3GPP TR 23.805 V0.3.1 (2005-09)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Selective Disabling of UE Capabilities; Report on Technical Options and Conclusions (Release 7)

Select keywords from list provided in specs database.

Keywords
<keyword[, keyword]>

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

To ensure that 3GPP users and network operators are protected from the effects of misbehaving mobile stations, in the case in which the effects have not been mitigated by preventative measures, it is necessary for network operators to be able to selectively disable services on the misbehaving MS. The requirements for this capability are defined in TS 22.011, Section 4.5.

There is a need to select the optimal service architecture that delivers the Selective Disabling of UE Capabilities functionality. This TR provides a study of the different possible service architectures.

Editor's Note: For reference the text from 22.011 is presented below:

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

1 Scope

The present document presents an assessment of different service architecture implementations for the new Selective Disabling of UE Capabilities specified in TS 22.011, Section 4.5.

For each service architecture the document provides:

- A detailed description of the architecture
- An assessment of the architecture against the SA1 requirements described in TS 22.011, Section 4.5.
- An assessment of the architecture's strengths and weaknesses

The document provides a conclusion identifying the preferred service architecture of the SA2 TSG.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[<seq>] <doctype> <#>[([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the [following] terms and definitions [given in ... and the following] apply.

Identification System: A system used to identify a 'misbehaving' UE through analysis of the network traffic that it creates. The nature of the system is out of scope of this document.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

IS Identification System

4 Architectural requirements

The service architecture should have the ability to disable the capabilities on a large number of UEs that are simultaneously misbehaving and execute this function in a timely manner in order to stop any negative impact on network service.

5 Analysis of Possible Architectures

5.1 Architecture 1

5.1.1 (U)SIM File Based Architecture: Description

The ability to Selectively Disable services on a misbehaving UE could be achieved by specifying a new 'Selective UE Capabilities list" stored on the (U)SIM and copied to the ME describing which services are enabled/disabled on a particular UE. The Selective UE Capabilities list could take the form of a list of *n*-bits indicating whether or not a particular service was active or disabled. It should be noted that it would only be necessary to disable mobile originating services to protect the network operator's resource.

The Selective UE Capabilities list could be sent from the HPLMN operator to the (U)SIM using SMS OTA. The information in the Selective UE Capabilities list would then be copied to the ME. The ME would then be required to act according to the information stored when requesting a specific service. For example, if the Selective UE Capabilities list indicated that GPRS was not allowed, the UE would not be able to initiate a GPRS session.

In the case that a visited network identifies the misbehaving UE, the visited network could make a request to the home network operator to selectively disable the services being abused.

To enable the selective disabling of services to be linked the ME and not the subscription, and also to allow efficient storage and recall of selective disabling information, a new entity – the IMEI database – could be implemented. For the purposes of this discussion the IMEI DB is described as a separate logical entity, located in the HPLMN. The IMEI database will store a list of all UEs that have been selectively disabled, indexed by IMEI. This will enable the list of disabled services for any particular UE to be refreshed by the HPLMN at any time and would, for example, enable the Selective UE Capabilities list to be updated whenever a new (U)SIM was inserted into the UE. The IMEI database would also provide a single point of reference for entities, for example customer care, wishing to discover which services have been disabled on a particular device.

It is suggested that the Identification System referred to in the following descriptions is a separate logical entity that can reside in either the HPLMN or VPLMN. The exact nature of the Identification System is outside of the scope of this TR, however, it is assumed that that it is capable of detecting a misbehaving MS, and which service is being abused, from the network traffic being generated.

