SIM OTA Provisioning Process for Korea Network

2023.05.17

ByungCheol Jun

www.quectel.com

Contents

1. Description

This documents desctibe OTA process for Korea network operator. There is no specific english document for Korea MNO.

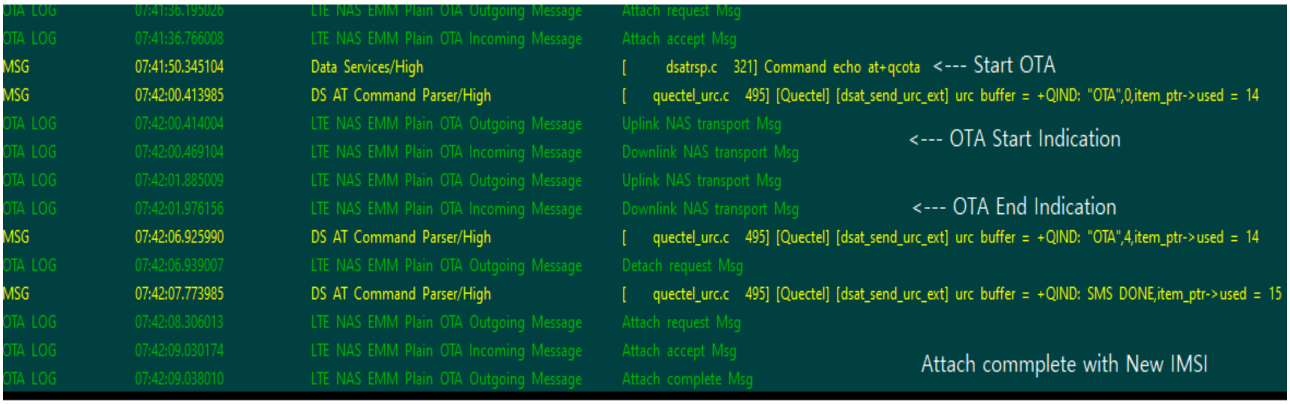
2. Network Operator for KOREA

- SK Telecom
- KT
- LGU+

2.1 OTA Configuration for KR MNOs

	SK Telecom	KT	LGU+
APN	[M2M] 012-XXXX-XXXX lte-Internet.sktelecom.com [Commecial] 010-XXXX-XXXX lte.sktelecom.com IMS	default.ktfwing.com lte.ktfwing.com ims	ota.lguplus.co.kr
Bearer	BIP SMS	BIP SMS	BIP
OTA Trigger	Power up EF_IMSI_P(2F24)	Specific Envelope Command	Specific Envelope Command
	See chapter 3.1	See chapter 4.1	See chapter 5.1
OTA Start	**AT+QCOTA**	**AT+QCOTA**	**AT+QCOTA**
OTA Status URC	**+QIND: "OTA",<result>**	**+QIND: "OTA",<result>**	**+QIND: "OTA",<result>**
	<result> 0 OTA SEND SUCCESS 1 OTA SEND FAIL 4 OTA SUCCESS 9 OTA failed		
Model	**EC25/BG770/BG950/EM06 /AG35/RM500**	**EC25/BG770/BG950/EM06 /AG35/RM500**	**EC25/BG770/BG950/EM06 /AG35/RM500**

AT Command Example



```
OTA LOG   07:41:36.195026   LTE NAS EMM Plain OTA Outgoing Message   Attach request Msg
OTA LOG   07:41:36.766008   LTE NAS EMM Plain OTA Incoming Message   Attach accept Msg
MSG       07:41:50.345104   Data Services/High                       [    dsatrsp.c   321] Command echo at+qcota  <--- Start OTA
MSG       07:42:00.413985   DS AT Command Parser/High                [   quectel_urc.c   495] [Quectel] [dsat_send_urc_ext] urc buffer = +QIND: "OTA",0,item_ptr->used = 14
OTA LOG   07:42:00.414004   LTE NAS EMM Plain OTA Outgoing Message   Uplink NAS transport Msg
                                                                                                <--- OTA Start Indication
OTA LOG   07:42:00.469104   LTE NAS EMM Plain OTA Incoming Message   Downlink NAS transport Msg
OTA LOG   07:42:01.885009   LTE NAS EMM Plain OTA Outgoing Message   Uplink NAS transport Msg
OTA LOG   07:42:01.976156   LTE NAS EMM Plain OTA Incoming Message   Downlink NAS transport Msg     <--- OTA End Indication
MSG       07:42:06.925990   DS AT Command Parser/High                [   quectel_urc.c   495] [Quectel] [dsat_send_urc_ext] urc buffer = +QIND: "OTA",4,item_ptr->used = 14
OTA LOG   07:42:06.939007   LTE NAS EMM Plain OTA Outgoing Message   Detach request Msg
MSG       07:42:07.773985   DS AT Command Parser/High                [   quectel_urc.c   495] [Quectel] [dsat_send_urc_ext] urc buffer = +QIND: SMS DONE,item_ptr->used = 15
OTA LOG   07:42:08.306013   LTE NAS EMM Plain OTA Outgoing Message   Attach request Msg
OTA LOG   07:42:09.030174   LTE NAS EMM Plain OTA Incoming Message   Attach accept Msg
                                                                                                Attach commplete with New IMSI
OTA LOG   07:42:09.038010   LTE NAS EMM Plain OTA Outgoing Message   Attach complete Msg
```

2.2 Global OTA provision process

The device shall support proactive commands from UICC.
See details for ETSI 102.223 and 3GPP TS 31.111

Proactive Command to support BIP operation.

- Profile Download
- SMS-PP Data Download
- Command Result
- Proactive UICC: Refresh
- Proactive UICC: Send Short Message
- Proactive UICC: Set Up Event List
- Event: Data Available
- Proactive UICC: Open Channel
- Proactive UICC: Close Channel
- Proactive UICC: Send Data
- Proactive UICC: Receive Data

The Korea Network Provider like SKTelecom, KT and LGU+ follows global standard for BIP.
But they have some specific rules for the their network.
The description describe for their own rules for SIM provisioning.
Also they KR MNOs does not provide English Requirement Documents.

3. SKTelecom OTA requirements

OTA (Over The Air Administration) is an interaction between the terminal and UICC for changing subscriber information contained in UICC (File management) and downloading applications (Application management).

OTA implementation in WCDMA/LTE mode: It is implemented according to the standards of 3GPP TS23.048 and TS 31.111. Terminals and USIMs supporting Bearer Independent Protocol must comply with GP v2.2 Amendment B v1.1, ETSI 102.226/102.223, RFC 2616/2246/4279/3546 standards for BIP USAT command and HTTPS protocol. The terminal and USIM must support the HTTPS protocol, and TLS (v1.0 or higher) for security is essential.
should support for the opening process. It should be able to proceed with the internal initialization operation so that the parameter can be applied to the NV of the terminal.
The device should be supported BIP provisioning as follows.

3.1 SKT OTA provision process

UICC card manufacturers must initialize and deliver ADF USIM/EF IMSI_P (IMSI for Personalization: 2F24) to the temporary number value stored in our COIS system for OTA Activation provisioning function. Upon opening, the company activates the SMS connection using the temporary number in IMSI_P and opens the real number for IMSI. ** For detailed USIM card structure, refer to our UICC Profile.

Device Requirements for OTA

Terminal requirements to support OTA opening.

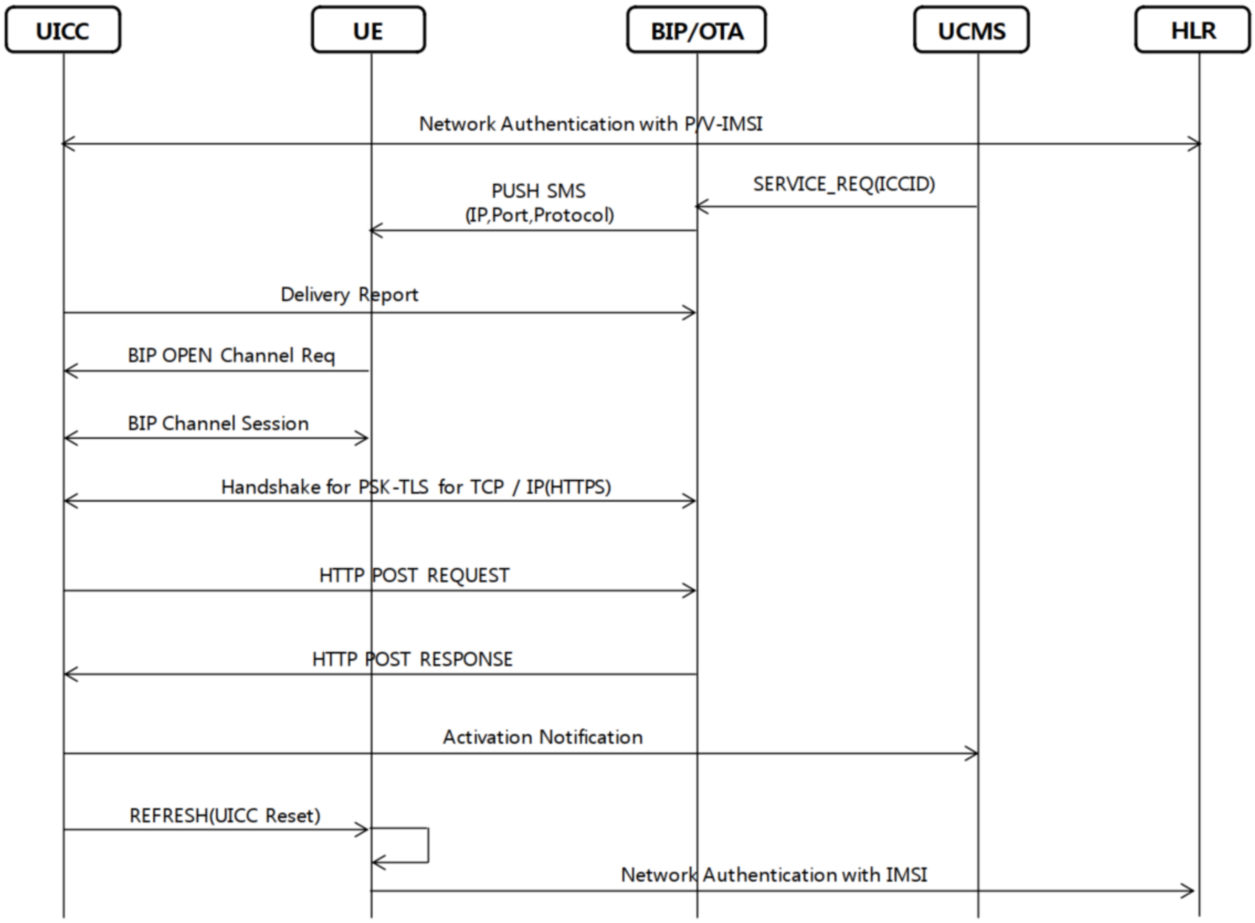
The terminal must have a normal mode and an provisioning mode.

The initially released terminal maintains the normal mode, and for the activated USIM card, normal call processing should be possible using IMSI in WCDMA/GSM mode. The terminal enters the provisioning mode by pressing #SKTELECOM#MIN# under any circumstances as long as the card is inserted.

