3GPP TSG SA WG3 Security — S3#17 **S3-010011**

27 February - 02 March, 2001

Gothenburg, Sweden

3GPP TSG-CN4 **Tdoc N4-010203**
CN#06 Meeting , Beijing, CHINA
15th January – 19th January 2001

Source: **TSG CN WG 4**

Title: **Proposed Response to SA3 on SA3 agreements on MAPSec**

To: **TSG SA WG3**

Contact Person:
Name: Peter Schmitt
E-mail Address: peter.schmitt@icn.siemens.de
Tel. Number: +49 6621 169 152

TSG CN WG4 thank TSG SA WG3 for their LS on SA3 agreements on MAPSec [S3-000760] and provide the following answers, comments, questions and information:

- **Structure of Security Header**
  The attached CR 168r1 to 29.002 modifies the internal structure of the Security Header according to the SA3 agreements.
  Can SA3 please confirm that a single Initialisation Vector (IV) in the Security Header is sufficient, i.e. if in protection mode 2 both the encryption Algorithm and the Integrity/Authenticity Algorithm require an IV, the same IV will be used.

- **Algorithm Selection for MAP Security**
  The selected Encryption Algorithm (AES) and the selected Integrity/Authenticity Algorithm (AES-MAC) may be used with various key lengths, block lengths and modes of operations. Furthermore the length of the Integrity Check Value produced by AES-MAC is not fixed. The length of the additional message overhead introduced by MAPSec very much depends on the chosen block length (IV length, padding), mode of operation (IV present/absent, padding present/absent) and on the length of the Integrity Check Value. Concerns have been raised that the additional overhead may result in an available message length for the MAP application which does not allow a single Authentication Quintet to be carried in worst case scenarios.
  SA3 are asked to refine their algorithm selection by determining
  - the block length which is to be mandatorily supported,
  - the key length which is to be mandatorily supported,
  - the mode of operation for AES which is to be mandatorily supported,
  - the mode of operation for AES-MAC which is to be mandatorily supported,
  - the length of the Integrity Check Value which is to be mandatorily supported

  in a way which minimises the overhead as far as possible while ensuring an acceptable level of security.

Specification of MAP-Protection Profiles
In addition to the alternatives given in the LS from SA3, protection Modes may also be specified against components of operations. This can be used to allow different components of the same operation, which are carried in different messages sent in different directions and thus being protected by different SAs, to be protected independently from each other.

If this alternative is chosen, CN4 proposes to standardise a limited number of profiles for Release 4. An example is given in the table:

Profile number	InfoRetrievalContext-v3			InterVlrInfoRetrievalContext-v3			AnyTimeInfoHandlingContext-v3		
	SAI invoke	SAI result	SAI error	SI invoke	SI result	SI error	ATM invoke	ATM result	ATM error
1	PM 1	PM 2	PM 0	PM 1	PM 2	PM 0	PM 1	PM 1	PM 0
2	PM 1	PM 1	PM 0	PM 1	PM 1	PM 0	PM 1	PM 1	PM 0

3	PM 2	PM 2	PM 0	PM 2	PM 2	PM 0	PM 2	PM 2	PM 0

SAI: SendAuthenticationInfo
SI: SendIdentification
ATM: AnyTimeModification
PM: Protection Mode

- **Use of Protection Mode 0**
  Protection mode 0 is relevant for cases where some but not all components need protection within a dialogue (e.g. error components). In cases where no component of a dialogue needs protection it is of course better and avoiding overhead not to make use of the MAP Security mechanism at all, rather than using the MAP security mechanism and "protecting" all components with protection mode 0.