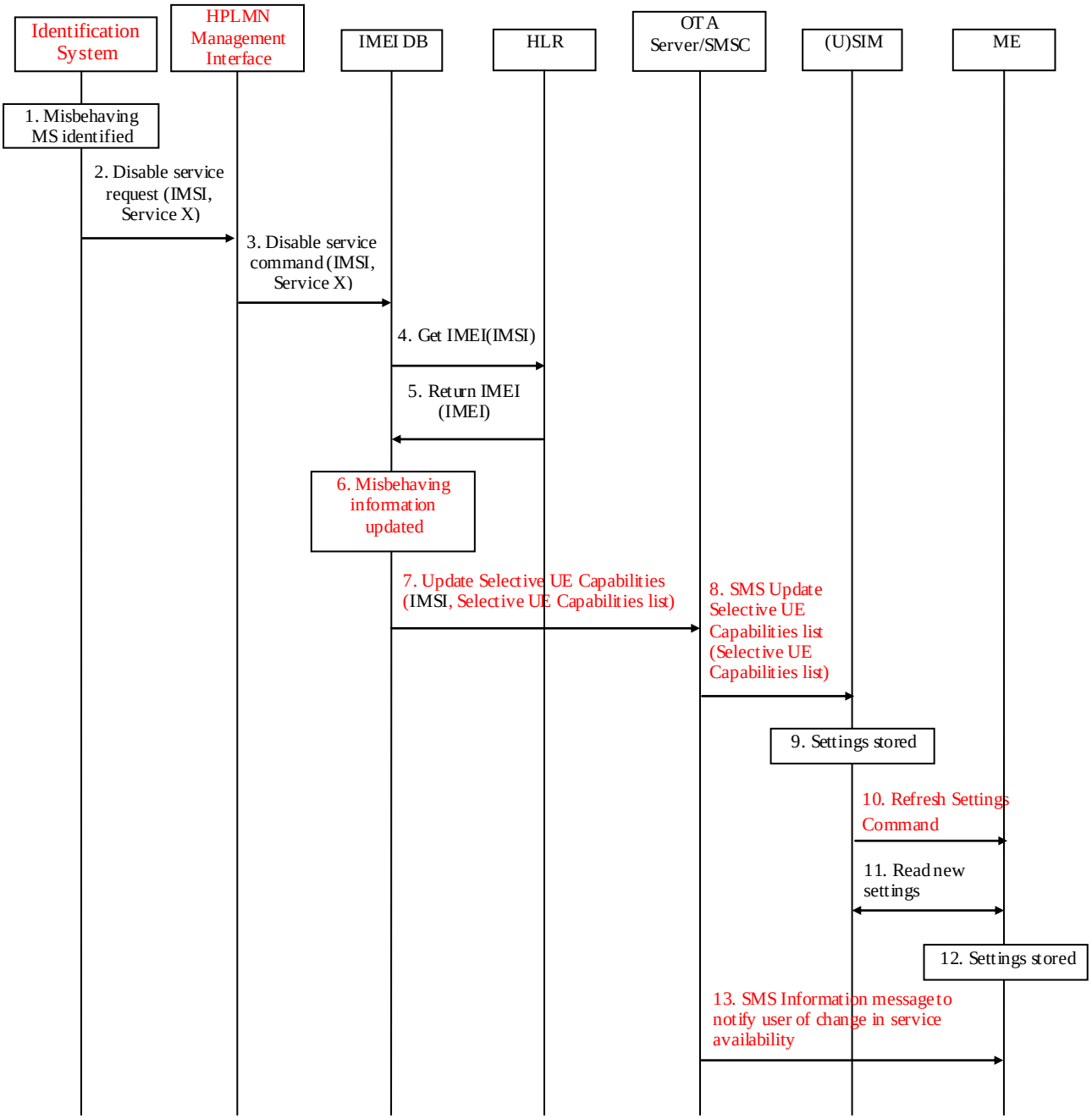

Figure 5.1.1: (U)SIM file based service architecture information flow – detection and selective disabling of a misbehaving MS

1. Misbehaving MS is identified by the Identification System.

2. Identification System sends a Disable Service Request (IMSI, Service X) message to the HPLMN Management interface. In the case in which the Identification System is located in the VPLMN, the message could take the form of an email or fax, to be analysed and acted on by the HPLMN. It is assumed that the Identification System only has access to the IMSI of the misbehaving device.

3. Disable service command (IMSI, Service X) sent from HPLMN Management Interface to IMEI database.

4. Get IMEI(IMSI) message sent from IMEI database to HLR.

5. Current IMEI associated with IMSI is returned to the IMEI DB by the HLR

6. IMEI DB updates the Misbehaving Information, storing the disabled service against the IMEI linked to the IMSI passed to it in the Disable service command.

