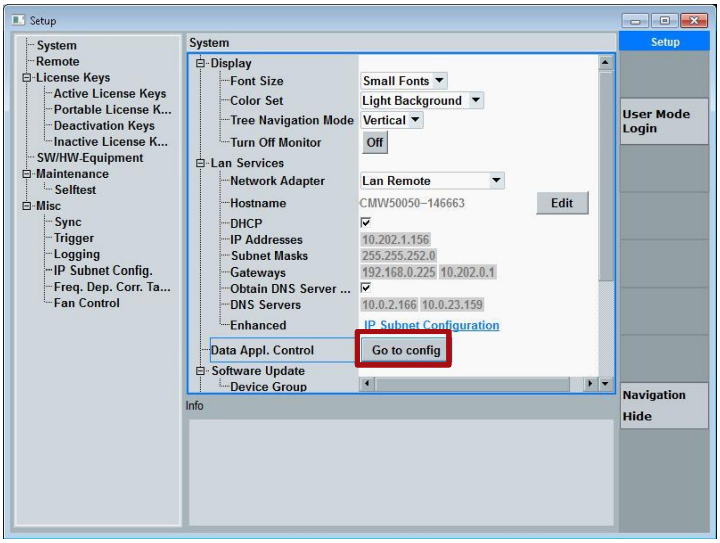
Info

Fig. 3-11: Example IP Settings of CMW LAN Remote Port

3.2.4.3 LAN DAU IP and Mobile IP Configuration

Data Application Unit (DAU) is required for the IP communication between CMW and test PC.

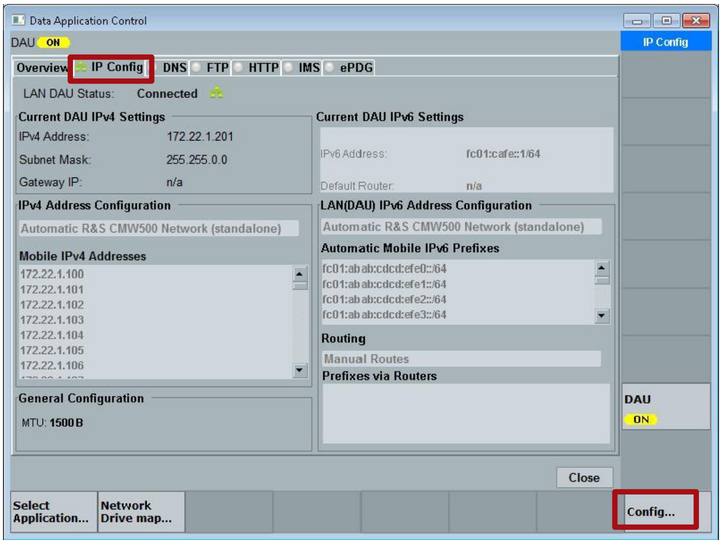
Click on "Go to config" button in the CMW System Setup shown in Fig. 3-12.



- Font Size: Small Fonts
- Color Set: Light Background
- Tree Navigation Mode: Vertical
- Turn Off Monitor: Off
- Network Adapter: Lan Remote
- Hostname: CMW50050–146663 [Edit]
- DHCP: ☑
- IP Addresses: 10.202.1.156
- Subnet Masks: 255.255.252.0
- Gateways: 192.168.0.225 10.202.0.1
- Obtain DNS Server ...: ☑
- DNS Servers: 10.0.2.166 10.0.23.159
- Enhanced: IP Subnet Configuration
- Data Appl. Control: Go to config

Fig. 3-12: Go to LAN DAU configuration on CMW

This opens the CMW Data Application Control setting page. Select "IP config" page and click on "Config" as shown in Fig. 3-13.



LAN DAU Status: Connected

Current DAU IPv4 Settings

- IPv4 Address: 172.22.1.201
- Subnet Mask: 255.255.0.0
- Gateway IP: n/a

Current DAU IPv6 Settings

- IPv6 Address: fc01:cafe::1/64
- Default Router: n/a

IPv4 Address Configuration

Automatic R&S CMW500 Network (standalone)

Mobile IPv4 Addresses

172.22.1.100
172.22.1.101
172.22.1.102
172.22.1.103
172.22.1.104
172.22.1.105
172.22.1.106

LAN(DAU) IPv6 Address Configuration

Automatic R&S CMW500 Network (standalone)

Automatic Mobile IPv6 Prefixes

fc01:abab:cdcd:efe0::/64
fc01:abab:cdcd:efe1::/64
fc01:abab:cdcd:efe2::/64
fc01:abab:cdcd:efe3::/64

Routing

Manual Routes

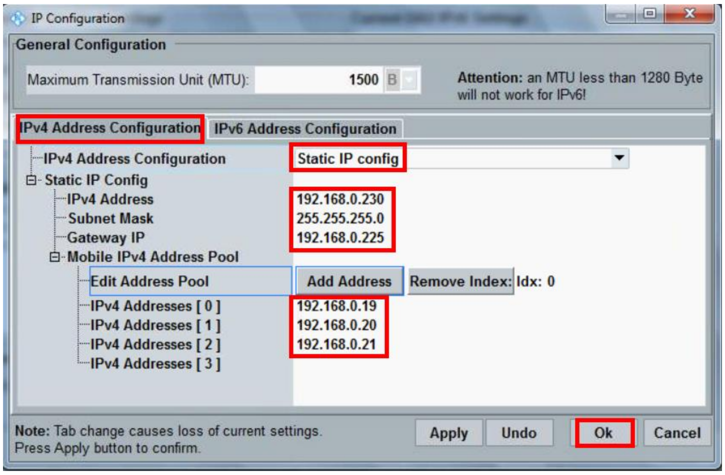
Prefixes via Routers

General Configuration

MTU: 1500 B

Fig. 3-13: CMW LAN DAU IP Configuration

In the opened "IPv4 Address Configuration" page shown in Fig. 3-14, select "Static IP config" and enter the IPv4 address, subnet mask and Gateway IP. Furthermore, the mobile IPv4 address should also be set within the same IP segment as LAN DAU IP. One of the mobile IP addresses will be assigned by CMW to DUT during the DUT's cell registration procedure. Press "OK" in the end to save the settings.



Maximum Transmission Unit (MTU): 1500 B

Attention: an MTU less than 1280 Byte will not work for IPv6!

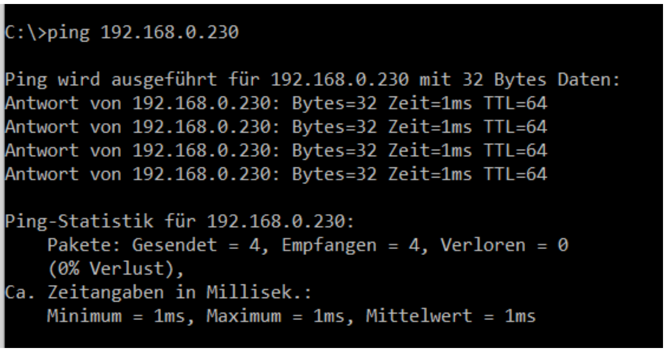
IPv4 Address Configuration: Static IP config

Static IP Config
- IPv4 Address: 192.168.0.230
- Subnet Mask: 255.255.255.0
- Gateway IP: 192.168.0.225
- Mobile IPv4 Address Pool
  - Edit Address Pool — Idx: 0
  - IPv4 Addresses [0]: 192.168.0.19
  - IPv4 Addresses [1]: 192.168.0.20
  - IPv4 Addresses [2]: 192.168.0.21
  - IPv4 Addresses [3]

Note: Tab change causes loss of current settings.
Press Apply button to confirm.

Fig. 3-14: Example static CMW LAN DAU IP configuration

Finally, after all the IP addresses are configured for CMW LAN remote, CMW LAN DAU and test PC, issue PING command in the DOS Prompt on test PC to ensure the successful connection between all entities. This is shown in Fig. 3-15 and Fig. 3-16 with the example IP addresses configured in the previous steps.

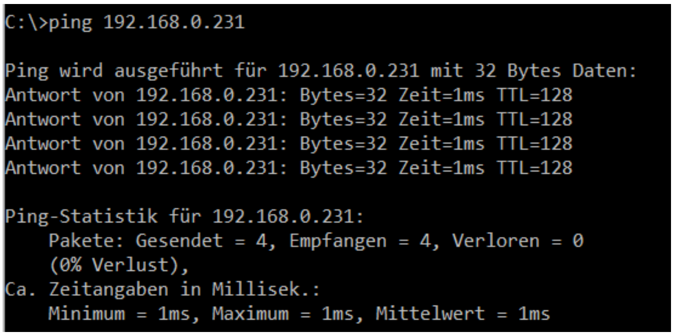


```
C:\>ping 192.168.0.230

Ping wird ausgeführt für 192.168.0.230 mit 32 Bytes Daten:
Antwort von 192.168.0.230: Bytes=32 Zeit=1ms TTL=64
Antwort von 192.168.0.230: Bytes=32 Zeit=1ms TTL=64
Antwort von 192.168.0.230: Bytes=32 Zeit=1ms TTL=64
Antwort von 192.168.0.230: Bytes=32 Zeit=1ms TTL=64

Ping-Statistik für 192.168.0.230:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 1ms, Maximum = 1ms, Mittelwert = 1ms
```

Fig. 3-15: PING CMW LAN DAU Port from Test PC



```
C:\>ping 192.168.0.231

Ping wird ausgeführt für 192.168.0.231 mit 32 Bytes Daten:
Antwort von 192.168.0.231: Bytes=32 Zeit=1ms TTL=128
Antwort von 192.168.0.231: Bytes=32 Zeit=1ms TTL=128
Antwort von 192.168.0.231: Bytes=32 Zeit=1ms TTL=128
Antwort von 192.168.0.231: Bytes=32 Zeit=1ms TTL=128

Ping-Statistik für 192.168.0.231:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 1ms, Maximum = 1ms, Mittelwert = 1ms
```

Fig. 3-16: PING CMW LAN Remote Port from Test PC

3.2.5 eUICC Profile Manager Installation

eUICC Profile Manager (ePM) from COMPRION® supports all eUICC related interfaces, i.e. ES5, ES6 and ES8 shown in Fig. 3-1 and interacts with CMW via TCP/IP connection.

Please follow the installation procedure described in eUICC Profile Manager Installation Guide which comes with the ePM software download from COMPRION®.

3.3 eUICC Testing with CMW and eUICC Profile Manager for M2M Devices

Prior to eUICC profile verification, following operations need to be done on CMW manually

- ► Start the Cellular Technology, see 3.3.1.1
- ► Optionally, path loss compensation needs to be done to set proper signal level so that the stable RF connection between CMW and DUT is guaranteed, see 3.3.1.2
- ► Configure the signaling to support packet data communication, see 3.3.1.3

Following cellular parameters of CMW are required to be set in ePM GUI. These settings are then sent by ePM per SCPI commands to control CMW remotely. See Chapter 3.3.2.1:

- ► Cellular Technology (GSM, WCDMA, LTE)
- ► Frequency Band and Channel
- ► Network Identities (MCC, MNC)
- ► IMSI
- ► Authentication / Integrity parameters

Furthermore, the parameters of eUICC that is under test need to be configured in ePM, see Chapter 3.3.2.2

Chapter 3.3.2.4 explains the verification of the eUICC by utilizing ePM.

3.3.1 Operations on CMW

3.3.1.1 Start the Cellular Technology

Start the cellular technology on CMW by pressing "SIGNAL GEN" hard key on the CMW front panel (Fig. 3-17). The operation described here to start cellular signaling is valid for all radio access technologies (RAT). For sake of simplicity, in the following chapters, LTE is selected as an example RAT.

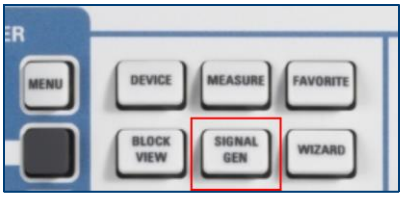


Fig. 3-17: Start the cellular signaling

In the opened Window, enable "Signaling 1" in LTE as shown in Fig. 3-18. The CMW LTE signaling firmware is then launched. The default RF output port is RF1COM

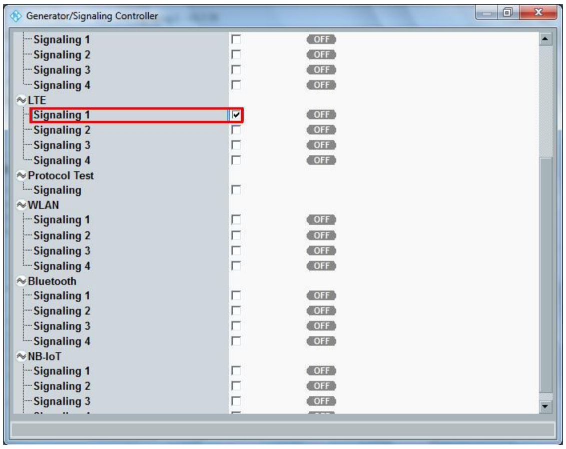


Fig. 3-18: Start the LTE signaling

If multiple cell is required for testing, e.g. in order to verify a new activated eUICC profile with the different LTE network identities on a second LTE cell, enable the second LTE cell as "Signaling 2" in the Signal Generator part shown in Fig. 3-19.

