TSG-RAN Working Group 2 (Radio layer 2 and Radio layer 3) ***TSGR2#2(99) 124***
Stockholm 8th to 11th March 1999

Agenda Item: 7.7.2

Source: Alcatel

Title: Ciphering function in UTRAN

Document for: Decision

---

1 Introduction

This document addresses the issue of the ciphering function in the UTRAN. It proposes where it should be done for the different transport channels, and what kind of counter it should use. The ciphering function may have a large impact on the radio interface protocol architecture, and it is therefore important to define its main principles. Text proposals for changes in S2.01 are also presented.

2 Location of the ciphering function within the UTRAN radio interface protocol architecture

Based on ETSI/SMG10 requirements, it has been decided by SMG12 (now SA/WG2) that ciphering has to be performed in the RNC. For transport channels using soft handover (i.e DCH), it should be done above the split of links, and therefore in the SRNC. If ciphering was done in the DRNC, this would require a duplication of the ciphering operation in case of inter-RNC soft handover, and the transmission on the Iur would moreover not be protected. For non-real time services, in order to be able to switch easily from DCH to CCH, ciphering should be performed above that split, i.e. above MAC sub-layer.

It is therefore proposed that ciphering be performed in the RLC sub-layer for all services using the acknowledged or unacknowledged mode of RLC, and in the MAC-d for services using the transparent mode of the RLC.

Regarding ciphering counters, SMG10 had requested to use a 32 bits ciphering counter. When ciphering is done in the MAC-d, the counter may use the UEFN, which can be based on 32 bits. When ciphering is done in the RLC, it can not use the UEFN because the RLC does not know at which frame the MAC will schedule the transmission of transport blocks. The counter may then be based on the RLC frame sequence number. However this FS number will not be a 32 bits counter, but probably only a 3 to 5 bits counter (the size is to be determined according to the retransmission protocol). Therefore it is proposed to use this FS counter as representing the Least Significant Bits of a 32 bits counter, whereas the Most Significant Bits of the 32 bits counter would have been exchanged once at the establishment of the connection (in clear or ciphered on a transparent DCH). A counter on 3 to 5 bits should be sufficient to recover from many subsequent frame losses and it will have to be sent unciphered. This two-steps approach for the ciphering counter will avoid a large overhead on the radio interface and the transmission of this short counter will also ease the synchronisation of ciphering between UTRAN and UE.

3 Text proposals for S2.01 document

It is proposed to describe the main principles of the ciphering function in the S2.01 document. Proposed changes are as follows :

In section 7.3.1.2 MAC functions :

- **Ciphering**. This function prevents unauthorised acquisition of data. Ciphering is performed in MAC for services using the transparent mode of RLC. The ciphering counter is based on the UEFN.

In section 7.3.2.2 RLC functions :

- **Ciphering**. This function prevents unauthorised acquisition of data. Ciphering is performed in RLC for services using the unackowledged or the acknowledged mode of RLC. The ciphering counter is based on the RLC frame sequence number (transmitted in the RLC header) representing the Least Significant Bits of a 32 bits counter.

A more detailed description of the ciphering function might be added in MAC and RLC documents once main principles are agreed in RAN/WG2. The editor's notes on ciphering in S2.01 could also be deleted.