TSG-RAN Working Group 2 (Radio layer 2 and Radio layer 3) **TSGR2#6(99)924**
Sophia Antipolis, France, August 16th to 20th 1999

Agenda Item:

Source: Nortel Networks

Title: **Procedure to change the ciphering key of a connection**

Document for: Approval

Following the discussion on procedures to change the ciphering key of a connection in the two-key solution, (Tdoc R299-829 and Tdoc R299-894), these are the proposed changes to S25.331.

8.3.8.5 Security control procedure

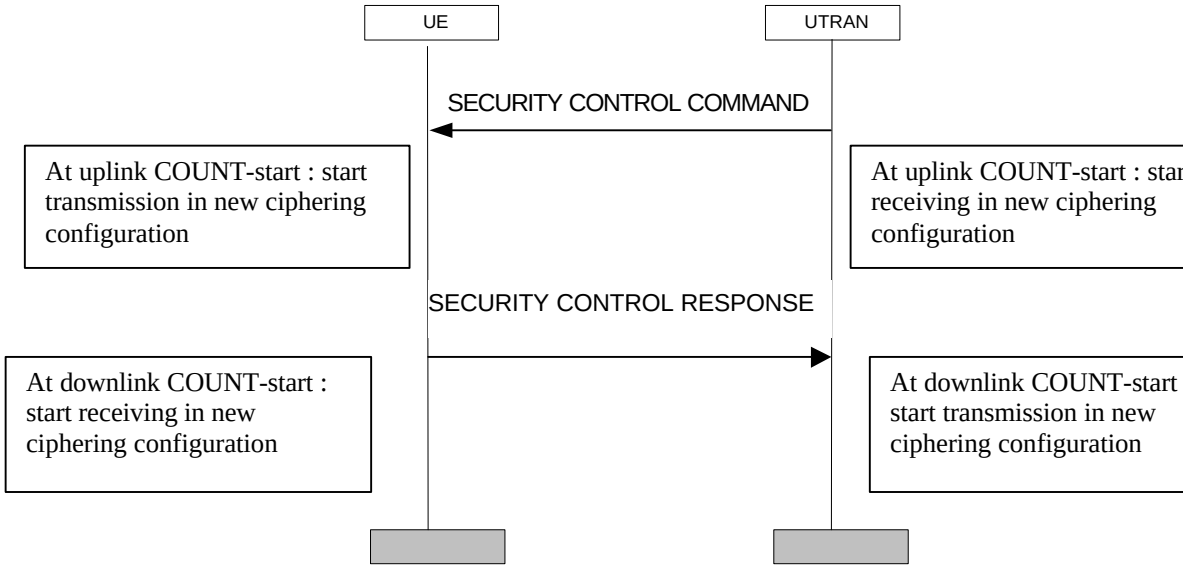

Figure 1*: Security control procedure*

This procedure is used to trigger the start of ciphering, or to command the change of the cipher key, both for the signalling link and for a user plane connection. The ciphering is configured in both directions.

The SRNC sends a SECURITY CONTROL COMMAND to the UE, which indicates the uplink COUNT-start number when the ciphering shall start to be applied in uplink. The SRNC then starts to decipher in the new ciphering configuration at the uplink COUNT-start.

When the UE receives the SECURITY CONTROL COMMAND message, it starts ciphering transmission in the uplink in the new configuration at the uplink COUNT-start number. It sends a SECURITY CONTROL RESPONSE message, which includes a downlink COUNT-start number, and starts to receive in the new ciphering configuration at that COUNT number. When the SRNC receives the SECURITY CONTROL RESPONSE, it starts ciphering transmission in the new configuration at the downlink COUNT-start.

Note : The same procedure can be used for integrity control. But this is FFS.

10.1.7.4 SECURITY CONTROL COMMAND

RLC-SAP: t.b.d.
Logical channel: DCCH
Direction: UTRAN to UE

Information element category	Information elements	REFERENCE	TYPE	NOTE
	Message Type		M	
CN Information Elements	CN domain identity		M	Indicates which cipher key is Applicable
RAB Information Elements	Radio bearer identity 0		M	Indicates the signalling link
	Radio bearer identity 1		O	For each radio bearer identity Start of the new ciphering configuration in uplink
	COUNT-start 1		O	
	COUNT-start n		O	
	Radio bearer identity n		O	
	COUNT-start n		O	

10.1.7.5 SECURITY CONTROL RESPONSE

RLC-SAP: t.b.d.
Logical channel: DCCH
Direction: UE to UTRAN

Information element category	Information elements	REFERENCE	TYPE	NOTE
	Message Type		M	
RAB Information Elements				
	Radio bearer identity 1		O	For each radio bearer identity : Start of the new ciphering configuration in downlink
	COUNT-start 1		O	
	.....			
	COUNT-start n		O	
	Radio bearer identity n		O	
	COUNT-start n		O	

10.2.8.3 COUNT-start

This Information Element indicates the ciphering sequence number at which the new ciphering configuration (e.g. new cipher key) starts to apply. It can be used for both directions.

Parameters	REFERENCE	TYPE	NOTE
COUNT-start		M	