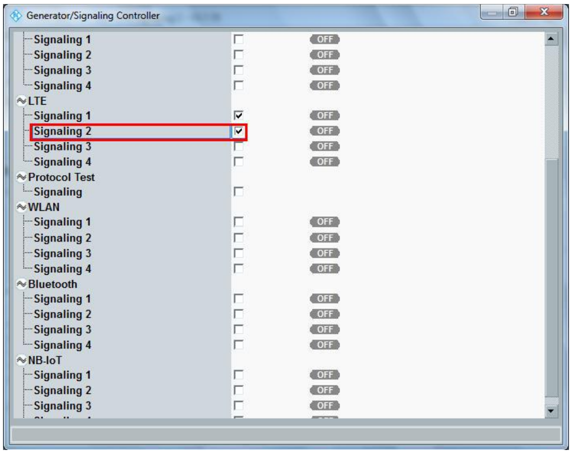
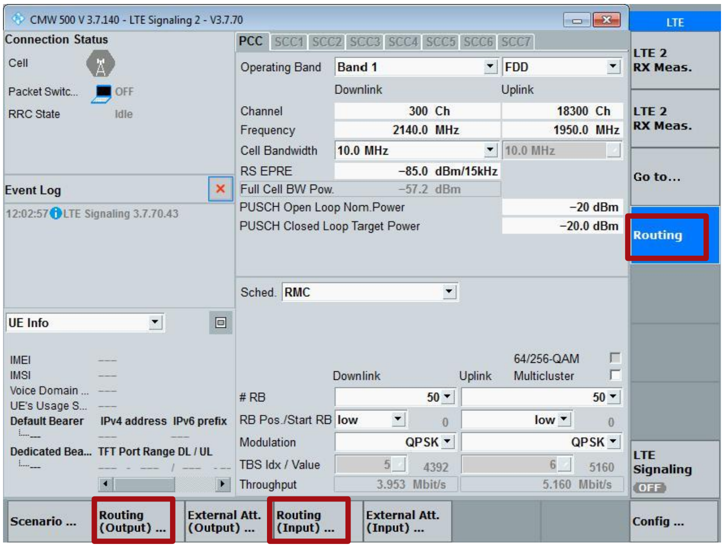


Fig. 3-19: Enable second cell (for multi-cell purpose)

To avoid resource conflict with LTE Signaling 1. Routing needs to be adjusted in LTE Signaling 2. Go to "Routing">"Routing (Output) …" and "Routing">"Routing (Input) …" shown in Fig. 3-20 with the settings as given in Fig. 3-21 and Fig. 3-22.


CMW 500 V 3.7.140 - LTE Signaling 2 - V3.7.70

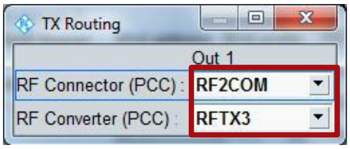
Connection Status
Cell
Packet Switc... OFF
RRC State Idle

Event Log
12:02:57 LTE Signaling 3.7.70.43

UE Info
IMEI ---
IMSI ---
Voice Domain ... ---
UE's Usage S... ---
Default Bearer IPv4 address IPv6 prefix
Dedicated Bea... TFT Port Range DL / UL

PCC SCC1 SCC2 SCC3 SCC4 SCC5 SCC6 SCC7
Operating Band: Band 1, FDD
Downlink / Uplink
Channel: 300 Ch / 18300 Ch
Frequency: 2140.0 MHz / 1950.0 MHz
Cell Bandwidth: 10.0 MHz / 10.0 MHz
RS EPRE: −85.0 dBm/15kHz
Full Cell BW Pow.: −57.2 dBm
PUSCH Open Loop Nom.Power: −20 dBm
PUSCH Closed Loop Target Power: −20.0 dBm
Sched.: RMC
64/256-QAM □
Multicluster □
Downlink / Uplink
RB: 50 / 50
RB Pos./Start RB: low 0 / low 0
Modulation: QPSK / QPSK
TBS Idx / Value: 5 4392 / 6 5160
Throughput: 3.953 Mbit/s / 5.160 Mbit/s

Fig. 3-20: Configure the RF Routing of the second cell

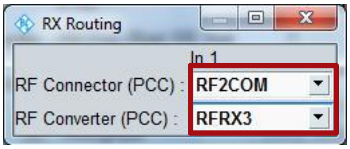

TX Routing

Out 1

RF Connector (PCC) : RF2COM

RF Converter (PCC) : RFTX3

Fig. 3-21: Setting for routing (Output)


RX Routing

In 1

RF Connector (PCC) : RF2COM

RF Converter (PCC) : RFRX3

Fig. 3-22: Setting for routing (Input)

After the above settings are done, the output port of the second cell is routed to RF2COM.

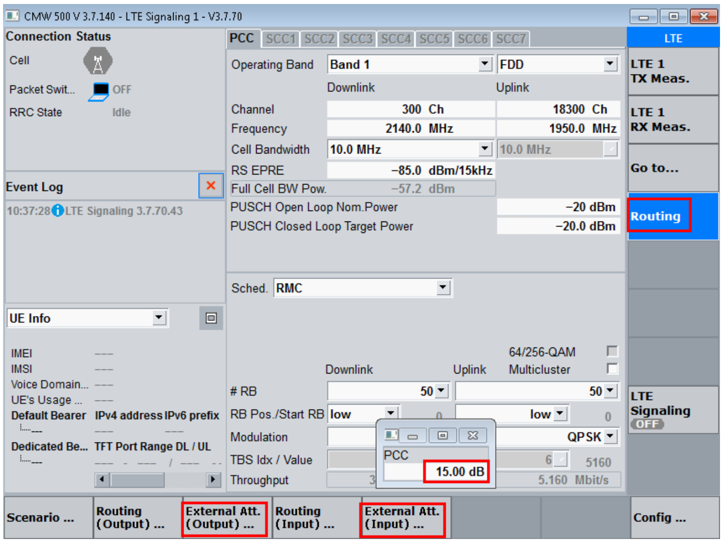
3.3.1.2 Free Space Path Loss Compensation (Optional)

In case there is no direct access to the DUT`s RF connector, that means, the DUT cannot register to the cell per connected mode via an RF cable, a shielding box Z10 or antenna coupler Z11 is required for the RF coupling between the DUT and CMW. Under such test condition, it might happen that DUT is unable to attach to CMW. One of the reasons might be the low signal power level at the DUT's receiver antenna due to the free space path loss (FSPL). Therefore, an extra FSPL compensation can be added roughly on the CMW side. The FSPL, or attenuation, can be added in each applied radio access technology (RAT). For example, in LTE configuration window shown in Fig. 3-23

Press "Routing" > "External Att. (Output) …", enter 15 dB

Press "Routing" > "External Att. (Input) …", enter 15 dB

Since the RF performance is not the focus of the eUICC test, therefore the compensated attenuation value 15 dB is just an experimental value. It can be adjusted by individual test needs. The goal of the compensation here is of course to ensure the stable RF condition between CMW and DUT.


CMW 500 V 3.7.140 - LTE Signaling 1 - V3.7.70

Connection Status

Cell

Packet Swit... OFF

RRC State Idle

Event Log

10:37:28 LTE Signaling 3.7.70.43

UE Info

IMEI ---

IMSI ---

Voice Domain... ---

UE's Usage ... ---

Default Bearer IPv4 address IPv6 prefix

Dedicated Be... TFT Port Range DL / UL

PCC

	Downlink	Uplink
Operating Band	Band 1	FDD
Channel	300 Ch	18300 Ch
Frequency	2140.0 MHz	1950.0 MHz
Cell Bandwidth	10.0 MHz	10.0 MHz
RS EPRE	−85.0 dBm/15kHz	
Full Cell BW Pow.	−57.2 dBm	
PUSCH Open Loop Nom.Power		−20 dBm
PUSCH Closed Loop Target Power		−20.0 dBm

Sched. RMC

64/256-QAM □

Multicluster □

	Downlink	Uplink
# RB	50	50
RB Pos./Start RB	low 0	low 0
Modulation		QPSK
TBS Idx / Value		6 5160
Throughput	3	5.160 Mbit/s

PCC 15.00 dB

Fig. 3-23: Compensate free space path loss when shield box/antenna coupler is used

FSPL is not a global setting and it is RAT dependent. Therefore, this needs to be repeated in each RAT individually.

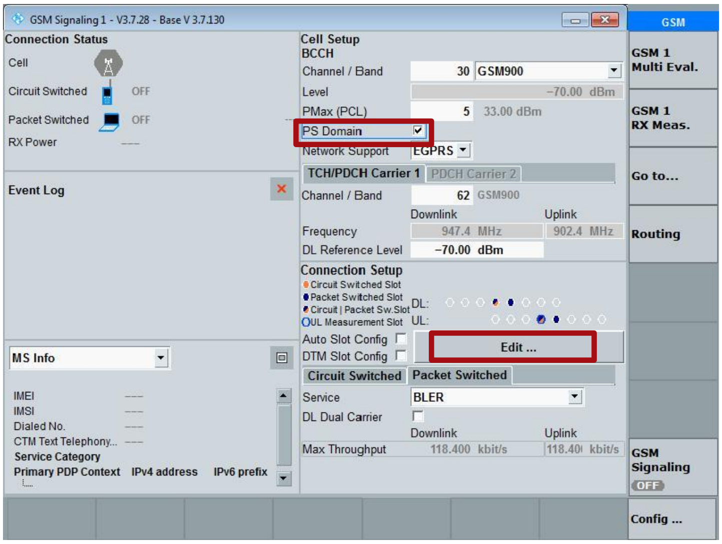
3.3.1.3 Signaling Configuration

In this chapter, the necessary settings of each RAT (GSM, WCDMA, LTE) signaling to enable the packet data connection are described. This step is required when an eUICC profile is downloaded to the eUICC through Secure Channel Protocol 81 (SCP81) which is usually the case.

3.3.1.3.1 GSM

Basically, the default CMW setting for GSM can be kept as shown in Fig. 3-24. Double check whether "PS Domain" is enabled. To enhance the data transfer rate in GSM technology, allocating more uplink and downlink slots is recommended. This can be achieved by pressing "Edit …" button in connection setup part which opens the "slot configuration" window.

In the slot configuration, set higher order modulation coding scheme (e.g. MCS9) for the uplink and downlink and enable both slot 3 and 4 for uplink and downlink communication. See Fig. 3-25. And press "OK" to save the settings.


GSM Signaling 1 - V3.7.28 - Base V 3.7.130

Connection Status
Cell
Circuit Switched OFF
Packet Switched OFF
RX Power ----

Event Log

MS Info
IMEI ----
IMSI ----
Dialed No. ----
CTM Text Telephony... ----
Service Category
Primary PDP Context IPv4 address IPv6 prefix

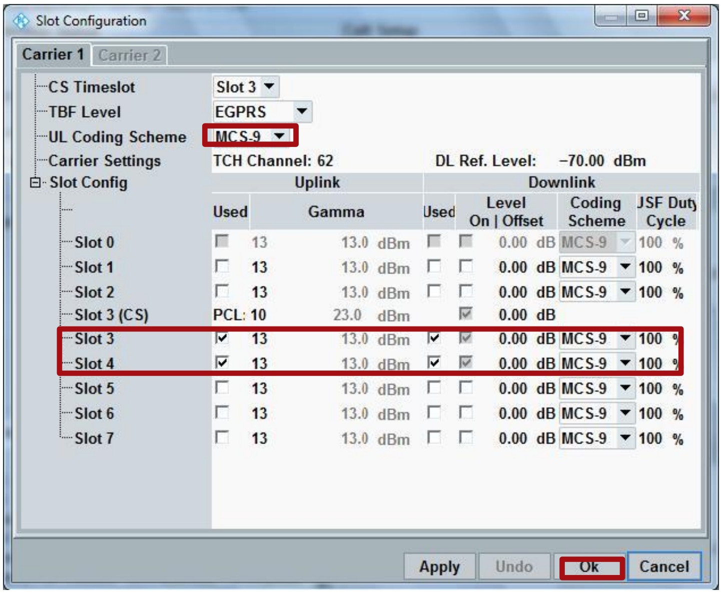
Cell Setup
BCCH
Channel / Band 30 GSM900
Level –70.00 dBm
PMax (PCL) 5 33.00 dBm
PS Domain ☑
Network Support EGPRS

TCH/PDCH Carrier 1 | PDCH Carrier 2
Channel / Band 62 GSM900
Frequency: Downlink 947.4 MHz, Uplink 902.4 MHz
DL Reference Level –70.00 dBm

Connection Setup
● Circuit Switched Slot
● Packet Switched Slot
● Circuit | Packet Sw.Slot
○ UL Measurement Slot
DL: ○ ○ ○ ● ● ○ ○ ○
UL: ○ ○ ○ ● ● ○ ○ ○
Auto Slot Config □
DTM Slot Config □
Edit ...

