3GPP TSG SA WG3 Security — S3#10 **S3-000056**

19-21 January, 2000

Antwerpen, Belgium

3GPP TSG-CN-WG1, Meeting #10
11 - 14.January. 2000
Abiko, Japan

Tdoc N1-000202

From: **TSG – CN1**

To: **TSG S3 and TSG N2**
Contact Person: Dieter Jacobsohn.
E-mail: dieter.jacobsohn@t-mobil.de
Tel: +49 228 936 3361

LS on Enhanced User Identity Confidentiality – open questions

TSG-CN1 received the LS from TSG-S3 and discussed the proposed solution. To finalise the equivalent CR for 3G TS 24.008 N1 identified the following questions and restrictions.
TSG-CN1 is kindly asking for answers and guidelines:

Questions:

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

Potential problems:

GSM R99 has a restriction in length (max. 20 octets, no segmentation) on lower layers for transmission of the CM service Request message, therefore introduction of the concept is possible for UTRAN only.

TSG N1 needs a finalised advise about content and coding of the requested information element.

Paging procedures can use IMSI without encryption to search for a mobile, this case is not covered by the current scenarios. This was seen as potential hole in the designed security mechanism.

If the intention is to store the HLR address on SIM / USIM card this makes moving subscribers from one HLR to another more difficult.

MSB / LSB of bit streams should be defined unless this is already specified somewhere or it is otherwise absolutely clear.

The criteria for the ME to use XEMSI or IMSI should be defined, in the current proposal this is not clear.

New concept is being introduced by the proposal and this is against the principle that was agreed in TSGN #6 that we should focus on the completion of the current open issues and not invent new ones.

TSG N1 started to draft the necessary CR for TS24.008 but put it on hold up to clarification of the given questions and problems.