3GPP TR 23.888 V1.2.0 (2011-04)

Technical Report

3rdGeneration Partnership Project;

Technical Specification Group Services and System Aspects;

System Improvements for Machine-Type Communications;

(Release 11)

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.  
The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.  
This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.  
Specifications and reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

3GPP, Architecture, Machine-to-machine

***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](http://www.3gpp.org/)

***Copyright Notification***

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© 2010, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TTA, TTC).

All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  
LTE™ is a Trade Mark of ETSI currently being registered for the benefit of its Members and of the 3GPP Organizational Partners

GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword [5](#__RefHeading___Toc290974479)

1 Scope [6](#__RefHeading___Toc290974480)

2 References [6](#__RefHeading___Toc290974481)

3 Definitions and abbreviations [7](#__RefHeading___Toc290974482)

3.1 Definitions [7](#__RefHeading___Toc290974483)

3.2 Abbreviations [7](#__RefHeading___Toc290974484)

4 Architectural Considerations [7](#__RefHeading___Toc290974485)

4.1 Architectural requirements [7](#__RefHeading___Toc290974486)

4.1A. Architecture Principles [8](#__RefHeading___Toc290974487)

4.2 Architecture Model [8](#__RefHeading___Toc290974488)

4.3 Architectural baseline [9](#__RefHeading___Toc290974489)

Figure 4.3-1: 3GPP Architecture for Machine-Type Communication [10](#__RefHeading___Toc27975_3320553937)

5 Description of envisioned System Improvements for Machine Type Communication, use cases [11](#__RefHeading___Toc290974490)

5.1 Key Issue - Group Based Optimization [11](#__RefHeading___Toc290974491)

5.2 Key Issue - MTC Devices communicating with one or more MTC Servers [12](#__RefHeading___Toc290974492)

5.3 Key Issue - IP Addressing [12](#__RefHeading___Toc290974493)

5.4 Key Issue - Online Small Data Transmission [13](#__RefHeading___Toc290974494)

5.5 Key Issue –Offline Small Data Transmission [14](#__RefHeading___Toc290974495)

5.6 Key Issue – Low Mobility [14](#__RefHeading___Toc290974496)

5.7 Key Issue – MTC Subscriptions [15](#__RefHeading___Toc290974497)

5.8 Key Issue - MTC Device Trigger [16](#__RefHeading___Toc290974498)

5.9 Key Issue –Time Controlled [17](#__RefHeading___Toc290974499)

5.10 Key Issue - MTC Monitoring [19](#__RefHeading___Toc290974500)

5.11 Key Issue - Decoupling MTC Server from 3GPP Architecture [19](#__RefHeading___Toc290974501)

5.12 Key Issue - Signalling Congestion Control [20](#__RefHeading___Toc290974502)

5.13 Key Issue - MTC Identifiers [25](#__RefHeading___Toc290974503)

5.14 Key Issue - Potential overload issues caused by Roaming MTC devices [25](#__RefHeading___Toc290974504)

5.15 Key Issue - Low Power Consumption [28](#__RefHeading___Toc290974505)

6 Solutions [28](#__RefHeading___Toc290974506)

6.1 Solution - FQDN Identifier Solution [28](#__RefHeading___Toc290974507)

6.2 Solution - Transfer data via SMS [30](#__RefHeading___Toc290974508)

6.3 Solution - Paging within configured area [31](#__RefHeading___Toc290974509)

6.4 Solution - Paging stepwise [31](#__RefHeading___Toc290974510)

6.5 Solution - Paging within reported area [32](#__RefHeading___Toc290974511)

6.6 Solution - Triggering of non-attached MTC Devices based on location information provided by MTC User [32](#__RefHeading___Toc290974512)

6.7 Solution – Network access control by the PLMN [33](#__RefHeading___Toc290974513)

6.8 Solution - Introduction of a 3GPP MTC Service Abstraction Layer [34](#__RefHeading___Toc290974514)

6.9 Solution - MTC Monitoring - General [36](#__RefHeading___Toc290974515)

6.10 Solution – SGSN/MME based detection [37](#__RefHeading___Toc290974516)

6.11 Solution - HLR/HSS based detection [38](#__RefHeading___Toc290974517)

6.12 Solution - GGSN/P-GW based detection [39](#__RefHeading___Toc290974518)

6.13 Solution - Reporting by SGSN/MME [40](#__RefHeading___Toc290974519)

6.14 Solution - Reporting by HLR/HSS [41](#__RefHeading___Toc290974520)

6.15 Solution - Reporting by GGSN/P-GW [41](#__RefHeading___Toc290974521)

6.16 Solution - Reporting by PCRF [42](#__RefHeading___Toc290974522)

6.17 Solution – Allowed Time Period after TAU/RAU [43](#__RefHeading___Toc290974523)

6.18 Solution - MT Communication with NATTT [44](#__RefHeading___Toc290974524)

6.19 Solution – MT Communication with Micro Port Forwarding [47](#__RefHeading___Toc290974525)

6.20 Solution - Optimizing periodic LAU/RAU/TAU Signalling [51](#__RefHeading___Toc290974526)

6.21 Solution - Randomized triggering of time-controlled MTC operations [54](#__RefHeading___Toc290974527)

6.22 Solution – Rejecting connection requests by the SGSN/MME [54](#__RefHeading___Toc290974528)

6.23 Solution – Low Priority Access Indication [58](#__RefHeading___Toc290974529)

6.24 Solution - Directly Reporting to MTC Server from CN entity [61](#__RefHeading___Toc290974530)

6.25 Solution - Reporting to MTC Server through the intermediate node [62](#__RefHeading___Toc290974531)

6.26 Solution – Rejecting RRC Connection and Channel Requests by the eNodeB/RNC/BSS [63](#__RefHeading___Toc290974532)

6.27 Time Control Solution Summary [66](#__RefHeading___Toc290974533)

6.28 Solution - Access Control by RAN [68](#__RefHeading___Toc290974534)

6.29 Solution – IP address assignment mechanisms [73](#__RefHeading___Toc290974535)

6.30 Solution - MME/SGSN overload control by DL MTC traffic throttling [77](#__RefHeading___Toc290974536)

6.31 Solution – Rejecting connection requests at partial signalling links [78](#__RefHeading___Toc290974537)

6.32 Solution – Rejecting connection requests based on request types [80](#__RefHeading___Toc290974538)

6.33 Solution – UE behaviour changes [81](#__RefHeading___Toc290974539)

6.34 Solution – M2M device indication to network [81](#__RefHeading___Toc290974540)

6.35 Solution - Overload control within an MTC access grant time interval [82](#__RefHeading___Toc290974541)

6.36 Solution - Time controlled feature via Operator and MTC User Business Agreements [83](#__RefHeading___Toc290974542)

6.37 Solution - Simple Subscription Control [84](#__RefHeading___Toc290974543)

6.38 Solution – Device identifier used over MTCSP [85](#__RefHeading___Toc290974544)

Figure 6.38.2-1: 3GPP Architecture for Machine-Type Communication [86](#__RefHeading___Toc27977_3320553937)

6.39 Solution – Triggering MTC devices via HSS and NAS signalling [88](#__RefHeading___Toc290974545)

6.40 Solution – Information sent to trigger a MTC Device [91](#__RefHeading___Toc290974546)

6.41 Solution – Triggering of attached MTC Devices by reusing Network Requested PDP Context Activation procedure [91](#__RefHeading___Toc290974547)

6.42 Solution - Triggering of attached MTC Device via Pre rel-11 SMS [94](#__RefHeading___Toc290974548)

6.43 Solution - Triggering of attached MTC Device via intermediate node [94](#__RefHeading___Toc290974549)

6.44 Solution – Device Triggering reuse of MT SMS WAP Push [95](#__RefHeading___Toc290974550)

NOTE 1): This operation is not used by the SGSN. [97](#__RefHeading___Toc27979_3320553937)

6.45 Solution – Device trigger gateway solution [99](#__RefHeading___Toc290974551)

6.46 Solution – MT communications address resolution via DT-GW [101](#__RefHeading___Toc290974552)

6.47 Solution – UE without unique MSISDN using ICCID [103](#__RefHeading___Toc290974553)

6.48 Solution - Transfer data via SMS for MTC Devices sharing one MSISDN [104](#__RefHeading___Toc290974554)

7 Conclusions [105](#__RefHeading___Toc290974555)

7.1 Interim conclusions for release 10 specification work [105](#__RefHeading___Toc290974556)

7.2 Later Conclusions [106](#__RefHeading___Toc290974557)

8 Impacts to normative specifications [106](#__RefHeading___Toc290974558)

8.1 Related to Interim conclusions for release 10 specification work [106](#__RefHeading___Toc290974559)

8.2 Related to Later Conclusions [106](#__RefHeading___Toc290974560)

Annex A: Stage 2 PS Dependencies on MSISDN-based Subscriptions [107](#__RefHeading___Toc290974561)

A.1 General Considerations [107](#__RefHeading___Toc290974562)

A.2 PS stage 2 MSISDN dependencies [107](#__RefHeading___Toc290974563)

A.3 Impact of MSISDN-less subscriptions for PS only MS/UEs [111](#__RefHeading___Toc290974564)

Annex B: Change history [111](#__RefHeading___Toc290974565)

# 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.

# 1 Scope

This Technical Report studies and evaluates architectural aspects of the System Improvements for Machine Type Communications requirements specified in TS 22.368 [1].

Specifically, the following system improvements are considered:

- Architectural enhancements to support a large number of Machine-Type Communication (MTC) devices in the network;

- Architectural enhancements to fulfil MTC service requirements;

- Support combinations of architectural enhancements for MTC, though not all combinations may by possible.

The end-to-end aspects of communication between MTC devices and MTC servers (which can be located outside or inside the network operator's domain) are out of the scope of this study. However, the transport services for MTC as provided by the 3GPP system and the related optimizations are considered in this study. In addition, the aspects needed to ensure that MTC devices and/or MTC servers and/or MTC applications do not cause peak loads of short duration (e.g. a "busy minute" rather than a "busy hour") are within the scope of this TR.

Even though some provided solutions may be beneficial for communications from a MTC Device towards another MTC Device, this particular type communication has not been explicitly considered in this Technical Report.

This Technical Report analyzes architectural aspects to achieve these objectives and to gather technical content until it can be included in the relevant technical specifications.

# 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*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.368: "Service Requirements for Machine-Type Communications".

[3] NAT Traversal through Tunnelling (NATTT) available at: <http://www.cs.arizona.edu/~bzhang/nat/nattt.htm>

[4] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based services and Packet Data Networks (PDN)".

[5] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[6] 3GPP TS 23.040: "Technical Realization of the Short Message Service (SMS)".

[7] ITU‑T Recommendation E.118: "Operation, numbering, routing and mobile service – International operation – General provisions concerning Administrations".

[8] ETSI TS 102 221: "UICC-Terminal interface; Physical and logical characteristics".

[9] 3GPP TS 23.142: “Value-added Services for SMS (VAS4SMS)”.

[10] 3GPP TS 23.040: “Technical realization of the Short Message Service (SMS)”.

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1], TS 22.368 [2], and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

**<Term:** Definition.>

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

MTC Machine Type Communications

M2M Machine-to-Machine

# 4 Architectural Considerations

## 4.1 Architectural requirements

Editor's note: Contributions to this clause should follow after agreements are achieved in the Required Functionality clause s of individual Key Issues.

1. The 3GPP Core Network can communicate with the MTC Server. An intermediary entity may be used for the control plane communication for topology hiding or protocol translation purposes. Any intermediary entity for the user plane communication is out of scope of 3GPP standardization.
2. Both mobile terminated and mobile originated communication shall be supported. To initiate mobile terminated communication, an MTC Server shall be able to uniquely identify an MTC Device.

Editor’s Note: Unique identification of an MTC Device when the UE comprises multiple TEs may imply further requirements.

1. The mobile network shall provide security mechanisms that can be used to:

* ensure that an MTC Server can only communicate with certain UEs used for MTC;

NOTE 1: This requirement does not imply that it applies to all MTC Server communication to UEs used for MTC. Some scenarios allowing for less restricted communication have been considered.

Editor’s Note: The association of an MTC Server to certain UEs used for MTC for means of restricting communication (e.g. between an MTC User and the MTC Subscriber) is FFS.

* ensure that only authorized PDN entities can communicate with the UEs used for MTC;
* ensure that a UE used for MTC can only communicate with the MTC Server(s) of its subscriber, and that communication with any other entity is not possible.

The existing 3GPP security functions e.g. authentication and encryption shall be unaffected by the above security measures.

1. It shall be possible to provide secure and encrypted communication between PLMN and MTC Server.
2. The reference points between the MTC Server and the PLMN shall enable message exchange to support the following services:

a. Device Triggering

b. …

## 4.1A. Architecture Principles

Editor’s Note: This subclause captures principles that can be agreed in discussion of architecture. Once agreed, these principles will guide further work in the TR.

1) Communication at the application level between the MTC Device and the MTC Application is out of scope of 3GPP standardization.

## 4.2 Architecture Model

Different models are foreseen for machine type of traffic in what relates to the communication between the MTC Application and the 3GPP network. In a so called Direct Model, the MTC Application communicates with the UE for MTC directly as an over-the-top application on 3GPP network. This is shown as Figure 4.2-1(A).

In a complementary way, several sub models are foreseen for an Indirect model, in which the MTC Application communicates with the UE for MTC by making use of additional services provided by the 3GPP network:

1. The MTC Application would make use of an MTC Server, for additional value added services, provided by a third party Service Provider, that is, outside the 3GPP responsibility. The interface between the MTC server and the MTC application is totally out of the scope of 3GPP. The MTC server communicates with the 3GPP network by means of an interface or set of interfaces. This is shown as Figure 4.2-1(B).

2. The MTC Application makes use of an MTC Server, again for additional value added services, provided by the 3GPP operator (which becomes a Service Provider). The interface between the MTC Server and the MTC application remains still out of the scope of 3GPP, whilst the communication between the MTC server and the 3GPP network becomes internal to the PLMN. This is shown as Figure 4.2-1(C),

,

MTC

Device

MTC

Device

UE

MTC Application

3GPP Boundary

3GPP Network

Direct Model

MTC

Device

MTC

Device

UE

MTC Application

3GPP Boundary

3GPP Network

Indirect Model

MTC Server

MTC

Device

MTC

Device

UE

MTC Application

Indirect Model

MTC Server

3GPP Network

B) Service Provider controlled communication

C) 3GPP operator controlled communication

A) Direct communication, under 3GPP operator control

Figure 4.2-1: MTC Application to UE for MTC Communication Models

3.- Since the sub models in the indirect scenario are not mutually exclusive but just complementary, it is possible for a 3GPP operator to combine them for different applications. Next figure provides a high level model in which the 3GPP operator provides value added services to an MTC Application and in addition, offers telecom services to a third party Service provider. This is shown as Figure 4.2-2.

The communication between the MTC server and 3GPP network is, as in bullet #1, within the scope of 3GPP, including when that communication becomes internal to the network, as in bullet #2. The communication between the MTC Application and the MTC Server is out of the scope of 3GPP.

MTC

Device

MTC

Device

UE

MTC Application

3GPP Boundary

Indirect Model

MTC Server

MTC Server

3GPP Network

MTC Application

Figure 4.2-2: Multiple MTC Applications using Diverse Communication Models

NOTE: The services provided by the MTC server within the 3GPP network maybe either:

- different from those offered by the external MTC Server

- the same as those in the external MTC Server

- a subset/superset of those offered by the external MTC Server

- The functionality provided by either MTC Server is out of the scope of this document.

## 4.3 Architectural baseline

The end-to-end application, between the UE used for Machine Type Communication (MTC) and the M2M Application, uses services provided by the 3GPP system, and optionally services provided by an MTC Server. The 3GPP system provides transport and communication services (including 3GPP bearer services, IMS and SMS) including various optimizations that can facilitate MTC.

Figure 4.3-1 shows a UE used for MTC connecting to the 3GPP network (UTRAN, E-UTRAN, GERAN, I-WLAN, etc) via the Um/Uu/LTE-Uu interface. With the indirect models the UE used for MTC communicates with a MTC Server or other UEs used for MTC using the 3GPP bearer services, SMS and IMS provided by the PLMN. The architecture covers the various architectural models described in Section 4.2.

- Direct Model - Direct Communication provided by the 3GPP Operator: The M2M Application connects directly to the operator network without the use of any MTC Server;

- Indirect Model – MTC Service Provider controlled communication: The MTC Server is an entity outside of the operator domain. The MTCi, MTCsp and MTCsms are external interfaces (i.e. to a third party M2M service provider);

- Indirect Model – 3GPP Operator controlled communication: The MTC Server is an entity inside the operator domain. The MTCi, MTCsp and MTCsms are internal to the PLMN;

- Hybrid Model: The direct and indirect models are used simultaneously in the hybrid model e.g. connecting the user plane using the direct model and doing control plane signalling using the indirect model.

The MTC Server is an entity which connects to the 3GPP network via MTCi/MTCsp/MTCsms interfaces and thus communicates with UEs used for MTC or nodes in the PLMN. MTC Server may be an entity outside of the operator domain or inside an operator domain.

Editor’s Note: Clarification and naming of the MTC Server may need further consideration e.g. to facilitate the alignment with the work of other SDOs.

Editor’s Note: Considerations for hybrid scenarios and for security and scalability for the direct model is FFS.

The ‘M2M Application’ entities in the figure are entities outside of 3GPP scope. They are solely used as abstract entities to show the end-to-end view for MTC and simplify mapping to MTC specifications of other standardization organizations.

When the MTC interfaces are to a third party M2M service provider, security measures need to be applied to avoid unauthorized access.

Editor’s Note: Security measures needed when the MTC interfaces are to a third party M2M service provider are FFS in WG SA3.

3GPP

Boundary

MTC Server

GGSN /

PGW / PDG

Proxy (TBD)

SGSN /

MME

HLR / HSS

API

MTCi

SMS-SC

IP-SM-GW

Legacy SMS

IP SMS

MTCsp

*Indirect model –*

*service provider controlled*

*Indirect model – operator controlled*

Gr/S6a

Um /

Uu /

LTE-Uu

Internal interfaces (TBD)

Control plane

User plane

*Direct model*

Gi/SGi

UE

MTC User

MTCsms

Figure 4.3-1: 3GPP Architecture for Machine-Type Communication

Editor’s Note: The term proxy in the above figure is a temporary name. Contributions are invited to name the termination point for the MTCsp. Other possible names are MTC Gateway, Signalling Gateway, Frontend, IWK or as proposed in subclause 6.45.

The reference points are listed as below:

**MTCi**: It is the reference point that the MTC Server uses to connect the 3GPP network and thus communicates with UEs used for MTC via 3GPP bearer services/IMS. MTCi could be based on Gi, SGi, and Wi interface.

**MTCsp**: It is the reference point the MTC Server uses for signalling purposes with the 3GPP network.

**MTCsms:** It is the reference point the MTC Server uses to connect the 3GPP network and thus communicates with UEs used for MTC via 3GPP SMS.

**API:** It is an interface where the operator/M2M service provider offers connection services for UEs used for MTC. This is out of scope for 3GPP.

The MTCi, MTCsp and MTCsms terminate in the MTC .

The MTC Server may be used to expose interfaces that are not 3GPP access specific to M2M Applications, e.g. in order to facilitate the deployment and operation of services that are access system independent.

The MTCi terminates in the GGSN/PGW. It could be based on Gi/SGi/Wi. Existing protocols over those reference points such as RADIUS/Diameter specified in TS 29.061 [4] are also supported over MTCi.

The MTCsp terminates in the Proxy. The Proxy hides the internal PLMN topology and relays or translates signaling protocols.

Editor’s Note: The term proxy is a temporary name. Contributions are invited to name the termination point for MTCsp (as well as other potential interfaces that may be identified).

The MTCsms terminates in the SMS-SC. The SMS-SC may connect to the IP-SM-GW to perform SMS interworking.

Editor’s Note: The potential internal PLMN interfaces connected to the Proxy is as will be agreed during the SIMTC study.

The 3GPP Architecture supports roaming scenarios in which the UE used for MTC obtains service by means of Um/Uu/LTE-Uuin a VPLMN.

Editor’s Note: The roaming architecture is FFS.

# 5 Description of envisioned System Improvements for Machine Type Communication, use cases

Editor's Note: This clause is intended to provide an overview of the alternative architecture fulfilling the requirements. Architecture solutions may apply to all or only some scenarios.

## 5.1 Key Issue - Group Based Optimization

### 5.1.1 Use case description

Editor's Note: Expand upon the Service Description use case, including technical constraints and interpretations.

MTC Devices can be grouped together for the control, management or charging facilities etc. to meet the need of operators. This optimization may provide easier mode to control/update/charge the MTC devices, in a granularity of group, which may decrease the redundant signalling to avoid congestion. Also the network resource could be saved by using group based optimization when the number of MTC devices is large. The MTC devices within the same group can be in the same area and/or have the same MTC features attributed and/or belong to the same MTC user, which provides the flexibility to allocate a group. Moreover, each of the MTC devices is visible from the network perspective.

Editor's Note: Group based optimization may include many optimizations. E.g. group based charging, group based signalling saving etc. It is not clear whether the solutions for these optimizations will be independent to each other or not. Whether this key issue will be split for evaluation is FFS.

### 5.1.2 Required Functionality

Editor's Note: Capture agreements on requirements for solving the key issue. This clause may be omitted if deemed unnecessary.

### 5.1.3 Evaluation

## 5.2 Key Issue - MTC Devices communicating with one or more MTC Servers

### 5.2.1 Use case description

A MTC subscriber may have one or more MTC servers that communicate with the subscriber's MTC devices through the PLMN, which is optimized for machine-type communications. This key issue focuses on the common service requirements as specified in TS 22.368 [1] (e.g. addressing, identifiers, charging, security, etc.) for communication between MTC devices and MTC servers.

### 5.2.2 Required Functionality

To enable communication between MTC devices and MTC servers the following requirements shall be met:

- It shall be possible to use one or more MTC servers for communicating with the MTC devices of a MTC subscriber.

- The PLMN shall allow transactions between an MTC device and an MTC server, either initiated by the MTC device or the MTC server.

- The PLMN shall be able to authenticate and authorize an MTC device before the device can communicate with an MTC server.

- It shall be possible to uniquely identify an MTC device;

- It shall be possible to uniquely identify an MTC Group i.e. a collection of MTC devices belonging to the same MTC subscriber;

## 5.3 Key Issue - IP Addressing

### 5.3.1 Use case description

This key issue focuses on the common service requirements regarding IP addressing as specified in TS 22.368 [1] for communication between MTC devices and MTC servers.

For some MTC Applications, there is a need for the MTC Server to be the initiator of communications between the MTC Server and the MTC Device (e.g. due to the need for centralized control). Typically due to the limitation of the public IPv4 address space, the MTC Device is assigned a private non-routable IPv4 address and is thus not reachable by the MTC Server. For IPv6 addressing, the number of available IPv6 prefixes is abundant and thus there is no limitation for the public IPv6 address space.



Figure 5.3.1-1: Server in a public address space sending a mobile terminated message to a MTC Device in a private IPv4 address space

For both IPv4 and IPv6 addressing, the network may employ network topology security techniques that are intended to thwart unauthorized mobile terminated communications over a pre-existing globally routable IP connection. These security techniques are employed by the network operator to address various security goals. These security goals may include, but are not limited to, the desire for end-system privacy (e.g. to prevent device profiling), topology hiding (e.g. to mitigate scanning attacks) and to prevent unauthorized or unwanted communications with the MTC device.

These techniques may result in blocking a MTC server from initiating the IP communications with a MTC device until granted by the network. Thus when the MTC server needs to communications with the MTC device over IP, a mechanism is required to request the network to grant the IP based communications with the MTC device.

### 5.3.2 Required Functionality

- The system shall provide a mechanism, according to operator policy, where an MTC Server in a public address space can successfully send a mobile terminated message to the MTC Device inside a private IPv4 address space or to the MTC device attached to a PLMN employing various security techniques that thwart mobile terminated communications triggered over a globally routable IP connection.

- The mechanism shall be scalable;

- The mechanism shall minimize the required configuration by the MNO and the MTC User;

- The mechanism shall minimize the required messaging transactions by the MTC Server to initiate MT communications;

- The mechanism shall minimize the messaging sent over the air to the MTC Device;

- The mechanism shall minimize any additional user plane latency;

- The mechanism shall minimize any additional security threats to the MTC Device.

## 5.4 Key Issue - Online Small Data Transmission

### 5.4.1 Use case description

Editor's Note: Expand upon the Service Description use case, including technical constraints and interpretations.

MTC Devices with Online Small Data Transmission frequently send or receive only small amounts of data. The exact amount that is considered to be small may differ per individual system improvement proposal. It is the amount of data where a specific system improvement proposal still provides its benefits.

For online small data transmission it is assumed that data transfer can happen any time when needed by the application.

### 5.4.2 Required Functionality

Editor's Note: Capture agreements on requirements for solving the key issue. This clause may be omitted if deemed unnecessary.

The following functionalities are required for Online Small Data Transmission:

- It shall be possible to transmit small amounts of data with very efficient resource usage when the MTC Device is attached and context activated.

- The definition of a small amount of data shall be configurable per subscription.

### 5.4.3 Evaluation

## 5.5 Key Issue –Offline Small Data Transmission

### 5.5.1 Use case description

Editor's Note: Expand upon the Service Description use case, including technical constraints and interpretations.

MTC Devices with Offline Small Data Transmissions infrequently send or receive only small amounts of data. The exact amount that is considered to be small may differ per individual system improvement proposal. It is the amount of data where a specific system improvement proposal still provides its benefits. Such MTC Devices may detach from the network when not transmitting data.

For offline small data transmission the MTC application may be able to know whether the MTC Device is available for communication and transfer data, or may also transfer data when the MTC Device is not available for communication, e.g. not reachable.

### 5.5.2 Required Functionality

Editor's Note: Capture agreements on requirements for solving the key issue. This clause may be omitted if deemed unnecessary.

The following functionalities are required for Offline Small Data Transmission:

- It shall be possible to transmit small amounts of data with very efficient resource usage when the MTC Device is not attached and not context activated.

- The definition of a small amount of data shall be configurable per subscription.

## 5.6 Key Issue – Low Mobility

### 5.6.1 Use case description

Editor's Note: Expand upon the Service Description use case, including technical constraints and interpretations.

For MTC Device with low mobility, several use cases should be captured in this TR as follows:

- not move frequently and may move only within small area: e.g. health monitoring at home.

- not move frequently but may move within wide area: e.g. mobile sales terminals.

- not move normally, i.e. with fixed location: e.g. water metering.

For this kind of MTC Device, it is studied how to reduce the frequency of mobility management procedures and how to optimize the paging.

### 5.6.2 Required Functionality

The required functionality for low mobility should result in:

- reduction in resource usage for low mobility MTC Devices (e.g. paging, location management signalling, mobility context in MME/SGSN/MSC)

### 5.6.3 Evaluation

## 5.7 Key Issue – MTC Subscriptions

### 5.7.1 Use case description

Based on stage1 requirements, MTC Features are subscribed and controlled by subscription.

Any usage of the subscribed MTC features is activated by default at the time of the subscribing the feature.

It should be possible to allow the MTC Subscribers to activate the unsubscribed MTC Features or deactivate the subscribed MTC Features based on the operator policy. The mechanisms used for activation/deactivation are outside the scope of 3GPP. The MTC solution shall make it possible to provision the home PLMN with MTC subscriptions and allow one or more MTC Devices to share this subscription. This key issue aims at specifying the architectural requirements related to MTC subscriptions as well as the relationship between MTC subscriptions, MTC Devices and MTC architecture enhancements.

### 5.7.2 Required Functionality

MTC Features are controlled by subscription in HSS.

NOTE: MTC Features should be subscribed by already existing methods; It is normally out of scope of 3GPP standardisation e.g. via the provisioning interface or via a web interface.

The capability to subscribe/unsubscribe MTC Features is provided to the MTC Subscriber. The subscription information (i.e. MTC Feature is subscribed) of the MTC Feature shall be stored in the relevant 3GPP CN entities.

It is also possible for a network operator to restrict incompatible MTC Feature subscription (according to network operator policy.) During the activation/deactivation, if the MTC Subscriber request results in a set of incompatible MTC Features (according to network operator policy), it shall be possible for the operator to reject the request.

Upon attachment or subscription update, it shall be possible for the SGSN/MME to support only a subset of the subscribed MTC features based on network capability and/or MTC device capability.

Editor's note: It is FFS how the device capability can be known to the network.

Editor's note: It is FFS, if MTC feature(s) may be designated as "essential". In which case, the MME/SGSN informs the MTC device and detaches the device when the MTC Features cannot be supported.

A feature is considered as essential if a MTC device cannot operate normally when the feature is not enabled.

A feature is considered as mandatory when the home operator forbids attachment to the network when this feature is not/cannot be enabled.

Editor's note: Upon attachment or subscription update when the MTC device is in roaming, it may be possible for the visited network operator to inform the home operator of the features are not supported.

It may be possible for the network operator to inform the MTC Device enabled/disabled status of the MTC features.

Editor's note: It is FFS which MTC features' enabled status may be notified to the MTC device.

The following requirements are relevant to MTC subscriptions:

- It shall be possible to provision the home PLMN with MTC Subscriptions, each one shared by one or more MTC Devices.

- Each MTC Device shall be associated to one MTC subscription and shall have a device subscription including the security credentials used to authenticate the device.

- An MTC subscription shall indicate MTC Features that are subscribed by the MTC Devices sharing this subscription.

- It shall be possible for all MTC Devices sharing the same MTC subscription to use all subscribed MTC Features belonging to this subscription.

Editor's Note: As it is assumed that subscribed MTC Features are activated whenever supported by the network, the above requirement may be redundant.

## 5.8 Key Issue - MTC Device Trigger

### 5.8.1 Use case description

For many M2M applications there may be an interest to have poll model for communications between MTC devices and the MTC Server. This may be because the MTC User wants to be in control of communication from MTC Devices, and does not allow MTC Devices to randomly access the MTC Server. Also for applications where normally the MTC Devices initiate communications, there may occasionally be a need for the MTC Server to poll data from MTC devices.

For MTC Devices that are not continuously attached to the network or that have no always-on PDP/PDN connection it is beneficial to trigger MTC Devices to attach and/or establish a PDP/PDN connection based on a trigger indication from the MTC server. It is important that it can be guaranteed to the MTC User that MTC Devices can only be triggered to attach and/or establish a PDP/PDN connection by authorized MTC Servers. If the network is not able to trigger the MTC Device, e.g. due to network congestion, the network may report the trigger failure to the MTC Server.

Triggering of MTC Devices is based on the use of an identifier identifying the MTC Device that needs to be triggered. The identifier used by the MTC User in the triggering request to the MTC Server can be different from the identifier used by the MTC Server in the triggering request to the PLMN network.

### 5.8.2 Required Functionality

The following functionality is required to trigger MTC Devices:

- The PLMN shall be able to trigger MTC Devices to initiate communication with the MTC Server based on a trigger indication from the MTC server.

- The network shall provide a mechanism such that the MTC Device can only receive trigger indications from authorized MTC Servers.

- Upon receiving a trigger indication from a source that is not an authorised MTC Server, the network shall be able to provide the details of the source (e.g. address) to the MTC User.

- The network shall provide a mechanism to the MTC User to provide a set of authorized MTC Server(s).

- The trigger mechanism shall be able to provide a scalable transmission of trigger request and trigger response messages for multiple MTC Devices in the PLMN and on the interfaces to the MTC Server.

- A MTC Device shall be able to receive trigger indications from the network and establish communication with the MTC server when receiving the trigger indication. Possible options are:

- Receiving trigger indication in detached state and establish communication.

- Receiving trigger indication in attached state and the MTC device has no PDP/PDN connection.

- Receiving trigger indication in attached state and the MTC device has a PDP/PDN connection.

NOTE 1: There are currently available solutions to trigger MTC Devices (e.g. unanswered CS call attempts, sending an SMS). However, these have disadvantage when used at a large scale (e.g. they are based on MSISDNs), and work only for attached MTC Devices. This key issue will investigate possible improvements over the currently available means for triggering.

- A HPLMN supporting the MTC device trigger feature shall provide an interface for reception of a trigger indication into the PLMN in order to be delivered by the network to the addressed MTC device. This interface:

- shall be globally consistent (i.e. the same) across PLMNs supporting the MTC device trigger feature.

- shall not require the MTC server to have prior knowledge of the current reachability state (e.g. attachment and PDP context/PDN connection states) of the targeted MTC device.

NOTE 2: This interface does not preclude an MTC server from interrogating/monitoring the network for the current reachability state of a MTC device.

### NOTE 3: For backwards compatibility reasons, this interface does not preclude a MTC server from using a pre-existing interface (e.g. submitting an SMS-based trigger indication directly to an SMS-SC).  However, the intention would be for MTC service providers to migrate towards utilizing this new interface for device triggering.

- If the network is not able to trigger the MTC Device, e.g. due to network congestion, the network may report the trigger failure to the MTC server.

Editor’s note: It is FFS that the network always needs to report the trigger failure to the MTC server for all the MTC device trigger solutions.

