3GPP TSG SA WG3 Security — S3#12 **S3-000235**

11-14 April, 2000, Stockholm, Sweden

Technical Specification Group Services and System Aspects ***TSGS#7(00)0092***
Meeting #7, Madrid, Spain, 15-17 March 2000

Source: **TSG SA WG2**
Title: **Liaison Statement on Enhanced User Identity Confidentiality**
Agenda Item: **5.2.3**

3GPP SA 2 *Tdoc S2-00-0587*
Tokyo, Japan, 6-9/3/00

To:	TSG-SA plenary
Cc:	RAN plenary, CN plenary, T plenary;

S2 has reviewed 3G PD 30.810, the Project Plan for Security for Release '99 and discussed EUIC.

S2 has considered whether EUIC is possible to be introduced in R2000, or, whether EUIC requires that it is "done in R'99 or discarded forever". S2 have concluded that introduction in R2000 is possible.

From discussion of the project plan, it seems that the issues listed below may hinder the full and complete specification of EUIC in R'99. Therefore S2 suggest that this item continues to be developed in R2000.

S2 is providing this document to TSG-SA plenary in order to aid SA's decision on whether EUIC is part of R'99 or R2000.

Open Issues

CN 1

a) The modification of all GMM and MM messages which carry IMSI is required. The specification of new identity types is required.
b) How are different Radio Access Technologies handled if EUIC is not applied to GSM?

CN 2

a) Handling of UMTS-VLR restart.
b) Handling of VLR restart when MSC/VLR serves both GSM and UMTS cells.

RAN 2

a) UMTS RACH messages only have a payload of about 20 octets. The "encrypted IMSI and UIDN address" is longer than this.
b) How is DRX handled? It is assumed that the DRX period is defined by the "real IMSI" and not the "encrypted IMSI" (however this may give information on the [3] Least Significant Digits of the IMSI).

RAN 3

a) Assuming that RANAP connections are identified by the 'real IMSI' (and not the 'encrypted IMSI'), RANAP paging messages need to be modified to be able to carry both the 'real IMSI' and the 'encrypted IMSI'.

S2

The detailed stage 2 description has not been seen by S2. In the absence of this, S2 cannot determine all the architectural aspects. There is no guarantee that all the potential problems have been identified yet. Some unresolved issues are:

a) The behaviour of a VPLMN that does not support this feature has yet to be defined.
b) The behaviour of a VLPMN that does not support this feature but has a mixture of GSM and UMTS coverage, and, dual mode GSM/UMTS EUIC mobiles roaming, has to be defined.
c) There are concerns that loss of synchronisation between MS and UIDN might severely reduce call success rates.

d) What happens when VPLMN does not allocate a TMSI?
e) How is the GSM radio access network handled? (Without solving this it seems that any dual mode mobile has no protection of its IMSI. Applying EUIC to the GSM radio interface seems feasible, but requires some extra standardisation.)
f) The impact on the mobile of TEMSI paging is not clear. For instance do all TEMSIs have to be received and passed into the USIM? What impact does this have on the mobile's idle mode power consumption?
g) What is the internal structure of the TEMSI? It seems likely that it needs MCC and MNC fields to be defined and sent "in clear".

S3

We understand that S3 has now completed the description of this feature in 33.102. However, the open issues listed in this document might lead to some further revisions being needed.

T3

a) Has a field been specified which allows the USIM to prevent the MS from sending the IMSI over the radio interface?

Contact person:
Chris Pudney
e-mail: chris.pudney@vf.vodafone.co.uk
Tel: +44 1635 67 3397