Technical Specification Group Services and System Aspects **TSGS#24(04) 0470**
Meeting #24, Seoul, Korea, 07-10 June 2004

Source:	**Ericsson, Motorola**
Title:	**New WI on Selective Disabling of UE Capabilities**
Document for:	**Approval**
Agenda Item:	**7.1.3**

Work Item Description

Title: Selective Disabling of UE Capabilities

1 3GPP Work Area

	Radio Access
X	Core Network
	Services

2 Linked work items

Access Class Barring and Overload Protection

There is work going on in OMA on "Content Screening" and in GSMA which may be partly related to the present work item. However, the present work item is intended to focus on a reactive network protection mechanism in the 3GPP specific protocols (layer3), whereas it is understood that the work in OMA and GSMA focuses on preventative application layer protection. Thus it is considered the work can progress independently. The relationship to work in OMA/GSMA and potential overlap with the OMA/GSMA work should be taken into consideration in the present work item.

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 consequences of downloading and activating a virus in a mobile telephone needs to be addressed.

Similar problems may also arise with downloaded applications that are not functioning correctly.

4 Objective

In particular a downloaded and activated application that repeatedly makes a connection request requiring both allocation of radio resources and network signalling processing can be substantial. The misbehaving application may be downloaded by the user through various means: e-mail, SMS and Push services, and (exceptionally) fail to be detected and disabled by application layer preventative measures. While operators may be able to maintain some degree of control this pose a significant threat to the industry at large. Similar problems may also arise with viruses.

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 maintaining the disabled status of the device, even if the mobile has been successively switched off and on.

The criteria for determining when an application is misbehaving are not included in the scope of this work item.

5 Service Aspects

Selective disabling of the mobile device should be provided to allow the establishment of connection types which are not impacted by a virus or application error, e.g., if the misbehaving application 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

8 Security Aspects

The present work item should analyse what threats a reactive network protection mechanism mitigates. New threats potentially introduced by a network protection mechanism should be carefully studied. The relation to existing “black list” features should be analysed.

9 Impacts

The end deliverable is a Technical Report. If the results are adopted, the following elements could potentially be impacted:

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
TR xxx.yy	Selective Disabling of UE Capabilities	SA1	SA3	TSG SA#26	TSG SA#27	

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

11 Work item rapporteur

Nigel Barnes, Motorola Ltd

12 Work item leadership

Initially TSG SA WG1 and later CN1

13 Supporting Companies

Motorola, Siemens, Vodafone, O2, Ericsson, Nokia, TIM

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"

Technical Specification Group Services and System Aspects **TSGS#24~~2~~(04) 0470~~302~~**
Meeting #24, Seoul, Korea, 07-10 June 2004

Source:	~~SA1~~Ericsson, Motorola
Title:	**New WI on Selective Disabling of UE Capabilities~~Network Protection against Virus Infected Mobiles~~**
Document for:	**Approval**
Agenda Item:	**7.1.3**

~~TSG-SA WG1 #24~~ ~~S1-040482~~
~~Shenzhen, China, 10 - 14 May 2004~~ ~~Agenda Item: 8~~

~~Proposed~~ Work Item Description

Title: ~~Network Protection against Virus Infected Mobiles~~Selective Disabling of UE Capabilities

1 3GPP Work Area

	Radio Access
X	Core Network
	Services

2 Linked work items

Access Class Barring and Overload Protection

There is work going on in OMA on "Content Screening" and in GSMA which may be partly related to the present work item. However, ~~tThe~~ the present work item is intended to focus on a reactive network protection mechanism in the 3GPP specific protocols (~~-~~layer3), whereas it is understood that the work in OMA and GSMA focuses on preventative application layer protection. Thus it is considered the work can progress independently. The relationship ~~interrelation~~ to work in OMA/GSMA and potential overlap with~~to~~ the OMA/GSMA work should be taken into consideration in the present work item.

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 consequences~~threat~~ of ~~a~~ downloading and activating a~~ed~~ virus ~~to~~in ~~–~~a mobile telephone needs to be addressed.

Similar problems may also arise with downloaded applications that are not functioning correctly.

4 Objective

In particular ~~the threat of~~ a ~~virus~~ downloaded and activated application that repeatedly makes a connection request requiring both allocation of radio resources and network signalling processing can be substantial. The ~~virus~~ misbehaving application may be downloaded by the user ~~unknowingly~~ through various means: e-mail, SMS and Push services, and (exceptionally) fail to be detected and disabled by application layer

preventative measures. While operators may be able to maintain some degree of control ~~over the latter, the former~~ this pose a significant threat to the industry at large. Similar problems may also arise with viruses.

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~~

2. 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~~.

The criteria for determining when an application is misbehaving are not included in the scope of this work item.

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~~ a virus or application error, e.g., if the ~~virus/~~misbehaving application 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

The present work item should analyse what threats a reactive network protection mechanism mitigates. New threats potentially introduced by a network protection mechanism should be carefully studied. The relation to existing “black list” features should be analysed. ~~Care needs to be taken to ensure that only a real 3GPP network can fully or partially disable a mobile device.~~

9 Impacts

The end deliverable is a Technical Report. If the results are adopted, the following elements could potentially be impacted:

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
TR xxx.yy	Selective Disabling of UE Capabilities	SA1	SA3	TSG SA#26	TSG SA#27	

Potentially aAffected 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 and later CN1

13 Supporting Companies

Motorola, Siemens, Vodafone, O2, Ericsson, Nokia, TIM

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"