7. IMEI DB sends an Update Selective UE Capabilities list (IMSI, Selective UE Capabilities list) message to the OTA server. The Selective UE Capabilities list contains the complete list of services and their current status (enabled/disabled).

8. OTA server sends SMS Update Selective UE Capabilities list (Selective UE Capabilities list) message to (U)SIM.

9. (U)SIM stores the information.

10. (U)SIM sends Refresh message to ME (3GPP 31.111).

11. ME reads new Selective UE Capabilities list from (U)SIM.

12. ME stores the new Selective UE Capabilities list.

13. Information message sent from OTA server to (U)SIM and displayed to user.

Note: Steps 4 and 5 assume that Automatic Device Detection (ADD) (3GPP 22.101) has been implemented by the HPLMN. This feature propagates the current IMEI associated with an IMSI from the MSC to the HLR at IMSI attach or location update. It is also possible that steps 4 and 5 could be removed from the information flow if the identification system is aware of the IMEI of the ME that it has identified as misbehaving. In this case the IMEI could be forwarded in the messages associated with steps 2 and 3. However, while it is thought likely that this scenario is probable, the alternative implementation has been shown to avoid making any assumptions that are beyond the scope of this report.

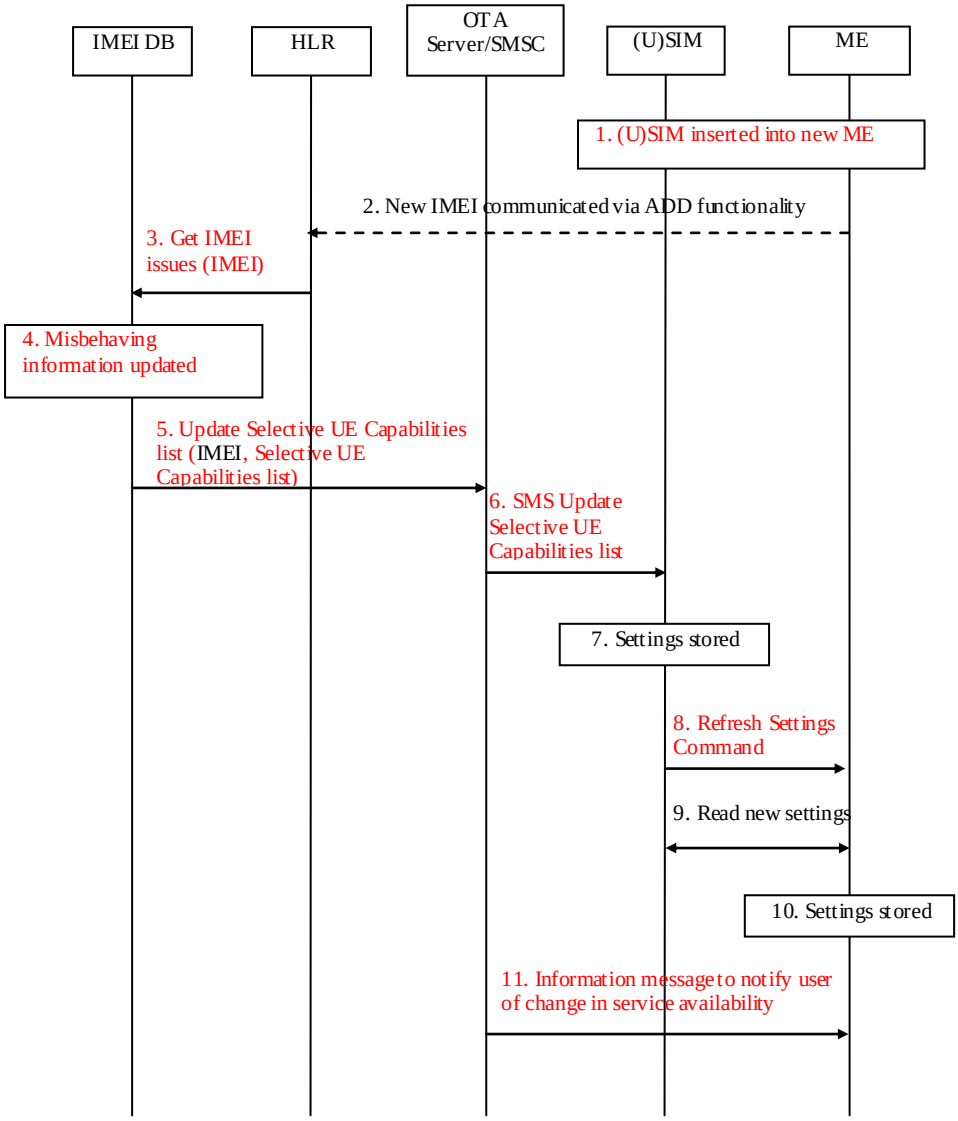

Figure 5.1.2: (U)SIM fie based service architecture information flow – insertion of new (U)SIM

1. (U)SIM inserted into new ME.
2. New IMEI propagated to HLR (via MSC/SGSN) using the Automatic Device Detection capabilities defined in 3GPP 22.101.
3. HLR queries IMEI DB for any disabling information related to the IMEI using Get IMEI issues (IMEI) message
4. The IMEI database checks the IMEI against its stored list of IMEIs with known issues, e.g. with services disabled.
5. IMEI database sends an Update Selective UE Capabilities list (IMEI, Selective UE Capabilities list) message to the OTA server. The Selective UE Capabilities list contains the complete list of services and their current status (enabled/disabled). If the IMEI is not present in the IMEI DB a fully enabled Selective UE Capabilities list is included in the message.
6. OTA server sends an Update Selective UE Capabilities list (Selective UE Capabilities list) message to (U)SIM.
7. (U)SIM stores the information.
8. (U)SIM sends Refresh message to ME (3GPP 31.111).

9. ME reads new Selective UE Capabilities list from (U)SIM.

10. ME stores new Selective UE Capabilities list.

11. Information message sent from OTA server to (U)SIM and displayed to user.

