3GPP TSG SA WG3 Security — S3#14 **S3-000497**

1-4 August, 2000, Oslo

Source:	France Telecom
Title:	Rejection of non ciphered connections
Document for:	Approval
Agenda Item:	7.10

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:

Two parameters will be present to define the rejection of non ciphered connections. One will be in the terminal (mandatory), and one in the SIM/USIM (optional). In case the SIM/USIM parameter is present, it should override the parameter in the terminal. The ME then behaves according to the SIM/USIM parameter (the ME parameter is unchanged and unused).
This is intended to make the mechanism work even if the user owns an SIM/USIM that does not have this parameter.

Case where there is no parameter on the SIM/USIM:

There is a parameter in the ME, that can take two values:
Value 0 : when a non ciphered connection is established, the user is informed and if he accepts it, the value switches to 1 and the call is established. Otherwise the connection is rejected. The ME can detect that event when a start cipher command is received indicating no encryption. This applies to both outgoing and incoming calls). In that case, we believe the PDP context should be deleted.
Value 1: the terminal accepts non ciphered connections.

We suggest that default value should be 0

Whenever a **ciphered** connection is established, the ME parameter value reverts to 0. 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 again.

Case where there is a parameter on the SIM/USIM:

That parameter is copied by the SIM/USIM to the ME when the ME is powered up or the SIM/USIM is inserted into the ME. This parameter overrides the terminal parameter which is then ignored (and remains the same whatever the value of the SIM/USIM parameter) by the ME.

The value of the parameter in the SIM/USIM is not changed by the ME and all changes to the parameter described below apply to the ME copy of the parameter.
The parameter originating from the SIM/USIM could take 3 values:
0 and 1 are defined like in the ME:
Value 0: when a non ciphered connection is established, the user is informed and if he accepts it, the value switches to 1 and the call is established. Else the connection is rejected.
Value 1: non ciphered connections are accepted, but the value reverts to 0 when a ciphered connection is established
Value 2: non ciphered connections are accepted and the parameter value does not change, whether a ciphered connection is established or not (for networks that do not use ciphering).

We suggest that default value should be 0 (for networks that apply encryption) or 2 (for networks that do not apply encryption). Value 1 should be an intermediate state for roaming situations.

The rejection of a non ciphered connection is done in the terminal and implemented along the ciphering indicator. Terminals behave according to the value of the parameter, sending if needed information to the user and either proceeding with the connection or releasing it.

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 that information is needed by the network 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.

Change of the ciphering status of a connection once the connection is established

It might be possible to change the ciphering mode of a connection once that connection has been established (using the security mode command in 3G, ??? in 2G). In that case, the same mechanism should be applied when that command is received, in the same way as it happens when a connection is established. This remains to be further investigated if the same process can be adopted (in particular in regard to the PDP context deletion).
.

Work to be done and involved groups:

CN needs to be involved to define if (and if yes, how) the networks reacts when it is informed that a non-ciphered connection has been rejected.
T2 needs to be involved to introduce the rejection of non ciphered connections by the terminal according to the parameter, for modifications of the SIM/ME and USIM/ME interfaces.
T3/SMG9 needs to be involved to define this new parameter and to include modifications necessary on the SIM/ME and USIM/ME interfaces.