3GPP TSG SA WG3 Security — S3#33 **S3-040419**
10 - 14 May 2004
Beijing, China

TSG-SA WG1 #24 **S1-040483**
Shenzhen, China, 10 - 14 May 2004 **Agenda Item: 8**

Title: Liaison statement Network Protection against Virus Infected Mobiles

Source: **SA1**
To: SA2, CN1,
Cc: OMA TP, OMA REQ, TSG SA3

Contact Person:
Name: **Nigel Barnes, Motorola Ltd**
Tel. Number: +44 1 256 790 169
E-mail Address: Nigel.Barnes@Motorola.com

Attachments: TDoc S1-040482

---

1. Overall Description:

At TSG SA WG1 #24 the need for protecting 3GPP networks against malicious applications in terminals was discussed. These discussions lead to the drafting and accepting of a new Work Item on the subject of “Network Protection against Virus Infected Mobiles” (Attached). The aim of this new work item is to specify a mechanism which, in the event of an infected mobile, allows the operator to limit the mobile’s capability to establish connections, which, e.g., could overload the network.

It is understood that there is work going on in OMA on "Content Screening", which may be partly related to the present work item. However, the present work item is intended to focus on a network protection mechanism in the 3GPP specific protocols (layer3), whereas it is understood that the work in OMA focuses on application layer protection. Thus it is considered the work can progress independently.

TSG SA WG2 and TSG CN WG1 are invited to review the work item and provide comments if any. As soon as TSG SA WG1 has established a stable set of requirements for this functionality, TSG SA WG1 will forward these as appropriate.

2. Actions:

To TSG SA WG2 & TSG CN WG1 group.

ACTION: TSG SA WG2 and TSG CN WG1 are invited to review the work item and provide comments, if any.

3. Date of Next TSG-SA1 Meetings:

SA1#25	28 June - 2 July 2004	Montreal, Canada

Proposed Work Item Description

Title: Network Protection against Virus Infected Mobiles

1 3GPP Work Area

	Radio Access
X	Core Network
	Services

2 Linked work items

There is work going on in OMA on "Content Screening" which may be partly related to the present work item. However the present work item is intended to focus on a network protection mechanism in the 3GPP specific protocols(layer3), whereas it is understood that the work in OMA focuses on application layer protection. Thus it is considered the work can progress independently.

3 Justification

Presently the virus threat to the IT organizations and consumers worldwide are well known. Significant damage has been caused and particularly so with rather simple but potent methods. With increasing data usage and the drive towards increasing the ARPU per subscriber from increased data usage, the need for effective methods of dealing with the threat of a downloaded virus to a mobile telephone needs to be addressed.

4 Objective

In particular the threat of a virus that repeatedly makes a connection request requiring both allocation of radio resources and network signalling processing can be substantial. The virus may be downloaded by the user unknowingly through various means: e-mail, SMS and Push services. While operators may be able to maintain some degree of control over the latter, the former pose a significant threat to the industry at large.

What is needed is therefore:

1. A means of disabling an infected device from registering again on the network, both in the current network and any other network, i.e. effectively quarantining the device.
2. A means of being able to repair the device

A means of maintaining the disabled status of the device, even if the mobile has been successively switched off and on, until it is repaired.

5 Service Aspects

Selective disabling of the mobile device should be provided to allow the establishment of connection types which are not impacted by the virus, e.g., if the virus impacts only the PS domain, then it should be possible to allow CS domain connections such as Emergency calls or vice-versa.

6 MMI-Aspects

Means should be provided to inform the user about the full or partial disabling of the mobile and the reason for this.

7 Charging Aspects

None/Text

8 Security Aspects

Care needs to be taken to ensure that only a real 3GPP network can fully or partially disable a mobile device.

9 Impacts

Affects:	UICC apps	ME	AN	CN	Others
Yes		X		X	
No			X		
Don't know	X				

10 Expected Output and Time scale (to be updated at each plenary)

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
22.101		Introduction of service requirements	TSG SA#26	
22.060		Adding of protection mechanism: Stopping of PDP context activations	TSG SA#26	
23.060		Adding of protection mechanism to GMM	TSG SA#27	
24.008		Adding of protection mechanism to MM/GMM	TSG SA#27	

11 Work item rapporteur

Nigel Barnes, Motorola Ltd

12 Work item leadership

Initially TSG SA WG1

13 Supporting Companies

Motorola, Siemens, Vodafone, O2

14 Classification of the WI (if known)

X	Feature (go to 14a)
	Building Block (go to 14b)
	Work Task (go to 14c)

14a The WI is a Feature: List of building blocks under this feature

TBD

14b The WI is a Building Block: parent Feature

(one Work Item identified as a feature)

14c The WI is a Work Task: parent Building Block

(one Work Item identified as a building block)

form change history:
2002-07-04: "USIM" box changed to "UICC apps"