Note: In step 5 it is necessary to send a fully enabled Selective UE Capabilities list as part of the Update Selective UE Capabilities list message in order to address the case in which a user has inserted a (U)SIM that has previously been used in a MS that has had services selectively disabled into an MS for which there are no records in the IMEI DB (i.e. a clean MS). In this scenario, if a new fully enabled Selective UE Capabilities list is not sent to the (U)SIM (via the OTA server) the new MS will be refreshed with the Selective UE Capabilities list containing disabled services but related to the previous MS.

5.1.2 (U)SIM Selective UE Capabilities list File Based Architecture: Assessment against SA1 requirements

Using the architecture described above in 5.1.1, only the HPLMN can directly disable services on a UE, as the SMS OTA server is capable of sending OTA updates only to subscribers belonging to the network by which it is operated. However, the SMS OTA server can send an OTA update to a user belonging to the HPLMN whenever the user is attached to a network, including when the user is roaming on a VPLMN. With this capability it is possible for the VPLMN to request that the HPLMN disable a specific service on a particular UE that it has identified as misbehaving on it's network. This enables the VPLMN, via interaction with the HPLMN, to disable services on a misbehaving UE.

The Selective UE Capabilities List will be temporarily stored in the UE and permanently stored on the (U)SIM. The information will be copied from the (U)SIM to the ME as depicted in step 12, figure 1. The information will remain valid until a new list is sent or the UE is powered down. As soon as the UE is turned on the ME will read the list stored on the (U)SIM, therefore the information can be though of as being permanently present on the ME while powered up.

In the case of the insertion of the a new (U)SIM, it is proposed that the information for a particular UE, as stored in the IMEI database, could be refreshed by the network. This process is shown in figure 2. It is recognized that this will require additional messaging each time a new (U)SIM is used in an ME, however, it is thought that this is a relatively infrequent event. It is also thought to be likely that this information will only be part of the information that a network operator wishes to check and possibly refresh on detection of a (U)SIM being used in a new ME. One possible limitation of this solution is that it will not work in the case in which the ME was disabled by a previous HPLMN, as the new HPLMNs IMEI database will have no record of the IMEI being disabled. One possible solution would be to encourage the sharing of disabling information between PLMNs. Alternatively it could be considered that the responsibility to detect the misbehaving UE should reside with the current HPLMN and therefore that the service would be re-disabled when the identification system of the new HPLMN detected the misbehaving UE.

