ASR 5x00 Series SGSN Authentication and PTMSI Reallocation Best Practices

Document ID: 119148

Contributed by Krishna Kishore DV, Sujin Anagani, and Parthasarathy M, Cisco TAC Engineers.

Jun 12, 2015

Contents

Introduction

This document provides a basic explanation of the benefits of the authentication procedure frequency configuration, Packet Temporary Mobile Subscriber Identity (PTMSI), and PTMSI signature reallocation. Specifically, this document is for an optional third−generation Partnership Project mobility management procedure for 2G and 3G on Serving GPRS Support Node (SGSN) that runs on Aggregated Service Router (ASR) 5000 Series.

This document explains these best practices:

- Authentication frequency setting
- PTMSI reallocation
- PTMSI signature reallocation
- The impact if you do not configure the authentication frequency setting and the PTMSI reallocation and signature reallocation (based on experience from customer cases)
- Configuration guidelines and the impact on external interfaces
- Options to troubleshoot issues

Overview

The authentication, PTMSI, and PTMSI signature reallocation framework under the call control profile enables the operator to configure authentication or allocation of the PTMSI and PTMSI signature per subscriber in the 2G and 3G SGSN and the Mobile Management Entity (MME). In the SGSN, authentication can currently be configured for these procedures − attach, service−request, routing−area−update (RAU), short−messaging−service, and detach.

MME also makes use of the same framework in order to configure authentication for service−requests and tracking−area−updates (TAUs). PTMSI reallocation is configurable for attach, service−request, and RAUs. PTMSI signature reallocation is configurable for attach, PTMSI reallocation command, and RAUs. Authentication and reallocation can be enabled for every instance of these procedures or for every nth instance of the procedure, called selective authentication/reallocation. Certain procedures also support the enablement of authentication or reallocation based on the time elapsed (periodicity or interval) since the last authentication or reallocation respectively.

Furthermore, these can be configured specifically for only Universal Mobile Telecommunications System (UMTS) (3G) or General Packet Radio Service (GPRS) (2G) or both. This configuration is checked only when it is optional for the SGSN to authenticate or reallocate the PTMSI/PTMSI signature of a subscriber. In scenarios where it is mandatory to do these procedures, this configuration is not checked.

There are three types of CLIs for every procedure's frequency configuration − a SET CLI, a NO CLI, and a REMOVE CLI. When you invoke a SET CLI, the operator wants to enable authentication or reallocation for the specific procedure. The NO CLI is to explicitly disable authentication or PTMSI reallocation for a procedure, and the REMOVE CLI is to restore the configuration to a state where the CLI (SET or NO) is not configured at all. All configurations are assumed to be REMOVED when the tree is initialized in the cc−profile allocation. Hence, REMOVE is the default configuration.

The SET CLI shall affect only one specific procedure in the tree while the NO CLI and REMOVE CLI shall affect the current procedure and also REMOVE the lower nodes. Also, if NO CLI or REMOVE CLI affects the common tree, the effect shall be propagated on the corresponding nodes in the access−specific trees also.

There are two types of CLIs for every procedure's periodicity configuration − the SET CLI and the REMOVE CLI. The SET and REMOVE completed against periodicity shall affect only the periodicity configuration and leave the frequency configuration untouched. The NO CLI performed for frequency (to be precise, the NO CLI is common in that it does not take any frequency or periodicity arguments, but is identified with the frequency configuration internally while storing) will also REMOVE the periodicity configuration.

Certain scenarios where authentication is completed unconditionally are as follows:

- International Mobile Subscriber Identity (IMSI) attach − all IMSI attaches are authenticated
- when the subscriber has not been authenticated before and you do not have a vector
- when there is a PTMSI signature mismatch
- when there is a Ciphering Key Sequence Number (CKSN) mismatch

Currently, authentication can be enabled for these under the call−control−profile:

- attach, service−request, RAU, detach, short−messaging−service, all−events, and TAU
- TAU is in use by MME
- attach and service−request are used both by SGSN and MME
- the rest are used exclusively by SGSN

SGSN Authentication and PTMSI Signature Procedure Blocks

This tree structure explains the procedure blocks that SGSN considers for frequency settings.