Circuit Switched | Packet Switched
Service BLER
DL Dual Carrier □
Max Throughput: Downlink 118.400 kbit/s, Uplink 118.40(kbit/s

Fig. 3-24: GSM Signaling Main Configuration


Slot Configuration

Carrier 1 | Carrier 2

CS Timeslot: Slot 3
TBF Level: EGPRS
UL Coding Scheme: MCS-9
Carrier Settings: TCH Channel: 62 DL Ref. Level: –70.00 dBm

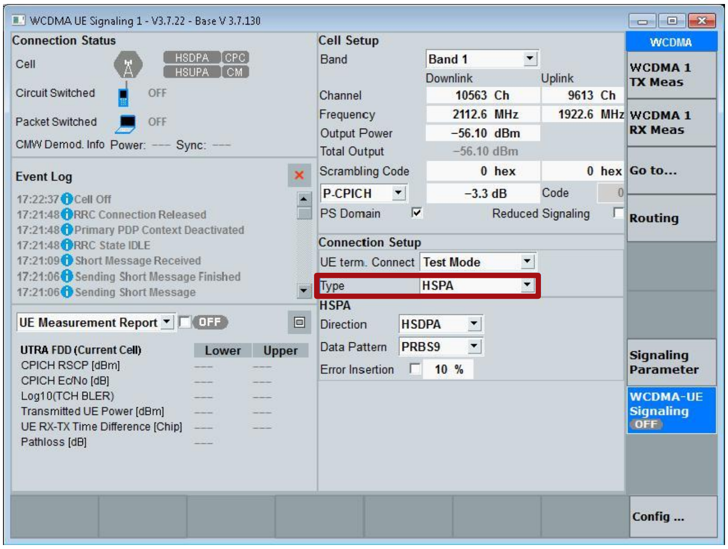
Slot Config

	Uplink			Downlink				
	Used	Gamma		Used	Level On | Offset		Coding Scheme	JSF Duty Cycle
Slot 0	□	13	13.0 dBm	□	□	0.00 dB	MCS-9	100 %
Slot 1	□	13	13.0 dBm	□	□	0.00 dB	MCS-9	100 %
Slot 2	□	13	13.0 dBm	□	□	0.00 dB	MCS-9	100 %
Slot 3 (CS)	PCL: 10		23.0 dBm		☑	0.00 dB		
Slot 3	☑	13	13.0 dBm	☑	☑	0.00 dB	MCS-9	100 %
Slot 4	☑	13	13.0 dBm	☑	☑	0.00 dB	MCS-9	100 %
Slot 5	□	13	13.0 dBm	□	□	0.00 dB	MCS-9	100 %
Slot 6	□	13	13.0 dBm	□	□	0.00 dB	MCS-9	100 %
Slot 7	□	13	13.0 dBm	□	□	0.00 dB	MCS-9	100 %

Fig. 3-25: Configure more downlink and uplink slots and higher order modulation coding scheme

3.3.1.3.2 WCDMA

Ensure that in WCDMA main configuration page, connection type HSPA is selected as shown in Fig. 3-26. The rest of the WCDMA default settings can be kept.



WCDMA UE Signaling 1 - V3.7.22 - Base V 3.7.130

Connection Status

Cell HSDPA CPC HSUPA CM
Circuit Switched OFF
Packet Switched OFF
CMW Demod. Info Power: --- Sync: ---

Event Log

```
17:22:37 Cell Off
17:21:48 RRC Connection Released
17:21:48 Primary PDP Context Deactivated
17:21:48 RRC State IDLE
17:21:09 Short Message Received
17:21:06 Sending Short Message Finished
17:21:06 Sending Short Message
```

UE Measurement Report □ OFF

UTRA FDD (Current Cell)	Lower	Upper
CPICH RSCP [dBm]	---	---
CPICH Ec/No [dB]	---	---
Log10(TCH BLER)	---	---
Transmitted UE Power [dBm]	---	---
UE RX-TX Time Difference [Chip]	---	---
Pathloss [dB]	---	

Cell Setup

	Downlink	Uplink
Band	Band 1	
Channel	10563 Ch	9613 Ch
Frequency	2112.6 MHz	1922.6 MHz
Output Power	-56.10 dBm	
Total Output	-56.10 dBm	
Scrambling Code	0 hex	0 hex
P-CPICH	-3.3 dB	Code 0
PS Domain ☑	Reduced Signaling □	

Connection Setup

UE term. Connect: Test Mode
Type: HSPA

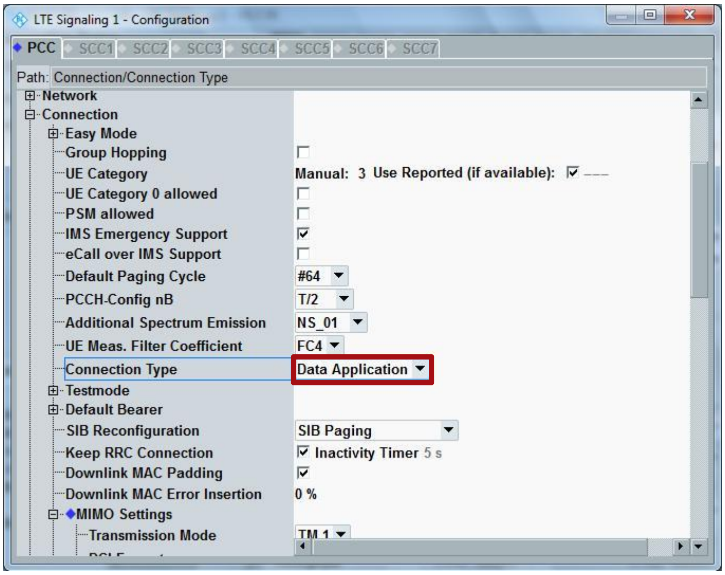
HSPA

Direction: HSDPA
Data Pattern: PRBS9
Error Insertion □ 10 %

Fig. 3-26: WCDMA Signaling Main Configuration

3.3.1.3.3 LTE

In the LTE signaling configuration part, set connection type to "Data Application" as shown in Fig. 3-27, and keep the rest of the default settings.



LTE Signaling 1 - Configuration

Path: Connection/Connection Type

⊞ Network	
⊟ Connection	
⊞ Easy Mode	
Group Hopping	□
UE Category	Manual: 3 Use Reported (if available): ☑ ---
UE Category 0 allowed	□
PSM allowed	□
IMS Emergency Support	☑
eCall over IMS Support	□
Default Paging Cycle	#64
PCCH-Config nB	T/2
Additional Spectrum Emission	NS_01
UE Meas. Filter Coefficient	FC4
Connection Type	Data Application
⊞ Testmode	
⊞ Default Bearer	
SIB Reconfiguration	SIB Paging
Keep RRC Connection	☑ Inactivity Timer 5 s
Downlink MAC Padding	☑
Downlink MAC Error Insertion	0 %
⊟ MIMO Settings	
Transmission Mode	TM 1

Fig. 3-27: Set the Connection Type to Data Application

3.3.2 Operations in eUICC Profile Manager (ePM)

COMPRION® eUICC Profile Manager (ePM) is a product under software license binding. Make sure that a valid license has been activated before the tool is launched on test PC. Details on this can be obtained from the documentation provided by COMPRION® when the license is purchased. In general, for any ePM related inquiries, please contact COMPRION® at support@comprion.com

3.3.2.1 Connection Management

Launch ePM by double mouse click on the eUICC Profile Manager icon on the test PC desktop and create a new CMW290/500 connection as shown in Fig. 3-28, if there is no existed one available.

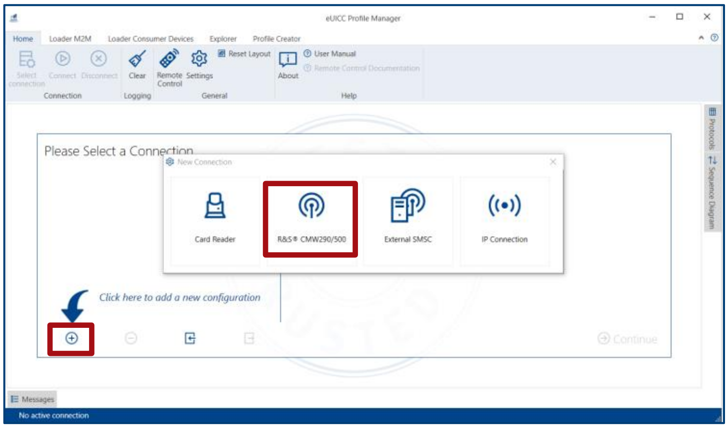
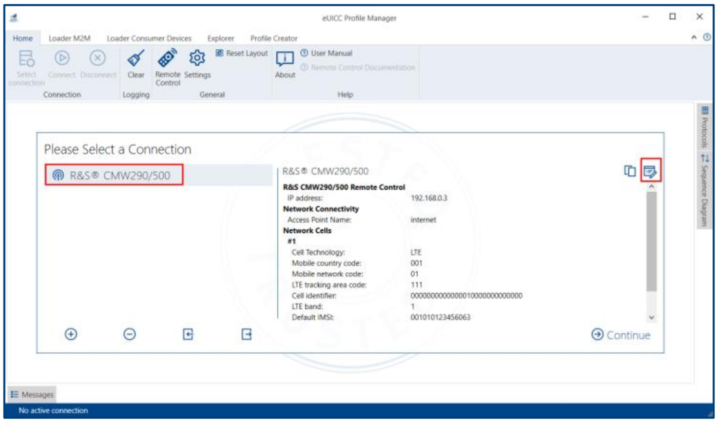


Fig. 3-28: Create a new CMW290/500 connection

In case there already exists a CMW290/500 connection, select it and press "Edit" button on the upper right corner as illustrated in Fig. 3-29 to adapt the settings.

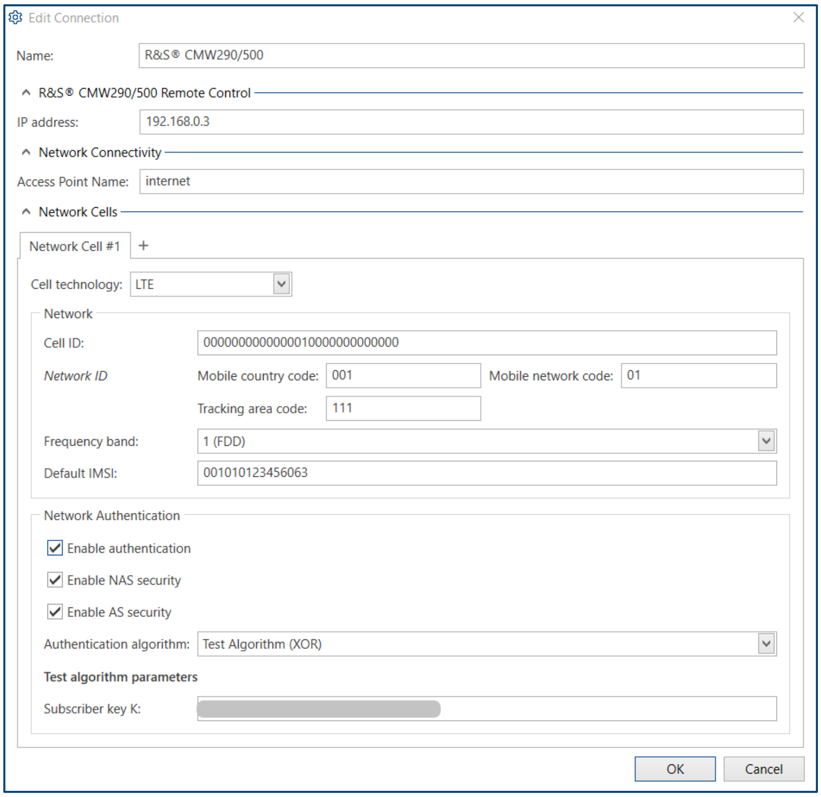


R&S® CMW290/500

R&S CMW290/500 Remote Control
IP address: 192.168.0.3
Network Connectivity
Access Point Name: internet
Network Cells
#1
Cell Technology: LTE
Mobile country code: 001
Mobile network code: 01
LTE tracking area code: 111
Cell identifier: 0000000000000010000000000000
LTE band: 1
Default IMSI: 001010123456063

Fig. 3-29: Select and edit an existing CMW290/500 connection

By creating a new connection or editing an existing connection, connection configuration page Fig. 3-30 is launched, where the cellular network configuration, authentication/security settings and associated key can be configured depending on the used RAT and parameters of the test eUICC. Those settings have to match the contents of the test eUICC. Otherwise, the DUT won't be able to attach to the cellular network.



