3GPP TSG SA WG 3 (Security) meeting #11 **S3-000173**
Mainz, 22-24 February, 2000

Proposed MAP Security Status Report (23. February 2000, to be updated)

Layer I
An example format of Key Exchange Messages is specified in 3GPP TS 33.102 (based on ISO Standard 11770-3). No standardisation of the transport mechanism for the Key Exchange Messages is envisaged for R'99.

Open Issues for S3:
Details of key transport between KACs need to be agreed bilaterally between network operators. This could be done in course of roaming agreements. GSMA is seen as the appropriate body to provide a recommendation regarding that issue (possibly based on initial input from S3). For R'00 a standardised, automatic mechanism for Layer I is needed.

Layer II
An example format of key transport messages in layer II is specified in Annex E of 33.102. A standardised mechanism for transporting the key transport messages including standardised interfaces is needed.
To this end, a liaison with S5 to deal with these issues will be established. We have some indications that S5 is willing to take up the issue, provided there is sufficient support from companies interested in MAP security. S3 is confident that the necessary work for standardising Layer II in R'99, that is:

- Identification of suitable transport mechanisms for key transport
- Specification of O & M interfaces between KACs and Network Elements for key transport

can be completed by S5, in co-operation with S3, by June.

Open Issues for S3:
- Select public key algorithms to be used and specify related parameters needed for Layer II.
- Provide further guidance and support to S5
- Establish method of collaboration with S5

Layer III
Collaboration with CN2 has been established. Most open issues concerning layer III transmissions have been resolved in joint meetings. Work has been progressed by CN2(B) and we assume that the necessary CRs for specifying protected MAP messages are reasonably stable. The exact status of work on MAP security in CN2 will be reported at SA#7 by a CN2 representative.

Encryption Algorithm
Only published encryption algorithms shall be used for encrypting Layer III messages.

Open Issue for S3:
ETSI TC SEC as owner of the for Layer III envisaged algorithm BEANO need to be asked if they agree on the publication. In case difficulties arise, an already published off-the-shelf algorithm (e.g. IDEA) needs to be selected by S3.