3GPP TSG SA WG3 Security — S3#19 **S3-010320**

3 - 6 July, 2001

Newbury, UK

3GPP TSG-CN WG4 Meeting #08 ***Tdoc N4-010669***

Rio Grande, Puerto Rico, 14-18 May 2001

Source: **TSG-CN WG4**

Title: **MAP security**

To: **TSG-SA WG3**

Contact Person:

Name: Ulrich Wiehe

E-mail Address: ulrich.wiehe@icn.siemens.de

Tel. Number: +49 6621 169 139

TSG-CN WG4 thank TSG-SA WG3 for the LS on MAPSec [S3z010033] from the TSG-SA WG3 ad hoc on network domain security and provide the following comments and information, although concerns have been raised within CN4 that the LS may not have received agreement from all companies within SA3:

- **IPsec**
  It is CN4's understanding that protection of MAP messages at the application level is not needed when MAP is transported over IP and IPsec is used for protection. However as long as the end points cannot be sure that MAP is transported over IP with IPsec protection for all the links in the connection, the use of MAPsec is necessary.

- **Granularity of protection**
  The technical concept for MAPsec as specified in 29.002 has been designed in a way which allows for protection of MAP payloads (invoke components, result components, error components and dialogue user info) independently with different protection modes. CN4 strongly recommends that 3GPP make use of this flexibility in order to minimise processing load, and to allow for compatibility with later releases which may require granularity of protection at the component level.
  CN4 consider that component level granularity of protection would not impose a major increase of implementation and administration effort compared with operation level granularity of protection. Therefore CN4 ask SA3 to change their working assumption, and to choose a granularity of protection at the component level.

- **Length of the Integrity Check Value**
  CN4 would like to minimise the overhead in message length imposed by MAPsec and thus avoid segmentation. Therefore we have chosen the minimum length acceptable from a security point of view for the Integrity Check Value: 32 bits.

- **Structure of the Security Header**
  CN4 have noted that among other issues to be resolved, the structure of the security header is still under discussion within SA3. Details of the length of the IV, requirements with impact on the IV-structure and the TVP structure need to be agreed by SA3 before CN4 can finalise the protocol details.

- **MAPsec shift to Rel-5**
  CN4 see the possibility that MAPsec cannot be finalised before the next TSG plenary meetings, and that MAPsec may therefore be shifted to Rel-5. CN4 therefore have prepared a CR to the Rel-4 version of

29.002, which undoes the changes done so far for MAPsec. This CR will be presented to CN plenary if the open issues cannot be resolved in time.

SA3 are asked to note that the next regular CN4 meeting is scheduled July 9 to 13. However an ad hoc meeting may be held on May 29 to 31, to complete MAPsec for Rel-4, if open issues can be resolved in due time.