Edit Connection

Name: R&S® CMW290/500

R&S® CMW290/500 Remote Control

IP address: 192.168.0.3

Network Connectivity

Access Point Name: internet

Network Cells

Network Cell #1 +

Cell technology: LTE

Network

Cell ID: 0000000000000010000000000000

Network ID Mobile country code: 001 Mobile network code: 01

Tracking area code: 111

Frequency band: 1 (FDD)

Default IMSI: 001010123456063

Network Authentication

☑ Enable authentication

☑ Enable NAS security

☑ Enable AS security

Authentication algorithm: Test Algorithm (XOR)

Test algorithm parameters

Subscriber key K: [redacted]

Fig. 3-30: LTE Connection setup in eUICC Tool

Fig. 3-30 indicates the LTE Connection setup as an example. Similar connection settings are valid for GSM and for WCDMA with minor changes. Ensure the IP address entered in the CMW290/500 Remote Control section is the LAN remote IP address.

Table 3-6 lists all the connection parameters of ePM. For more detailed information, refer to COMPRION ePM online user manual [7] coming along with the ePM installation.

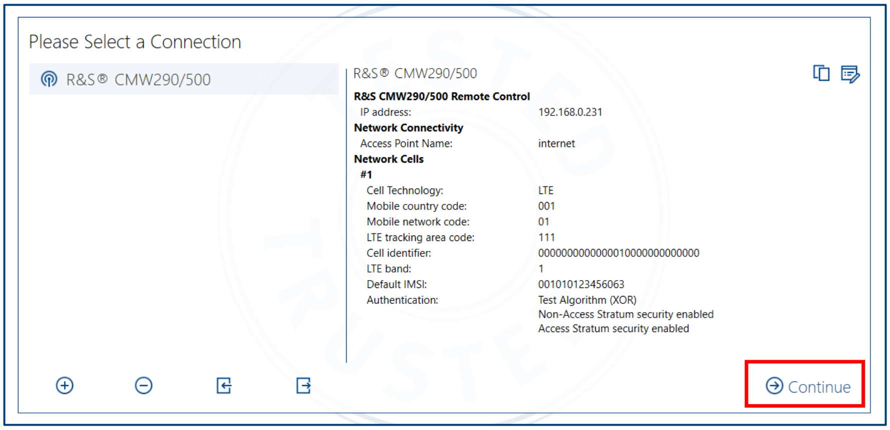
Field	Comment
IP address	The IP address of CMW LAN remote port
Access Point Name	The access point name that DUT used for generating the default bearer. Default setting "internet" can be used
Cell technology	Choose the RAT between LTE, GSM and UMTS(W-CDMA)
Cell ID	Used for generation of the physical synchronization signals. Default value can be used
Mobile country code	Three-digit mobile country code (MCC). The first three-digit of IMSI.
Mobile network code	Two or three-digit mobile network code (MNC). The next two or three digits after the MCC in IMSI
Tracking area code	Default value can be used here, only relevant for LTE
Location area code	Default value can be used here, only relevant for GSM and WCDMA
Routing area code	Default value can be used here, only relevant for GSM and WCDMA
Frequency band	Enter the frequency band that the DUT supports
Default IMSI	Enter the same IMSI stored on the eUICC
Enable authentication	Enable or disable the authentication process
Enable NAS security	Enables or disables non-access stratum (NAS) security. With enabled NAS security, the UE uses integrity protection for NAS signaling. This setting is only relevant for LTE and if authentication is enabled.
Enable AS security	Enables or disables access stratum (AS) security. With enabled AS security, the UE uses integrity protection for RRC signaling. This setting is only relevant for LTE and if authentication is enabled
Authentication algorithm	Choose the authentication algorithm stored on the eUICC between "Test Algorithm (XOR)" and "MILENAGE".
OPc	Authentication and integrity check procedure parameter related to MILENAGE algorithm. The same value as the one on the eUICC should be entered here.

Field	Comment
Subscriber key K	Subscriber key used for the authentication process. The same value as the one on the eUICC should be entered here.

Table 3-6: Parameters of a Connection

After all the settings are configured in connection setup page, press OK button. A summary of connection is displayed in Fig. 3-31

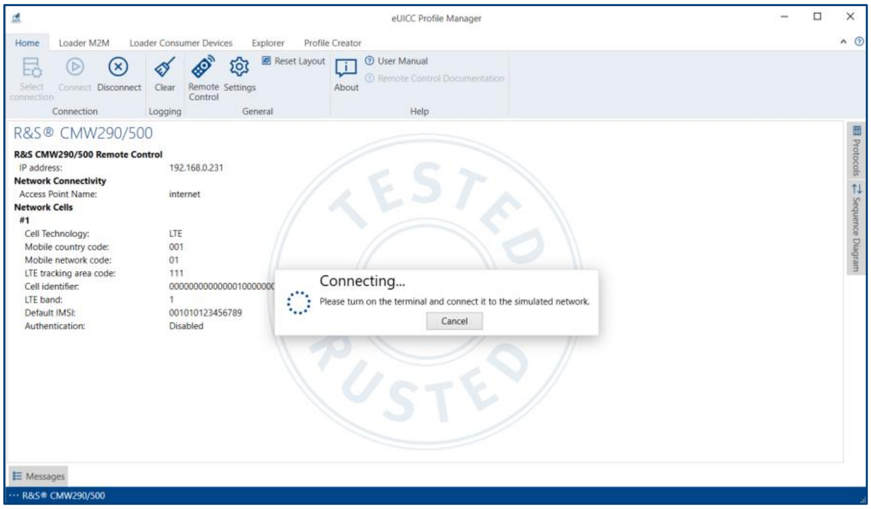
Make sure that the RAT intends to be used is already launched and set properly on CMW as described in Chapter 3.3.1.



```
R&S® CMW290/500
R&S CMW290/500 Remote Control
  IP address:                  192.168.0.231
Network Connectivity
  Access Point Name:           internet
Network Cells
  #1
    Cell Technology:           LTE
    Mobile country code:       001
    Mobile network code:       01
    LTE tracking area code:    111
    Cell identifier:           0000000000000001000000000000
    LTE band:                  1
    Default IMSI:              001010123456063
    Authentication:            Test Algorithm (XOR)
                               Non-Access Stratum security enabled
                               Access Stratum security enabled
```

Fig. 3-31: Summary of connection

Now, if "Continue" button is pressed, the connection setup settings of Fig. 3-30 are sent to CMW remotely by ePM and the signaling of the selected RAT is turned on consequently. At the meanwhile, ePM prompts up the message box to ask to turn on the DUT, see Fig. 3-32. The message box vanishes automatically as long as the DUT successfully attaches to the cell, see Fig. 3-33.



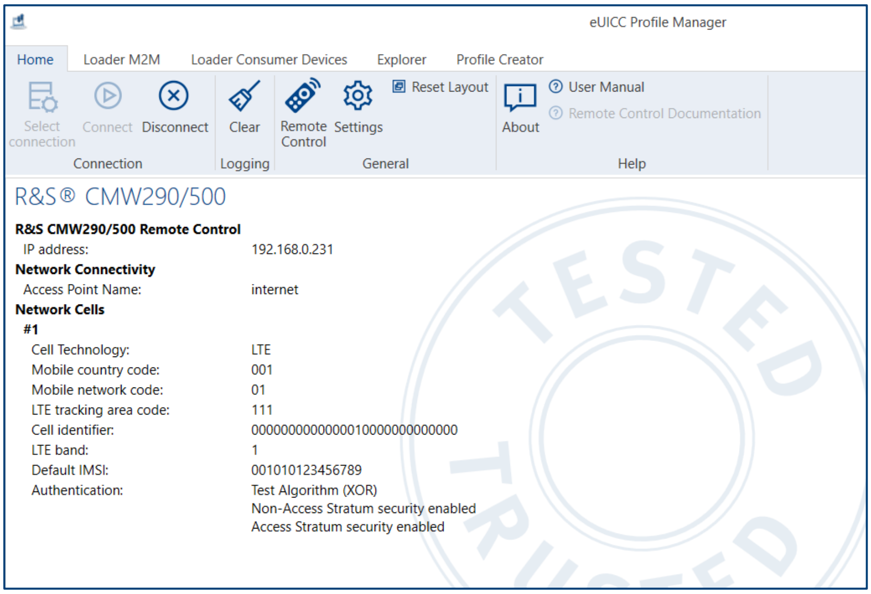
```
R&S® CMW290/500
R&S CMW290/500 Remote Control
  IP address:                  192.168.0.231
Network Connectivity
  Access Point Name:           internet
Network Cells
  #1
    Cell Technology:           LTE
    Mobile country code:       001
    Mobile network code:       01
    LTE tracking area code:    111
    Cell identifier:           00000000000000010000000
    LTE band:                  1
    Default IMSI:              001010123456789
    Authentication:            Disabled
```

Connecting...

Please turn on the terminal and connect it to the simulated network.

Cancel

Fig. 3-32: eUICC Tool remotely switches on the cell and wait for DUT registration



R&S® CMW290/500

R&S CMW290/500 Remote Control

IP address: 192.168.0.231

Network Connectivity

Access Point Name: internet

Network Cells

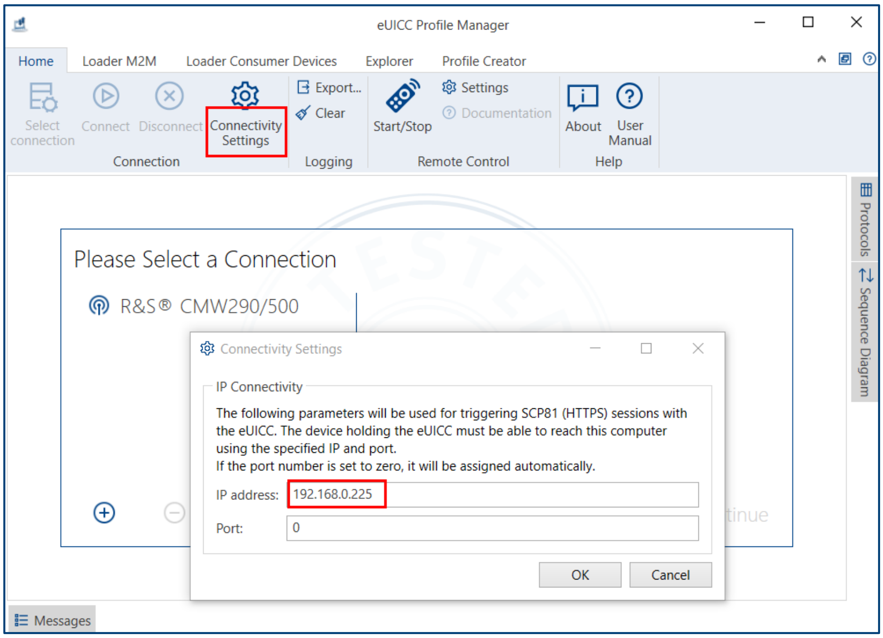
#1

Cell Technology: LTE
Mobile country code: 001
Mobile network code: 01
LTE tracking area code: 111
Cell identifier: 0000000000000010000000000000
LTE band: 1
Default IMSI: 001010123456789
Authentication: Test Algorithm (XOR)
Non-Access Stratum security enabled
Access Stratum security enabled

Fig. 3-33: Connection successfully established

For the packet switched communication using SCP81 (SCP81 configuration is going to be explained later in 3.3.2.2), it is required to enter the correct test PC IP address in the connectivity setting as shown in Fig. 3-34 in ePM. The default port number value "0" can be kept there.

