

# ASR 5x00 Series SG/N-verificatie en PTMSI-hertoewijzing beste praktijken

## Inhoud

[Inleiding](#)

[Overzicht](#)

[SG500N-verificatie en PTMSI-handtekeningen](#)

[Waarom opnieuw verificatie en PTMSI-signaaltoewijzing vereist is](#)

[Probleem](#)

[Stabilisatie-aanpak](#)

[Fix Plan](#)

[Configuratierichtsnoeren](#)

[Problemen oplossen](#)

[Risico's](#)

[Complexe](#)

## Inleiding

Dit document geeft een basisuitleg van de voordelen van de authenticatieprocedure, de frequentieconformatie van Packet Tijdelijke Mobiele Subscriber Identity (PTMSI) en de hertoewijzing van PTMSI-handtekeningen. Dit document is met name bedoeld voor een optionele procedure voor het beheer van de mobiliteit van een derde generatie-project voor 2G en 3G ten behoeve van GPRS Support Node (SGSN), die wordt uitgevoerd op Aggregated Service Router (ASR) 5000 Series.

Dit document legt uit wat de beste praktijken zijn:

- Instelling van verificatiefrequentie
- PTMSI-hertoewijzing
- Hertoewijzing van PTMSI-handtekeningen
- Het effect als u de instelling van de authenticatiefrequentie niet configureren en de PTMSI-hertoewijzing en hertoewijzing van handtekeningen (gebaseerd op ervaringen uit klantcases)
- Configuratierichtsnoeren en het effect op externe interfaces
- Opties voor problemen oplossen

## Overzicht

Met de authenticatie, PTMSI en PTMSI-herverdelingsstructuur onder het aanspreekprofiel kan de exploitant de verificatie of toewijzing van de PTMSI- en PTMSI-handtekening per abonnee configureren in het 2G- en 3G-SGN en de mobiele beheerentiteit (MME). In het SGSN kan de authenticatie momenteel worden ingesteld voor deze procedures - attach, service-request,

Routing-Area-update (RAU), short-Messaging-Service en detach.

De MME maakt ook gebruik van hetzelfde kader om authenticatie te configureren voor serviceaanvragen en tracking-Area-updates (TAU's). PTMSI-hertoewijzing is configureerbaar voor attach, service-request en RAU's. PTMSI-hertoewijzing is configureerbaar voor attach, PTMSI-hertoewijzing en RAU's. Verificatie en hertoewijzing kunnen mogelijk zijn voor elk geval van deze procedures of voor elk nieuw geval van de procedure, selectieve authenticatie/hertoewijzing genaamd. Bepaalde procedures ondersteunen ook de mogelijkheid van echtheidscontrole of hertoewijzing op basis van de tijd die is verstreken (frequentie of interval) sinds de laatste echtheidscontrole of hertoewijzing respectievelijk.

Bovendien kunnen deze specifiek worden geconfigureerd voor alleen Universal Mobile Telecommunications System (UMTS) (3G) of General Packet Radio Service (GPRS) (2G) of beide. Deze configuratie wordt alleen gecontroleerd als het optioneel is voor SGN om de PTMSI/PTMSI-handtekening van een abonnee te echalisieren of opnieuw toe te wijzen. In scenario's waarin het verplicht is deze procedures te volgen, wordt deze configuratie niet gecontroleerd.

Er zijn drie types van CLIs voor de frequentieconfiguratie van elke procedure - een SET CLI, een NO CLI, en een REMOVE CLI. Wanneer u een SET CLI inroept, wil de operator authenticatie of hertoewijzing voor de specifieke procedure mogelijk maken. NO CLI moet verificatie of PTMSI-hertoewijzing expliciet uitschakelen voor een procedure, en de REMOVE CLI moet de configuratie herstellen in een toestand waarin de CLI (SET of NO) helemaal niet is ingesteld. Alle configuraties worden verondersteld REMOVED te worden wanneer de boom in de c-profieltoewijzing wordt geformatteerd. REMOVE is dus de standaardconfiguratie.