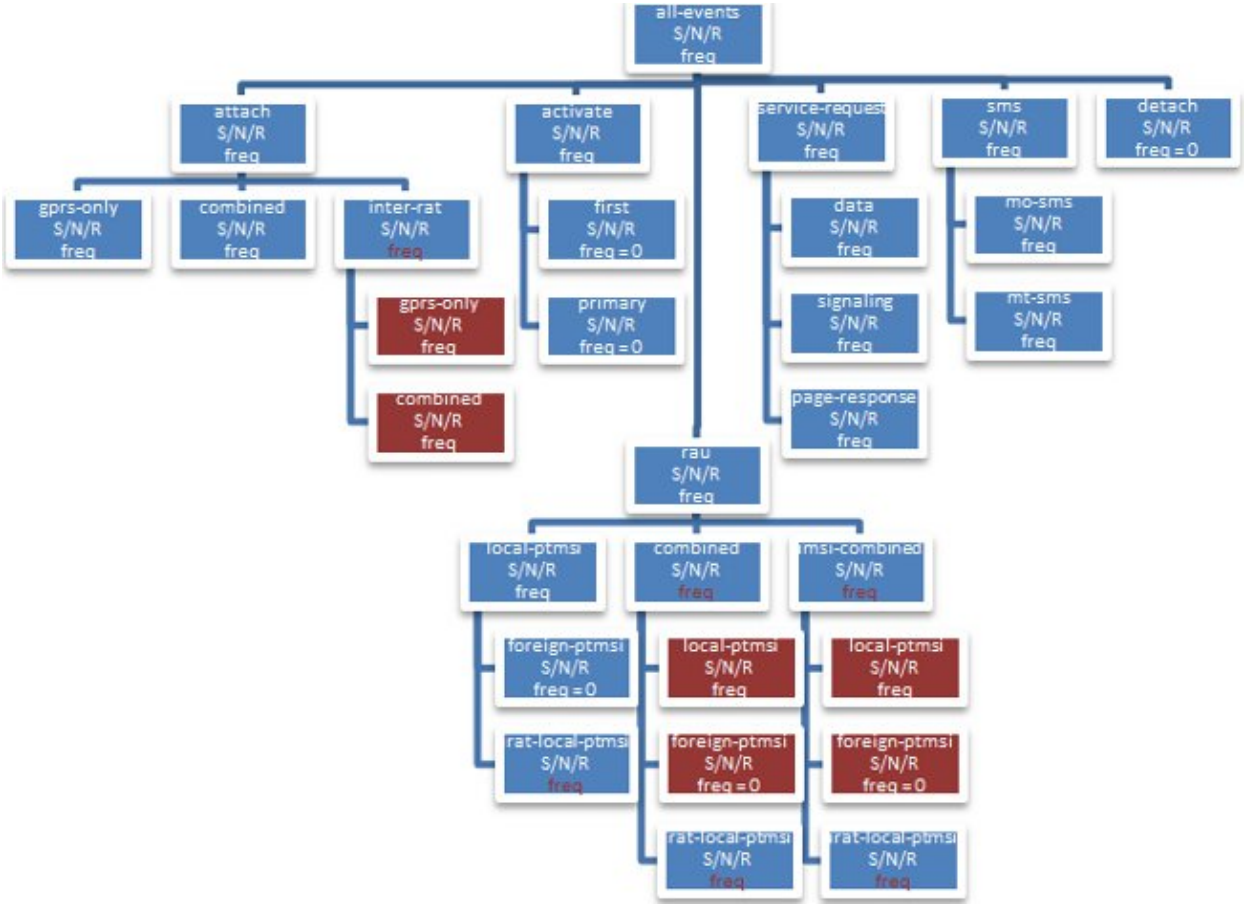

Figure 1: Procedure Blocks SGSN Considers for Frequency Settings

The trees for the PTMSI reallocation procedure are shown here.