If the setting is incorrect, SCP81 session is failed to be established. This will force the data connection, for example profile downloading, to fall back to SCP80, i.e. using the normal SMS for data transfer instead of HTTPs.



IP Connectivity

The following parameters will be used for triggering SCP81 (HTTPS) sessions with the eUICC. The device holding the eUICC must be able to reach this computer using the specified IP and port.
If the port number is set to zero, it will be assigned automatically.

IP address: 192.168.0.225
Port: 0

Fig. 3-34: Connectivity Settings

3.3.2.2 eUICC Configuration

As long as DUT is attached to the CMW or CMX, select "Loader M2M" module to add a new or edit an existing eUICC configuration (Fig. 3-35). With the launch of this module, no end user interactions are required. Profile management, eUICC provisioning are all initiated from the network side.

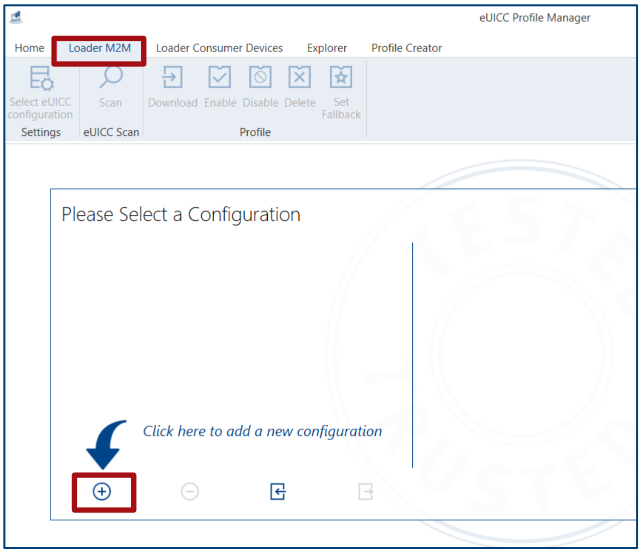
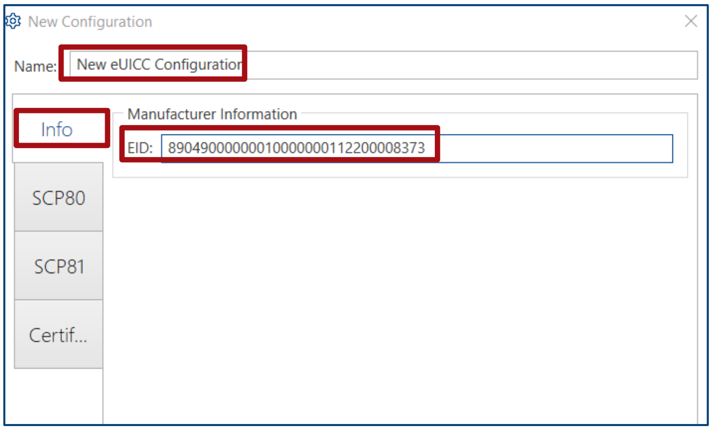


Fig. 3-35: Add a new eUICC configuration on a M2M device (non-SAS compliant)

In the configuration window, name the configured eUICC in the Name field.

Enter the proper eUICC ID (EID) in the Info tab as shown in Fig. 3-36. The EID on the eUICC is an unique ID which is created by the vendor and resides on the eUICC. It is used in the context of remote provisioning and management of the eUICC. The EID mismatch between the configuration in ePM and the one written on the eUICC will lead to the failure of any profile provision or management procedure.



Name: New eUICC Configuratior

Manufacturer Information

EID: 89049000000010000000112200008373

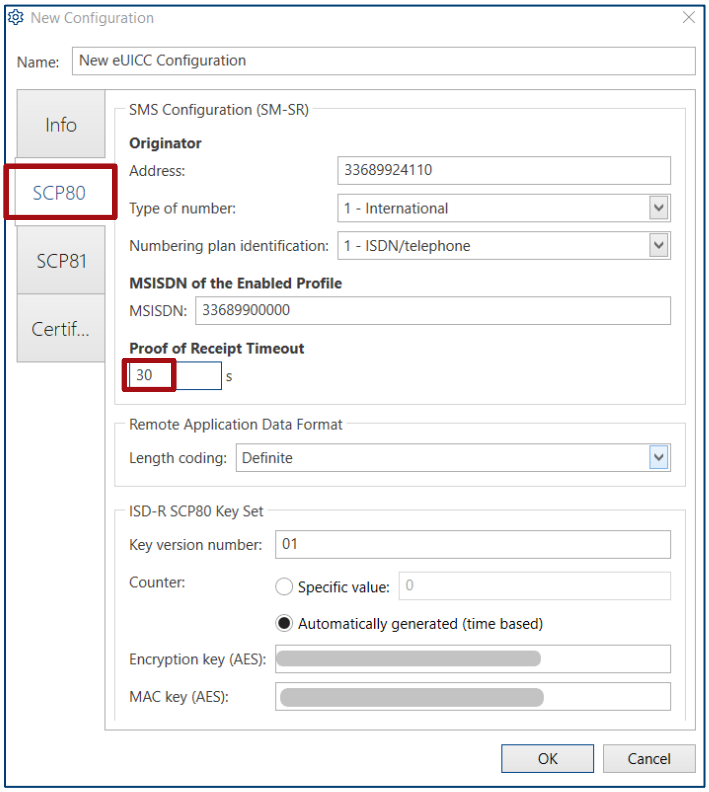
Fig. 3-36: Enter EID number

For the secure communication between eUICC and SM-SR (ES5 interface of Fig. 3-1), mandatory secure communication protocol SCP80 (SMS or CAT_TP) is utilized. The optional SCP81 (HTTPs) can be applied in addition.

Secure Channel Protocol 80 (SCP80) Tab shown in Fig. 3-37 includes the parameters of an outgoing SMS, as well as the parameters of the SCP80 key set.

In most cases, the default settings can be applied as long as the eUICC is provided by COMPRION. Otherwise, the settings should be adapted according to the contents of the eUICC under test.

Parameter "Proof of Receipt Timeout" can be adjusted according to the used RAT. The timeout timer is applied by ePM to wait for the message acknowledgement sent by the DUT. In normal case, the default value 30s is sufficient. However, for legacy RAT with low transmission rate, e.g. GSM, an experience value of greater than 60s is recommended.


New Configuration

Name: New eUICC Configuration

SMS Configuration (SM-SR)

Originator

Address: 33689924110

Type of number: 1 - International

Numbering plan identification: 1 - ISDN/telephone

MSISDN of the Enabled Profile

MSISDN: 33689900000

Proof of Receipt Timeout

30 s

Remote Application Data Format

Length coding: Definite

ISD-R SCP80 Key Set

Key version number: 01

Counter: ○ Specific value: 0

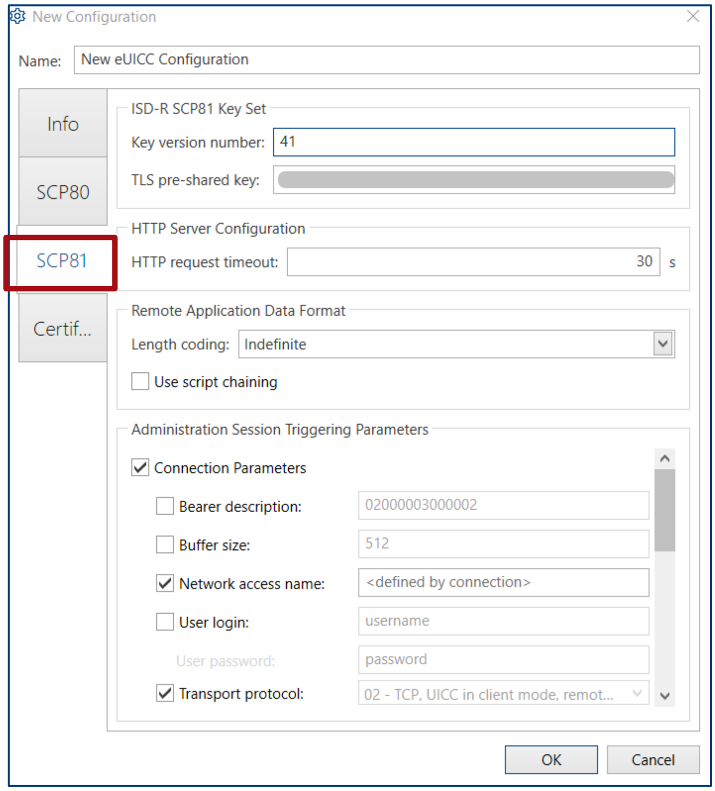
● Automatically generated (time based)

Encryption key (AES):

MAC key (AES):

Fig. 3-37: SCP80 settings

SCP81 and Certificate Tab, shown in Fig. 3-38 and Fig. 3-39 respectively, contains the parameters required for HTTPs communication.


New Configuration

Name: New eUICC Configuration

ISD-R SCP81 Key Set

Key version number: 41

TLS pre-shared key:

HTTP Server Configuration

HTTP request timeout: 30 s

Remote Application Data Format

Length coding: Indefinite

□ Use script chaining

Administration Session Triggering Parameters

☑ Connection Parameters

□ Bearer description: 02000003000002

□ Buffer size: 512

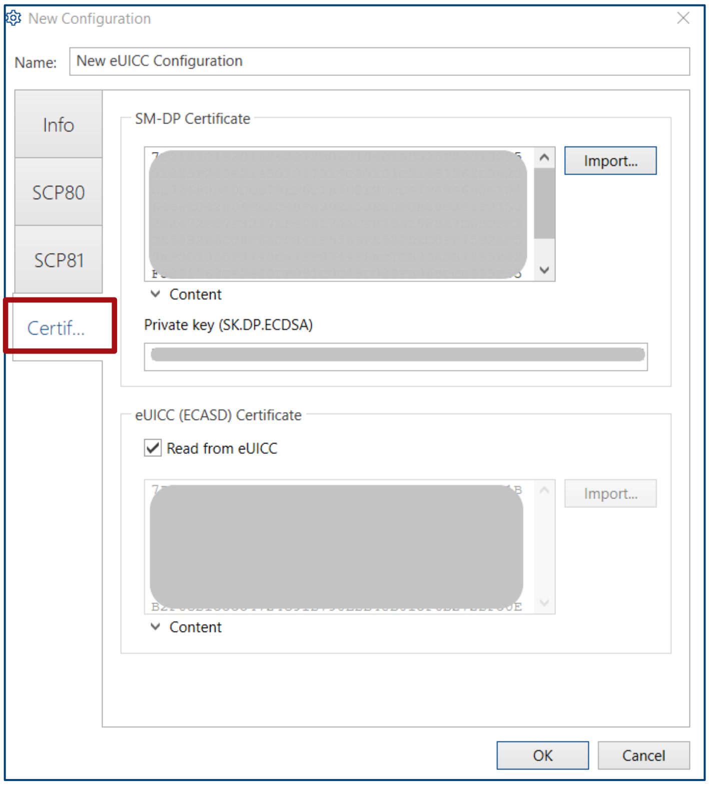
☑ Network access name: <defined by connection>

□ User login: username

User password: password

☑ Transport protocol: 02 - TCP, UICC in client mode, remot...

Fig. 3-38: SCP81 default settings



Name: New eUICC Configuration

SM-DP Certificate

[redacted]

Content

Private key (SK.DP.ECDSA)

[redacted]

eUICC (ECASD) Certificate

☑ Read from eUICC

[redacted]

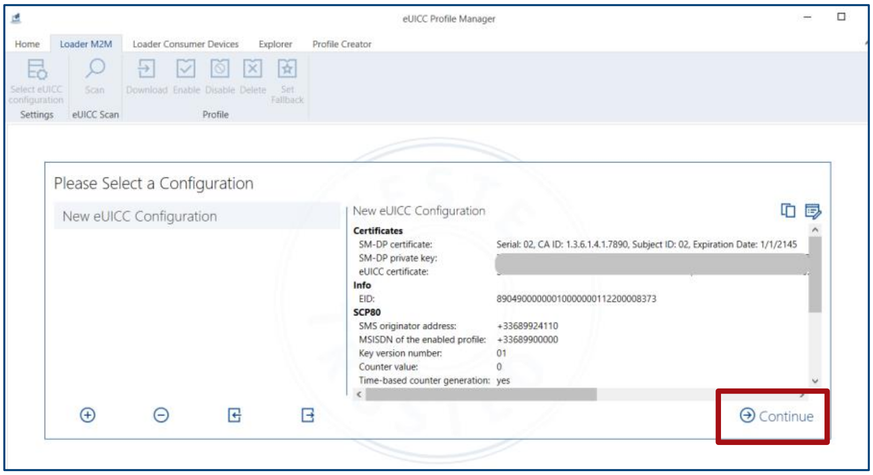
Content

Fig. 3-39: Certificate default settings

The majority of the default settings in both tabs can be kept. "HTTP request timeout" timer can be adjusted to allow longer response time.

