3GPP TSG GERAN/SA WG3 ad hoc **version 0.0.1**
Madrid, Spain
27 April 2001

Source: **Secretary (Maurice Pope, MCC)**

Title: **Draft report version 0.0.1**

Document for: **Information (NOT FOR COMMENT AT THIS TIME)**

---

1 Opening of the meeting

The Chairman, Marc Blommaert, opened the meeting, welcomed delegates and provided the domestic arrangements.

2 Approval of the agenda, organisation and objective of the meeting

TD S3z010014 provided that agenda for the meeting which was approved.

The documents were allocated to their appropriate agenda items.

The Chairman outlined that this was a GERAN meeting and output to SA WG3 would need to be done formally by LS.

The objectives of the meeting were:

- To conclude the specification of ciphering in GERAN 'Iu' mode. (proposed CR)
- To progress the stage 2 work on integrity protection in GERAN 'Iu' mode. (set of working assumptions).
- To study/progress/solve other security related problems affecting GERAN (e.g. use of the Iur-g interface)

3 Letters from other groups

The LSs from other groups were considered with other related contributions under their appropriate agenda item.

4 Status of the Work Item

TD S3z010042 GERAN security ~ WI status (presentation slides). This was presented by Vodafone and provided the status, open issues and the expectations from the meeting. Release 5 integrity protection had been worked on for a few months, but problems arose and SA WG3 were asked for this joint meeting to help progress the work.

Problems include, that there were vague requirements, the ciphering has not progressed over last meetings; although it was thought to be near completion. Open issues included ciphering and integrity protection. Other open issues were LCS and use of the Iur-g interface.

GERAN would like to obtain from this meeting: Clarification of requirements; Completion of ciphering, i.e. production of CR to stage 2; Progress integrity protection, providing a set of working assumptions. Also, if possible to progress other issues, e.g. LCS and use of the Iur-g

A request for advice from SA WG3 on the use of IMSI and TMSI was received, when IMSI can be used and when TMSI is used. It was clarified that the TMSI should always be used, and it was also suggested the solution as used in UTRAN should also be considered.

Requirements on integrity protection: GERAN are working on the assumption that S3 want to align GERAN and UTRAN security. SA WG3 have only said this in LSs and do not cover GERAN security in the specifications. It is the wish that GRRAN Security should be aligned as closely as possible to the UTRAN Security. It was explained that the approach for UTRAN is to integrity protect the Control Plane and not the user Plane, in order to protect against attacks on the signalling over the air. This is done to protect against more sophisticated attacks, which may be possible in the future, in order to try to avoid continuous patching up of the system, which would be expensive.

It was clarified that ciphering is not mandatory for UTRAN, but integrity protection is. Integrity protection should also be mandatory in GERAN, also recommended that ciphering is optional, unless there are no restrictions in areas where GERAN will be used.

It was stated that there are problems in integrity protecting all messages in GERAN as the architecture is not the same as UTRAN, and clarification of which messages are necessary to protect was requested. It was clarified that at least the same messages as must be protected in UTRAN should be considered. This was discussed further based on other contributions.

The presentation was then noted. The agreed working assumptions were provided in TD S3z010065.

TD S3z010043: Current status of stage 2. This was presented by Vodafone, and requested conclusions are aimed for at this meeting:

1 A decision be made at this meeting as to where the stage 2 description of the GERAN security should be, along whit the scope if it is to be split between different specifications.
2 SA3 confirm the validity of the working assumptions regarding ciphering; the remaining open points should be closed at this meeting.
3 The sub-clause in the stage 2 is enhanced so that other issues regarding GERAN security are dealt with; these at least include integrity protection.
4 The scenarios where the Iur-g interface is used are studied from the security point of view so that security matters can be considered by GERAN during the ongoing work on this interface.

