Source:	**SA3**
Title:	**LS to TSG-SA and TSG-CN on MAP security**
Agenda item:	**4.2**
Document for:	**Information**

Tdoc S3-99xxx
TSG-SA WG3 (Security) meeting #9
Helsinki, 7-9 December, 1999

From:	*SA WG3 (Security)*
To:	*CN, SA*
Title:	*LS to TSG-SA and TSG-CN on MAP security*

With reference to a recent liaison statement from N2 on MAP security (S3-99435=N2-99G32), S3 would like to express their disappointment that N2 cannot do the work on 3G TS 29.002 before the December 1999 TSG plenary meetings. S3 consider MAP security to be a very important feature for R99 and would request that TSG-SA allow for the MAP security work for R99 to be completed by the March 2000 TSG plenary meetings.

S3 have noted that the addition of the security header may result in a requirement to segment some already overloaded MAP messages since a size limit on the MAP payload of approximately 200 bytes (160 bytes for the first two messages of a dialogue) may be imposed by lower layers of the signalling architecture. To help reduce the impact of this, the following principles are proposed by S3:

- Where the length restriction imposed by lower layers of the signalling architecture does not exist, it must be possible to protect all MAP messages.

- Where the length restriction does exist, the following principles should be adopted:

    - All new MAP messages specified in R99 should be protected. It is appreciated that this may involve revisions to existing MAP dialogues for some new messages because the security header extends the MAP payload above the size limit.

    - Remaining MAP messages will be prioritised by S3. It is appreciated that this may involve revisions to existing MAP dialogues for some messages because the security header extends the MAP payload above the size limit. A prioritised list of MAP messages requiring protection will be produced at S3#10 (19-21 January 2000).

It is understood that a new application context would be used to distinguish messages which include the security header from messages which do not include the security header.

S3 have noted a number of other questions on MAP security from the liaison statement. A joint ad hoc meeting of experts from S3 and N2 is proposed to resolve the questions raised by N2, progress the work according to the above principles, and draft the necessary CR to 29.002. It is proposed that the meeting will be held in Darmstadt, Germany on 6th and 7th January 2000, hosted by Deutsche Telekom.