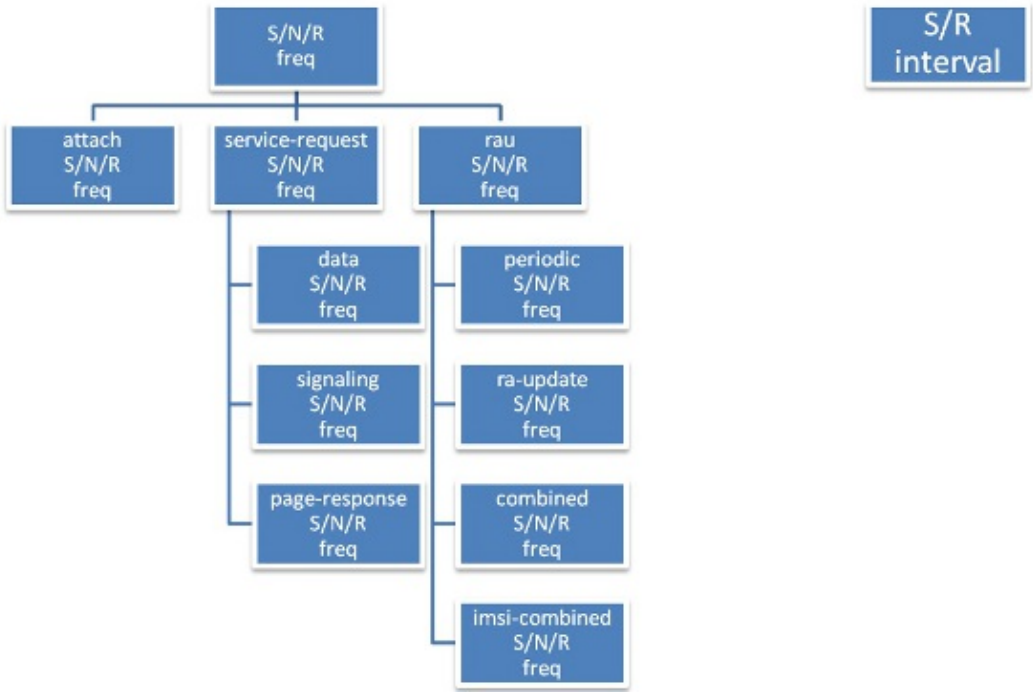

Figure 2: Authentication Configuration Tree

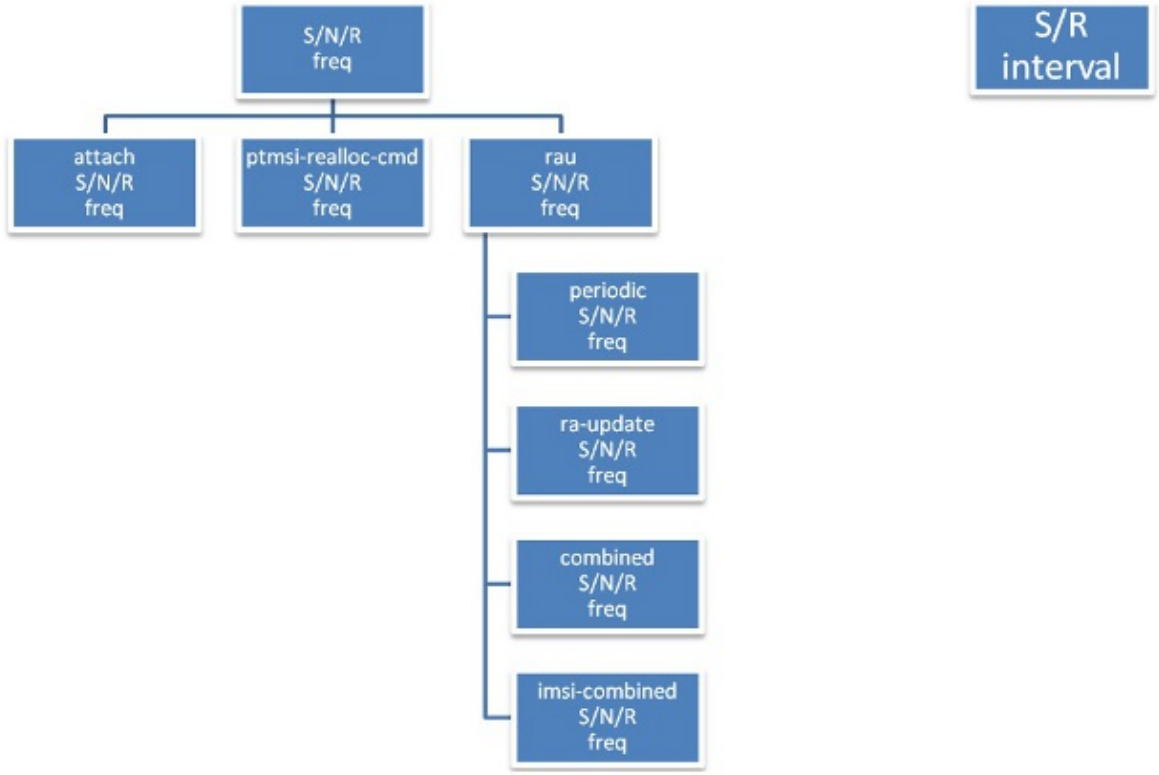

Figure 3 : PTMSI Reallocation Configuration Tree

Why Authentication and PTMSI Signature Reallocation is Required

Per 3GPP Technical Specifications (TS) 23.060, section 6.5.2, step (4), the authentication functions are defined in the clause "Security Function". If no Mobility Management (MM) context for the Mobile Station (MS) exists anywhere in the network, then authentication is mandatory. Ciphering procedures are described in clause "Security Function". If PTMSI allocation will be completed and the network supports ciphering, the network shall set the ciphering mode.

As mentioned, SGSN performs authentication only for new registration requests such as IMSI attaches and inter−SGSN RAUs in some call flows where validation of the PTMSI signature or the CKSN is mismatched with the stored one. For example, procedures such as periodic RAU and intra−RAUs are not required to be authenticated as they already have an existing database with a registered SGSN. Authentication is optional here. Not completing authentication is not always good as the User Equipment (UE) can stay in the network for days together without performance of a fresh registration request. There are chances that the security context setup between the SGSN and the UE might get compromised, so it is always good to periodically authenticate and check the validity of the subscriber that was registered in SGSN based on some frequency. This is explained in detail in 3GPP 23.060, section 6.8.

Security functions and the related references are located in 33.102, section 6.8. For example, if optional authentication is enabled based on Figures 18 and 19 in section 6.8 of 33.102, and if SGSN tries to authenticate the UE with incorrect security context parameters, the UE will never be able to match the Send Response (SRES) or Expected Response (XRES) with SGSN which results in reattachment to the network. This prevents the UE staying in the network with a false database for a longer time.