It was recommended that the stage 2 description of GERAN Security is keep it in 43.051 at present, and to include a reference to 43.051 in 33.102, until the GERAN Stage 2 work is stable enough for a decision to be made to move the architectural aspects of GERAN Security into 33.102. There were no objections to this, and it was taken as a **working assumption** of the joint meeting (see TD S3z010065 for agreed text).

Other items (ciphering, integrity protection, Iur-g) were dealt with as the subject of other contributions.

TD S3z010046 SA WG3 LS to GERAN: Reply to LS on integrity protection for GERAN. This was considered during the discussions of TD S3z010016 and noted.

TD S3z010045: GERAN LS to SA WG3: LS on integrity protection for GERAN. - this was included in text of TD S3z010046 and noted.

TD S3z010015: LS on LCS message security from SA WG3 drafting group. This was not handled at the meeting due to lack of time.

5 Technical discussion

5.1 Requirements

5.2 Ciphering

5.3 Integrity protection (General, RRC, RLC/MAC)

TD S3z010044: On integrity protection and the effects of additional segmentation. This was introduced by Vodafone and the SA WG3 details were highlighted. It had been suggested that adding integrity protection to GERAN messages may cause segmentation, which can give performance problems. This provided the

results of a study that Vodafone made and concluded that the benefits of integrity protection outweigh the side effects of possible (additional) segmentation and it is requested that the use of integrity protection in GERAN be adopted as the working assumption, unless other significant impacts are found. Further study is felt to be needed before this is ratified for the case of RLC/MAC control messages.

The document was noted (see TD S3z010065 for agreed working assumptions).

TD S3z010037: GERAN RRC Messages and Integrity Protection. This was introduced by Nokia and lists the RRC messages and the applicability of and criticality of integrity protecting each message.

There was some discussion on the messages that were not protected, e.g. IMMEDIATE_ASSIGNMENT messages, which were protected in UTRAN. These messages could not be protected as the user was not known at the time. For immediate assignment, however, there is no further interaction after this. This was considered a significant threat by SA WG3.

It was noted that the question of protection of Immediate assignment procedures should be provided by GERAN to SA WG3 for analysis of the threat scenarios and possible solutions. GERAN need to clearly describe the scenario in order that SA WG3 can understand the problem. The immediate assignment set up procedure was outlined and discussed, where messages are exchanged before the integrity checking is done and the user either provided with service or rejected. This was the same set-up procedure as for the UTRAN set-up. The radio bearers are established after authentication, and this is integrity protected. The problem is for non- RT services when the Radio bearer is established but there are no physical resources allocated, so that the UE sends the service request, which does not include the ID. The UE sends the ID it has received from the GERAN (8-11 bits), which could be guessed by an attacker (there are only 256 possible IDs).

Exceptions to the list in table 9.1 were accepted as a current assumed status, except for the IMMEDIATE-ASSIGNMENT messages which need to be checked against the methods used in UTRAN.

Note 3 was considered as FFS, and replaced by the working assumption below.

The following **working assumption** on RRC message integrity protection was established and agreed and included in TD S3z010065.

<Add Working Assumption here?>

It was asked whether the draft CR to 25.331 could be updated to include the results of the discussions with the endorsement of the joint meeting - with the knowledge that the draft CR would be available for comment by SA WG3. There was no opinion on this, as draft CRs can be produced by companies, and their correctness can be discussed in relevant WGs before approval.

TD S3z010038: Simulation results on RLC/MAC signalling. This was presented by Ericsson and discusses some of the issues raised in GERAN on integrity protection for RLC/MAC signalling. It provides simulation results on the impact of integrity protection and reports that difficult to conclude on the frequency of RLC/MAC messages and the real impact of integrity protection, but it is clear that the introduction of delayed TBF release will reduce the amount RLC/MAC signalling and therefore also the impact of integrity protection on the system performance.

It was concluded that more work was needed in order to identify whether there will be any security questions to SA WG3. However, it was also agreed that the issue needs to be addressed as it will not be possible to produce simulation results for all possible cases. The contribution was then noted.

