Technical Specification Group Services and System Aspects
Meeting #3, Yokohama, Japan, 26-28 April 1999

TSGS#3(99)142

Source: **SA WG3 chairman**

Title: **Proposed method for acquiring cryptographic algorithms for 3G systems**

Document for: **Discussion / Approval**

Agenda Item: **5.3.2**

A document has been drafted by SA WG3 which discusses the possibilities for acquiring cryptographic algorithms for 3G systems. It considers possible design strategies, evaluation strategies, the possibilities for the distribution of the algorithms, and the options for the liability and responsibility for the algorithms. The advantages and disadvantages of several of the more realistic scenarios were considered and based on this SA WG3 have proposed the following method.

SA WG3 will create the algorithm requirements specifications which will be passed to an algorithm design group (e.g. ETSI SAGE) for design, or selection, of the algorithms, followed by a commissioned, closed evaluation of the algorithms and finally, the production of the 3GPP algorithm specifications. The algorithm specification will then be made available for public evaluation. Part of the public evaluation will run in parallel with the implementation phase, due to timescale requirements. It is recognised by SA3 that an open evaluation will leave any algorithm open to criticism during the commercial operation of the system. The process of responding to public criticism of the algorithm in this case will need to be carefully handled by an appropriate 3G body.