3GPP TSG GERAN/SA WG3 ad hoc **Tdoc S3z010062**
Madrid, Spain 27 April 2001

Source: **Siemens**

Title: **Iur-g related security issues**

Agenda item: 5.4

Document for: **Discussion and Decision**

1 Introduction

During the last GERAN meetings the Iur-g interface (interface between GERAN BSCs and interface between GERAN BSC and UTRAN RNC, see [1]) was discussed. The Iur-g is an interface containing a control plane and no user plane and will allow the definition of GERAN registration areas (GRAs) exceeding the area served by one BSC. Then the benefit of reducing location management messages (GRA_Update) can be achieved for MSs in RRC_GRA_PCH state (in this state the mobile has only a logical connection towards the "serving" BSC but is not consuming any physical resources).

2 Security related issues

Assuming a GRA exceeding the BSC area and a MS in RRC_GRA_PCH state, then this MS can move within the GRA without performing location management procedures (except e.g. periodic location updates). If the MS wants to send user data or was paged then it has to send a Cell Update message. This Cell Update message might be received by a new BSC (serving a part of this GRA), which is not the serving BSC initially serving the MS before the transition to RRC_GRA_PCH state. Therefore the new BSC has to deliver the Cell Update message to the serving BSC via Iur-g to trigger a Relocation procedure (as there is no user plane on Iur-g a Relocation procedure has to be performed towards the new (controling) BSC). A detailed discussion can be found in [2].

An open issue is to identify the earliest possible instant for triggering the Relocation procedure taking into account that CN procedures shall not be changed and security requirements are fulfilled.

Another open issue is that a CN initiated paging (triggered from the CS domain) might be lost. In [3] a possible solution for the identified CN initiated paging problem can be found. The following discussion is based on this proposal with some changes with the main focus on security issues:

Starting point in Figure 1 is a MS in RRC_GRA_PCH state initially served by the *Serving* BSC but now moved to the area served by the other BSC (named *Controling* BSC, because the term "Drift" BSC is not correct as there is no user plane on Iur-g). This MS has a logical connection to the Serving BSC and towards the PS-domain a Iu-ps connection is established for this MS, but the MS is not consuming any services from the CS-domain.

1. A MTC has to be delivered to the MS, therefor the MSC1 initiates the Paging procedure by sending a RANAP Paging message to the Serving BSC (message (1) in Figure 1). Note that the RANAP Paging message is sent using connectionless SCCP service and no Iu-cs signaling connection is established so far.
2. As the RANAP Paging message contains the "Permanent NAS UE Identity" IE (IMSI), the serving BSC will recognize that this specific MS is in RRC_GRA_PCH state and has to be paged in the whole GRA. Therefor the paging request is delivered by the Serving BSC via Iur-g to all BSCs assigned to that GRA.
3. All BSCs receiving the RNSAP Paging message will page the MS.
4. The MS answers the paging by sending a CELL UPDATE message and the NAS-paging response to the Controling BSC (In UTRAN this information is sent using more than one RRC message, in GERAN there might be a single message possible).
5. The Controling BSC collects the received information (CELL UPDATE message and NAS-Paging response) and sends it to the Serving BSC via Iur-g using RNSAP UL Signaling Transfer message.
6. The Serving BSC sends a RANAP INITIAL UE MESSAGE to MSC1 which contains the NAS-Paging response.