The default settings of "Administration Session Triggering Parameters" can be kept. Those settings are composed in the SMS which trigger the HTTPs session. The HTTPs session trigger procedure can refer to Chapter 3.1.3.

Press OK after eUICC configuration is finalized. The summary of eUICC configuration is then displayed in Fig. 3-40.



Please Select a Configuration

New eUICC Configuration

New eUICC Configuration

Certificates

SM-DP certificate:	Serial: 02, CA ID: 1.3.6.1.4.1.7890, Subject ID: 02, Expiration Date: 1/1/2145
SM-DP private key:	[redacted]
eUICC certificate:	[redacted]

Info

EID:	89049000000010000000112200008373

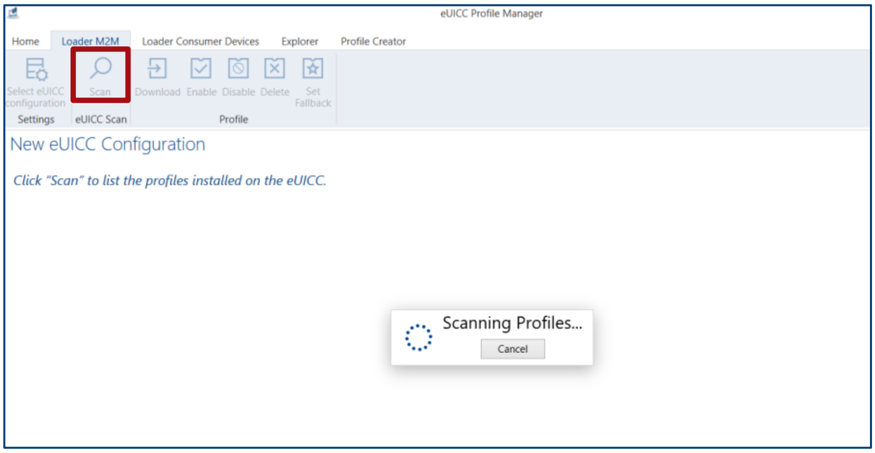
SCP80

SMS originator address:	+33689924110
MSISDN of the enabled profile:	+33689900000
Key version number:	01
Counter value:	0
Time-based counter generation:	yes

Fig. 3-40: Summary of eUICC configuration

3.3.2.3 Profile Scanning

Press "Continue" button in the Fig. 3-40 and start the eUICC profile scanning (Fig. 3-41) by pressing "Scan" button. This operation invokes the eUICC Capability Audit function and scans all the installed profiles on the eUICC.



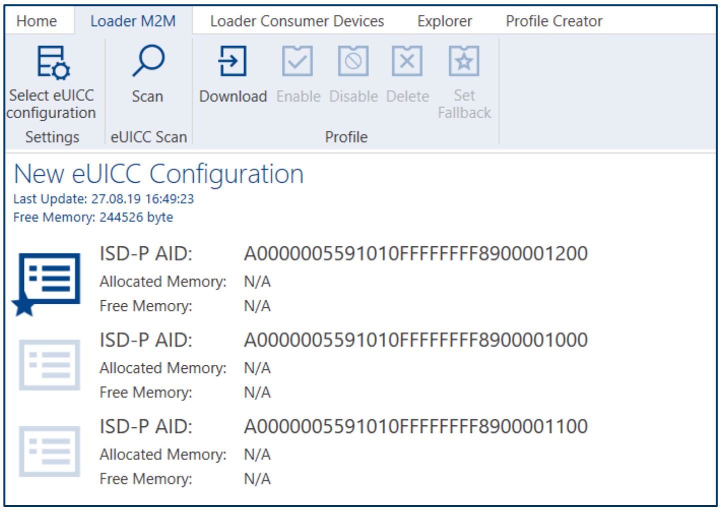
New eUICC Configuration

Click "Scan" to list the profiles installed on the eUICC.

Scanning Profiles...

Fig. 3-41: eUICC Profile Scan

After the successful profile scanning, all available eUICC Profiles on the eUICC are listed as shown in Fig. 3-42. The activated profile is highlighted in comparison to the deactivated ones.



New eUICC Configuration

Last Update: 27.08.19 16:49:23
Free Memory: 244526 byte

ISD-P AID: A0000005591010FFFFFFFF8900001200
Allocated Memory: N/A
Free Memory: N/A

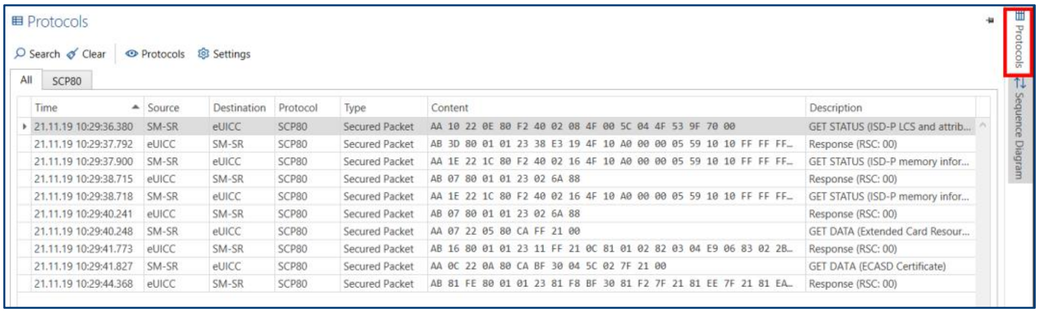
ISD-P AID: A0000005591010FFFFFFFF8900001000
Allocated Memory: N/A
Free Memory: N/A

ISD-P AID: A0000005591010FFFFFFFF8900001100
Allocated Memory: N/A
Free Memory: N/A

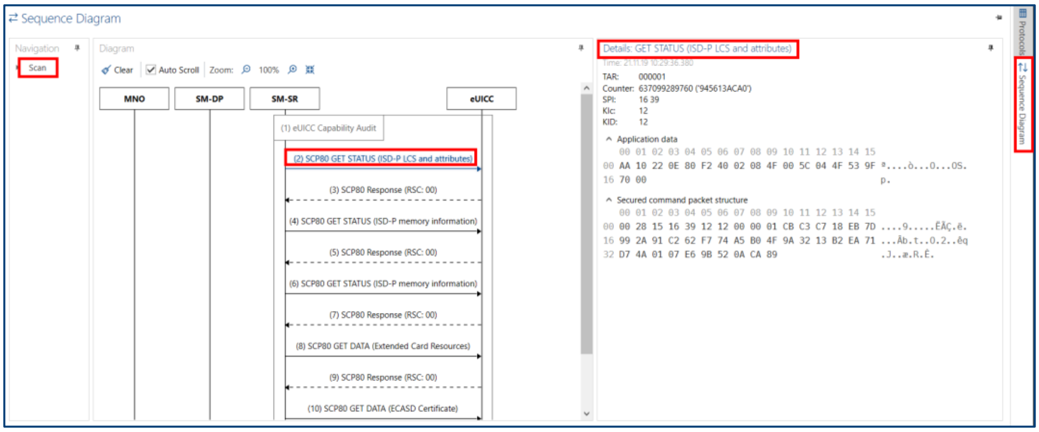
Fig. 3-42: eUICC Profile Scan result shows all the available eUICC profiles

The successful profile scanning is the prerequisite for the subsequent profile operations in Chapter 3.3.2.4.

For debugging purpose, ePM provides also comprehensive protocol logging and sequence diagram view of occurred operation and its associated procedure. An example is shown in Fig. 3-43.



Time	Source	Destination	Protocol	Type	Content	Description
21.11.19 10:29:36.380	SM-SR	eUICC	SCP80	Secured Packet	AA 10 22 0E 80 F2 40 02 08 4F 00 5C 04 4F 53 9F 70 00	GET STATUS (ISD-P LCS and attrib...
21.11.19 10:29:37.792	eUICC	SM-SR	SCP80	Secured Packet	AB 3D 80 01 01 23 38 E3 19 4F 10 A0 00 00 05 59 10 10 FF FF FF...	Response (RSC: 00)
21.11.19 10:29:37.900	SM-SR	eUICC	SCP80	Secured Packet	AA 1E 22 1C 80 F2 40 02 16 4F 10 A0 00 00 05 59 10 10 FF FF FF...	GET STATUS (ISD-P memory infor...
21.11.19 10:29:38.715	eUICC	SM-SR	SCP80	Secured Packet	AB 07 80 01 01 23 02 6A 88	Response (RSC: 00)
21.11.19 10:29:38.718	SM-SR	eUICC	SCP80	Secured Packet	AA 1E 22 1C 80 F2 40 02 16 4F 10 A0 00 00 05 59 10 10 FF FF FF...	GET STATUS (ISD-P memory infor...
21.11.19 10:29:40.241	eUICC	SM-SR	SCP80	Secured Packet	AB 07 80 01 01 23 02 6A 88	Response (RSC: 00)
21.11.19 10:29:40.248	SM-SR	eUICC	SCP80	Secured Packet	AA 07 22 05 80 CA FF 21 00	GET DATA (Extended Card Resour...
21.11.19 10:29:41.773	eUICC	SM-SR	SCP80	Secured Packet	AB 16 80 01 01 23 11 FF 21 0C 81 01 02 82 03 04 E9 06 83 02 2B...	Response (RSC: 00)
21.11.19 10:29:41.827	SM-SR	eUICC	SCP80	Secured Packet	AA 0C 22 0A 80 CA BF 30 04 5C 02 7F 21 00	GET DATA (ECASD Certificate)
21.11.19 10:29:44.368	eUICC	SM-SR	SCP80	Secured Packet	AB 81 FE 80 01 01 23 81 F8 BF 30 81 F2 7F 21 81 EE 7F 21 81 EA...	Response (RSC: 00)



(1) eUICC Capability Audit
(2) SCP80 GET STATUS (ISD-P LCS and attributes)
(3) SCP80 Response (RSC: 00)
(4) SCP80 GET STATUS (ISD-P memory information)
(5) SCP80 Response (RSC: 00)
(6) SCP80 GET STATUS (ISD-P memory information)
(7) SCP80 Response (RSC: 00)
(8) SCP80 GET DATA (Extended Card Resources)
(9) SCP80 Response (RSC: 00)
(10) SCP80 GET DATA (ECASD Certificate)

Details: GET STATUS (ISD-P LCS and attributes)

Time: 21.11.19 10:29:36.380

```
TAR:      000001
Counter:  637099289760 ('945613ACA0')
SPI:      16 39
KIc:      12
KID:      12

^ Application data
   00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
00 AA 10 22 0E 80 F2 40 02 08 4F 00 5C 04 4F 53 9F ª....ò...O...OS.
16 70 00                                           p.

^ Secured command packet structure
   00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
00 00 28 15 16 39 12 12 00 00 01 CB C3 C7 18 EB 7D ....9.....ËÃÇ.ë.
16 99 2A 91 C2 62 F7 74 A5 B0 4F 9A 32 13 B2 EA 71 ...Âb.t..O.2..êq
32 D7 4A 01 07 E6 9B 52 0A CA 89                   .J..æ.R.Ê.
```

Fig. 3-43: Protocol and Sequence Diagram in eUICC Profile Manager

3.3.2.4 Work with Profiles

Now, there are several operations that can be applied to the profiles on the eUICC:

- Download - download the new eUICC profile which is generated beforehand by Profile Creator or directly from the eUICC vendor
- Enable - To activate an installed eUICC profile
- Disable - To deactivate an installed eUICC profile
- Delete - To delete an installed eUICC profile
- Set Fallback - To set the fallback attribute for a profile. A eUICC profile with fallback attribute is active in case the swapping to another profile fails due to e.g. loss of a network connectivity during the activation.

Utilize the message logging and sequence diagram provided by ePM to get insights of the messages and the entire procedure flow. For specification reference to check the conformity of each procedure, please refer to [1].

