3GPP TSG SA WG3 Security — S3#16 **S3-000651**

28-30 November, 2000

Sophia Antipolis, France

3GPP TSG GERAN **GP-(00)0588**
Meeting no 2 **Agenda item 7.3**
Norrtälje, Sweden
6 – 10 November 2000

3GPP TSG GERAN Adhoc #2 **Tdoc GERAN Adhoc 0114/ 00**
Münich, Germany **Agenda item 7.2**
9th-13th October 2000

Title:	**Draft LS on Integrity Protection in GERAN**
Source:	**TSG GERAN AdHoc #2**[1]
To:	**TSG SA3**
Cc:	**-**

Contact Person:

Name:	**Guillaume SEBIRE**
E-mail Address:	**guillaume.sebire@nokia.com**
Tel. Number:	+358 40 569 2657

TSG GERAN is studying how to provide in GERAN the same security level as in UTRAN, and therefore thanks TSG SA3 for their valuable inputs and advices on this issue. In this perspective, the working assumption on ciphering for GERAN from TSG SA3 was studied and also adopted as a working assumption at TSG GERAN#1.

Now TSG GERAN has started to consider the introduction of integrity protection into the GERAN framework for R4. An initial study of the impacts was made in the attached contribution: GAHW-000053. Based on this document TSG GERAN concluded that the overall impact is very difficult to assess due to the complexity of the procedures involved and the high number of optional information elements in some of the RRC messages (e.g. HANDOVER COMMAND). Nevertheless TSG GERAN agreed that when causing message segmentation, integrity protection would induce a significant and likely unacceptable overhead over the air interface.

Therefore TSG GERAN considers the following alternatives for future work, on which guidance/advice is kindly asked from TSG SA3:

- To adapt the method of UTRAN for GERAN, by defining a Message Authentication Code smaller than 32 bits in GERAN in order to limit the overhead

- To set Integrity Protection as optional, i.e. to be set on or off by the network operator

- Not to include integrity protection in GERAN

TSG GERAN would be grateful if TSG SA3 could provide an answer for TSG GERAN#2 (6th-10th November, 2000), TSG GERAN AdHoc #3 (11th-15th December, 2000).

[1] Alcatel, AT&T, Cingular (SBC/Bellsouth), Comsys, DSPC/Intel, Ericsson, France Telecom, Interdigital Communications, Lucent Technologies, Motorola, Nokia, Nortel Networks, Sharp Labs, Siemens, Telia, Vodafone

3GPP TSG GERAN AdHoc #2
Münich, Germany
October 9th-13th, 2000

Tdoc GERAN AdHoc GAHW 000053
Agenda Item 6.1.3

Source: Nokia

On Integrity Protection for GERAN

1. INTRODUCTION

Although a working assumption for ciphering in GERAN is defined [1], it is still open whether integrity protection will be supported by GERAN. This paper for discussion analyzes the impacts of integrity protection when imported from UTRAN to GERAN.

2. PRINCIPLE OF INTEGRITY PROTECTION

2.1 Integrity Protection

Integrity consists in the protection of data from accidental or intentional change, deletion or substitution (OSI). In order to provide data integrity protection on the network access link, the following security features must be available [1]:

- *integrity algorithm agreement*: the property that the MS and the Serving Network (SN) can securely negotiate the integrity algorithm that they shall use subsequently;

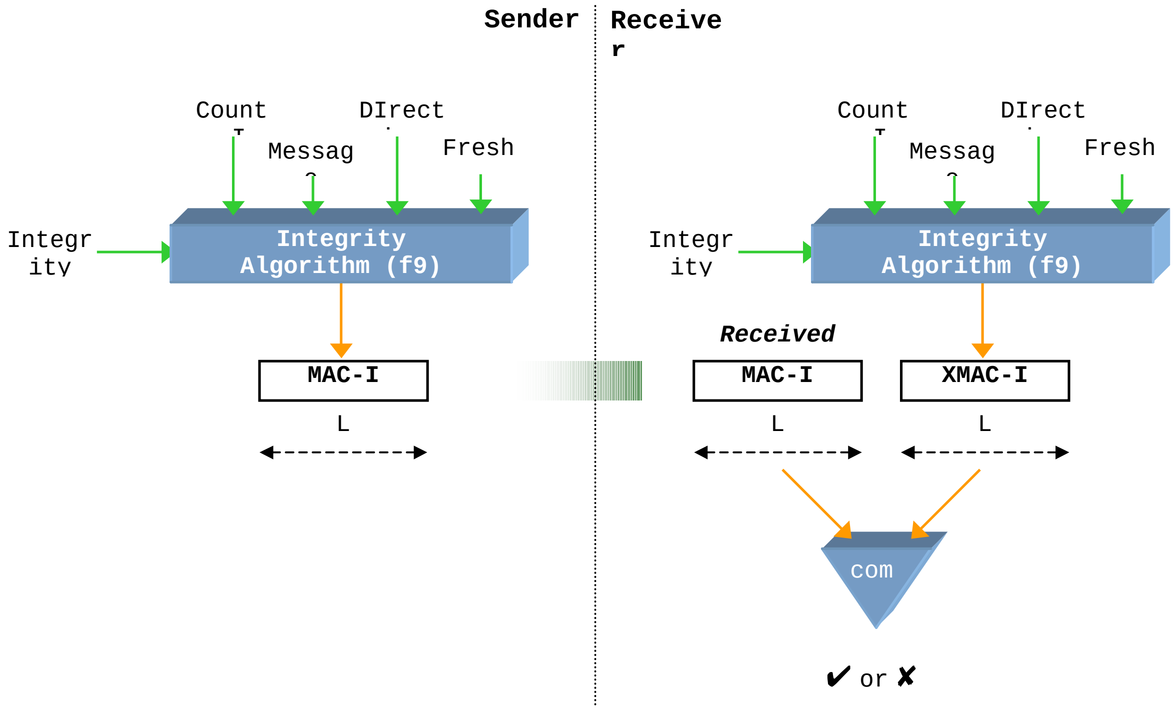
- *integrity key agreement*: the property that the MS and the SN agree on an integrity key that they may use subsequently;