When entering the provisioning mode, in WCDMA/GSM mode, the temporary number IMSI_P is used to register in the network, and the minimum call processing registered in the HLR such as SMS transmission and reception must be possible.

When the terminal transmits a Refresh Proactive Command (UICC Reset) using the USIM Application Toolkit (USAT) Framework from the USIM card, it should respond normally and initialize the terminal (warm reset).

After entering the opening mode with #SKTELECOM#MIN#, the terminal can be switched to the normal mode only when the opening OTA process operates normally and receives Refresh Proactive (Refresh Proactive Command (UICC Reset) or power off/on and battery removal).

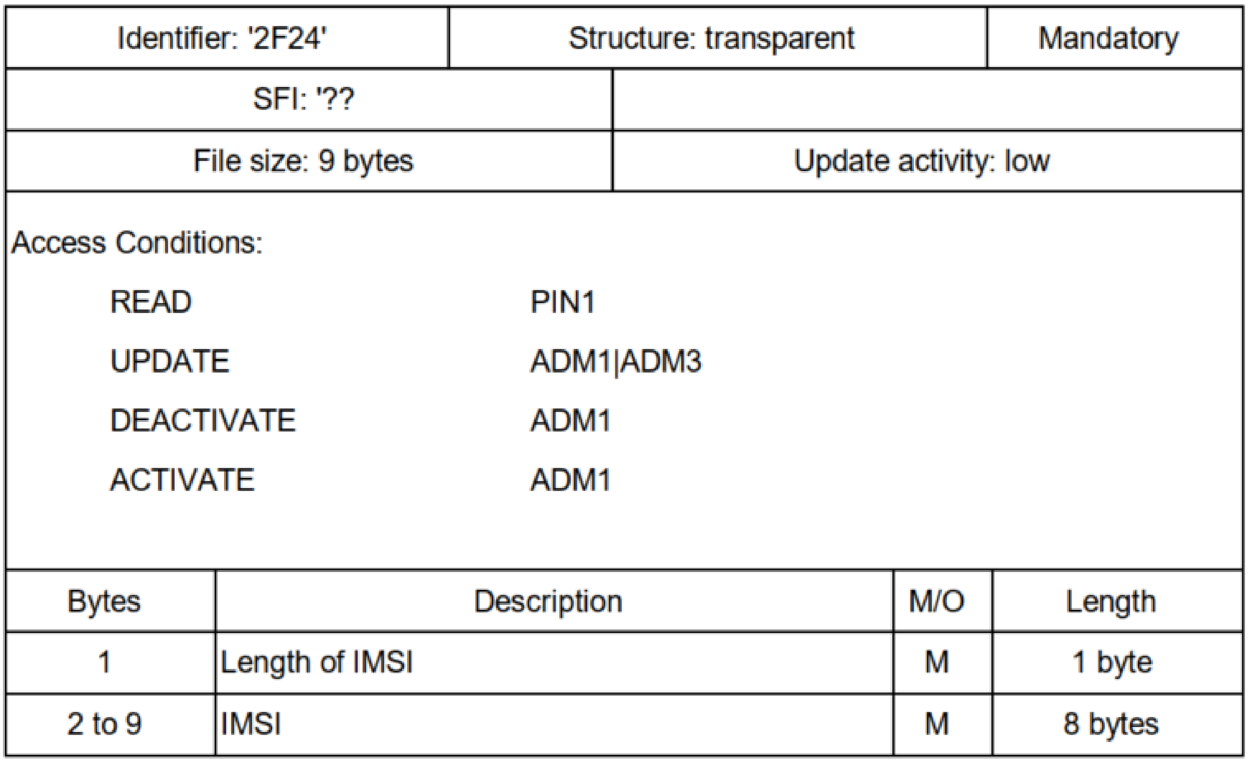


OTA test procedure.

1) Power on Device

2) Swith Temporary IMSI and Registered with Temporary IMSI(EF_IMSI_P: see below table)

   a. Register with PS+CS Mode.



Identifier: '2F24'	Structure: transparent	Mandatory
SFI: '??		
File size: 9 bytes	Update activity: low	

Access Conditions:

READ	PIN1
UPDATE	ADM1|ADM3
DEACTIVATE	ADM1
ACTIVATE	ADM1

Bytes	Description	M/O	Length
1	Length of IMSI	M	1 byte
2 to 9	IMSI	M	8 bytes

Test Command to Read EF_IMSI_P

```
AT+CSIM=14,"00A40004023F00"
+CSIM: 4,"6131"
OK

AT+CSIM=14,"00A40004027FFF"
+CSIM: 4,"613C"
OK

AT+CSIM=14,"00A40004022F24"
+CSIM: 4,"611D"
OK
Read IMSI_P
AT+CSIM=10,"00B0000000"
+CSIM: 22,"08490550 79598918859000"    //450059795988158
OK
AT+CSIM=14,"00A40004026F07"
+CSIM: 4,"611E"
OK
Read IMSI
AT+CSIM=10,"00B0000000"
+CSIM: 22,"08490550 21840786879000"    // 4500512487688678
OK
```

3) Device will try to register with PS mode. (See Figure 3)

    a. must be received Reject code as 7 or 14.

4) Device will try to register with CS mode. (See Figure 3)

    a. Location update will be completed.

5) OTA Data will be received from network.

6) After complete OTA, SIM Refresh is triggered from SIM proactive command.

7) Warm Reset form SIM

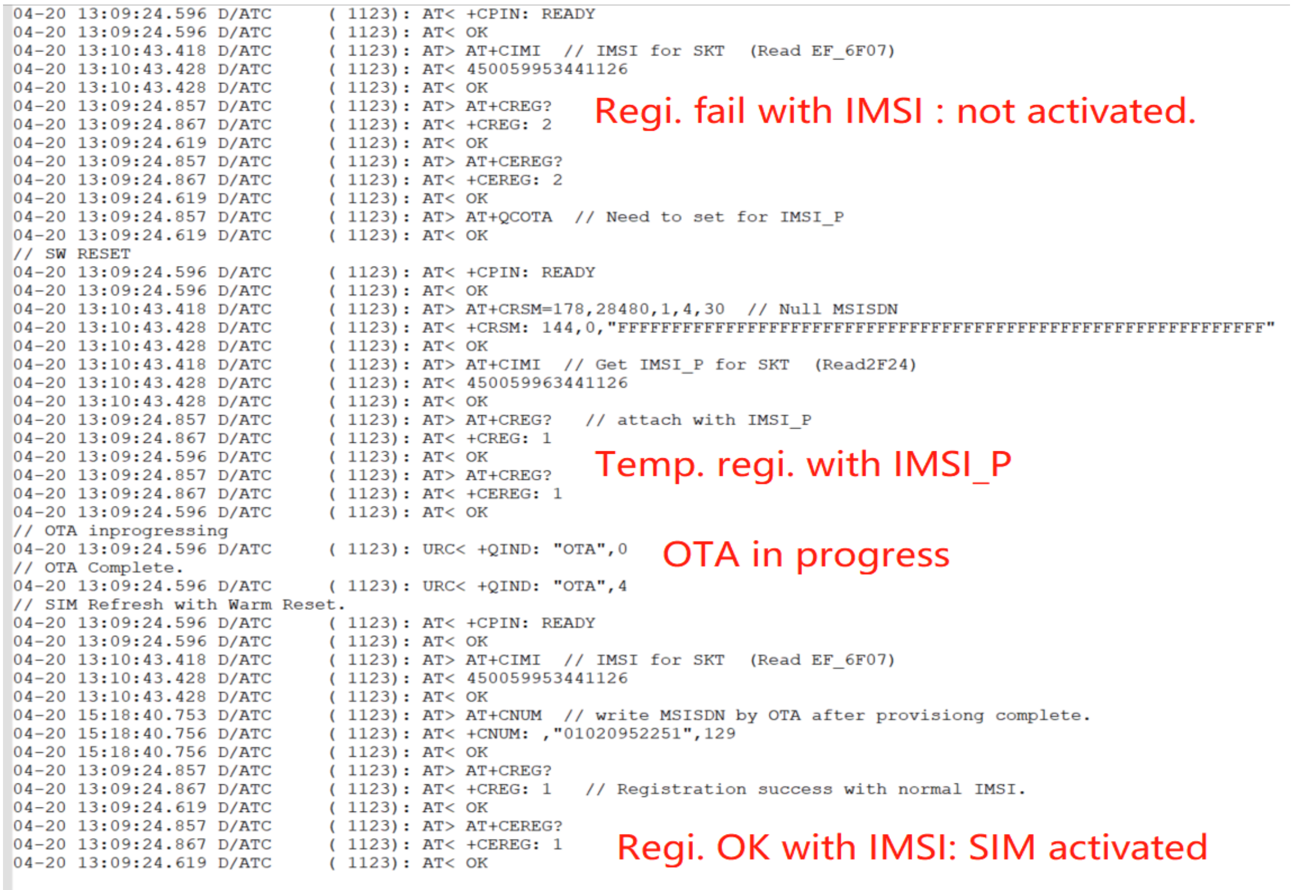
8) Modem will be registered with IMSI(EF_6F07). (See Figure4)

3.2 AT command and Log analysis.

STEP1. AT+QCOTA

Restart with IMSI_P(7FFF/2F04) instead of IMSI(7FFF/6F07)

Figure 1. OTA process with AT command Set



```
04-20 13:09:24.596 D/ATC      ( 1123): AT< +CPIN: READY
04-20 13:09:24.596 D/ATC      ( 1123): AT< OK
04-20 13:10:43.418 D/ATC      ( 1123): AT> AT+CIMI  // IMSI for SKT  (Read EF_6F07)
04-20 13:10:43.428 D/ATC      ( 1123): AT< 450059953441126
04-20 13:10:43.428 D/ATC      ( 1123): AT< OK
04-20 13:09:24.857 D/ATC      ( 1123): AT> AT+CREG?
04-20 13:09:24.867 D/ATC      ( 1123): AT< +CREG: 2
04-20 13:09:24.619 D/ATC      ( 1123): AT< OK
04-20 13:09:24.857 D/ATC      ( 1123): AT> AT+CEREG?
04-20 13:09:24.867 D/ATC      ( 1123): AT< +CEREG: 2
04-20 13:09:24.619 D/ATC      ( 1123): AT< OK
04-20 13:09:24.857 D/ATC      ( 1123): AT> AT+QCOTA  // Need to set for IMSI_P
04-20 13:09:24.619 D/ATC      ( 1123): AT< OK
// SW RESET
04-20 13:09:24.596 D/ATC      ( 1123): AT< +CPIN: READY
04-20 13:09:24.596 D/ATC      ( 1123): AT< OK
04-20 13:10:43.418 D/ATC      ( 1123): AT> AT+CRSM=178,28480,1,4,30  // Null MSISDN
04-20 13:10:43.428 D/ATC      ( 1123): AT< +CRSM: 144,0,"FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"
04-20 13:10:43.428 D/ATC      ( 1123): AT< OK
04-20 13:10:43.418 D/ATC      ( 1123): AT> AT+CIMI  // Get IMSI_P for SKT  (Read2F24)
04-20 13:10:43.428 D/ATC      ( 1123): AT< 450059963441126
04-20 13:10:43.428 D/ATC      ( 1123): AT< OK
04-20 13:09:24.857 D/ATC      ( 1123): AT> AT+CREG?   // attach with IMSI_P
04-20 13:09:24.867 D/ATC      ( 1123): AT< +CREG: 1
04-20 13:09:24.596 D/ATC      ( 1123): AT< OK
04-20 13:09:24.857 D/ATC      ( 1123): AT> AT+CREG?
04-20 13:09:24.867 D/ATC      ( 1123): AT< +CEREG: 1
04-20 13:09:24.596 D/ATC      ( 1123): AT< OK
// OTA inprogressing
04-20 13:09:24.596 D/ATC      ( 1123): URC< +QIND: "OTA",0
// OTA Complete.
04-20 13:09:24.596 D/ATC      ( 1123): URC< +QIND: "OTA",4
// SIM Refresh with Warm Reset.
04-20 13:09:24.596 D/ATC      ( 1123): AT< +CPIN: READY
04-20 13:09:24.596 D/ATC      ( 1123): AT< OK
04-20 13:10:43.418 D/ATC      ( 1123): AT> AT+CIMI  // IMSI for SKT  (Read EF_6F07)
04-20 13:10:43.428 D/ATC      ( 1123): AT< 450059953441126
04-20 13:10:43.428 D/ATC      ( 1123): AT< OK
04-20 15:18:40.753 D/ATC      ( 1123): AT> AT+CNUM  // write MSISDN by OTA after provisiong complete.
04-20 15:18:40.756 D/ATC      ( 1123): AT< +CNUM: ,"01020952251",129
04-20 15:18:40.756 D/ATC      ( 1123): AT< OK
04-20 13:09:24.857 D/ATC      ( 1123): AT> AT+CREG?
04-20 13:09:24.867 D/ATC      ( 1123): AT< +CREG: 1   // Registration success with normal IMSI.
04-20 13:09:24.619 D/ATC      ( 1123): AT< OK
04-20 13:09:24.857 D/ATC      ( 1123): AT> AT+CEREG?
04-20 13:09:24.867 D/ATC      ( 1123): AT< +CEREG: 1
04-20 13:09:24.619 D/ATC      ( 1123): AT< OK
```