In order to provide identity hiding, a SGSN generates a temporary identity for an IMSI called the PTMSI. Once the MS attaches, the SGSN issues a new PTMSI to the MS. The MS then stores this PTMSI and uses it

in order to identify itself to the SGSN in any new future connection it initiates. Since the PTMSI is always given to the MS in a ciphered connection, no one will be able to map an IMSI to the PTMSI outside, although they might see a plain−text message with IMSI going at times. (For example, the first time an IMSI attaches and identity−responses with an IMSI).

PTMSI reallocation is explained in 3GPP 23.060, section 6.8 as a standalone procedure. The same can be completed as part of any uplink procedure in order to reallocate PTMSI and PTMSI signatures to protect UE identities. This will not increase network signalling on any interface. PTMSI and PTMSI signature reallocation is always good as these are the key identities that SGSN assigns to the UE in the initial registration step. Reallocation of these based on some frequency helps SGSN to hide the identity of the UE with different values for a prolonged time instead of the use of just one PTMSI value. Identity−hiding refers to the hiding of information such as IMSI and IMEI of the MS, when messages from/to the MS are still sent in plain−text and when encryption has not started yet.

Problem

In some customer networks, it was observed that some key identities such as MSIDN/PTMSI are mixed up between different subscribers and sent in GTPC signalling messages on the Gn interface and in Call Data Records (CDRs).

Cisco bug IDs CSCut62632 and CSCuu67401 deal with some corner cases of session recovery, which map the identity of one subscriber with another. Three cases are listed below. All of these cases are code reviewed, Quality Assurance team analyzed, and reproduced.

Scenario #1 (Double fault on sessmgr that results in loss of the subscriber identities)

UE1 − Attach − IMSI1 − Mobile Station International Subscriber Directory Number (MSISDN) 1 − PTMSI1 − Smgr#1

Double kill of sessmgr instance, SGSN lost UE1 details.