- In the triggering request to the PLMN the MTC Server shall use an identifier to indicate the MTC Device that is required to be triggered. The identifier used:

- can be a new identifier; or

- can be an existing identifier such as an IMSI.

NOTE 4: The identifier used by the MTC User in the triggering request to the MTC Server can be a different identifier than the one used by the MTC Server in the triggering request to the PLMN. The identifier used by the MTC User is out of scope of 3GPP standardisation and may e.g. be an application specific identifier.

### 5.8.3 Evaluation

## 5.9 Key Issue –Time Controlled

### 5.9.1 Use case description

MTC Devices with Time Controlled MTC Feature send / receive data only at certain pre-defined time periods. Network operators can pre-define / alter the time period based on criteria (e.g. daily traffic load) and only allow MTC Devices to access the network (attach to the network or send / receive data) during the pre-defined time period. The key issue aims at describing how to restrict MTC Device's access to the network and avoid unnecessary network load outside these pre-defined time periods. The home network operator may restrict altering the time period by the visited network operator e.g. to avoid traffic when the MTC server is in maintenance by means of a 'forbidden time interval.' During this forbidden interval, the network shall reject access requests per MTC Device. This allows for maintenance, e.g. of the MTC Server.

Editor's Note: The interaction of PAM and Time Control are FFS.

Typically, an MTC User agrees with an operator on a predefined time period for a group of MTC Devices. The time in which access is permitted is termed a 'grant time interval.' The network shall communicate the (altered) grant time interval to the MTC Device and may also do so to the MTC Server and MTC User. A 'grant time interval' does not overlap with a 'forbidden time interval.'

In roaming scenarios, the local network operator may alter the access grant time interval based on local criteria, e.g. (daily traffic load, time zones) but the forbidden time interval may not be altered.

It is desirable that access of MTC Devices with the same access grant interval is distributed across this interval in a manner to reduce peaks in the signalling and data traffic.

For many applications, individual MTC Devices do not need the total duration of this predefined time period to communicate with the MTC Server. Typically a 5-10 minutes communication window is sufficient for an individual MTC Device. The network operator may limit the duration of these communication windows. To avoid network overload, signalling and data traffic the communication windows of the devices shall be distributed over the pre-defined time period e.g. through randomization of the start time of the individual communication windows. For a network operator, it can be beneficial that the MTC Devices are not attached outside their communication window. Therefore, the network operator should be able to enforce detach of an MTC Device from the network at the end of the communication window of a device.

The network operator may allow MTC Devices to exchange signalling and send and receive data outside of defined time intervals but charge differently for such traffic.

Time Control terminology is illustrated in Figure 5.9.1-1.



Figure 5.9.1-1: Time Control Terminology

NOTE: The Communication Window can be expressed as a start and stop time, a start time and duration, an offset from the beginning of the Grant Time Interval and a duration, etc dependent on the solution.

The MTC Device may defer access of the network until it will originate communication, provided that the MTC Device's upper layers do not require reception of mobile terminated communication during the period of time the MTC Device remains Detached.

### 5.9.2 Required Functionality

The following requirements can be derived from the Time Controlled MTC feature requirements specified in TS 22.368 [2]:

- the network operator shall be able to allocate for a group of MTC devices time periods during which signalling or user plane traffic to/from the network is allowed. This is termed 'grant time interval';

- the network operator shall be able to further restrict the time during which signalling or user plane traffic to/from the network is allowed for individual MTC devices in the group to a time window with a defined duration.

- the network shall be able to inform the MTC Device of the (altered) time periods during which signalling or user plane traffic to/from the network is allowed. The network may communicate the (altered) time periods to the MTC Server or MTC User;

- enforcement of a detach of an MTC Device from the network at the end of the of the Device's communication window shall be supported;

- roaming shall be supported for MTC devices with Time Controlled Feature. The local network operator (in roaming scenarios) may alter the grant time interval based on local criteria;

- the network shall be able to alter above time periods.

- the network operator shall be able to allocate for a group of MTC devices a time period during which signalling or user plane traffic to/from the network is disallowed. This is termed 'forbidden time interval.' A forbidden time interval and a grant time interval shall not overlap. The forbidden interval shall not be altered. The home network operator or MTC User use the 'forbidden interval' to restrict the extent to which change of the time periods is allowed by the (visited) network operator (e.g. to avoid traffic when the MTC server is in maintenance);

- peaks in traffic (including signalling traffic) shall be avoided (e.g. by randomization of the time during which the MTC Devices communicate.)

NOTE: It is possible for the network operator to allow or reject the MTC device's access to the network according to the operator policy, when it is out of time period.

### 5.9.3 Evaluation

## 5.10 Key Issue - MTC Monitoring

### 5.10.1 Use case description

MTC Devices may be deployed in locations with high risk, e.g. possibility of vandalism or theft of the communication module. For those MTC Devices, it is desirable that the network detects and reports events (including location) caused by those devices that may result, for example, from vandalism or theft of the communication module. If such an event is detected, the network might be configured to perform special actions, e.g. limit the access or reduce the allocated resource.

### 5.10.2 Required Functionality

The following functionalities are required for MTC monitoring:

- It shall be possible for the MTC User to configure the monitoring events, e.g. monitoring the association of the MTC Device and UICC, misalignment of the MTC feature, change in the point of attachment, loss of connectivity.

- The MTC User shall configure the action to be executed by the network.

- It shall be possible for the network to detect monitoring events.

- It shall be possible for the network to report the detected events to the MTC User or the appropriate MTC Server and optionally to perform action to reduce services provided to the MTC Device.

- It shall be possible to configure the maximum time between the actual loss of connectivity and its detection in the MTC subscription. The maximum detection time can be in the order of 1 minute to 1 hour.

## 5.11 Key Issue - Decoupling MTC Server from 3GPP Architecture

### 5.11.1 Use Case Description

Machine to machine communications exist today, over a variety of access systems. These essentially make use of particular features exposed by individual access systems, devices and aggregation services to build a unique 'vertical system' to support an application for an end customer. Examples include logistics, point of sale and power metering.

The current direction of the industry is to eventually provide general service interfaces to enable a new class of 'layered' applications that can work with diverse MTC devices, network operators, accesses and diverse business logic components without requiring a unique 'from scratch' system integration effort.

The current abstraction shown in the SA1 service aspects specification TS 22.368 [2] represents the MTC server as an entity with which the 3GPP PLMN and the MTC Device directly communicate. This depicts a service delivery representation well, but has very misleading implications if accepted as a basis for the MTC architecture,

Two potential deployment scenarios exist for MTC Services – either under the control of a mobile network operator or by a third party.

To support MTC services deployed by third parties, it is assumed that additional interaction between MTC service logic components and the 3GPP PLMN are required, beyond data communications (SMS and packet domain communication.), These interactions include at least the ability for service logic components to securely interact with the 3GPP PLMN and the ability for the service logic components to obtain certain information regarding MTC Subscriptions and modifying this information (if allowed by the network operator).

Some service logic components only interact with MTC Devices by means of established user plane communication (e.g. SMS or TCP/IP based applications). These service logic components may have no direct means to interact with or become aware of MTC Features. For example, there are existing M2M applications that employ GPRS and/or SMS to communicate with MTC Devices. For such service logic components, no additional mediating interfaces as proposed in this key issue shall be required.

A 3GPP MNO can restrict or deliberately allow access to information, resources and services in the core network by means of the Service Abstraction Layer.

### 5.11.2 Required Functionality

MTC Service Logic components may be deployed within a mobile network operator's control or externally.

The Baseline Architecture in clause 4.3 shall be updated with additional interfaces for secure communications between MTC Service Logic Components and the 3GPP PLMN as well as for MTC Service Logic Components to query or possibly update MTC subscription information.

It is desirable to minimize the requirements for MTC Service Logic components to support 3GPP interfaces and 3GPP-specific configuration. This facilitates the design of MTC services that function over multiple access systems.

## 5.12 Key Issue - Signalling Congestion Control

### 5.12.1 Use Case Description

MTC related signalling congestion and overload is an urgent issue that network operators are currently facing. Not only network operators that are providing MTC services, but also network operators in which MTC Devices are roaming can be affected by MTC related signalling congestion and overload.

MTC related signalling congestion and overload can be caused by:

- a malfunctioning in the MTC application and/or MTC Server.

This cause leads to a congestion situation for which the operator wants to protect its network without affecting other MTC users.

- an external event triggering massive numbers of MTC Devices to attach/connect all at once.

This cause leads to an overload situation for which the operator wants to prevent its network from a complete collapse. As the overload situation relates to abnormal usage from a multitude of applications and customers, a protection mechanism will affect all or a significant number of MTC applications.

- recurring applications that are synchronised to the exact (half/quarter) hour.

This cause leads to a peak load situation for which the operator wants to spread the required capacity over time with the goal of reducing the investment needed to fulfil the required capacity demand.

Though some of the signalling congestion issues could be avoided if MTC applications behave more mobile network operator friendly, there is little a network operator can do to influence the application developers. It is important that the mobile network operator has the capability to control signalling network congestion independent of the application providers.

Signalling network nodes that may suffer from MTC related signalling congestion include all PS domain control plane nodes and gateways. With large scale attach requests, mainly the SGSN/MME is vulnerable. With connection requests, also the SGSN/MME is vulnerable as this node has a relative large load per connection request. GGSNs/PGWs are especially vulnerable as often M2M applications use a dedicated APN which may be terminated at one GGSN/PGW unless DNS and load balancing mechanisms are used. All connection requests for that particular application will then have to be handled by a single GGSN/PGW. MTC devices may concurrently attempt signalling interaction only in a limited area. That means the signalling congestion could occur just at one or several particular signalling links and no overall congestion appears on network nodes.

In order to combat signalling congestion, network nodes shall be able to reject or prevent attach or connection requests. The challenge is to block the traffic of the particular MTC application(s) that is causing the congestion, without restricting non-MTC traffic or traffic from other MTC applications that are not causing a problem. A dedicated APN or a MTC Group Identifier are possible identifiers to indicate particular large scale MTC applications. How to identify applications that are causing recurring signalling congestion (e.g. mail applications, buddy finders, etc) that are often downloaded applications on a smart phone is still a challenge.

Care shall be taken that rejecting connection requests or attach requests does not result in a MTC Device immediately re-initiating the same request. The network should be able to instruct MTC Devices not to initiate a similar request until after a back off time. This back off time may also be used to instruct MTC Devices with recurring applications to change their timing of attach/connection requests.

Care shall be taken that preventing attachment or connection requests by a targeted group of MTC Devices does not immediately or sometime thereafter result in the same group of MTC Devices almost simultaneously attempting signalling or data interactions with the same or different PLMN. Randomization should be applied to spread any resultant network access attempts by the group.

### 5.12.2 Required Functionality

The required functionality depends on the identified congestion and overload situation.

Congestion control provides means to manage the network load from a particular MTC group and/or related to a specific APN. Congestion control requires the following functionalities:

Editor's Note: Further architecture work is required on the MTC Group concept before it is possible to progress solutions depending on MTC Group Identifiers.

- It shall be possible to reduce signalling load (Attach, PDP/PDN Activation, Service Request, …) from MTC devices related to a specific APN or from MTC Devices belonging to a particular MTC Group.

- Congestion control per APN or MTC group shall be possible with a granularity of a single SGSN, MME, GGSN or PGW.

- In order to reduce network load due to congestion situation, it shall be possible for the network to detach MTC devices belonging to a particular MTC Group and/or related to a specific APN and/or deactivate the bearers belonging to a specific APN or to a particular MTC device group.

- In order to avoid network congestion, it shall be possible for the network to prevent MTC devices related to a specific APN and/or belonging to a particular MTC group from too frequent initiation of attach and/or connection requests.

Congestion control shall also be taken with a granularity of a single signalling link between BSC/RNC and SGSN or eNodeB and MME, or a signalling link set which contain all links connecting to a single BSC, RNC, eNodeB, RA or TA(List).

Overload control provides means to manage the network load from all MTC devices independently from other devices. Overload control requires the following functionalities:

- It shall be possible to reduce signalling load caused by MTC Devices independently from signalling load caused by non-MTC devices.

- Overload control shall be possible with a granularity of a single SGSN, MME, GGSN and/or PGW.

- In order to reduce network load due to overload situation, it shall be possible for the network to detach MTC devices selectively and/or deactivate the bearers selectively among APNs or MTC device groups.

- In order to avoid network overload, it shall be possible for the network to prevent MTC Devices from too frequent initiation of attach and/or connection requests.

NOTE 1: It is for further study how it can be prevented that large numbers of devices re-initiate their deferred attach and/or connection requests at (almost) the same time to avoid excessive network congestion.

Peak shaving requires the following functionalities:

- It shall be possible to reduce (quarter/half) hourly signalling peaks from recurring MTC applications

- It shall be possible to spread over time signalling load of requests from all MTC Devices.

NOTE 2: The relation of this key issue with the key issue Time controlled is for further study especially regarding the treatment of MTC devices that are sending/signalling during their assigned time period is FFS.

### 5.12.3 Evaluation

#### 5.12.3.1 General

Editor's Note: The evaluations for this clause were approved distinctly and are complimentary. They are provided without any attempt to merge them.

#### 5.12.3.2 Evaluation for Congestion Control

For congestion control, a combined solution from "Solution - Rejecting connection requests by the SGSN/MME", see clause 6.22, and "Solution - Broadcasting MTC Access Control by RAN", see clause 6.28, provides the most complete, fast and efficient means to manage the network load from a particular MTC group and/or related to a specific APN.

At the immediate onset of a congestion scenario, the first few MTC Devices from the congesting MTC Group/APN requesting RRC and/or NAS access can be rejected assuming there are enough signalling resources available to receive and reject the RRC and/or NAS access requests. To prevent the remaining MTC Device from the congesting MTC Group/APN from sending any access requests during the remainder of the congestion scenario, MTC access barring can be broadcast by the RAN to efficiently bar the specific congesting MTC Group/APN from attempting access. The RRC and/or NAS rejection back-off times and MTC access barring randomization can successful prevent the rejected/barred MTC Devices from almost simultaneously initiating access attempts after the congestion scenario has subsided.

Given this solution is dependent on the implementation of MTC Groups, it does not provide for a low impact on existing 3GPP standards and products and thus is not feasible in Rel‑10.

#### 5.12.3.3 Evaluation for Overload Control

For overload control, a combined solution from "Solution – Rejecting connection requests by the SGSN/MME", see clause 6.22, "Solution - Rejecting RRC Connection and Channel Requests by the eNodeB/RNC/BSS", see clause 6.26, and "Solution - Broadcasting MTC Access Control by RAN", see clause 6.28, provides the most complete, fast and efficient means to manage the network load from all MTC Devices independently from other devices.

At the immediate onset of an overload scenario, the first few MTC Devices requesting RRC and/or NAS access can be rejected assuming there are enough signalling resources available to receive and reject the RRC and/or NAS access requests. To prevent the remaining MTC Device from sending any access requests during the remainder of the overload scenario, MTC access barring can be broadcast by the RAN to efficiently bar all MTC Devices, low-priority MTC Devices, and/or MTC Devices of a PLMN type from attempting access. The RRC and/or NAS rejection back-off times and MTC access barring randomization can successful prevent the rejected/barred MTC Devices from almost simultaneously initiating access attempts after the overload scenario has subsided.

Given this solution is not dependent on the implementation of MTC Groups, it provides for a low impact on existing 3GPP standards and products that may be feasible in Rel‑10.

#### 5.12.3.4 Comparison of Each Solution

The pros and cons of each solution are as follows.

1. Access Control by the RAN (eNB/RNC/BSS) as per 6.28.

a. Pros :

There is no wasted signalling with the MTC devices

It can be used for controlling the overload of the RAN node and also for the CN node with the extension of the S1AP: Overload Start and Stop message.

b. Cons:

For applying the barring with the finer granularity such as per group, the more information should be broadcasted in the system information.

NOTE 1: The randomized barring computed as T303= (0.7+ 0.6 \* rand) \* ac-BarringTime may decrease the possibility that a large number of MTC devices simultaneously access the network. But the possibility still exists. Due to this possibility, we may need to enhance the current RACH mechanism that limits the number of the UE identifying the opportunities at the same time. For the other two solutions, it is also required to enhance the current RACH mechanism.

2. Rejecting RRC connection and channel requests by the eNB/RNC/BSS as per 6.26.

a. Pros:

This solution wastes the smaller number of signals than rejecting the request by the SGSN/MME.

b. Cons:

It is possible to use the solution for finer granularity control, such as per group. But, per group, the group ID should be included and then the RRC message; that is, including the group ID in the RRC connection setup complete rather than the RRC connection request. This is needed because the RRC connection request message is sent using CCCH before the dedicated control channel to the UE. Hence, for the finer granularity control, more signals (Precisely, RRC connection request, RRC connection setup, RRC Connection Setup complete) are wasted.

NOTE 2: When a low priority cause value in the RRC connection request is used as the low priority MTC device indicator, the network may experience confusion in deciding the policy for the low priority normal UE and the low priority MTC device. The details of the argument is in S2-103122.

3. Rejecting connection requests by the SGSN/MME as per 6.22 (and S2-103120 for Mobile Terminated communication.)

a. Pros:

The mechanism can be implemented without any change on the RAN node.

The SGSN/MME can consider various conditions (such as roaming restriction, group, APN etc.) in order to determine whether to accept or reject the request from the MTC device.

b. Cons:

Before the SGSN/MME receives the NAS message from the MTC device, the network and the MTC device exchange the many signals (RRC signals for connection establishment, S1AP/RNANP message from the RAN to the SGSN/MME.) All these exchanged signals may be wasted just for rejecting the request from the MTC device.

Congestion/overload control solutions proposed so far describe mechanisms that start to block signalling traffic or transactions when the system load reaches certain thresholds. There are three basic solutions:

- Broadcast based solutions that prevent any access from MTC (or low priority) devices, and

- reject based solutions that imply some MTC device individual signalling. The reject based solution may be further categorised into:

- Reject by RAN, and

- Reject by CN nodes.

Table 5.12.3.4-1 collects pros and cons for the three solution alternatives: broadcast based, reject by RAN and reject by SGSN/MME. The reject by GGSN/PGW can be considered as covered by the reject by SGSN as the functionality is similar and the rejection to the MTC device is finally the SGSN/MME may need to send.

Table 5.12.3.4-1: Pros and Cons for the three solution alternatives

|  |  |  |  |
| --- | --- | --- | --- |
|  | Broadcast control | Reject by RAN | Reject by SGSN/MME |
| pros | Reduces load without any signalling with the device.  It is the only solution that allows for preventing any signalling from MTC devices.  Also suitable for cell/RAN node overload control. | Reduces load by rejecting already the first RRC message of the device (assuming proper criteria are available with first RRC message, like the proposed "low priority" indication).  Also suitable for cell/RAN node overload control. RAN node can quickly start to reduce load by rejection.  Suited for SGSN/MME MTC load control on higher granularity as RAN based reject can be started by SGSN/MME, e.g. as specified for MME overload.  Load control granularity per SGSN/MME, per shared PLMN and also per low/high priority is possible. | Reduces load by rejecting NAS requests (MM or SM) of the device (ideally rejecting already the first message when proper criteria are available)  SGSN/MME can have group/APN information, and therefore suited for controlling load with group/APN granularity.  Load control granularity per certain PLMN or roaming conditions and also per low/high priority are also possible, specifically when it can be derived from already existing signalling. |
| cons | Reacts slower on load than reject solutions as it depends on frequency of sending and reading the control information. (How slow in absolute figures?)  Less suited for reducing load per group/APN or per CN node as extensive broadcast information seems needed to indicate a group/APN. | Less suited for reducing load per group/APN.  Requires device individual RRC signalling.  Some interference with NAS timers and repetitions might occur when the proposed long wait timers are longer than the NAS timers. | Requires certain amount of device individual signalling: first RRC setup needs to be performed and at least some initial NAS signalling before the SGSN/MME can reject.  Without further enhancements the SGSN/MME needs more signalling before it can reject an attach, e.g. get subscriber data from HSS, to know the group/APN of the device. |
| others | Additional mechanism may be needed to avoid that all devices start immediately when the broadcast indication changes to allow access. | Some new identity handling is proposed (e.g. indicate IMSI when re-selecting PLMN) to provide specific criteria fro deciding on reject.  RNC could also reject based on establishment cause, e.g. "background traffic". | NAS/MM (e.g. attach) may need extensions to allow for rejecting already first NAS message  Some delay/wait mechanism is needed in addition (e.g. the proposed back-off timer) to prevent frequent retry from device  If SGSN/MME stores all MM contexts from MTC devices after detach then the SGSN/MME may have sufficient information to reject group/APN based already with initial NAS message. |

The only safe method to block MTC signalling load without impacting other traffic is the broadcast mechanism. As it is hard to predict whether reject mechanisms alone would be able to manage all potential situations it seems useful to adopt a broadcast solution. The granularity would be rather high so that some reject solution may be needed in addition to perform a more fine granular control.

Broadcast control granularity could be all MTC or with some high granularity it could prevent access from devices that change PLMN. Allowing access again may cause many devices to access at the same time. Some load distribution mechanism may be needed in addition.

The adoption of a reject mechanism in addition to a broadcast mechanism seems useful for more fine granular load control. As the RAN reject seems not suited to control based on group/APN the SGSN/MME based rejection may be used in addition to it. Also here some wait time is needed before the UE is allowed to retry.

However, as the eNodeB reject mechanism exists already it may be enhanced with reasonable effort to reduce an MME's MTC load. The MME could request the eNodeB to reject MTC devices before it request to reject all UEs besides emergency services. Applying this mechanism for GERAN/UTRAN may need further study.

## 5.13 Key Issue - MTC Identifiers

### 5.13.1 Use Case Description

The amount of MTC Devices is expected to become 2 orders of magnitude higher than the amount of devices for human to human communication scenarios. This has to be taken into account for IMSI, IMEI and MSISDN. Regulatory bodies indicate shortages of IMSIs and MSISDNs.

The MTC Feature PS Only in 22.368 includes a requirement that PS Only subscriptions shall be possible without an MSISDN. In principle an MSISDN is not used in any of the PS based signalling procedures. However, it will have to be assured that all PS procedures indeed work and subscriptions can be uniquely identified without providing an MSISDN. Furthermore, 22.368 specifies that remote MTC Device configuration shall be supported for PS only subscriptions without an MSDISDN assigned. Current remote MTC Device configuration solutions (i.e. Device Management and Over-the-Air configuration) are based on SMS, which assumes the use of MSISDNs. So a solution to support remote MTC Device configuration that does not require the use of MSISDNs is needed.

An MTC Group is a group of MTC Devices that share one or more Group Based MTC Features and which belong to the same MTC Subscriber. A so-called MTC Group identifier uniquely identifies such a group across 3GPP networks.

### 5.13.2 Required Functionality

- It shall be possible to uniquely identify the ME.

NOTE 1: This requirement relates to the ME which is generally identified by the IMEI.

- It shall be possible to uniquely identify the MTC Subscription

NOTE 2: The two requirements above also apply to human-to-human communications. However, for Machine-Type Communication identifiers will have to be able to cater for a number of identifiers up to two orders of magnitude higher than for human-to-human communications.

- A network operator shall be able to provide PS only subscription without the need to assigning an unique MSISDN per device or subscription.

- If no (unique or common) MSISDN is assigned to a PS only subscription, the IMSI shall be used as charging identifier.

- Remote MTC Device configuration shall still be supported for subscriptions without an MSISDN.

NOTE 3: Current remote MTC Device configuration solutions (i.e. Device Management and Over-the-Air configuration) are based on SMS, which assumes the use of MSISDNs.

- If a solution is selected that allows the IMSI to be used on the external interface to the MTC Server, security measures shall be applied on the external interfaces to avoid eavesdropping of the device identifier.

- MTC Group shall be identified uniquely across 3GPP networks.

### 5.13.3 Evaluation

## 5.14 Key Issue - Potential overload issues caused by Roaming MTC devices

### 5.14.1 Use Case Description

#### 5.14.1.1 What is the likelihood of M2M devices being roamers?

In many cases (possibly the vast majority of cases) M2M devices will be used as part of a contract between one network operator (or network operator group with operations in multiple countries) and a large (possibly multi-national) company.

***Coverage:***

One of the key aspects that the operator will "sell" to the corporate customer is coverage. The use of "national roaming" obviously improves geographic coverage, but, its utilisation poses several challenges. An obvious solution to some of these national roaming challenges is for the operator to use "international roaming", either with a SIM from a different company within the same operator group, or, by using a SIM with "non-geographic" Mobile Country Code (e.g. MCC 901).

Both of these options appear to already be in use, and are likely to be used widely in the future.

***Multi-national customer:***

Typically a multi-national customer will want to be delivered devices and choose in which country they are used. This inevitably leads to 'roaming' for their M2M devices.

This situation is exacerbated by the use of factory "pre-fitted" SIMs.

***Chance of Roaming Summary:***

Overall, for devices sending low data volumes, there seem to be some strong reasons to expect most devices to be camped on a PLMN that is different to their IMSI's PLMN-ID, i.e. it may be that MOST M2M devices ARE ROAMING.

#### 5.14.1.2 What are the consequences if most M2M devices are roaming?

##### 5.14.1.2.1 Commercial arrangements

Currently, most roaming agreements seem to implicitly assume some degree of balance/mutual benefit between the two operators.

However, the subscribers of a network with a non-geographic Mobile Country Code are "all outbound roamers". And, the outbound roaming M2M devices are likely to generate very little traffic per device but still generate 'normal' levels of signalling and occupy 'normal' levels of VLR space. This "imbalance" might lead to the VPLMN operator being "unhappy".

At the moment the only 3GPP-standards consequence of this would seem to be, that, we should ensure that the VPLMN has sufficient counters and capabilities to measure the level of "imbalance".

##### 5.14.1.2.2 Devices that only power‑up/attach when they need to do something

If the M2M devices with foreign SIMs are normally not-attached to the network, then the VPLMN may only discover that these devices are in its territory when an event happens that causes the device to report back to the "MTC server".

If a large set of such devices get activated by the same event (e.g. burglar alarms with foreign SIMs responding to a power cut or earthquake) then the VPLMN may suddenly get loaded by huge numbers of M2M devices: yet, potentially, the VPLMN would have been totally unaware of the existence of (millions of) these devices.

Without prior knowledge of the number of inactive devices in the geographic area, network capacity planning is close to impossible.

Such scenarios lead to the need for a VPLMN to be able to "survive" a potentially massive increase in unplanned /unpredicted signalling load.

Some "tools" in the 3GPP standards may be needed to help manage this scenario.

##### 5.14.1.2.3 Failure of "M2M partner" network

It is likely that many M2M "roaming" devices will be using the network of a PLMN within the same operator group, but not necessarily the same operator within a certain country.

For example, "OperatorX UK" might have a contract to supply 5 million electricity meters in the South of England. To 'enhance' their coverage area, they could equip them with SIM cards from their partner network "OperatorX in country A".

But what then happens if the "OperatorX UK" network fails? These devices will NOT have "OperatorY UK" as a forbidden PLMN and so, when their periodic update fails, they are likely to change network, and, over a potentially fairly short time period, up to 5 million new devices appear on the "OperatorY UK" network.

Again, we need "tools" in the 3GPP standards to permit networks to "survive" these situations.

### 5.14.2 Required Functionality

Tools are required to protect a VPLMN from any overload caused by the failure of one (or more) other networks in that country. However, it should be noted that a degree of co-operation from the HPLMN is still likely to be required.

The following tools needed to be ***investigated*** further:

a) counters/alarms (on e.g. a per MCC and MNC basis) to detect unusual increases in the number of roaming devices in a VPLMN;

b) the ability to remotely configure M2M devices to indicate that they are "low value" M2M devices;

c) signalling from the UE to the RAN to permit the IDNNS function in the RAN to steer "low value" M2M devices towards Core Network nodes with large VLR/storage capacity and/or large processing capacity, especially in the CS domain;

d) "access class barring" functionality that can be used to bar e.g.:

- low value" M2M devices that are not on their HPLMN or a PLMN in the (U)SIM's preferred PLMNs list;

- low value" M2M devices that are not on their HPLMN or an Equivalent HPLMN;

- low value" M2M devices that are not on their HPLMN;

- low value" M2M devices;

e) control of the "more preferred PLMN background search timer" so that M2M devices do not return too rapidly to a failed PLMN, and/or do not scroll through multiple different PLMNs in that country;

f) minimising M2M device to network signalling at inter-PLMN change, e.g. by using Attach rather than RAU/TAU and using IMSI rather than a temporary ID;

g) slowing down the rate at which "low value" M2M devices detect network failure, e.g. by having mechanisms to give "low value" M2M devices relatively long CS and PS domain periodic update timers;

h) modifications to the existing specification of how the M2M device reacts to some MM/GMM/EMM reject cause values such as "IMSI unknown in HLR"; "illegal ME"; and "PLMN not allowed";

i) inclusion of a "low value" M2M device indicator in the M2M device to RAN signalling to permit the RAN to provide special handling to such devices in times of congestion (e.g. by rejecting them with a back off time);

j) inclusion of a "low value" M2M device indicator in the M2M device to Core Network signalling to permit the CN to provide special handling to subsets of such devices in times of congestion (e.g. by checking the IMSI and/or APN and/or MTC group ID and rejecting certain groups with a back off time);

k) specification of new MM/GMM/EMM functionality (e.g. reject cause values or "abuse" of the Accept message) that causes new UE behaviour (e.g. a cause value that says "LA not allowed, but stay in this LA for X deci-hours before searching for another PLMN", or, sending RAU accept with a 20 minute PRU timer value and locally loading a "no services permitted" subscription into the SGSN's database);

l) modification of signalling to/from the EIR to permit the EIR e.g. to allow rejection/parking of an M2M device without overloading the inter-operator signalling links;

m) the specification of a new Network Mode of Operation that permits the VPLMN to offer NMO=II to their existing devices while minimising signalling from "low value" M2M devices by getting those M2M devices to use NMO=I.

### 5.14.3 Evaluation

#### 5.14.3.1 Evaluation for M2M "access class barring" functionality

The "PLMN type" option from "Solution - Broadcasting MTC Access Control by RAN", see clause 6.28, defines the required mechanisms for barring MTC Devices based on their current PLMN type (e.g. not in HPLMN, PLMN in the (U)SIM's preferred PLMNs list, Equivalent HPLMN, etc). Given this solution is not dependent on the implementation of MTC Groups and can use a very efficient encoding of the PLMN type to take advantage of spare bits in pre-existing system information messages, it provides for a low impact on existing 3GPP standards and products that may be feasible in Rel-10.

NOTE: The detailed "PLMN type" indication parameters should be specified in stage 3.

Editor's note: Text to be added for remaining functionality requirements

## 5.15 Key Issue - Low Power Consumption

### 5.15.1 Use case description

For some types of MTC Devices, operation with very low power consumption is a critical requirement. For some devices, such as those used for gas metering and animal, cargo, prisoner, elderly and children tracking, low power consumption is critical because it is not easy to re-charge or replace the battery, This creates the need for system enhancements that would minimize the power consumption of MTC Devices.

### 5.15.2 Required Functionality

It shall be possible to save battery energy consumption for UEs.

### 5.15.3 Evaluation

# 6 Solutions

Editor's Note: Solutions to all Key Issues are listed here. Under Problem Solved / Gains Provided, please list the Key Issue(s) that are addressed by the solution.

## 6.1 Solution - FQDN Identifier Solution

### 6.1.1 Problem Solved / Gains Provided

See Key Issue 5.2 "MTC Devices communicating with one or more MTC Servers".

### 6.1.2 General

MTC devices relying on IP communications that need to be reachable for mobile terminated communications are assigned a static unique "host name" (i.e. an FQDN identifier specific to the MTC device). The "host name" is assigned in addition to any EPS-level identity (such as IMSI or MSISDN) of the MTC device.

NOTE 1: The "host name" may be defined via the EPS-level identity. For instance, assuming that the MTC device has an IMSI as the EPS-level identity, the "host name" can be defined as "mtc.IMSI.pub.3gppnetworks.org". The exact definition of the "host name" is a Stage 3 matter.

The "host name" is used as the primary addressing identifier for mobile terminating communications.

Upon attachment to the PLMN the MTC device that relies on IP communications is assigned dynamic IP address. In roaming scenarios the dynamic IP address may be assigned in the Visited PLMN.

The association between the "host name" and the dynamically assigned IP address is stored in the authoritative DNS server in the Home PLMN.

When the MTC device is assigned a dynamic IP address, the authoritative DNS server is kept up-to-date using DNS Update mechanisms.

The entity performing DNS updates is preferably located in the Home PLMN in order to reduce the number of trusted interfaces to the DNS server.

The call flow depicted in Figure 6.1.2-1 describes how MT communication with MTC devices inside public IP address space works in step by step fashion:



Figure 6.1.2-1: Call flow for MT communication with MTC device inside public IP address space

1. MTC device performs the EPS Attach procedure as described in TS 23.401. As part of the EPS Attach procedure the MTC device is assigned a public IP address, referred to here shortly as "D". The S5/S8/S11 Create Session Response message (not shown) is used to convey "D" from the PGW to the MME.

NOTE 2: For IPv6 it is assumed that the MTC device relies on DHCPv6 for stateful address allocation.

