**3GPP TSG SA WG3 Security — S3#18** **S3-010231**

**21 - 24 May, 2001**

**Phoenix, USA**

---

**Title: Reply to the following LSs:**

**LS on "Security for IM SIP session Signaling"**
**(Tdoc N1-010588, received as S3-010152)**

**LS on " IM User Identities"**
**(Tdoc S2-010757, received as S3-010160)**

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

**To:** **TSG CN WG1, SA WG2**

**Contact Person:**

**Name: Guenther Horn**

**Email: Guenther.Horn@mchp.siemens.de**

**Tel : +49 89 636 41494**

---

**Attachments: None**

TSG SA WG 3 thanks the joint N1-S2 meeting and S2 for their liaison statements. They are answered in one LS as the question raised in the LS from S2 (Tdoc S2-010757) was also raised in Tdoc N1-010588, see"*Usage of the User Private Identity*" below.

TSG SA WG 3 is pleased to accept N1's offer to give a presentation at the next S3 meeting (S3#19) in London, 3-6 July 2001.

S3 would like to make the following comments on the bullet points towards the end of the LS from the joint N1-S2 meeting (Tdoc N1-010588):

- *"SIP Header Parameter modification by I-CSCF"*
  This is possible because integrity protection is done in a hop-by-hop fashion.
- *"Via and Record Route Header Hiding by I-CSCF"*
  A new WI on hiding mechanisms needs to be created by S3, this has not happened at S3#18.
- *"Contact header modification by P-CSCF"*
  This is possible because integrity protection is done in a hop-by-hop fashion.
- *"Useage of the User Private Identity"*
  S3 sees no security problem with the current working assumption by S2 and N1 "that the Registration flow is definitely the only time the Private User Identity is sent to the network in SIP signalling messages".

- *“Authentication of Invite and other SIP session signaling messages”*
  It is the current working assumption of S3 that authentication is only required for registration and re-registration.

- *“Integrity protection of SIP signalling messages (especially the first message that is sent)”*
  The mechanism for integrity protection of SIP signalling messages between the UE and the P-CSCF is still under study by S3, the mechanism for integrity protection of SIP signalling messages between other IMS entities is IPSec (ESP). The first message that is sent (REGISTER) cannot be integrity protected as no integrity key establishment has yet taken place. However, when REGISTER is sent a second time it can be integrity-protected. The precise mechanism for this is still under discussion in S3.

- *“Requirement for SIP signaling to support Key exchange for encryption of bearer*”
  S3 understands that “ encryption of bearer” refers to end-to-end encryption of user data. S3 would like to inform N1 and S2 that an S3 work item relating to end-to-end security in UMTS exists. S3 can confirm that SIP signalling messages will be required to support key exchange for IMS end-to-end encryption. However, no solutions are currently available.