3GPP TSG SA WG3 Security — S3#10 **S3-000063**

19-21 January, 2000

Antwerp, Belgium

From: **TSG S3**

To: **TSG N1**

cc: **TSG N2**

Response to LS on Enhanced User Identity Confidentiality – open questions

TSG S3 thanks TSG N1 for their LS on open question on Enhanced User Identity Confidentiality (N1-000202 – S3-000056). The open questions and restrictions are discussed within S3 and the following answers and guidelines are provided.

Q: Which entity on the subscriber side does perform the encryption process? Is it a SIM or Terminal functionality?

A: The encryption process will be performed by an USIM functionality.

Potential problems:

1. TSG S3 has designed the Enhanced User Identity Confidentiality mechanism for UMTS with the option to adopt this solution for GSM. Restrictions of the CM service Request message that avoid introduction for GSM R99 will not affect the introduction of the Enhanced User Identity Confidentiality mechanism for UTRAN.

2. TSG S3 will deliver finalised advise about content and coding of the requested information elements by N1#11.

3. Paging procedures that use the IMSI to search for a mobile are treated less sensitive compared to requesting the mobile's IMSI because an attacker has to know the mobile's IMSI in before.

4. Discussion with TSG N2 has clarified the benefit of introducing a new logical HE-network functionality UIDN (User Identity Decryption Node) to reveal encrypted identities. This was considered to give operators enough flexibility.

5. S3 will provide information on MSB/LSB of bit streams if necessary.

6. ME shall use XEMSI if that HE-option is active.

TSG S3 thanks TSG N1 for starting to draft the CR for TS24.008.

Contact person: Stefan Pütz
stefan.puetz@t-mobil.de
+49 228 936 3377