3GPP TSG SA WG3 Security — S3#15 **S3-000602**

12-14 September, 2000

Washington D.C., USA

Source: **3GPP S3**

To: **SAGE**

Title: **Draft LS about 3G algorithms**

S3 has revisited a few issues raised by SAGE in S3#14 meeting (Oslo, August) about the special task force work on 3G authentication and key generation algorithms. In addition, S3 would like to consult SAGE in one matter concerning 3G confidentiality and integrity protection algorithms.

S3 likes to make the following clarifying remarks about the AKA algorithm work:

1) It is not required that SAGE task force produces any example on generating RAND parameter values (f0 function);
2) It is sufficient that the example algorithm family designed by SAGE task force produces only RES parameter values with length of 64 bits or less;
3) S3 has approved an attached CR (Tdoc S3-000602) on TS 33.102 which contains a change on the generation mechanism of the parameter AUTS. The change is believed to be favored by SAGE as it was done based on request from SAGE;
4) S3 proposes SAGE to be prepared to publish their example algorithm design at the earliest convenient time. In addition, it would be useful to encourage external experts to study the example. During the S3 meeting, Greg Rose from Qualcomm already volunteered to carry out this kind of study.

Another SAGE task force designed the 3G confidentiality and integrity protection algorithms based on the requirements specification TS 33.105. Because of recent developments in the 3GPP R2 group, S3 would like to make the attached change (Tdoc S3-000587) into the requirements specification. SAGE is kindly asked to review the proposed CR and express their view about it.

Contact: Valtteri.Niemi@nokia.com