TSG-RAN Working Group 2 (Radio layer 2 and Radio layer 3) ***TSGR2#3(99) 267***
Yokohama, Japan 13th to 16th April 1999

Agenda Item: 7.5

Source: **Nokia**

Title: HFN initialization

Document for: Discussion and action

---

1. INTRODUCTION

This paper presents one possible solution how to initialize the HFN (most significant bits of UEFN) taking into account possible security risks.

This 'problem' is common for all proposed ciphering methods. The difference between the proposed ciphering methods [1] is that in method 1 (the MAC ciphering) only one HFN is needed, whereas in method 2 (MAC+RLC ciphering) at least two HFNs (or equivalent counters) are needed, possibly even more (one for each parallel radio access bearer).

2. HFN INITIALIZATION

HFN has been described e.g. in [2]. Open question is how to initialize HFN. Following "requirements" exists:

a) Initialise the HFN before the ciphering is activated.

b) Avoid to reuse the same SN value in input of the ciphering algorithm twice or more in a "short" time (especially with the same ciphering key, Kc). This reduces the security of the system.

A problem exists when UE uses the same Kc (ciphering key) in two subsequent RRC connections. If in both connections the HFN is initialised to zero, the same inputs to the ciphering algorithm (FN and Kc) are used twice and the same ciphering mask may be reused in a relatively short period of time. This may occur also with a random initialisation of HFN. This is not 'secure' and should be avoided.

On possible solution to this is that when the RRC connection is released, the terminal (SIM card) stores the last HFN(s) used.

At a new RRC connection setup or at RRC connection re-establishment, UE initialises the HFN(s) to a value higher than the last used HFN(s) value, and transmits this/these to the SRNC, either in the RRC Connection Request message or in the first message after the RRC connection is established.

Depending on the requirements (e.g. how many successive RRC Connections can use the same ciphering key), it may be enough to use only the most significant bits of HFN in the re-initialization (and set LSBs implicitly to zero). This may be necessary at least if the HFN value needs to be included in the RRC Connection Request message.

3. PROPOSAL

It is proposed that the 'problem' identified in this paper is noted in WG2 ciphering documentation (???) and the presented solution is added as one candidate. This item should also be clarified in the possible joint SA WG3 – RAN WG2 meeting.

4. REFERENCES

[1] TDoc TSGR2#3 237 Report from Radio Interface Ciphering email discussion

[2] TDoc TSGR2#2 111 Radio Interface Ciphering, Nokia