The use of the IMEI database allows the Selective Capabilities List to be related to the ME and not the subscription.

The architecture described above should ensure that it is nearly always possible to restore the UE to its original state, as the HPLMN is always responsible for the disabling of services on a device, it should be possible for the HPLMN to re-enable the services. One possible exception is when a users device is disabled and the user changes their network provider before the services have been re-enabled. In this situation it is recognized that the new network operator might not have the capability to re-enable the service(s). However it is expected that network operators not capable of updating the Selective UE Capabilities list would issue (U)SIMs with the Selective UE Capabilities list indicating all services allowed or not present at all. This would re-enable all services on the ME.

It is possible to inform the user of any updates to the Selective UE Capabilities list by including the relevant text in the SMS OTA Message, as depicted in step 13, figure 5.1.1.

The disabling network operator can provide the user with an optional customer service number to call for assistance, contained within the Information Message, step 13, figure 5.1.1.

As the user will be stopped from using a disabled UE before any messages have been sent to the network, there UE Capabilities list will always take precedence over subscribed services.

It is possible for the architecture described to disable the following services:

Call Control functions

Supplementary Services

Emergency Calls (subject to regional regulatory requirements)

SMS, via CS and PS

LCS, via CS and PS

GPRS based services

MBMS

IMS

It is not possible for the architecture described to disable:

Emergency Calls in the (U)SIM-less case (i.e. when the UE has been identified as misbehaving but does not have a valid (U)SIM inserted.)

This is due to the SMS OTA server not being able to send an update directly to the ME, step 8, figure 5.1.1.

5.1.3 (U)SIM File Based Architecture: Strengths and Weaknesses

5.1.3.1 Security

The security of SMS OTA is documented in 3GPP 23.048 and is a tried and tested security architecture. It should also be specified that the security of the Selective UE Capabilities list, when stored on the ME, should be at least at an equivalent level to that of the control functions to which it refers. As a more general security comment, it is thought that it would be worth considering the ideas from the Trusted Computing Group on the protection of the software relating to the lower level functionality of the ME. However, this is felt to be beyond the scope of the current Technical Report.

5.1.3.2 Customer Care

Using the architecture described in 5.1.1, the HPLMN will always have all of the information available as to when and why the service was disabled. The HPLMN should also always be able to re-enable services. The user will therefore be able to contact their HPLMN customer care centre to resolve the issue with their UE.

5.1.3.3 Roaming

Using the architecture described above, only the HPLMN is able to disable services on a misbehaving UE. However, as described above, the HPLMN will be able to disable services on behalf of a VPLMN.

5.1.3.4 Operational Aspects for Deployment

[Editors note: This sub-clause should cover operational aspects of deployment such as: Equipment/Nodes impacted (E.g. SGSNs, UEs, (U)SIMs), number of nodes impacted and estimated timescales to deploy complete service architecture]

Implementing the architecture described in figures 1 and 2, the following elements are expected to be impacted:

IMEI database – The IMEI database would need to be implemented to provide the functionality described in the above sections. No network element currently provides the functionality required.

HLR – the HLR would need to be updated to recognise and respond to the Get IMEI request from the IMEI DB.

OTA Server – the OTA server would need to be configured to send the Update Allowed Services file.

ME – MEs would need to store the new (U)SIM Selective UE Capabilities list file and act accordingly.

(U)SIMs – the (U)SIM would need to implement a new data structure.

Operational procedures will need to be established to allow VPLMNs to disable services via the HPLMN Management Interface.

5.2 Architecture 2

5.2.1 Architecture 2: Description

Architecture 2 covers the UE, or more specifically ME, (supporting Selective Disabling Management Object), and the Device Management Server (DMS). These elements have similar role as the OTA Server/SMSC, USIM, and ME of the Architecture 1. Other network elements, their interactions, IMEI retrieval, and association of IMEI with IMSI can be similar as in the Architecture 1. The DMS receives the information on malfunctioning UEs , e.g., the same way as in the Architecture 1. The DMS sends a message using OMA DM protocol, to update (replace) the values in the nodes of the Selective Disabling Management Object, i.e., to update the Selective (UE) Disabling List.

