3GPP TSG SA WG3 Security — S3#16 **S3-000681**

28-30 November 2000, Sophia Antipolis

Source:	France Telecom, Telia
Title:	Rejection of non ciphered connections
Document for:	Discussion, 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.[But a clear decision must be made by S3 and probably S1]
It should be noted that the mechanism described below shall NOT be applied in the case of emergency calls.

Mechanism:

For backward compatibility purposes we should have a flag in the terminal, in order to offer the service with old SIM (or R99 USIM) that would not have a flag in them. Therefore we need a parameter in the terminal and, optionally, in the SIM/USIM (that overrides the parameter in the terminal) that can be transferred to the terminal.

The term CM connection used in the following descriptions means either a PS PDP context or a CS CC, SS or SMS connection.

The ME specific parameter can take four values:

Value 0 (default): The terminal rejects non-ciphered CM connections.
When a CM connection is established non-ciphered or if for a already established ciphered CM connection ciphering is disabled the connection shall be rejected or released by the ME and the ME informs the user about this. At the same time the UE offers the user the possibility (via the MMI) to change the parameter value to 1, so that future non ciphered CM connections will be accepted.

The rejection of a non-ciphered connection is done by the ME. 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.

Value 1: The terminal accepts non ciphered CM connections (temporary state)
If the connection is set up, as non-ciphered, this fact shall be displayed by the ciphering indicator.

Whenever a **ciphered** CM connection is established or ciphering is enabled on a already established CM connection, the parameter value is set to 0 by the ME. This ensures that if the user has been roaming in a non-ciphering network and comes back to a ciphering network (the

general case), rejection of non ciphered connections is activated automatically again. Also whenever a new SIM card is inserted in the ME or the ME is switched on the parameter shall be set to 0 by the ME.

Value 2 and Value 3: These can be set by the SIM/USIM. If the SIM/USIM does not support a field to store the parameter value (see below), the ME does not use these values.

Value 2: The terminal rejects any non ciphered CM connection, and informs the user. The user may not have the possibility to change the parameter value in the terminal.

Value 3: The terminal accepts any non ciphered CM connection. This state is permanent and even if a ciphered connection is established, the value does not change. The user may not have the possibility to change the parameter value in the terminal.

By default, all terminals should have the default value 0 built in. 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, and that only once at each time he roams to (or comes back to) a network where ciphering is not possible.).

Control by the SIM/USIM

It should be possible to have the control of the terminal parameter from the SIM/USIM. In the case where the SIM/USIM supports that parameter, it shall override the parameter in the terminal. When the terminal is powered up, or a SIM/UICC inserted in it, the value in the SIM/USIM is read by the ME and overrides the previous setting in the terminal.

The SIM/USIM parameter shall only be possible to be set to value 0, 2 or 3.

In practice, when the SIM/USIM parameter does not exist, the ME behaves as if it was a value 0 and if it had only the ME specific parameter set to 0. Only when roaming to networks where ciphering is not possible the terminal temporarily takes on value 1.
When the parameter exists in the SIM/USIM, it opens two new possibilities for operators.

Work to be done and involved groups:

S1 involvement needed? (rejection of circuit switched non-ciphered calls)

CN1 needs to be involved because the call set-up procedure is affected.

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. Also, the ME shall be able to receive the SIM/USIM parameter and behave accordingly to it.

T3 needs to be involved to define the storage of the SIM/USIM parameter and its provision over the SIM-ME or USIM-ME interface.