3GPP TSG SA WG3 Security — S3#20 **S3-010537**

16 - 19 October, 2001

Sydney, Australia

Title: **Liaison Statement on HFN Reset and THRESHOLD**

Source: S3

To: RAN2

Cc:

Response to:

Contact Person:

Name: Greg Rose
Tel. Number: +61 2 9817 4188
E-mail Address: ggr@qualcomm.com

Attachments: S3-010474, S3-010476

---

1. Overall Description:

S3 would like to bring attention to two recent changes to RAN2 documents which have had consequences for security and/or documents under the control of S3.

The first of these concerns the RESET procedure, which was changed to allow the HyperFrame Number HFN to be resynchronised. The variable COUNT-C is derived from HFN, and it is a critical assumption for UMTS security that COUNT-C values shall not be repeated during the lifetime of a ciphering or integrity key. Tdoc S3-010476 (attached) examines this problem and some possible solutions. S3 would prefer that the RESET procedure be constrained so that only increasing HFNs could be specified, possibly restricted to be only slightly (1 or 2) larger than the current HFN value.

The second issue concerns a mismatch between the words “reaches” and “is greater than” in relation to START and THRESHOLD. It was S3’s intent that “reaches” means “greater than or equal to”. See Tdoc S3-010474 for a CR to 33.102 which attempted to align the two specifications. This CR was not accepted as the required changes are more far-reaching than was at first realised.

In both of these cases security problems have been introduced without the changes being referred to S3. S3 requests that any changes to text involving keys, HFN values, COUNT, START, or THRESHOLD should be referred here, as the security issues might be subtle but quite important.

2. Actions:

To RAN2 group.

ACTION: S3 requests that RAN2 review the HFN Reset procedure, and in future refer changes involving security parameters to S3.

3. Date of Next S3 Meetings:

S3 #21	27-30 November, 2001 (Sophia Antipolis, France)
S3 #22	26 February-1 March, 2002 (Bristol, UK)