Technical Specification Group Services and System Aspects **TSGS#18(02)0812**

Meeting #18, New Orleans, USA, 9-12 December 2002

3GPP TSG SA WG3 Security — S3#26 **S3-020686**
19- 22 November 2002
Oxford, UK

Title: **Introduction of a second UMTS encryption and integrity protection algorithm (UEA2 and UIA2)**

Release:

Source: SA3
To: TSG-SA
Cc: GSMA-SG, ETSI-SAGE, 3GPP2 SA4, TIA TR45-AHAG

Contact Person:

Benno Tietz
Email: Benno.Tietz@vodafone.com
Tel: +49 172 33099 2168

1. Rationale

a) Introduction

As the past has taught us (e.g. GEA2) the deployment of new encryption (and integrity protection) algorithms into networks and handsets takes some years (from the very beginning - writing the requirements - to the sale of handsets supporting the new algorithm). Therefore it is not possible to react within a short time period in the case that the first UMTS algorithms (the KASUMI-based UEA1 and UIA1) should be broken (currently there are no indications that these algorithms contain any weaknesses). Therefore it is sensible to start with the development of a new algorithm now to have a second one in place and ready for use.

b) Requirements

A requirements list is needed. As a basis the requirements list of UEA1 and UIA1 (3G TS 33.105 V 4.1.0) could be used and reviewed (e.g. number of gates, bit rates). One new requirement (among others) is that the cryptographic foundations must be different from UEA1 and UIA1.

c) Algorithm Designer and Evaluation.

It is proposed that the actual work should be done by ETSI SAGE. Similar to UEA1 and UIA1 an evaluation by (invited and paid) experts is recommended. The terms and conditions for usage and distribution of the algorithm might be the same as for UEA1 and UIA1. The re-use of existing work (e.g. within 3GPP2 or from the EU-funded Nessie project) could be considered.

Since there is currently no time pressure the requirements capture, design and evaluation process should be done carefully and will be finalised within one to two years.

d) Funding

It is proposed that 3GPP provides the funding for the work.

2. Actions:

TSG SA is kindly asked to approve the proposal and to forward it to PCG in order to arrange the funding.

3. Date of Next TSG-SA3 Meeting:

SA3#27	25th – 28th Feb 2003	Sophia Antipolis