3GPP TSG SA WG3 Security — S3#28 **S3-030216**
6 - 9 May 2003
Berlin, Germany

TSG-SA WG1 #20 **S1-030559**
Seoul, Korea, 7th–11th April 2003 **Agenda Item: 5.6**

Title: LS on Privacy and Security Requirements within GSM/UMTS Devices

Response to: LS (SerG Doc 101/03, S1-030458) on Privacy and Security Requirements within GSM/UMTS Devices

Work Item: Privacy, LCS

Source: **SA1**
To: GSMA SerG LBS, SA3
Cc: GSMA OMAop (Operators), OMA LOCATION, OMA REQUIREMENTS

Contact Person:
Name: John Watson
Tel. Number: + 44 1635 254685
E-mail Address: John.Watson@vodafone.co.uk

Attachments: None

---

1. Overall Description:

TSG SA1 would like to thank GSMA SerG for their Liaison Statement LS (Serg Doc 101/03) on Privacy and Security Requirements within GSM/UMTS Devices and for the opportunity to comment on this issue.

During the SA1#20 plenary discussion it was recognised that there is a need for a privacy framework in the terminal and that this should be further studied in the SA1 Privacy and GUP SWGs. It was also decided that, because there are significant security issues associated with the establishment of a secure domain in the handset, SA3 should also be consulted on this matter.

2. Actions:

To SA3 group.

ACTION: SA1 kindly asks SA3 to study the security implications and to provide details of any new requirements needed to specify a secure privacy domain in UEs, as described in the attached GSMA SerG document (101/03).

3. Date of Next TSG-SA WG1 Meetings:

SA1 SWGs #21	12 - 16 May 2003,	San Diego, USA, North American Friends
SA1#21	07 - 11 July 2003,	Sophia Antipolis, hosted by ETSI

4. Attachments:

Original LS from GSMA SerG (SerG Doc 101/03, S1-030458)

TSG-SA WG1 #20 **S1-030458**
Seoul, Korea, 7th–11th April 2003 **Agenda Item:**

Meeting Number **SerG#51**

SerG Doc 101/03

Meeting Date **May 20th -22nd 2003**
Meeting Location **Paris, FRANCE**

Title Privacy and Security Requirements within GSM/UMTS Devices

Source **Vodafone**
Date **4th April 2003**

Security Classification Category*:		**Please mark with "X" where applicable**
Unrestricted - Industry		**X**

Status
Please mark with "X" one of the following actions relating to this document:
For Approval ☒ **For Information** ☐

Associated Knowledge Basis	Enter if applicable

Document History		
Revision	**Date**	**Brief Description**

Summary
Liaison statement to 3GPP, OMA, & JCP regarding operator requirements for privacy and security within GSM & UMTS devices.

Liaison Statement

From: **GSM Association SerG**

To: 3GPP SA1, GSMA OMAop (Operators), OMA LOCATION, OMA REQUIREMENTS, JSR-179, JSR-185,

Copy:

Subject: **Privacy and Security Requirements for GSM/UMTS Compliant Devices**

Date: 17th March 2003

GSMA SERG are aware of the the work within JCP on JSR 179 and have an interest in the concept of a Java Location API.

However, for handsets that are in open markets (for example where Java applications could be downloaded from any source), it is necessary that it be possible to provide a security framework for services that is consistent with the operators' privacy mechanisms and compliant to local regulations.

The motivation for such a security framework can be summarised by the following key privacy requirements:

- It is in the overall interests of the mobile telecommunications industry to meet subscribers' privacy requirements. This is most likely to be achieved by avoiding a disintegrated approach to privacy management, such as by allowing terminals to bypass existing trust relationships and privacy controls already established by network operators.
- Privacy settings are most effective if related to a subscriber, not a piece of equipment. Therefore, it should be possible for the privacy settings of a subscriber to be maintained when a subscriber switches terminals.
- Service providers and network operators are subject to specific duties and obligations with regards to the protection of their subscribers' privacy, as established by regional regulation authorities. There are therefore established regulatory frameworks designed to ensure that the highest standards of privacy prevail for subscribers, e.g. in Europe, USA, Japan, etc.
- If some privacy settings for services offered by the Network Operator are resident within the terminal, then they should be consistent with equivalent privacy settings stored within the operator's network, e.g. the HLR flag, the privacy exception list, any settings in the PPR etc...
- It can be more secure and convenient for the subscriber and gives more legal certainty to the user and service provider to rely on network based systems rather than those that are equipment based. The applicable law in the case of a network based solution is very likely to be that of the home network, which will be familiar to the end user, while an equipment based solution, being mobile, may trigger the application of different privacy laws as the equipment moves across different jurisdictions.

It would be desirable for a security framework for services to address these issues. For example in the case that a terminal be positioned independently of the network (i.e. position is determined based on terminal capabilities only) it would be desirable that in order for applications to be able to utilise a subscriber's location information these applications still be

subject to privacy checks under the control of the operator. A rigorous testing and certification process by the operator for applications prior to execution could provide an environment in which it would be possible to protect the privacy of the subscriber.

Whereas, the proceeding requirements are specifically targeted at location information , SerG believes that similar requirements may be applicable to other types of private information associated with other services as well. However, this issue requires further study within SerG and no conclusions have been reached in this area at present.

SERG respectfully requests that the requirements outlined in this letter are reviewed and that SERG is informed of any relevant work that is being performed in your organisation regarding privacy and security.