3GPP TSG SA WG3 Security — SA3#36 **S3-041076**
November 23-26, 2004
Shenzhen, China

Title:	**[DRAFT]** LS on key separation for GSM/GPRS encryption algorithms
Response to:	
Release:	
Work Item:	GERAN Security
Source:	SA3
To:	ETSI SAGE
Cc:	

Contact Person:
Name: Sylvie Fouquet
Tel. Number: +33 1 45 29 49 19
E-mail Address: sylvie.fouquet@francetelecom.com

Attachments: S3-040983, Adoption of key separation for GSM/GPRS in the short term

1. Overall Description

SA3 has discussed for several meetings the introduction of key separation between GSM/GPRS encryption algorithms as a countermeasure against Barkan-Biham-Keller attack [1]. SA3 has also taken the decision to remove A5/2 from the handsets in release 6.
However, SA3 has not decided yet whether key separation should be introduced in the short term or whether it should be included in long term security enhancements.

SA3 would like to ask SAGE advice on whether key separation introduction should be done in the short term or whether this could be postponed to long term. SAGE is also requested to assess the security risk taken if the second option is selected.
In particular, as A5/3 support in handsets is mandatory for release 6, SA3 would appreciate to have SAGE feedback on potential attacks on handsets which would support A5/1 and A5/3 algorithms but no key separation mechanism.

SAGE is also requested to comment the attached company contribution [S3-040983] which provides an analysis of the key separation introduction timing.

2. Actions:

To ETSI SAGE :

ACTION: SA3 kindly asks ETSI SAGE to provide guidance on the above issues.

3. Date of Next TSG-SA3 Meetings

SA3#37	21 - 25 February 2005	Sophia Antipolis, France
SA3#38	25 - 29 April 2005	Switzerland (TBC)

4. References

[1] 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