3GPP TSG_CN
Plenary Meeting #9, Oahu, Hawaii
20th – 22nd September 2000.

Tdoc NP-000412

3GPP TSG-CN-WG1, Meeting #13
14-18 August, 2000
Vancouver/Canada

Tdoc N1-001023
Tdoc N1-001022

Title: **Liaison statement on the introduction of GEA2.**

Source: **CN1**

TO: **SA2, TSG CN**

Cc: **CN4, SA3, TSG SA**

WI: **Security**

Contact Person:
Name: **Robert Zaus**
E-mail Address: **robert.zaus@icn.siemens.de**
Tel. Number: **+49 89 722 26899**

Date: **17.08.00**

While studying the possibility to introduce the GPRS ciphering algorithm GEA2 for R97/R98 mobile stations, CN1 detected a problem which occurs on the network side in case of an interworking between R99 and R97/R98 SGSNs. Note that the problem is not tied to the introduction of GEA2 for R97 /R98 mobile stations, but will also exist for a R99 mobile station supporting GEA2 and roaming in a mixed R97/R98 – R99 network environment.

Description of the problem:
A mobile station supporting GEA2 will indicate this capability to the network in the MS network capabilities sent during GPRS attach or routing area update. To this purpose the information element has to be enhanced by an additional octet. According to the draft CR currently under discussion in CN1, a R97/R98 network shall ignore this new octet.

The problem occurs, if a R99 SGSN activated GEA2 and the MS subsequently performs an inter-SGSN routing area update to a R97 /R98 SGSN. As the R97/R98 SGSN does not support GEA2, a new authentication and ciphering procedure has to be performed to change the ciphering algorithm to GEA1. This behaviour is not covered by the current R97/R98 specifications GSM 03.60, 04.08 and 09.60 and cannot be introduced without a functional change to a R97/R98 SGSN. Especially, it is not possible with GTP version 0 to indicate to the R97/R98 SGSN a used ciphering key different from GEA1

The following changes would be necessary to R97/R98 specifications:

GSM 03.60: It has to be described that if during an inter-SGSN routing area update the new SGSN does not know or is not able to support the ciphering algorithm used by the old SGSN, the new SGSN has to change the ciphering algorithm by performing a new authentication and ciphering procedure.

GSM 09.60: In the information element MM Context which is passed from the old to the new SGSN, the range of codepoints for the parameter ‘used cipher’ has to be extended so that ciphering algorithms different from GEA1 can be indicated to the new SGSN without triggering an error handling in the new SGSN.

(Note: CN1 considered also alternative solutions, but all of these require some changes to the R97/R98 SGSN. – Furthermore, it is not possible mandate the R99 SGSN to change the ciphering algorithm to GEA1 before the inter-SGSN routing area update is performed, because the R99 SGSN cannot control when the MS performs the routing area update.)

Conclusion:
Based on this analysis and previous decision in TSGN #8 that functional changes to the R97/R98 SGSN specifications can not be made any more TSGN1 has come to the conclusion that the GEA2 ciphering algorithm can not be activated in mixed R97/R98 – R99 networks but all R97/R98 SGSNs must be updated to R99 first.

TSGN1 is working on R97 and R98 CRs to allow the mobile stations to support GEA2 algorithm.

TSGN1 wish to inform TSG CN and TSGS2 on this decision.