2. As part of the previous step, or at the end of the EPS Attach procedure, the MME notifies the HSS/AAA with "D". Currently there is no direct interface between the PGW and the HSS/AAA, which is why the Notification is sent from the MME.

NOTE 3: If an interface between the PGW and the HSS/AAA is defined in the future, the MTC device’s IP address “D” can be notified directly without passing through the MME.

3. The association between the “host name” of the MTC device and the dynamically assigned IP address “D” is stored in the authoritative DNS server in the Home PLMN. The HSS/AAA sends a DNS Update to the authoritative DNS server.

4. At some point the MTC server wishes to send a Mobile terminated (MT) message to the MTC device whose unique identifier is FQDN.

5. MTC server sends a DNS query that eventually reaches the authoritative DNS server.

6. The DNS response of the authoritative DNS server includes "D".

7. MTC server sets the Destination IP address in the packet it wishes to send to the MTC device to “D”.

8. The PGW hosting the MTC device's public IP address delivers the packet to the MTC device via an appropriate EPS bearer.

The proposed solution also applies to GERAN and UTRAN devices, in which case MME and PGW are replaced with SGSN and GGSN.

It also applies to MTC device-to-device communications, where both MTC devices are located inside public IP address space. In this case it is the source MTC device itself that performs the DNS query to resolve the FQDN of the target MTC device.

Editor's note: If the MTC device has multiple PDN connections, it is FFS which IP address the MTC Server selects for sending packets to the MTC device.

NOTE 4: Further details on mobile terminated communications to MTC devices inside a private Ipv4 address space are described as a separate key issue, see clause 5.3 "IPv4 Addressing."

### 6.1.3 Impacts on existing nodes or functionality

For IP address assignment via DHCPv4, the PGW needs to notify the SGSN/MME of the assigned IPv4 address outside of the Attach procedure (e.g. via the Bearer Modification procedure).

SGSN/MME needs to notify the HSS of the device’s IP address “D” (e.g. new parameter in the Notify Request message).

HSS need to perform DNS updates of the authoritative DNS server that stores the association between the “host name” of the MTC device and the dynamically assigned IP address “D”.

### 6.1.4 Evaluation

Benefits:

- Low impact on existing Core Network nodes;

- Generic IP-level solution that does not rely on application-level identifiers (e.g. SIP URI);

- Works in all scenarios (non-roaming, roaming with home routed traffic, roaming with local breakout);

- The solution does not rely on alternative communication channels (e.g. SMS) for delivery of a “push” stimulus;

- Works also for device-to-device communication;

- Compatible with the solution for Mobile Terminated communication into private IPv4 address space (refer to clause 6.18).

Drawbacks:

- For IPv6 the solution requires stateful address configuration via DHCPv6.

## 6.2 Solution - Transfer data via SMS

### 6.2.1 Problem Solved / Gains Provided

See clause 5.4 "Key Issue – Online Small Data Transfer".

### 6.2.2 General

MTC Devices with low data usage send or receive data utilizing SMS via SGSN/MSC or SMS over SGs. The MTC Server connects with the SM-SC or behaves as a SM-SC (e.g. has an integrated SM-SC) to send or receive MTC service data encapsulated in short message. SMS transfer is suited for MTC users that infrequently transfer amounts of data that can be carried by SMS(s) and where SMS transfer generates less system load compared to the usage of packet data bearers.

Editor's Note: The impact of storing and forwarding nature of SMS delivery on MTC service is FFS.

The SGSN/MME is aware that the MTC Device has the low data usage feature (e.g. the usage of that feature is known from the HLR/HSS subscription data). The MME and MTC Device will not create any EPS bearer for MTC service.

Editor's Note: In Rel-9 EPC and E-UTRAN it is not possible to connect to the network without establishing at least the default EPS bearer. The impact on EPC and E-UTRAN needs further study.

### 6.2.3 Impacts on existing nodes or functionality

### 6.2.4 Evaluation

## 6.3 Solution - Paging within configured area

### 6.3.1 Problem Solved / Gains Provided

See clause 5.6 "Key Issue – Low Mobility".

### 6.3.2 General

For MTC devices that do not move frequently or move only within a small area, the paging area (e.g. TAI, CGI, ECGI) is configured in the HLR/HSS as a part of the subscription of the MTC subscriber. The SGSN/MME stores the paging area as part of the subscriber data as received from HLR/HSS.

During the mobile terminated service, the SGSN/MME pages the MTC Device within the specific area. The configured paging area is assumed to be smaller than typical paging areas for other UEs. Thereby paging traffic can be reduced.

An issue might be needed for reconfiguring subscription data when the network reconfigures some cells or the MTC Device is roaming.

### 6.3.3 Impacts on existing nodes or functionality

### 6.3.4 Evaluation

## 6.4 Solution - Paging stepwise

### 6.4.1 Problem Solved / Gains Provided

See clause 5.6 "Key Issue – Low Mobility".

### 6.4.2 General

For the MTC Device with low mobility, the SGSN/MME stores the RAI/TAI(s) like for any other UE and in addition the last known cell (i.e. CGI/ECGI) or last known service area (i.e. SAI) as provided by RAN in S1/Iu/Gb signalling. For low mobility MTC devices the MME preferentially includes only one TAI for TAI List in the accept message.

During the mobile terminated service, the SGSN/MME may page stepwise, e.g. first in the last known cell (i.e. CGI/ECGI) or last known service area (i.e. SAI) and if there is no response the SGSN/MME pages the MTC Device in a wider area, i.e. within the RAI or TAI List allocated to the MTC Device.

### 6.4.3 Impacts on existing nodes or functionality

### 6.4.4 Evaluation

## 6.5 Solution - Paging within reported area

### 6.5.1 Problem Solved / Gains Provided

See clause 5.6 "Key Issue – Low Mobility".

### 6.5.2 General

For the MTC Device with fixed location (i.e. not move normally), which can be deduced by the SGSN/MME when receiving the same area identifier (e.g. CGI, ECGI, SAI, RAI or TAI) via S1/Iu/Gb signalling during a predefined period or receiving a explicit report from the MTC Device. The SGSN/MME stores the area identifier and pages the MTC Device within the specific area.

When the MTC Device moves (e.g. for maintain purpose), the SGSN/MME detects the moving and pages within the new area which is reported by RAN or by the MTC Device explicitly.

### 6.5.3 Impacts on existing nodes or functionality

### 6.5.4 Evaluation

## 6.6 Solution - Triggering of non-attached MTC Devices based on location information provided by MTC User

### 6.6.1 Problem Solved / Gains Provided

See clause 5.8 "Key Issue - MTC Device Trigger".

### 6.6.2 General

With non-attached MTC Devices, the network has no knowledge of the location of the MTC Device. However, in many cases the MTC User does have knowledge about the location of the MTC Device. In these cases the MTC User can provide the PLMN with information on the location of the MTC Device. Based on that information the PLMN can then broadcast a trigger message in a relevant cell or group of cells. The MTC Device, while not attached, will still listen to the broadcast channel of the PLMN.

A possible solution to broadcast the triggers may be by using the Cell Broadcast Service (CBS) as specified in TS 23.041. A Cell Broadcast Center (CBC) is under control of a mobile network operator and connected to the radio network i.e. to the BSCs in case of GSM and to the RNCs in case of UMTS. Connected to a CBC are one or more Cell Broadcast Entities (CBEs) which may originate CBS messages. A mobile network operator may make available the interface on the CBC to trusted 3rd parties to interconnect their CBE to the CBC of the mobile network operator. The MTC Devices are programmed to monitor a preset CB channel(s), even when they are not attached to the network, and have assigned a Unique Paging Identity (UPID). This way the MTC Server of the 3rd party is able to send CBS messages, including one or more UPIDs, to its MTC Devices in certain areas based on location information available in the MTC Server. But also other broadcast solutions (such as using the BCCH) can be considered to trigger the MTC Devices that are not attached to the network to attach and establish PDP/PDN connectivity. Solutions to reduce the amount of trigger request and trigger response messages to be transmitted through these broadcast solutions shall also be considered together.

### 6.6.3 Impacts on existing nodes or functionality

### 6.6.4 Evaluation

## 6.7 Solution – Network access control by the PLMN

### 6.7.1 Problem Solved / Gains Provided

See clause 5.9 "Key Issue - Time Controlled"; clause 5.12, "Key Issue - Signalling Congestion Control".

### 6.7.2 General

The 3GPP network supports policing of the MTC Device's access to the network to prevent or allow (e.g. with specific charging) traffic to/from the network during unauthorized time periods. This may be accomplished as follows:

i) the operator provisions the access duration, grant time interval and forbidden time interval within the MTC subscription in the HLR/HSS;

ii) the SGSN/MME receives the access duration, grant time interval and forbidden time interval periods from the HLR/HSS during the Attachment, Routing Area Update or Tracking Area Update procedure;

iii) the SGSN/MME alters the grant time interval periods for MTC devices base on the value received from HLR/HSS or local operator policies, e.g. due to locally determined congestion overload conditions;

a. SGSN/MME randomly determines a communication window within the grant time interval to improve uniform utilization of the network and reduce the chance of overload at the beginning or end of the grant time interval

b. The length of the communication window shall not be less than the Access Duration agreed between the MTC Subscriber and network operator, though it could be longer.

iv) The SGSN/MME provides the communication window to the GGSN/P-GW, e.g. for the purpose of specific charging rate, or stopping data transmission when outside of the authorized time period.

v) the SGSN/MME police the MTC Device's access to the network to prevent or allow (e.g. with specific charging) traffic to/from the network outside of the communication window. In the former case, the SGSN/MME reject the access request message (e.g. Attach Request or Tracking Area Update Request) or Service Requests initiated by the MTC device outside of the communication window. In all cases, the SGSN/MME indicates the communication window to the MTC device in the accept or reject message.

Editor's Note: It is FFS whether the network detaches MTC devices which remain attached to the network when the communication windowexpires.

Editors Note: It is FFS whether the network should let MTC Devices attach to the network outside of the communication window, but reject session management requests (e.g. Activate PDP Context Request in GPRS).

The network may inform the MTC Devices of the communication window as follows:

i) the network provides the communication window to the MTC Server; the MTC Server distributes them to the MTC Devices via application level data; this approach has however the following drawbacks:

- a modification of the communication window may generate important signalling/traffic between the MTC Server and a possibly significant number of MTC Devices;

- MTC Devices' accesses to the network may be rejected or unduly charged until the MTC Server communicates them the communication window in-use in the Mobile Network.

Or

ii) the SGSN/MME provides the communication window directly to the MTC Devices via NAS signalling, e.g. the first time the MTC Device registers to the network, and upon subsequent NAS signalling from the MTC Device if the communication window has changed. Following an operator's update of the communication window, the MTC Device might initiate NAS signalling outside of the new communication window. In that case, the network may either:

- reject the MTC Device request and return the new communication window in the response; or accept the first access outside of the new communication window and provide at that time the new communication window for subsequent accesses. E.g. the MME/SGSN could store both the 'Time-Intervals In-Use' (i.e. the last time intervals communicated to the MTC Device) and the 'Subscribed Time-Intervals' received from the HLR/HSS, and accept the first access of the MTC Device during the 'Time-Intervals In-Use'.

In all cases where a communication window is supplied to the MTC Device, a timestamp is also provided to aid in synchronization.

### 6.7.3 Impacts on existing nodes or functionality

The HLR/HSS need to support provisioning of authorized time periods (i.e. access duration, grant time interval and forbidden time interval) in MTC subscriptions.

The SGSN/MME needs to determine the communication window and grant time interval for MTC devices based on the value received from the HLR/HSS randomization or the local operator policies, e.g. due to locally determined congestion or overload conditions.

The SGSN/MME needs to police the MTC Device's access to the network according to the authorized time periods.

The SGSN/MME needs to provide the MTC Devices with the communication window and timestamp information in NAS signalling (if NAS signalling is used to inform MTC Devices of the communication window).

The SGSN/MME needs to store both the new and last communication window. The SGSN/MME uses both the last and new communication windows to authorize the MTC device access to the network (e.g. reject or accept access request of the MTC Device) until the MTC device is updated with the new communication window.

MTC Devices need to store the communication window and check the stored communication window before accessing the network.

NOTE: This implies some time management and possibly buffering in the MTC Device to defer\* the sending of application traffic until the next authorized time period.

Editor's Note: PGW impact is still FFS. If some information needs to be transferred to PGW from MME/SGW, the information is expected to be sent using GTP if S5/S8-GTP is used, or using PCC infrastructure if S5/S8-PMIP is used.

### 6.7.4 Evaluation

Network Access control by the PLMN satisfies all requirements listed in clause 5.9.2. The access duration, grant time interval and forbidden interval are taken into consideration. Randomization occurs for access to prevent non-uniform utilization of the network and peaks in traffic. The VPLMN policy can be accommodated by means of applying local policy at the serving SGSN or MME. Use of the network can be enforced as required, either by detaching the MTC Device, refusing to allow it to attach or surcharging it, outside of the authorized time period.

This solution introduces some complexity in that the MTC Device and the network must agree to time periods allowed for communication. This synchronization should not be needed in the ordinary case, as the communication window is retained by both the MTC Device and the network and can be reused.

## 6.8 Solution - Introduction of a 3GPP MTC Service Abstraction Layer

### 6.8.1 Problem Solved / Gains Provided

See clause 5.11 "Key Issue – Decoupling the MTC Server from 3GPP Architecture".

### 6.8.2 General

**A) Add additional terminology to clause 3.1:**

**MTC Service Logic Components**: Business logic, configuration, data and other elements that implement an MTC Application and provide service to the MTC User. MTC Service Logic Components communicate with MTC Devices and may be deployed under or external to mobile network operator control.

**3GPP MTC Service Abstraction Layer**: A functional entity that shares reference points with network elements in the 3GPP PLMN that are specified by 3GPP. The Service Abstraction Layer also exposes interfaces to PDNs to allow Service Logic Components to communicate with MTC Devices and services offered by mobile network operators to support interaction with MTC Devices.

**B) Modify clause 4.3 Architecture Baseline, as follows:**

The end to end application, between the MTC device and the MTC server, uses services provided by the 3GPP system. The 3GPP system provides transport and communication services (including 3GPP bearer services, IMS and SMS) optimized for the Machine-Type Communication. For the purposes of 3GPP standardization, the MTC Server - including its internal state, operations and interfaces remain out of scope.

As shown in Figure 4.3.1, MTC Device connects to the 3GPP network (UTRAN, E-UTRAN, GERAN, etc) via MTCu interface. MTC Device communicates with MTC Service Logic Components by means of an MTC Service Abstraction Layer or other MTC Devices using MTC Functions, 3GPP bearer services, SMS and IMS Application Servers provided by the PLMN. The MTC Server is an entity which connects to the 3GPP network via a Generic Service Layer API which remains out of scope of 3GPP standardisation. The MTC Service Abstraction Layer separates the MTC Service Logic Components from access specific interfaces. The MTC Service Abstraction Layer presents generic capabilities that map to concrete ones offered by the specific access. For example, communication capabilities in the 3GPP access are supplied using the MTCi/MTCsms interfaces and thus communicates with MTC Devices. MTC Server Logic Components may be outside of the operator domain or inside an operator domain.



Figure 4.3-1: MTC Service Abstraction architecture

The reference points are listed as below:

**MTCu**: It provides MTC Devices access to 3GPP network for the transport of user plane and control plane traffic. MTCu interface could be based on Uu, Um, Ww and LTE-Uu interface.

**MTCi**: It is the reference point that MTC Server uses to connect the 3GPP network and thus communicates with MTC Device via 3GPP bearer services/IMS. MTCi could be based on Gi, Sgi, and Wi interface.

**MTCsms**: It is the reference point MTC Server uses to connect the 3GPP network and thus communicates with MTC Device via 3GPP SMS.

NOTE: Both MTCi and MTCsms may be defined in such a way as to traverse the Service Abstraction Layer transparently.

**MTCsh:** It provides transport of service-related data (opaque to the 3GPP system) as well as user / subscriber related data. This reference point may be based upon Sh.

Additional reference points between the 3GPP PLMN and the 3GPP MTC Service Abstraction Layer (e.g. for IMS) are FFS.

It is FFS whether the 3GPP MTC service abstraction layer applies to pre-release 8 3GPP core networks and I-WLAN.

### 6.8.3 Impacts on existing nodes or functionality

### 6.8.4 Evaluation

## 6.9 Solution - MTC Monitoring - General

### 6.9.1 Problem Solved / Gains Provided

See clause 5.10 "Key Issue – MTC Monitoring".

### 6.9.2 General

The MTC Monitoring events are configured in the HLR/HSS as part of the MTC subscription. The related criteria (e.g. the mapped IMSI/IMEI or the allowed location area) for reporting purpose are configured together with the event as well unless the event type is self explanatory, e.g., loss of connectivity. For those configured MTC Monitoring events, default action can be predefined as well, e.g. detaching the MTC Device when the IMEI and IMSI are not mapped.

According to the requirement, the following MTC Monitoring events shall be configured in the HLR/HSS:

1. Monitoring the association of the MTC Device and UICC.

In this case, the HLR/HSS shall also configure the mapped IMSI and IMEI as the criteria together with this event.

2. Monitoring the alignment of the MTC feature.

In this case, the activated MTC features and the expected behavior for the special MTC Device, which is configured in the HLR/HSS as part of the MTC subscription, apply for this monitoring event.

3. Monitoring change in the point of attachment.

In this case, the allowed location information may also need to be configured as the criteria in the HLR/HSS (e.g. the Low Mobility feature is also activated for the MTC Device).

4. Monitoring loss of connectivity.

The network shall be able to detect such configured MTC monitoring events. The following alternatives (i.e. solution 1 to solution 3) can be used for the detecting purpose. The alternatives (solution 6.24 to solution 6.25) can be used for the MTC Event Reporting entity to get the MTC Server identity.

Editor's Note: It is FFS whether other alternatives can be used for the event detecting purpose.

Editor's Note: It is FFS whether MTC Device can be used for assisting in MTC monitoring.

When such event is detected, the network shall be able to report to the MTC Server and/or MTC User. The following alternatives (solution 4 to solution 7) can be used for the reporting purpose.

Editor's Note: It is FFS for whether other alternatives can be used for the reporting purpose.

When any event is detected, the network may also trigger MTC Monitoring actions accordingly, i.e. reduce services provided to the MTC Device or restrict access of the MTC Device or detach the MTC Device completely. When default action is predefined in the MTC subscription, the network triggers the default action (s). Dynamic action indication from the MTC server/user is not supported.

When the MTC monitoring action "reduce services provided to the MTC device" is triggered, the SGSN initiates the PDP Context Modification procedure or the MME initiates the Modify Bearer Command to the Serving GW with included modified QoS parameters for the reduced service.

When the MTC monitoring action "restrict access of the MTC Device" is triggered, in order to restrict the access of an MTC Device in idle mode, the SGSN rejects based on access restriction the Routing Area Update procedure or the MME rejects based on access restriction the Tracking Area Update procedure initiated by the MTC device. In order to restrict the access of an MTC Device in active mode, the SGSN or MME informs the RAN about the access restriction during the attach procedure or TAU/RAU procedure (the allowed location). The RAN restricts the handover only to allowed locations.

When the MTC monitoring action "detach the MTC Device" is triggered, the SGSN or MME initiates the Detach procedure.

Editor's Note: How to handle the roaming scenario for this monitoring key issue is FFS.

Editor's Note: How to guarantee a MTC Monitoring action will not restrict network access to the MTC Device in a way that prevents the network or MTC Server to update the MTC Device to resolve the issue that triggered the MTC Monitoring action is FFS.

## 6.10 Solution – SGSN/MME based detection

### 6.10.1 Problem Solved / Gains Provided

See clause 5.10 "Key Issue - MTC Monitoring" and 6.9 "Solution - MTC Monitoring - General".

### 6.10.2 General

For this solution, the SGSN/MME is responsible for detecting monitoring event, so the configured MTC monitoring events along with the related criteria and default action are downloaded from the HLR/HSS to the SGSN/MME during the Insert Subscription procedure along with the MTC subscription e.g. during Attach procedure.

Basically, the SGSN/MME monitors the MTC Device behavior according to the MTC monitoring event trigger and performs corresponding action. The following table shows the procedures of the SGSN/MME.

Table 6.10.2-1: SGSN/MME based detection

|  |  |
| --- | --- |
| Monitoring Event | Procedures |
| Monitoring the association of the MTC Device and UICC | The SGSN/MME asks for the MTC Device IMEI (e.g. Identity procedure).  2> The SGSN/MME checks whether the IMEI provided by the device is the same as the configured IMEI.  3> If not, the SGSN/MME shall trigger the reporting. |
| Monitoring the alignment of the MTC feature | The SGSN/MME checks whether the MTC Device behavior is aligned with the activated MTC features for the device.  2> If not (e.g. the MTC Device with low mobility feature performs RAU/TAU or handover procedure frequently), the SGSN/MME shall trigger the reporting. |
| Monitoring change in the point of attachment | The SGSN/MME checks whether there is change in point of attachment by comparing the location area information from RAN against the configured location area information from the HLR/HSS (e.g. the allowed location area information).  2> If yes, the SGSN/MME shall trigger the reporting. |
| Monitoring loss of connectivity | The SGSN/MME checks whether the MTC Device is offline.  2> If yes, the SGSN/MME shall trigger the reporting. |

### 6.10.3 Impacts on existing nodes or functionality

Impacts on HLR/HSS:

- Support configuring and provisioning of monitoring related information (e.g. monitoring event, criteria, default action and etc) in MTC subscription.

Impacts on SGSN/MME:

- Support storing the monitoring related information (e.g. monitoring event, criteria, default action and etc) for a particular MTC Device.

- Support monitoring detecting behaviour.

- Support executing monitoring action, e.g. according to the pre-defined action.

### 6.10.4 Evaluation

All events can be detected and the signals to obtain the information for detecting the events can be optimized.

However the load of the SGSN/MME may increase depending on the number of events and actions.

## 6.11 Solution - HLR/HSS based detection

### 6.11.1 Problem Solved / Gains Provided

See clause 5.10 "Key Issue - MTC Monitoring" and 6.9 "Solution - MTC Monitoring - General".

### 6.11.2 General

For this solution, the HLR/HSS is responsible for detecting monitoring event with the assistance of other nodes. The MTC monitoring events along with the related criteria and default action are configured in the HLR/HSS. The HLR/HSS monitors the MTC Device behaviour according to the MTC monitoring event trigger and performs corresponding action.

The following table shows the procedures of the HLR/HSS.

Table 6.11.2-1: HLR/HSS based detection

|  |  |
| --- | --- |
| Monitoring Event | Procedures |
| Monitoring the association of the MTC Device and UICC | 1. The SGSN/MME provides the MTC Device IMEI together with the IMSI to the HLR/HSS.   2> The HLR/HSS checks whether the IMEI provided by the SGSN/MME is the same as the configured IMEI for the MTC Device.  3> If not, the HLR/HSS shall trigger the reporting. |
| Monitoring the alignment of the MTC feature | 1. The HLR/HSS checks whether the MTC Device behaviour is aligned with the activated MTC features for the device.   2> If not (e.g. the HLR/HSS is aware that the MTC Device with low mobility feature changes the serving SGSN/MME), the HLR/HSS shall trigger the reporting. |
| Monitoring change in the point of attachment | 1. The SGSN/MME reports the UE location (e.g. RAI, TAI, CGI, E-CGI and etc) to the HLR/HSS during MM procedure.   2> The HLR/HSS checks whether the UE location is allowed comparing to the configured location.  3> If not, the HLR/HSS shall trigger the reporting. |
| Monitoring loss of connectivity | 1. The HLR/HSS checks whether the MTC Device is offline, e.g. the GGSN/P-GW information for the M2M APN is deleted, or receives Purge message.   2> If yes, the HLR/HSS shall trigger the reporting. |

### 6.11.3 Impacts on existing nodes or functionality

Impacts on HLR/HSS:

- Support configuring monitoring related information (e.g. monitoring event, criteria, default action and etc) in MTC subscription.

- Support monitoring detecting behaviour.

Impacts on SGSN/MME:

- Support reporting location information to the HLR/HSS so that the HLR/HSS can detect a change by comparing with a subscribed location, or by comparing with the earlier stored location.

- Support registering GGSN/P-GW information to the HLR/HSS. To detect loss of connectivity quicker the SGSN/MME may need to configure very short periodic update timers, which increases MM signalling considerably.

- Support reporting MTC Device IMEI to the HLR/HSS.

### 6.11.4 Evaluation

Without any impacts on other nodes or signalling the HLR/HSS is able to detect when another device (IMEI) uses the UICC (IMSI). Also an action (e.g. cancel location or invalidate UICC) can be added and affects only the HLR/HSS.

Monitoring of feature activation clearly requires additional functions in other nodes and related signalling. Also monitoring of the point of attachment by the HLR/HSS requires additional functions in other nodes and related signalling.

Monitoring of the connectivity is not necessarily suited for the HLR/HSS as other HLR/HSS signalling is much less frequent. Detection of lost connectivity may require frequent indications to the HLR/HSS that connectivity exists.

## 6.12 Solution - GGSN/P-GW based detection

### 6.12.1 Problem Solved / Gains Provided

See clause 5.10 "Key Issue - MTC Monitoring" and 6.9 "Solution - MTC Monitoring - General".

### 6.12.2 General

For this solution, the GGSN/P-GW is responsible for detecting monitoring event with the assistance of other nodes. The GGSN/P-GW obtains such information from the HLR/HSS, and monitors the MTC Device behavior according to the MTC monitoring event trigger and performs corresponding action.

The following table shows the procedures of the GGSN/P-GW.

Table 6.12.2-1: GGSN/P-GW based detection

|  |  |
| --- | --- |
| Monitoring Event | Procedures |
| Monitoring the association of the MTC Device and UICC | 1. The SGSN/MME provides the MTC Device IMEI together with the IMSI to the GGSN/P-GW during the bearer establishment procedure.   2> The GGSN/P-GW obtains the mapped IMEI and IMSI pair from e.g. the HLR/HSS.  3> The GGSN/P-GW checks whether the IMEI and IMSI provided by the SGSN/MME is matches with the configured IMEI and IMSI pair.  4> If not, the GGSN/P-GW shall trigger the reporting. |
| Monitoring the alignment of the MTC feature | 1. The GGSN/P-GW checks whether the MTC Device behaviour is aligned with the activated MTC features for the device.   2> If not (e.g. the GGSN/P-GW is aware that the MTC Device with low mobility feature changes location), the GGSN/P-GW shall trigger the reporting. |
| Monitoring change in the point of attachment | 1. The GGSN/P-GW activates the MS Info Change Reporting Action when PDN connection is created.   2> The SGSN/MME reports the UE location (e.g. RAI, TAI, CGI, E-CGI and etc) to the GGSN/P-GW during bearer management procedure.  3> The GGSN/P-GW checks whether the UE location is allowed comparing to the configured location.  4> If not, the GGSN/P-GW shall trigger the reporting. |
| Monitoring loss of connectivity | 1. The GGSN/P-GW checks whether the MTC Device is offline, e.g. the PDN connection for the M2M APN is deactivated.   2> If yes, the GGSN/P-GW shall trigger the reporting. |

### 6.12.3 Impacts on existing nodes or functionality

Impacts on HLR/HSS:

- Support configuring monitoring related information (e.g. monitoring event, criteria, default action and etc) in MTC subscription.

Impacts on SGSN/MME:

- Support provisioning of monitoring related information (e.g. monitoring event, criteria, default action and etc) to the GGSN/P-GW.

Impacts on GGSN/P-GW:

- Support monitoring detecting behaviour.

Impacts on PCRF/BBERF/PCEF:

- Support provisioning of monitoring related information (e.g. monitoring event, criteria, default action and etc) to the P-GW, if PMIP is used over S5/S8.

### 6.12.4 Evaluation

With a proper subscription it can be prevented that a UICC can be used for anything else than the PDP/PDN connection provided for MTC. PDP/PDN connections are then only possible with the subscribed APN/P-GW/GGSN. The GGSN/P-GW can refuse PDP/PDN activation when the IMEI does not match. Compared to the HLR/HSS with the existing signalling the GGSN/P-GW cannot detach the device and also not invalidate the UICC.

The GGSN/P-GW gets location information by setting "the MS Info Change Reporting Action" to start in the create session response to the MME and then the GGSN/P-GW can monitor change of the point of attachment using the existing procedure of the MS info change reporting procedure.

If the MTC device has only one PDN connection, the P-GW may detect the monitoring of the connectivity by detecting the PDN disconnection, but when the multiple PDN connections is used, a PDN disconnection does not imply that the UE is detached and the connectivity with the UE is lost. Hence, the GGSN/P-GW is not necessarily suited for detecting lost connectivity.

Editor's Note: Evaluation for PMIP based S5/S8 is FFS.

## 6.13 Solution - Reporting by SGSN/MME

### 6.13.1 Problem Solved / Gains Provided

See clause 5.10 "Key Issue – MTC Monitoring" and 6.9 "Solution – MTC Monitoring – General".

### 6.13.2 General

For this solution, the SGSN/MME is responsible for reporting the event.

This solution can only be used for solution 1, i.e. the SGSN/MME is responsible for detecting (clause 6.10.)

When the event is detected, the SGSN/MME reports towards the MTC Server

### 6.13.3 Impacts on existing nodes or functionality

The SGSN/MME needs to provide a new reference point for event reporting.

### 6.13.4 Evaluation

## 6.14 Solution - Reporting by HLR/HSS

### 6.14.1 Problem Solved / Gains Provided

See clause 5.10 "Key Issue - MTC Monitoring" and 6.9 "Solution - MTC Monitoring – General".

### 6.14.2 General

For this solution, the HLR/HSS is responsible for reporting the event. When the event is detected, the HLR/HSS reports towards the MTC Server.

This solution can be used with solution 1 and 2, i.e. the SGSN/MME or the HLR/HSS is responsible for detecting. The following table shows the procedures for different detecting solution.

Table 6.14.2-1: HLR/HSS based Reporting

|  |  |
| --- | --- |
| Detecting solution | Procedures |
| Solution 1: SGSN/MME based detection (clause 6.10) | The SGSN/MME reports the event related information (e.g. event type, MTC Device identifier) to the HLR/HSS.  The HLR/HSS forwards the warning notification request message to the MTC Server.  3> The HLR/HSS receives the warning notification acknowledgement message from the MTC Server and forwards it to the SGSN/MME. |
| Solution 2: HLR/HSS based detection (clause 6.11) | The HLR/HSS sends the warning notification request message to the MTC Server, which includes the event related information (e.g. event type, MTC Device identifier).  2> The HLR/HSS receives the warning notification acknowledgement message from the MTC Server. |

### 6.14.3 Impacts on existing nodes or functionality

The path between the HLR/HSS and the MTC Server needs to be updated in order to exchange the warning notification.

For solution 1, the message between SGSN/MME and the HLR/HSS e.g. Notify Request message, also needs to be updated.

### 6.14.4 Evaluation

## 6.15 Solution - Reporting by GGSN/P-GW

### 6.15.1 Problem Solved / Gains Provided

See clause 5.10 "Key Issue – MTC Monitoring" and 6.9 "Solution – MTC Monitoring – General".

### 6.15.2 General

For this solution, the GGSN/P-GW is responsible for reporting the event. The GGSN/P-GW reports towards the MTC Server.

This solution can be used with solution 1 and 3, i.e. the SGSN/MME or the GGSN/P-GW is responsible for detecting. The following table shows the procedures for different detecting solution.

Table 6.15.2-1: GGSN/P-GW based Reporting

|  |  |
| --- | --- |
| Detecting solution | Procedures |
| Solution 1: SGSN/MME based detection (clause 6.10) | The SGSN/MME reports the event related information (e.g. event type, MTC Device identifier) to the GGSN/P-GW through S-GW via GTP-C message (e.g. reusing the Change Notification Request message) for GTP based S5/S8. Those information are transferred to PGW via PCC for PMIP based S5/S8.  The GGSN/P-GW encapsulates and sends the warning notification request message to the MTC Server.  3> The SGSN/MME receives the warning notification acknowledgement message from the MTC Server and forwards it to the SGSN/MME via the GTP-C path. |
| Solution 2: GGSN/P-GW based detection (clause 6.12) | The GGSN/P-GW sends the warning notification request message to the MTC Server, which includes the event related information (e.g. event type, MTC Device identifier).  2> The GGSN/P-GW receives the warning notification acknowledgement message from the MTC Server. |

### 6.15.3 Impacts on existing nodes or functionality

The GGSN/P-GW needs to be updated to communicate with the MTC Server.

For solution 1, the GTP-C message also needs to be updated to transfer the warning notification. For PMIP based S5/S8, PCRF/BBERF/PCEF: shall support provisioning of monitoring related information (e.g. monitoring event, criteria, default action and etc) to the P-GW, if PMIP is used over S8.

### 6.15.4 Evaluation

## 6.16 Solution - Reporting by PCRF

### 6.16.1 Problem Solved / Gains Provided

See clause 5.10 "Key Issue – MTC Monitoring" and 6.9 "Solution – MTC Monitoring – General".

### 6.16.2 General

For this solution, the GGSN/P-GW or S-GW (PMIP based) is responsible for reporting the event via PCRF. The GGSN/P-GW/S-GW exchanges warning notification message with the PCRF, and the PCRF reports towards the MTC Server.

