

19-21 January, 2000

Antwerpen, Belgium

Source: ETSI SAGE 3GPP Task Force

Title: Finalisation of the f8 and f9 algorithm design work

Document for: Discussion

Agenda Item:

LIASON STATEMENT

To: 3GPP TSG SA WG3
From: ETSI SAGE 3GPP Task Force
Date: 28th December 1999
Topic: Finalisation of the f8 and f9 algorithm design work

The ETSI SAGE Task Force for the design of the 3GPP Confidentiality and Integrity Algorithms (SAGE TF 3GPP) has finalised its work.

The last phase in the work was an independent evaluation of the algorithms by three groups of evaluators. The results of these evaluations and consequent decisions of ETSI SAGE TF 3GPP are summarised in liaison statement ETSI SAGE 3GPP Task force (99) 50.

ETSI SAGE TF 3GPP will deliver before the end of 1999 the following three documents to the chairman of 3GPP TSG SA3.

- (1) The algorithms specifications (4 part document)
- (2) A report on the work undertaken by ETSI SAGE TF 3GPP
- (3) A report on the evaluation of the algorithms

All documents can be made public. Document 3 contains detailed information on the algorithms. So if 3GPP should decide that, for whatever reason, the algorithms specifications (document 1) will not be published, it should also be considered to keep document 3 confidential.

The decision on and method for publication of the documents is left to 3GPP. However ETSI SAGE TF 3GPP again recommends publishing all documents, since this will increase public confidence in the algorithms.

If needed document 2 and 3 can be published as formal ETSI SAGE reports. Should this be required then 3GPP TSG SA3 is requested to inform ETSI SAGE. It is also possible for 3GPP to comment on these documents.