- *data integrity and origin authentication of signalling data*: the property that the receiving entity (MS or SN) is able to verify that signalling data has not been modified in an unauthorised way since it was sent by the sending entity (SN or MS) and that the data origin of the signalling data received is indeed the one claimed;

2.2 Principle

In UTRAN, *all control signalling information elements* (except e.g. RRC Connection messages, Broadcast information) exchanged between MS and network are integrity protected as described in the figure below. Integrity protection is applied at the RRC layer.

The input parameters are the integrity key (128 bits), the integrity sequence number (Count-I: 32 bits), a random value generated by the network side (Fresh: 32 bits), the direction (1 bit) and the signalling data Message. Based on these parameters, the message authentication code for data integrity (*MAC-I: 32 bits*) is computed using the algorithm f9. MAC-I is then *appended to the message* when sent over the air interface. The receiver computes XMAC-I on the message received in the same way the user computed MAC-I and verifies the data integrity of the message by comparison with the received MAC-I.



3. IMPACTS ON GERAN

Introducing integrity protection in GERAN with the same level of security as UTRAN and in an acceptable timeframe, would mean to import the integrity protection mechanism from UTRAN.

As said earlier, almost *all control signalling information elements* are integrity protected in UTRAN and integrity protection is performed in RRC.

If integrity protection is introduced in GERAN, a 32-bit MAC-I information element would be appended to the corresponding RRC messages. Those messages are later transferred as signalling messages using CS1.

Examples of such messages are: HANDOVER COMMAND, HANDOVER FAILURE, HANDOVER ACCESS, RADIO BEARER SETUP, RADIO BEARER SETUP COMPLETE, etc [3].

Now, signalling control messages are to fit within one radio block. However when needed and if possible segmentation may be used: the message content is carried by more than one radio block. In the downlink, segmentation is not an issue as the network is the sender and is in control of the resources, but in the uplink segmentation cannot be used freely by the MS as the network controls the UL resources: if segmentation is used in UL, the network must have allocated resources to make segmentation possible.

Therefore integrity protection, *when causing segmentation*, will imply a much larger overhead than 32 bits for the considered message and may also make a procedure fail (handover): one more radio block will have to be sent over the air interface, meaning 100% overhead if the original message fitted into one radio block. However *it is very difficult to assess* when exactly integrity protection would cause segmentation, because the exact size of the message very much depends on what it carries at a given moment, for/from a given MS: the message might already have room for 32 bits (and already be segmented or not).

Not having integrity protection in GERAN would mean that UTRAN RRC messages that could have been reused, cannot because of the MAC-I IE, and therefore need to be redefined for GERAN.

4. CONCLUSIONS

Defining integrity protection in GERAN would allow for the same level of security as UTRAN, and therefore lead to an harmonized 3G security between the two Radio Access Systems. However integrity protection in GERAN would mean some overhead that may be unacceptable in some cases, but globally the overhead impact on GERAN is very difficult to assess, due to the variable sizes of the message and the complexity of the procedures involved. In order to attenuate the impact on GERAN of integrity protection, it could also be considered to modify the method used in UTRAN when adapting it to GERAN.

5. REFERENCES

[1] 3GPP TSG GERAN AdHoc#2, Tdoc GAHW-000045, "GERAN Overall Description, Stage 2", Rapporteur (Nokia), 8th-13th October, 2000, Münich, Germany

[2] UMTS TS 33.102, "3G Security; Security Architecture", 3GPP, July 2000

[3] UMTS TS 25.331, "RRC Protocol Specification", 3GPP