3GPP TSG_CN **Tdoc NP-000332**
Plenary Meeting #8, Düsseldorf, Germany
21st – 23rd June 2000.

Source: **CN Chair**

Title: **MERGED WG STATUS REPORT FOR WI R'99 SECURITY**

Agenda item: **6.3**

Document for: **INFORMATION**

Excerpts from N1 Status Report (NP-000256)

4.1.2 Removal of P-TMSI signature from SERVICE REQUEST message

- N1 cannot decide whether P-TMSI signature should be included in the SERVICE REQUEST even though S2 have agreed a CR on 23.060 on this issue.

If P-TMSI signature is always included in SERVICE REQUEST then it increases signaling load because a new one must be allocated to a mobile after the P-TMSI signature has been used once. Not including it adds to the signaling load when there is a need to authenticate the mobile.

BT and Lucent objected to the proposal in document NP-000266 / N1-000644.

The proposal was discussed in the TSGS3-TSGN ad-hoc meeting 13.-14.6.2000. There was no recommendation from the meeting but the delegations were invited to bring their own contributions to TSGN #8 if necessary.

4.1.4 Support of GPRS ciphering algorithm GEA2

Tdoc NP-000267 contains R99 CR N1-000722 and NP-000303 / N1-000798 is the corresponding R98 CR. Both were agreed by TSGN1 but with the following comments which TSGN #8 is asked to consider:

- There was strong reservations from one company (BT) on **whether this R98 CR should be acceptable**. At least it must be clear that the support of the new ciphering algorithms is optional for R98 mobiles.
- To be marked as strategic for TSGN #8
- The **concern that this change makes R97 and R98 GPRS different** was shared by several delegations.

The issue was discussed in TSGS3 – TSGN ad-hoc 13.-14.6.2000 and the recommendation of the meeting was that similar CRs should be generated for R97 also. The principle should be that for R99 the support of the GEA2 algorithm is mandatory and for R97 and R98 the support of the new algorithm(s) is not mandatory for the MS or the network but the support of the signalling mechanism to negotiate the algorithm is mandatory.

4.5.6 Security

TSGN1 had to report some open items to TSGN #7. R99 WI status sheet in NP-000262. These open items were consequently divided by TSGS #7 to different releases as follows:

- MS reaction after failure of the network authentication by the MS (R99)
- Integrity protection of emergency calls (R99)
- Encrypted IMSI (R00)
- USIM triggered re-authentication (R00)

The outstanding CRs to complete the R99 part are forwarded for plenary approval in tdoc NP-000273.These CRs complete the TSGN1 task on R99 security.
Additionally there is a controversial issue not related with the above in GEA2 support for earlier releases than R99 (section 4.1.4).

Excerpts from N4 Status Report (NP-000281)

Work Item Security (Agenda 6.3.4)

The Security CRs addresses necessary corrections to the MAP message ***Send-Authentication-Info*** and editorial modifications to improve the description of the IMEISV on the handling of security requirements. These CRs are in Tdocs ***NP-000295*** (IMEI Security) and ***NP-000xxx*** (Security)