3GPP TSG RAN-WG2
August 1999
Sophia Antipolis

Tdoc TSGR2-99845

Source: **Telecom Modus**

Title: **Ciphering procedure on the Radio interface**

Document For: **Discussion**

1 Introduction

This document proposes two possible signaling procedures to establish and maintain ciphering on the Radio Interface.

2 Discussion

The ciphering function is performed in MAC-d or RLC level, depending on the RLC mode used for the logical channel to be ciphered.

The procedure on the radio interface is triggered by the SRNC, by means of a likely RRC message towards the UE (e.g. CIPHERING MODE COMMAND): this message conveys at least the ciphering algorithm to be used. As described in [3], the ciphering on the uplink and downlink channels is started separately. This is achieved by starting deciphering in the uplink immediately at the SRNC after the sending of the CIPHERING MODE COMMAND, and starting ciphering in the uplink and deciphering in the downlink at the UE side, as soon as the RRC message is received. Finally, the SRNC starts the downlink ciphering at the reception of the RRC confirmation message (e.g. CIPHERING MODE COMPLETE) or the first correctly deciphered uplink frame. The message sequence chart resume this mechanism, referring to the case of ciphering on the RLC:

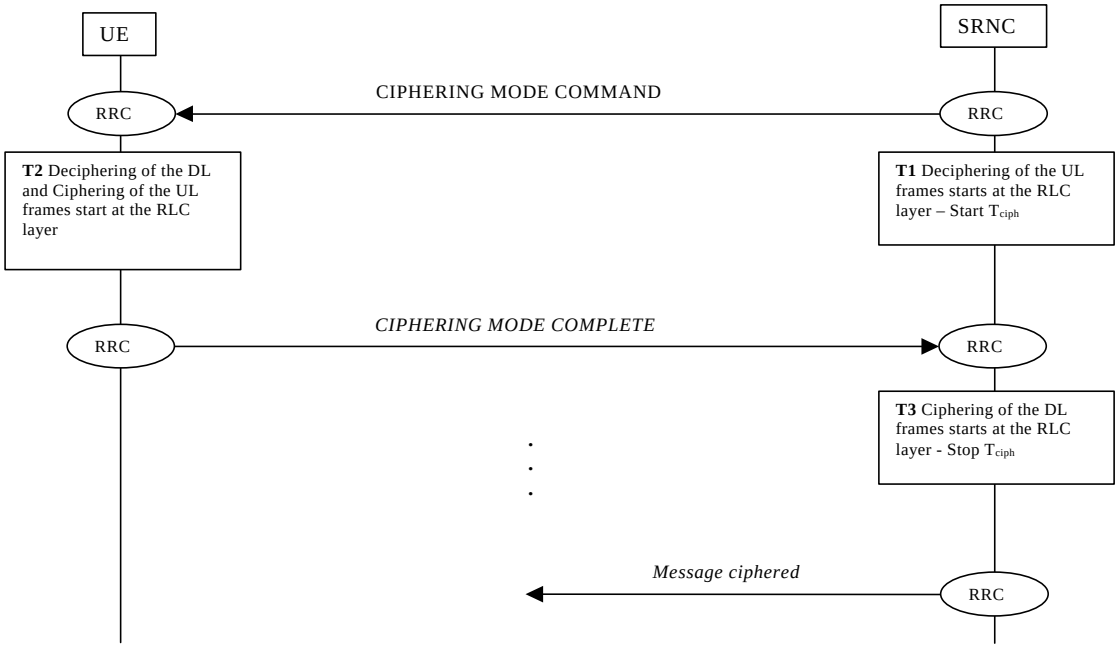


fig.1

This procedure should be used for the Ciphering Key (CK) change as well, because an agreement between SRNC and UE is necessary.