TD S3z010016: Integrity Protection at RLC/MAC. This was introduced by Nokia and analyses the impact of integrity protection on the segmentation mechanism in GERAN.

The paper addressed the extreme cases for the different messages (maximum size), but did not address the cases where the authentication code for integrity protection causes segmentation (i.e. segments one into two radio blocks). The status of Packet Cell Change Order was left open, however was thought that a variable size MAC-I with a minimum guaranteed size can be introduced. The same would apply to Immediate Assignment for TBF establishment.

The contribution concluded that for the scenarios analysed, no major redesign of the RLC/MAC protocols is needed for supporting integrity protection of RR flavoured RLC/MAC control messages, as the existing segmentation mechanism is enough. A variable sized, with guaranteed minimum, MAC-I was suggested to be introduced, with the introduction on a 32-bit MAC-I, if the segmentation overhead is acceptable (this needs to be studied).

Note: SA WG3 recommended the use of variable MAC-I, with a minimum MAC-I length of 8-bits in TD S3z010046.

It was reported that variable-length MAC-I also has an overhead implication to signal it's length, alternatively, the MAC-I could be set to exactly fit the length of the message and then the length be derived.

A **working assumption** was agreed that a that GERAN should specify a variable length MAC-I, with length indicator, where the maximum number of MAC-I bits would be used in messages (up to 32 bits), with a minimum size of 8 bits in order to avoid segmentation where possible. SA WG3 were asked to specify the mechanisms for dealing with truncated MAC-I (see TD S3z010065 for agreed text).

The RLC/MAC messages in this contribution were agreed as a **working assumption**. RLC/MAC messages will have a fixed MAC-I of 32 bits. (see TD S3z010065 for agreed text).

<MARC - I think I have reversed RRC and RLC/MAC discussions here - PLEASE CHECK>

There was some discussion over the validity of using a variable length field, as the overall security level of the system will be down to the weakest link - i.e. 8 bit MAC-I in this case. This concern over the added complexity was noted.

TD S3z010063: Some GERAN-specific security issues. This was presented by Alcatel, The issues not covered already by agreements were discussed:

Ciphering of layer 2 signalling

There is no possibility for the source BSS to control the integrity protection when the user is in a drift BSS. It was suggested that when moving from a BSS, a Cell update is performed, triggering update location. During this procedure the assignment messages are not protected. This is seen by Alcatel as a security void, even though it is limited.

The conclusion of discussions on this topic were covered by the working assumption on integrity protection (TD S3z010065).

Integrity protection of RLC/MAC control messages.

The user plane is used in UTRAN but this is not possible in GERAN. As this was an open issue within GERAN, the proposals here should be further discussed in GERAN.

The document was then noted.

5.4 Other

TD S3z010062: Iur-g related security issues. This was presented by Siemens. It reports that assuming a GRA exceeding the BSC area and a MS in RRC_GRA_PCH state, then an MS can move within the GRA without performing location management procedures (except e.g. periodic location updates). There were 2 open issues:

- 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.
- a CN initiated paging (triggered from the CS domain) might be lost. A possible solution for the identified CN initiated paging problem can be found in GAHW-010134. The following discussion is based on this proposal with some changes with the main focus on security issues:

  Security-related assumptions made in the contribution were:

- 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 signalling 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.

SA WG3 were asked whether the NAS-Paging response to be ciphered and integrity protected. If so, further analyses are needed to identify a solution, how to transport a ciphered message towards Serving BSC without having security related information within Controlling BSC.

In summary, the 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 above and discusses the issues raised.

It was considered to be an architecture-related problem, which SA WG3 would look at when there are stable architectural solutions available.

There was some discussion between GERAN delegates on these issues, but the SA WG3 delegates needed time to study the issues in order to understand the problem and provide advice. It was agreed that this should be further discussed in GERAN and provided as a LS to SA WG3. This was added to the list of open issues in TD SP-01065.

