**Technical Specification Group GERAN** *TSGG#4(01)0570*
**Meeting #4, Biarritz, France, 2-6 April 2001** **Agenda Item: 4.1**
3GPP TSG-SA3 Ad Hoc on 'Network Domain Security' S3z010046
Madrid 23-24 April, 2001

3GPP TSG SA WG3 Security — S3#17 S3-010135
27 February - 02 March, 2001
Gothenburg, Sweden

**Title:** **Reply to LS on integrity protection for GERAN**

**Source:** **TSG SA WG3**
**To:** **TSG GERAN ad hoc**
**Cc:** **TSG GERAN**
**Contact Person:** **valtteri.niemi@nokia.com**

S3 thanks GERAN ad hoc for their LS on integrity protection for GERAN (GAHW#4(01)0102). In this reply we follow the same section numbering than in the original LS.

**1. Integrity protection for RRC messages**

S3 is happy to see that the list of protected RRC messages is as extensive as possible.

**2. Integrity protection for RLC/MAC messages**

Control messages dealing with resource allocation should be integrity protected to prevent any possibilities to steal bandwidth. That is why the referred RLC/MAC control messages should be integrity protected unless this implies major re-design of the protocols.

**3. Implications of the introduction of integrity protection in GERAN**

S3 acknowledges there are potentially harmful implications of adding integrity protection to GERAN because of segmentation issues. If these implications (e.g. in the form of delays or overhead) are shown to be significant, S3 may consider shorter integrity protection checksums (MAC-I) as a solution in the critical cases. Anyhow, as many bits of MAC-I should be appended to the message as fits without forcing segmentation, minimum number of added bits of MAC-I being 8 (while maximum is naturally 32). Additionally, S3 would like to check all these critical cases from the security point of view. It should be noted that there are some messages like the SECURITY MODE COMMAND for which the full length MAC-I is essential.

Integrity protection is as much needed for uplink control messages as for downlink control messages. It should protect against both "false network" and "false MS" cases.

**4. Misc.**

For the miscellaneous points, S3 concludes:

- No issues have been identified with the setting where control BSC differs from the serving BSC.
- A suggestion to reduce the harmful impact of integrity protection is described in the section above.
- The fact that some control messages read by several MSs cannot be ciphered is confirmed by S3.

**5. GERAN meeting schedule**

S3 thanks for the proposal about S3/GERAN joint session on the integrity protection. A few possible ways to organize the joint meeting are listed below (in the order of preference from S3 point of view):

- Attached to another GERAN joint meeting in Helsinki in 10-11. April
- During GERAN plenary 2-6. April in Toulouse
- Attached to a S3 ad hoc in Madrid 24-26. April
- Standalone meeting on the end of March, e.g. in Helsinki
- During GERAN ad hoc in Seattle 7-11. May (this is quite late).

---

**Title:** **LS on integrity protection for GERAN**

**Source:** TSG GERAN ad hoc #4[1]
**To:** TSG SA WG3
**Cc:** TSG GERAN
**Date:** 16 February 2001

**Contact person**: José Luis Carrizo Martínez
E-mail: jose-luis.carrizo@vodafone.co.uk
Tel: +44 1635 676093

---

**1. Integrity protection for RRC messages**

During the TSG GERAN ad hoc meeting #4, integrity protection for GERAN has been discussed. With the working assumption that integrity protection is to be used in GERAN, and in order to satisfy the principle of offering a similar level of security in UTRAN and GERAN, it is the working assumption that integrity protection would be applied to most of the GERAN RRC messages. Some exceptions are foreseen, although they are aligned with UTRAN's exceptions. These exceptions are as follow:

- Paging Request Type 1-3
- RRC Connection Request
- RRC Connection Setup
- RRC Connection Setup Complete
- RRC Connection Reject
- System Information Type 1-20

TSG GERAN (ad hoc) will inform SA3 on any modifications to the list above.