UE2 − Attach − IMSI2 − MSISDN 2 − PTMSI1 − Smgr#1

PTMSI1 is reused for UE2.

UE1 − Intra RAU − PTMSI1− SGSN processes this uplink, as authentication for intra−RAU is not mandatory.

This results in mixing of records of two different sessions.

Scenario #2 (Transaction Capabilities Application Part (TCAP) abort of one session that results in mixing up of subscriber identities)

UE1 − Attach − IMSI1 − UGL set (TCAP − internally aborted due to sessmgr crash)

UE2 − Attach − IMSI2 − UGL sent with same TCAP − OTID

HLR sends TCAP − continued from previous request, UE1's MSISDN

SGSN updates the incorrect MSISDN of UE1 with UE2 in this case. This results in mixing of records of two different sessions.

Scenario #3 (TCAP abort of one session that results in mixing up of subscriber identities)

UE1 − Attach − IMSI1 − SAI sent (TCAP − internally aborted due to sessmgr crash)

UE2 − Attach − IMSI2 − SAI sent with same TCAP − OTID

HLR sends TCAP − continued from previous request, UE1's authentication vectors (triplets or quintuplets)

SGSN updates the incorrect authentication vectors of UE1 with UE2

This results in SGSN using UE1 vectors for authentication of UE2.

Stabilization Approach

If authentication for intra−RAU is enabled or PTMSI reallocation is enabled, SGSN authenticates the client with a stored vector set. If the UE is different than what was stored for, UE/SGSN will not pass the authentication stage to proceed further in the network. With this, the chance of the UE staying in network with an incorrect database comes down. These are some known areas in the code. The business unit will continue to analyze more cases in order to understand this issue better.

Fix Plan

The fix from the Cisco bug IDs is a best effort approach. Analyze more areas of code and deploy this in less dense node for monitoring before you take it to a high density node.

Configuration Guidelines

The enablement of authentication increases the Gr and Iu interface signalling as SGSN needs to fetch the authentication vector set from the Home Location Register (HLR) and perform additional authentication procedures towards access. Operators need to be careful to choose frequency values that impact the network less.

GPRS Mobility Management (GMM)/Mobile Application Protocol (MAP) Key Performance Indicators (KPIs) are important to analyze before you derive frequency values for each procedure. Based on the KPIs, check the procedure that executes high. For this procedure, set high values of frequency. (This is the way to fine−tune each parameter based on a network call model).

An ideal way to configure these parameters is to set values to leafs, but not at the root of the tree. For example, Figure 2 explains the authentication configuration tree. Operators might choose to set the value to a lower level, as shown here, instead of the configuration of "authenticating attach" directly.

```
authenticate attach attach−type gprs−only frequency 10
authenticate attach attach−type combined frequency 10
```

It is always good to set high frequency values (units as 10s) and then monitor Gr/Iu interface signalling thresholds. If signalling is well within the limits, define values until signalling reaches a safe place near thresholds that the operator would like to set for their networks.

Set frequency on the various procedures in 20/30 and bring them down to 5−10 with close monitoring on external interface traffic. It is required to check the impact on linkmgr and sessmgr memory CPU with this excess load.

PTMSI and PTMSI signature reallocations will not cause the spike in signalling directly, but it is always important to set high frequency values so that the PTMSIs are available with sessmgr instances (which happens rarely). It is not recommended to change PTMSI for every uplink procedure from the UE, as this is

not the best practice. A value of 10 might be decent. After all these changes it is important to monitor and perform standard health checks on the system.

As an example:

```
Authentication:

authenticate attach ( we can still fine tune this based on KPIs of
 Inter RAT attach & attach type).

authenticate rau update-type periodic frequency 10

authenticate rau update-type ra-update frequency 5



PTMSI & PTMSI signature allocation:

ptmsi-reallocate attach

ptmsi-reallocate routing-area-update update-type ra-update

ptmsi-signature-reallocate attach frequency 10

ptmsi-signature-reallocate routing-area-update frequency 20

ptmsi-reallocate routing-area-update update-type periodic frequency 10
```

Troubleshoot

When authentication is to be performed or PTMSI or PTMSI signature is to be allocated, debug logs will be printed to capture why the procedure was completed. This aids in troubleshooting in the event of any discrepancies. These logs include the configuration from cc-profile and the current value of all counters and the movement of the decision logic via the various configuration and counters. Also, the current counter values per subscriber can be viewed with the ***show subscribers sgsn-only*** or ***show subscribers gprs-only*** commands.

