TSG-Terminals Working Group 3 (USIM) meeting #1
Nice 25th - 27th January, 1999

TSGT3#1(99)027

Liaison to TSG-SA WG3 (Security)

Source: **TSG-T3 (USIM)**

Title: **Variable length of security-related parameters**

The security architecture and authentication framework is a key building block in the design of the 3GPP USIM.

In TSG-T3, a proposal was made to allow for variable lengths of the security-related parameters (e.g., RAND, SRES, Kc) to ensure future-proofing. This would allow to easily extend the strength of the algorithm later on if so required.

To meet the very tight time scales of the USIM work, an input with guidelines on this matter would be appreciated for the 2nd meeting of TSG-T3 (17.-19. February, 1999).