Source: **ETSI**

Title: **ETSI position on A5/3 funding and ownership**

Agenda item: **6.1**

Document for:

Decision	**X**
Discussion	
Information	

1 Background

GSM currently uses an Algorithm known as A5/2for ciphering and encryption purposes. The Algorithm is available from the GSM Association upon signature of a non-disclosure agreement.

This algorithm has been in use for about ten years and 3GPP technical experts predict that it will not be too much longer before the algorithm is compromised. It has been agreed by SA3 that a new algorithm is now required. The GSM Association has also studied the matter in their security group and strongly support the need for a new algorithm.

The proposal is that the ETSI SAGE Group should be subcontracted to prepare an algorithm which will be known as A5/3 and that it should be based on the Kasumi kernel which forms the heart of the 3GPP Ciphering and Integrity algorithms (f8 and f9). A draft work plan has been prepared with an estimated development cost of about 100 kEUR.

The GSM Association has volunteered to pay for the development cost and in return they are seeking joint ownership rights of the end product.

The issue of funding and ownership rights has been debated by the Organizational Partners for some months and a conclusion has not yet been reached. However, due to the growing urgency for this work to begin, the Funding and Finance Group have allocated the requisite resources from the contingency as a temporary measure and until an agreement is reached on the outstanding issues.

2 The ETSI position

2.1 Funding

ETSI believes that, as a principle, the funding of 3GPP activities can be derived from any source. The Organizational Partners by default fund activities but other sources should be pursued wherever possible.

If funding is forthcoming from the GSM Association then this should be gratefully received (unless unacceptable conditions are attached to their offer, cf 2.2 below).

In the case of the new GSM Algorithm, those Organizational Partners which will be the end beneficiary of the results should contribute to any funding requirement.

2.2 Ownership

ETSI believes that, as a principle, the *"ownership"* of 3GPP results must remain with the 3GPP Organizational Partners that form the project. This was one of the building blocks on which 3GPP was created and should be maintained. The sharing of the "ownership" of specific results with third parties is viewed by ETSI as a dangerous principle to establish.

2.3 Distribution of the A5/3 algorithm

In the case of the new A5/3 algorithm it seems appropriate that the GSM Association should be able to continue its role of distribution. ETSI then sees no problem at all in granting "*distribution*" rights to the Association in this case.

It should be noted that the intention is for A5/3 to be "distributed" in exactly the same was as for the f8 and f9 algorithms, that is to say that they will be placed on the website for free download but a licence will be required by those wishing to use it. The licence will be obtainable from the Organizational Partners (and the GSM Association).

3 Decisions required

Option 1

The preferred solution would be for the GSM Association offer of funding to be accepted in return for "*distribution*" rights of the algorithm.

Option 2

If the GSM Association are not able to fund the development of the algorithm, then the work should be funded from the 3GPP contingency. In this case, the funding would be accountable to those Organizational Partners that would be the end beneficiary of the work. This in itself may lead to debate in the context of GSM/3G roaming. Even if the GSM Association are unable to fund the activity they should nevertheless be granted distribution rights in recognition of the role they have performed to date.