

3GPP TSG SA WG3 Security — S3#18

S3-010290

21 - 24 May, 2001

Phoenix, USA

Source: TSG-SA WG3

To: GERAN

Title: Reply to LS on revised working assumptions made at joint GERAN/S3 meeting

Contact: Michael Walker, Vodafone Group, SA3 Chair
Email: mike.walker@vodafone.co.uk

S3 would like to thank GERAN for the liaison statement in S3-010150 (GAHW-010245).

With regard to the use of MACs (message authentication codes) for integrity protection. S3 is in agreement with the defacto industry position that a MAC of less than 32 bits does not provide adequate integrity protection. In particular, a MAC of 24, 16 or 8 bits is so vulnerable as to not warrant the effort expended in computing or verifying it.

S3 therefore advise that RLC/MAC control messages in GERAN should not be integrity protected unless a full 32 bit MAC-I can be provided in all cases for a particular message – anything less presents a totally false sense of security.