A sample output of this is provided. The current counters and the latest authenticated timestamp are added to the ***show subscribers*** command full output.

```
[local]# show subscribers sgsn-only full all
.
.
.
DRX Parameter:
 Split PG Cycle Code: 7
 SPLIT on CCCH: Not supported by MS
 Non-DRX timer: max. 8 sec non-DRX mode after Transfer state
 CN Specific DRX cycle length coefficient: Not specified by MS
Authentication Counters
 Last authenticated timestamp          : 1306427164
 Auth all-events UMTS                  : 0    Auth all-events GPRS                 : 0
 Auth attach common UMTS               : 0    Auth attach common GPRS              : 0
 Auth attach gprs-only UMTS            : 0    Auth attach gprs-only GPRS           : 0
 Auth attach combined UMTS             : 0    Auth attach combined GPRS            : 0
 Auth attach irat UMTS                 : 0    Auth attach irat GPRS                : 0
 Auth attach irat-gprs-only UMTS       : 0    Auth attach irat-gprs-only GPRS      : 0
 Auth attach irat-combined UMTS        : 0    Auth attach irat-combined GPRS       : 0
 Auth  UMTS                            : 0    Auth  GPRS                           : 0
 Auth serv-req                         : 0    Auth serv-req data                   : 0
 Auth serv-req signaling               : 0    Auth serv-req page-rsp               : 0
```

```
 Auth rau UMTS                          : 0    Auth rau GPRS                          : 0
 Auth rau periodic UMTS                 : 0    Auth rau periodic GPRS                 : 0
 Auth rau ra-upd UMTS                   : 0    Auth rau ra-upd GPRS                   : 0
 Auth rau ra-upd lcl-ptmsi UMTS         : 0    Auth rau ra-upd lcl-ptmsi GPRS         : 0
 Auth rau ra-upd irat-lcl-ptmsi UMTS    : 0    Auth rau ra-upd irat-lcl-ptmsi GPRS    : 0
 Auth rau comb UMTS                     : 0    Auth rau comb GPRS                     : 0
 Auth rau comb lcl-ptmsi UMTS           : 0    Auth rau comb lcl-ptmsi GPRS           : 0
 Auth rau comb irat-lcl-ptmsi UMTS      : 0    Auth rau comb irat-lcl-ptmsi GPRS      : 0
 Auth rau imsi-comb UMTS                : 0    Auth rau imsi-comb GPRS                : 0
 Auth rau imsi-comb lcl-ptmsi UMTS      : 0    Auth rau imsi-comb lcl-ptmsi GPRS      : 0
 Auth rau imsi-comb irat-lcl-ptmsi UMTS: 0    Auth rau imsi-comb irat-lcl-ptmsi GPRS: 0
 Auth sms UMTS                          : 0    Auth sms GPRS                          : 0
 Auth sms mo-sms UMTS                   : 0    Auth sms mo-sms GPRS                   : 0
 Auth sms mt-sms UMTS                   : 0    Auth sms mt-sms UMTS                   : 0
PTMSI Realloc Counters
 Last allocated timestamp               : 1306427165
 PTMSI Realloc Freq UMTS                : 0    PTMSI Realloc Freq GPRS                : 0
 PTMSI Realloc Attach UMTS              : 0    PTMSI Realloc Attach GPRS              : 0
 PTMSI Realloc Serv-Req                 : 0    PTMSI Realloc Serv-Req Data            : 0
 PTMSI Realloc Serv-Req Signaling       : 0    PTMSI Realloc Serv-Req Page-rsp        : 0
 PTMSI Realloc Rau UMTS                 : 0    PTMSI Realloc Rau GPRS                 : 0
 PTMSI Realloc Rau Periodic UMTS        : 0    PTMSI Realloc Rau Periodic GPRS        : 0
 PTMSI Realloc Rau Ra-Upd UMTS          : 0    PTMSI Realloc Rau Ra-Upd GPRS          : 0
 PTMSI Realloc Rau Comb-Upd UMTS        : 0    PTMSI Realloc Rau Comb-Upd GPRS        : 0
 PTMSI Realloc Rau Imsi-Comb-Upd UMTS   : 0    PTMSI Realloc Rau Imsi-Comb-Upd GPRS   : 0
PTMSI Sig Realloc Counters
 Last allocated timestamp               : 0
 PTMSI Sig Realloc Freq UMTS            : 0    PTMSI Sig Realloc Freq GPRS            : 0
 PTMSI Sig Realloc Attach UMTS          : 0    PTMSI Sig Realloc Attach GPRS          : 0
 PTMSI Sig Realloc Ptmsi-rel-cmd UMTS   : 0    PTMSI Sig Realloc Ptmsi-rel-cmd GPRS   : 0
 PTMSI Sig Realloc Rau UMTS             : 0    PTMSI Sig Realloc Rau GPRS             : 0
 PTMSI Sig Realloc Rau Periodic UMTS    : 0    PTMSI Sig Realloc Rau Periodic GPRS    : 0
 PTMSI Sig Realloc Rau Ra-Upd UMTS      : 0    PTMSI Sig Realloc Rau Ra-Upd GPRS      : 0
 PTMSI Sig Realloc Rau Comb-Upd UMTS    : 0    PTMSI Sig Realloc Rau Comb-Upd GPRS    : 0
 PTMSI Sig Realloc Rau Imsi-Comb UMTS   : 0    PTMSI Sig Realloc Rau Imsi-Comb GPRS   : 0
CAE Server Address:
Subscription Data:
.
.
```

