3GPP TSG SA WG3 Security — S3#10 **S3-000057**

19-21 January, 2000

Antwerpen, Belgium

Source: **Vodafone**

Title: **Draft LS to SAGE on the design of a standard authentication algorithm**

Document for: **Approval**

Agenda Item:

To:	**ETSI SAGE**
Copy	**GSM Association Security Group, 3GPP TSG T WG3 / ETSI SMG9**
From:	**3GPP TSG SA WG3**
Title:	**Authentication algorithm for 3GPP**

S3 would like to provide an authentication algorithm for 3GPP that could be used by operators that do not wish to provide one of their own. SAGE are kindly asked to consider whether they would be willing and able to act as the design authority for such an algorithm following a similar procedure used for the development of the cipher/integrity algorithms for 3GPP.

The basic principles of the algorithm design, as agreed by S3, are listed below:

- It is required that the algorithm fulfill the requirements specified in 3G TS 33.105. In particular, it is required that controlled personalisation of the algorithm is possible based on a 128 bit operator variant key.
- It is desirable that the algorithm is designed around a replaceable kernel function to provide an additional degree of variety. However, the decision on whether to provide an additional level of variety in this way is left to SAGE since S3 do not want to impose undue contraints on the algorithm design process.
- If an algorithm is to be designed around a kernel function, then it is required that one specific kernel function is provided.
- If an algorithm is to be designed around a kernel function, then it is desirable that a list of suitable alternative kernal functions is provided.
- If an algorithm is to be designed around a kernel function, then it is desirable that standard / publicly available algorithms may be used to implement the kernel function. However, the type or types of kernel function that could be supported is left to SAGE.
- It is required that the algorithm is resistant to Simple Power Analysis, Differential Power Analysis and other side-channel attacks as appropriate when implemented on a USIM. It is acknowedged that SAGE may need to consult with smart card experts in order to be able to address this requirement.

The algorithm would be published as a 3GPP specification. Based on the likely timescales for 3GPP implementation, the specifications are required within the next 6 months.

It is understood that the GSM Association Security Group are intending to ask SAGE to develop a new algorithm for GSM, known as COMP128-3. S3 request that the GSMA make the requirements specification available to 3GPP and consider developing an algorithm which may also be used for 3G.

Attached:

CR-xx to 3G TS 33.105 Cryptographic algorithm requirements: This CR contains the requirements on the 3G authentication algorithm. The requirements were updated and approved based on a technical discussion at S3#10. The CR will be submitted for approval at SA#7 in March.