De SET CLI heeft slechts betrekking op één specifieke procedure in de boom, terwijl de NO CLI en de REMOVE CLI de huidige procedure zullen beïnvloeden en ook de onderste knooppunten zullen verwijderen. Indien NO CLI of REMOVE CLI de gemeenschappelijke boom niet beïnvloedt, wordt het effect ook verspreid op de overeenkomstige knooppunten in de toegangsspecifieke bomen.

Er zijn twee typen CLI's voor de periodieke configuratie van elke procedure: de SET CLI en de REMOVE CLI. De met een frequentie voltooide SET en REMOVE hebben alleen invloed op de frequentieconfiguratie en laten de frequentieconfiguratie onaangetast. De NO CLI uitgevoerd voor frequentie (om precies te zijn, de NO CLI komt vaak voor in die zin dat er geen frequentie- of frequentiecijfers worden gebruikt, maar wordt geïdentificeerd met de frequentieconfiguratie intern, terwijl er wordt opgeslagen) zal ook de frequentieconfiguratie VERWIJDEREN.

Bepaalde scenario's waarbij de authenticatie onvoorwaardelijk wordt voltooid zijn:

- IMSI-bijlagen (International Mobile Subscriber Identity) worden bevestigd - alle IMSI-bijlagen zijn authentiek
- wanneer de abonnee niet eerder is geauthentiseerd en u geen vector hebt
- wanneer er een fout in de PTMSI-handtekening optreedt
- wanneer er een tegenvaller van CKSN-sequentienummer (Ciphering Key Sequence Number) is

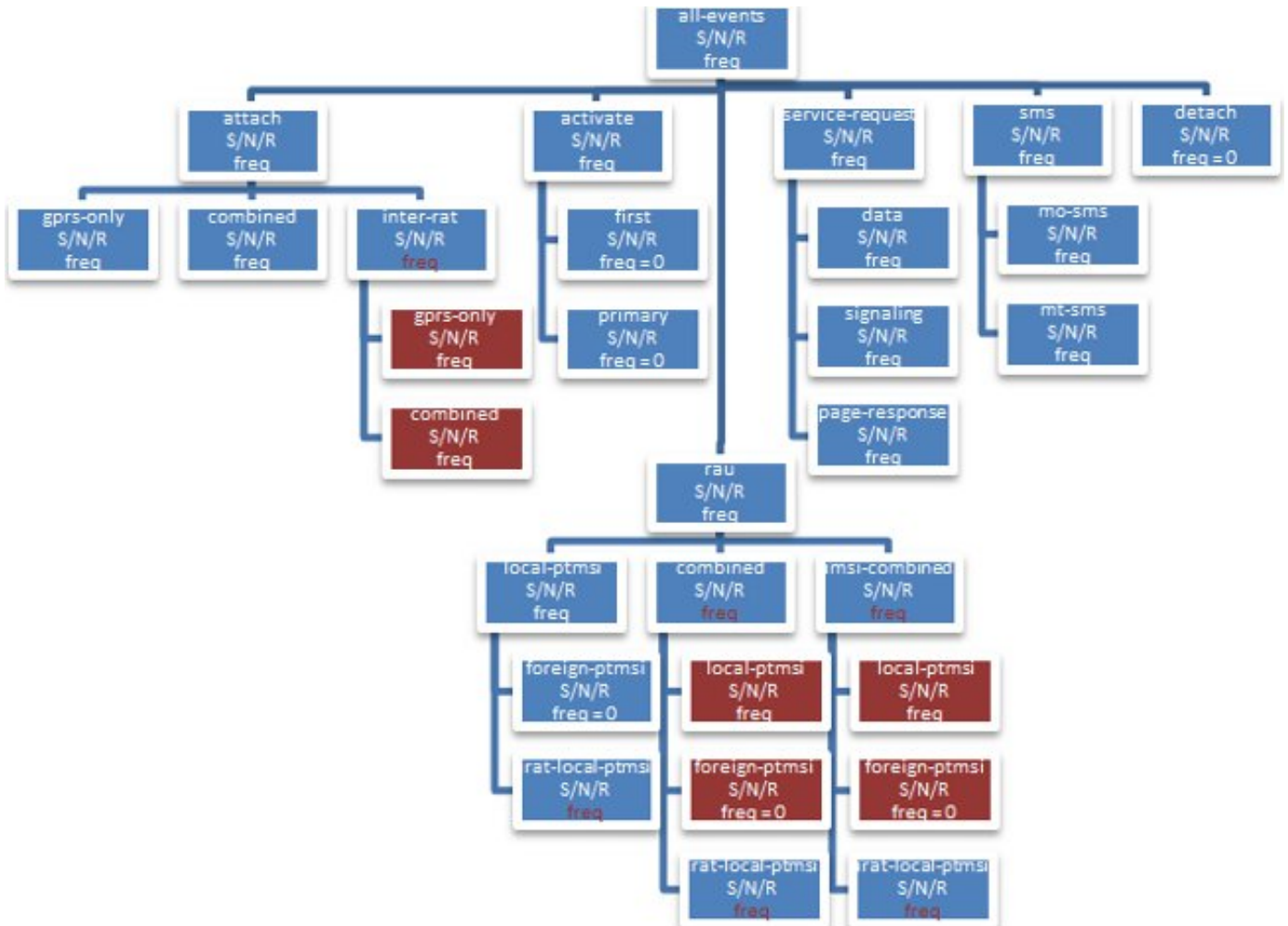
Op dit moment kan authenticatie voor deze instellingen worden ingeschakeld onder het aanroepcontrole-profiel:

- attach, service-request, RAU, detach, short-messaging-service, alle gebeurtenissen en TAU
- TAU is in gebruik door MME

- attach and service request is zowel door SGSN als door MME gebruikt
- de rest wordt uitsluitend door SGSN gebruikt

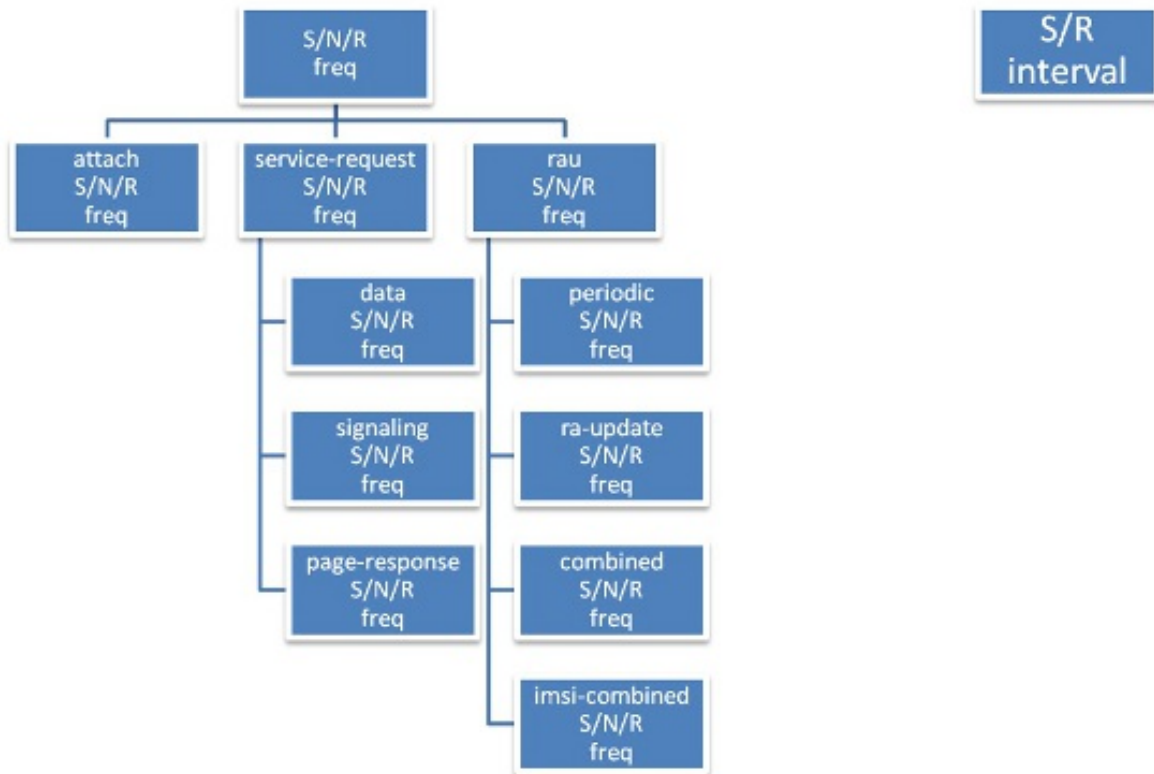
## SG500N-verificatie en PTMSI-handtekeningen

Deze boomstructuur verklaart de procedureblokken die SGSN voor frequentie instellingen overweegt.