This solution can be used with solution 1 and 3, i.e. the SGSN/MME or the GGSN/P-GW is responsible for detecting. The following table shows the procedures for different detecting solution

Table 6.16.2-1: PCRF based Reporting

|  |  |
| --- | --- |
| Detecting solution | Procedures |
| Solution 1: SGSN/MME based detection (clause 6.10) | The SGSN/MME reports the event related information (e.g. event type, MTC Device identifier) to the GGSN/P-GW through S-GW via GTP-C message (e.g. reusing the Change Notification Request message) for GTP based S5/S8. For PMIP based S5/S8, the SGSN/MME reports the event to the S-GW.  For GTP based S5/S8 case, the GGSN/P-GW encapsulates and sends the warning notification request message to the PCRF by reusing the IP-CAN session modification request message.  For the PMIP based S5/S8 case, the S-GW directly informs the PCRF by reusing Gateway Control session modification message.  The PCRF reports the event to the MTC Server and obtains acknowledge from the MTC Server.  The PCRF forwards the acknowledgement message to the GGSN/P-GW or S-GW (i.e. PMIP based S5/S8).  5> The GGSN/P-GW or S-GW forwards the warning notification acknowledgement message to the SGSN/MME. |
| Solution 2: GGSN/P-GW based detection (clause 6.12) | The GGSN/P-GW sends the warning notification request message to the PCRF by reusing the IP-CAN session modification request message.  The PCRF forwards the warning notification request message to the MTC Server, which includes the event related information (e.g. event type, MTC Device identifier).  3> The PCRF receives the warning notification acknowledgement message from the MTC Server and forwards it to the GGSN/P-GW. |

### 6.16.3 Impacts on existing nodes or functionality

The PCC related messages needs to be updated to transfer warning notification.

For solution 1, the GTP-C message also needs to be updated to transfer the warning notification.

For solution 2, PCC/BBERF/PCEF need to be updated to transfer the warning notification if PMIP is used over S8.

NOTE: PCRF impacts are expected to be the same as GTP based S5/S8.

### 6.16.4 Evaluation

## 6.17 Solution – Allowed Time Period after TAU/RAU

### 6.17.1 Problem Solved / Gains Provided

See clause 5.9 "Key Issue –Time Controlled" and clause [TBD] "Key Issue – Extra Low Power".

### 6.17.2 General

The solution specified in this clause can be used for Extra-low power consumption, possibly together with Time-controlled MTC communications.

The basic idea behind the solution is that downlink data transfer is only possible during an allowed time period after the MTC Device performed a TAU/RAU procedure. During that allowed time period the MTC server can communicate with the MTC device. After the allowed time period the MTC device may switch off the receiver and communication is not possible.

Editor's Note: It is FFS how this solution can cope with MTC Devices with low mobility, which may perform the TAU/RAU procedure very rarely.

Editor's Note: It is FFS how this solution can cope with MTC Devices performing TAU/RAU often during network-determined forbidden time interval (i.e., assuming that TAU/RAU is allowed during the forbidden time).

After the MTC Device performs a TAU/RAU procedure the MTC Device may stay in power-up mode and inform the MTC Server that is available for communication so that the MTC Server(s) can forward all buffered traffic to the device. The MTC Device may be configured not to inform the MTC Server after every TAU/RAU procedure and thus reduce the frequency of allowed time periods based on the applicable time-controlled requirements. How often an allowed time period occurs is thus configurable. For example, the MTC Device may be configured to stay in power-up mode after a TAU/RAU and inform the MTC Server about its availability only between 1am – 5am every day.

The MTC Server buffers downlink traffic for the MTC Device until the MTC Device informs the server that is ready for MTC communications.

NOTE 1: Since this solution requires downlink traffic buffering, it is appropriate for time-tolerant MTC applications.

The EPS network configures the MTC Device as to initiate allowed-time periods (after a RAU/TAU) according to the operator requirements and the MTC subscription options. Normally, downlink traffic does not occur outside of an allowed time period because the MTC Server(s) expect the device to send first a message to announce its availability for MTC communications. However, if downlink traffic for the MTC Device occurs outside an allowed time period, then the EPS network rejects/drops this traffic (i.e. the EPS network does not page the MTC Device outside the allowed time period).

### 6.17.3 Impacts on existing nodes or functionality

### 6.17.4 Evaluation

## 6.18 Solution - MT Communication with NATTT

### 6.18.1 Problem Solved / Gains Provided

See clause 5.3 "Key Issue – Ipv4 Addressing".

### 6.18.2 General

What follows below are some additional considerations, beyond the FQDN Identifier Solution described in clause 6.1, when the assigned Ipv4 address belongs to the range of private Ipv4 addresses. Depicted in Figure 6.18.2-1 is a general MTC scenario with MTC device roaming in a VPLMN. The MTC device is assigned a private IP address (referred to as "D") that is hosted on the PGW node residing in the VPLMN (i.e. Local breakout). All the relevant EPS nodes are located in the VPLMN, except for the HSS/AAA node that resides in the HPLMN.

The MTC server wishing to establish a Mobile Terminated (MT) communication may be owned by the HPLMN, by the VPLMN or by a third party. It is located somewhere on the Internet, which is why a Network Address Translation (NAT) device is needed at the public/private boundary.



Figure 6.18.2-1: NATTT applied to the MTC context

In order to support MT communications to MTC devices inside private IP address space, the NAT device on the public/private boundary is replaced by a NATTT-capable device ([3]) i.e. a NAT device capable of UDP encapsulation for packets exchanged on the "public" side (i.e. to/from the MTC server), in addition to its traditional role as a NAT device. The reason for using UDP encapsulation (instead of simple IP-in-IP encapsulation) is because the NATTT device relies on a well-known UDP port number to identify the encapsulated packets.

The call flow depicted in Figure 6.18.2-2 describes how MT communication with MTC devices inside private IP address space works in step by step fashion:



Figure 9.18.2-2: Call flow for MT communication with MTC device inside private IP address space

1. MTC device performs the EPS Attach procedure as described in TS 23.401. As part of the EPS Attach procedure the MTC device is assigned a private IP address, referred to here shortly as "D". Also as part of this procedure, the PGW node returns the public IP address of the NATTT device ("N") through which the private address "D" is reachable. If there are several NATTT devices on the border of the private IP network, the PGW selects any that provides access to the private address "D". The S5/S8/S11 Create Session Response message (not shown) is used to convey both "D" and "N" from the PGW to the MME.

2. As part of the previous step, or at the end of the EPS Attach procedure, the MME notifies the HSS/AAA with "D" and "N". Currently there is no direct interface between the PGW and the HSS/AAA, which is why the Notification is sent from the MME.

3. The HSS/AAA sends a DNS Update to the authoritative DNS server in order to associate "D" and "N" with the DNS record for the MTC device (the latter being referenced via its unique FQDN). This requires a new type of DNS record.

4. At some point in time the MTC server wishes to send a Mobile terminated (MT) message to the MTC device whose unique identifier is FQDN.

5. MTC server sends a DNS query that eventually reaches the authoritative DNS server.

6. The DNS response of the authoritative DNS server includes "D" and "N".

7. MTC server performs UDP encapsulation of the IP packet it wishes to send to the MTC device. The destination IP address in the outer IP header is set to "N". The destination IP address in the inner IP header is set to "D". The UDP port in the UDP encapsulation header is set to a well known value, as described in [3]. The source IP address in both the inner and outer IP headers is set to the public IP address of the MTC server.

8. The NATTT device identifies the packet as a NAT tunnelled packet because it arrives on a well-known UDP port. It strips off the outer IP/UDP header and forwards the inner IP packet on the private IP network.

9. The inner IP packet reaches the PGW hosting the MTC device's private IP address. The PGW delivers the packet to the MTC device via an appropriate EPS bearer.

The proposed solution also applies to GERAN and UTRAN devices, in which case MME and PGW are replaced with SGSN and GGSN.

It also applies to MTC device-to-device communications, where either or both MTC devices are located inside private IP address space. In this case it is the source MTC device itself that performs the DNS query to resolve the FQDN of the target MTC device (i.e. to obtain the private IP address of the target MTC device, as well as the public address of the NATTT device in the target network). It is also the source MTC device that performs the packet encapsulation.

NOTE: It is FFS how to prevent unwanted traffic from being sent to the MTC device.

### 6.18.3 Impacts on existing nodes or functionality

The PGW needs to notify the SGSN/MME of the NAT device’s public address “N” (e.g. new parameter in the Create Session Response message).

For IP address assignment via DHCPv4, the PGW needs to notify the SGSN/MME of the assigned IPv4 address outside of the Attach procedure (e.g. via the Bearer Modification procedure).

SGSN/MME needs to notify the HSS of the MTC device’s private address “D” and the NAT device’s public address “N” (e.g. new parameters in the Notify Request message).

HSS needs to perform DNS updates of the authoritative DNS server that stores the association between the “host name” of the MTC device on one hand, and the dynamically assigned private IP address “D” plus the NAT device’s public address “N” on the other.

Requires definition of a new DNS record, capable of storing the NAT device’s IP address “N”.

### 6.18.4 Evaluation

Benefits:

- Low impact on existing Core Network nodes;

- Generic IP-level solution that does not rely on application-level identifiers (e.g. SIP URI);

- Works in all scenarios (non-roaming, roaming with home routed traffic, roaming with local breakout) to an attached MTC device with an established PDN connection;

- The solution does not rely on alternative communication channels (e.g. SMS) for delivery of a “push” stimulus;

- Works also for device-to-device communication;

- The solution is based on the generic FQDN Identifier solution described in clause 6.1, but the public DNS functionality needs to be extended.

Drawbacks:

- Requires support of a new DNS record (supporting D and N addresses) in the public DNS infrastructure, this DNS record needs to be standardised by the IETF and globally deployed as part of the public DNS infrastructure. Such a deployment may take a relatively long period of time.

Editor's Note: a solution may exist not requiring support of the new DNS record by the public DNS infrastructure, whereby the private IP address "D" would be transferred in the DNS infrastructure via transparent strings. This is FFS.

- If the failure of a NATTT box requires to modify the public IP address "N" through which the private address "D" is reachable, then all the DNS entries of all MTC devices served by this NATTT must be updated (via the MME in this case). In addition the DNS cache entries at the MTC Server need to be cleared, generally after a timeout of few minutes (depending on the implementation).

- additional complexity in the MTC Server to support new DNS records and UDP/IP encapsulation (according to [3] this may require the support of a NAT Daemon in the MTC Server which intercepts DNS queries and user plane traffic to hide the DNS extension and UDP/IP encapsulation to the application).

## 6.19 Solution – MT Communication with Micro Port Forwarding

### 6.19.1 Problem Solved / Gains Provided

See clause 5.3 "Key Issue – IP Addressing".

### 6.19.2 General

The general concept of this solution is that during initial PDP context / PDN connection establishment, the network will setup special very narrow port forward rule(s) (i.e. a Micro Port Forward rule) with the NAT to allow MT messages only from a defined MTC Server(s). Not only is the port forward narrowed based on the MTC Server IP address, it is further narrowed by only allowing specific source and destination port numbers. This effectively creates the same size pinhole in the NAT that UE used for MTC creates with a normal outbound packet. The difference being that this pinhole is now more specifically managed.

When NAPT (Network Address and Port Translation) port forwarding only uses a mandated SRC IP address (i.e. public MTC Server IP address) and DST port number (i.e. public UE port number), this yields only 65,536 (2^16) unique port forwarding rules per public UE IP address per public MTC Server IP address. However, when the port forward rule is extended to a MPF rule (additionally mandate of the SRC port number (i.e. public MTC Server port number), this yields ~4 billion (2^32) unique port forwarding rules per public UE IP address per public MTC Server IP address.

More than one MPF rule may be established for a particular UE used for MTC. The UE needs a MPF rule for each MTC Server it requires MT messaging support for.

The set of MPF rule configuration parameters that can be specified as input into the NAT entity establishing a new MPF rule could include the following:

- Per UE subscription:

- default MPF enablement flag;

- default set of authorized MTC Server public IP address(es) that can use an established PDP context / PDN connection for IP communications;

- default private UE DST port # range (optional)(Eases the requirement on the UE to only have to listen to pre-configured static ports);

- public MTC Server port # range (optional);

- protocol constraints (optional);

- lease time (time for the NAT to maintain the MPR rule) (optional).

- Per authorized MTC Server public IP address (optional configuration parameters that overrides the default above):

- reference to the authorized MTC Server public IP address;

- private UE DST port # range constraints (optional);

- public MTC Server port # range constraints (optional);

- protocol constraints (optional);

- lease time (time for the NAT to maintain the MPR rule) (optional).

- Per APN configuration / PDN subscription context (optional configuration paremeter that overrides the default above);

- reference to APN configuration / PDN subscription context;

- MPF enablement flag;

- references to the subset of authorized MTC Server public IP address(es) that can use an established PDP context / PDN connection for IP communications.

These MPF rule configuration parameters could be configured in the UE used for MTC (e.g. by the MTC Server through Device Management procedures) and/or in the subscription data for the UE in the HSS/HLR. If there is a conflicting parameter value between a parameter stored both in the UE and the HSS/HLR, the subscription data value in the HSS/HLR will have priority over the value stored in the UE. Furthermore, if there is still a conflicting parameter value between the default value and a MTC Server or APN configuration / PDN subscription context specific value, the latter will have priority over the default value.

An established MPF rule contains the following parameters:

- reference to the established PDP context / PDN connection;

- set of authorized MTC Server public IP address(es) that can use the established PDP context / PDN connection for IP communications;

- public UE IP address;

- public MTC Server port number;

- public UE port number.

- private UE IP address;

- private UE port number;

- lease time (optional);

- protocol constraints (optional).

Once a MPF rule is established, the methods to communicate the public portion of the MPF rule to the MTC Server so that it can be used for MT communications includes:

1) UE used for MTC sends MPF rule to MTC Server - The UE used for MTC receives the public portion of the MPF rule from the network during the PDN connection establishment procedure. Then the UE used for MTC sends a message(s) to the MTC Server(s) containing the information regarding the public portion of the MPF rule that was created. The UE used for MTC can do this by simply sending a transport layer (e.g. UDP or TCP) message using the appropriate IP address and port numbers. Alternatively, the UE used for MTC can send this information via an application layer message;

2) MTC Server request MPF rule from DNS server - This option uses the FQDN Identifier Solution described in clause 6.1. When the MTC Server wants to send a MT message it will do a DNS query of the FQDN of the UE used for MTC. The DNS response will contain the information defining the public portion of the MPF rule;

3) MTC Server obtains MPF rule from DT-GW - This option uses the MT communications address resolution via DT-GW solution described in clause 6.46. When the MTC Server wants to send a MT message to a UE used for MTC and the address of the assigned DT-GW is not known, the MTC Server will first perform a DNS query of the hostname of the UE. The DNS response will contain the IP addresses of the assigned DT-GW for the UE. Once the address of the assigned DT-GW for the UE is known, the MTC Server communicates with the DT-GW to ascertain the public portion of the MPF rule.

Figure 6.19.2-1 illustrates how the IP address(es) and port numbers of a MPF rule are then used to route a MT IP packet from the MTC Server to the UE used for MTC in both the public and private address space.



Figure 6.19.2-1: MT message sent into a private IPv4 address space using Micro Port Forwarding

Figure 6.19.2-2 illustrates how a MPF rule is established for a new PDN connection, communicated to the MTC Server and utilized for MT communications.



Figure 6.19.2-2: Call flow for MPF rule establishment for a PDN connection

1. UE used for MTC sends initial attach request specifying any MPF configuration preferences for the default PDN connection e.g. that may have been configured using Device Management procedures by the MTC service provider.

2. If the MME does not have the subscription data for the UE, the Update Location request is sent to the HSS.

3. The HSS sends the Update Location ACK to the MME containing subscription data for any MPF configuration parameters and, if a DT-GW is employed for the UE, the assigned NAT entity for the new PDN connection, if not co-locate with the P-GW and the assigned DT-GW. The MME resolves any duplicate and conflicting MPF configuration parameter values by applying the appropriate priority.

4. The MME and S-GW include any MPF configuration parameters in their respective Create Session requests.

5. If the MPF enablement flag is set for the new PDN connection and the NAT entity and P-GW are not co-located, the P-GW sends a MPF request to the NAT entity responsible for the establishing the MPF rule for the new PDN connection.

6. NAT entity establishes the MPF rule for the new PDN connection using any specified MPF configuration parameters.

7. If a MPF rule was established and the NAT entity and P-GW are not co-located, the NAT entity includes the entire MPF rule (both public and private portions) in the MPF response to the P-GW.

8. If a DT-GW is assigned for the UE, the P-GW sends a PDN establishment status update to the assigned DT-GW containing the complete MPF rule.

9. If a MPF rule was established, the P-GW and S-GW includes the entire MPF rule in their respective Create Session responses.

10. If a MPF rule was established, the MME includes the entire MPF rule in the Attach Accept message.

11. UE responds with the Attach Complete message.

12. The UE used for MTC sends a transport layer (e.g. UDP or TCP) message using the appropriate IP address and port numbers. Alternatively, the MTC device can send this information via an application layer message.

12'.In an alternative to step 12, the MTC server obtains the public portion of the MPF rule from the DT-GW.

13a. When the NAT entity receives an incoming packet from the MTC server that matches the MPF rule (i.e. public MTC Server SRC IP and port #, public UE DST IP and port #), it performs the normal NAPT on the public UE device IP address and DST port #.

13b. The NAT entity then forwards the packet to the UE.

### 6.19.3 Impacts on existing nodes or functionality

Impacts on CN nodes:

- NAPT functionality is extended to employ MPF (addition of the SRC port number to the port forwarding rule);

- If NAT entity is not co-located with the GGSN/P-GW, a new interface and messaging between the GGSN/P-GW and NAT entity is required to establish MPF rules;

- HSS/HLR additional storage of MPF configuration parameters as part of subscription data;

- PDP context / PDN establishment procedure messaging to be extended to include MPF configuration parameters and MPF rule;

- if DT-GW is used for MTC Server to obtain public portion of MPF rule, the “MT communications address resolution via DT-GW” solution described in clause 6.46 shall be supported.

### 6.19.4 Evaluation

Benefits:

- Increases the number of possible unique port forwarding rules per public UE IP address per public MTC server IP address from 65,536 (2^16) to ~4 billion (2^32);

- For security, reduces scanning attack success rate from malicious network entities.

- Works in all scenarios (non-roaming, roaming with home routed traffic, roaming with local breakout);

- The solution does not rely on alternative communication channels (e.g. SMS) for delivery of a “push” stimulus to an attached MTC device with an established PDN connection, but this requires the network to periodically re-new the MPF rule in the NAT entity;

Drawbacks:

- MPF rule adds additional port forwarding requirements on NAPT in network;

- MPF rule adds additional subscription data and/or UE configuration.

- If the application payload need to transport IP addresses then there is a need for ALG (Application Level Gateway), which may not be possible if the payload is encrypted end to end; If no encryption is used then the NAT needs to parse the application level payload.

- NAT single point of failure (the MPF rules are lost if the NAT box fails) but this is similar to traditional port forwarding;

- MTC Device needs an explicit protocol to discover the NAT and also set the MPC filter in the NAT.

## 6.20 Solution - Optimizing periodic LAU/RAU/TAU Signalling

### 6.20.1 Problem Solved / Gains Provided

See clause 5.6 "Key Issue – Low Mobility," clause 5.12 "Key issue – Signalling Congestion Control", clause 5.14 "Key Issue – Potential overload issues caused by Roaming MTC devices" and clause [TBD] "Key Issue – Extra Low Power".

### 6.20.2 General

This solution can be used for low mobility and/or extra low power MTC devices (CS and PS domain specific systems), MTC devices that indicate "Low-Priority-Access" (PS domain specific system) (see clause 6.23), and for signalling congestion control and potential overload issues caused by roaming MTC devices.

For CS domain specific systems, MTC devices can be pre-provisioned with MTC\_T3212 \_Multiplier. If provisioned, the MTC device shall calculate the periodic LAU timer by multiplying T3212 (received from BCCH) with MTC\_T3212 \_Multiplier. MTC\_T3212\_Multiplier is also configured at MSC/VLR in order to derives new implicit detach timer. Alternatively, MTC\_T3212\_Multiplier may be part of an MTC subscription data stored in HLR/HSS and downloaded to MSC/VLR during attach procedure.

NOTE: The MTC device may need to be configured to apply the specific timer, e.g. whether to adopt the special timer value from broadcast information.

Editor's Note: It is FFS if dynamic synchronization of MTC\_T3212\_Multiplier is needed between MSC/VLR and MTC device.

Alternatively, a separate setting for the T3212 timer can be added into the LAU procedure. Details for such solution including whether to add specific MS capability sent from the MTC device can be decided in stage 3.

For PS domain specific systems, in order to reduce periodic RAU/TAU signalling the granularity of T3312/T3412 and Mobile reachable timer can be increased. New binary coding can be added for example to indicate GPRS timer value is incremented in multiple of 10 or 100 decihours.

Editor's Note: Exact changes to coding of the GPRS timer value is FFS and will be specified as part of stage-3 specification.

A long periodic RAU/TAU timer (T3312/T3412) or specific coding to deactivate the timers may be part of an MTC subscription data stored in HLR/HSS and downloaded to the SGSN/MME during the Attach procedure. During Attach and periodic RAU/TAU procedures the SGSN/MME sets the device's periodic RAU/TAU timer and the mobile reachable timer to long values or deactivate the timers according to the parameter received from the MTC subscription data. Alternatively, if periodic RAU/TAU timer is not stored as part of MTC subscription data, or if SGSN/MME is experiencing overload situation, or if MTC device indicates "Low priority Access", SGSN/MME may decide to set them to higher values or decide to deactivate them.

If the subscribed periodic timer changes the SGSN/MME provides the MTC device with the new timer value during the next RAU/TAU procedure. Alternatively the SGSN/MME can initiate an SGSN/MME-Initiated Detach procedure with a re-attach indication to enforce an Attach procedure and provide the MTC device with the new timer value.

For M2M devices that support both the PS and CS domains, an alternative implementation is that these devices are commanded to use Network Mode of Operation (NMO) I and use a long PRU timer in the PS domain. With NMO=I, the MSC deactivates its implicit detach functionality and the device only performs periodic updates to the PS domain. By using a new broadcast indication, the network operator can maintain the use of NMO=II for existing devices and only use NMO=I for M2M devices.

### 6.20.3 Impacts on existing nodes or functionality

Impacts to HLR/HSS:

- Support configuring and provisioning of periodic LAU/RAU/TAU information (e.g. MTC\_T3212\_Multiplier, T3312/T3412 timer value or special encoding to disable them) as part of MTC subscription.

Impacts on SGSN/MME:

- Support configuring and storing the periodic RAU/TAU information (e.g. T3312/T3412 timer value or special encoding to disable them) and mobile reachable timer for a particular MTC Device, according to the parameter received from the HSS/HLR.

- Support modification of periodic RAU/TAU and mobile reachable timer values, if the subscribed periodic timer value changes, and provide the MTC device with the new timer value during the next RAU/TAU procedure or by initiating detach with "re-attach indication".

- Support configuring longer timer values for RAU/TAU or disable them based on local configuration, if periodic timer is not present in subscription information, or if SGSN/MME is experiencing overload situation, or if the device indicates "low priority access".

- Support for an extended coding of the timers (e.g. T3312/T3412)

Impacts on MSC/VLR:

- Support configuring and storing the periodic LAU information (e.g. MTC\_T3212\_Multiplier).

- Using MTC\_T3213\_Multiplier to derive new implicit detach timer.

- Downloading MTC\_T3213\_Multiplier during the attach procedure, if it is stored as part of subscription data.

Impact on the MTC Device / UE

- Support pre-configuring MTC\_T3213\_Multiplier and calculating the periodic LAU timer.

- Configuration flag on whether to use MTC\_T3213\_Multiplier or special periodic timer value from broadcast information.

- MTC devices need to be able to read the NMO I indication in the broadcast information

Impacts on the RAN/GERAN:

- New broadcast indication telling specifically MTC devices to use NMO I (In UTRAN this can be an existing spare bit in one of the 'transparent containers' of NAS information that the UTRAN broadcasts),

- For CS domain system, generation of special periodic timer value in the broadcast information

### 6.20.4 Evaluation

Following conclusion can be drawn:

- For the protection of other networks in the case of one network's failure, long periodic timers seem to be useful in slowing down the rate at which low activity mobiles detect the network failure. Hence mechanisms with the minimal impact on VPLMN equipment are desirable.

- Extending the periodic timer in one domain (e.g. PS) and not the other (e.g. CS) will not slow down the rate at which mobiles detect network failure unless NMO=1 is used.

- Proposed solution does not avoid overload or provide a congestion control mechanism, but it provides a simple way to limit the signalling load in the network.

- Extending the existing periodic LAU/RAU/TAU timers and defining configuration of new parameter (MTC\_T3212 \_Multiplier) is fairly simple.

- MTC device indication of "Low Priority Access" to SGSN/MME can be added by using new IE on existing NAS messages.

- HLR/HSS control of the periodic timer ranges is useful longer term functionality. Operator can control the frequency of the periodic update performed by MTC devices by configuring the periodic timer related parameters in the MTC subscription database.

- Adding the new timer values or indication to broadcast information may have an impact on RAN and GERAN. In general Broadcast channels are a scarce resource.

Based on the above conclusion following items are proposed for normative work:

- Add normative stage 2 requirements for enabling the long periodic LAU/RAU/TAU update timer for MTC devices.

- Add encoding of the extended periodic LAU/RAU/TAU timers and MTC\_T3212\_Multiplier.

- Standardization and encoding for new subscription parameters in HLR/HSS for extended periodic LAU/RAU/TAU timers and MTC\_T3212\_Multiplier.

- Standardization of mechanism for MTC device to indicate "Low priority Access" to SGSN/MME/MSC.

- GERAN broadcast information and the existing NAS information broadcast by UTRAN is modified so that M2M devices can be commanded to use NMO=I (Gs interface) while existing devices use NMO=II.

## 6.21 Solution - Randomized triggering of time-controlled MTC operations

### 6.21.1 Problem Solved / Gains Provided

See clause 5.9, "Key Issue – Time Controlled"; clause 5.12, "Key Issue – Signalling Congestion Control."

### 6.21.2 General

Simultaneous operations by too many MTC devices especially at the beginning of the time period may cause serious network or MTC server overload. Therefore, the triggering of time-controlled MTC operations needs to be randomized.

The time-controlled operation can be triggered by MTC device or the network including MTC server. When triggered by the network, the operation of MTC device can be started after receiving paging from the network elements (e.g. SGSN/MME) or application-level data from the MTC server directly if the MTC device is online.

Therefore, two alternatives to randomize triggering point of time-controlled operation can be considered:

1) Randomization of triggering at the MTC device – The MTC device randomizes triggering of the operation over the authorized time-controlled period informed by the network or MTC server.

NOTE: The MTC devices shall not trigger operations due to signalling congestion/overload situations, e.g. based on access control by RAN via broadcast system information.

2) Randomized triggering from the MTC server – Based on the poll model for communications between MTC devices and the MTC server, the MTC server randomizes the initiation of communication for the MTC devices during the time-controlled period provided by the network.

NOTE: The MTC server shall quit triggering operations if indicated from the network due to signalling congestion/overload situations.

Editor's Note: It is FFS how the MTC server can communicate with VPLMN when the MTC device is roaming.

Editor's Note: It is FFS if applying the two above-mentioned approaches concurrently would be more beneficial. In other words, it is FFS if the operation of the MTC device should start immediately after the MTC device is paged or if it would be beneficial that the operation starts only after a randomly selected time.

### 6.21.3 Impacts on existing nodes or functionality

### 6.21.4 Evaluation

## 6.22 Solution – Rejecting connection requests by the SGSN/MME

### 6.22.1 Problem Solved / Gains Provided

See clause 5.12, "Key Issue – Signalling Congestion and Overload Control", more specifically congestion control.

### 6.22.2 General

The solution is applied for both GTP and PMIP based EPC. A number of variants of rejecting connection requests by the SGSN/MME can be distinguished:

**Rejecting connection requests per APN**

The SGSN/MME and/or GGSN/PGW can reject connection requests targeted at a particular APN. When the MTC application uses a dedicated APN, the specific MTC application can be targeted that causes the congestion.

**Rejecting connection requests and attach requests per MTC Group**

The SGSN/MME can reject connection requests targeted at a particular MTC Group. With the attach procedure the MTC Group Identifier can be downloaded as part of the service profile from the HSS into the SGSN/MME. When a connection request is received by the SGSN/MME, the SGSN/MME can find in the service profile if the particular MTC Device is part of a MTC Group that causes congestion. In case only the GGSN/PGW is congested, the SGSN/MME need to be informed about which MTC Group is causing that congestion.

The SGSN/MME can reject attach requests on the basis of MTC Group is the only option. One option is that the MTC Group is downloaded from the HSS during the attach procedure. However this implies the service profile is only downloaded when most of the attach procedure is already done.

Another option would be to add the MTC Group ID to the connection requests and attach requests from the MTC Device. That way the SGSN/MME can easily identify that a particular request comes from a MTC Application that is causing congestion.

**Rejecting service request and attach attempts based on MTC Device provided low priority access indication**

With availability of an access priority indication from the MTC Device the SGSN/MME can take an early decision to reject the request. Depending on internal SGSN/MME congestion mechanisms the SGSN/MME can appropriately treat the "low priority access" (e.g. used by Time Tolerant MTC device) in comparison to other accesses.

The treatment can be performed without inducing or consuming further load in the SGSN/MME and the network as it could be performed prior to the download of the service profile from the HSS. The treatment could include returning an extended back-off time to the MTC Device requesting the "low priority access".

When using SGSN/MME level rejection of devices, care is needed to guard against the possibility that the devices use the result as a soft (or hard) trigger for network reselection. This is because triggering network reselection can lead to the device repeatedly, cyclically attempting access on all the local competing networks and adding load to all of them.

#### **Providing a back-off time and a reject indication to the MTC Device**

To avoid a MTC Device from re-initiating a connection request or attach request immediately after a reject to an earlier request, the SGSN/MME can provide a back off time to the MTC Device in the reject message. If it is the GGSN/PGW that sent the reject originally, the SGSN/MME may append a back off time to the reject message.

In case of large number of MTC Devices, to avoid them from re-initiating access requests simultaneously, the back off time should be randomized. SGSN/MME may randomize the back off time with certain range and assign it to each individual MTC Device directly.

Alternatively, SGSN/MME may just send "back-off time" to MTC device and the MTC device can randomize its local back-off time.

The reject message from the SGSN/MME may contain a reject indication informing the MTC Device about the reject cause. For example a reject indication could inform that there is a signalling congestion at the SGSN/MME, or overload at the GGSN/PGW, or restricted access per requested APN, or the QoS requirements of the requested PDN connection cannot be fulfilled etc.

The reject indication may inform the MTC Devices capable of dealing with multiple connections how to proceed when establishing additional connections. In one example the MTC Devices could be informed that no additional connection to a particular APN shall be established. In another example when the resources at the GGSN/PGW are limited per MTC Device, if the MTC Device has an existing connection and initiates an additional connection establishment, the reject indication can inform the MTC Device about the limited available resources. Additionally the MTC Device may be allowed to keep the already existing PDN connection(s) at time, and/or the MTC Device is allowed to establish multiple connections within the limited resources and/or number of possible PDN connections. In this case, if the MTC Device has an existing connection and has higher priority data to send over new connection, the MTC Device may decide to share the resources among the existing and additional connections or to release the existing connection and establish the new one. When the reject message contains reject indication together with a back off time, the reject indication is valid only during the back off time.

The MTC Device shall not re-initiate a similar request during the back off time depending on the reject indication.

The SGSN/MME may store the back off time for a particular MTC Device and immediately reject any subsequent requests from that MTC Device before the back off time is expired. A new (longer) back off time may be provided to further deter the MTC Device from repeated attempts before its back off time is expired.

Providing a back off time could also be a solution to the issue of recurring (quarter/half) hourly applications. If the MTC Device could identify the recurring applications, it could delay attach request or connection requests for these applications with the back off time. How to identify such recurring applications is unclear.

### 6.22.3 Impacts on existing nodes or functionality

Impact on the SGSN/MME:

Additional functionality for SGSN/MME with this solution includes:

- Rejection of a connection request targeted at a particular APN.

- Rejection of attach and connection requests by MTC Devices belonging to a particular MTC Group.

- Detection if an MTC Device is part of a particular MTC Group (e.g. based on subscription information requested from the HSS/HLR).

- Determining the MTC Group or APN that causes congestion, within SGSN/MME, or upon reception of indication from GGSN/PGW.

- Providing a reject cause including a back off time in the reject messages.

- Providing a reject indication in the reject message.

- Randomization of the back off time that is applicable for a particular MTC Device.

- Determination of the reject indication that is applicable for a particular MTC Device and connection.

- (For SGSN) Indicating MTC Group ID to GGSN.

- (For MME) Indicating MTC Group ID to SGW.

- In the case that the MTC device supports the Time Controlled feature and the subscriber data is available, based on implementation the SGSN/MME may take this into consideration when calculating a wait time.

