3GPP TSG SA WG3 Security — S3#35 **S3-040745**

5 - 8 October 2004

St Paul's Bay, Malta

Title:	**Key separation mechanism in GSM/GPRS**
Source:	**Orange, Nokia**
Document for:	**Discussion and Decision**
Agenda Item:	**6.6**
Work Item:	**GERAN Security**

1 Introduction

Two main countermeasures to Barkan-Biham-Keller [Bark] attack have been discussed in previous meetings: Authenticated Ciphering Instruction and Special RAND. They both introduce a form of key separation between encryption algorithms.

In last SA3, it was decided to postpone that work to release 7 and to finalise it as soon as possible for release 7.

2 Discussion

Key separation mechanism timescale

Concerning the need to introduce a key separation mechanism, we remind the recommendation made by GSMA Security Group in an LS about A5/3 introduction [S3-030490]:

"Having considered the matter at its last meeting, in the light of the new attacks that have recently been presented on GSM ciphering, SG came to the conclusion that it should be a priority to introduce a mechanism that separates keys for use with different encryption algorithms. For this reason SG wishes to express that the introduction of such a key separating mechanism should be aligned with the introduction of A5/3. This combined introduction can hopefully be achieved before the end of 2004. An absolute deadline should be that both security features are part of Rel-6."

Then, even if it is not part of release 6, the key separation mechanism should be introduced as soon as possible.

Mechanism selection

Several contributions have been produced describing Special RAND features as it has been on the table for about one year now. [S3-030588] was presented at SA3#30 and [S3-030693] at SA3#31. The last version of the proposed CR to TS 43.020 can be found in [S3-040529].

In last meeting, a comparison of the 2 alternatives was provided in [S3-040528]. That contribution mentioned some concerns with the Authenticated Ciphering Instruction as it seems that its deployment could take a long time. In particular, it requires all the GSM networks to be upgraded before the handsets implementing it can be released and then before the mechanism can be activated in the first network.

On the contrary, Special RAND requires minimum modifications in the networks and allows for a smooth migration. An operator can deploy the mechanism independently of the other operators' schedule.

As it is discussed in a Nokia's contribution to this meeting [S3-040723], Special RAND also provides with a generic mechanism for security context separation.

3 Conclusion

Even now that it has been decided to remove A5/2 from the handsets, it is still necessary to introduce a key separation mechanism for GSM/GPRS. The decision should be made as soon as possible.

Taking into account the different arguments given in previous meetings, we propose that the Special RAND mechanism should be selected to provide a key separation mechanism in GSM/GPRS and to counteract BBK attack.

4 References

[Bark] E. Barkan, E. Biham, N. Keller: “Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication”, In D. Boneh (Ed.): Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings. Lecture Notes In Computer Science Volume 2729, Springer 2003, pp600-616

[S3-030588] 3GPP SA3 Tdoc S3-030588: "Further development of the Special RAND mechanism", SA3 meeting #30, Povoa de Varzim, Portugal, 7-10 October 2003.

[S3-030693] 3GPP SA3 Tdoc S3-030693 "More elements on the Special RAND mechanism", SA3 meeting #31, Munich, Germany, 18-21 November 2003.

[S3-040528] 3GPP SA3 Tdoc S3-030528: "Analyse of the countermeasures to Barkan-Biham-Keller attack ", SA3 meeting #34, Acapulco, Mexico, 6-9 July 2004.

[S3-040529] 3GPP SA3 Tdoc S3-030529: "Proposed CR to TS 43.020 : Introducing the special RAND mechanism as a principle for GSM/GPRS ", SA3 meeting #34, Acapulco, Mexico, 6-9 July 2004.

[S3-040723] 3GPP SA3 Tdoc S3-030723: "Security context separation ", SA3 meeting #35, St Paul's Bay, Malta, 6-9 October 2004.