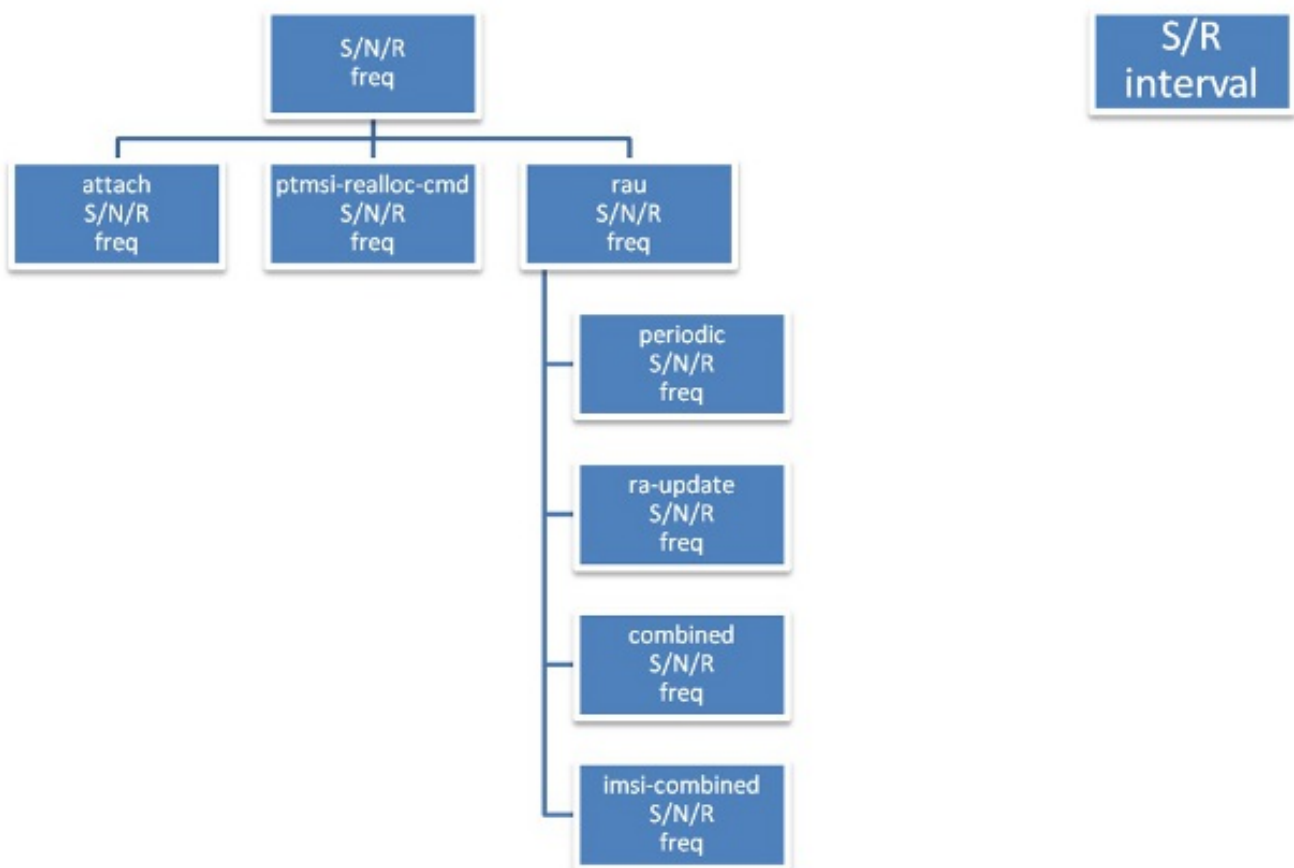


Afbeelding 1: Procedure-blokkering SGN acht voor frequentietoestellen

De bomen voor de PTMSI-hertoewijzingsprocedure worden hier aangegeven.



