**Title:**        **Updated WID on Network Protection**

**Source:**       **MCC**

**Contact:**

This document is a revision of S1-050234 and S2-050386.

**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 and/or CRs may need to be created by SA3 ~~and/or~~, C~~N~~T1, CT4 and/or CT~~3~~6. 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~~ | |
| TR23.8sd | Report on different architectures for providing selective disabling of UE capabilities | SA2 | | TSG SA #28 | N/a | It is anticipated that by SA #28 the architectural solution will have been decided upon. Subsequent completion and approval of this 800 series TR will then be unnecessary. |

| Potentially affected existing specifications | | | | | |
|---|---|---|---|---|---|
| Spec No. | CR | Subject | | Approved at plenary# | Comments |
| 22.010~~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 | | | |
| | | The list of CRs should be identified when the architecture choice has been made. | | #29 and/or #30 | |
| | | | | | |

# 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)