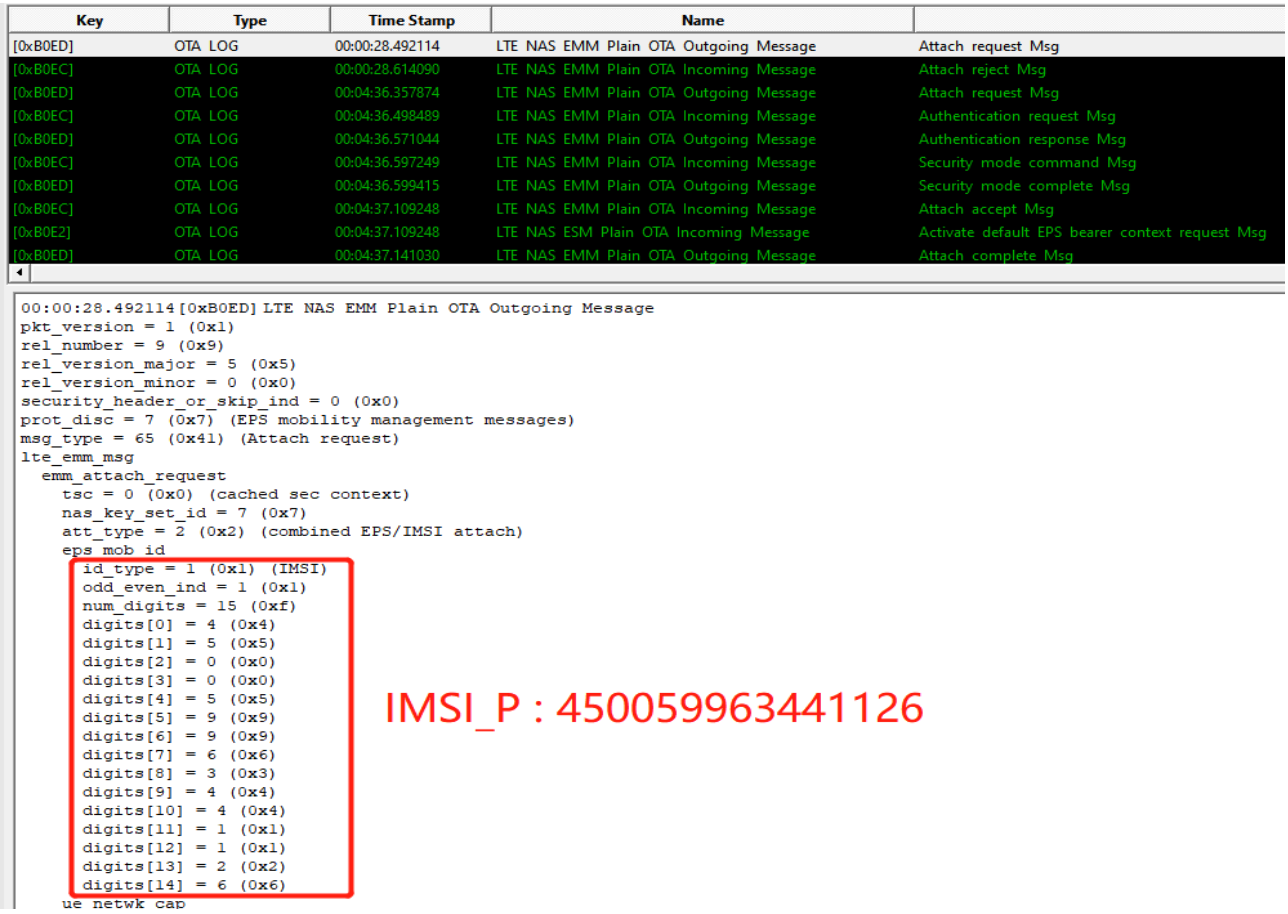
Regi. fail with IMSI : not activated.

Temp. regi. with IMSI_P

OTA in progress

Regi. OK with IMSI: SIM activated

STEP 2. Register to Network with IMSI_P

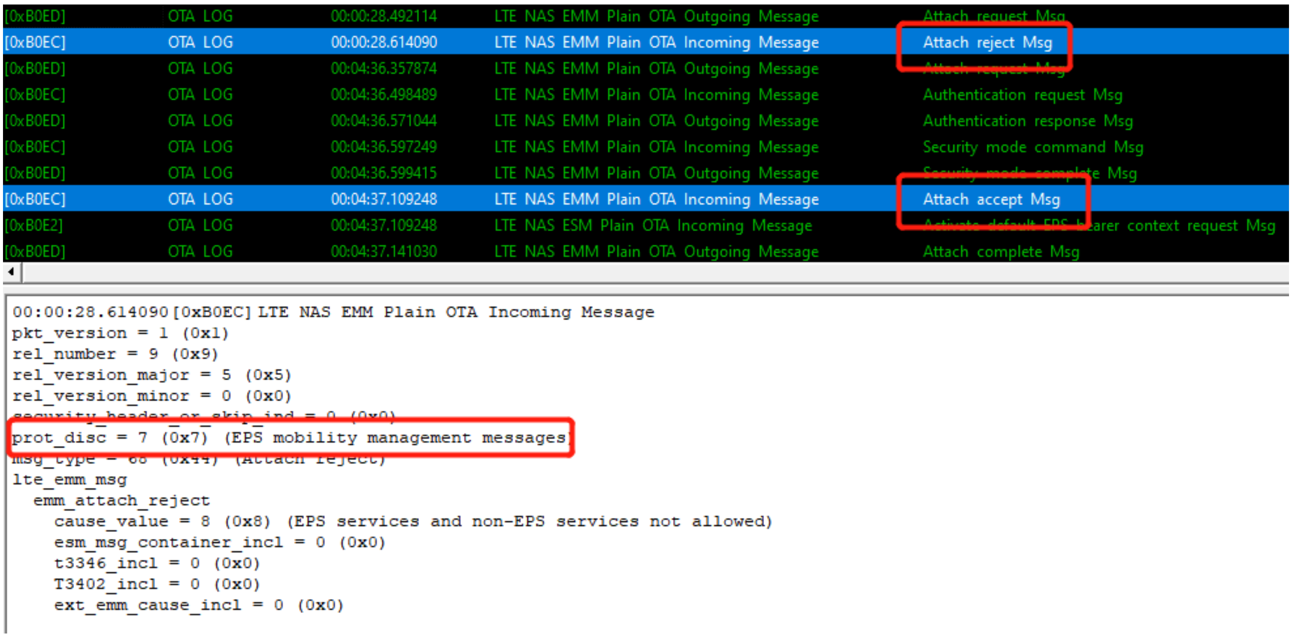


Key	Type	Time Stamp	Name	
[0xB0ED]	OTA LOG	00:00:28.492114	LTE NAS EMM Plain OTA Outgoing Message	Attach request Msg
[0xB0EC]	OTA LOG	00:00:28.614090	LTE NAS EMM Plain OTA Incoming Message	Attach reject Msg
[0xB0ED]	OTA LOG	00:04:36.357874	LTE NAS EMM Plain OTA Outgoing Message	Attach request Msg
[0xB0EC]	OTA LOG	00:04:36.498489	LTE NAS EMM Plain OTA Incoming Message	Authentication request Msg
[0xB0ED]	OTA LOG	00:04:36.571044	LTE NAS EMM Plain OTA Outgoing Message	Authentication response Msg
[0xB0EC]	OTA LOG	00:04:36.597249	LTE NAS EMM Plain OTA Incoming Message	Security mode command Msg
[0xB0ED]	OTA LOG	00:04:36.599415	LTE NAS EMM Plain OTA Outgoing Message	Security mode complete Msg
[0xB0EC]	OTA LOG	00:04:37.109248	LTE NAS EMM Plain OTA Incoming Message	Attach accept Msg
[0xB0E2]	OTA LOG	00:04:37.109248	LTE NAS ESM Plain OTA Incoming Message	Activate default EPS bearer context request Msg
[0xB0ED]	OTA LOG	00:04:37.141030	LTE NAS EMM Plain OTA Outgoing Message	Attach complete Msg

```
00:00:28.492114 [0xB0ED] LTE NAS EMM Plain OTA Outgoing Message
pkt_version = 1 (0x1)
rel_number = 9 (0x9)
rel_version_major = 5 (0x5)
rel_version_minor = 0 (0x0)
security_header_or_skip_ind = 0 (0x0)
prot_disc = 7 (0x7) (EPS mobility management messages)
msg_type = 65 (0x41) (Attach request)
lte_emm_msg
  emm_attach_request
    tsc = 0 (0x0) (cached sec context)
    nas_key_set_id = 7 (0x7)
    att_type = 2 (0x2) (combined EPS/IMSI attach)
    eps_mob_id
      id_type = 1 (0x1) (IMSI)
      odd_even_ind = 1 (0x1)
      num_digits = 15 (0xf)
      digits[0] = 4 (0x4)
      digits[1] = 5 (0x5)
      digits[2] = 0 (0x0)
      digits[3] = 0 (0x0)
      digits[4] = 5 (0x5)
      digits[5] = 9 (0x9)
      digits[6] = 9 (0x9)
      digits[7] = 6 (0x6)
      digits[8] = 3 (0x3)
      digits[9] = 4 (0x4)
      digits[10] = 4 (0x4)
      digits[11] = 1 (0x1)
      digits[12] = 1 (0x1)
      digits[13] = 2 (0x2)
      digits[14] = 6 (0x6)
    ue_netwk_cap
```