4 eUICC Handling of Non-SAS Compliant Consumer Devices

For non-SAS compliant consumer devices, the same test procedures as described in Chapter 2 for non-SAS compliant M2M devices are still hold here except that the function module "Load Consumer Devices" needs to be selected in ePM instead (see Fig. 4-1).

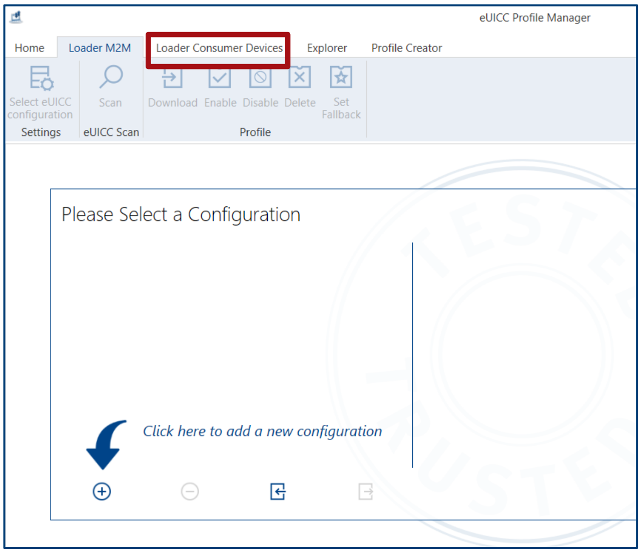


Fig. 4-1 Add a new eUICC configuration on a consumer device (non-SAS compliant)

Please be aware of the limitation of the ePM support as mentioned in the footnote 3 below.

5 eSIM Test Profile Service for SAS-Compliant Consumer Devices[3]

eSIM Test Profile Service, a service developed by COMPRION®, is the only tool to provision the eSIM profile onto a consumer device that follows the stringent GSMA SAS framework (for more information about GSMA SAS, please visit: https://www.gsma.com/security/security-accreditation-scheme) which is essential for market ready consumer devices. This is typically the case for the user group in the area of device production, conformance, service and network operator. At the time of the release of this document, eSIM Test Profile Service supports only consumer devices. Whereas the support of SAS compliant M2M devices is expected to be specified and released in the near future.

When testing such market ready eSIM consumer devices on CMW or CMX, the conventional plug-in R&S test SIM is now tailored by COMPRION® as an eSIM test profile and downloadable via eSIM Test Profile Service under full GSMA SAS compliant environment.

Test Profile Service can be ordered through COMPRION® web shop (https://www.comprion.com/shop/esim-test-profiles/) or COMPRION's sales representatives. Access to the self-service portal (https://rsp.console.truphone.com/) is only granted after the purchase of the service credits. The self-service portal contains eSIM profile repository where out-of-the-box (with standard GSMA test profiles) and purchased eSIM profiles (e.g. R&S test eSIM) are located. The usage of the eSIM profile is based on pay-per-use price model. For more detailed information about eSIM Test Profile Service, please get in contact with COMPRION® directly or visit https://www.comprion.com/comprion-test-profile-service/

Hereafter, steps of using the R&S® test eSIM profile via eSIM Test Profile Service are highlighted provided that service credits are purchased at COMPRION® beforehand:

[3] eSIM Test Profile Service can NOT serve devices that assume a protocol for profile downloading which differs from what is described by GSMA, e.g. there are devices which utilize in the overall download process also an entitlement server. Such devices can NOT be served (this also holds true for the eUICC Profile Manager for non-SAS-compliant devices).

1. To get the access to the self-service portal, you need to have followings from COMPRION®
   a) A certificate in .pfx format that has to be installed on your test PC
   b) Login credentials (user name and password)

   Fig. 5-1 shows the log-in page of self-service portal (visit https://rsp.console.truphone.com/).

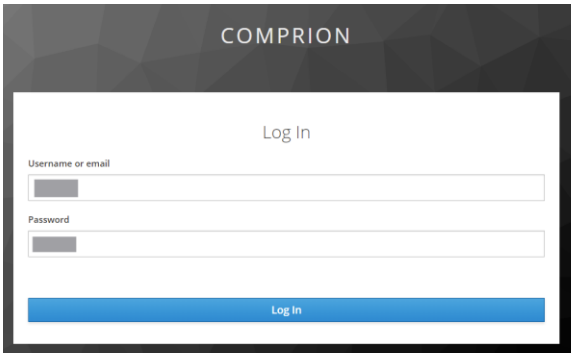


Fig. 5-1 COMPRION® self-service portal login (https://rsp.console.truphone.com/)

2. In the self-service portal, a collection of out-of-the-box eSIM profiles and purchased R&S Test eSIM profiles are available for selection in profile inventory of the "Profiles" area. Choose available R&S eSIM test profile "XYZ-B-R&S GSMA Test Profile", where XYZ is the customer number and B is the indicator of the profile class. Press on "ORDER" button to generate a QR code that contains the download link of the selected eSIM profile. After the QR code generated, the profile status of the selected profile is changed from "Available" to "Released"

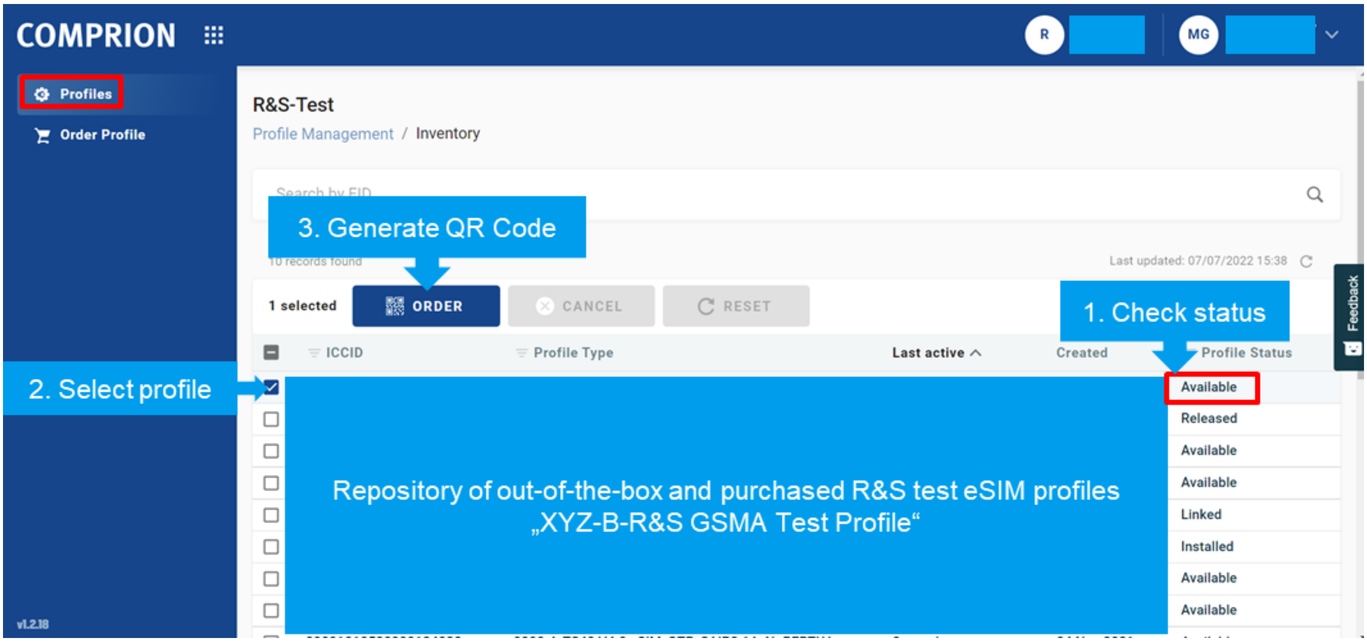
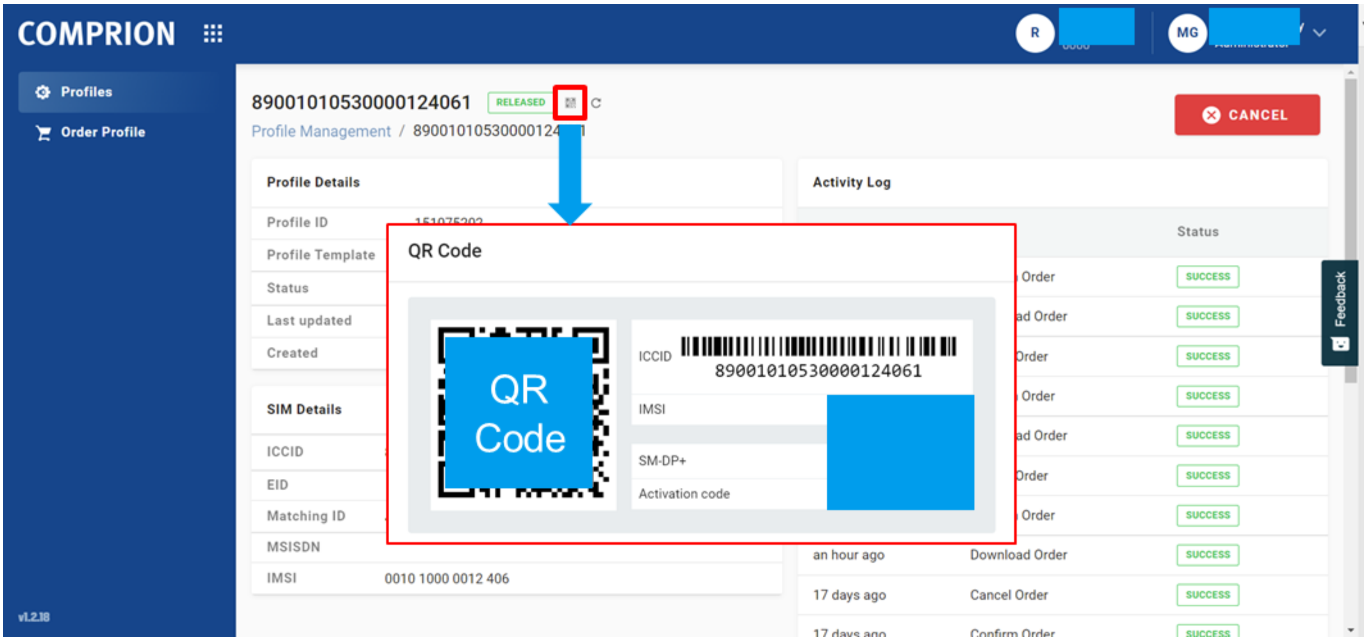


Fig. 5-2 QR code generation for an eSIM profile

3. Click on a profile with "Released" profile status, its profile details, SIM details and activity log are displayed. Mouse click on ▦ button will show the generated QR code.

   Please bear in mind that an unique IMSI is associated with each profile. Make sure that IMSI of the R&S eSIM test profile should match the one that is set on the CMW or CMX.



