Source: **TSG SA**

Title: **Financing Requirements for 3GPP Ciphering development work**

Agenda item: **8**

Document for:

Decision	**X**
Discussion	
Information	

1 Introduction

During 3GPP TSG-SA #3 in Yokohama TSG-SA discussed the attached document TSGS#3(99)142 method for acquiring cryptographic algorithms for 3G systems.

TSG-SA agreed that TSG SA WG3 will create the algorithm requirements specifications which will be passed to an algorithm design group 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. TSG-SA agreed that the best suitable design group will be the ETSI SAGE. The design group will be requested to provide a detailed time plan to TSG-SA (TSG_SA WG3). This should allow TSG-SA to monitor the progress of the work and the fulfilment of the overall time schedule.

It was further agreed that the algorithm specification would then be made available for public evaluation. Part of the public evaluation, should run in parallel with the implementation phase, due to time scale requirements. IT was fully understood by TSG-SA that an open evaluation would leave any algorithm open to criticism during the commercial operation of the system. Therefore the process of responding to public criticism of the algorithm will need to be carefully handled.

The above mentioned decision has some financial impacts, as there is a need to pay for the work performed by the design group as well as for the external evaluation. The total cost is estimated to **330.000 Euro**, some more details on the estimate of the required funding is provide in section 2 of this document. It should be noted that in order to ensure fulfilment of the tight time schedule, the question of funding need to be resolved by end of June 1999.

> ***The 3GPP PCG and 3GPP organisational partners are requested to discuss how to provide the financing of the ciphering algorithm development. This discussion should conclude in availability of the necessary funding no later than by the end of June 1999.***
>
> ***Further there is a need for defining the ownership of the algorithm. This should also be discussed and decided upon by the PCG.***

2 Funding of the 3GPP Ciphering work

Based on the decisions of TSG-SA the cost of the ciphering work has be estimated as stated below, by the TSG-SA WG3 chairman Mike Walker. The below figures needs final verification, to ensure that

the cover all costs)

ETSI SAGE would need about 2 man-year of effort. 300 000 Euro

ETSI SAGE will pay for the external evaluation. Approximately 30 000 Euro

In total (needs to be verified) 330 000 Euro

Payment of SAGE is assumed to be through ETSI and on a monthly basis once the work starts.

Technical Specification Group Services and System Aspects ***TSGS#3(99)142***

Meeting #3, Yokohama, Japan, 26-28 April 1999

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.