Afbeelding 2: Verificatieconfiguratieboom



Afbeelding 3: Configuratie-boom van PTMSI-hertoewijzing

**Waarom opnieuw verificatie en PTMSI-signaaltoewijzing vereist**

## is

Per 3GPP technische specificaties (TS) 23.060, paragraaf 6.5.2, stap (4), zijn de echtheidsfuncties gedefinieerd in de paragraaf "Beveiligingsfunctie". Als er geen context voor Mobility Management (MM) voor het mobiele station (MS) op het netwerk bestaat, is verificatie verplicht. De coderingsprocedures worden beschreven in de clausule "Beveiligingsfunctie". Indien de PTMSI-toewijzing zal worden voltooid en het netwerk ondersteuning biedt bij de codering, stelt het netwerk de coderingsmodus in.

Zoals reeds vermeld, voert SGSN alleen authenticatie uit voor nieuwe registratieaanvragen zoals IMSI-bijlagen en intra-SGSN-RAU's in sommige callstromen waarbij de validatie van de PTMSI-handtekening of de CKSN niet overeenkomt met de opgeslagen. Bijvoorbeeld, procedures zoals periodieke RAU's en intra-RAU's hoeven niet te worden geauthentiseerd aangezien zij reeds een bestaande databank met een geregistreerd SGSN hebben. Verificatie is hier niet verplicht. Het niet voltooiën van de authenticatie is niet altijd goed, aangezien de gebruikersapparatuur (UE) dagen samen in het netwerk kan blijven zonder dat een nieuwe registratieaanvraag wordt ingediend. Er zijn kansen dat de veiligheidscontext die is ingesteld tussen SGSN en de EU gecompromitteerd raakt, dus het is altijd goed om periodiek de geldigheid van de abonnee die in SGSN is geregistreerd op enige frequentie te authenticeren en te controleren. Dit wordt uitvoerig toegelicht in 3GPP 23.060, paragraaf 6.8.

Beveiligingsfuncties en de bijbehorende referenties bevinden zich in punt 6.8 van 33.102. Indien bijvoorbeeld optionele authenticatie is ingeschakeld op basis van de figuren 18 en 19 in punt 6.8 van 33.102, en indien SGSN de EU probeert te authenticeren met onjuiste veiligheidscontextparameters, zal de EU nooit kunnen voldoen aan de Send Response (SRES) of de verwachte respons (XRES) met SGSN die leidt tot een versterking van het netwerk. Dit voorkomt dat de UE langer in het netwerk blijft met een valse database.

Om identiteitsdekking te bieden, genereert een SGSN een tijdelijke identiteit voor een IMSI genaamd PTMSI. Zodra de lidstaten zich daaraan hechten, geeft het SGSN de lidstaten een nieuwe PTMSI. De lidstaten slaan deze PTMSI vervolgens op en gebruiken deze om zich te identificeren met het SGSN in elke nieuwe toekomstige verbinding die het initieert. Aangezien de PTMSI altijd aan de MS in een gecodeerde verbinding wordt gegeven, zal niemand een IMSI aan de PTMSI buiten in kaart kunnen brengen, hoewel zij soms een duidelijk-tekstbericht met IMSI zien gaan. (Bijvoorbeeld de eerste keer dat een IMSI zich aansluit bij en identiteitsreacties met een IMSI).

PTMSI-hertoewijzing wordt in 3GPP 23.060, paragraaf 6.8, als een standalone procedure uitgelegd. Dit kan ook worden ingevuld als onderdeel van een uplink-procedure om PTMSI- en PTMSI-handtekeningen opnieuw toe te wijzen om de UE identiteit te beschermen. Dit zal netwerk signalering op geen enkele interface verhogen. De hertoewijzing van PTMSI- en PTMSI-handtekeningen is altijd goed, aangezien dit de sleutelidentiteiten zijn die SGSN aan de EU toekent in de eerste registratiestap. Herverdeling van deze op een bepaalde frequentie helpt SGSN de identiteit van de EU met verschillende waarden gedurende langere tijd te verbergen in plaats van slechts één PTMSI-waarde. Verhulling van identiteit heeft betrekking op het verbergen van informatie zoals IMSI en IMEI van de lidstaten, wanneer berichten van/naar de lidstaten nog steeds in gewone tekst worden verzonden en wanneer de encryptie nog niet is begonnen.

