IREG Doc 47_056 Rev 1

Response to LS to 3GPP on Evaluation of the alternatives for SMS fraud countermeasures

Meeting Name & Number:	**IREG Plenary 47**
Meeting Date:	**30th September, 2004**
Meeting Location:	**Singapore**
Document Source:	**Vodafone-UK, T-Mobile,**
Document Creation Date:	**18th September 2004**

Document Status:	**For Approval**	**X**
	For Information	
	For Discussion	

Associated Knowledge Base(s):	

Circulation Restricted *:	**GSM Association:**	
	Members	**X**
	Associate Members	**X**

Document History:	

N.B. All GSM Association meetings are conducted in full compliance with the GSM Associationís anti-trust compliance policy

High Level Document Summary:
This document is the response to a LS from 3GPP CN4 on the evaluation of the alternatives for SMS fraud countermeasures. The response has been generated as part of the GSMA SS7 SMS Fraud Taskforce activities and is based on work carried out in the Long Term Containment workstream.

Specifically this document proposes a pragmatic and implementable roadmap to enhance security against SM Faking and Spoofing in the first phase, and generally enhance SS7 security in the second phase.

To: 3GPP CN4,

Copy: 3GPP SA3, GSMA-SG,

From: GSMA/IREG

Subject: Response to CN4 Liaison Statement on
Evaluation of the alternatives for SMS fraud countermeasures.

Date: 18th September 2004

Contact person:
Name: John Boggis, Vodafone UK
Email: john.boggis@vodafone.com
Telephone +44-1635-673712

Introduction
IREG thanks 3GPP CN4 for their liaison statement (N4-041204 : LS on Evaluation of the alternatives for SMS fraud countermeasures presented as IREG Doc 47_038, SIGNAL Doc 19_006)

IREG appreciates the work done in CN4 and the identification of the TCAP handshake mechanism to be set alongside other alternatives such as MAPsec and SIGTRAN/IPsec.

IREG seeks solutions to two issues. The first is specifically to combat the SS7-SMS fraud (Faking/Spoofing); the second is to add security to the SS7 infrastructure which has hitherto been immune from misuse because all bodies with access were ìtrustedî, quasi governmental, or closely regulated.

IREG also desires to have designs which can be implemented in a staggered manner by operators, so as to provide immediate protection to those operators who implement early. Conversely any mechanism which requires all bodies to install before any security uplift can be achieved would fail to achieve success.

Based on the strategy described above IREG has the following set of comments:-

A) IREG requests the TCAP Handshake as soon as possible.
because:-
1. It is a defence against Spoofing and Faking attacks.
2. It would require implementation in SMSC, MMSC and MSCs (and possibly SGSN and voicemail systems) only.
3. It can be partially implemented i.e. it gives benefit to the parties involved (i.e.. protected against being the innocent targeted operator) as soon as they implement and agree to turn on "mandatory" handshake by a policing function in the receiving network-element. It could also be turned off PLMN by PLMN when MAPsec/IPsec is introduced.
4. The protocol (but not "per PLMN policing" functionality) is already in use for long SMs from MAP ph2 onwards.
5. We can accept the penalty of doubling of MAP message quantities for Forward SM for the benefit gained.

B) IREG request the MAPsec work be completed because we are concerned that as the trusted status of SS7 networks has been discredited, that other more evil attacks may follow.

However the architecture must support the use of "gateways" which perform the appropriate authentication/encryption of MAP messages between pairs of PLMNs because:-

1. There would be no need to develop MAPsec functionality in end nodes such as MSC, HLR, SGSN, SMSC, CAMEL-Server.....Hence MAPsec development does not need to distract the suppliers from their current product plans,
2. Architectural simplicity. Some type of SS7 firewalling is now anticipated to become commonplace. Suppliers of firewalls could and will develop SS7-MAPsec gateway products (as could the big element manufacturers of course). MAPsec gateway could be implemented at STP.
3. Gateway architecture eliminates the rollout issues of ensuring that all network elements within a PLMN are enabled with MAPsec before turning on the protection.
4. Simplifies key management (and may mean that the Ze work may not be needed) because there will only a few gateways in a PLMN
5. Can be partially implemented across GSMA and enabled per "PLMN roaming-pair", and provides protection for the two PLMNs incrementally.

If this is not possible to deliver a gateway solution then we see little or no point in continuing the MAPsec specification because it will take too long to rollout and turn on.

C) Whilst we understand that the use of SIGTRAN M2PA (as a broadband linkset replacement) is currently happening between C7PM operators, we believe that the rollout of SIGTRAN (specifically M3UA) in the international space is still several years in the future and will not be universal for many more.
We are uncomfortable about the integrity of the security of a hybrid SIGTRAN/legacy SS7 because any SIGTRAN/legacy gateways will perpetuate address faking loopholes, and we will want the confidence of MAPsec PLMN-PLMN security mechanisms until a separated International SIGTRAN network is achieved (even with IPsec enabled between PLMNs and/or legacy portals.)

Actions

IREG would like CN4 and SA3 to confirm:-

1. that they understand the IREG response.
2. are able to proceed with the design and specification of TCAP handshake mechanism.
3. are able to complete the ìgatewayî design and specification of the MAPsec mechanism.
4. the dates when items 2 and 3 will be complete and approved by 3GPP.