



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<sup>1</sup>:** GSM Association  
Members  
Associate Members

---

<sup>1</sup>**Restricted – Confidential Information**

Access to and distribution of this document is restricted to the persons listed under the heading Circulation Restricted. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those listed under Security Restrictions without the prior written approval of the Association. The GSM MoU Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

**\* 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](mailto: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.