3GPP TSG SA WG3 Security — S3#20 **S3-010555**

16 - 19 October, 2001

Sydney, Australia

Source:	**TSG-SA WG3**
To:	**TSG-RAN WG2**
Title:	**Response to LS from RAN2 (R2-011763) on Security Mode Reconfiguration**
Contact person:	**Guenther Horn**

Guenther.horn@mchp.siemens.de
Phone: +49 89 636 41494

In their LS, RAN2 asks the following question:

Is it possible that the ciphering algorithm or/and the integrity protection algorithm is changed while the security key set is kept unchanged during the security mode reconfiguration?

SA3 would like to thank RAN2 for raising this question. SA3 can provide the following answer:

It is good security practice not to use the same key with two different algorithms. For Rel'99, Rel4 and Rel5 no problems can arise from this as there is only one confidentiality algorithm and one integrity algorithm. The current specifications (in particular TS 33.102), however, allow that a security mode set-up procedure (which may be used to change the algorithms) is run without a previous authentication, (i.e. in particular without a change of the cipher and integrity keys). This makes sense as a security mode set-up is needed for every connection set-up, but an authentication should not be required for every connection set-up. However, this implies that, if in future releases more confidentiality and integrity algorithms are introduced, then changes to the specifications will be necessary to ensure that the same key is not used with two different algorithms. SA3 will keep this in mind when working on future releases.