- In the case of the SGSN/MME rejecting a service request the Mobile Reachable Timer may be compensated by the extended wait time to take into consideration that a periodic TAU/RAU may be suppressed during this period.

Impact on the MTC Device / UE:

Additional functionality for the communication module in MTC Device / UE with this solution includes:

- Not re-initiating further attach or connection requests before the back off time is expired, if timer value is provided by the network.

- Possibly needing to randomize the local back off time according to the back off time received in reject signalling, if such information is provided by the network.

- Determining how the MTC Device deals with additional connections depending on the reject indication.

- Handling of reject causes such that network reselection is not triggered.

- Capability to configure the device with a low priority indication.

Impact on the SGW:

Additional functionality for SGW with this solution includes:

- Forwarding MTC Group ID received from MME to PGW.

- Forwarding low priority device indication to PGW.

- Forwarding the overload/congestion situation indication received from PGW to MME for a particular APN or MTC Group.

- Forwarding a reject cause in the reject messages received from PGW to MME.

- Forwarding a reject indication in the reject messages received from PGW to MME.

Impact on the GGSN / PGW:

Additional functionality for the GGSN and PGW with this solution includes:

- Detecting the overload/congestion.

- Determining the MTC Group or APN that causes overload/congestion.

- Rejection of a connection request targeted at a particular APN.

- Rejection of connection requests by MTC Devices belonging to a particular MTC Group, possibly taking the low priority device indication into account.

- Indicating the overload/congestion situation to SGSN/MME for a particular APN or MTC Group.

- Suggesting value of back off time to SGSN/MME.

- Providing a reject cause in the reject messages.

Impact on the HSS/HLR:

Additional functionality for HSS/HLR with this solution includes:

- Storing the MTC Group Identifier as part of the subscription profile of an MTC Device.

Impact on the PCC:

- Forwarding MTC Group ID received from MME to PGW (via BBERF, PCRF, PCEF).

Editor's Note: It is FFS how PGW exactly indicates the congestion situation back to MME and how SGW(BBERF) correlates such information.

Editor's Note: It is FFS if PCC needs to be used. PMIP mobility related information may be used instead.

### 6.22.4 Evaluation

In the case that the MTC device also supports the Time Controlled feature and the subscriber data is unavailable, the calculated wait time may coincide with a Time Controlled "Forbidden Time Interval". This is not considered significant as the MTC device as per Time Control implementation would access the network at the next available Grant Time Interval.

Benefits:

- Low impact on existing 3GPP RAN standards and products.

- Allows for CN node specific load control in flex or sharing scenarios (in UTRAN and E-UTRAN, but not GSM)

- For roaming scenarios, the SGSN/MME rejects or accepts the connection requests of roaming MTC device based on the load situation and operator's policy.

- Within the network, only requires changes to core network nodes

- By using back-off time, devices are prohibited from generating any more signalling traffic, both in the core network and in the radio network, from requests that would be denied anyway.

- Back-off times allow for peak shaving; making more efficient use of existing capacity.

Drawbacks:

- This solution consumes the RAN and CN resource even at the congestion and overload situation.

- Requires updates to mobiles (their behaviour while a MM/GMM/EMM and/or CM/SM/ESM back off timer is running needs to be defined, specified and tested).

## 6.23 Solution – Low Priority Access Indication

### 6.23.1 Problem Solved / Gains Provided

See clause 5.12, "Key Issue – Signalling Congestion Control", more specifically overload control; and 5.14 "Key Issue - Potential overload issues caused by Roaming MTC devices".

### 6.23.2 General

This solution introduces the concept that access attempts from certain MTC devices or applications (e.g. "time tolerant" utility meters) can be treated as a low priority requests.

In the abnormal case of congestion due to many simultaneous connection requests it is of benefit that the connection requests are rejected as early on in the access procedures such that resources are not consumed or induced further into the network.

NOTE: It is assumed that the network is appropriately dimensioned i.e. congestion or close to maximum resource usage is an abnormal situation.

This solution addresses (unexpected) unacceptable high load resulting from MTC devices in the Low-Priority-Access category. High load resulting from MTC devices out of this category is not covered.

This is a solution that avoids problems in the network that affects both MTC devices that do and MTC devices (in the Low-Priority-Access category) that do not generate an unacceptable high load.

At a high level the following stages occur for UE access from RRC Idle state:

1. Read broadcasted System Information

2. Identifying a RACH opportunity

3. RRC Connection Establishment (E-UTRAN/UTRAN), Channel Request/EGPRS Packet Channel Request (GERAN)

4. Service Request, EPC ATTACH Procedure or GPRS ATTACH/PDP Context Activation)

At step 1 the access class barring mechanism can protect the network.

At step 2 contention based random access procedure exists for identifying an access opportunity on acquiring the Random Access Channel.

At step 3 reception of a priority indication at the access attempt can be used to manage access attempts in RAN (GERAN, UTRAN, E-UTRAN) prior to knowing (decoding and authentication) of the specific identity of the accessing MTC device.

At step 4, reception of a priority indication at the access attempt can be used to manage the requests received in the MME/SGSN early on in the process, i.e. prior to decoding any NAS messages of the accessing "time tolerant" MTC device is attempted. If the request is admitted the indication can also possibly be used to verify the behaviour towards subscription data for the MTC user. An extended use case of the indication can also be to propagate the information for charging purposes.

A priority indication allowing for "Low-Priority-Access" can be used to determine whether to reject the service request or attach attempt depending on the current load.

This indication can be used by MTC devices (e.g. "time tolerant" utility meters) during their normal operating access or access attempts following a power failure (i.e. mass simultaneous registration scenario) as means to request a "Low-Priority-Access". Note that in other scenarios these same devices when accessing the network could use other priorities as required. For example this may be the case of a MTC device supporting multiple MTC applications requiring different priorities (i.e. the MTC application will determine the priority to be indicated during an access attempt).

In the case of overload condition in the RAN, where RACH overload isn't a factor, the RAN may take the decision to reject these requests without further propagating signalling into the core network. In addition, the RAN can use the "low-Priority-Access" indicator to signal a longer back off time to a "low priority access" device compared to any back-off time sent to a normal UE (e.g. one attempting a voice call).

The MME/SGSN can initiate gradual overload procedures by first reducing low priority traffic. The MME/SGSN can notify the RAN to allow all traffic except low priority, using a similar overload mechanism as defined currently for requesting the RAN to reject all non-emergency traffic by sending the OVERLOAD START message.

In the absence of overload condition in the RAN or notification to RAN, the request is eventually transported to the SGSN/MME. Depending on internal MME/SGSN congestion mechanisms the MME/SGSN can appropriately treat the "Low-Priority-Access" request in comparison to other priorities. The treatment can be performed without inducing or consuming further load in the SGSN/MME and for example could be performed prior subscriber profile retrieval.

Also, the "Low-Priority-Access" should be passed to the GGSN/S-GW/P-GW. For Mobile Originating communication, in the absence of overload condition in the RAN and the SGSN/MME and the signal screening at the SGSN/MME for GGSN/S-GW/P-GW, the GGSN/S-GW/P-GW can appropriate treat the request related with the existing session marked as "Low-Priority-Access". For Mobile Terminating call, the S-GW can decide whether to send downlink data notification or not for the existing session marked as "Low-Priority-Access"

This indication conveyed by MTC Devices at the access attempt implies the MTC application is less critical. It can be used as a criterion by the network to determine which MTC Devices/bearers should be detached / deactivated prior to others in case of congestion. When the network status is normal without congestion, the "low priority" MTC Devices will be accepted by the network and bearers will be established. When the network starts to get congested, the already attached "low priority" MTC Devices or established "low priority" MTC bearers can be detached / deactivated first.

This Low Priority Access Indication can be used in combination with Group ID or APN, e.g. when the network decided to detach devices/deactivate bearers belonging to a certain group, the "low priority" MTC Devices within the group can be detached/bearers deactivated first, followed by the remaining devices in the group.

### 6.23.3 Impacts on existing nodes or functionality

In E-UTRAN a new RRC Establishment cause could be introduced. The purpose of the *RRC Establishment* *Cause* IE is to indicate to the eNB the reason for RRC Connection Establishment (ref TS 36.331 clause 6.2.1 - "RRCConnectionRequest" message). Existing values can indicate emergency, highPriorityAccess, mt-Access, mo-Signalling, mo-Data. Following this model of "normal", emergency and high priority causes it is proposed that some MTC device accesses could be viewed as "Low-Priority-Access" as compared to the existing establishment causes. The *RRC establishment cause* IE is as currently specified (ref TS 36.413 clause 9.1.7.1) forwarded to the MME in the "Initial UE message" over the S1-AP protocol.

In the UTRAN case a new *establishment cause* could be used by MTC "time tolerant" devices in the RRC Connection Request. Signalling would be impacted to include the establishment cause such that SGSN can be made aware of a low priority access (e.g. by a MTC "time tolerant" device).

NOTE 1: the existing UTRAN establishment cause "Originating Low Priority Signalling" is used for mobile originating SMS and is unsuitable for re-use as this code-point.

For the GERAN case a priority indication may be introduced in the access message (e.g. EGPRS Packet Channel Request or by partial re-coding of the existing Channel Request message) to indicate when an access is attempted by an MTC device and the priority of the corresponding MTC message requiring transmission. The priority indication should allow for the equivalent of a "Low-Priority-Access". MM/GMM Signalling would be impacted to include a priority indication such that MSC/SGSN can be made aware of a low priority access (e.g. by a MTC "time tolerant" device).

NOTE 2: The above mechanisms are provided as examples. If the solution is supported, it is the responsibility of the RAN/GERAN to specify the messages and parameters in which the low priority indicator would be passed.

For E-UTRAN/UTRAN/GERAN, the OVERLOAD START message would need to support the ability to request RAN to reject low priority access requests.

For E-UTRAN, UTRAN and GERAN it is likely that the "low priority access" codepoint should be used for EMM, GMM and MM signalling as well as for initiating data transfer/responding to paging. However, some further study on this aspect may be needed.

The SGSN/MME should include the "Low Priority Access" indicator in the session create message in order to notify it to GGSN/S-GW/P-GW. A GGSN/S-GW/P-GW that experience overload, may decide to reject any additional "Low Priority" session creation requests in order not to increase its number of sessions and any potential traffic related to these sessions. If a GGSN/S-GW/P-GW reject a session create request due to an overload condition, a specific reject cause shall be indicated back to the SGSN/MME so that the SGSN/MME can take appropriate action (e.g. try another GGSN/S-GW/P-GW instead or reject with a wait time).

A low priority access indication usage control parameter may be pre-configured (e.g. at manufacturing) or set via OMA device management in the MTC Device SIM/USIM to allow for:

- MTC Device that uses the low priority access indication for all its access attempts

- MTC Device that uses the low priority access indication for all its delay tolerant accesses attempts, but which may use other priorities for services that require immediate response

The MTC Device low priority indication usage could be according to the Service Level Agreement (SLA) established between the mobile operator and the MTC service provider.

SGSN/MME/GGSN/P-GW are required to store the "Low-Priority-Access" indication for each attached MTC Device. SGSN/MME need to forward this indication to GGSN/P-GW.

### 6.23.4 Evaluation

Benefits:

- Should be possible to easily add parameters/mechanisms to the UTRAN and E-UTRAN RRC protocol and to GERAN although the network's support/non-support for these new parameters may probably need to be broadcast.

NOTE: Whether necessity to broadcast network's support/non-support for these new parameters should be decided at the stage 3.

- Works in a roaming environment. A network upgraded with "low priority" functionality can take advantage of this as soon as there are terminals also supporting this regardless if terminals are roaming or not.

- Low impact on existing 3GPP standards and products and may be feasible in Rel-10.

- allows for CN node specific load control in flex or sharing scenarios

- Initially provides, from the time RAN decides to start rejecting low-priority-access requests until the first low-priority-access barring is broadcast in system information, a faster way to protect from overload compared to mechanisms relying on broadcasted system information (e.g. ACB)

- Allows GGSN/S-GW/P-GW to handle signalling overload appropriately

- Allows the UE flexible access to the network by indicating the priority that is suitable for use (e.g., low priority MTC service vs normal priority when not in MTC low priority mode).

- Provides a criterion for the network to determine the MTC Devices to be detached / bearers to be deactivated for congestion control.

Drawbacks:

- Doesn't allow to switch off specific groups or applications (vs. broadcasting in system information which can prevent low-priority-access requests from devices that have not received access rejections).

- the node specific load control or network sharing specific control might not work if the device signals the IMSI instead of temporary IDs e.g. during PLMN changes

- As it bases on UE individual signalling it might not be possible to completely avoid Radio Resource congestion. There are also related work in RAN e.g. usage of concentrators.

- In the case that the MTC device also supports the Time Controlled feature, the calculated wait time may coincide with a Time Controlled "Forbidden Time Interval". This is not considered significant as the MTC device as per Time Control implementation would access the network at the next available Grant Time Interval.

## 6.24 Solution - Directly Reporting to MTC Server from CN entity

### 6.24.1 Problem Solved / Gains Provided

In the MTC Monitoring solution, clause 5.10 "Key Issue – MTC Monitoring" and 6.9 "Solution – MTC Monitoring – General", the MTC Event Reporting entity (e.g. SGSN/MME or GGSN/PGW or PCRF) is not aware of the MTC Server identity, thus it cannot send the MTC Event Report to the MTC Server.

### 6.24.2 General

In this solution, the MTC Server identity (e.g. FQDN or IP address) is stored in the HLR/HSS as part of MTC subscription per MTC device or per MTC group, and is downloaded to the SGSN/MME through Insert Subscription Data procedure. The SGSN/MME then stores this MTC Server identity.

If the CN entity for MTC Event Reporting is the GGSN/PGW, the SGSN/MME transfers the MTC Server identity to the GGSN/PGW through Create PDP Context Request / Create Session Request, or carries the MTC Server identity within the MTC Event Report when it sends MTC Event Report to the GGSN/PGW, and PCEF may send the Event Report to PCC if GTP is used over S5/S8. If PMIP is used, these information are transferred via PCC i.e. BBERF sends MTC Event Report to PCRF.

If the CN entity for MTC Event Reporting is the PCRF, after receiving the MTC Server identity, the GGSN/PGW then transfers the MTC Server identity to the PCRF through PCC procedure, or carries the MTC Server identity within the MTC Event Report when it sends MTC Event Report to the PCRF. The PCRF uses the MTC Server identity to send MTC Event Report.

If the MTC server is out of the operator control, a security connection between the CN entity and the MTC server may be needed.

Editor's Note: It is FFS how to setup a security connection to the MTC Server, and where the security connection information is stored and how to establish the secure connection.

Editor Note: It is FFS how to report MTC events to multiple MTC servers.

### 6.24.3 Impacts on existing nodes or functionality

HLR/HSS:

- The HLR/HSS stores the MTC Server identity as part of MTC subscription.

SGSN/MME:

- SGSN/MME stores the MTC Server identity

- The SGSN/MME includes the MTC Server identity in the Create PDP Context Request / Create Session Request.

GGSN/PGW:

- The GGSN/PGW includes the MTC Server identity during the Gx session procedure to the PCRF.

SGW(BBERF)

- The BBERF forwards the MTC Server identity during the Gxx session procedure to the PCRF, if PMIP is used over S5/S8.

PCRF

- The PCRF receives MTC Server Identity from PCEF (if GTP is used over S5/S8) and from BBERF (if PMIP is used over S5/S8)

- The PCRF uses the MTC Server identity to send MTC Event Report.

### 6.24.4 Evaluation

## 6.25 Solution - Reporting to MTC Server through the intermediate node

### 6.25.1 Problem Solved / Gains Provided

See clause 6.24.1.

### 6.25.2 General

In this solution, there is an operator controlled intermediate node (e.g. MTC Monitoring GW or IWKF) deployed to collect MTC event reports. The CN entity for MTC event reporting (e.g. the SGSN/MME or GGSN/PGW or the PCRF) sends MTC Event Report to this intermediate node, and the intermediate node then gets the corresponding MTC server identity and forwards the MTC Event Report to that MTC server.

The CN entity for MTC event reporting can get the identity of this intermediate node through the following methods:

A) Static configuration based on the local configuration for the home PLMN or the roaming agreement for the visited PLMN.

B) The MTC subscription from HLR/HSS.

The CN entity for MTC event reporting needs not know where the MTC server is, the intermediate node will find MTC server through the following methods:

The intermediate node locally configures the MTC Server identity.

Or, the MTC Server(s) contact the Intermediate Node (e.g. the3GPP PLMN-MTC Server IWK Function) and register. The Intermediate node then requires no configuration or information from the CN to locate the MTC Server(s).

If the MTC server is out of the operator control, the security connection between the intermediate node and the MTC Server may be needed.

Editor's Note: It is FFS how to setup a security connection to the MTC Server, and where the security connection information is stored.

Editor's Note: Whether there are changes to the roaming architecture and message flow are FFS.

Editor's Note: It is FFS whether new interface between the CN entity and the intermediate node is introduced.

Editor's Note: It is FFS how to report MTC events to multiple MTC servers.

### 6.25.3 Impacts on existing nodes or functionality

HLR/HSS:

- The HLR/HSS stores the intermediate node identity as part of MTC subscription if the CN entity for MTC event reporting gets the intermediate node identity from HLR/HSS.

CN nodes for MTC event reporting (SGSN/MME, GGSN/PGW, PCRF):

- The CN entity for MTC event reporting shall send MTC Event report to the intermediate node (e.g. MTC Monitoring GW or IWKF) located in the HPLMN.

- A new network entity (e.g. MTC Monitoring GW) may be introduced and new interfaces are introduced.

Editor's Note: Whether there are additional impacts in roaming scenario is FFS.

### 6.25.4 Evaluation

## 6.26 Solution – Rejecting RRC Connection and Channel Requests by the eNodeB/RNC/BSS

### 6.26.1 Problem Solved / Gains Provided

See clause 5.12, "Key Issue – Signalling Congestion Control", more specifically overload control, and 5.14 "Key Issue – Potential overload issues caused by Roaming MTC devices".

### 6.26.2 General

This solution introduces the concept that accesses from certain MTC devices (e.g. "time tolerant" Utility meters) can be treated as a low priority access and could be rejected with an extended wait time.

In the abnormal case of massive simultaneous connection requests it is of benefit that the connection requests be rejected as early on as possible in the access procedure such that resources are not consumed or induced further into the network.

NOTE: It is assumed that the network is appropriately dimensioned i.e. congestion or close to maximum resource usage is an abnormal situation.

This solution addresses (unexpected) unacceptable high load resulting from MTC devices in the Low-Priority-Access category. High load resulting from MTC devices out of this category is not covered.

This is a solution that avoids problems in the network that affects both MTC devices that do and MTC devices (in the Low-Priority-Access category) that do not generate an unacceptable high load.

In the case of priority indication being received from the MTC Device the RAN (E-UTRAN, UTRAN, GERAN) has the opportunity to reject the connection request with a wait time that is appropriate for the access priority indicated by the MTC Device.

It is proposed that the existing wait time range in the rejection messages be extended to allow better control of such MTC "Time Tolerant" devices.

It is proposed that a new "extended wait time" could potentially range in the order of minutes or even hours.

With this potentially wide timer range the RAN could have for example the logic to assign a wait time ranging from 5 to 60 minute or even from 1- 24 hours to better control the MTC devices and ensure an even distribution of future incoming requests of low priority accesses into the system.

Some care is needed to ensure that these rejections do not lead to network reselection attempts that repeatedly load the local competing networks.

To ensure an even distribution of the re-initiated access attempts by a large group of "low priority access" MTC Devices, it is proposed that, when allocating the extended wait time for a MTC Device, eNB/RNC/BSS could apply randomization of the extended wait time within the overall maximum allowed wait time, and optionally allocate longer wait times to "low priority access" MTC Devices compared to that for normal MTC Devices.

The randomized wait times allocated to MTC Devices should be different from one another as much as possible. On the other hand, for each MTC Device, the start time of re-initiation is the current time of rejection + randomized wait time. When the wait time is being randomized, the current time of rejection should also be taken into account to ensure that the start time of re-initiation of different MTC Devices is sufficiently different from one another.

Alternatively, eNB/RNC/BSS could send one "reference wait time" to the MTC Devices, and each MTC Device calculates its own randomized offset time independently. Then for each MTC Device, the start time of re-initiation could be calculated as current time of rejection + reference wait time (from the network) + randomized offset (calculated by individual MTC Device).

### 6.26.3 Impacts on existing nodes or functionality

The E-UTRAN, UTRAN and GERAN would be impacted by the introduction of an extended and randomized wait time whose range would extend beyond the following documented values:

- For E-UTRAN the RRC Protocol Spec (36.331 v.9.1.0) shows a waitTime of between 1-16 seconds for the RRCConnectionReject.

- For UTRAN the RNC (25.331 RRC UTRAN) can return an RRC Connection Reject which includes a waitTime of between 0-15 seconds.

- For GERAN the BSS (TS 44.018 RRC) can return an IMMEDIATE ASSIGNMENT REJECT which includes wait indication octet (i.e. 0-255 seconds).

E-UTRAN, UTRAN and GERAN devices and networks extended and randomized wait time support would benefit from support of the Low priority access value (see solution "Low Priority Access Indication") that is indicated by the MTC Device when the MTC Device attempts to connect to the network and evaluated by the RAN when allowing/rejecting the request.

MME/SGSN in the case of MTC devices shall set the mobile reachable timer to be longer than the periodic update timer used by an MS and may take into consideration (i.e. through configuration) the value of the extended wait time that the RAN may use when rejecting channel requests in overload conditions.

MTC Devices receiving an extended wait time shall start any necessary the periodic update procedure following expiration of the extended wait time.

Impact on the MTC Device/UE

Additional functionality for the communication module in MTC Device/UE for this solution includes:

- Possibly randomizing the local offset time according to the reference wait time received in RRCConnectionReject/ IMMEDIATE ASSIGNMENT REJECT, if such information is provided by the network.

- Not re-initiating further attach/connection requests before the extended wait time is expired.

### 6.26.4 Evaluation

Benefits:

- Based on an existing concept of a wait time parameter in the E-UTRAN, UTRAN and GERAN protocols.

- Works in a roaming environment as solution is not dependent on coordinating any specific MTC application level identifiers between operators. Instead broad control is possible in the serving network based on devices making access attempts as a low-priority-access. If a rejection is required an extended wait time can be returned for those accesses.

- Low impact on existing 3GPP standards and products and may be feasible in Rel-10.

- allows for CN node specific load control in flex or sharing scenarios (in UTRAN and E-UTRAN, but not GSM)

- Provides a faster way to react to varying levels of overload/unused capacity compared to mechanisms relying on broadcasted system information (e.g. ACB.

Drawbacks:

- Doesn't allow to target specific MTC groups or applications

- Allows each unique low-priority-access device to send a connect request followed by a corresponding reject sent by the RAN, thus adding to the current congestion load in the RAN (vs, broadcasting which can prevent the remaining low-priority-access devices from sending any access requests).

- In the case that the MTC device also supports the Time Controlled feature, the calculated wait time may coincide with a Time Controlled "Forbidden Time Interval". This is not considered significant as the MTC device as per Time Control implementation would access the network at the next available Grant Time Interval.

- Doesn't protect the core/centralized network elements in the case that, say, two M2M mobiles per cell access every cell in the network at the same time.

## 6.27 Time Control Solution Summary

This solution considers the Time Control MTC Feature Solutions thus far included in the TR and several that have not yet been included. The goal is to make progress towards understanding the solution space better and facilitating a comparison of alternatives. This solution neither replaces other existing solutions in the TR nor do the summarized solutions necessarily suffice as a 'key issue solutions.'

Table 6.27-1

| Solution | Status | Randomization of Communication Window in the Grant Time Interval | Informs MTC Device of altered Grant Time Interval | Informs MTC Server or User of altered Grant Time Interval | Enforcement of Grant Time Interval and Forbidden Interval | Information Storage of Grant Time Interval and Forbidden Interval |
| --- | --- | --- | --- | --- | --- | --- |
| 1) Network Access Control by the PLMN | 6.7 | Not considered in solution 6.7 yet. | (1) The MTC Server via application level data  (2) MME/SGSN via NAS initially or when the time period changes (accepting the first access outside the interval or informing when to use the network.) | "The network provides the information." | GGSN/P-GW (for charging and stopping data transmission.) MME/SGSN may prevent access outside of the Grant Time Interval. | HLR/HSS, SGSN/MME may alter the Grant Time Interval to conform with local policies. |
| 2) "Randomized Time Control"  [S2-102404] | tdoc | Either in the HSS or in the MME or SGSN (if local policy is applied.) A time window is selected within the Grant Time Interval to uniformly distribute access | (1) O&M procedure (2) NAS procedures as per 6.7 or during Grant Time Interval initiated by the MME/SGSN (notifying the MTC Device). Also synchronizes the device with respect to the MME/SGSN. | Not discussed | As 6.7 | In HSS/HLR (the time window is stored along with the grant time interval and forbidden interval). |
| 3) "Time control for MTC Time Controlled"  [S2-102588] | tdoc | The MME or SGSN selects a random start time and duration. Local policy may reset the start time and duration to a new value. | NAS procedure communicate the time window during attach or connection request. A time stamp may be added by the network to synchronize the MTC Device to the network | Not discussed | As 6.7 | In HSS/HLR (the grant time interval and forbidden interval) |
| 4) "Allowed Time Period after TAU/RAU" [S2-102572] | 6.17 | The TAU or RAU will occur randomly within the Grant Time Interval. | "The EPS network configures the MTC Device ... according to operator requirements and MTC subscription options."  NAS will be used to inform the length of the communication window. | Not discussed | Not discussed | Presumably in the HSS/HLR for subscription options. |
| 5) "Randomized triggering of time-controlled MTC operations" | 6.21 | 1) the MTC Device  2) the MTC server | interval from the network or the MTC Server | by the network | Not discussed | Not discussed |
| 6) PCRF based network access control [S2-102475] | tdoc | not discussed | The PCRF informs the MTC Device during IP CAN session establishment | The PCRF receives the grant time interval from the SPR | The PCRF rejects IP CAN sessions outside of the grant time interval or terminates IP CAN sessions that exceed the time limit. | SPR |
| 7) Time control according to MTC Device Identifiers [S2-102330] | tdoc | Use of MTC Identifier to randomly distribute at a fixed point (based on a known start time and a randomized offset) | not discussed | not discussed | not discussed | not discussed |
| 8) Time controlled feature via Operator and MTC Business Agreements [S2-102436] | tdoc | not discussed (It is asserted that the application will be 'well behaved' and randomize communication through the grant time interval.) | not discussed | off-line (the MTC User informs the MTC Server) | not discussed | not discussed |
| 9) MTC Request to Release Resources [S2-102519] | tdoc | not discussed | the network sends this using NAS as part of detach or S1 release.  The MTC Device may propose a time. | "The network then ... forwards the ... notification to the MTC User" | not discussed | not discussed |
| 10) Proactive congestion control  [S2-102225] | tdoc | Randomization algorithm in the device | Periodically through broadcast | not discussed (the network or the UE may notify the MTC Server/User when communication is granted) | not discussed (as 6.7) | Not necessary when this method is used. |

## 6.28 Solution - Access Control by RAN

### 6.28.1 Problem Solved / Gains Provided

See clause 5.12, "Key Issue – Signalling Congestion Control", more specifically congestion control and overload control and clause 5.14, "Key Issue – Potential overload issues caused by Roaming MTC devices."

### 6.28.2 General

To avoid and handle the overload situations caused by MTC Devices, the MME/SGSN can send OVERLOAD START message to the RAN node, O+M action can be directed to the RAN node, and/or internal congestion alarm in RAN node can trigger the broadcasting of access control for MTC Devices to avoid further access to the network. The OVERLOAD START message, O+M action and internal congestion alarm in the RAN can include specific MTC Access Class Barring (ACB) overload actions as follows:

- Coarse-grained access control for MTC Devices with "Low-Priority-Access". MME/SGSN, O+M action and/or internal RAN congestion alarm will request MTC access control with indication of "Low-Priority-Access". Based on that, RAN will broadcast "access barring for MTC Devices with Low-Priority-Access" in system information.

- Fine-grained access control for MTC Devices with specific group. MME/SGSN O+M action and/or internal RAN congestion alarm will provide group related access control information, (e.g. an MTC Group or specific APN,) to RAN node. Based on that, RAN node will broadcast "access barring for MTC Devices with specific group" in the system information; or

- Coarse-grained access control for MTC Devices with specific "PLMN type". MME/SGSN, O+M action and/or internal RAN congestion alarm will provide PLMN type related control information, i.e. "MTC Devices that are not on their HPLMN or a PLMN in the (U)SIM's preferred PLMNs list", "MTC Devices that are not on their HPLMN or an Equivalent HPLMN", "MTC Devices that are not on their HPLMN" and "all MTC Devices",, to RAN node and/or RAN will determine from internal. Based on that, RAN node will broadcast "access barring for MTC Devices with specific PLMN type" in the system information.

MTC access control with different granularities could be triggered by signalling thresholds in the RAN, SGSN/MME and/or GGSN/PGW. In the case of the GGSN/PGW, the GGSN/PGW informs the SGSN/MME when a congestion threshold is exceeded. P-GW/GGSN can reject the connection request for a particular MTC group, e.g. a specific APN, when the congestion control policy is trigged, and indicates a delay value to the MME/SGSN in the reject message. The delay value is set by P-GW/GGSN for the requested MTC group. By receiving the reject message, MME/SGSN can reject the connection request described under "6.22 Solution – Rejecting connection requests by the SGSN/MME" for the corresponding MTC group until the delay value expires, and the MME/SGSN can also be triggered to provide the congestion indication to RAN nodes.

NOTE 1: This functionality is supported for both PMIP and GTP based S5/S8.

Editor's note: It is FFS if and how access control for MTC Devices with specific groups can be triggered by signalling thresholds in the RAN.

Editor's note: This functionality is supported for both PMIP and GTP based S5/S8. It is FFS how PGW informs its congested status to the SGSN/MME.

When a SGSN/MME needs to trigger a MTC access control due to the MME/SGSN's load situation or the congestion indication received from P-GW/GGSN,, the SGSN/MME sends the specific OVERLOAD START message to the RANs (eNodeBs/RNCs/BSCs) specifically for MTC Devices, i.e. OVERLOAD START message with an indication of the type (i.e. "Low-Priority-Access" or one of the "PLMN type" options) or group (e.g. MTC Group Identifier) of MTC access to be barred and any load status information.

Similar to general MME overload control procedures in TS 23.401 [5], the set of eNodeBs/RNCs/BSCs to send an OVERLOAD START message should be randomly selected (so that if two SGSNs/MMEs within a pool area are overloaded, they do not both send OVERLOAD START messages to exactly the same set of eNodeBs/RNCs/BSCs) and, in total, be proportional to reflect the amount of load that the SGSN/MME wishes to reduce. In addition, the set of eNodeBs/RNCs/BSCs to consider sending an OVERLOAD START message may be limited to a particular location area or subset of eNodeBs/RNCs/BSCs (e.g. where MTC Devices of the targeted type are registered).

The RAN uses the information from the SGSN/MME in the OVERLOAD START message, from the O+M action or from the internal RAN congestion alarm t to determine if and when to broadcast the corresponding MTC ACB information in the system information to the Ues. Any barring factor and/or barring time or functional equivalent included in the barring information will be derived internally by RAN (similar to general ACB) but should take into consideration any load status information provided by the SGSN/MME or input from the O+M action.The RAN uses the information from the SGSN/MME in the OVERLOAD STOP message, from the O+M action, or from internal RAN congestion alarms to determine if and when to stop broadcasting the corresponding MTC ACB information in the system information to the Ues. The RAN should not have to wait for indication from or be prevented by SGSN/MME from starting or stopping the broadcast of a particular MTC ACB action.

NOTE 2: OVERLOAD START/STOP messages from SGSNs/MMEs to RAN are considered amongst other inputs that can influence the decisions RAN ultimately makes in management of MTC access barring.

When using pooling of CN nodes, the RAN shall only broadcast a SGSN/MME-triggered MTC overload action when all connected MMEs/SGSNs from the same pool area have enabled the MTC overload action. When only a subset have triggered the MTC overload action, the RAN shall instead reject RRC connection requests, as described in clause 6.26, for specific access to a barring SGSN/MME from a MTC Device type or group that the SGSN/MME is barring. An O+M or internally RAN-triggered MTC overload action can be broadcasted regardless of the set of SGSNs/MMEs that have enabled the same MTC overload action.

The MTC Device which is going to access the network will receive the broadcasted system information for MTC access barring and uses this information to determine whether this access is barred or not. If so the corresponding MTC Devices will delay the access to the network. Subsequent initial access attempts to the network will be randomized by each MTC Device using the last barring time or equivalent value(s) provided by the RAN.

Editor's note: Broadcasting access control barring information in a large area, e.g. whole PLMN, caused by GGSN/PGW congestion should be avoided.

A MTC Device priority (i.e. "low" or "normal") shall be configured in a MTC Device in order to determine when "Low-Priority-Access" is barred by the network,

Editor's note: It is FFS how to configure the MTC access priority in the MTC Device, e.g. SIM OTA or OMA DM.

Editor's note: It is FFS how MTC Device priority will be applied to all applications on the device for Rel-10.