COMPRION [redacted] [redacted]

- Profiles
- Order Profile

v1.2.18

89001010530000124061 RELEASED

Profile Management / 890010105300001241

CANCEL

Profile Details

Profile ID	151075202
Profile Template	
Status	
Last updated	
Created	

SIM Details

ICCID	
EID	
Matching ID	
MSISDN	
IMSI	0010 1000 0012 406

Activity Log

		Status
	Order	SUCCESS
	ad Order	SUCCESS
	Order	SUCCESS
	Order	SUCCESS
	ad Order	SUCCESS
	Order	SUCCESS
	Order	SUCCESS
an hour ago	Download Order	SUCCESS
17 days ago	Cancel Order	SUCCESS
17 days ago	Confirm Order	SUCCESS

QR Code

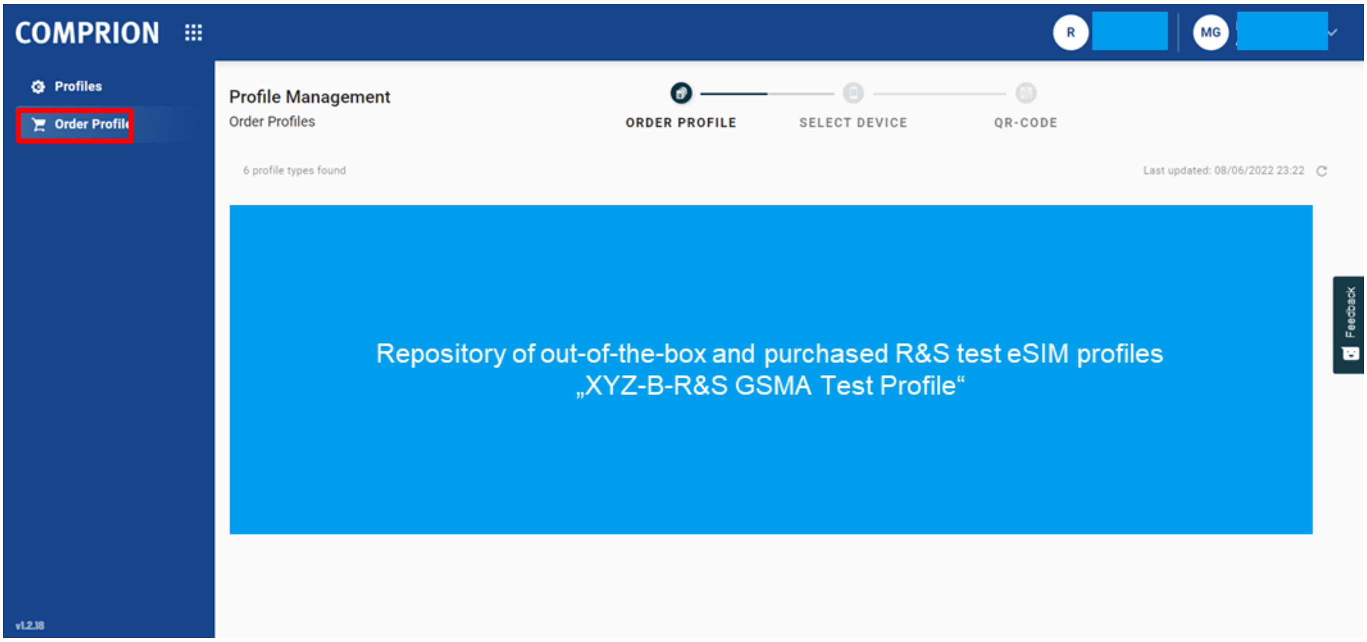
[redacted]

ICCID	89001010530000124061
IMSI	[redacted]
SM-DP+	
Activation code	

Fig. 5-3 QR code display

Alternatively, the QR code can be generated in the "Order Profile" area in the self-service portal.

1. In "Order Profile" area, choose R&S eSIM test profile "XYZ-B-R&S GSMA Test Profile". Fig. 5-4 represents the eSIM profile repository in the portal.



COMPRION R [redacted] MG [redacted]

- Profiles
- Order Profile

v1.2.18

Profile Management

Order Profiles

ORDER PROFILE — SELECT DEVICE — QR-CODE

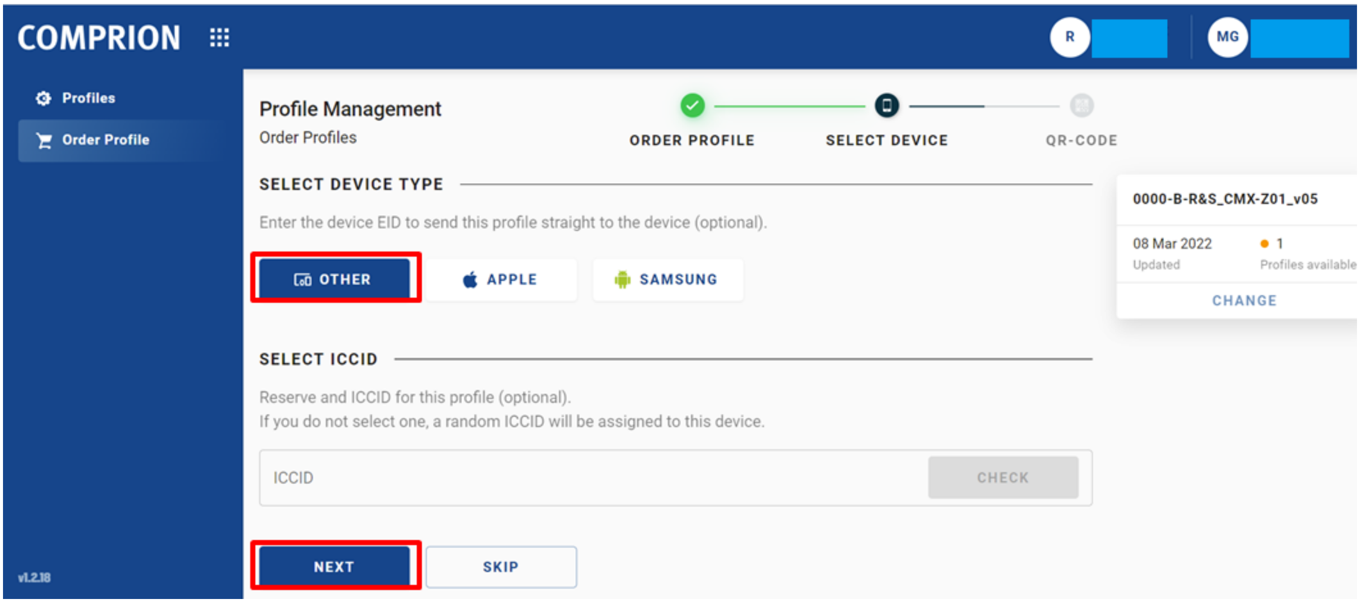
6 profile types found

Last updated: 08/06/2022 23:22

Repository of out-of-the-box and purchased R&S test eSIM profiles „XYZ-B-R&S GSMA Test Profile“

Fig. 5-4 Select R&S eSIM test profile in the portal

2. In the next step, select 'Other' for the device type and confirm the step by pressing 'Next' button as shown in Fig. 5-5.



Profile Management
Order Profiles

SELECT DEVICE TYPE

Enter the device EID to send this profile straight to the device (optional).

SELECT ICCID

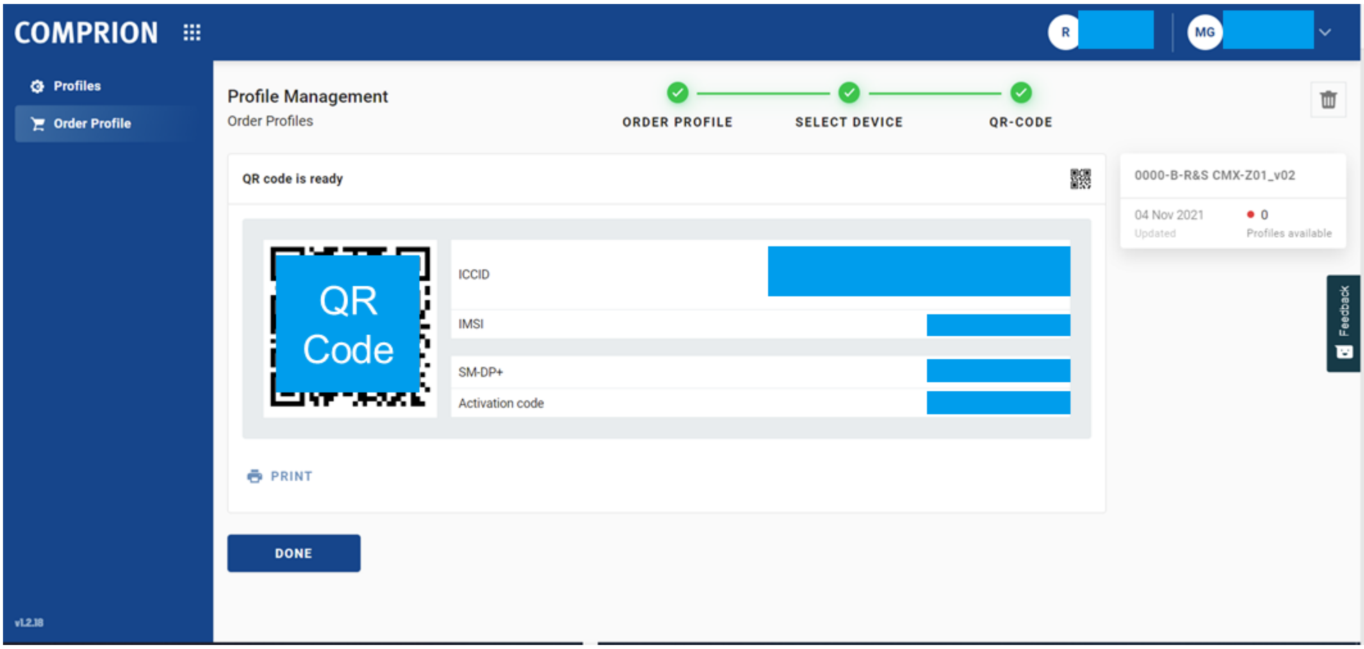
Reserve and ICCID for this profile (optional).
If you do not select one, a random ICCID will be assigned to this device.

ICCID

0000-B-R&S_CMX-Z01_v05
08 Mar 2022 Updated
1 Profiles available

Fig. 5-5 Select other device

3. An QR code is then generated in the end (see Fig. 5-6).



Profile Management
Order Profiles

QR code is ready

ICCID
IMSI
SM-DP+
Activation code

0000-B-R&S CMX-Z01_v02
04 Nov 2021 Updated
0 Profiles available

Fig. 5-6 QR code generation

After the QR code is created through one of the ways shown in the above steps, the user can use eSIM capable consumer device to scan the QR code that will in turn initiate the download process via an Internet connection, e.g. over Wifi or in a live network. If the download is completed successfully, then the eSIM test profile is visible on the device (e.g. for Andriod OS, in menu Settings > SIM card manager > eSIM) and can be installed to use accordingly.

Remarks:

The profile status of an eSIM profile in self-portal is changed along with the operations (download, install, delete) on device.

- Download triggers "Downloaded" profile status
- Install triggers "Installed" profile status

- Delete triggers "Allocated" profile status

Visit https://www.comprion.com/comprion-test-profile-service/how-to-use/4-use-the-service/order-a-test-profile for more details about the usage of eSIM profile service.

In case there are questions of using COMPRION® eSIM Test Profile Service, please refer to FAQ section under https://www.comprion.com/comprion-test-profile-service/faq/.

6 Informative

As described in Chapter 3.1.3, Mobile Terminated SMS (MT-SMS) plays an important role in eUICC provision or management procedure over OTA.

For ease of use, all required SMS settings of CMW are set by ePM via SCPI commands. These configurations are fully integrated in the ePM tool and therefore no additional user intervention is desired on CMW side.

Just for information purpose, the summary of the outgoing SMS settings are listed below in Table 6-1.

Parameter	Setting	Comment
Large SMS Handling	Multiple SMS	Up to five concatenated messages are sent, consisting in sum of up to 800 characters.
Outgoing Message Handling	Use Internal	Use the message text configured via the CMW GUI
Data Coding / Character Set	8 bit	Binary SMS
Protocol Identifier	7F	(U)SIM Data download
Use Data Header	Enabled 7000 hex	Add a header to the TP user data field, (U)SIM toolkit security headers
Coding Group	Data Coding / Mesg. Class	TP Data Coding Scheme specified in 3GPP TS 23.038
Message Class	Class 2	(U)SIM-specific message

Table 6-1: Outgoing SMS settings of CMW remotely controlled by eUICC Profile Manager

7 Literature

[1] GSMA SGP.02 ver 4.0, 25 February 2019, Remote Provisioning Architecture for Embedded UICC Technical Specification

[2] GSMA SGP.22 ver 2.2.2, 05 June 2020, RSP Technical Specification

[3] GlobalPlatform Card, Remote Application Management over HTTP Card Specification v2.2 – Amendment B

[4] ETSI TS 101 220, ETSI numbering system for telecommunication application providers

[5] ETSI TS 102 225, Secured packet structure for UICC based applications

[6] ETSI TS 102 226, Remote APDU structure for UICC based applications

[7] COMPRION eUICC Profile Manager Online Help

Rohde & Schwarz

The Rohde & Schwarz electronics group offers innovative solutions in the following business fields: test and measurement, broadcast and media, secure communications, cybersecurity, monitoring and network testing. Founded more than 80 years ago, the independent company which is headquartered in Munich, Germany, has an extensive sales and service network with locations in more than 70 countries.

www.rohde-schwarz.com

Certified Quality Management
ISO 9001

Rohde & Schwarz training

www.training.rohde-schwarz.com

Rohde & Schwarz customer support

www.rohde-schwarz.com/support

R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG
Trade names are trademarks of the owners.
GFM342 | Version 4e | 02.2023
Application Note | eUICC Provisioning for Consumer and M2M Devices
Data without tolerance limits is not binding | Subject to change

www.rohde-schwarz.com