

3GPP TSG SA WG3 Security — S3#18

S3-010167

21 - 24 May, 2001

Phoenix, USA

**3GPP T3 Meeting #19
St John, US VI, 8 - 11 May, 2001**

Tdoc T3-010324

Liaison Statement

Source: TSG-T3

To: TSG-T1

Copy: TSG-SA3

**Subject: LS on authentication test algorithm to be
implemented in test USIM**

Contact Person: JF Rubon (<mailto:jean-francois.rubon@gemplus.com>)

TSG-T3 received a copy of the LS sent by S3 (S3-010137) to T1 regarding the test algorithm to be implemented in test USIMs.

TSG-T3 sent an LS on that matter (T3-010246) to T1, in which T3 agreed on the CR to 34.108 proposed by T1 (T1-010082).

TSG-T3 would like to comment that any further change on the test algorithm would cause delay in the implementation.

Furthermore, about the point raised by SA3 (f1 being identical to f1*), T3 would like to point out that if the test USIM is used to test MEs, it does not matter if f1 is identical to f1*. Both functions are implemented in the USIM as parts of the authentication algorithm, and therefore the ME cannot trigger f1 instead of f1*.

3GPP T3 Meeting #19
St John, US VI, 8 - 11 May, 2001

Tdoc T3-010269

3GPP S3 Meeting #17
Gothenberg, Sweden, 27 Februar – 2 March,
2001

S3-010137

Liaison Statement

Source: TSG-SA3

To: TSG-T1

Copy: TSG-T3

**Subject: LS on authentication test algorithm to be
implemented in test USIM**

Contact Person: Marc Blommaert(<mailto:Marc.blommaert@siemens.atea.be>)

TSG SA3 would like to thank TSG T1 for updating the test algorithm as reported by Liaison Statement T1-010105.

SA3 likes to bring T1 under the attention that the functions f1 and f1* are identical defined in T1-010082 (CR on 34.108) and consequently the usage of f1 in stead of f1* during the test of the re-synchronisation procedure is undetectable. The same concern applies to the definition of f5 and f5*.