The operator may configure in a MTC Device (using OMA DM) a penalty level to be applied (i.e. weighted) to the received barring factor and/or barring time or equivalent when MTC Low-Priority-Access is barred by all MTC Devices.

NOTE: When using a penalty level, computed barring values should not be less than originally ordered by RAN in order to prevent an MTC Device from gaining an advantage in access.

### 6.28.3 Impacts on existing nodes or functionality

Impact on the RAN:

Additional RAN functionality for RAN-triggered solution includes:

- For coarse-grained MTC access barring:

- Determining when overall congestion situation within the RAN warrants starting/stopping a particular MTC ACB action

- Broadcasting MTC access barring with the indication of the type (i.e. "Low-Priority-Access or one of the "PLMN type" options)

- For fine-grained MTC access barring:

- Determining the MTC Group or APN that is causing congestion within RAN.

- Determine the barring time and/or barring factor or equivalent for a new MTC access barring start operation.

- Broadcasting MTC access barring with the indication of the type or group of MTC access to be barred, barring time and/or barring factor or equivalent in the system information to the Ues.

- Control via O+M input to the RAN node is less 'automatic' but impacts fewer network entities and may attract the human/management attention needed to handle cases of very high overload.

Additional RAN functionality for CN-triggered solution includes:

- Receive the OVERLOAD START/STOP messages from the SGSN/MME with the indication of the type (i.e. "Low-Priority-Access" or one of the "PLMN type" options) or group of MTC access to be barred.

- Determine if CN provided OVERLOAD START/STOP request influences MTC ACB and/or RRC rejection operations for the requesting CN node and other CN nodes sharing a pool area with the requesting CN node.

- Determine the barring time and/or barring factor or equivalent for a new MTC access barring start operation.

- Broadcasting MTC access barring with the indication of the type (i.e. "Low-Priority-Access" or one of the "PLMN type" options) or group of MTC access to be barred, barring time and/or barring factor or equivalent in the system information to the Ues.

Impact on the SGSN/MME

Additional SGSN/MME functionality for CN-triggered solution includes:

- For coarse-grained MTC access barring:

- Determining when overall congestion situation, within SGSN/MME or upon reception of congestion indication from GGSN/PGW, warrants starting/stopping a particular MTC ACB action.

- For fine-grained MTC access barring:

- Determining the MTC Group or APN that is causing congestion, within SGSN/MME, or upon reception of indication from GGSN/PGW.

- (For GGSN/PGW-triggered) Indicating MTC Group ID to GGSN/SGW

- Determining the proportion and specific set of RANs to send a new MTC ACB action.

- Sending the OVERLOAD START/STOP messages to the targeted RANs specifically for MTC Devices with the indication of the type (i.e. "Low-Priority-Access" or one of the "PLMN type" options) or group of MTC access to be barred.

- For penalty level configuration:

- A mechanism is required to configure a penalty level in the MTC Device to be used for processing MTC access barring information for Low-Priority-Access attempts by the MTC Device.

NOTE: The detailed message name and indication parameters should be specified in stage 3.

Impact on the HSS/HLR

Additional HSS/HLR functionality for CN-triggered solution includes:

- For fine-grained MTC access control:

- Storing the MTC Group Identifier as part of the subscription profile of an MTC Device.

Impact on the SGW

Editor's note: It is FFS whether such information may be transferred via PCC, if PMIP is used on S5/S8.

Additional SGW functionality for PGW-triggered solution includes:

- For coarse-grained MTC access barring:

- Forwarding the overall PGW congestion situation indication received from PGW to MME

- For fine-grained MTC access barring:

- Forwarding MTC Group IDs received from MME to PGW

- Forwarding the congestion situation indication received from PGW to MME for a particular MTC Group or APN

Impact on the GGSN/PGW

Additional GGSN and PGW functionality for GGSN/PGW-triggered solution includes:

- The GGSN/PGW needs to provide the different overload actions for MTC Devices to the SGSN/MME node.

- For coarse-grained MTC access control:

- Detecting the overall GGSN/PGW congestion condition.

- Indicating the overall GGSN/PGW congestion situation to SGSN/MME.

- For fine-grained MTC access control:

- Receiving MTC Group ID from SGSN/SGW.

- Determining the MTC Group or APN that is causing congestion within GGSN/PGW.

- Indicating the congestion situation within GGSN/PGW to the SGSN/SGW for a particular MTC Group or APN.

Impact on the MTC Device / UE

Additional functionality for the communication module in MTC Device / UE with this solution includes:

- The MTC Device needs to recognize the different MTC specific access control types and groups that are applicable to it.

- The MTC Device uses the latest received MTC access barring information to determine if, and for how long, not to initiate any access requests.

- For penalty level configuration:

- A mechanism is required to configure a penalty level in the MTC Device to be used for processing MTC access barring information for Low-Priority-Access attempts by the MTC Device.

### 6.28.4 Evaluation

Benefits:

- RAN and core network resource consumption can be avoided during congestion situation and there will be no further AS and NAS signalling initiated from the targeted, access barred MTC Devices.

- Can be used for both congestion control as well as overload control as described in clause 5.12.

- Can reuse existing UE functionality (e.g. GSM Immediate Assignment Reject already specifies Wait Times out to 255 seconds).

- With broadcasting MTC access barring it may be possible to completely stop congestion even if RRC and/or NAS signalling are almost instantaneously overwhelmed with access attempts.

- Different combinations of MTC ACB actions provides for a low impact on existing 3GPP standards and products that may be feasible in Rel‑10 (e.g. coarse-grained via RAN and/or SGSN/MME triggering) while allowing reuse for expanded functionality in Rel‑11 (e.g. fine- and coarse-grained via RAN, SGSN/MME and/or GGSN/PGW).

- Complements RRC and NAS access request rejection mechanisms i.e. initial few requests rejected and remaining subsequent requests prevented through MTC access barring.

- Barring time randomization or equivalent prevents simultaneous subsequent initial access attempts by a previously blocked group.

- Provides solution for "unhappy" VPLMN operator to handle signalling and VLR space congestion from roaming MTC Devices.

- For RAN triggered options:

- Does not impact CN entities (coarse-grained options).

- Permits the VPLMN to activate barring because of a situation reported by another PLMN operator and/or due to severe abnormalities in the levels of core network signalling to particular HSS(s).

- For CN triggered options:

- Allows aggregated MTC specific congestion at the SGSN/MME and/or GGSN/PGW to be stopped and/or prevented without guaranteed signalling bandwidth for worse-case individualized access request rejections.

- For O+M triggered options:

- An effective yet relatively simple solution for catastrophic overload is probably the use of O+M controlled "access class barring" functionality that can be used to bar e.g.:

- "low value" M2M devices that are not on their HPLMN or a PLMN in the (U)SIM's preferred PLMNs list;

- "low value" M2M devices that are not on their HPLMN or an Equivalent HPLMN;

- "low value" M2M devices that are not on their HPLMN;

- "low value" M2M devices;

- This may be achievable with just 2 broadcast bits. Reducing the core network load by X% can be achieved by the O+M barring of X% of the base stations/Node Bs/eNodeBs.

- For coarse-grained options:

- Not dependent on implementation of MTC Group Identifier support.

- Allows for efficient encoding of MTC access barring information that should fit in the spare bits of pre-existing System Information messages used for Access Class Barring.

- For fine-grained options:

- Does not impact/block MTC applications that are not causing a problem.

- When a MTC application uses a dedicated APN, the specific MTC application that causes the congestion can be targeted.

- For penalty level configuration:

- When broadcast MTC barring information includes uniform barring info toward all MTC Devices, a penalty level can be used to discriminate some MTC Devices (i.e. this selectively assigns MTC Devices an advantage or disadvantage).

Drawbacks:

- The broadcast information for access barring needs to be enhanced to restrict the further MTC device access with different granularity triggered by RAN, SGSN/MME or GGSN/PGW.

- Initially, from the time determined to start rejecting and barring connect requests from MTC Devices from a particular group until the barring is broadcast, not as fast as RRC and NAS signalling access request rejections.

- For CN-triggered options:

- When using pooling of core network nodes, care is needed in the use of ACB functionality as it can limit load on all MMEs/SGSNs/MSCs in the pool.

- Added complexity during MME/SGSN overload to determine cause of overload type (e.g. Group/APN, PLMN type and/or "Low-Priority-Access") in order to request specific MTC overload action when not combined with rejecting connection requests by the SGSN/MME in clause 6.22 (can uses same mechanisms within CN to make this determination).

- Added complexity in RAN to evaluate CN MTC overload action request amongst status of other CNs, O+M request and internal RAN MTC overload process.

- For coarse-grained options:

- Impacts MTC applications that are not causing a problem.

- For fine-grained options:

- Requires enhancements for broadcasting one or more unique MTC Group Identifiers.

- Requires enhancements to HLR/HSS to store the MTC Group Identifier as part of the subscription profile of an MTC Device

- Requires new mechanisms for detecting and indicating between nodes the MTC Group or APN that is causing congestion

## 6.29 Solution – IP address assignment mechanisms

### 6.29.1 Problem Solved / Gains Provided

See clause 5.3. "Key Issue – Ipv4 addressing".

NOTE: The stage 1 requirement that an MTC Server in a public address space can successfully send a mobile terminated message to the MTC Device inside a private Ipv4 address space is not addressed by this solution.

### 6.29.2 General approach based on existing standards

This solution shows how the key issue Ipv4 addressing can be addressed based on the mechanisms in the existing standards. Minor further optimization might be required. The alternatives outlined should be seen as examples and additional alternatives or variants may exist. An operator can choose to deploy one of the configurations for all its customers or deploy different configurations for different customers.

The MTC server is either deployed by the PLMN operator or by an application provider who owns an MTC Server and uses a specific APN assigned by the PLMN. In both cases a tunnelling mechanism is used between the GGSN/P-GW and the PDN of the MTC server to allow carrying the IP packets enabling assignment of private IP addresses to the MTC Devices. The tunnelling allows for connecting the PLMN with the MTC server(s) using public IP networks. Furthermore that tunnelling allows for setting up private network with multiple GGSNs/P-GWs and multiple MTC servers where every GGSN, P-GW or MTC server can be deployed at a different location. By using a separate APN per application (provider) the MTC servers from different applications can use the same overlapping private IP addresses as needed without the need for the network to implement a NAT function as the MTC devices and MTC servers belonging to one application share the same private IP address space.

Such a segregation of the traffic also reduces the motivation for subscribers to try to use this subscription for other purposes (e.g. free Internet service) since they cannot reach the public Internet. It also helps to simplify other operational issues, such as monitoring that all the MTC devices obey potential access restrictions like being active only during the network's low traffic periods. Traffic within this private intranet at other times would indicate the devices or applications are not working properly.

A PGW/GGSN can serve one or multiple APNs. A GGSN/PGW can be configured to use an AAA server for address allocation and protocol configuration options notification. When serving multiple APNs the PGW/GGSN may be configured with an AAA server per APN. The use of the AAA server and the communication and security feature needed to dialogue with this / those AAA server(s) e.g. tunnel, IPSec security association are specified in TS 29.061 [4].

The following figure shows just one MTC server per PDN/APN. There may be however multiple MTC Servers in the same PDN/APN.



Figure 6.29.2-1: IP address assignment when the MTC Server is owned by the MNO or by a M2M Application Provider using a specific dedicated APN

In clause 6.29.5, the MTC Server is located on Internet (i.e. using an APN providing Internet connectivity) and hence no tunnelling is required between the GGSN/PGW and the MTC Server. This solution in clause 6.29.5 also assumes no NAT is used and is hence optimized for usage of Ipv6 addresses or public Ipv4 addresses.

### 6.29.3 IP address assignment by the PDN of the MTC server

A RADIUS or Diameter client at the GGSN/P-GW can obtain an IP address from the MTC server (providing an AAA server) upon receiving a PDP context/PDN connection request with the APN corresponding to the MTC server and assign that address to the MTC Device. The GGSN/P-GW indicates an MTC device provided PDN specific ID, an MSISDN or an IMSI to the MTC server when obtaining an IP address. Thereby the MTC server knows the IP address for an MTC device.

The application in the MTC Device may provide a PDN specific id potentially together with a related password in e.g., the PCO IE at PDP Context /PDN Connection establishment. Alternatively a PDN specific ID may be provided by the SGSN/MME at PDP Context /PDN Connection establishment. The PDN specific ID or the MSISDN or the IMSI are used to identify the MTC device. The ID is conveyed to the MTC Server when an IP address is requested via a RADIUS or Diameter interface from the MTC Server. The IP address assigned can be a private or public IP address. Overlapping IP address ranges can be handled by using different APNs.

A separate AAA server can be used to enable multiple MTC servers to forward MT data to an MTC device. The GGSN/P-GW obtains IP addresses from the AAA server and the AAA server updates the DNS entries of the DNS server functionality administered by the PDN with the assigned IP address. The MTC servers or other entities of the MTC User query the DNS server for the IP addresses of the MTC devices.

NAT functionality (along with related ALG) can be implemented by the MTC Server or on a separate entity if needed by the MTC business logic.

### 6.29.4 IP address assignment by the GGSN/P-GW

This is an alternative for the address allocation described in 6.29.3. In difference to the IP address allocation by an AAA server from the MTC specific PDN here the IP address is assigned by the GGSN/P-GW from a specific private or public address pool that is used for this particular APN. In the case when the address is a private, traffic will be tunnelled to the MTC Server(s).

The rest of the approach is the same as for 6.29.3. The application in the MTC Device may provide its PDN specific device id in e.g., the PCO IE at PDP Context /PDN Connection establishment. Alternatively a PDN specific ID may be provided by the SGSN/MME at PDP Context /PDN Connection establishment. The PDN specific ID, or IMSI or MSIDN are used as identity for the MTC device. Although the IP address is assigned locally, there can be RADIUS or Diameter signalling providing the AAA server with the IP address and the identity, which triggers the AAA server to update the DNS entry of the DNS server functionality administered by the PDN with a domain name including the identity and the IP address. The same mechanism needs to be used to update the MTC Device DNS entry once the IP address is released by the GGSN/P-GW.

An alternate to the use of DNS is that the MTC Server receives AAA accounting messages from the GGSN/P-GW. The AAA accounting messages provide the MTC Server with the IP address assigned to the UE. From that the MTC server can also deduce the presence of the device (at accounting start) as well as when it is no longer available (e.g. accounting stop). This may for example be used by the MTC Server to decide when device triggering is required or not.

### 6.29.5 MTC Server located on Internet and public IP addresses for MTC devices

For this scenario a dedicated APN with public IP addresses is used for the MTC Server. A general APN for Internet access might not be used as the AAA server needs to provide a special interface towards MTC servers and also because updating an AAA server by a GGSN/P-GW is not necessarily required for every Internet APN. The IP address allocation is done by either the GGSN/PGW or by an AAA server within the PLMN domain. When the MTC device application registers its ID (PDN specific ID, IMSI, MSISDN) at the MTC server the MTC server can use an SMTC interface to verify with the AAA server whether the MTC device with the specific ID got the IP address allocated.

The basic idea of the proposal is that it is left for the application layer in the MTC Device and the MTC Server to do the necessary registration of the MTC device and make an MTC device ID and its IP address known in the MTC Server. The 3GPP system provides the communication connection and a means to verify that the IP address is assigned to a specific ID (IMSI, MSISDN, PDN specific ID). A notification of bearer releases can optionally be provided to the MTC Server, e.g. for cases when the MTC Device cannot deregister because of lost coverage. Existing protocols and nodes are used in the 3GPP system and enhanced for this scenario here. This scenario assumes public Ipv4 addresses or Ipv6 addresses.

Editor's Note: In case MTC Monitoring is part of Rel-10, the optional notification of bearer releases mentioned above may be replaced by corresponding MTC Monitoring features.



Figure 6.29.5-1: MTC Device doing registration at the MTC Server, authenticating the IP address, and subscribing to bearer releases from the network

The flow of events in the figure above:

1. The device establishes its communication connection by attaching to the network and creating a PDP Context or PDN Connection.

2. The Sgi/Gi/RADIUS protocol as specified in TS 29.061 [4] clause 16 is used to provide the IP address of the device to a AAA server. The AAA server stores the IP address as long as the bearer is active together with an ID (IMSI, MSISDN, PDN specific ID provided by MTC device in PCO). Optionally the PGW/GGSN may let the AAA do the IP address allocation. If a PDN specific ID is used the AAA server needs to be configured with a PDN specific ID for each MSISDN or IMSI. If a PDN specific ID is used the AAA server needs to verify that the UE provided ID matches the GGSN/P-GW provided IMSI or MSISDN. However the effort of configuring the UE might be avoided and the configuration of the AAA server, which is needed for verifying a UE provided ID, can directly be used to map the PLMN internal IMSI to an ID that can be used by the MTC application.

The AAA Server is deployed in the PLMN.

3. The application in the MTC Device registers at the MTC Server. At a minimum the PDN specific ID or the IMSI or the MSISDN and the IP address of the device is provided.

Editor's Note: It is FFS how to handle communication scenarios with multiple MTC Servers belonging to the same application/APN/PDN.

4. The MTC Server checks at the AAA Server the relationship between the IP address and the MTC Device provided ID thus checking the validity of the MTC Device provided id. This checking is the same mechanism as the GIBA mechanism that is already specified in TS 33.203 [4]. Only the PDN specific ID allocation needs to be managed in a different way.

NOTE: Similar restrictions and limitations apply as with GIBA, e.g. the IP address spoofing needs to be prevented.

5. A notification may optionally be sent to the MTC Server at a later stage when the PDP Context/PDN Connection is released and the IP address of the Device becomes invalid.

### 6.29.6 Impacts on existing nodes or functionality

This solution has a low impact on the existing mobile system as:

- RADIUS client is already part of the GGSN/P-GW as per TS 29.061 [4];

- Need to add a mechanism to dynamically update the DNS function in the MTC Server or on a separate DNS server. The existing RADIUS client in the GGSN (accounting message) may be used; in that case, the AAA server may need new functionality if not located on the MTC server.

An MTC device that needs to support simultaneous access to different MTC Servers associated with different APNs establishes multiple PDN connections and support multiple IP addresses.

### 6.29.7 Evaluation

Benefits:

- Avoids the need for NAT in the operator network as overlapping private IP addresses can be used among different MTC Servers on different APNs;

- Minimum or no impact on the existing standard/ existing Core Network nodes;

- the solutions described in 6.29.3 and 6.29.4 are generic IP-level solution that does not rely on application-level identifiers (e.g. SIP URI);

- The solution does not rely on alternative communication channels (e.g. SMS) for delivery of a “push” stimulus to an attached MTC device with an established PDN connection;

Drawbacks:

- requires tunnelling mechanism to be used between the GGSN/P-GW and the PDN of the MTC Server to enable assignment of private IP addresses to the MTC Devices;

- if the MTC device needs to have simultaneous access to MTC Servers associated with different APNs, the solutions described in 6.29.3 and 6.29.4 require that the MTC device support multiple PDN connections (i.e. multiple IP addresses);

- the solutions described in 6.29.3 and 6.29.4 may not be suitable for local breakout scenarios;

- the solution in 6.29.5 works with Ipv6 and public Ipv4 addresses only.

## 6.30 Solution - MME/SGSN overload control by DL MTC traffic throttling

### 6.30.1 Problem Solved / Gains Provided

See clause 5.12, "Key Issue – Signalling Congestion Control".

### 6.30.2 General

An MME or SGSN starting to experience overload should be able to trigger partial or complete throttling of the signalling traffic generated by low priority MTC devices/applications while still allowing normal operations for other traffic (e.g. voice, data, signalling).

This solution specifically addresses throttling of DL traffic received on low priority PDN connections for MTC devices in ECM-Idle state or PMM-Idle mode, i.e. traffic for which the SGW would normally send a Downlink Data Notification message to the MME/S4-SGSN to trigger a network-initiated service request procedure.

An S4-SGSN or MME starting to experience overload (i.e. whose load exceeds a threshold to start MTC low priority traffic throttling) may reduce its load by requesting the SGW to throttle DL low priority MTC traffic for MTC devices in idle mode according to a throttling factor (%) and for a throttling delay specified in the request, e.g. within the Downlink Data Notification Ack message.

During that throttling delay, the SGW drops DL packets received on all its PDN connections marked as low priority served by that MME/S4-SGSN and without an S1/12 bearer in proportion to the throttling factor, and sends a Downlink Data Notification message to the MME/S4-SGSN only for the non throttled PDN connections.

The SGW resumes normal operations at the expiry of the throttling delay. The last received value of the MTC throttling factor and throttling delay supersedes any previous values received from that MME/S4-SGSN. The reception of an "MTC throttling delay" restarts the SGW timer associated with that MME/S4-SGSN.

When dropping a DL IP packet the SGW may send an ICMP packet (e.g. ICMP "destination un-reachable") that should tell the source that there is no use in repeating the packet.

When setting up the PDN connection, the MME/S4-SGSN signal to the SGW whether the PDN connection is for low priority MTC traffic or not.



Figure 6.30.2-1

Editor's Note: Any relation to ARP for the throttling mechanism in SGW is FFS.

Editor's Note: Throttling in GPRS core is FFS.

This solution allows selective throttling of low priority DL MTC traffic in case of overload in the EPS Network, at the closest point of the source of the DL traffic. This allows to reduce immediately the load in MME/SGSN induced by low priority DL MTC traffic. It also allows to stop the sending of further DL packets by the application.

### 6.30.3 Impacts on existing nodes or functionality

MME/S4-SGSN signals MTC throttling parameters to the SGW.

The SGW throttles DL low priority MTC traffic according to the MME/S4-SGSN request.

### 6.30.4 Evaluation

This approach enables an MME/SGSN to reduce its load by reducing the signalling traffic resulting from DL user traffic received for PDN connections marked as low priority for MTC devices in ECM-Idle state or PMM-Idle mode (Downlink Data Notification / Downlink Data Notification Ack messages on S11/S4, paging and service request procedures).

It provides mainly benefits by protecting MME/S4-SGSN from massive simultaneous push or poll transactions from ("badly implemented") MTC server for devices with established low priority PDN connections.

It is complementary to an UL MTC signalling traffic throttling approach.

## 6.31 Solution – Rejecting connection requests at partial signalling links

### 6.31.1 Problem Solved / Gains Provided

See clause 5.12, "Key Issue – Signalling Congestion and Overload Control", more specifically congestion control.

### 6.31.2 General

MTC devices maybe concurrently attempt signalling interaction only in a limited area. That means the signalling congestion could occur just in one or several particular signalling links and no overall congestion appears on network elements. For example, in 2G network, the link congestion would be met frequently for Gb interface over Frame Relay because of limited capacity of the interface protocol. It is not appropriate to reject all the MTC related signalling requests receiving from every signalling link for the control of the congestion existed only at partial signalling links.

Editor's Note: It is FFS whether this problem can be addressed purely as a network element implementation issue or by means of an effect application of mechanisms available through SCTP, to be further studied in stage 3.

**Rejecting signalling requests at separate signalling links**

The signalling link could be the connection between BSC/RNC and SGSN or eNodeB and MME. SGSN/MME or other network functions (e.g. OAM) shall detect whether the congestion caused by MTC devices just occurs at the partial signalling links or the overall network node. Upon the congestion of the partial links, SGSN/MME can reject MTC related signalling requests received from other network nodes at one or several signalling links.

**Rejecting signalling requests at a single signalling link set**

A signalling link set contains all links connecting to a single BSC, RNC, eNodeB, RA or TA (List). The SGSN/MME or other network functions (e.g. OAM) shall detect whether the signalling congestion caused by MTC devices just occurs within one kind of link set or not. If yes, SGSN or MME can reject all MTC related signalling requests belonging to a BSC, RNC, eNodeB, RA or TA(List).

The mechanism of back-off time to the MTC Device as described in the clause 6.22 is also applicable for this solution.

### 6.31.3 Impacts on existing nodes or functionality

Possible impacts on SGSN/MME

- Rejection of a connection request targeted at a particular signalling link

- Rejection of a connection request targeted at signalling links connecting to a BSC, RNC, eNodeB, RA or TA(List).

- Detection if the congestion only occurs on one or several signalling links.

- Detection if the congestion only occurs on signalling links belonging to one BSC, RNC, eNodeB, RA or TA(List).

- Providing a reject cause including a back off time in the reject messages (same as the solution specified in 6.22),

- Determination of the back off time that is applicable for a particular MTC Device (same as the solution specified in 6.22).

Possible impact on the MTC Device / UE

- Same as the solution specified in 6.22.

### 6.31.4 Evaluation

Benefits

Avoids that most innocent MTC signalling requests are rejected when congestion only occurs on partial signalling links.

Drawbacks

MME/SGSN will make more complex detections for the congestion.

## 6.32 Solution – Rejecting connection requests based on request types

### 6.32.1 Problem Solved / Gains Provided

See clause 5.12, "Key Issue – Signalling Congestion and Overload Control", more specifically congestion control.

### 6.32.2 General

Sometimes the congestion is triggered only by part of MTC devices controlled by one APN or one MTC group. For example, parts of MTC devices belonging to an APN concurrently attach to the network and cause the congestion for the network node. At the same time the other MTC devices with the same APN that already have PDP context and are in IDLE state attempt Service Request to the network, and their requests will be rejected.

Additionally, the different signalling request indicates the different application's appeal. For example, Attach request with Follow-on indicator may mean a MTC device wants to initiate data transfer immediately, which is more important than the one without Follow-on indicator. If undistinguished signalling rejection by the network node is executed on the congestion time, any MTC device requests can not survive. In fact the congestion may be also released while keeping some important requests unaffected.

Two alternatives to accomplish the solution of rejecting connection requests based on signalling types can be considered.

1) The network node count numbers of different kinds of signalling requests around the congestion time. The O&M periodic counting data created in the nearest time to the congestion occurrence can be used. The network nodes reject one or more signalling requests with the largest amount and extend the scope of rejection until the congestion disappears.

Editor's Note: It is out of the specification scope how to get the O&M statistic data for the signalling requests.

2) The operator or MTC users provide the configuration for the priority of different kinds of signalling requests. The network nodes reject one or more signalling requests with the lowest importance firstly and extend the scope of rejection until the congestion disappears.

The both alternatives could be used together for congestion control. How many kinds of signalling requests shall be selected once time to the rejection list can be decided by the operator's configuration.

The mechanism of back-off time to the MTC Device as described in the clause 6.22 is also applicable for this solution. This solution could be used together with other basic solutions for congestion control, e.g. solution .6.22 Rejecting connection request per APN or MTC group.

### 6.32.3 Impacts on existing nodes or functionality

Additional impacts on CN nodes (SGSN, GGSN, MME, S-GW, P-GW)

- Rejecting a connection request with a particular type

- Counting numbers of different kinds of signalling requests in the statistics period nearest to the time of congestion occurrence.

### 6.32.4 Evaluation

Benefits

On the congestion time part kinds of signalling request can still be handled normally.

Drawbacks

Rejecting part kinds of signalling request at the beginning and extending the signalling scope of rejection gradually may not resolve the congestion in a short time.

## 6.33 Solution – UE behaviour changes

### 6.33.1 Problem Solved / Gains Provided

5.14 "Key Issue – Potential overload issues caused by Roaming MTC devices".

### 6.33.2 General

The scenarios outlined in clause 5.14 highlight some areas where the UE internal behaviour would benefit from small but important changes:

a) the ability to remotely configure a device as, a "low value M2M" device. Typically this could be done via OMA DM.

b) modification (increase) of the minimum value of the timer for the background PLMN search, e.g. to greater than one hour, for a "low value M2M" device. This UE internal value would over-rule any smaller value contained on the (U)SIM.

It is FFS whether this modification applies to just the background search for a more preferred VPLMN, or, to the background search for both VPLMN and HPLMN.

c) for ALL M2M devices, modification of the behaviour following receipt of 'fatal' MM/GMM/EMM cause values such as "IMSI unknown in HLR", "illegal ME" and "persistent" cause values such as "PLMN not allowed". These cause values could be wrongly sent "in panic" by an overloaded (V)PLMN, or, in a denial of service attack by a (mobile) false base station. Following receipt of these cause values, a site visit to all M2M devices is untenable, however, so is immediate re-accessing by the device. Some new middle ground is needed (e.g. retry at a randomly selected time between 24 and 48 hours later).

It is FFS whether the behaviour following receipt of "PLMN not allowed" needs modification or not.

d) For a "low value M2M" device, always use IMSI when Attaching to a new network, or, performing an RA update into a different PLMN that is not an ePLMN. This decreases UE-network signalling in a potentially heavily loaded network.

It is FFS whether this solution is applicable to EUTRAN.

e) In the CS domain, at power on in a new location area, perform a location update with LU type=Attach rather than "normal".

f) Modification of "low value M2M" device behaviour following repeatedly unsuccessful MM/GMM/EMM procedures so that the device does NOT move to competing network(s) and inflict them with similar levels of signalling (over)load.

### 6.33.3 Impacts on existing nodes or functionality

The above features are internal to the M2M device (and/or application on the M2M device).

### 6.33.4 Evaluation

These features seem useful to be developed in more detail (e.g. by CT 1) and specified as part of 3GPP release 10.

## 6.34 Solution – M2M device indication to network

### 6.34.1 Problem Solved / Gains Provided

5.14 "Key Issue – Potential overload issues caused by Roaming MTC devices".

### 6.34.2 General

By providing the network with indications that the UE is a "low priority" M2M device, the network is able to more easily protect itself against overload, and/or to detect that an increase in load is being caused by M2M devices.

Clause 5.14 highlighted the utility of M2M device indicators in the following signalling:

a) in the GSM Channel Request message, and UTRAN and E-UTRAN RRC Connection Establishment messages;

b) in the IDNNS signalling at Attach and RA update from a non-equivalent PLMN;

NOTE: From the stage 2 design point of view, there is no harm in always sending this M2M indicator in the IDNNS. It is left to stage 3 to decide whether to do this simplification.

c) in the NAS signalling to the MME/SGSN/MSC.

### 6.34.3 Impacts on existing nodes or functionality

For the Channel Request message (and its equivalents), the RAN will probably need to broadcast its support/non-support for the new code points.

For b, c the signalling should be able to be added in a backwards compatible manner.

### 6.34.4 Evaluation

These indicators appear useful to specify in 3GPP Release 10.

## 6.35 Solution - Overload control within an MTC access grant time interval

### 6.35.1 Problems solved / Gains provided

See Clause 5.9 "Key Issue –Time Controlled" and Clause 5.12 "Key Issue – Signalling Congestion Control".

### 6.35.2 General

The network may suffer from a dramatic increase in its load at the beginning of the MTC access grant time interval due to the simultaneous signalling actions (e.g., simultaneous attachment operations) of many MTC devices. The main idea of the solution presented here is to let SGSN/MME restrict the number of its attached MTC devices in such a manner that the total number of attached UEs (including both MTC and non-MTC devices) is always under, or, at most, fluctuates slightly around, a pre-defined upper bound during the MTC access grant time interval.

Developed to restrict MTC device accesses only, this solution recommends that each MTC device carry an MTC indication with which the network can distinguish MTC devices from normal human-to-human (H2H) devices. Also, we suggest that the MTC devices remain detached if they are not expected to have any mobile terminated communications.

To implement this method, the network operator needs to set an upper bound of the number of attached UEs. This upper bound is supposed to be the maximum number of attached UEs while keeping the network in a normal working condition. It can be determined according to the network equipment capability and the operating experience.

As the load increases or decreases, the allowed number of UE sessions may have to be adjusted, as a number that is too high will ensure congestion, while a number that is too low will ensure underutilization.

A series of discrete time points (e.g., with a spacing of 1 second) are selected within the MTC access grant time interval as the time instants at which the MTC devices are allowed to request attachment. At other times, the network shall reject the MTC attachment requests and tell each of those MTC devices to resend the request at an aforementioned time point.

At each of the time points described above, the SGSN/MME checks the number of attached non-MTC UEs, the margin between this number and the aforementioned upper bound is regarded as the maximum number of MTC devices allowed to attach at this moment. If the number of currently attached MTC devices is less than that maximum number, the SGSN/MME accepts the attach requests from MTC devices until the number of attached MTC devices reaches the maximum number, otherwise the attach requests are rejected. While rejecting an attach request, the SGSN/MME selects a subsequent MTC attachment time point and tells the MTC device to resend the attach request at that specific time point.

The algorithm is first-come-first-serve. Any device that requests access after the maximum number have been allowed access, will be given a deferral. It is therefore anticipated that devices will attempt to access the network as soon as possible (at the beginning of the Grant Time Interval). Further, it is possible that devices may get deferrals repeatedly, and there is no bound to the number of deferrals that may occur.

The SGSN/MME must select a subsequent MTC attach time such that the MTC Device can complete its minimum Access Duration.

After completing the communication tasks in the MTC access grant time interval, the MTC devices shall get detached (either by themselves or by the network) from the SGSN/MME so that other MTC devices can have chances to successfully attach to the network.

Editor's Note: It is FFS how surcharging instead of detaching can be supported by this solution.

### 6.35.3 Impacts on existing nodes or functionality

Impacts on the SGSN/MME:

- With the MTC indication carried by each MTC device, the SGSN/MME needs to be able to distinguish MTC devices from normal H2H devices.

