3GPP TSG SA WG3 Security — S3#37 **S3-050007**
21 - 25 February 2005
Sophia Antipolis, France

TSG-SA WG1 #27 **S1-050235**
Cape Town, South Africa, 17th to 21st January 2005 **Agenda Item:**

Title: Reply LS on Clarification of SA3 work on Selective Disabling of UE Capabilities WI
Response to: LS (S1-050040) on LS on Clarification of SA3 work on Selective Disabling of UE Capabilities WI from SA3

Source: **SA1**
To: **SA3**
Cc: -

Contact Person:
Name: Jan Ignatius
E-mail Address: jan.ignatius@nokia.com

Attachments: S1-050233, S1-050234

1. Overall Description:

SA1 would like to thank SA3 for their LS on Selective Disabling of UE Capabilities. SA1 has reviewed the document S3-040873 describing the current status of SA3 work on Network Protection. SA1 agrees on the conclusions presented in the document that operator's resources can be protected transparently with the technology already available today (e.g. firewalls) and no specific new requirements at this time are needed for the stage 1. If, at a later stage, SA3 reconsiders their position and finds that new requirements are needed for network protection in stage 1, SA3 is asked to inform SA1 so that appropriate actions can be taken.

2. Actions:

To SA3 group.

ACTION: none.

3. Date of Next TSG-SA1 Meetings:

SA1#28	4 – 8 April 2005	Beijing, China
SA1#29	27th June – 1st July 2005	TBD

CR-Form-v7

CHANGE REQUEST

⌘ **22.011** **CR** **066** ⌘ **rev** **-** ⌘ Current version: **7.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: | UICC apps⌘ ☐ ME [X] Radio Access Network ☐ Core Network [X]

Title:	⌘	Addition of "Network Control of UE Capabilities"
Source:	⌘	Motorola
Work item code:	⌘	Network Protection
Date:	⌘	19/12/2004
Category:	⌘	**B**
Release:	⌘	Rel-7

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	At the TSG SA(#24) meeting a new work item (WI) on 'Selective Disabling UE Capabilities' was approved (SP-040477). The intention is to disable MSs when necessary on criteria to be decided by the operator. There is a need to include the requirements in TS 22.011
Summary of change:	⌘	Introduction of an additional list of Selective MS Capabilities in the MS to indicate disabled services which can not be used in the PLMN code of the network on which the list was received and any other network. The MS shall not request services that are indicated as disabled. The Selective MS Capabilities list is stored in the ME and it shall not be deleted at switch off. Therefore, the mobile station maintains the status of specific MS capabilities at switch on. Additionally, the MS should use the indications given in the Selective MS Capabilities list to inform the user about the availability of the appropriate services, e.g. SMS via PS are not allowed
Consequences if not approved:	⌘	

Clauses affected:	⌘	4.5 (new)

	Y	N		
Other specs Affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	

	X	O&M Specifications

Other comments: ⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

4.5 Control of UE Capabilities

To protect the user from the effects of a misbehaving UE (e.g causing additional charges, degraded performance) and to protect the network operator's network capacity, including radio resources and network signaling and processing, means shall be provided for the HPLMN and the VPLMN to provide an indication to the UE as to which network provided services or functions it is not allowed to use.

The Selective UE Capabilities list, shall be maintained in the UE and the UE shall not request any services indicated as disabled. At registration the HPLMN or VPLMN may interrogate the status of the list and provide a new list.

The Selective UE Capabilities list shall not be deleted at switch off and will remain valid until a new list is provided by the network. The Selective UE Capabilities list relates to the ME and not to the subscription.

It should be ensured that UEs are not maliciously disabled, including malicious disabling by a VPLMN, or accidentally disabled, or kept disabled, and there shall be a mechanism for restoring disabled UEs in all situations (e.g. in the case that the serving network does not support the control of UE Capabilities).

The UE should use the indications given in the Selective UE Capabilities list to inform the user of the non-availability of services or functions.

There shall be a means for the network to provide an optional customer service number(s) which can be used, by the user, to assist in determining the cause of non-availability of specific services. The specifications should also provide the capability for the network to include an optional text string that will be displayed by the UE.

The UE Capabilities list shall take precedence over subscribed services.

The services to be included in the list are:

- Call Control functions
- Supplementary Services
- Emergency Calls (including the (U)SIM-less case and subject to regional regulatory requirements, i.e. emergency calls shall not be disabled in regions where support of them is required)
- SMS, via CS and PS
- LCS, via CS and PS
- GPRS based services
- MBMS
- IMS

TSG-SA WG1 #27 **S1-050234**
Cape Town, South Africa, 17th to 21st January 2005 **Agenda Item:**

Title: **Updated WID on Network Protection**

Source: **T-Mobile**

Contact: Johannes Achter
T-Mobile International
Johannes.Achter@t-mobile.at

~~Revised WID~~

Work Item Description

Title: Selective Disabling of UE Capabilities

1 3GPP Work Area

	Radio Access
X	Core Network
	Services

2 Linked work items

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 a substantial threat. 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 poses 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~~set of change requests to existing technical specifications in SA1. Depending on the consequences of such requirements one or more new TS may need to be created by SA3 ~~and/or~~, CN1 and/or T3. If the results are adopted, the following elements could potentially be impacted:

Affects :	UICC apps	ME	AN	CN	Others
Yes	X	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
22.0101~~0~~1		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"