Technical Specification Group Services and System Aspects
Meeting #7, Madrid, Spain, 15-17 March 2000

TSGS#7(00)131

Source: MCC

Title: Status of Ciphering and Integrity Algorithm distribution

Document for: Information

Agenda Item: 8

1 Introduction

3GPP has developed Ciphering and Integrity algorithms (otherwise known as the f8 and f9 algorithms) for the 3GPP system. These algorithms were prepared by the ETSI SAGE group with additional participation by other 3GPP Individual Members. The algorithms have been approved by SA3 and will be approved by TSG SA during this meeting.

[Note: due to the confidentiality of these algorothms they have not been distributed within SA3 and will not be distributed within TSG SA].

2 Traditional approach to algorithm distribution

Traditionally, such algorithms which have been distributed in paper form only and on satisfactory completion of an application form and non-disclosure agreement. It has been necessary to apply to the national authorities for an export licence before the algorithm can be despatched outside of the home country and this had led to delays and subsequent complaints from Industry.

In more recent months, there has been increasing pressure to openly publish security algorithms which would end the problems associated with export licences. Such a move is strongly promoted by the ETSI SAGE, and TSG SA3 committees, these representing the core competence on security algorithm issues within 3GPP. They firmly believe that the best demonstration of the quality of their work is by making it openly available and thereby subject to public scrutiny. It is also believed that this will prevent the frequent claims (often by academics) that the algorithms have been obtained and that this in itself is portrayed as a security weakness.

The open publication process is not new, since many such algorithms outside of 3GPP are already published in this way, particularly in the case of Internet security algorithms.

3 Discussion by 3GPP Partners

The 3GPP Partners have discussed the merits of open publication, but have also discussed the urgent need for these algorithms to be made available to Industry without delay.

The Partners have agreed that in the first instance they would pursue the traditional approach by preparing a 3GPP "Management Agreement" for the distribution of the 3GPP algorithms, whereby each Partner becomes a "Custodian" of the algorithms and distributes them to successful applicants in their country or region.

In parallel to this proposal, the Partners are pursuing the possibility of open publication.

4 Current status

The current situation is as follows.

a) The Algorithms have been delivered by ETSI SAGE to the ETSI Director General and are ready for distribution.
b) The “Management Agreement” has now been prepared and will be signed during the week of 15 March by ARIB, ETSI, T1 and TTA (“The Custodians”).
c) The algorithms will be delivered to the “Custodians” at the time of signing the “Management Agreement”.
d) Applicants who wish to obtain the algorithms may submit their applications to one of the Custodians from week commencing 20 March

5 Expectations for the future

It is expected that in the near future, permission will be granted by national authorities to enable the algorithms to be published openly.