**2. Integrity protection for RLC/MAC messages**

As a difference with UTRAN, GERAN has located part of the RRC functionality for shared channels at RLC/MAC level, for backward compatibility reasons. Thus TSG GERAN ad hoc foresees that integrity protection may also apply to some RLC/MAC control messages. An initial list of RLC/MAC control messages that should be integrity protected is:

- Packet Uplink Assignment
- Packet Downlink Assignment
- Packet Timeslot Reconfigure
- Packet TBF Release
- Packet Cell Change Order

TSG GERAN (ad hoc) will inform SA3 on any modifications to the list above.

---

[1] Alcatel, AT&T, Ericsson, Cingular, Interdigital Communications, Lucent Technologies, Mannesmann, Mitsubishi, Motorola, Nokia, Nortel Networks, Siemens, Telia, Vodafone.

## 3. Implications of the introduction of integrity protection in GERAN

The companies represented in TSG GERAN ad hoc are currently engaged in a more detailed study of the possible harmful implications of adding integrity protection to GERAN, i.e. whether there is an actual decrease in the performance of the procedures performed over the radio interface. Note that some of the candidate messages to be integrity protected are sent *quite frequently* during a session, causing potentially a significant overhead.

As well as their frequency, a calculation of the size of the messages that need to be integrity protected is being done in order to determine whether the addition of the MAC-I will cause segmentation. This is particularly important due to the restrictions regarding segmentation that RLC/MAC has. Currently, the segmentation is limited to two radio blocks for control messages in the downlink. The situation is even more critical in the uplink, where segmentation functionality is lacking. Should integrity protection force messages to span over three radio blocks in the downlink or segmentation be necessary in the uplink, a redesign of RLC/MAC would be then needed. Further, TSG GERAN ad hoc would like to know if integrity protection is equally important in the uplink and the downlink.

## 4. Misc.

TSG GERAN ad hoc would also like to communicate to SA3 the following points:

- In GERAN, control signalling (i.e. RRC and RLC/MAC signalling) may be performed from a controlling BSC which is not the same as the serving BSC. It remains to be analysed whether there are any issues if integrity protection is performed when the controlling and serving BSC are not the same.
- It would be desirable to reduce the impact of integrity protection. TSG GERAN (ad hoc) would welcome any suggestions from SA3 as to how this could be achieved.
- Information Elements in the payload of some control messages addressed to a particular MS will be read by other MSs. TSG GERAN ad hoc would like confirmation of the following consequences:
  - Ciphering of these RLC/MAC control messages is not possible.
  - These messages can still be integrity protected.

## 5. GERAN meeting schedule

As stated above, individual companies are currently performing some investigations. The results of these investigations may affect the way integrity protection is introduced in GERAN and will be communicated to SA3. However, it is felt that a better dialog could be achieved by organising a joint SA3/GERAN session on this particular issue. Regarding whether this session would be within an SA3 or a TSG GERAN ad hoc meeting, or whether standalone one should be set up, TSG GERAN ad hoc has no preference. The meeting calendar for TSG GERAN is included below for information. Note that TSG GERAN is working on features for an “early Release 5” —one of which should be integrity protection— which aim to be completed in June 2001.

| Dates | Meeting | Place | Host |
|---|---|---|---|
| 19 Mar 2001 | Teleconference on RRC | N/A | Ericsson |
| 20 Mar 2001 | Teleconference on RRC | N/A | Ericsson |
| 2 – 6 Apr 2001 | TSG GERAN #4 | Toulouse, France | Nortel Networks |
| 7 – 11 May 2001 | GERAN ad hoc on R4 and beyond #5 | Seattle, USA | AT&T |
| 28 May – 1 Jun 2001 | TSG GERAN #5 | Chicago, USA | Motorola, SBC |
| 25 – 29 Jun 2001 | GERAN ad hoc on R4 and beyond #6 | [Europe] | TBD |