IMSI_P : 450059963441126

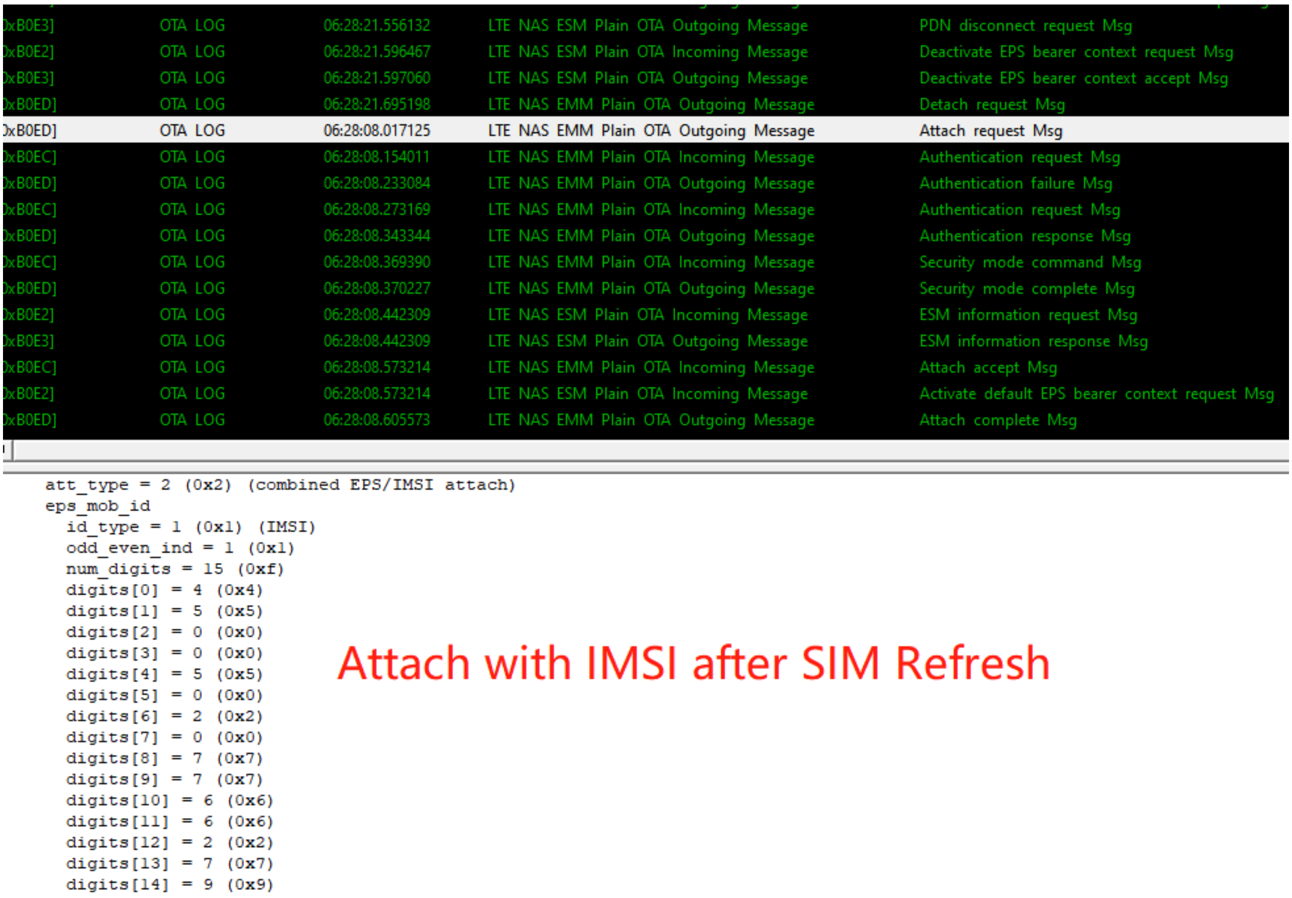
STEP 3. PS fail and CS attach success.



[0xB0ED]	OTA LOG	00:00:28.492114	LTE NAS EMM Plain OTA Outgoing Message	Attach request Msg
[0xB0EC]	OTA LOG	00:00:28.614090	LTE NAS EMM Plain OTA Incoming Message	Attach reject Msg
[0xB0ED]	OTA LOG	00:04:36.357874	LTE NAS EMM Plain OTA Outgoing Message	Attach request Msg
[0xB0EC]	OTA LOG	00:04:36.498489	LTE NAS EMM Plain OTA Incoming Message	Authentication request Msg
[0xB0ED]	OTA LOG	00:04:36.571044	LTE NAS EMM Plain OTA Outgoing Message	Authentication response Msg
[0xB0EC]	OTA LOG	00:04:36.597249	LTE NAS EMM Plain OTA Incoming Message	Security mode command Msg
[0xB0ED]	OTA LOG	00:04:36.599415	LTE NAS EMM Plain OTA Outgoing Message	Security mode complete Msg
[0xB0EC]	OTA LOG	00:04:37.109248	LTE NAS EMM Plain OTA Incoming Message	Attach accept Msg
[0xB0E2]	OTA LOG	00:04:37.109248	LTE NAS ESM Plain OTA Incoming Message	Activate default EPS bearer context request Msg
[0xB0ED]	OTA LOG	00:04:37.141030	LTE NAS EMM Plain OTA Outgoing Message	Attach complete Msg

```
00:00:28.614090 [0xB0EC] LTE NAS EMM Plain OTA Incoming Message
pkt_version = 1 (0x1)
rel_number = 9 (0x9)
rel_version_major = 5 (0x5)
rel_version_minor = 0 (0x0)
security_header_or_skip_ind = 0 (0x0)
prot_disc = 7 (0x7) (EPS mobility management messages)
msg_type = 68 (0x44) (Attach reject)
lte_emm_msg
  emm_attach_reject
    cause_value = 8 (0x8) (EPS services and non-EPS services not allowed)
    esm_msg_container_incl = 0 (0x0)
    t3346_incl = 0 (0x0)
    T3402_incl = 0 (0x0)
    ext_emm_cause_incl = 0 (0x0)
```

STEP 4. OTA complete after SIM Refresh



```
xB0E3]   OTA LOG   06:28:21.556132   LTE NAS ESM Plain OTA Outgoing Message   PDN disconnect request Msg
xB0E2]   OTA LOG   06:28:21.596467   LTE NAS ESM Plain OTA Incoming Message   Deactivate EPS bearer context request Msg
xB0E3]   OTA LOG   06:28:21.597060   LTE NAS ESM Plain OTA Outgoing Message   Deactivate EPS bearer context accept Msg
xB0ED]   OTA LOG   06:28:21.695198   LTE NAS EMM Plain OTA Outgoing Message   Detach request Msg
)xB0ED]  OTA LOG   06:28:08.017125   LTE NAS EMM Plain OTA Outgoing Message   Attach request Msg
xB0EC]   OTA LOG   06:28:08.154011   LTE NAS EMM Plain OTA Incoming Message   Authentication request Msg
xB0ED]   OTA LOG   06:28:08.233084   LTE NAS EMM Plain OTA Outgoing Message   Authentication failure Msg
xB0EC]   OTA LOG   06:28:08.273169   LTE NAS EMM Plain OTA Incoming Message   Authentication request Msg
xB0ED]   OTA LOG   06:28:08.343344   LTE NAS EMM Plain OTA Outgoing Message   Authentication response Msg
xB0EC]   OTA LOG   06:28:08.369390   LTE NAS EMM Plain OTA Incoming Message   Security mode command Msg
xB0ED]   OTA LOG   06:28:08.370227   LTE NAS EMM Plain OTA Outgoing Message   Security mode complete Msg
xB0E2]   OTA LOG   06:28:08.442309   LTE NAS ESM Plain OTA Incoming Message   ESM information request Msg
xB0E3]   OTA LOG   06:28:08.442309   LTE NAS ESM Plain OTA Outgoing Message   ESM information response Msg
xB0EC]   OTA LOG   06:28:08.573214   LTE NAS EMM Plain OTA Incoming Message   Attach accept Msg
xB0E2]   OTA LOG   06:28:08.573214   LTE NAS ESM Plain OTA Incoming Message   Activate default EPS bearer context request Msg
xB0ED]   OTA LOG   06:28:08.605573   LTE NAS EMM Plain OTA Outgoing Message   Attach complete Msg
```

```
att_type = 2 (0x2) (combined EPS/IMSI attach)
eps_mob_id
  id_type = 1 (0x1) (IMSI)
  odd_even_ind = 1 (0x1)
  num_digits = 15 (0xf)
  digits[0] = 4 (0x4)
  digits[1] = 5 (0x5)
  digits[2] = 0 (0x0)
  digits[3] = 0 (0x0)
  digits[4] = 5 (0x5)
  digits[5] = 0 (0x0)
  digits[6] = 2 (0x2)
  digits[7] = 0 (0x0)
  digits[8] = 7 (0x7)
  digits[9] = 7 (0x7)
  digits[10] = 6 (0x6)
  digits[11] = 6 (0x6)
  digits[12] = 2 (0x2)
  digits[13] = 7 (0x7)
  digits[14] = 9 (0x9)
```

Attach with IMSI after SIM Refresh

4. LGU+ OTA requirements

LGU+ follows global OTA process

Conditions

A) Attach type = ‘combined EPS/IMSI attach’

B) PDN type = ‘IPv4v6’

C) UE’s usage setting = ‘voice centric’

D) Voice domain preference = ‘IMS PS voice preferred, CS voice as secondary’

E) ESM information transfer flag = ‘0’ (APN = null)

4.1 LGU+ OTA provision process

[First Provisioning Command]

Start BIP APDU command with ENVELOPE(SMS-PP DOWNLOAD) Msg.

```
80 C2 00 00 36 D1 34 02 02 83 81 06 06 98 33 11 11 11 11 0B 26 E4 0A 98 33 11 11
11 11 7F 16 0C 01 09 15 57 32 36 14 02 70 00 00 0F 0D 00 01 20 20 B0 00 06 00 00
00 00 00 00 02
```

[Reactivation Command]

Start BIP APDU command with ENVELOPE(SMS-PP DOWNLOAD) Msg.

```
80 C2 00 00 36 D1 34 02 02 83 81 06 06 98 33 11 11 11 11 0B 26 E4 0A 98 33 11
11 11 11 7F 16 0C 01 09 15 57 32 36 14 02 70 00 00 0F 0D 00 01 20 20 B0 00 06
00 00 00 00 00 00 05
```

If MSIN starts with 9 on the IMSI values read from UICC at boot time, it is judged as psudo IMSI and LTE attach and PDN connection should be attempted with OTA APN to open BIP. OTA APN is “ota.lguplus.co.kr”. (referred to as OTA PDN) Multiple PDN terminals must also open only one PDN as an OTA APN.

