TSG-RAN Working Group 3 meeting #2
Stockholm 15th to 19th March 1999

TSGR3#2(99)149

Agenda Item : 6.2

Source : SIEMENS , NEC

Title : Study Item [Iu/6] "Ciphering Algorithm"

Document for : Status Report

---

1. Introduction

This contribution is to report the status of e-mail discussion on the study item [Iu/6] "Ciphering Algorithm". Several comments have been received and it seems that it has already reached a tentative conclusion.

2. Discussion on the E-mail reflector

The discussion point on this item [Iu/6] is quoted below:

"The difference between the ETSI and TTC/ARIB procedure is that the RNC gets the ciphering algorithm from the UE, and in ETSI procedure the algorithms are received from the CN, and the RNC may select the algorithm based on the UE's capabilities."

Two alternative solutions has been raised during the discussion:

Solution1:

The Ciphering Algorithms can be provided in the UE Capabilities. The UE Capabilities appear in the first RRC message i.e. RRC Connection Setup Request(?). Therefore the RNC can acquire the Ciphering Algorithms from the first RRC message. The CN selects possible ciphering algorithms then send them to the RNC (*one comment pointed out that this sentence is not correct)* .The RNC will then select a specific algorithm by taking into account the UE capabilities,

Solution2:

The CN selects possible ciphering algorithms then send them to the RNC (*one comment pointed out that this sentence is not correct)*. The RNC then selects a specific algorithm and send it to the UE. If the UE can support the selected algorithm, it is happy, but if it is not supported, then the UE will reject the algorithm, then a new one has to be chosen by RNC.

The solution1 is appropriate because solution2 seems to cause much more abnormal procedure then solution1.
And the sentence "The CN selects possible ciphering algorithms then send them to the RNC" is not correct

3. Conclusion

The discussion result is reflected at the statement below.

This statement will be incorporated in the Iu specification related part: Chapter 8.10.1 Successful operation, S3.13 ver0.0.2 or chapter 9.2.2.10.1 Successful operation, merged description of Iu Interface.

In the RANAP CIPHER MODE COMMAND the CN specifies which of the ciphering algorithms may be used by the UTRAN. The UTRAN then selects internally an appropriate algorithm, taking into account the UE ciphering capabilities. The UTRAN can deduce from the UE capability information of the supported algorithms. The RANAP CIPHER MODE COMPLETE message returned to the CN indicates the chosen ciphering algorithm. The set of permitted ciphering algorithms specified in the RANAP CIPHER MODE COMMAND shall remain applicable for subsequent Assignments and Intra-UTRAN Handovers.

4. Further clarification

When the CN receives the information of ciphering algorithms from UE, it transfers the information to RNC by using RANAP CIPHER MODE COMMAND message. Nothing should be done in CN.