SG Doc XX_03

Liaison Statement to 3GPP SA3 on introduction of A5/3 in GSM handsets

Meeting Name & Number:	**SG#48**
Meeting Date:	**22 to 23 September 2003**
Meeting Location:	**Warsaw, Poland**
Document Source:	**Per Christoffersson, TeliaSonera**
Document Creation Date:	**23 Sept 2003**
Document Status:	**For Approval X**
	For
	Information
Associated Knowledge Basis:	
Circulation Restricted[1]:	**GSM Association**
	Members
	Associate Members

[1] **Restricted – Confidential Information**

* ***All GSM Association meetings are conducted in full compliance with the GSM Association's anti-trust compliance policy***

High Level Document Summary:

This liaison statement to TWG requests support for the inclusion of cipher indicator tests in the GCF testing regime for GSM handsets.

A5/3 introduction

To: **3GPP TSG SA WG3**

From: **GSM Association Security Group**

Contact: **James Moran, Director, Fraud and Security (jmoran@ghsm.org)**

SG has previously recommended that A5/3 should be introduced in GSM handsets as from October 2004 and as far as we have understood this has also been advised in SA3.

Having considered the matter at its last meeting, in the light of the new attacks that have recently been presented on GSM ciphering, SG came to the conclusion that it should be a priority to introduce a mechanism that separates keys for use with different encryption algorithms. For this reason SG wishes to express that the introduction of such a key separating mechanism should be aligned with the introduction of A5/3. This combined introduction can hopefully be achieved before the end of 2004. An absolute deadline should be that both security features are part of Rel-6.

We hope SA3 will look favourably on this request and we thank you in advance for your assistance.