3GPP TSG SA WG3 Security — S3#15 **S3-000522**

12-14 September, 2000

Washington D.C., USA

Source: France Telecom, Telia

Title: Rejection of non ciphered connections

Document for: Approval

Agenda Item:

We propose to introduce the following mechanism for packet connections for 2G and 3G systems release 2000. The need for this feature in circuit switched domain seems less important.
It should be noted that the mechanism described below shall NOT be applied in the case of emergency calls.

Mechanism:

There is a parameter in the ME that can take two values:

Value 0 (default): The terminal rejects non-ciphered connections.
When a ciphered connection is not possible to establish because no common algorithm is available in the cipher mode setup, connection setup is halted and the ME informs the user about this. At the same time the ME offers the user the possibility to change the parameter value to 1. If the user changes the parameter, the connection setup procedure is continued. If the user does not change the parameter the connection set up is now rejected. The rejection of the call should happen if the user confirms he refuses the connection or if the terminal receives no answer after a certain time.

The rejection of a non-ciphered connection is done in the terminal and implemented along the ciphering indicator. In case of the rejection of a non-ciphered connection by the terminal, the terminal might need to inform the network if the network needs to take actions upon this rejection. N1 should be the group deciding whether the network needs that information and define what has to be done in such a case. It seems likely that if the PDP context is to be deleted, the network shall receive a proper message in order to realize that deletion.

Value 1: The terminal accepts non-ciphered connections. This state is a temporary one.

Note that a non-ciphered connection shall only be allowed to be set up if no common algorithm has been found in the cipher mode setup, independent if the value of the parameter is set to 1. If the connection is set up, as non-ciphered, this fact shall be displayed by the ciphering indicator.

Whenever a **ciphered** connection is established, the ME parameter value reverts to 0. This ensures that if the user has been communicating in a non-ciphering network and comes to a ciphering network (the general case), rejection of non-ciphered connections is activated again.

Also whenever a new SIM card is inserted in the ME (or is detected to have been inserted after power up) the parameter shall revert to 0.

By default, we expect that terminals should have the default value 0 built in, with the exception of the operators that do not use ciphering in their network and would specifically ask for value 1 (which would be a limited number of operators hopefully). Since the mechanism is designed to be simple, we do not expect that the user would need to manually change the value of the parameter in normal operation (the user would just manually confirm the change from state 0 to state 1).

It should not be possible to change the ciphering mode of a connection once that connection has been established. It remains to be further investigated if this is not already the case.

Work to be done and involved groups:

CN needs to be involved to define how the networks reacts when it is informed that a non-ciphered connection has been initially rejected (if not already covered by the case “no common algorithm has been found”) and specifically in the case when the user chooses to change the parameter value directly so that a non-ciphered connection setup can proceed.

T2 needs to be involved to introduce the rejection of non-ciphered connections by the terminal according to the parameter, the automatic changes to the parameter and the MMI for user setting of the parameter value.

S3 to revisit “old 03.20” to check cipher mode setup for GPRS and to introduce needed changes in 3G security architecture.