## Probleem

In sommige klantennetwerken werd opgemerkt dat sommige zeer belangrijke identiteiten zoals MSISDN/PTMSI tussen verschillende abonnees worden gemengd en in GTPC-signaleringsberichten op de Gn-interface en in Call Data Records (CDR's) worden verstuurd.

Cisco bug-ID's [CSCut62632](#) en [CSCu67401](#) behandelen enkele hoekgevallen van sessieherstel, die de identiteit van de ene abonnee met de andere in kaart brengen. Hieronder staan drie gevallen. Al deze gevallen zijn codevaluatie, analyse van het kwaliteitsborgingsteam en reproductie.

### **Scenario #1 (Dubbele fout op sessgr waardoor de identiteit van de abonnee verloren gaat)**

UE1 - Attach - IMSI1 - Mobile Station International Subscriber Directory Number (MSISDN) 1 - PTMSI1 - SMGR#1

Dubbele moord op sessmgr bijvoorbeeld, SGSN verloor de UE1 details.

UE2 - Attach - IMSI2 - MSISDN 2 - PTMSI1 - SMGR#1

PTMSI1 wordt opnieuw gebruikt voor UE2.

UE1 - Intra RAU - PTMSI1-SGSN verwerkt deze uplink, omdat verificatie voor intra-RAU niet verplicht is.

Dit resulteert in het mengen van records van twee verschillende sessies.

### **Scenario #2 (Transaction Capability Application Part (TCAP) - abort van één sessie die resulteert in het mixen van de identiteit van abonnees)**

UE1 - Attach - IMSI1 - UGL set (TCAP - intern afgebroken als gevolg van een sessmgr-crash)

UE2 - Attach - IMSI2 - UGL verzonden met dezelfde TCAP - OTID

HLR stuurt TCAP - vervolg van eerder verzoek, 's MSISDN van UE1

SGSN werkt in dit geval het onjuiste MSISDN van UE1 met UE2 bij. Dit resulteert in het mengen van records van twee verschillende sessies.

### **Scenario 3 (afbreken van TCAP van één sessie die resulteert in het mixen van de identiteit van de abonnee)**

UE1 - Attach - IMSI1 - SAI verzonden (TCAP - intern afgebroken als gevolg van een sessmgr-crash)

UE2 - Attach - IMSI2 - SAI verzonden met dezelfde TCAP - OTID

HLR stuurt TCAP - vervolg op eerder verzoek, de echtheidscontroles van UE1 (triplets of vijfling)

SGSN actualiseert de onjuiste authenticatie vectoren van UE1 met UE2

Dit resulteert in SGSN waarbij UE1-veters worden gebruikt voor de authenticatie van UE2.

## **Stabilisatie-aanpak**

Als verificatie voor intra-RAU is ingeschakeld of PTMSI-hertoewijzing is ingeschakeld, authenticereert SGN de client met een opgeslagen vectorset. Als de EU anders is dan waarvoor werd opgeslagen, zal UE/SGSN de authenticatiefase niet doorlopen om verder te gaan in het netwerk. Hierdoor wordt de kans kleiner dat de EU in een netwerk blijft met een onjuiste databank. Dit zijn enkele bekende gebieden in de code. De bedrijfseenheid zal meer gevallen blijven analyseren om dit probleem beter te begrijpen.

## Fix Plan

De oplossing van de Cisco bug ID's is een optimale aanpak. Analyseer meer gebieden van code en stel dit in minder dichte knoop voor controle in alvorens u het in een hoge dichtheid knooppunt neemt.