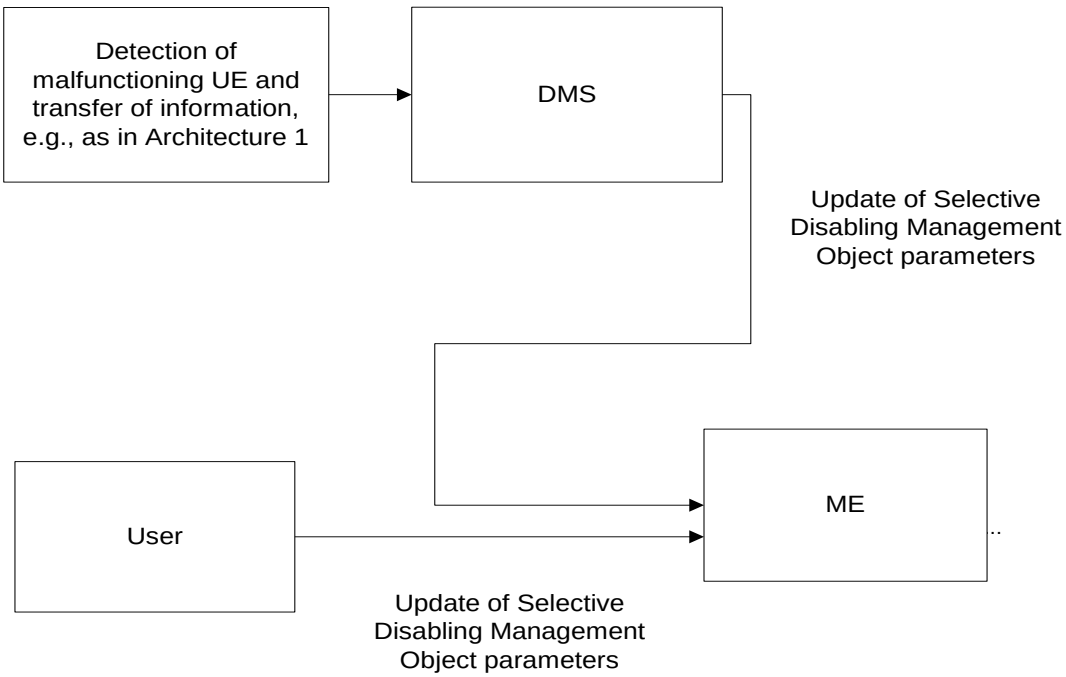

Figure 4.2.1

Figure 5.2.1: Basic architecture

Figure 5.2.2 exemplifies graphical notation of (a part of) the Selective Disabling Management Object.

The leaf nodes “Mobile originated CS voice call”, etc. could have “disabled” or “enabled” as values, and also alphanumerical strings (e.g., customer support numbers or e-mail addresses) as values. Access types would be Get and Replace. However, these are only examples; the actual structure (interior nodes / leaf nodes), names, optionality of nodes, etc. are stage 3 decisions.

Manufacturer specific and other extensions can also be introduced, if seen relevant by OMA.