- The SGSN/MME needs to store the discrete time points at which the MTC devices are allowed to request attachment, and reject MTC attach requests except at those time points. While rejecting an attach request, the SGSN/MME needs to select a subsequent MTC attachment time point and inform the MTC device.

- The SGSN/MME needs to count the numbers of both MTC and non-MTC devices separately. At the time points when MTC devices are allowed to request attachment, the SGSN/MME needs to calculate the maximum number of MTC devices allowed to attach at this moment, and decide how many more MTC attach requests it can accept.

- The SGSN/MME must take into account the Grant Time Interval, Forbidden Time Interval and Access Duration policy that applies to the subscription corresponding to the MTC Device when it calculates the deferred access time point. The MTC Device must be able to fulfil its Access Duration within a Grant Time Interval.

Impacts on the MTC device:

- Each MTC device needs to carry an MTC indication.

- MTC devices need to remain detached if they are not expected to have any mobile terminated communications.

- When its attach request is rejected, the MTC device needs to resend the request at the time point provided by the SGSN/MME in the rejection message.

- After completing the communication tasks, the MTC device needs to get detached (either by themselves or by the network) from the SGSN/MME.

### 6.35.4 Evaluation

## 6.36 Solution - Time controlled feature via Operator and MTC User Business Agreements

### 6.36.1 Problem Solved / Gains Provided

See clause 5.9 "Key Issue – Time Controlled".

### 6.36.2 General

The outline of the solution is as follows:

- The operator informs the MTC user about preferred time-window for MTC devices to communicate with the network. This is performed as part of business agreement between the operator and the MTC User.

- The MTC device informs the MTC Server about its current location and PLMN via application layer.

NOTE: Finer granularity than PLMN may be needed if the time-window is based on geographical location within the PLMN, e.g. for a PLMN covering a large geographical area

- The MTC user via the MTC Server informs the MTC device about the appropriate time window to communicate with the network via application layer.

- The charging for MTC communication may be set such that the communication has higher charges if these occur outside of the preferred time-window.

- The Operator keeps track, via regular OAM, about the time when the communication with MTC device occurs. The operator provides this information, e.g. as part of bill, to the MTC User. The MTC user takes appropriate action if certain MTC devices are communicating outside of the desired time-window. The operator may also take appropriate action, based on analyzing the call-records, e.g. cancel MTC devices subscription.

- Based on traffic pattern, the operator may modify the preferred time-window for MTC device communication and provide this information to the MTC User. The MTC user updates the new time-window of communication to MTC device via application layer.

### 6.36.3 Impacts on existing nodes or functionality

None

### 6.36.4 Evaluation

The over-the-top solution exists independent to 3GPP standardization.

This solution cannot enforce time control policy as defined by 22.368 [2], clause 7.2.2. It would be possible to configure a surcharging policy using PCC.

Dynamic local criteria, e.g. current load on network beyond perhaps 'time zone information', especially from the VPLMN, cannot be taken into account by in a real-time manner, as it is based upon subscription and roaming agreements.

This solution is based on application control. If the same MTC Device uses more than one application, all applications will need to be controlled in a coordinated manner.

## 6.37 Solution - Simple Subscription Control

### 6.37.1 Problem Solved / Gains Provided

This solution answers the requirements of 5.7 "Key Issue - MTC Subscriptions."

### 6.37.2 General

**Solution 1) "Do Nothing"**

It is possible that there will be no MTC Features in release 10. If this is the case, it would suffice that the lack of any MTC subscription elements indicates that no MTC Features are subscribed.

**Solution 2) "Simple Solution"**

The MTC Subscription identifies subscribed MTC Features (as an IE or as IEs) in the HSS.

It is assumed for this release of this specification that all subscribed MTC Features may be considered by the network to be 'essential' and mandatory. If an MTC Device or visited network does not support one or more subscribed MTC Features, the MME/SGSN may inform the MTC Device and the MTC Device detaches.

To determine whether a subscribed MTC Feature is activated:

- The Network may determine if a given MTC Device supports a given MTC Feature through implementation dependent evaluation of the IMEI. For example, the operator may maintain a database of MTC Devices types based upon the IMEI.

- Further, it may be assumed that a subscribed MTC Feature is supported by the MTC Device. If this is not the case, the MTC Device will fail to operate

- If either the network or the MTC Device (e.g. based on IMEI or due to missing but expected parameters during the attach request) does not support a subscribed MTC Feature, the MME/SGSN may reject the MTC Device when it attempts to attach. The MME/SGSN includes information regarding the unsupported MTC Feature in the rejection cause.

An indication of capabilities from the MTC Device is unnecessary to define in a general way. For each MTC Feature, such interaction between the MTC Device and the network may be defined (as has been done for other features, e.g. SR VCC capability, etc.)

If the MME/SGSN is pre-Rel 10 and accepts the MTC devices without any notification about the MTC features, and the device expects such an indication for the feature, the MTC device performs detach procedure.

### 6.37.3 Impacts on existing nodes or functionality

**Solution 1)**

None

**Solution 2)**

The HSS must support an IE (or IEs) representing MTC Features included in the MTC subscription.

The MME/SGSN determine whether an MTC Device supports the subscribed set of MTC Features on the basis of the IMEI the device capabilities (e.g. by means of a database) or by checking whether expected IEs are present.

The MME/SGSN knows (due to local policy) whether a given MTC Feature is supported by the network.

The MME/SGSN may reject MTC Devices attempting to attach using a new rejection code.

### 6.37.4 Evaluation

Solution 1 is preferable if no MTC Feature is standardized in release 10. This solution has no impact on the standard and will not complicate future MTC Feature control mechanisms.

Solution 2 is preferable if MTC Features are standardized in release 10. A simple approach is taken in which the minimum semantics are assumed in order to support the architecture requirements expressed by the Key Issue.

## 6.38 Solution – Device identifier used over MTCSP

### 6.38.1 Problems solved / Gains provided

See   
clause 5.8 “Key Issue –MTC Device Trigger”,   
clause 5.13 “Key Issue - MTC Identifiers”,   
clause 5.10 “Key Issue - MTC Monitoring”,  
clause 5.11 “Key Issue - Decoupling MTC Server from 3GPP Architecture”.

### 6.38.2 General



Figure 6.38.2-1: 3GPP Architecture for Machine-Type Communication

The reference points are listed as below:

**MTCu**: It provides MTC Devices access to 3GPP network for the transport of user plane and control plane traffic. MTCu interface could be based on Uu, Um, Ww and LTE-Uu interface.

**MTCi**: It is the reference point that MTC Server uses to connect the 3GPP network and thus communicates with MTC Device via 3GPP bearer services/IMS. MTCi could be based on Gi, Sgi, and Wi interface.

**MTCsp:** It is the reference point the MTC Server uses for signaling with the 3GPP network.

**MTCsms:** It is the reference point MTC Server uses to connect the 3GPP network and thus communicates with MTC Device via 3GPP SMS.

Editor’s Note: It is ffs if MTCsms exists as a separate reference point or whether MTCsp is used for 3GPP SMS as well.

In the general case the MTC Server is located outside the operator domain. In the special case when the MTC Server is located in the operator domain, the MTCSP and the MTCi becomes internal in the operator network. In a deployment there may simultaneously be MTC Server located inside the operator domain and MTC Servers located outside the operator domain. There might be one or several functional entities in the mobile operator network that terminate the MTCSP reference point. In the text below these entities(s) are simply referred to as “Service Centre configured for MTC”. The MTC Server and the MTC User may either be separate entities or co-located.

Guiding requirements for a device identifier to be used instead of MSISDN and IMSI at signaling between the MTC Server and the mobile operator network are:

* The new identifier should have a one-to-one mapping to the IMSI. That is, it shall identify one active UE (e.g. MTC device).

Editor’s Note: It is ffs if some flexibility in the mapping similar to the one between MSISDN and IMSI would be useful.

* The identifier must be globally unique since some MTC service providers operate word wide.
* The allocation of the new identifier should be efficient e.g. administration on country level
* The identifier shall also be possible to use towards other access networks such as 3GPP2, etc.
* “Number portability” should be supported. That is, a service provider should be able to switch to another operator network, without changing the identifier. Number portability for the MTC User might be a requirement to consider too, or alternatively a different device identifier is used on the API between the MTC User and the MTC Server .

Editor’s Note: It is ffs if “number portability” is required or if modern IT tools in the M2M domain make this unnecessary.

* The new identifier should support certain functions in the operator domain
  + Facilitate routing of signaling, that is, discovering which MTC Server or service provider the MTC device belongs to and its signaling shall be routed to
  + Facilitate charging and billing. One device (and the charging data produced from its activities) should easily be traced back to which service provider it belongs to. Optionally also which user at the service provider it belongs to.
  + Selective congestion control or enabling/disabling e.g. per MTC User and per Service Provider
* Migration aspects when changing from MSISDN to the new identifier should be considered
* Other?

The details for a device identifier used in MTCSP protocols should be specified in stage 3 (already established protocols such as HTTP RESTful may be candidates for a MTCSP protocol). However in the SA2 requirements of a device identifier, there may also be requirements such as what information it contains (see example below).

In this example below the “Service Provider ID” is a domain name that belongs to the MTC service provider. The “topdomain” would ensure that the “Service Provider ID” becomes internationally unique. The “topdomain” would be a FQDN in itself such as “.com”, “.se”, “.co.uk”, “.operator.com”, etc. The “User ID” should identify a subscriber within the service provider domain, for example an enterprise or even a person using MTC services. There would be a unique “Device ID” part for each MTC device a user has (at least unique within the user domain). The “Device ID” may for example be a serial number of the hardware running the “application part” of the MTC device (i.e. not the IMEI) or any other number used by the MTC user to distinguish the MTC device. All these different parts together constitute the full device identifier, as used over a MTCSP interface. In the reminder of this document, the term “International Service provider Subscription Identifier” (abbreviated to ISSI) is used for a device identifier used over the MTCSP interface and meeting the requirements listed above.

Editor’s Note: The name for the device identifier “International Service provider Subscription Identifier” (ISSI) is tentative and may change.

**FQDN:**deviceid.userid.serviceproviderid.topdomain.

**Dedicated 3GPP URN:** urn:issi:deviceid.userid.serviceproviderid.topdomain.

**SIP URI:**sip:deviceid@userid.serviceproviderid.topdomain.

Figure 6.38.2-2: Examples of different URI style formats of a device identifier (ISSI)

An advantage with an URI style format of a device identifier is that this can be considered mainstream internet technology and that the administration and allocation of the different identifier parts, e.g. the Service Provider ID part, does already exist as part of the normal domain name administration. A slight disadvantage could be that if the different identifiers parts are domain names, such as the “serviceproviderid.topdomain”, care need to be taken so that clashes with other usages of the same domain name is avoided.

Alternative a) above using a FQDN for identifying a device should work but there is an implicit assumption of the content/structure of the domain name that needs to be specified.

Alternative b) using a Uniform Resource Name (URN) is probably more correct way to use a URI when the intention is to specify an identity. By using a new specific Namespace ID in the URN such as “ISSI” in the example, the syntactic interpretation of the Namespace Specific String would be defined. There may be other already registered Namespace ID’s that can be used more or less according to 3GPP requirements.

Alternative c) using a SIP URI is also a possibility. The syntax associated with SIP URI’s should be possible to use for what 3GPP requires of a device identifier, but when following it strictly the SIP protocol is also expected for a SIP URI which may not be the case for the MTCSP interface.

Note: Depending on what type of URI is selected as device identifier, there might be assumptions on what protocol is used over the MTCsp.

### 6.38.3 Impacts on existing nodes or functionality

Impact on GPRS/EPS architecture

* A new termination point for the MTCSP reference point in the operator network.

Impacts on the HSS/HLR:

* Storage of a new parameter (ISSI) in the subscription information. Making ISSI searchable to be able to find a specific subscriber profile based on an ISSI.
* A new or modified existing protocol is specified for the reference point between the HSS/HLR and a Service Centre configured for MTC. It is ffs how the Service Centre configured for MTC can find the HLR/HSS when there are multiple HLR/HSS.

Editor’s Note: The place where to store the ISSI is still subject for discussion. Hence the HSS/HLR impacts may change.

### 6.38.4 Evaluation

## 6.39 Solution – Triggering MTC devices via HSS and NAS signalling

### 6.39.1 Problem Solved / Gains Provided

See clause 5.8, "Key Issue – MTC Device Trigger" and clause 5.13 "Key issue - MTC Identifiers".

### 6.39.2 General

#### 6.39.2.1 Overview

A network application server (e.g. Device Management Server) that needs to trigger a connection request from a UE informs the HSS/HLR about this need by providing "UE application trigger request" information defined in § 6.40.2

Each of the UE targeted by the network application server request is then notified about that request via signalling exchange through the serving MME/SGSN, during the next NAS signalling exchange with the UE if there is no on-going signalling connection between the UE and MME/SGSN, or immediately if there is an on-going signalling connection with the UE or if this is an urgent request.

Upon reception of this "UE application trigger request" information, the UE application is triggered and contacts the network application server.

#### 6.39.2.2 Detailed solution

The procedure is illustrated in figure 6.39.2-1 and works as follows:



Figure 6.39.2-1: Triggering MTC devices via HSS and NAS signalling

1) Each time a network application server wants to contact a UE, it informs the HSS/HLR about this need by providing "UE application trigger request" information.

The interface between an external application and the HSS/HLR needs to be secured. Limitation may be enforced to avoid simultaneous storage of too many "UE application trigger request" in the network.

The HSS/HLR (or a gateway between the application and the network):

a) validates the request from the application (e.g. checking the application rights to issue such requests, enforcing application throttling , …);

b) translates the identity of the target UE received from the application into a network identity of the UE (e.g. corresponding to the IMSI of the target UE);

c) stores this request in its database record associated with the target UE;

d) determines the MME/SGSN that currently serves the target UE or waits for such a MME/SGSN to be allocated to the UE (i.e. waits for a subsequent Update Location from an MME/SGSN for that user).

2) The HSS/HLR notifies/updates the serving MME or/and SGSN with this "UE application trigger request" information, immediately if the UE is already served by a SGSN/MME, otherwise when the UE registers to the network.

The "UE application trigger request" may be sent within the MAP (Gr) or Diameter (S6a/S6d) Insert Subscriber Data operation. The MME/SGSN stores this request in its database record associated with the UE and returns an Insert Subscriber Data answer.

3) The serving MME/SGSN transfers the "UE application trigger request" information to the UE upon the next NAS signalling exchange with the UE:

a) RAU / TAU procedure:

- the RAU/TAU Accept message may carry the "UE application trigger request" notification;

- the TAU/RAU Complete message acknowledges the correct UE reception of the "UE application trigger request" notification. The UE has to send a TAU/RAU Complete message as if a new GUTI or a new P-TMSI had been assigned.

b) Attach procedure:

- the Attach Accept message may carry the "UE application trigger request" notification;

- the Attach Complete message acknowledges the correct UE reception of the "UE application trigger request" notification. The UE has to send an Attach Complete message as if a new GUTI or a new P-TMSI had been assigned.

c) a dedicated Notification procedure (with a UE acknowledgment) which takes place immediately if there is an on-going signalling connection with the UE when the MME/SGSN receives the request from the HSS/HLR.

This may be implemented as follows:

- for LTE access: the Network and UE initiated Generic transport of NAS messages procedures (see TS 24.301 subclauses 5.6.4.3 and 5.6.4.2) may be used to carry the "UE application trigger request" notification to the UE and its acknowledgment by the UE. I.e. using the DOWNLINK GENERIC NAS TRANSPORT message and the UPLINK GENERIC NAS TRANSPORT message with a Generic message container type IE set to a specific value for the transfer of "UE application trigger request" and with the Generic message container IE containing the "UE application trigger request" information.

- For 2G/3G access, a similar mechanism may be defined or an existing GMM message may be extended to carry the UE application trigger request, e.g. GMM Information message (see 3GPP TS 24.008 subclause 9.4.19).

4) Upon reception of this "UE application trigger request" information, the UE

a) acknowledges the reception of this information via NAS signalling to the MME/SGSN;

b) checks that this is not a duplicate request (using the request counter). If this is a duplicate step 4) stops here. Otherwise, the UE application is triggered;

c) establish the relevant PDN connection / PDP context using the existing EPC/GPRS procedures, if it is not already established;

d) triggers the UE application which then contacts the network application server in the network. The addressing information to contact the application server in the network may be known in advance on the UE or may have been communicated in the "UE application trigger request" notification.

1. Upon receipt of the acknowledgement from the UE,

a) the MME/SGSN removes the UE application trigger request information from its database record associated with the UE and notifies the HLR/HSS that the UE has received the "UE application trigger request" by sending a Diameter Notification message or a MAP Update GPRS Location message.

b) When the HSS/HLR receives the acknowledgement from either the MME or the SGSN about a UE, the HSS/HLR removes this request in its database record associated with this UE.   
The HSS/HLR does not need to wait for the acknowledgement from both MME and SGSN to remove the request. This means that an UE may receive twice (once via MME, once via SGSN) such a notification. If so, the UE can detect a duplicated request via the request counter, discards the repeated request and returns a positive acknowledgement to the sending node. Another alternative would be for the HSS/HLR to remove an obsolete UE application trigger request from a MME/SGSN.

An application may cancel an UE application trigger request using its application Id and the request counter.

If an MME/SGSN fails and loses the information about not yet transferred "UE application trigger request" notifications, this is not an issue as the HSS/HLR sends to an MME/SGSN that starts serving an UE all "UE application trigger request" notification information it has in its database record associated with this UE.

An urgency request parameter may also be associated with the "UE application trigger request" notification. If the request is urgent, the UE is notified as soon as possible i.e. the serving MME/SGSN pages the UE as soon as it receives the "UE application trigger request" information from the HSS/HLR. Otherwise the UE is notified only the next time it exchanges signalling with the MME/SGSN.

### 6.39.3 Impacts on existing nodes or functionality

HLR/HSS stores UE application trigger requests, transfer them to serving MME/SGSN and erase them upon getting the acknowledgement that they have been successfully delivered to the UEs. The signaling cost of this procedure on HSS/HLR should be equivalent to the cost of a triggering based on terminating SMS.

MME/S4-SGSN stores UE application trigger requests, transfers them via NAS signalling to the UE and erase them upon getting the acknowledgement that they have been successfully delivered to the UEs.

UEs receive and acknowledge UE application trigger requests via NAS signalling and trigger the corresponding application.

### 6.39.4 Evaluation

## 6.40 Solution – Information sent to trigger a MTC Device

### 6.40.1 Problem solved

This solution describes the information to be provided by a network application server (e.g. Device Management Server) that needs to trigger a connection request from a UE. See clause 5.8, "Key Issue – MTC Device Trigger"

### 6.40.2 Required Functionality

A network application server (e.g. Device Management Server) that needs to trigger a connection request from a UE provides "UE application trigger request" information containing e.g.:

- the identity of the target UE;.

- the identity of the application;

- a request counter associated to this request allowing to detect duplicated requests, to correlate requests with their acknowledgement and to allow the application to cancel a request;

- optionally the IP@ (or FQDN) and/or TCP (or UDP) port of the application server that the UE has to contact;

- optionally an urgency request indication;

- optionally a validity timer (allowing to remove storage of the UE application is triggered when it is no more needed)

- optionally application specific information (of limited size).

Editor's Note: It is FFS whether other parameters such as provided within a SMS based trigger are needed.

## 6.41 Solution – Triggering of attached MTC Devices by reusing Network Requested PDP Context Activation procedure

### 6.41.1 Problem Solved / Gains Provided

See clause 5.8 “Key Issue – MTC Device Trigger”.

### 6.41.2 General

This solution proposes to trigger the attached MTC Devices by reusing Network-Requested PDP Context Activation procedures. This solution supports the scenario where an MTC Device has a subscribed static IP address and the scenario where only dynamic IP address assignment for MTC Devices is supported. The MTC Device can obtain IP address dynamically during the subsequent PDP context activation procedure in case there is no subscribed static IP address.

The MTC Server initiates DNS query to retrieve the IP address for the MTC Device if it is not available in the MTC Server. The DNS Server can be standalone or the front-end of the AAA Server. The DNS Server lookup the entry based on the query input (i.e. a FQDN, which includes the device identifier) provided by the MTC Server. If there is a valid record in the DNS Server, the DNS Server returns IP address to the MTC Server (e.g. a PDP context or PDN connection has been established) directly, otherwise, it requires the AAA Server to trigger the MTC Device to establish PDP context or PDN connection firstly.

Editor's Note: The device identifier format, e.g. FQDN is FFS.

NOTE 1: For E-UTRAN access, a default PDN connection is established during Attach procedure, so the DNS Server can return the IP address directly.

NOTE 2: The AAA Server and DNS Server can be deployed as standalone physical entities or as functional entities collocated in a Device Trigger Gateway (DT-GW; refer to Figure 6.45.2-1).

There are two alternatives for the AAA Server to trigger the MTC Device.

**Alternative 1:**

**MTC Server**

**AAA**

**Server**

**HSS**

**GGSN**

**SGSN**

**MTC**

**Device**

**1**

**2**

**3**

**4**

**5**

**8**

**7**

**6**

**Request Device’s IP**

**Request Device’s infor**

**Connectivity Request**

**Network initiates PDP activation**

**Device initiates PDP activation**

**Registration**

MTCsp

Figure 6.41.2-1: Illustration of alternative 1

The AAA Server selects the HLR/HSS based on the IMSI, which is derived from the device identifier (i.e. the IMSI is included in the device identifier) or mapped from the device identifier based on local configuration, and sends an information request (IMSI) message to the HLR/HSS. The HLR/HSS returns the serving SGSN address for the MTC Device.

The APN can be provided by the MTC Server (e.g. included in the FQDN for DNS query), or derived from, e.g. the FQDN according to local configuration.

The AAA Server selects a GGSN based on e.g. APN, and initiates Network-Requested PDP Context Activation procedure as specified in TS 23.060, with the exception as follows:

1. In step 3 of above figure, the AAA Server sends a Connectivity Request message (IMSI, APN, SGSN address) to the selected GGSN.
2. In step 4 of above figure, the GGSN sends PDU Notification Request (IMSI, APN, PDP address) message to the SGSN. The PDP address is set to zero or the static IP address configured in the GGSN.
3. In step 7 of above figure, the GGSN registers the MTC Device to the DNS Server via AAA Server as specified in TS 29.061, with providing the device identifier, APN and the IP address (i.e. the subscribed static IP address or the dynamically allocated IP address during the PDP context activation procedure in step 6), which are provided by the MTC Device in PCO IE.

NOTE 3: For IPv6 it is assumed that the MTC Device relies on DHCPv6 for stateful address allocation.

**Alternative 2:**

**MTC Server**

**AAA**

**Server**

**HSS**

**GGSN**

**SGSN**

**MTC**

**Device**

**1**

**2**

**3**

**4**

**5**

**8**

**7**

**6**

**Request Device’s IP**

**Request Device’s infor**

**Connectivity Request**

**Network initiates PDP activation**

**Device initiates PDP activation**

**Registration**

MTCsp

Figure 6.41.2-2: Illustration of alternative 2

The AAA Server selects a GGSN based on e.g. APN which is provided by the MTC Server (e.g. included in the FQDN for DNS query), or derived from, e.g. the FQDN according to local configuration, and then initiates Network-Requested PDP Context Activation procedure as specified in TS 23.060, with the exception as follows:

1. In step 2 of above figure, the AAA Server sends a Connectivity Request message (IMSI, APN) to the selected GGSN. The IMSI is derived from the device identifier (i.e. the IMSI is included in the device identifier) or mapped from the device identifier based on local configuration.
2. In step 3 of above figure, the GGSN sends MAP\_SEND\_ROUTING\_INFO\_FOR\_GPRS Service (IMSI) message to the HLR/HSS. The HLR/HSS address is derived from the IMSI. The HLR/HSS returns the serving SGSN address.
3. In step 4 of above figure, the GGSN sends PDU Notification Request (IMSI, APN, PDP address) message to the SGSN. The PDP address is set to zero or the static IP address configured in the GGSN.
4. In step 5 of above figure, the SGSN sends a Request PDP Context Activation (APN, PDP address) message to the MTC Device.
5. In step 7 of above figure, the GGSN registers the MTC Device to the DNS Server via AAA Server as specified in TS 29.061, with providing the device identifier, APN and the IP address (i.e. the subscribed static IP address or the dynamically allocated IP address during the PDP context activation procedure in step 6), which are provided by the MTC Device in PCO IE.

NOTE 4: For IPv6 it is assumed that the MTC Device relies on DHCPv6 for stateful address allocation.

Afterwards, the DNS Server returns the IP address of the MTC Device to the MTC Server, so that the MTC Server can transmit packet data to the MTC Device.

Editor's Note: The alternative with using dynamic address allocation needs to solve issues addressed in TR 23.976. The solution with using static IP address allocation needs to detail how static address allocation is performed as it has been removed from 23.060 and 23.401.

### 6.41.3 Impacts on existing nodes or functionality

Impacts on the Network-Requested PDP Context Activation procedure:

* It is triggered by a signalling over Gi interface instead of a PDU;
* It needs to support dynamical IP address allocation;
* In alternative 1, the GGSN does not communicate with HLR/HSS via Gc interface.

### 6.41.4 Evaluation

## 6.42 Solution - Triggering of attached MTC Device via Pre rel-11 SMS

### 6.42.1 Problem Solved / Gains Provided

See clause 5.8 “Key Issue - MTC Device Trigger”. The solution focuses on the scenario that MTC devices receive trigger indication in attached state w/o PDP/PDN connection.

### 6.42.2 General

The MTC server sends indication to MTC Devices via SMS and make MTC Devices initially establish data communication with the MTC server. The short message should contain MTC Server address and required triggering information.

### 6.42.3 Impacts on existing nodes or functionality

None

### 6.42.4 Evaluation

Benefits:

- No impact for existing network.

Drawbacks:

- The subscription of MTC Device must associate with a MSISDN.

- CS network is involved in case the short message is only supported by the CS domain and/or LTE access is deployed.

## 6.43 Solution - Triggering of attached MTC Device via intermediate node

### 6.43.1 Problem Solved / Gains Provided

See clause 5.8 “Key Issue - MTC Device Trigger”. The solution focuses on the scenario that MTC devices receive trigger indication in attached state.

### 6.43.2 General

This solution re-uses the intermediate node introduced by MTC Monitoring solution specified in clause 6.25. MTC Server may first register its desired events with IMSI or device ID. Towards the triggering purpose, the monitoring event should include CN node-level location change (e.g. SGSN/MME change) of the MTC device and it might be configured in SGSN/MME by operators or inserted into SGSN/MME along with the subscription. SGSN/MME shall report location changes to the intermediate node once the new MTC device enters into or the already camping MTC device changes location. Upon the location report, the intermediate node shall store the SGSN/MME address associated with the IMSI or device ID and then push registered location information to the related MTC server. Above procedures shall follow monitoring mechanism covered in clause 6.25.

When the MTC user wants to trigger an attached MTC Device which can be located, the MTC Server sends notification message with the IMSI or device ID and the MTC Server address to the intermediate node, which thus forwards the message to the SGSN/MME that sends location update message last time. SGSN/MME might use the existing or new NAS message to initiate data communication between the MTC device and MTC server.

In case of no PDP context, the MTC device activates a PDP context after receiving trigger indication. Or SGSN may initiate PDP context activation directly.

Editor's Note: How SGSN initiates a PDP based on the notification from the intermediate node is FFS.The MTC server can also trigger the MTC device without register location monitoring service if all related MTC device are monitored with location by default. Since the MTC Server does not know whether the MTC device is attached before triggering, the triggering might not success.

The intermediate node shall keep the SGSN/MME address per IMSI or device ID in this solution.

Editor's Note: Whether there are changes to the roaming architecture and message flow are FFS.

### 6.43.3 Impacts on existing nodes or functionality

CN nodes:

- Event reporting function through the intermediate node specified in clause 6.25 shall be supported by SGSN/MME, HLR/HSS.

- A new network entity may be introduced and new interfaces are introduced.

Editor's Note: Whether there are additional impacts in roaming scenario is FFS.

### 6.43.4 Evaluation

Benefits:

- MSISDN is not mandatory for this solution.

- It is applicable for PS only network.

Drawbacks:

- The new network entity and new interfaces add complexity of the system.

- SGSN/MME need report location changes to the intermediate node.

## 6.44 Solution – Device Triggering reuse of MT SMS WAP Push

### 6.44.1 Problems solved / Gains provided

See Clause 5.7 "Key Issue –MTC Device Trigger".

### 6.44.2 General

The solution described and evaluated below addresses the Key issue “MTC Device Triggering” and allows an MTC server to trigger registered devices (i.e. IMSI attached or GPRS attached) without a PDP connection to establish a connection making communication with the MTC server possible.

The solution is based on the introduction of a Service Centre configured for MTC capabilities.

The Service Centre configured for MTC (e.g. potentially collocated with SMS-SC) would use a standardized protocol over the MTCsp interface point. The Service Centre resides at the edge of the operators’ network (see figure x). The MTC Server could request the Service Centre to deliver a device trigger over the MTCsp.

The role of the Service Centre is to hide the details of the triggering mechanism in the operator’ domain and provide the MTC Server a generalized interface for it to make a device triggering request. An additional role of the Service Centre would also be to map the globally unique device id provided by the MTC Server to an existing globally unique 3GPP identifiers (i.e. MSISDN, IMSI).

A new functional entity, the Service Center configured for MTC is introduced into the GPRS architecture. The functionality includes:

* Support for a function for MTC device triggering and acknowledgement over the MTCsp reference point between the MTC server and the Service Centre.
* May be collocated with the SMS SC
* May operate in PS domain only or it may operate in both PS and CS domain. In the latter case it may do the triggering through the MSC
* Reuse of a existing SMS infrastructure and protocols
* Reuse of existing functionality in the terminal to trigger the application (i.e. no terminal impact).

A first solution can allow the MTC Server to request a Device Trigger using an optimized MTC device identifier (see clause 6.38 Solution – Device identifier used over MTCsp). This device identifier could be mapped by the Service Centre to the MSISDN and allow for delivery of device trigger using the existing SMS WAP Push functionality. This approach allows reuse of the SMS nodes with no system impact.

A later evolution could be a MSISDN-less mode of operation allowing the Service Centre to map the device identifier to the IMSI. In conjunction with updates allowing for a MSISDN-less mode (e.g. SMS interfaces and nodes would be impacted) the MT SMS would be delivered using the IMSI.



Figure 6.44.2-1 Service Centre at edge of Mobile Operator Domain

From 23.040 [6] clause 4.1 the follow entities are in the provision of SMS.



Figure 6.44.2-2 Entities involved in the provision of short message

The MTC Server takes the role of the SME (Short Message Entity). The Service Centre configured for MTC may be co-located with the SMS-SC. As per 23.040[6] the Service Centre may be integrated with the SMS GMSC/SMS IWMSC.

Steps for the MTC Server to request a device trigger include:

* The Service Centre would receive the Device Trigger Request over the MTCsp interface point. The Device Trigger request may use the new device identifier as per Solution – Device Identifier used over MTCsp (clause 6.38)
* The Service Centre maps the received device identifier and maps this to the MSISDN and initiates a message transfer that eventually results in a MT SMS (e.g. WAP PUSH – MT SMS with embedded URL) that triggers the MS to establish a PDP connection.
* The existing flow as per clause 10 of 23.040 [6] would be triggered by the Service Centre without impacts to the SMS interfaces and involved nodes. The Service Centre sends the short message to the SMS GMSC. The SMS GMSC interrogates the HLR to retrieve routing information necessary to forward the short message, and then sends the message to the relevant MSC or SGSN, transiting other networks if necessary. The MSC or SGSN then sends the short message to the MS.
* The MTC Server receives Device Trigger Report from the Service Centre



MTC Server

Device Trigger

(Device ID)

Device Trigger evice Trigger

PLMN Server Provider domain from R/HSS.in the SA2 folder.

report

NOTE 1): This operation is not used by the SGSN.

Figure 6.44.2-3 Successful short message transfer attempt via the MSC or the SGSN

A further evolution of the MT SMS WAP PUSH mechanism could be considered for a MSISDN-less mode of operation on the SMS provisioned interfaces.

The MAP message the SMS GMSC uses to interrogate the HLR to retrieve routing information necessary to forward the short message currently carries the MSISDN. The HLR uses the MSISDN to retrieve the IMSI as well as other necessary information (e.g. Network Node Number/GPRS Node indicator) to which to forward the short message.

The MSIDSN usage for MT SMS would have to be replaced by the IMSI. Two possibilities include:

* The Service Centre could maintain a mapping of the Device Identifier to the IMSI. The intent would be to use the IMSI instead of the MSISDN in the MAP message possibly introducing a new IMSI IE. The HLR would use the received IMSI as the index to retrieve the subscriber record containing the routing information.
* Alternately the device identifier used on the MTCsp interface could be stored in the subscription information and the HLR can return the IMSI based on the device identifier. This option requires introduction of new Device Identifier IE in the existing MAP message.

NOTE: Typically the MSISDN (e.g. using MNC, MCC) and/or IMSI number series is used to determine which HLR to interrogate. If a solution is pursued such that the Service Centre does not map the new device identifier to an existing 3GPP Identifier (i.e. MSISDN, IMSI) an alternate means to determine which HLR to interrogate would be required and be FFS.