- **Synchronization aspects**

As far the synchronization between SRNC and UE is concerned, it could be possible for any side to receive messages ciphered while the deciphering is not yet started or to receive messages not ciphered while the deciphering is already started. If this case is not very likely in the C-plane (the SRNC should avoid sending messages to the UE, which are not ciphered, between T1 and T3/T_{ciph}), it could be a problem on the U-plane, i.e. for the ciphering of DTCH channels, especially in these cases:

- the CN invokes the ciphering procedure to the RNC while any DTCH is currently used for the related RRC connection.
- the ciphering key CK is changed during a connection (this necessarily involves a sort synchronization between SRNC and UE)

- **Proposed solutions for Synchronization**

RRC solution

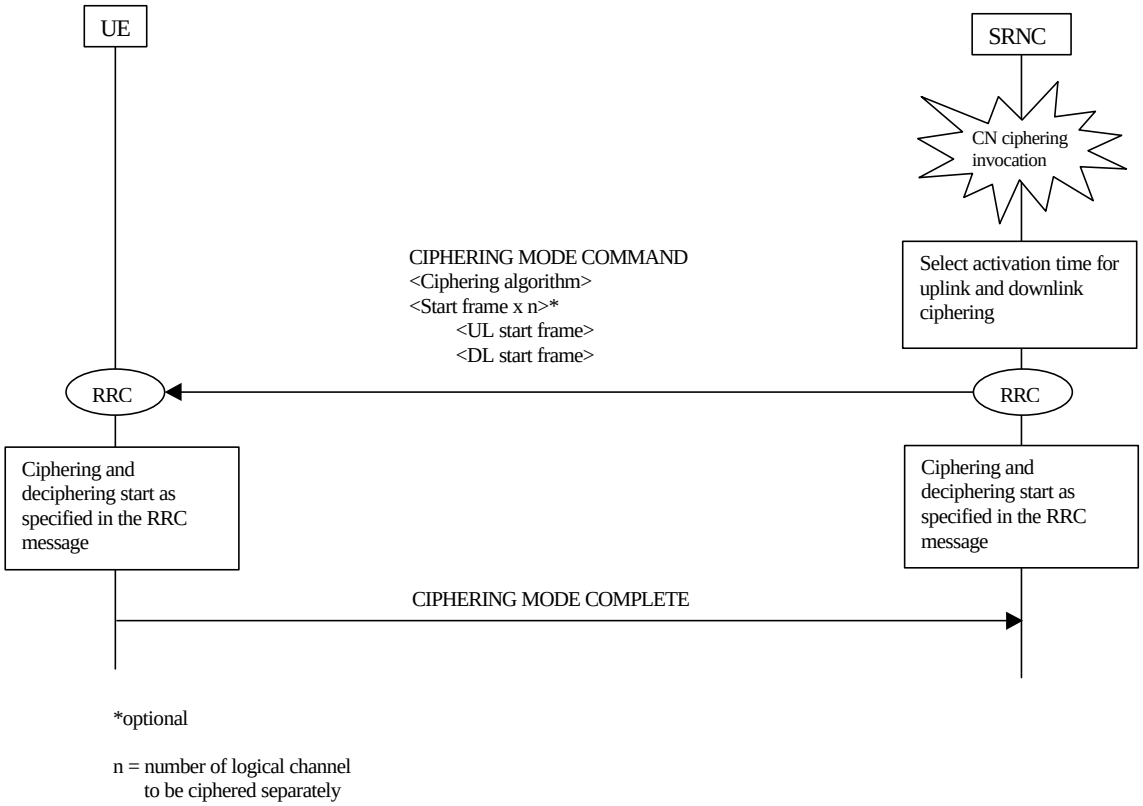
The basic idea is to communicate to the UE the real instant in which the process must start. This instant is identified by a particular value of the Ciphering Sequence Number (CSN), one of the input parameter for the ciphering algorithm [2].

The lower part of the CSN, called short sequence number, would be inserted in the CIPHERING MODE COMMAND to indicate the initial frame for the ciphering/deciphering process on a particular logical channel. The same approach can be adopted for the CK change problem.

