3GPP TSG SA WG3 Security — S3#16 **S3-000760**

Sophia Antipolis (France), 28th-30th November, 2000

Title: **LS to CN4 on SA3 agreements on MAPSec**

Source: **TSG SA WG3**

To: **TSG CN WG4**

Contact Person: **david.castellanos-zamora@ece.ericsson.se**

TSG SA WG3 would like to inform TSG CN WG4 of the latest progress achieved at S3, in the field of MAP application layer Security.

During S3#15bis, ad-hoc meeting on "Network Domain Security" WI (8th-9th November) and S3#16 plenary meeting (28th-30th November), a significant number of contributions and input papers were reviewed. In particular, the following agreements were reached:

- **'General Structure of Secure MAP Operations':**

  The former text describing the structure of Secure MAP Messages is reformulated to define protection mechanisms on a per MAP operation basis.

- **'Structure of Security Header':**

  The internal structure of the Security Header has been agreed. "Sending PLMN Id", "Security Parameter Index - SPI", "Initialisation Vector - IV" and "Original Component Id" will be the parameters to be considered.

- **'Refinement of MAP Security Association':**

  Some changes in the former structure of MAP Security Association for MAP Security were agreed. In particular the removal of "Encryption Key Version Number" and "MAC Key Version Number" parameters and the modification of the definition for "MAP Protection Profile".

These agreed changes are already incorporated in the latest version of TR 33.800, v0.3.5 ("Principles for Network Domain Security") attached for information (chapters 7.2.1 and 7.4).

- **Algorithm Selection for MAP Security**

  S3 discussed the choices of encryption and integrity/authenticity algorithms suitable to protect MAP signalling. The conclusion was to recommend the mandatory support for the following algorithms:

Encryption Algorithm	Integrity/Authenticity Algorithm
AES	AES-MAC

  Although only one algorithm has been recommended at this time, S3 would like to indicate that the negotiation of algorithms is still being considered.

- **Specification of MAP-Protection Profiles:**

  S3 also discussed the possible alternatives to specify MAP-PPs. Two main alternatives have been identified as equally valid from a security point of view. S3 leaves to the discretion of CN4 which specific approach is more convenient from a MAP implementation perspective.

The first alternative specifies Protection Modes against MAP operations. For example:

MAP Operation	Protection Mode
SendAuthenticationInfo	2 (integrity/authenticity and confidentiality)

The second alternative specifies Protection Modes against MAP-ACs. For example:

MAP-AC	Protection Mode
infoRetrievalContext-v3	2 (integrity/authenticity and confidentiality)

TSG SA WG3 would also like to inform TSG CN WG4 on the level of discussion on the following open items:

- **<u>Use of Protection Mode 0:</u>**

  In the specification of MAP-PPs, a large number of MAP Operations/ACs will be protected using Protection Mode 0 (no protection). For these Operations/ACs it is proposed to allow that the Operation/AC is performed in cleartext instead, thus avoiding the extra overheads introduced by the use of Secure MAP Operations.

  In this context, it is then natural to question whether Protection Mode 0 is still relevant.

S3 informs with this LS that these reached agreements can be already considered by CN4 in order to progress/complete MAP Security stage 3 specifications. At the same time, S3 kindly asks CN4 for their comments and preferences (if any) on the issues presented in this document.