Example MSIN(Not actvated USIM)

MCC	450	KOREA
MNC	06	LGU+
MSIN	987654321	

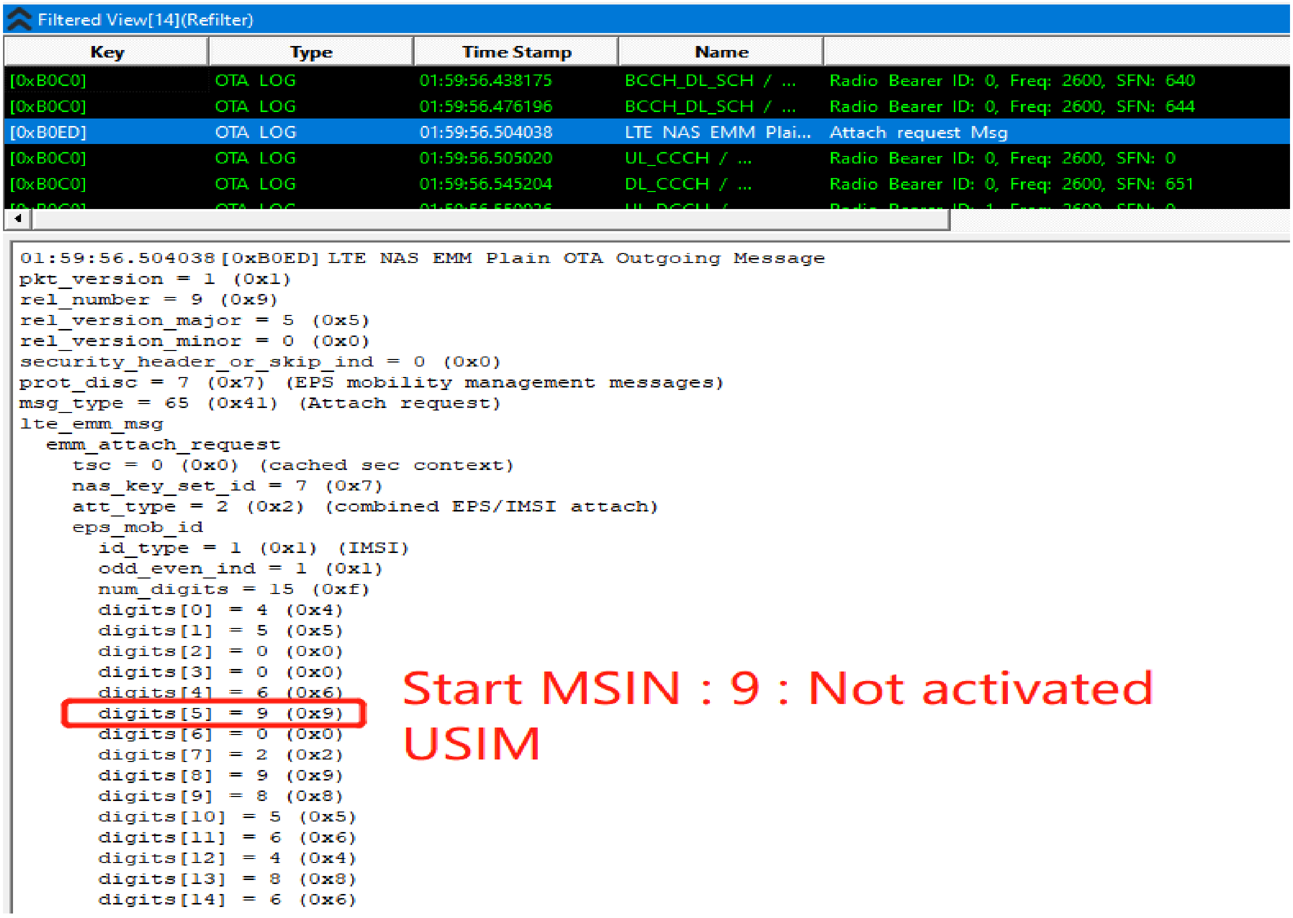
4.2 AT command and Log analysis

STEP 1. AT+QCOTA

START OTA with USIM Envelope command.(First Provisioning)

AT+CSIM=118,"80C2000036D1340202838106069833111111110B26E40A9833111111117F160C010915 57323614027000000F0D00012020B00006000000000000002"

STEP 2. Attach with psudo IMSI.(450069029856486)



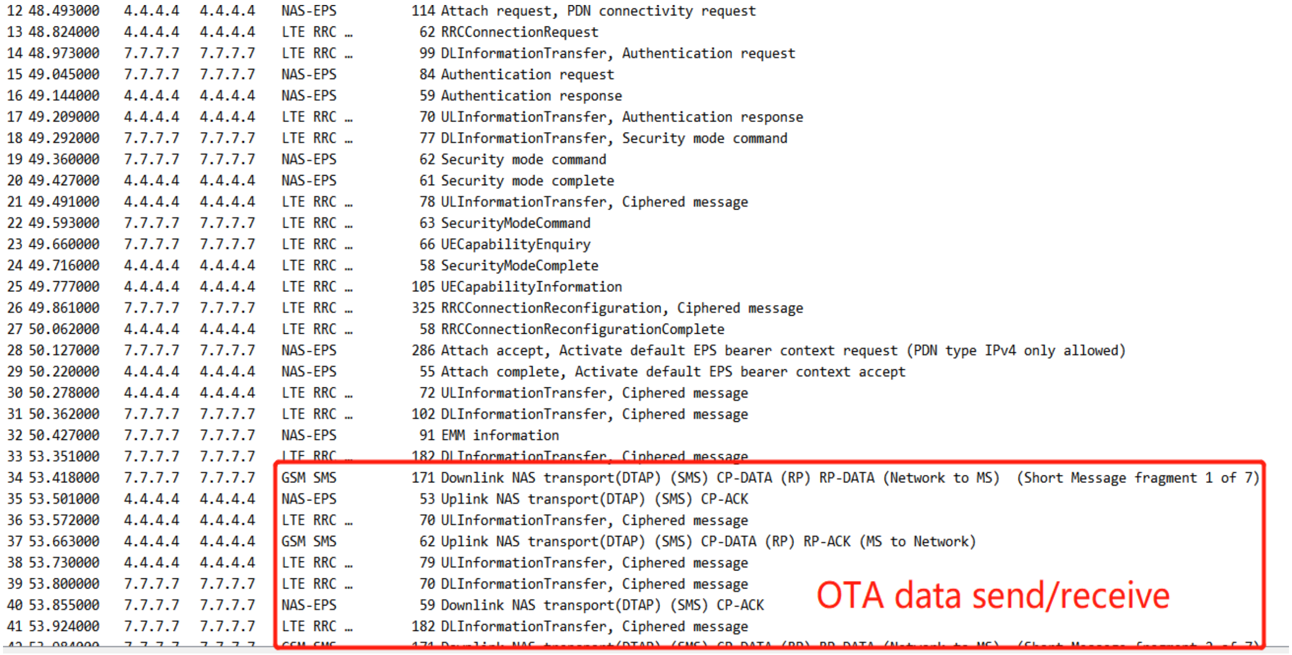
Filtered View[14](Refilter)

Key	Type	Time Stamp	Name	
[0xB0C0]	OTA LOG	01:59:56.438175	BCCH_DL_SCH / ...	Radio Bearer ID: 0, Freq: 2600, SFN: 640
[0xB0C0]	OTA LOG	01:59:56.476196	BCCH_DL_SCH / ...	Radio Bearer ID: 0, Freq: 2600, SFN: 644
[0xB0ED]	OTA LOG	01:59:56.504038	LTE NAS EMM Plai...	Attach request Msg
[0xB0C0]	OTA LOG	01:59:56.505020	UL_CCCH / ...	Radio Bearer ID: 0, Freq: 2600, SFN: 0
[0xB0C0]	OTA LOG	01:59:56.545204	DL_CCCH / ...	Radio Bearer ID: 0, Freq: 2600, SFN: 651

```
01:59:56.504038 [0xB0ED] LTE NAS EMM Plain OTA Outgoing Message
pkt_version = 1 (0x1)
rel_number = 9 (0x9)
rel_version_major = 5 (0x5)
rel_version_minor = 0 (0x0)
security_header_or_skip_ind = 0 (0x0)
prot_disc = 7 (0x7) (EPS mobility management messages)
msg_type = 65 (0x41) (Attach request)
lte_emm_msg
  emm_attach_request
    tsc = 0 (0x0) (cached sec context)
    nas_key_set_id = 7 (0x7)
    att_type = 2 (0x2) (combined EPS/IMSI attach)
    eps_mob_id
      id_type = 1 (0x1) (IMSI)
      odd_even_ind = 1 (0x1)
      num_digits = 15 (0xf)
      digits[0] = 4 (0x4)
      digits[1] = 5 (0x5)
      digits[2] = 0 (0x0)
      digits[3] = 0 (0x0)
      digits[4] = 6 (0x6)
      digits[5] = 9 (0x9)
      digits[6] = 0 (0x0)
      digits[7] = 2 (0x2)
      digits[8] = 9 (0x9)
      digits[9] = 8 (0x8)
      digits[10] = 5 (0x5)
      digits[11] = 6 (0x6)
      digits[12] = 4 (0x4)
      digits[13] = 8 (0x8)
      digits[14] = 6 (0x6)
```

