3GPP TSG SA WG3 Security — S3#23 **S3-020238**
14 - 17 May 2002
Victoria, Canada

SAGE (02) 21

Liaison Statement

To: **3GPP SA3**

From: **ETSI SAGE**

Subject: **Test data for MILENAGE algorithm**

The test data for the MILENAGE algorithm has been designed by SAGE to fully test the algorithm against the requirements of 3G TS 33.105.

ETSI notes that a comment has been made that in practice the value of AMF is set to 0 (all zeros) in order to generate f1* and that the test data does not contain tests sets where the value of AMF is set to 0.

Though this should not be a problem when testing a MILENAGE implementation against the specification, SAGE can provide test data for which the value of AMF is set to 0 (all zeros). Two such test sets are given below.

TEST SET 1

K:	465b5ce8 b199b49f aa5f0a2e e238a6bc
RAND:	23553cbe 9637a89d 218ae64d ae47bf35
SQN:	ff9bb4d0 b607
AMF:	0000
OP:	cdc202d5 123e20f6 2b6d676a c72cb318
OPc:	cd63cb71 954a9f4e 48a5994e 37a02baf
f1*:	cf44e935 96e355c6

TEST SET 2

K:	0396eb31 7b6d1c36 f19c1c84 cd6ffd16
RAND:	c00d6031 03dcee52 c4478119 494202e8
SQN:	fd8eef40 df7d
AMF:	0000
OP:	ff53bade 17df5d4e 793073ce 9d7579fa
OPc:	53c15671 c60a4b73 1c55b4a4 41c0bde2

f1*: 1fb5eba7 4924b0e0