Technical Specification Group Services and System Aspects **_TSGS#7(00)0005_**

Meeting #7, Madrid, Spain, 15-17 March 2000

3GPP TSG SA WG3 Security — S3#11 **S3-000200**

22-24 February, 2000

Mainz, Germany

From: **S3**

To: **ETSI SAGE**

Copy to: **3GPP TSG SA**

Title: **Delivery of algorithm specifications**

3GPP TSG SA WG3 Chairman is pleased to have received the specifications of the confidentiality and integrity algorithms including the underlying block cipher Kasumi. SA WG 3 thanks the ETSI SAGE Task Force 3GPP for the successful work that has been carried out in a short time.

The report on the work performed by the Task Force and the report on the evaluation results have been considered by S3 and the working group has found that the results very well satisfies the most important stage in the process of providing standard algorithms for confidentiality and integrity protection to 3GPP.

The documents are thus to be considered as formally endorsed by S3 and the work of SAGE fulfilled.

As regards the SAGE Task Force 3GPP recommendation for publication of the algorithms we can confirm that this wish is shared by S3. It is also stated in the algorithms requirements specification that the algorithms should be made public to achieve maximum public trust in the systems. 3GPP has however decided to allow some time to collect the views on this topic from its organisational partners before the final decision is taken.

Therefore the algorithm specifications will not be published immediately, but hopefully this will be the case very soon. Therefore also the publication of the evaluation results should wait for this formal decision. ETSI SAGE will be advised when it is possible to publish the evaluation report. The report on task force work can be published now.