If the issue is seen in the network, enter these commands in order to collect information for the business unit to use to analyze the issue further:

```
show subscribers gprs-only full msisdn <msisdn>
show subscribers gprs-only full imsi <imsi>
show subscribers  sgsn-only msisdn <msisdn>
show subscribers  sgsn-only msisdn <imsi>
show subscribers gprs-debug-info callid <callid> (get o/p for both callid)
show subscribers debug-info callid <callid>       (get o/p for both callid)
task core facility sessmgr instance < >
task core facility imsimgr instance < >
Mon sub using MSISDN or pcap traces
SSD during issue.
Syslogs during the issue.
```

Risks

Increased signalling towards Gr/Iu interfaces plus a slight internal process (linkmgr) CPU impact if you authenticate too frequently.

Command Syntax

All the commands are in the configuration/call−control−profile mode and operator privileges apply. A snapshot of the commands under the cc−profile is as follows:

```
Authentication
1.          Attach
authenticate attach {inter−rat} {attach−type [gprs−only | combined ]}
 {frequency <1..16>} {access−type [umts | gprs]}
no authenticate attach {inter−rat} {attach−type [gprs−only | combined ]}
 {access−type [umts | gprs]}
remove authenticate attach {inter−rat} {attach−type [gprs−only | combined ]}
 {access−type [umts | gprs]}

2.          Service−request
authenticate service−request {service−type [data | signaling | page−response]}
 {frequency <1..16> | periodicity <1..10800>}
no authenticate service−request {service−type [data | signaling | page−response]}
remove authenticate service−request {service−type [data | signaling | page−response]}
 {periodicity}
3.          Rau
authenticate rau {update−type periodic} {frequency <1..16> | periodicity <1..10800>}
 {access−type [umts | gprs]}
authenticate rau {update−type [ra−update | combined−update | imsi−combined−update]}
 {with [local−ptmsi | inter−rat−local−ptmsi]} {frequency <1..16> |
 periodicity <1..10800>}
 {access−type [umts| gprs]}
authenticate rau {update−type [ra−update | combined−update | imsi−combined−update]}
 {with foreign−ptmsi} {access−type [umts| gprs]}
no authenticate rau {update−type periodic} {access−type [umts | gprs]}
no authenticate rau {update−type [ra−update | combined−update | imsi−combined−update]}
 {with [local−ptmsi | inter−rat−local−ptmsi | foreign−ptmsi]}
 {access−type [umts| gprs]}
remove authenticate rau {update−type periodic} {periodicity}
 {access−type [umts | gprs]}
remove authenticate rau {update−type [ra−update | combined−update |
 imsi−combined−update]}
 {with [local−ptmsi | inter−rat−local−ptmsi]} { periodicity} {access−type [umts| gprs]}
remove authenticate rau {update−type [ra−update | combined−update |
 imsi−combined−update]}
 {with foreign−ptmsi} {access−type [umts| gprs]}
4.          Sms
authenticate sms {sms−type [mo−sms | mt−sms]} {frequency <1..16>}
 {access−type [umts | gprs]}
no authenticate sms {sms−type [mo−sms | mt−sms]} {access−type [umts | gprs]}
remove authenticate sms {sms−type [mo−sms | mt−sms]} {access−type [umts | gprs]}
