
Technical Specification Group GERAN

TSGG#4(01)0573

Meeting #4, Biarritz, France, 2-6 April 2001

Agenda Item: 4.1

3GPP TSG GERAN ad hoc meeting no 4
Sophia-Antipolis, France
12 – 16 February 2001

GAHW#4(01)0102

Title: LS on integrity protection for GERAN
Source: TSG GERAN ad hoc #4¹
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.

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

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.

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:
 - Cipherring 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