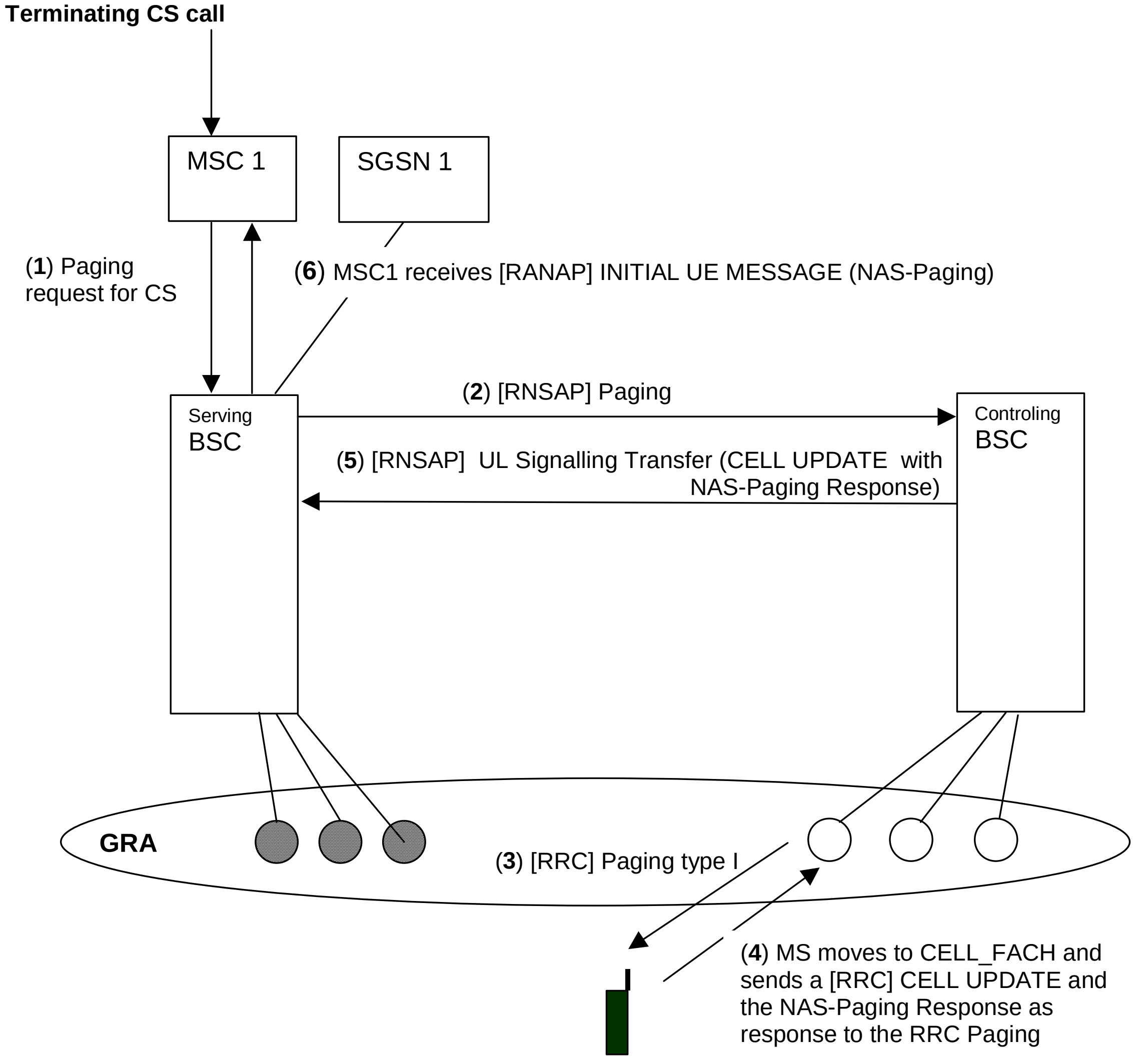
Terminating CS call
MSC 1
SGSN 1
(1) Paging request for CS
(6) MSC1 receives [RANAP] INITIAL UE MESSAGE (NAS-Paging)
(2) [RNSAP] Paging
Serving BSC
Controling BSC
(5) [RNSAP] UL Signalling Transfer (CELL UPDATE with NAS-Paging Response)
GRA
(3) [RRC] Paging type I
(4) MS moves to CELL_FACH and sends a [RRC] CELL UPDATE and the NAS-Paging Response as response to the RRC Paging

Figure 1: NAS-Paging response piggy-packed on the CELL UPDATE message (based on Fig.5 of [3])

With message 6 the SCCP connection establishment between Serving BSC and MSC1 is initiated.
To complete the CS call establishment a Relocation procedure has to be executed (including the completion of the Cell Update procedure) due to the fact that no dedicated resources can be allocated on Iur-g. Also NAS procedures have to be considered, this is not depicted in Figure 1, but some of the issues are listed below:

2.1 General issues

- MSC1 has to complete the SCCP connection establishment by sending the SCCP CC message (possibly) containing a RANAP message, to complete the establishment of the Iu-cs signaling connection.
- MSC1 does not know whether the MS is consuming resources of Serving BSC or a different Controling BSC (the Iur-g interface is not visible to the CN). Therefor MSC1 will initiate the RANAP RAB Assignment procedure to request the establishment of the user plane. (If at the same instant the Serving BSC is allowed to initiate the Relocation procedure, the behaviour of RNC could be applied: i.e. in UTRAN the RNC has to coordinate the two initiated procedures by terminating one of them and further processing the other – a detailed description can be found in [4]).
- It has to be checked whether the NAS-Paging response can be transported piggy-packed on the CELL UPDATE message (message 5 in Figure 1).

2.2 Security related assumptions

- MSC1 may execute the Authentication and Key Agreement procedure to be able to check, whether the TMSI (received in the NAS-Paging response) belongs to the correct subscriber. This requires NAS signaling between MSC1 and the MS, and is currently performed in UTRAN using dedicated resources on Iur.
- MSC1 has to send the RANAP Security Mode Command to the Serving BSC before a Relocation procedure is allowed.
- The RRC CELL_UPDATE_CONFIRM message has to be protected because security parameters can be delivered with this message. This message has to be transmitted to terminate the Cell Update procedure.

2.3 Additional questions

- Has the NAS-Paging response to be ciphered and integrity protected (related to messages 4 and 5 in Figure 1) ? If yes, further analyses are needed to identify a solution, how to transport a ciphered message towards Serving BSC without having security related information within Controling BSC.

3 Conclusion

This contribution lists some security related issues (besides general ones) which are related to the intra GERAN Iur-g interface as well as to the inter-RAN Iur-like interface. No concrete solution is provided, but some of the issues listed in section 2 have to be discussed / answered. It is proposed that the Joint GERAN / SA3 Ad hoc meeting agrees on the security related assumptions listed in section 2.2 and discusses and possibly provides answers to the issues raised in section 2.3.

4 References

[1]: TS 43.051:	GERAN Overall description – stage 2
[2]: GAHW-010150:	Inter-RAN I_{ur}–like interface (Joint GERAN/SA2/RAN3 meeting)
[3]: GAHW-010134:	Iur-g with no user plane (Nortel Networks)
[4]: TS 25.413:	UTRAN Iu interface RANAP signalling