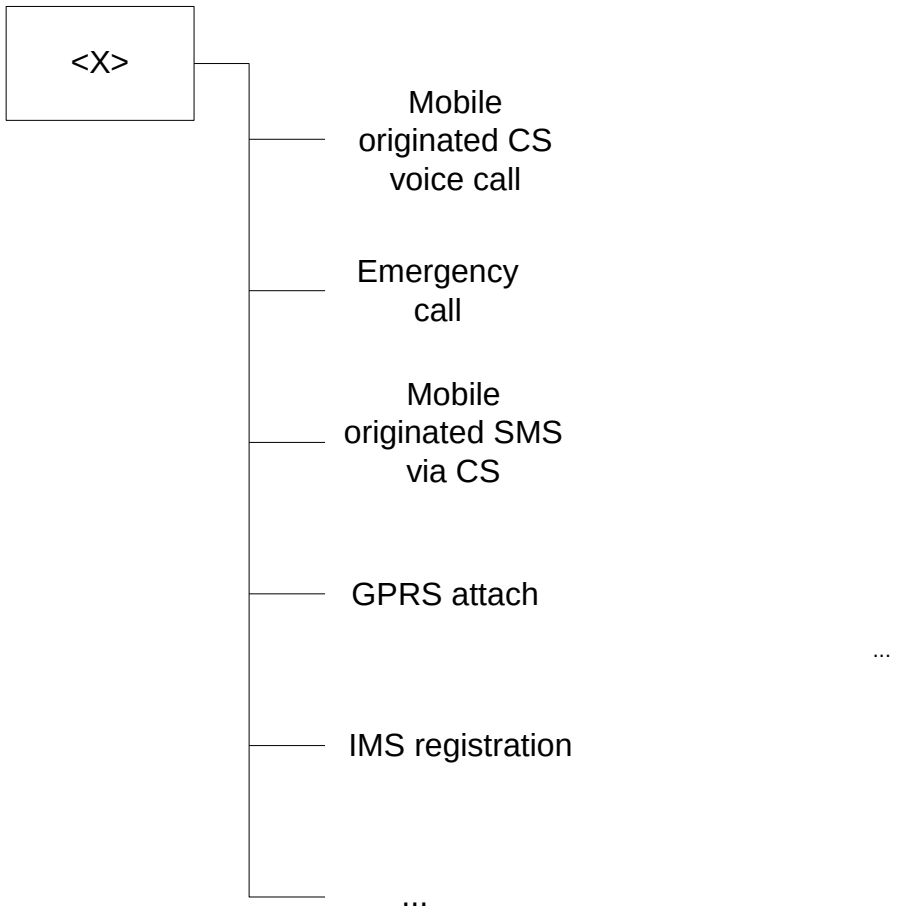

Figure 4.2.2

Figure 5.2.2: Selective Disabling Management Object

5.2.2 Architecture 2: Assessment against SA1 requirements

The original SA 1 requirements are presented below in *italics*, and comments in regular text:

1. *The Selective UE Capabilities list, shall be maintained in the UE, and UE shall not request any services indicated as disabled*. Parameters stored on ME.

2. *At registration the HPLMN or VPLMN may interrogate the status of the list and provide a new list.* (To be assessed after the actual requirement on VPLMN clarified.)

3. *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.* The parameters are to be stored in the ME permanent memory, and the values remain in the ME also when (U)SIM card is changed.

4. *It should be ensured that UEs are not maliciously disabled, including malicious disabling by a VPLMN, or accidentally disabled, or kept disabled,* The same authentication mechanisms, which are used in context of other OMA DM management objects, can be used to ensure the authenticity of the messages.

5. *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 user has access to modify the settings (to re-enable the disabled services).

6. *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.* Leaf nodes of management objects can contain alphanumerical strings, the strings can be updated by the DMS and presented to the user.

7. *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.* As above.

8. *The specifications should also provide the capability for the network to include an optional text string that will be displayed by the UE.* As above.

9. *The UE Capabilities list shall take precedence over subscribed services.* The implementation of this requirement is not restricted by the architecture.

10. *The services to be included in the list are:* These services are included as nodes in the Selective Disabling Management Object.

    - *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*

5.2.3 Architecture 2: Strengths and Weaknesses

The main strength of this alternative is the compatibility with existing device management architecture, procedures and implementations.

The weakness of this alternative is that the standardisation takes place in two organisations, 3GPP and OMA.

5.2.3.1 Security

The same authentication mechanisms, which are used in context of other OMA DM management objects, can be utilized for Selective Disabling Management Object, too.

5.2.3.2 Customer Care

The DMS(s) updating the Selective Disabling Management Object parameters can be accessed by customer care personnel the same way as they access DMS(s) for other purposes, e.g., when provisioning service parameters to customers.

5.2.3.3 Roaming

HPLMN can update the Selective Disabling Management Object parameters while the user is roaming, whenever there is a possibility to carry the messages between DMS and UE (e.g., over GPRS, or CS data).

(The actual stage 1 requirements for VPLMN access need to be clarified.)

5.2.3.4 Operational Aspects for Deployment

[Editors note: This sub-clause should cover operational aspects of deployment such as: Equipment/Nodes impacted (E.g. SGSNs, UEs, (U)SIMs), number of nodes impacted and estimated timescales to deploy complete service architecture]

This architecture has impacts on DMS and ME. Impacts on network elements providing the disabling information to the DMS are similar to impacts in the Architecture 1, if the overall architecture is similar to the Architecture 1 (see chapter 5.2.1).