An appropriate CSN value would avoid the loss of any data frames. Every channel is generally ciphered using two independent CSN(s), one per direction: they should both be sent to the UE. The setting of the appropriate value for the lowest part of the CSN in uplink and downlink for each ciphering sequence should be done at the RRC level, on the basis of some indication sent by the MAC/RLC sublayer.
It should be noted that there is one ciphering sequence per logical channel using RLC AM or UM mode plus one for all logical channels using the transparent mode (and mapped onto one DCH). A couple of values (uplink and downlink) must be included for each cipher sequence. If, for example, at the ciphering invocation two DTCH(s) in RLC non transparent mode are used, six CSN(s) must be provided, two for the DCCH and two for each DTCH.

The insertion of this information in the CIPHERING MODE COMMAND message could be regarded as optional: in case no information on the CSN is present in the CIPHERING MODE COMMAND, both the SRNC and the UE start autonomously the ciphering process following the rules shown in fig.1.

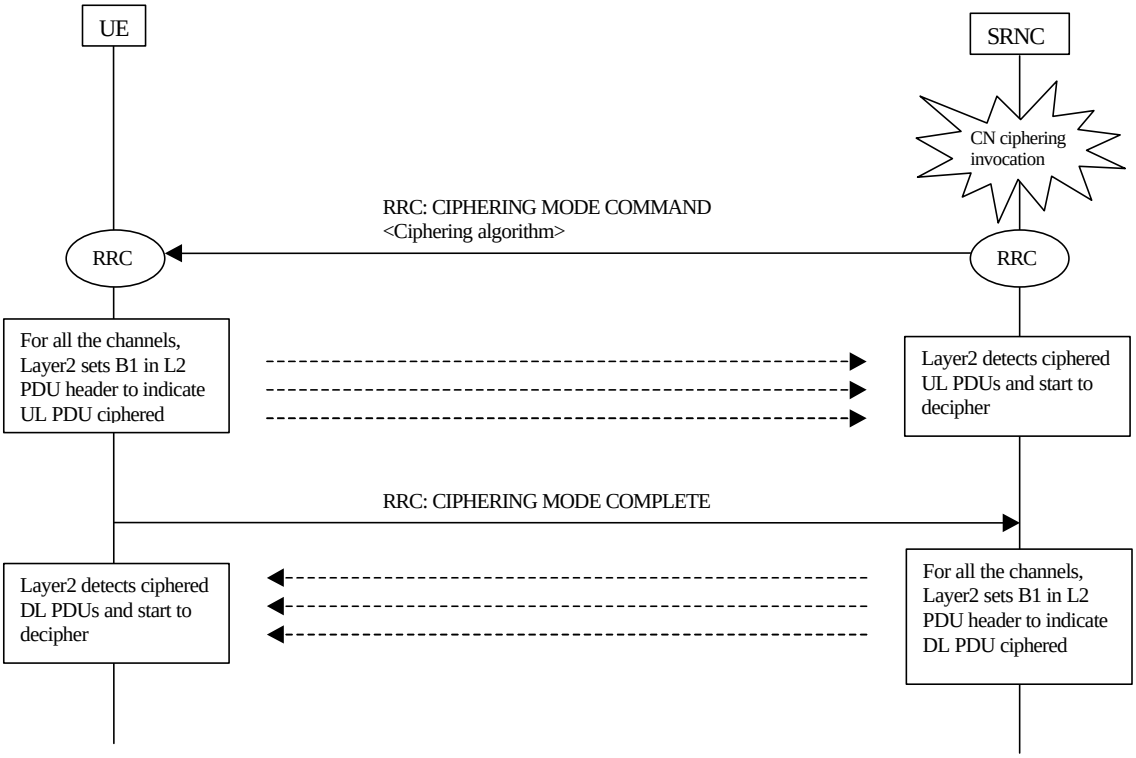
The following figure shows the modified mechanism:



Layer2 solution

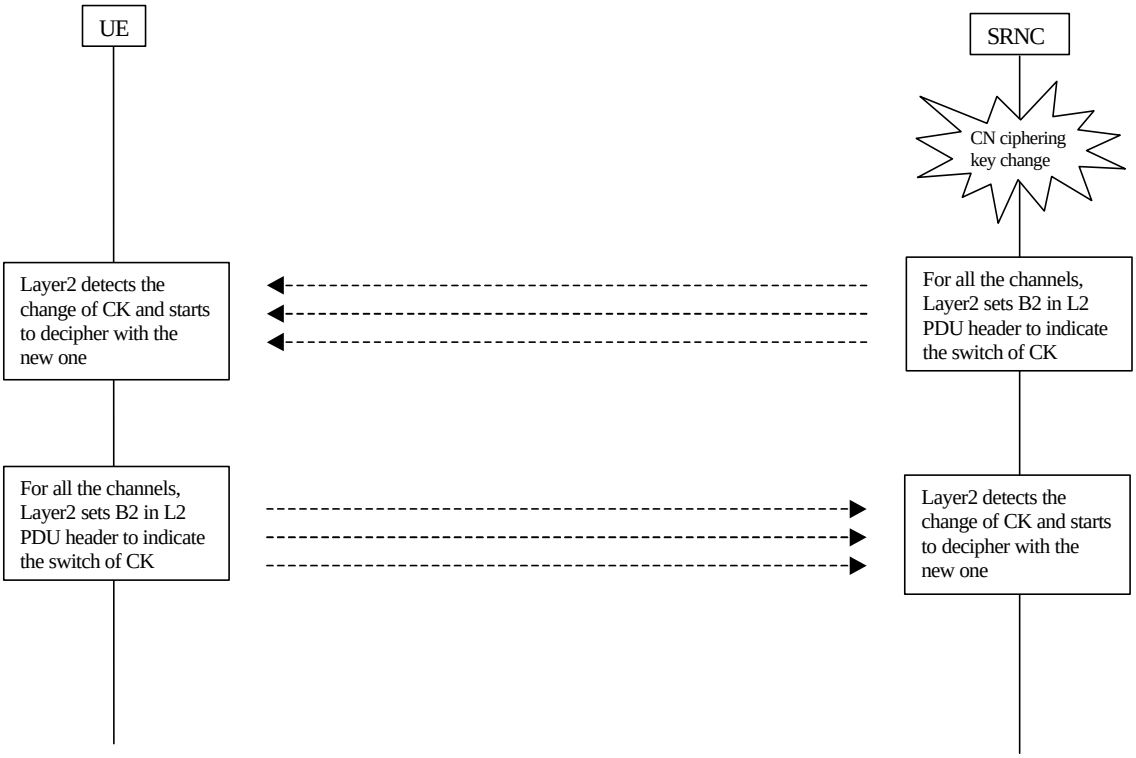
The basic idea is to use an information in the MAC/RLC PDU to indicate if that PDU is ciphered or not and if a switch to the new CK is to occur.
Two bits are enough in the PDU header for this purpose.

The SRNC does not start to decipher just after the sending of the CIPHERING MODE COMMAND message. At the reception of this message the UE shall set the bit (B1) in the first PDU to be ciphered in uplink. At the reception of this PDU the layer 2 in the SRNC shall recognize that it is ciphered and it starts the deciphering process.
The ciphering in the SRNC shall start at the reception of the CIPHERING MODE COMPLETE, setting the bit in the first PDU to be ciphered in the downlink. This PDU will be recognized in the UE as ciphered and the deciphering process will start.



Ciphering initialisation on the radio interface

The other bit (B2) is used to trigger the change of CK. The SRNC shall set this bit in the first PDU ciphered with the new CK; the UE will detect it and start to decipher with the new CK. At the same time, the UE shall start to cipher the uplink channel with the new CK, setting the bit in the first PDU. The SRNC shall recognize it and start the deciphering in the uplink.



Change of Ciphering Key on the radio interface

Advantages: RRC message not necessary in the CK change procedure; ciphering of each DTCH is totally independent from the ciphering of the other ones and this could be useful especially if it will be possible cipher only a subset of DTCH in one RRC connection (FFS).

3 References

[1] RRC Protocol Specification, 25.331

[2] Radio interface Protocol, 25.301

[3] Security Architecture, 33.102