The document was therefore noted in this meeting.

6 Output of the meeting

6.1 Preparation of the results

The results, agreements and working assumptions from the meeting were captured in a document which was reviewed and modified on-line, the final text was provided in TD S3z010065 which was agreed.

6.2 Letters to other groups

It was agreed that TD S3z010065 (see agenda item 6.1) would be used for input to SA WG3 and GERAN.

7 Closing of the meeting

The Chairman thanked delegates for their co-operation and hard work during the meeting and the Host (Ericsson) for the meeting facilities and closed the meeting.

Annex A: List of attendees at the SA WG3/GERAN joint ad-hoc meeting

Name			Company	e-mail	3GPP Member	
Mr.	Stephen	Billington	Hutchison 3G UK Limited	adrian.escott@hutchison3G.com	ETSI	x
Mr.	Marc	Blommaert	SIEMENS ATEA NV	marc.blommaert@siemens.atea.be	ETSI	x
Ing.	Krister	Boman	Telefon AB LM Ericsson	krister.boman@emwericsson.se	ETSI	x
Mr.	Daniel	Brown	Motorola Inc.	adb002@email.mot.com	T1	x
Ms.	Tao	Bu	NOKIA Corporation	tao.bu@nokia.com	ETSI	x
Mr.	David	Castellanos	Telefon AB LM Ericsson	david.castellanos@ece.ericsson.se	ETSI	x
Ms.	Chen	Lily	Motorola Inc.	Lily.chen@motorola.com	T1	x
Dr.	Adrian	Escott	Hutchison 3G UK Limited	adrian.escott@hutchison3G.com	ETSI	x
Mr.	Louis	Finkelstein	Motorola Inc.	louisf@labs.mot.com	T1	x
Mr.	Guenther	Horn	SIEMENS AG	guenther.horn@mchp.siemens.de	ETSI	x
Mr.	Peter	Howard	VODAFONE Group Plc	peter.howard@vf.vodafone.co.uk	ETSI	x
Mr.	Mathias	Johansson	Telefon AB LM Ericsson	mathias.p.johansson@era.ericsson.se	ETSI	x
Mr.	Michael	Marcovici	Lucent	marcovici@lucent.com	T1	x
Mr.	Vincent	Muniere	ALCATEL S.A.	Vincent.Muniere@alcatel.fr	ETSI	x
Mr.	Valtteri	Niemi	NOKIA Corporation	valtteri.niemi@nokia.com	ETSI	x
Mr.	Bradley	Owen	Lucent Technologies Network Systems UK	bvowen@lucent.com	ETSI	x
Mr.	Olivier	Paridaens	ALCATEL S.A.	olivier.paridaens@alcatel.be	ETSI	x
Mr.	Maurice	Pope	ETSI	maurice.pope@etsi.fr	ETSI	x
Mr.	Guillaume	Sebire	NOKIA Corporation	guillaume.sebire@nokia.com	ETSI	x
Mr.	Hugh	Shieh	AT&T Wireless Services, Inc.	hugh.shieh@attws.com	T1	x
Mr.	Jean-Michael	Traynard	Siemens AG	jean-michael.traynard@icn.siemens.de	ETSI	x

registered but not signed in as attending:

Mr.	José Luis	Carrizo Martínez	VODAFONE Group Plc	jose-luis.carrizo@vodafone.co.uk	ETSI	
Mr.	Vineet	Kumar	Intel Sweden AB	vineet.kumar@intel.com	ETSI	
Mr.	Tomi	Mikkonen	SSH Communications Security Corp	tomi.mikkonen@ssh.com	ETSI	
Mrs.	Susana	Ochoa	AIRTEL Movil SA	sochoag@airtel.es	ETSI	
Mr.	Lee	Valerius	NORTEL NETWORKS (EUROPE)		ETSI	