3GPP TSG SA WG3 Security — S3#10 **S3-000026**

19-21 January, 2000

Antwerpen, Belgium

Source:	**ETSI SAGE 3GPP Task Force**
Title:	**Results of independent evaluation of 3GPP f8 and f9 algorithms**
Document for:	**Discussion**
Agenda Item:	

LIASON STATEMENT

To:	3GPP TSG SA WG3
From:	ETSI SAGE 3GPP Task Force
Date:	28th December 1999
Topic:	Results of independent evaluation of 3GPP f8 and f9 algorithms

The ETSI SAGE Task Force for the design of the 3GPP Confidentiality and Integrity Algorithms (SAGE TF 3GPP) has received the reports from all three of the teams paid to evaluate the proposed 3GPP encryption and integrity algorithms.

The evaluations are of high quality and the evaluation teams have provided detailed reports.

The headline from all three evaluations is that no practical attacks on the algorithms were found. The best attacks found on reduced or simplified versions suggest that the algorithms also include a reasonable amount of leeway ("security margin") against possible improvements in cryptanalytic techniques. The attacks found by the evaluators did not differ substantially from those anticipated by the designers.

It was inevitable that the evaluators would make suggestions for change to the algorithms. We considered each of these suggestions in detail. We accept that some of them would increase the security margin, but at the expense of increasing the running time and/or power requirements; we decided in the end that the algorithms as they stand strike the right balance between these two objectives. We therefore will submit the algorithms unchanged to 3GPP.

There were two suggestions from the evaluators that did not require changes to the algorithms themselves. One was for an additional set of statistical tests, which we have since performed. The other concerned what to do if either algorithm were to be used with a cryptographic key of fewer than 128 bits; we accept this recommendation and therefore pass it on as a recommendation to 3GPP. Details are given in a separate liaison statement (ETSI SAGE 3GPP Task force (99) 51).

ETSI SAGE TF 3GPP thanks 3GPP and Ericsson for their funding of the evaluation, and the evaluators themselves for their excellent work, which has given us great confidence in the algorithms we are submitting.