3GPP TSG SA WG 3 (Security) meeting #11 **S3-000196**
Mainz, 22-24 February, 2000

LS concerning Enhanced User Identity Confidentiality (EUIC) Status (24 February 2000)

Source: S3
To: N2, SA

1. Status of Specifications

Work has been progressed and CRs have been prepared to accomodate the feature in the following groups: S3, S2, N1, N2, R2, T3.
The current S3 specification deals with the areas of

- User registration/call setup by encrypted IMSI (EMSI)
- Paging by Temporary Encrypted IMSI (TEMSI) in case TMSI is lost

The CRs prepared in the other groups should have enough maturity to ensure that the feature can be implemented in R'99. One open issue remains, that is: How to proceed in case TEMSI is lost by VLR/SGSN.

2. Security Goals achieved by the present S3 approach

The following security features related to user identity confidentiality shall be provided in UMTS according to chapter 5.1.1 of 33.102:

- **user identity confidentiality:** the property that the permanent user identity (IMUI) of a user to whom a services is delivered cannot be eavesdropped on the radio access link;
- **user location confidentiality:** the property that the presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link;
- **user untraceability:** the property that an intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link.

Most of the passive user identity eavesdropping attacks on the air interface are already covered by the GSM approach using temporary identities.
The current S3 CR (Tdoc S3-000098) solves the problems of active IMSI catching and eavesdropping (cleartext) IMSI paging messages. Also, active IMSI paging attacks are prevented. However, an attacker can get information about a user's location by other, non-IMSI related attacks that are not covered by the current solution. We assume that these attacks are of a very generic kind which are inherent to the system and cannot be countered by cryptographic means.

3. Impact on each Network Operators (due to mandatory implementation of EUIC)

3.1 Operators providing the feature for their subscribers

Operators that want to offer their subscribers EUIC need to implement a UIDN, including a complete subscriber data base, and need to support transport and storage of EMSIs and TEMSIs in their network.

3.2 Operators providing the necessary infrastructure for roaming EUIC subscribers

Operators that do not want to offer their subscribers EUIC, nevertheless need to provide some infrastructure, i.e. support of transport and storage of EMSIs and TEMSIs in their network, especially in VLR/SGSN. This has led to an objection by one network operator to the current CR S3-000098.

Furthermore, the EUIC feature requires terminal and USIM support, but this is considered a minor issue.

Conclusion

Based on the status information given above, a decision is needed between three options on how to proceed further with EUIC:

1) The feature is included in R'99
2) The feature is included in R'99, but is optional for terminals
3) The feature is included in R'00