Start MSIN : 9 : Not activated USIM

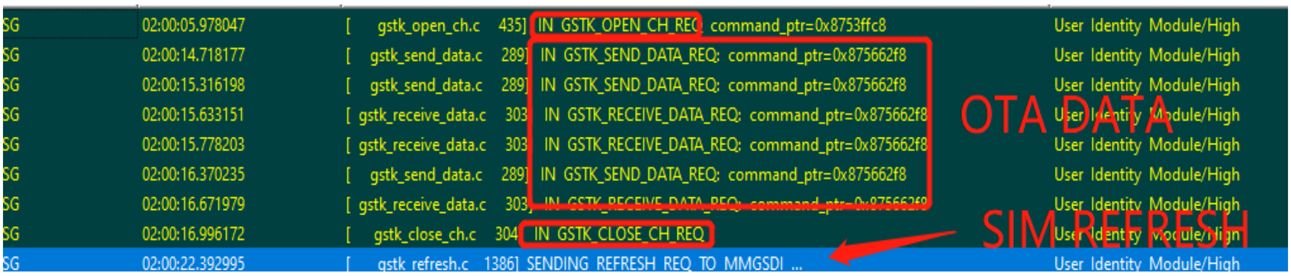
STEP3. OTA is in inprogress afeter envelope command.



```
12 48.493000   4.4.4.4  4.4.4.4   NAS-EPS        114 Attach request, PDN connectivity request
13 48.824000   4.4.4.4  4.4.4.4   LTE RRC …       62 RRCConnectionRequest
14 48.973000   7.7.7.7  7.7.7.7   LTE RRC …       99 DLInformationTransfer, Authentication request
15 49.045000   7.7.7.7  7.7.7.7   NAS-EPS         84 Authentication request
16 49.144000   4.4.4.4  4.4.4.4   NAS-EPS         59 Authentication response
17 49.209000   4.4.4.4  4.4.4.4   LTE RRC …       70 ULInformationTransfer, Authentication response
18 49.292000   7.7.7.7  7.7.7.7   LTE RRC …       77 DLInformationTransfer, Security mode command
19 49.360000   7.7.7.7  7.7.7.7   NAS-EPS         62 Security mode command
20 49.427000   4.4.4.4  4.4.4.4   NAS-EPS         61 Security mode complete
21 49.491000   4.4.4.4  4.4.4.4   LTE RRC …       78 ULInformationTransfer, Ciphered message
22 49.593000   7.7.7.7  7.7.7.7   LTE RRC …       63 SecurityModeCommand
23 49.660000   7.7.7.7  7.7.7.7   LTE RRC …       66 UECapabilityEnquiry
24 49.716000   4.4.4.4  4.4.4.4   LTE RRC …       58 SecurityModeComplete
25 49.777000   4.4.4.4  4.4.4.4   LTE RRC …      105 UECapabilityInformation
26 49.861000   7.7.7.7  7.7.7.7   LTE RRC …      325 RRCConnectionReconfiguration, Ciphered message
27 50.062000   4.4.4.4  4.4.4.4   LTE RRC …       58 RRCConnectionReconfigurationComplete
28 50.127000   7.7.7.7  7.7.7.7   NAS-EPS        286 Attach accept, Activate default EPS bearer context request (PDN type IPv4 only allowed)
29 50.220000   4.4.4.4  4.4.4.4   NAS-EPS         55 Attach complete, Activate default EPS bearer context accept
30 50.278000   4.4.4.4  4.4.4.4   LTE RRC …       72 ULInformationTransfer, Ciphered message
31 50.362000   7.7.7.7  7.7.7.7   LTE RRC …      102 DLInformationTransfer, Ciphered message
32 50.427000   7.7.7.7  7.7.7.7   NAS-EPS         91 EMM information
33 53.351000   7.7.7.7  7.7.7.7   LTE RRC …      182 DLInformationTransfer, Ciphered message
34 53.418000   7.7.7.7  7.7.7.7   GSM SMS        171 Downlink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)  (Short Message fragment 1 of 7)
35 53.501000   4.4.4.4  4.4.4.4   NAS-EPS         53 Uplink NAS transport(DTAP) (SMS) CP-ACK
36 53.572000   4.4.4.4  4.4.4.4   LTE RRC …       70 ULInformationTransfer, Ciphered message
37 53.663000   4.4.4.4  4.4.4.4   GSM SMS         62 Uplink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-ACK (MS to Network)
38 53.730000   4.4.4.4  4.4.4.4   LTE RRC …       79 ULInformationTransfer, Ciphered message
39 53.800000   7.7.7.7  7.7.7.7   LTE RRC …       70 DLInformationTransfer, Ciphered message
40 53.855000   7.7.7.7  7.7.7.7   NAS-EPS         59 Downlink NAS transport(DTAP) (SMS) CP-ACK
41 53.924000   7.7.7.7  7.7.7.7   LTE RRC …      182 DLInformationTransfer, Ciphered message
42 53.984000   7.7.7.7  7.7.7.7   GSM SMS        171 Downlink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)  (Short Message fragment 2 of 7)
```

STEP 4. Check OTA complete with Proactive log analys for OTA

1. Open channel
2. Send/Receive Data
3. Close Channel
4. SIM Refresh.: OTA Done…



```
SG   02:00:05.978047   [    gstk_open_ch.c    435]  IN GSTK_OPEN_CH_REQ  command_ptr=0x8753ffc8           User Identity Module/High
SG   02:00:14.718177   [   gstk_send_data.c   289]  IN GSTK_SEND_DATA_REQ: command_ptr=0x875662f8        User Identity Module/High
SG   02:00:15.316198   [   gstk_send_data.c   289]  IN GSTK_SEND_DATA_REQ: command_ptr=0x875662f8        User Identity Module/High
SG   02:00:15.633151   [ gstk_receive_data.c  303   IN GSTK_RECEIVE_DATA_REQ: command_ptr=0x875662f8     User Identity Module/High
SG   02:00:15.778203   [ gstk_receive_data.c  303   IN GSTK_RECEIVE_DATA_REQ: command_ptr=0x875662f8     User Identity Module/High
SG   02:00:16.370235   [   gstk_send_data.c   289]  IN GSTK_SEND_DATA_REQ: command_ptr=0x875662f8        User Identity Module/High
SG   02:00:16.671979   [ gstk_receive_data.c  303   IN GSTK_RECEIVE_DATA_REQ: command_ptr=0x875662f8     User Identity Module/High
SG   02:00:16.996172   [    gstk_close_ch.c   304   IN GSTK_CLOSE_CH_REQ                                 User Identity Module/High
SG   02:00:22.392995   [    gstk_refresh.c   1386]  SENDING REFRESH REQ TO MMGSDI ...                    User Identity Module/High
```

5. KT OTA requirements

5.1 KT OTA provision process

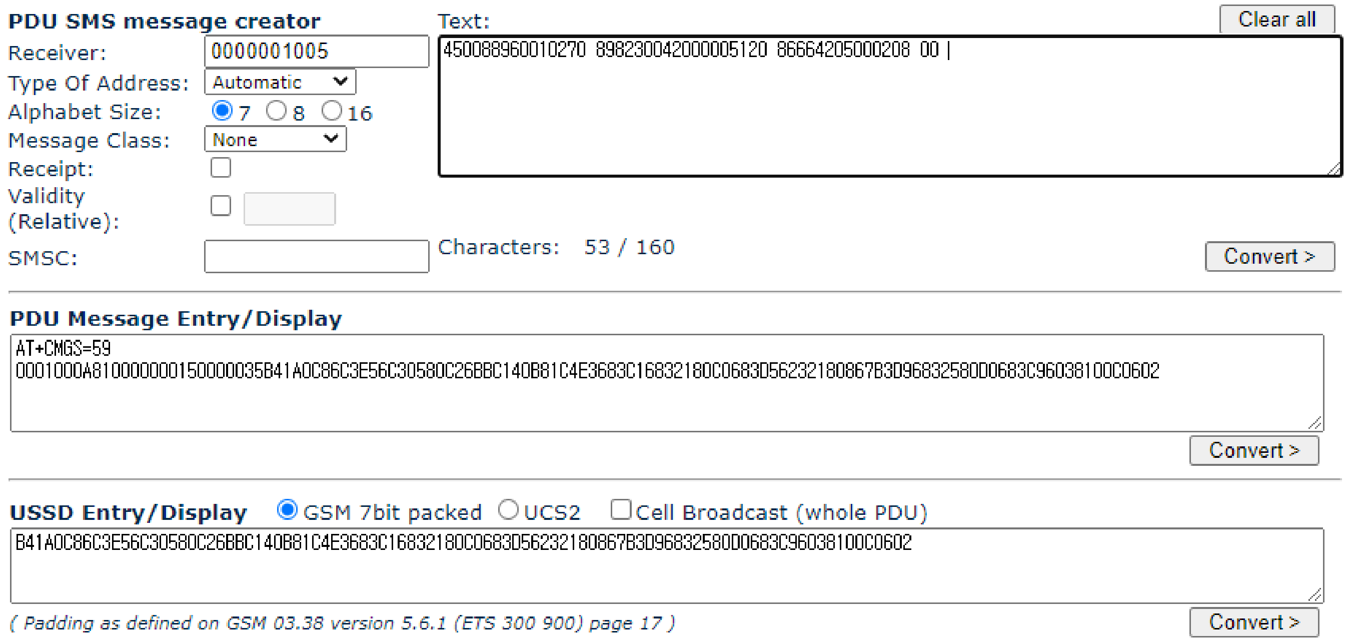
The terminal must configure the OTA number registration request message using the SMS-SUBMIT message as follows.

- The RP-DA value should use the SMSC address of the EF_SMSP of the USIM card.
- For TP-DA value, ‘0x0000001005’ should be used.
- For PID value, ‘0x7F’ should be used.
- For TP-DCS value, ‘0x00’ should be used.
- The value in TP-UD of SMS-SUBMIT must be encoded in GSM 7BIT.
- The value in TP-UD of SMS-SUBMIT is “IMSI(15Digit)+ICCID(18Digit)+IMEI(14Digit)+EFtype” (2Digit)+” must be used. (“+” is SPACE, so total 53 digits)

- For EFtype value, '00' (MSISDN) should be used.

7	6	5	4	3	2	1	0	Type	비 고
RP	UDHI	SRR	VPF		RD	MTI		M	
TP-MR								M	
Address-Length								M	TP-DA 3GPP TS 23.040 참조
Type-of-Address **"unknown"**								M	
Value **"0000001005" hex**								M	
TP-PID **"7F" hex**								M	해당 PID/DCS 참조
TP-DCS **"00"hex**								M	해당 PID/DCS 참조
TP-VP								O	VPF=00 이면 필드 생략
TP-UDL								M	
TP-UDHL								M	
IEI								O	CallBack IEI : 0x50
IEI_DataLength								O	데이터 길이
IEI_DigitNumber (최대 20 Digits)								O	CallBack Digit 개수
Digit 2				Digit 1				O	
• • •				• • •				O	
Digit n				Digit n-1				O	
TP-UD **"IMSI 15Digit + ICCID 18Digit + IMEI 14Digit + EFtype 2Digit+"GSM 7bit encoding**								O	

See below example.



PDU SMS message creator

Receiver: 0000001005

Type Of Address: Automatic

Alphabet Size: ● 7 ○ 8 ○ 16

Message Class: None

Receipt: □

Validity (Relative): □

SMSC:

Text:

```
450088960010270 898230042000005120 86664205000208 00 |
```

Characters: 53 / 160

PDU Message Entry/Display

```
AT+CMGS=59
0001000A8100000000150000035B41A0C86C3E56C30580C26BBC140B81C4E3683C16832180C0683D56232180867B3D96832580D0683C960381000C0602
```

USSD Entry/Display ● GSM 7bit packed ○ UCS2 □ Cell Broadcast (whole PDU)

```
B41A0C86C3E56C30580C26BBC140B81C4E3683C16832180C0683D56232180867B3D96832580D0683C960381000C0602
```

(Padding as defined on GSM 03.38 version 5.6.1 (ETS 300 900) page 17)

5.2 AT command and Log analysis

STEP 1. AT+QCOTA

SMS PDU MODE for OTA trigger.

1) AT+CMGF=0
2) AT+CMGS=59
   `>`0001FF0A8100000001507F0035B41A0C86C3D16EB0D84D26ABC540B81C4E3683C16C32180C66CBE560B118685693C572B3580C0683D96831100C0602

`Ctrl + Z` or `0x1A`

Here for decoding for above example.