## Configuratierichtsnoeren

Door de mogelijkheid van authenticatie wordt de Gr- en lu-interface-signalering vergroot, aangezien SGSN de verificatiestoornis moet halen die is ingesteld in het huislocatieregister (HLR) en aanvullende verificatieprocedures moet uitvoeren om toegang te verkrijgen. Exploitanten moeten ervoor zorgen dat ze frequentiewaarden kiezen die het netwerk minder beïnvloeden.

GPRS Mobility Management (GMM)/Mobile Application Protocol (MAP) Key Performance Indicators (KPI's) zijn belangrijk om te analyseren voordat u de frequentiewaarden voor elke procedure afleidt. Op basis van de KPI's, controleer de procedure die hoog uitvoert. Stel voor deze procedure een hoge frequentie-waarde in. (Dit is de manier om elke parameter te verfijnen op basis van een netwerk aanroep model).

Een ideale manier om deze parameters te configureren is waarden in te stellen op bladeren, maar niet bij de wortel van de boom. Afbeelding 2 legt bijvoorbeeld de configuratieboom voor de verificatie uit. Exploitanten kunnen ervoor kiezen de waarde op een lager niveau in te stellen, zoals hier wordt getoond, in plaats van de configuratie van "voor echt maken" direct.

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

Het is altijd goed om hoge frequentiewaarden (eenheden als 10s) in te stellen en dan Gr/lu interface signaleringsdrempels te controleren. Als signalering binnen de grenzen goed is, definieert u waarden totdat signalering een veilige plaats in de buurt van drempels bereikt die de operator voor hun netwerken zou willen instellen.

Stel de frequentie van de verschillende procedures in 20/30 in en breng ze terug naar 5-10 met nauwgezette controle op het externe interfaceverkeer. Deze overbelasting moet de impact op de koppeling en het geheugen van de opslagprocessor met deze overbelasting controleren.

Aanwijzingen voor ondertekening door PTMSI en PTMSI zullen niet direct de piek in signalering veroorzaken, maar het is altijd belangrijk om hoge-frequentiewaarden in te stellen zodat PTMSI's beschikbaar zijn met sessor gevallen (wat zelden gebeurt). Het wordt niet aanbevolen om PTMSI voor elke uplink-procedure van de EU te veranderen, aangezien dit niet de beste praktijk is. Een waarde van 10 is misschien fatsoenlijk. Na al deze wijzigingen is het belangrijk dat het systeem wordt gecontroleerd en aan standaardgezondheidscontroles wordt onderworpen.

## Als voorbeeld:

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
```

## Problemen oplossen

Wanneer verificatie moet worden uitgevoerd of een PTMSI- of PTMSI-handtekening moet worden toegewezen, worden debug-logbestanden afgedrukt om op te nemen waarom de procedure is voltooid. Dit helpt bij het oplossen van problemen in geval van verschillen. Deze logbestanden omvatten de configuratie vanuit een c-profiel en de huidige waarde van alle tellers, en de beweging van de besluitvormingslogica via de verschillende configuratie en tellers. Tevens kunnen de huidige tegenwaarden per abonnee worden bekeken met de opdrachten **alleen** van de **show-abonnees** of **alleen** de **abonnees gprs-only** weergegeven.

Hiervan wordt een steekproefuitvoer voorzien. De huidige tellers en de laatste geauthentiseerde timestamp worden toegevoegd aan de opdracht **van de showabonnees** volledige uitvoer.

```
[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:
.
.

```

Als de kwestie in het netwerk wordt gezien, voer deze opdrachten in om informatie te verzamelen voor de bedrijfseenheid om het probleem verder te analyseren:

```

show subscribers gprs-only full msisdn <msisdn>
show subscribers gprs-only full imsi <imsi>
show subscribers sgsn-only msisdn <msisdn>
show subscribers sgsn-only imsi <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.

```

## Risico's

Toegenomen signalering naar Gr/Iu-interfaces plus een klein intern proces (linkor) CPU-effect als

u te vaak voor authenticatie zorgt.

## Complexe

Alle opdrachten bevinden zich in de configuratie/aanroep-control-profielmodus en zijn van toepassing op de exploitatierechten. Een momentopname van de opdrachten in het c-profiel is als volgt:

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]}
```