5.3 Architecture 3

6 Conclusion

The feasibility study has studied different alternatives to provide a solution for the feature called Selective Disabling of UE Capabilities. This TR details two possible solutions for the Selective Disabling of UE Capabilities, one based on SMS OTA and one based on OMA Device Management (DM).

Selective Disabling of UE Capabilities is a feature to be used as a drastic action to selectively disable services on misbehaving UEs. A misbehaving UE is a UE which contains application(s) which is(are) misbehaving due to e.g. wrong implementation or virus infection. Typically, the misbehaving UEs cause downgrades to the network capacity and additional charges through abnormal repetitions of, e.g., transmission of service indications to the network.

The list of SA1 required services to be able to disable is limited to mobile originated services as follows:

- Mobile originated CS calls
- CS Emergency calls
- Mobile originated Supplementary Services
- Mobile originated SMS over CS
- Mobile originated SMS over PS
- Mobile originated location services over CS
- Mobile originated location services over PS
- Mobile originated PDP Contexts
- Mobile originated MBMS Contexts
- IMS Service (Deregister and disable IMS Registration Requests)

Note that disabling of PDP Contexts will be a second step to disable a misbehaving IMS application sending repeatedly IMS registrations. The need for selectively disable the IMS Emergency service needs further studies when IMS Emergency has been specified.

A reasonable requirement on a mobile is that applications downloaded to the mobile will work on APIs that cannot have influence on the type-approved behaviour of the mobile's signalling stack e.g. RR, MM, GMM, CM etc.

This feasibility study recommends that the OMA DM solution described in section 45.2.1 will be specified in 3GPP using standard OMA DM version 1.2 functions. Note that the OMA DM 1.2 standards permit the DM server address to be configured on the UICC, and, the subsequent 3GPP specifications should provide guidance on this topic.

To complete the specifications of this feature an OMA DM Management Object needs to be specified as a stage 3 specification under CT1 control. Note that the Management Object standardisation is to be carried out in 3GPP, and none of the contents of the Management Object need to be standardised in OMA. Such Management Object shall also include text information to be displayed for the end user to inform about the disabling in effect as well as contact information to customer care.

Regarding the OMA DM need to use bearers to contact the mobile and configure the Selective Disabling Management Object, it should be seen as a network initiated bearer request and not a mobile originated. Mobile terminated SMS is never disabled and OMA DM is using the WAP Push mechanism to establish the GPRS bearer. It is recommended to allow a WAP Push application to trigger PDP context activations to a DM server, while other applications in the mobile are blocked by the disabling feature.

The following rules are needed for when a UE, which has been disabled regarding mobile originated PDP Context activations, are allowed to make a PDP Context activation for Device Management usage:

In the OMA DM solution for Selective Disabling the feature is activated in a mobile that has been bootstrapped with and configured by a Device Management Server. The DM client will only request PDP Context activation when it has received an OMA DM notification through the WAP push mechanism. The DM Notification carries the DM Server ID as well as an MD5 Hash (Current OMA DM functionality).

To further strengthen the malicious triggered PDP Context activations by a misbehaving application the implementation of the selective disabling feature in the mobile should have a gate control where PDP Context requests are only acceptable in the API when a WAP Push notification has been received towards the OMA DM client (Application ID in WAP Push notification).

Annex <A>:
Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
06/04/2005	*SA2 #45*				*Editorial Update*	*0.0.0*	*0.0.1*
08/04/2005	*SA2 #45*				*Inclusion of approved documents S2-050590, S2-050890*	*0.0.1*	*0.1.0*
04/05/2005					*Editorial update to add the TR number 23.805*	*0.1.0*	*0.1.1*
23/05/2005	*SA2 #46*				*Inclusion of approved document – S2-051395rev1* *Editorial update to style format of section headings*	*0.1.1*	*0.2.0*
09/09/2005	*SA 2 #48*				*Conclusion agreed and text from S2-052280 added.*	*0.2.0*	*0.3.0*
09/09/2005	*SA2 #48*				*Editorial update to internally referenced subclause*	*0.3.0*	*0.3.1*