Source: S2 (Version 1.0)

Title: **Liaison statement on R99 Security Features**

To: S3

CC: TSG-SA

On some markets, 3G service is scheduled for launch within two years. Short timescales imply that two modes of specification work are needed in 3GPP. Rapid progress is necessary for those features that are mandatory in Release 99 specs. On the other hand, study of features which are included in future releases must proceed in parallel. In the 3G Security Architecture specification draft TR S3.03 no distinction is made between the two classes of features.

One specific feature that S2 believes shall be included in Release 99 spec is ciphering of user and signaling data in radio access network. As ciphering algorithm requirements are not yet fully stabilised, the schedule for the algorithm design process seems to be very tight. In order to guarantee that user data and speech confidentiality is offered from the very beginning, it is essential that specifications for at least one ciphering algorithm are ready well in advance of the launching time. Hardware implementation and testing requirements imply that detailed description of the algorithm is available at least 18 months before the system is introduced to public use. Some backup plan is needed in order to minimise the risk that due to tight time schedule constraints 3G service begins with no user data or speech confidentiality at all.

S3 is kindly asked to

1) make it clear which security features that are to be developed for inclusion in Release 99

2) if possible, guide S2 on what functional entities (CN, RNC, Node B etc) and on what protocol level these features are to be implemented.

3) clarify the plans for exact schedule for the new ciphering algorithm.

4) create a backup plan to minimise the risk that due to tight time constraints new ciphering algorithm cannot be delivered early enough.