3GPP TSG SA WG3 Security **S3-020545**

8th – 11th October, 2002

Munich, Germany

Agenda Item: 7.5

Source: Ericsson

Title: A5/3 and GEA3 and their relation with EGPRS

Document for: Discussion

1. Introduction

The new algorithms A5/3 and GEA3 has been delivered from SAGE. These specifications were presented at the SA3 meeting in July 2002 and SA has endorsed theses specifications.

While reviewing these new specifications some unclear issues was discovered that we would like to discuss in this meeting to find a common understanding.

2. Discussion

2.1 Use of A5/3 for EDGE

The first issue is that SAGE is using the term EDGE in a way, which is not inline with how Ericsson interpret the term. We have understood that the term EDGE incorporates both ECSD and EGPRS. Hence we believe that statements like e.g.
"Specification of the A5/3 Encryption Algorithms for GSM and EDGE, and the GEA3 Encryption Algorithm for GPRS" could be interpreted that A5/3 shall be used for GSM, ECSD as well as EGPRS. However our understanding is that GEA3 shall be used for both EGPRS and GPRS.

2.1 Data-rate for EGPRS (EDGE GPRS)

Since EDGE is using a different modulation scheme (8-PSK) than standard GSM (GMSK) the 'raw' bit rate should be 3 times the bit-rate of GMSK. This according to our understanding is not reflected in clause 6.4.2 in TR 55.919 since there it is stated that the highest bit-rate for GPRS is 21.4 kbps per timeslot but for EGPRS it should be of order 50-60kbps. That means that the number of initialisations is impacted as well. It seems like this clause has not been considered for EGPRS.

3. Conclusions

If we assume that a new modified A5/3 algorithm has been defined for ECSD, then if there is a cryptographic gain to have two different input constants for GSM A5/3 and ECSD A5/3 then Ericsson can accept this. And if there is a cryptographic gain to have two different input constants for GPRS GEA3 and EGPRS GEA3 then Ericsson can accept a new modified GEA3 for EGPRS as well.

It is proposed to discuss the raised issues and take a decision how to proceed in order to present CR's to the next SA3 meeting in November.

4. References

[1] ETSI/SAGE Specification, Specification of the A5/3 Encryption Algorithms for GSM and EDGE, and the GEA3 Encryption Algorithm for GPRS, Document 1: A5/3 and GEA3 Specifications, version 1.0.

[2] ETSI/SAGE Specification, Specification of the A5/3 Encryption Algorithms for GSM and EDGE, and the GEA3 Encryption Algorithm for GPRS, Document 2: Implementors' Test Data, version 1.0.

[3] ETSI/SAGE Specification, Specification of the A5/3 Encryption Algorithms for GSM and EDGE, and the GEA3 Encryption Algorithm for GPRS, Document 3: Design Conformance Test Data, version 1.0.

[4] ETSI/SAGE Technical Report, Specification of the A5/3 Encryption Algorithms for GSM and EDGE, and the GEA3 Encryption Algorithm for GPRS, Document 4: Design and Evaluation Report, version 1.0.