**3GPP TSG SA WG3 Security — S3#19** **S3-010379**

**4 - 6 July, 2001**

**Newbury, UK**

**Source:** **TSG-SA WG3**

**To:** **TSG-RAN WG2**

**Cc:** **TSG-GERAN, TSG-RAN WG3, TSG-SA WG2**

**Title:** **Response to LS (R2-010978) on Optimised IP speech and header removal support in GERAN**

**Contact person:** **Guenther Horn**
Guenther.horn@mchp.siemens.de
phone: +49 89 636 41494

SA3 have received this LS at their meeting #19 and would like to share the following information which may be useful for discussions within RAN2 and other groups:

RAN2 had stated in their LS that the use of IPSec would reduce the efficiency of header compression.
SA3 would like to point out that

- this is generally only true if IPSec was used for encryption. The use of IPSec for integrity protection would have the effect on the efficiency of header compression that the appended Message Authentication Code of 96 bits could not be compressed. The rest of the information added by IPSec could be compressed.
- the only potential use of IPSec over the radio interface which SA3 are currently considering is for protection of SIP messages between the UE and the P-CSCF, as part of the IMS. Only integrity protection of these SIP messages is mandated, encryption is optional for implementation. As an alternative to this use of IPSec, SA3 are currently also studying an application layer security solution. A decision between IPSec and the application layer security solution has not yet been taken.