Header *Userdata length*, **Data**(gsm7bit) are as follows (Data needs to be corrected, use gsm7bit converter)

0001FF0A8100000001507F00
35
B41A0C86C3D16EB0D84D26ABC540B81C4E3683C16C32180C66CBE560B118685693C572B3580C0683D96831100C0602

Text message
- To: 0000001005
- Message: 450088470172251 898230062000699011 35219311000641 00

Format: `IMSI` `ICCID` `IMEI` `SVN`

IMSI	ICCID	IMEI	SVN
450088470172251	898230062000699011	35219311000641	00

- USER DATA

B41A0C86C3D16EB0D84D26ABC540B81C4E3683C16C32180C66CBE560B118685693C572B3580C0683D96831100C0602

SMS PDU Item	DATA
##Additional information	
PDU type	SMS-SUBMIT
Reference	255
Val. format	None
Data coding	SMS Default Alphabet
## Original Encoded PDU fields	
SMSC	00
PDU header	01
TP-MTI	01
TP-RD	00
TP-VPF	00
TP-SRR	00
TP-UDHI	00
TP-RP	00
TP-MR	FF
TP-DA	0A8100000000150
TP-PID	7F
TP-DCS	00

TP-UDL	35
TP-UD	B41A0C86C3D16EB0D84D26ABC540B81C4E3683C16C32180C66CB E560B118685693C572B3580C0683D96831100C0602

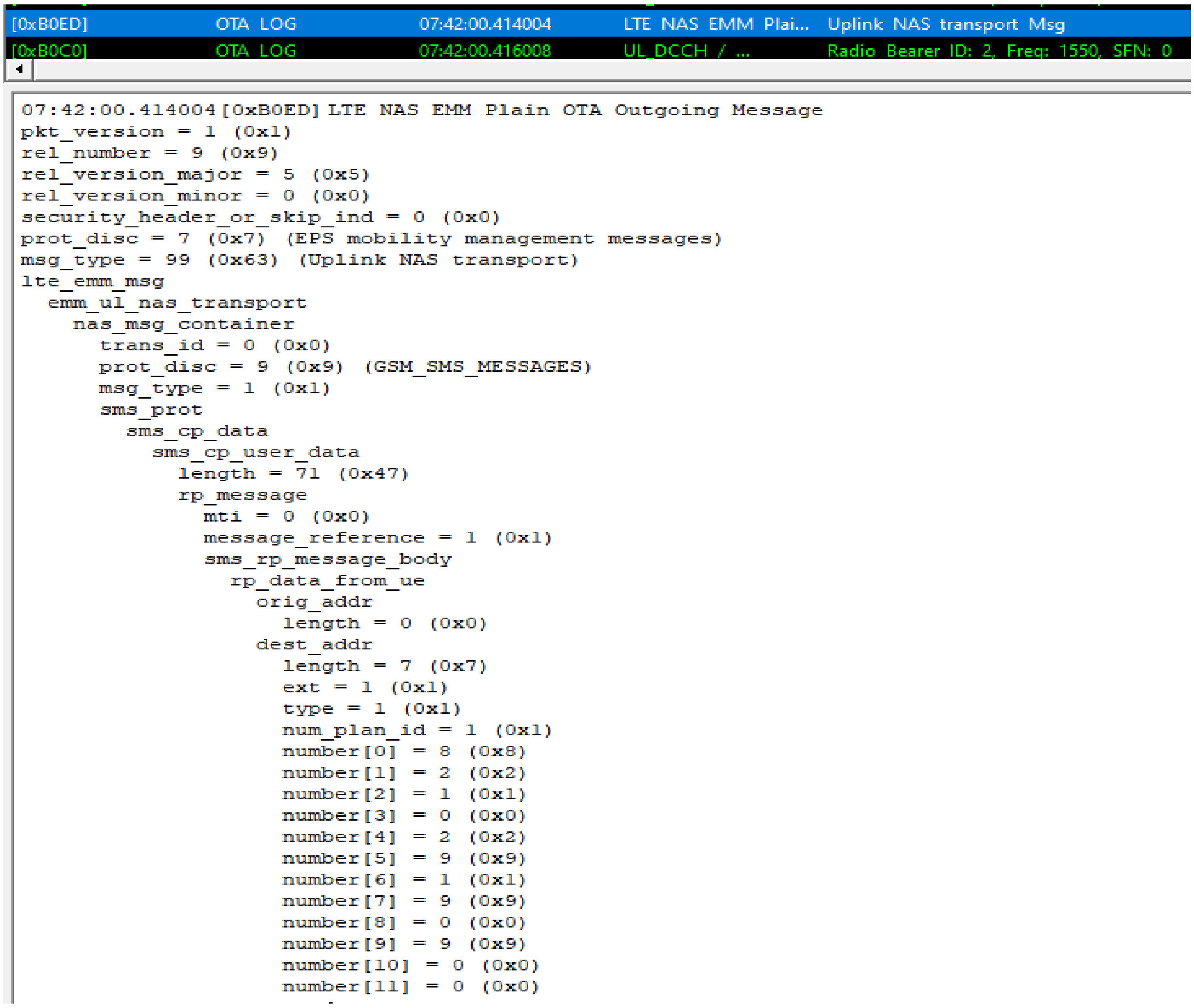
STEP 2. Send to SIMTK envelope command to UIM

Start triggered OTA by SIMTK envelopment command.

Start BIP APDU command with ENVELOPE(SMS-PP DOWNLOAD) Msg.

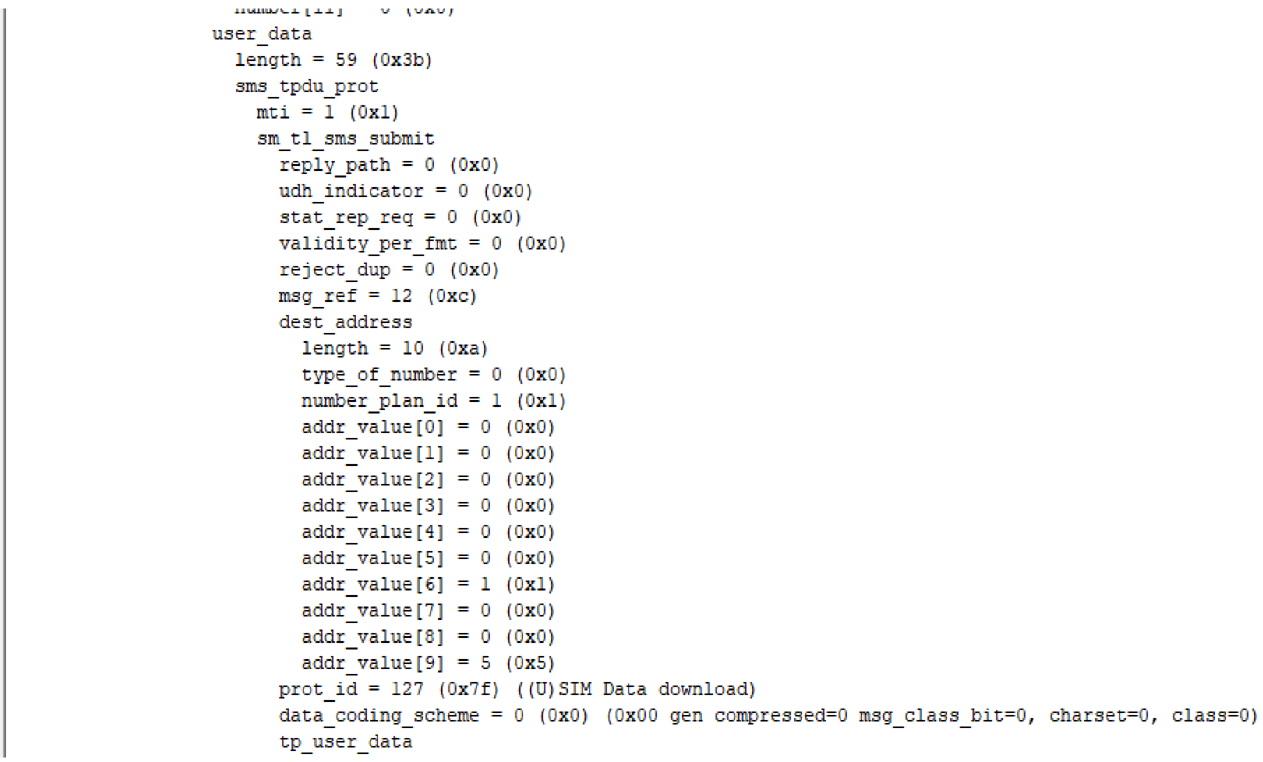
```
C> ENVELOPE (SMS-PP Download)
80C200005DD15B820283818B554406890900007FF6607021210504634502700000401512092
525B000010000000003002E66CF7A32D297B000A4000C026F4000DC01041EFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
R> SW=6200
C> GET RESPONSE
00C0000000
R> SW=6C18
C> GET RESPONSE
00C0000018
R> 027100001312B000010000000003000223A62572B25EF793 + SW=9000

<Response Packet Analysis>
02 : UDHL 02h=length of the IEI/RPI + IEIDL fields
71 : IEI-RPI 71h=presence of SIM toolkit security headers
00 : IEIDL 00h=Information Element Data Length
0013 : RPL = Response Packet Length
12 : RHL=Response Header Length
B00001 : TAR B00001h=USIM
0000000003 : CNTR=3
00 : PCNTR
02 : RSC 02h=CNTR is too low
23A62572B25EF793 : Cryptographic Checksum
```

STEP 3. SMS-SUBMIT Message for OTA trigger.

