Source: **GSMA**

Title: **GSMA response to Action PCG 10/1 Alternative 3G Ciphering and Encryption Algorithm**

Agenda item: **3.1**

Document for:

Decision	
Discussion	
Information	**X**

Meeting Name & Number: **GSMA Security Group**

Meeting Date:

Meeting Location:

Document Source: **Bill Best GSMA CTO**

Document Creation Date: **1st December 2003**

Document Status: **For Approval**

For Information **X**

Associated Knowledge Basis:

Circulation Restricted[1]**:** **UNRESTRICTED**

**** All GSM Association meetings are conducted in full compliance with the GSM Association's anti-trust compliance policy*High Level Document Summary:**

This document is in response to the action emanating from PCG 10 regarding the view of GSMA on an alternative 3G ciphering and encryption algorithm.

Title: GSMA response to Action PCG 10/1 Alternative 3G Ciphering and Encryption Algorithm

Response to: PCG 10/1 Action Point
Release:

Source: GSMA CTO and Security Group
To: 3GPP PCG
Cc: GSMA SG Chair

Contact Person:

Name: Bill Best
Tel. Number: +44 7956 202120
E-mail Address: bbest@gsm.org

Attachments: None.

At PCG 10 the GSMA were asked to comment upon the urgency and need for an alternative 3G Ciphering and Encryption Algorithm.

By way of background, earlier this year, GSMA SG reviewed an internal proposal to develop a second algorithm for UMTS and considered how this development may be funded – one option being for GSMA to exclusively fund. It was acknowledged that the existing algorithm is not under threat, but the development of a new encryption algorithm was worthy of consideration because of the lead-time for manufacturers to incorporate new algorithms into network infrastructure and handsets. The GSMA is aware that if the existing algorithm is compromised it would be impossible to have an alternative deployed within a short time and this fact could justify the development of a second algorithm, to have in reserve.

However, GSMA is not aware that the existing algorithm is in danger of being broken, and even acknowledging that cryptanalysis continues to advance at pace, SG considered the development of a second algorithm not to be an urgent priority.

GSMA believes that any cross industry agreement on the need and urgency of a second algorithm needs to be established and if such consensus existed the GSMA would consider part funding the development work but should not be be expected to fund exclusively.

GSMA is not aware that any of the 3GPP partners have expressed a willingness to co-fund the development of the proposed algorithm from their own budgets. In the absence of other industry stakeholders expressing a willingness to acknowledge the need, by way of financial contribution, GSMA SG feels that there is no justification for GSMA to totally fund a second UMTS cipher algorithm at this point.

In summary, GSMA SG view is that the development of a new UMTS cipher algorithm is not currently justified, particularly in the absence of support from organistions.