5.          Detach
authenticate detach {access−type [umts | gprs]}
no authenticate detach {access−type [umts | gprs]}
remove authenticate detach {access−type [umts | gprs]}
6.          All−events
authenticate all−events {frequency <1..16>} {access−type [umts | gprs]}
no authenticate all−events {access−type [umts | gprs]}
remove authenticate all−events {access−type [umts | gprs]}

PTMSI Reallocation
1.          Attach
ptmsi−reallocate attach {frequency <1..50>} {access−type [umts | gprs]}
no ptmsi−reallocate attach {access−type [umts | gprs]}
remove ptmsi−reallocate attach {access−type [umts | gprs]}
2.          Service−request
ptmsi−reallocate service−request {service−type [data | signaling | page−response]}
 {frequency <1..50>} no ptmsi−reallocate service−request
 {service−type [data | signaling | page−response]}
remove ptmsi−reallocate service−request {service−type [data | signaling |
```

```
 page-response]}
3.          Routing-area-update
ptmsi-reallocate routing-area-update {update-type [periodic | ra-update |
 combined-update | imsi-combined-update]} {frequency <1..50>}
 {access-type [umts | gprs]}
no ptmsi-reallocate routing-area-update {update-type [periodic | ra-update |
 combined-update | imsi-combined-update]} {access-type [umts | gprs]}
remove ptmsi-reallocate routing-area-update {update-type [periodic | ra-update |
 combined-update | imsi-combined-update]} {access-type [umts | gprs]}
4.          Interval/frequency
ptmsi-reallocate [interval <60..1440> | frequency <1..50>] {access-type [umts | gprs]}
no ptmsi-reallocate [interval | frequency] {access-type [umts | gprs]}
remove ptmsi-reallocate [interval | frequency] {access-type [umts | gprs]}
```

PTMSI-Signature Reallocation

```
1.      Attach
ptmsi-signature-reallocate attach {frequency <1..50>} {access-type [umts | gprs]}
no ptmsi-signature-reallocate attach {access-type [umts | gprs]}
remove ptmsi-signature-reallocate attach {access-type [umts | gprs]}
2.      PTMSI Reallocation command
ptmsi-signature-reallocate ptmsi-reallocation-command {frequency <1..50>}
 {access-type [umts | gprs]}
no ptmsi-signature-reallocate ptmsi-reallocation-command {access-type [umts | gprs]}
remove ptmsi-signature-reallocate ptmsi-reallocation-command
 {access-type [umts | gprs]}
3.      Routing-area-update
ptmsi-signature-reallocate routing-area-update {update-type [periodic | ra-update |
 combined-update | imsi-combined-update]} {frequency <1..50>}
 {access-type [umts | gprs]}
no ptmsi-signature-reallocate routing-area-update {update-type [periodic | ra-update |
 combined-update | imsi-combined-update]} {access-type [umts | gprs]}
remove ptmsi-signature-reallocate routing-area-update {update-type [periodic |
 ra-update | combined-update | imsi-combined-update]} {access-type [umts | gprs]}
4.      Interval/frequency
ptmsi-signature-reallocate [interval <60..1440> | frequency <1..50>]
 {access-type [umts | gprs]}
no ptmsi-signature-reallocate [interval | frequency] {access-type [umts | gprs]}
remove ptmsi-signature-reallocate [interval | frequency] {access-type [umts | gprs]}
```