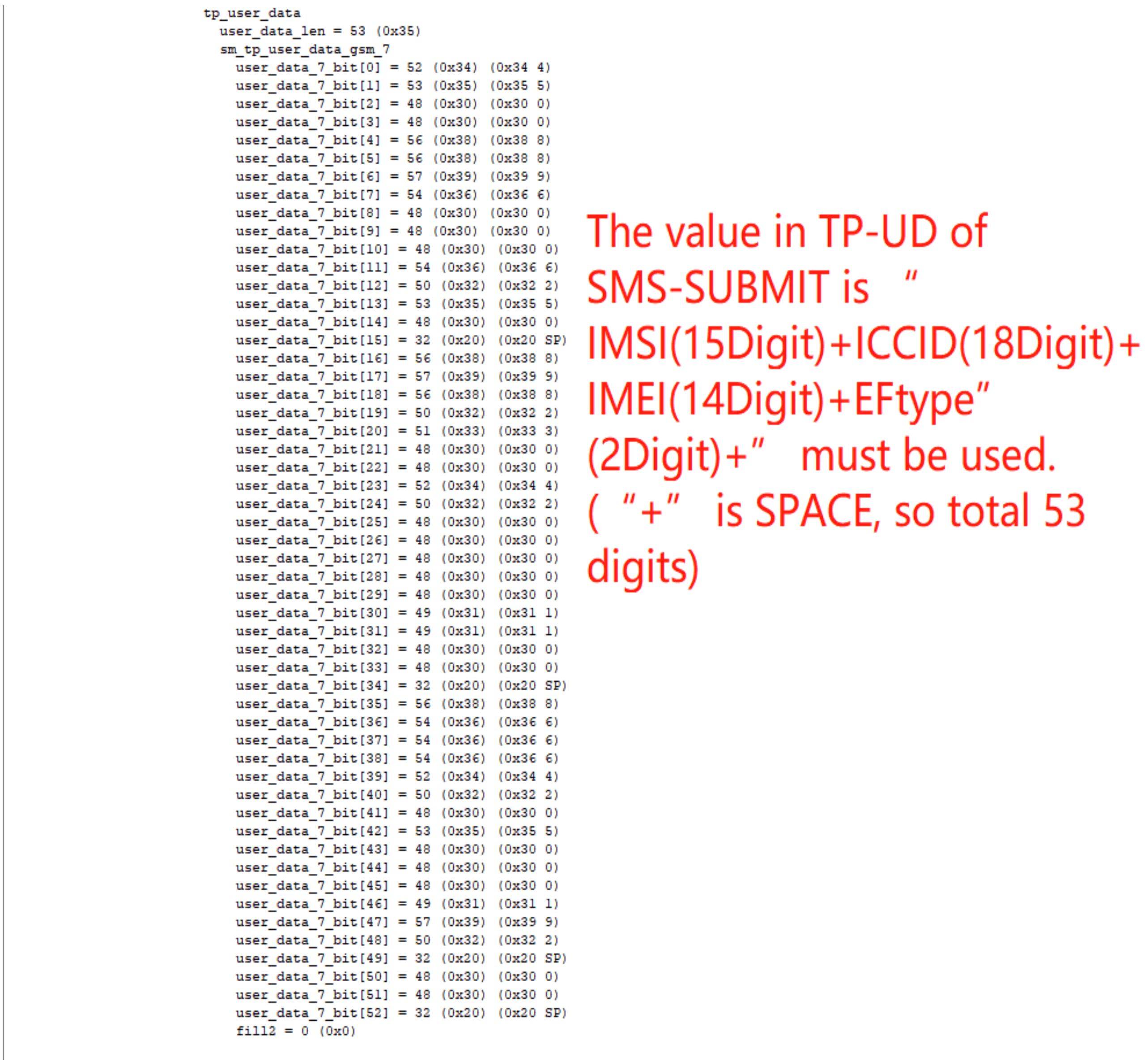


```
[0xB0ED]          OTA LOG          07:42:00.414004          LTE NAS EMM Plai...   Uplink NAS transport Msg
[0xB0C0]          OTA LOG          07:42:00.416008          UL_DCCH / ...         Radio Bearer ID: 2, Freq: 1550, SFN: 0
```

```
07:42:00.414004 [0xB0ED] LTE NAS EMM Plain OTA Outgoing Message
pkt_version = 1 (0x1)
rel_number = 9 (0x9)
rel_version_major = 5 (0x5)
rel_version_minor = 0 (0x0)
security_header_or_skip_ind = 0 (0x0)
prot_disc = 7 (0x7) (EPS mobility management messages)
msg_type = 99 (0x63) (Uplink NAS transport)
lte_emm_msg
  emm_ul_nas_transport
    nas_msg_container
      trans_id = 0 (0x0)
      prot_disc = 9 (0x9) (GSM_SMS_MESSAGES)
      msg_type = 1 (0x1)
      sms_prot
        sms_cp_data
          sms_cp_user_data
            length = 71 (0x47)
            rp_message
              mti = 0 (0x0)
              message_reference = 1 (0x1)
              sms_rp_message_body
                rp_data_from_ue
                  orig_addr
                    length = 0 (0x0)
                  dest_addr
                    length = 7 (0x7)
                    ext = 1 (0x1)
                    type = 1 (0x1)
                    num_plan_id = 1 (0x1)
                    number[0] = 8 (0x8)
                    number[1] = 2 (0x2)
                    number[2] = 1 (0x1)
                    number[3] = 0 (0x0)
                    number[4] = 2 (0x2)
                    number[5] = 9 (0x9)
                    number[6] = 1 (0x1)
                    number[7] = 9 (0x9)
                    number[8] = 0 (0x0)
                    number[9] = 9 (0x9)
                    number[10] = 0 (0x0)
                    number[11] = 0 (0x0)
```



```
                    number[11] = 0 (0x0)
                  user_data
                    length = 59 (0x3b)
                    sms_tpdu_prot
                      mti = 1 (0x1)
                      sm_tl_sms_submit
                        reply_path = 0 (0x0)
                        udh_indicator = 0 (0x0)
                        stat_rep_req = 0 (0x0)
                        validity_per_fmt = 0 (0x0)
                        reject_dup = 0 (0x0)
                        msg_ref = 12 (0xc)
                        dest_address
                          length = 10 (0xa)
                          type_of_number = 0 (0x0)
                          number_plan_id = 1 (0x1)
                          addr_value[0] = 0 (0x0)
                          addr_value[1] = 0 (0x0)
                          addr_value[2] = 0 (0x0)
                          addr_value[3] = 0 (0x0)
                          addr_value[4] = 0 (0x0)
                          addr_value[5] = 0 (0x0)
                          addr_value[6] = 1 (0x1)
                          addr_value[7] = 0 (0x0)
                          addr_value[8] = 0 (0x0)
                          addr_value[9] = 5 (0x5)
                        prot_id = 127 (0x7f) ((U)SIM Data download)
                        data_coding_scheme = 0 (0x0) (0x00 gen compressed=0 msg_class_bit=0, charset=0, class=0)
                        tp_user_data
```

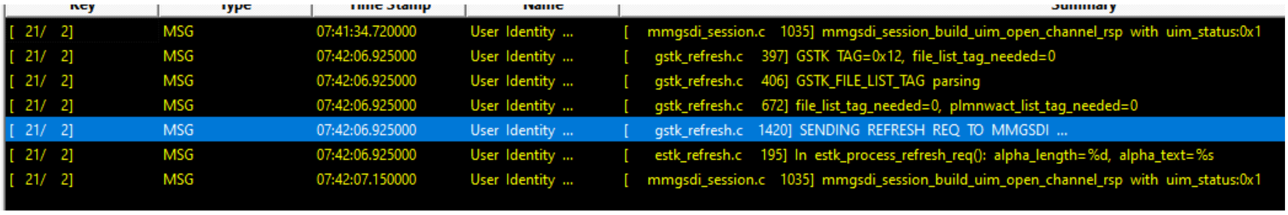


```
tp_user_data
  user_data_len = 53 (0x35)
  sm_tp_user_data_gsm_7
    user_data_7_bit[0] = 52 (0x34) (0x34 4)
    user_data_7_bit[1] = 53 (0x35) (0x35 5)
    user_data_7_bit[2] = 48 (0x30) (0x30 0)
    user_data_7_bit[3] = 48 (0x30) (0x30 0)
    user_data_7_bit[4] = 56 (0x38) (0x38 8)
    user_data_7_bit[5] = 56 (0x38) (0x38 8)
    user_data_7_bit[6] = 57 (0x39) (0x39 9)
    user_data_7_bit[7] = 54 (0x36) (0x36 6)
    user_data_7_bit[8] = 48 (0x30) (0x30 0)
    user_data_7_bit[9] = 48 (0x30) (0x30 0)
    user_data_7_bit[10] = 48 (0x30) (0x30 0)
    user_data_7_bit[11] = 54 (0x36) (0x36 6)
    user_data_7_bit[12] = 50 (0x32) (0x32 2)
    user_data_7_bit[13] = 53 (0x35) (0x35 5)
    user_data_7_bit[14] = 48 (0x30) (0x30 0)
    user_data_7_bit[15] = 32 (0x20) (0x20 SP)
    user_data_7_bit[16] = 56 (0x38) (0x38 8)
    user_data_7_bit[17] = 57 (0x39) (0x39 9)
    user_data_7_bit[18] = 56 (0x38) (0x38 8)
    user_data_7_bit[19] = 50 (0x32) (0x32 2)
    user_data_7_bit[20] = 51 (0x33) (0x33 3)
    user_data_7_bit[21] = 48 (0x30) (0x30 0)
    user_data_7_bit[22] = 48 (0x30) (0x30 0)
    user_data_7_bit[23] = 52 (0x34) (0x34 4)
    user_data_7_bit[24] = 50 (0x32) (0x32 2)
    user_data_7_bit[25] = 48 (0x30) (0x30 0)
    user_data_7_bit[26] = 48 (0x30) (0x30 0)
    user_data_7_bit[27] = 48 (0x30) (0x30 0)
    user_data_7_bit[28] = 48 (0x30) (0x30 0)
    user_data_7_bit[29] = 48 (0x30) (0x30 0)
    user_data_7_bit[30] = 49 (0x31) (0x31 1)
    user_data_7_bit[31] = 49 (0x31) (0x31 1)
    user_data_7_bit[32] = 48 (0x30) (0x30 0)
    user_data_7_bit[33] = 48 (0x30) (0x30 0)
    user_data_7_bit[34] = 32 (0x20) (0x20 SP)
    user_data_7_bit[35] = 56 (0x38) (0x38 8)
    user_data_7_bit[36] = 54 (0x36) (0x36 6)
    user_data_7_bit[37] = 54 (0x36) (0x36 6)
    user_data_7_bit[38] = 54 (0x36) (0x36 6)
    user_data_7_bit[39] = 52 (0x34) (0x34 4)
    user_data_7_bit[40] = 50 (0x32) (0x32 2)
    user_data_7_bit[41] = 48 (0x30) (0x30 0)
    user_data_7_bit[42] = 53 (0x35) (0x35 5)
    user_data_7_bit[43] = 48 (0x30) (0x30 0)
    user_data_7_bit[44] = 48 (0x30) (0x30 0)
    user_data_7_bit[45] = 48 (0x30) (0x30 0)
    user_data_7_bit[46] = 49 (0x31) (0x31 1)
    user_data_7_bit[47] = 57 (0x39) (0x39 9)
    user_data_7_bit[48] = 50 (0x32) (0x32 2)
    user_data_7_bit[49] = 32 (0x20) (0x20 SP)
    user_data_7_bit[50] = 48 (0x30) (0x30 0)
    user_data_7_bit[51] = 48 (0x30) (0x30 0)
    user_data_7_bit[52] = 32 (0x20) (0x20 SP)
    fill2 = 0 (0x0)
```

The value in TP-UD of SMS-SUBMIT is " IMSI(15Digit)+ICCID(18Digit)+ IMEI(14Digit)+EFtype" (2Digit)+" must be used. ("+" is SPACE, so total 53 digits)

STEP 4. Check OTA complete with Proactive log analys for OTA

5. Open channel
6. Send/Receive Data
7. Close Channel
8. SIM Refresh.: OTA Done…



```
Key          Type    Time Stamp        Name              Summary
[ 21/  2]    MSG     07:41:34.720000   User Identity ...  [  mmgsdi_session.c   1035] mmgsdi_session_build_uim_open_channel_rsp with uim_status:0x1
[ 21/  2]    MSG     07:42:06.925000   User Identity ...  [   gstk_refresh.c    397] GSTK TAG=0x12, file_list_tag_needed=0
[ 21/  2]    MSG     07:42:06.925000   User Identity ...  [   gstk_refresh.c    406] GSTK_FILE_LIST_TAG parsing
[ 21/  2]    MSG     07:42:06.925000   User Identity ...  [   gstk_refresh.c    672] file_list_tag_needed=0, plmnwact_list_tag_needed=0
[ 21/  2]    MSG     07:42:06.925000   User Identity ...  [   gstk_refresh.c   1420] SENDING REFRESH REQ TO MMGSDI ...
[ 21/  2]    MSG     07:42:06.925000   User Identity ...  [   estk_refresh.c    195] In estk_process_refresh_req(): alpha_length=%d, alpha_text=%s
[ 21/  2]    MSG     07:42:07.150000   User Identity ...  [  mmgsdi_session.c   1035] mmgsdi_session_build_uim_open_channel_rsp with uim_status:0x1
```

6. Check Point for SIM Provisioning

When you get Certification, you have pass for OTA provisioning necessary.
This is mandatory requirement.

For the OTA provision test, you have to prepare NULL MSISDN SIM card for first activation.

- You can purchase this in the Card Store.
- You can trigger OTA and you can download by OTA process.
- AT Command (Null MSISDN)

  ```
  AT+CNUM
  ERROR
  ```

For the reactivation process, the is MSISDN already installed MSISDN number as follows.

```
AT+CNUM
+821012345677
```

In this case, you have to visit to each mobile store. (POS provisioning)
For certification, you have to contact network manager.
In this case server status is ready to reprovisionging.