### 6.44.3 Impacts on existing nodes or functionality

#### 6.44.3.1 Impacts for MT-SMS WAP Push - MSISDN based

In the case of a solution using MT SMS WAP Push and the existing MSISDN based SMS interfaces it is expected that the entities and interfaces (i.e. interfaces 1 thru 5 of figure ZA below) are not impacted.

Impact on GPRS/EPS architecture

* New functionality entity Service Configured for MTC is introduced.

Impact on the SMS-SC:

* May be impacted for solution that co-locates the Service Centre with the SMS-SC

Introduction of a new protocol over the MTCsp interface point between MTC Server and the Service Centre configured for MTC.

The Device Trigger Request could contain new MTC device identifier (e.g. URI based) that the Service Centre will map to an existing 3GPP identifier (i.e. MSISDN) thereby eliminating impacts to interfaces 2-5 in figure 6.44.3-1 below.

#### 6.44.3.2 Impacts for MT-SMS WAP Push and MSISDN-less based

Impacts include the above along with SMS entities and related interface to allow MT-SMS based on IMSI

The main network structure from 23.040 [6] illustrated in figure ZA below highlights potential scope of impacts.



NOTE 1: Reference point 4 is not used for SMS transfer via the SGSN

NOTE 2: The SMS Router is an optional entity that may be present in the MT case only. If it is not present, reference point 3 extends from the SMS-GMSC directly to the MSC/SGSN.

Figure 6.44.3-1 Main network structure and reference pts

MSISDN usage in existing messages on interfaces 1-5 would have to allow for an equivalent MSISDN-less mode. MSISDN usage primarily appears in operation in interface pts 1, 2, and 4. On interface pt 3 and 5 IMSI appears to be use and may not be impacted by an MSISDN-less mode of operation.

HLR

* The interrogation to the HLR to retrieve routing information would be based on new device identifier. HLR would store and access information based on this new device identifier

SMS-GMSC/SMS-IWMSC

* Interrogation of the HLR to retrieve routing information will be based on the new device identifier

Other non SMS functionality may be affected by the absence MSISDN in the subscriber record. For example charging records generated by the SGSN may be populated with the MSISDN.

### 6.44.4 Evaluation

This solution minimizes system impacts by building on and extending the existing SMS functionality.

Benefits for both solutions include:

* Allows for use of new Device identifier within the MTC Server Provider domain
* Provides over a standardized interface the means for the MTC Server to trigger a device to establish a connection and to start to communicate with the MTC Server.
* The MTCsp interface can be a stable interface to the MTC Server, while allowing device triggering methods internal in the PLMN to evolve (e.g. MT SMS – MSISDN-less, or even new non-SMS triggering techniques).
* Can be used as a first phase in a migration towards a more optimized triggering solution. The interface towards the MTC Server is stable regardless what triggering method is used internally in the PLMN.

Drawbacks for both solutions include:

* SMS infrastructure and interface impacts

MT-SMS WAP Push - MSISDN based

Benefits

* Service Configured for MTC that performs MTCsp device id mapping to MSISDN allows for complete re-use of MT-SMS and associated infrastructure with no impacts to the SMS nodes and interfaces

MT-SMS WAP Push – MSISDN-less

Benefits

* Re-uses existing SMS infrastructure (though with some impacts)
* Address part of the “Key Issue - MTC Identifiers” whereby MT SMS can be delivered without MSISDN

## 6.45 Solution – Device trigger gateway solution

### 6.45.1 Problem Solved / Gains Provided

See clauses 5.8 "Key Issue – MTC Device Trigger" and clause 5.3 "Key Issue – IP Addressing"

### 6.45.2 General

This solution shows how the key issue MTC Device Trigger can be achieved using a new simple Device Trigger Gateway (DT-GW) in the HPLMN in combination with several services provided in the existing standards. That is, once these services are optimized, as needed, to support a subscription without a unique MSISDN. The set of existing services to be leveraged can be seen in this clause as an example and additional alterative service combinations can exist. To support the MTC device trigger feature, an operator can choose to utilize one or more of the existing services for all its customers or utilize a combination of different existing services for different customers.

A DT-GW could be a standalone physical entity or a functional entity. At least one DT-GW is owned by and deployed in a HPLMN that supports the MTC device trigger feature for subscribed devices. The DT-GW is deployed on the boundary between the HPLMN and the public Internet. Alternatively, the DT-GW is owned and operated by a 3rd party on behalf of the HPLMN and/or deployed in the public Internet. In which case, a secure tunnelling mechanism between the DT-GW and the HPLMN is utilized.

At any given point of time, there is at least one globally routable DT-GW assigned for each subscribed MS/UE that supports the MTC device trigger feature. A DT-GW terminates an MTCsp interface for reception of trigger indications from a submitting node (e.g. an authorized MTC server or IWK function on behalf of the MTC server). The MTC server is configured with a DT-GW IP address and optionally the SRC and DST ports to be used to transmit a trigger indication for a particular MTC device. Alternatively, the DT-GW information for a particular subscribed device could be made available and determined through DNS mechanisms. The MTC server sends a trigger indication request to the appropriate DT-GW encapsulated in an IP packet. The trigger indication request could contain pertinent information needed to route the trigger (e.g. device subscriber identity, trigger command/arguments, relevant device location information, security parameters, etc.).

When a trigger indication is received from a submitting node, the DT-GW should first authorize the received request; making sure it originated from a trusted MTC server and is targeted for a device for which the MTC server is authorized to trigger. The next step is for the DT-GW to determine the reachability of the MTC device. Per the requirements specified in clause 5.8, a trigger-able MTC device can be received in the detached state, in the attached state without a publically routable PDP context/PDN connection and in the attached state with a publically routable PDP context / PDN connection. To determine “how” reachable the device is, the DT-GW interrogates the HLR/HSS using the C and/or Sh interface.



Figure 6.45.2-1: MTC device trigger gateway architecture

The DT-GW uses the reachability information obtained from the HLR/HSS, the GGSN/P-GW Radius/Diameter interface (as described in clause 16 of TS 29.061 [4]) and MNO configured policy information to determine the most efficient and effective service and route to use for forwarding of the trigger indication to be delivered to the MTC device. Some trigger delivery services that could be considered are shown in Figure 6.45.2-1, for which the DT-GW reformats, as needed, and forwards the trigger indication to the appropriate:

a) GGSN/P-GW for delivery over an already established PDP context / PDN connection;

b) GGSN for delivery over a newly established PDP context (via a Network-Requested PDP Context Activation Procedure initiated by the DT-GW);

c) S-CSCF for delivery over SIP/IMS service;

d) SMS-SC for delivery over SMS; or

e) CBC for broadcast delivery over CBS (assumes location information available in trigger indication request or from other source in order to limit the broadcast area).

When a globally routable PDP context / PDN connection is pre-established in the MTC device (as described in bullet a) or is newly established (as described in bullet b), the DT-GW utilizes this connection to forward trigger indications using IP-based communications. If the MTC server has prior knowledge of the public address/route for a publicly reachable PDP context / PDN connection for a targeted MTC device, the MTC server may skip the device trigger procedure provided by the DT-GW and initiate direct communications with the targeted MTC device over the available PDP context / PDN connection.

The DT-GW functionality includes the following:

- ingress of trigger indication messages into the PLMN;

- authorization that the trigger indication is from a trusted MTC server;

- authorization that the MTC device addressed in a trigger indication is from a MTC server that is authorized to trigger the addressed MTC device;

- selection of the delivery service and route to forward the trigger indication to for delivery to the MTC device (e.g. based on collected reachability information and network operator policy);

- reformatting, as needed, of the trigger indication payload to match the format required for the selected delivery service;

- egress of trigger indication from the DT-GW to the to the selected delivery service entity for delivery to the MTC device; and

- Appropriate e.g. error handling, error logging and/or error notification when trigger indication is determined to be invalid or unauthorized.

The DT-GW solution can be applied to achieve many of the goals of the Service Centre configured for MTC concept described in clause 6.44.

### 6.45.3 Impacts on existing nodes or functionality

### 6.45.4 Evaluation

## 6.46 Solution – MT communications address resolution via DT-GW

### 6.46.1 Problem Solved / Gains Provided

See clause 5.3 "Key Issue - IP Addressing" and clause 5.13 "Key Issue - MTC Identifiers".

### 6.46.2 General

Similar to the solution in clauses 6.1 and 6.38, UEs used for MTC that need to be reachable for mobile terminated communications are assigned a static unique hostname (e.g. a FQDN, dedicated 3GPP URN or SIP URI). The hostname is assigned in addition to any 3GPP/EPS-level subscription identity (e.g. MSISDN, IMSI, and/or ICCID) of the UE used for MTC.

Distinct from the solutions in clause 6.1 and 6.38, the hostname of the device is used to perform a DNS query for the address of the MTCsp reference point terminating in the assigned DT-GW. This address is then used for initiating mobile terminated messaging to the UE used for MTC, as required in clause 5.3.2.

When a message related to a particular UE used for MTC is sent over MTCsp, the device identity included in the message could be the hostname of the device and/or the 3GPP/EPS-level subscription identity. In either case, this solution can simultaneously support both MSISDN-based and MSISDN-less subscriptions. However, to allow for a phased rollout of MTC features, initially this solution may only support device triggering for subscriptions with an assigned MSISDN.

As the assigned DT-GW for a particular UE used for MTC will rarely change, if at all, the MTC Server will infrequently need to perform the DNS query to resolve the assigned DT-GW address. This approach significantly reduces the number of DNS query procedures to be performed relative to if a DNS query were to be performed each time a MTC Server needed to determine the current reachable IP addresses of a particular UE used for MTC. Additionally, this approach significantly reduces the number of DNS updates that must be performed relative to if a DNS update were to be performed each time a PDN connection was established or disconnected for a UE used for MTC (aka dynamic DNS).

The sample call flow scenario depicted in Figure 6.x.2-1 illustrates how MT communication can be achieved through the use of the hostname device identity lookup of the IP address of the assigned DT-GW, followed by initiation of MT communications via the assigned DT-GW over the MTCsp reference point.

 Figure 6.46.2-1: Call flow scenario for MT communications address resolution via DT-GW

1. Initially, e.g. when the UE used for MTC subscription is provisioned or changed, a DT-GW of the HPLMN is assigned as part of the subscription data stored in the HSS/HLR. Afterwards, the DT-GW performs a DNS update to the DNS authoritative server that stores the association between the hostname of the UE and the assigned DT-GW address.

1'. Alternatively, the HSS/HLR can perform the DNS update to the DNS server.

2. At some point thereafter, the MTC Server performs a DNS query for the hostname of the UE in order to determine the address of the assigned DT-GW. The MTC Server may then store the assigned DT-GW address for later use while assuming the assigned DT-GW will largely not be changed for the UE.

3. At some point thereafter, the MTC Server needs to initiate MT communicate with the UE, and thus will send the device trigger indication to the assigned DT-GW over MTCsp.

4. The network delivers the device trigger indication to the UE.

5. A PDN connection is initiated and established for the UE that is reachable by the MTC Server.

6. Once the IP and/or port numbers to use for IP communications is known, the MTC server can initiate the IP communications.

### 6.46.3 Impacts on existing nodes or functionality

Impacts on CN nodes:

- DT-GW solution specified in clause 6.45 shall be supported by the Core Network;

- Either:

- a network interface between authoritative DNS server and DT-GW is required to perform DNS updates when the assigned DT-GW for a UE used for MTC is initially assigned or changed; or

- the HSS/HLR is required to perform DNS updates when the assigned DT-GW for a UE used for MTC is initially assigned or changed.

- DT-GW must be able to map between the hostname of the device and the 3GPP/EPS-level subscription identity (e.g. MSISDN, IMSI and/or ICCID)..

### 6.46.4 Evaluation

Benefits:

- DNS update and DNS query frequency drastically less vs. requiring a DNS update/query each time a PDN connection is established/disconnected or the IP address of the device changes;

- As assigned DT-GW will rarely change, if at all, little risk of “middlemen” ISPs ignoring the TTL for a DNS record containing the association of the hostname of the UE used for MTC and the assigned DT-GW address;

- For security, DNS updates of the authoritative DNS server can be limited to only originating from within the HPLMN;

- Can support both MSISDN-based and MSISDN-less subscriptions (with phased rollout approach and/or simultaneously);

Drawbacks:

- Dependency on DT-GW entity deployment in HPLMN.

## 6.47 Solution – UE without unique MSISDN using ICCID

### 6.47.1 Problem Solved / Gains Provided

See clause 5.8 "Key Issue – MTC Device Trigger", see clause 5.13 "Key Issue – MTC Identifiers".

### 6.47.2 General

A unique Integrated Circuit Card ID (ICCID), defined by ITU-T Recommendation E.118 [7], is stored today in every UICC. The ICCID may be used by a UE used for MTC, mobile network, MTC Server, MTC user, DT-GW, etcetera as a unique 3GPP/EPS-level device subscriber identity for PS only devices that do not specifically require an MSISDN (i.e. no Circuit-Switched support).

The ICCID is a 20-digit number comprised of a variable length (maximum 7-digits) Issue Identification Number (IIN), a variable length (11 to 14 digits) Individual account identification number and a check digit. It is stored in the UICC Elementary File, EFICCID and efficiently encoded in BCD format (1-nibble per digit) as described in ETSI TS 102.221 [8].

An ICCID with the minimum sized Individual account identification number (11-digits) provides ~10^11 or 100B unique identifiers per IIN. This amount per issuer (e.g. per MNO) would appear to be more than adequate to provide a new unique subscription identifier for the expected onslaught of new M2M devices.

Similar to the MSISDN, the composition of the ICCID contains enough routeing information that can be used to identify the HSS/HLR of the MS/UE. The IIN is composed of a Country code field (analogous to the CC in the MSISDN or MCC in the IMSI) and an Issue identifier number field (analogous to the NDC in the MSISDN or the MNC in the IMSI). If further routeing information is required, it could be contained in the first few digits of the Individual account identification number field.

A hostname device identity (e.g. FQDN, URI or 3GPP specific URN) could be used inside and/or outside the mobile network to resolve the ICCID. The ICCID could be included as part of the hostname device identity (e.g. FQDN: mtc.ICCID.pub.3gppnetworks.org or ICCID.userid.serviceproviderid.topdomain) in order to associate a hostname with a particular UE used for MTC.

If flexibility for 1-to-1 mapping between the new unique subscription identifier and IMSI are required (i.e. multiple unique subscription identifiers per IMSI) then the ICCID could be used as a base for a set of multiple unique IDs associated with a particular IMSI.

The impacted network entities and interface protocols may be enhanced to support the above functionality so that a subscription can alternatively be identified by either:

a) a common MSISDN used in combination with a unique ICCID; or

b) just a unique ICCID

With regards to SMS, for approach a, the ICCID could be added to a new address field or as the first few bytes of user data. For the latter case, care should be taken that the extra user data bytes to hold the ICCID do not cause SM fragmentation. For approach b, the ICCID could replace the MSISDN as the address field. Similar mechanisms could be used for addressing in the SIP headers for SMS over IP.

### 6.47.3 Impacts on existing nodes or functionality

### 6.47.4 Evaluation

Benefits:

- provides a pre-existing unique ID that is generated and available today at the device;

- could be a base for unique IDs when multiple subscription identifiers per IMSI are required;

- plethora (~100B) of unique IDs per Issue Identification Number;

- efficiently encoded.

Drawbacks:

- if (U)SIM needs to be swapped to change network operator subscription, ICCID will not be portable to new network operator;

- if (U)SIM is permanently coupled to ME, when subscription needs to be swapped to a different UE/MS, ICCID will not be portable to new device and MNO cannot use ICCID as a permanent identifier for the subscription;

Editor's Note: It is FFS if subscription identifier portability is required for PS only subscriptions without MSISDN.

- the granularity for the ICCID is per MT and there could be multiple TEs per MT;

- similar to MSISDN, ICCID identifier of a UE/MS is easily ascertainable (e.g. sometimes printed on inside device).

## 6.48 Solution - Transfer data via SMS for MTC Devices sharing one MSISDN

### 6.48.1 Problem Solved / Gains Provided

See clause 5.2 “Key Issue – MTC Devices communicating with one or more MTC Servers.” and 5.13 “Key Issue - MTC Identifiers”

### 6.48.2 General

For the lack of MSISDN, MTC Devices belonging to the same MTC Subscriber could share one MSISDN for the purpose of transferring data via SMS. For these MTC Devices, a static unique “MTC Device ID” (e.g. an FQDN identifier or a private number specific to the MTC device) needs to be assigned and the association between the “MTC Device ID” and the IMSI is stored in HLR/HSS and optionally in the VAS AS.

Editor’s note: The static MTC Device ID” can be configured into the MTC Device via OMA DM or SIM OTA. How the “MTC Device ID” is made secure/unalterable is FFS.

Editor’s note: How the coupling between the common MSISDN and a static unique “MTC Device ID” can support number portability requirements, if needed, is FFS.

For MO communication of MTC devices sharing one MSISDN via SMS (i.e. the SMS is sent from the MTC Device to the MTC Server), the MTC Device shall insert the “MTC Device ID” into the SMS. The MTC Server identifies the MTC Device by the “MTC Device ID” contained in the SMS.

Alternatively, the “MTC Device ID” is inserted by the MSC/SGSN in the MAP-MO-FORWARD-SHORT-MESSAGE similar to how it works with the MSISDN in current specifications.

For MT communication of MTC devices sharing one MSISDN via SMS (i.e. the SMS is sent from the MTC Server to the MTC Device), the following procedures are performed:

* The MTC Server sends a SMS with the “MTC Device ID” in the header or the body of the SMS and the DA (destination address) of the SMS is set to the common MSISDN of the target MTC Device. And the SMS is routed to the VAS AS serving the MTC Devices identified by the common MSISDN.
* The VAS AS acts as an SMS GMSC to interrogate the HLR/HSS with the “MTC Device ID” which is obtained from the SMS directly. Or, if the VAS AS has stored the mapping information between the IMSI and the “MTC Device ID” of the MTC Device, the VAS AS interrogates the HLR/HSS with the IMSI of the MTC Device, based on the “MTC Device ID” in the SMS.
* The VAS AS delivers the SMS to the MTC Device according to the routing info returned from the HLR/HSS.
* The MTC Device verifies the “MTC Device ID” in the message upon receiving the SMS.

Alternatively, in case having stored the internal association between “MTC Device ID” and the IMSI, VAS AS can submit to the SMS Center a new SMS as specified in TS 23.142 [9] with the DA of the SMS set to the IMSI of the MTC Device. After receiving the SMS submitted by the VAS AS, SMS GMSC interrogates the HLR/HSS with the IMSI. With the returned routing information from HLR/HSS, SMS GMSC delivers the SMS to the MTC Devices as specified in TS 23.040.

Another alternative method is that the SMS GMSC interrogates the HLR/HSS with the “MTC Device ID” which is obtained from the SMS and delivers the SMS as specified in TS 23.040 [10] when receiving **t**he SMS from the MTC Server. No VAS AS is involved in this alternative.

Editor’s Note：The use of the shared MSISDN in the delivery of SMSs needs to be further developed.

### 6.48.3 Impacts on existing nodes or functionality

### 6.48.4 Evaluation

Drawbacks:

* Including the “MTC Device ID” inside the SMS would decrease the effective payload size. Some “MTC device ID” proposed in this TR may exceed the size of SMS, e.g. an URI.
* The MSC/SGSN may have problems with large numbers of devices sharing the same MSISDN.

# 7 Conclusions

Editor's Note: This clause is intended to list conclusions that have been agreed during the course of the work item activities.

## 7.1 Interim conclusions for release 10 specification work

This clause contains the agreed conclusions corresponding to Key Issue 5.12 and 5.14. 3GPP Release 10 specifications should be developed in the following areas:

a) the UE behaviour changes outlined in bullets a, b, c, d, and e in clause 6.33;

b) the M2M device indicators outlined in bullets a, b,and c in clause 6.34 (some of which are also mentioned in clause s 6.20, 6.23 and 6.26;

c) the non HPLMN (PLMN type) and Low-Priority-device style access class barring functionality outlined in clause s 5.12, 5.14 and 6.28.4;

NOTE: Updates to SA1 specifications such as TS 22.011 may be needed.

'Course grained' (i.e. "Low-Priority-Access" and "PLMN type") MTC access barring triggered via O+M into the RAN, internal RAN functionality, and by signalling from the Core Network is expected to be included in Rel-10. Other options for broadcasting of MTC access barring by RAN (e.g. based on the APN or MTC Group) may be considered for Rel-11.

d) the use of RR(C) connection reject messages with extended Wait Times outlined in clause s 6.23 and 6.26;

e) the use of M2M device specific (long) periodic update timers in MM, GMM and EMM signalling, including signalling from HSS to MSC/SGSN/MME (see clause 6.20);

f) in combination with the use of long, MTC specific PTU/PRU/PLU timers, the specification of signalling that permits the operator to command M2M devices to use Network Mode Of Operation I while keeping existing mobiles in Network Mode of Operation II (see clause s 5.14 and 6.20);

g) the specification of MM/GMM/EMM functionality that can limit load on CN entities of all local PLMNs (e.g. by the transmission of an RA Update ACCEPT message with PRU timer of 20 minutes rather than an RA Update Reject message);

h) the use of NAS-level back-off timer per APN to reject Attach and connectivity establishment requests as outlined in 6.22;

i) The use of connectivity establishment request rejection at MME/SGSN and PGW/GGSN as outlined in 6.22.

j) The use of the MME/SGSN overload control by DL MTC traffic throttling such as described in sect 6.30;

k) ///list to be completed. ///

## 7.2 Later Conclusions

Editor's note: text to be added.

# 8 Impacts to normative specifications

Editor's Note: This clause is intended to capture the impacts to normative specifications within the responsibility of SA2. It can be used as a placeholder to document agreements until a set of normative CRs can be generated for the selected solutions(s)

## 8.1 Related to Interim conclusions for release 10 specification work

The changes outlined in bullets a through g in clause 7.1 have minimal impact on SA2's specifications. Probably, some general clause s could be added to TS 23.060 and TS 23.401 to describe the overall problem and solutions.

With the exception of TS 23.122, and a new OMA DM Managed Object, stage 3 work is probably also relatively limited: e.g. a few new codepoints or information elements are needed in the NAS signalling (TSs 24.008 and 24.301); the HSS-MSC/SGSN/MME signalling (TS 29.002 and TS 29.272); the UE-RAN signalling (TS 36.331, TS 25.331 and TS 44.018); and possibly in the S1/Iu/Gb/A interface Overload messages.

Modified TS 23.122 procedures and the associated UE interactions with multiple local PLMNs probably represents the major complex task ahead in Release 10.

Editor's note: The impact of bullets h, i and j in clause 7.1 still has to be checked.

## 8.2 Related to Later Conclusions

# Annex A: Stage 2 PS Dependencies on MSISDN-based Subscriptions

## A.1 General Considerations

In order to facilitate the enhancement of the stage 2 architecture to support MSISDN-less subscriptions for PS only devices, this annex attempts to:

a) summarize all the stage 2 PS dependencies on the MSISDN; and

b) analyse the stage 2 impact of supporting MSISDN-less subscriptions for PS only MS/UEs.

## A.2 PS stage 2 MSISDN dependencies

### A.2.1 General network architecture

1) TS 23002-a11 (3GPP PLMN network architecture overview);

a) clause 4.1.1.1.3 - HSS user identification handling includes providing relationship between MSISDN and other appropriate user identities in the PS domain;

2) TS 23008-920 (organization of subscriber data);

a) clause 2.1 – specifies MSISDN, basic MSISDN and MSISDN-Alert indicator as permanent UE/MS subscriber data stored in Gn/Gp-SGSN as conditionally appropriate;

b) clause 3B.1.2 – specifies MSISDN is used for WLAN-IW subscription;

c) clause 5 – possible to retrieve or store subscriber data for a particular MS/UE from the HSS, 3GPP AAA Server , 3GPP AAA Proxy, WAG, PDG through reference to the MSISDN and IMSI;

3) TS 23228-a31 (IMS);

a) clause 4.2.4a – Sh interface supports mechanisms for transfer of user related data stored in the HSS, including the MSISDN;

Editor's Note: Additional dependencies are FFS.

### A.2.2 GPRS

1) TS 23060-a20 (GPRS);

a) MSISDN is stored as part of HLR/HSS GPRS/EPS subscription data (clause 13.1), SGSN MM and PDP/EPS bearer contexts (clause 13.2.3) and GGSN PDP Context (clause 13.3);

b) clause 9.2.2.1 - SGSN sends MSISDN to GGSN in PDP Context Activation procedure;

c) clause 9.2.2.1A - SGSN sends MSISDN to S-GW in Create Session Request procedure;

### A.2.3 EPS

1) TS 23401-a21 (EPS);

a) clause 5.7.1 – The basic MSISDN is optionally stored in the subscription data stored in the HSS;

b) clauses 5.7.2, 5.7.3 and 5.7.4 – The presence of the basic MSISDN in the MM context and EPS bearer context information stored in the MME, S-GW and P-GW is dictated by its storage in the HSS;

Editor's Note: Additional dependencies are FFS.

### A.2.4 WLAN

1) TS 23234-900 (WLAN interworking)

a) clause F.3.1 – TTG retrieves the IMSI and MSISDN from the AAA server during (Interworking procedure over Gn') Tunnel establishment procedure;

Editor's Note: Additional dependencies are FFS.

### A.2.5 SMS

Figure A.2.5-1 aims at illustrating the use of MSISDN for SMS communication today. Depicted is a scenario where both the SMS Originator (UE-O) and SMS Recipient (UE-R) are roaming in VPLMN-O and VPLMN-R, respectively, and there is no Home Routeing of SMS.

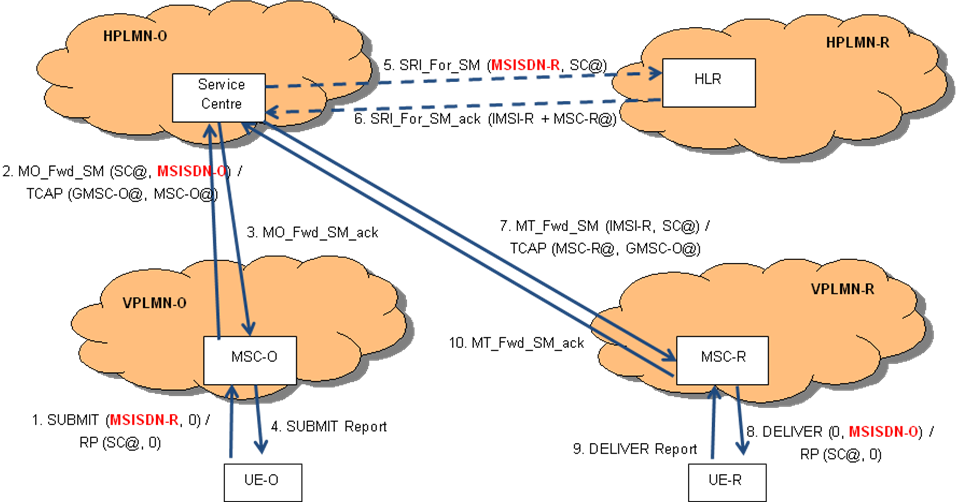


Figure A.2.5-1: Use of MSISDN for SMS communication (no Home Routeing)

1) TS 23040-920 (SMS)

a) SM-RL (Short Message Relay Layer) protocol messages can include MSISDN / MSIsdn-Alert in the following messages:

1) clause 3.2.6 - SMS-GMSC/IP-SM-GW includes MSISDN and conditionally MSIsdn-Alert to set the Message Waiting Data into the HLR or to inform the HLR of successful SM transfer after polling via MAP-REPORT-SM-DELIVERY-STATUS (see 29.002 clause 12.3);

2) clause 9.3.2.4 - conditionally includes the MSIsdn-Alert in RP‑ERROR => MAP-REPORT-SM-DELIVERY-STATUS (see 29.002 clause 12.3) when transfer attempt failed because the MS is not reachable or because the MS memory capacity was exceeded;

3) clause 9.3.2.1 - RP MO DATA => MAP-MO-FORWARD-SHORT-MESSAGE (see 29.002 clause 12.2);

4) clause 9.3.2.2 - RP-MT-DATA => MAP-MT-FORWARD-SHORT-MESSAGE (see 29.002 clause 12.9);

b) clause 8.1.4 – SMS Router may store the MSISDN against the MT Correlation ID as part of the a routing information retrieval operation;

c) clause 8.2.1 – MSC/SGSN retrieves MSISDN from VLR/HLR after receiving a short message TPDU from the MS/UE;

d) clauses 9.2.2 and 9.1.2.5 – the Short Message Transfer Layer (SM-TL) protocol allows for MSISDN (E.164) or other types of number-plan-identification. However the address size is limited to 12 octets, which may not be sufficient for some very long identifiers. The MSISDN is used as the address in the following messages:

1) SMS‑DELIVER (clause 9.2.2.1);

2) SMS‑SUBMIT (clause 9.2.2.2);

3) SMS‑STATUS‑REPORT (clause 9.2.2.3);

4) SMS‑COMMAND (clause 9.2.2.4).

e) There is no impact on the SS7 TCAP, the addresses used on these layers being node addresses (MSC, GMSC) rather than device addresses;

2) TS 23204-a20 (SMS over generic 3GPP IP access)

a) clause 5.3.1 - IP-SM-GW acquires and maintains knowledge of the association between the MSISDN, IMSI and the address of the S-CSCF serving of the user;

b) clause 5.3.1 – For SM MT, IP-SM-GW maps the recipient’s address from an MSISDN/IMSI to TEL URI format when receiving an SMS for an IP-based UE;

Editor's Note: Additional dependencies are FFS.

### A.2.6 IMS

1) TS 23167-b01 (IMS emergency sessions);

a) clause 7.5.1 – PSAP uses the MSISDN (E.164) of the user for call back;

Editor's Note: Additional dependencies are FFS.

### A.2.7 PCC

1) TS 23203-b01 (PCC architecture);

a) clauses 6.2.1.1, A.1.3.2.1.1 and A.1.3.2.2.1 – subscriber identity (e.g. IMSI, MSISDN) provided to PCRF as input for PCC decisions;

b) clause A.1.3.2.2.1 - For each PDP context, the PCEF shall accept the MSISDN during bearer establishment and modification and shall use this information in the OCS request/reporting or request for PCC rules;

Editor's Note: Additional dependencies are FFS.

### A.2.8 LCS

1) TS 23271-a11 (LCS);

Editor's Note: Dependencies are FFS.

### A.2.9 SIPTO

1) TS 23060-a20 (GPRS);

a) Clause 5.3.12.2 and Annex B.1-2 – to support activation of "SIPTO at Iu-ps" function, the SGSN sends MSISDN to target RNC during the:

1) SRNS Relocation procedures (clauses 6.9.2.2.1, 6.9.2.2.2 and 6.9.2.2.3);

2) Service Request Procedures (clauses 6.12.1 and 6.12.2);

3) the intersystem change procedures from A/Gb mode to Iu mode (clauses 6.13.1.2.1 and 6.13.2.2.1);

4) RAB Assignment procedure (clause 12.7.4.1).

Editor's Note: Additional dependencies are FFS.

### A.2.10 CAMEL

1) TS 23078-910 (CAMEL Phase 3);

a) clause 6.6.1.5 – for GPRS interworking for CAMEL, basic MSISDN included in the gprsSSF to gsmSCF Initial DP GPRS IF when a trigger is detected at a DP in the GPRS state model, to request instructions from the gsmSCF:

b) clause 7.6.1.2 – for MO/MT SMS interworking for CAMEL, MSISDN included as the Called/Calling Party Number in the gprsSSF to gsmSCF Initial DP SMS IF when a trigger is detected at a DP in the SMS state model, to request instructions from the gsmSCF:

c) clause 7.6.2.1 – for MO/MT SMS interworking for CAMEL, MSISDN may be included as the Calling Party Number in the gsmSCF/gsmSSF or gprsSSF Connect SMS IF to request the gsmSSF/gprsSSF to perform the actions to route the Short Message to a specific destination (for MO SMS) or to deliver the Short Message to the MS (for MT SMS);

d) clause 9.4.1.1 – for GPRS Mobility Management in CAMEL, basic MSISDN included as GPRS mobile subscriber identity in SGSN to gsmSCF Mobility Management event IF;

e) clause 10.3.1.1 –for control and interrogation of subscription data by CAMEL, MSISDN or IMSI used as subscription identity in gsmSCF to HLR Any Time Modification Request IF;

f) clause 10.3.1.2 – for control and interrogation of subscription data by CAMEL, MSISDN and/or IMSI used as subscription identity in gsmSCF to HLR Any Time Subscription Interrogation Request IF;

g) clause 10.3.2.2 – for control and interrogation of subscription data by CAMEL, MSISDNs used as subscription identity in HLR to gsmSCF Any Time Subscription Interrogation ack IF;

h) clause 10.3.2.3 – for control and interrogation of subscription data by CAMEL, MSISDN used as subscription identity in HLR to gsmSCF Notify Subscriber Data Change IF;

i) clause 10.3.3.1 – for control and interrogation of subscription data by CAMEL, MSISDN or IMSI used as subscription identity in IP-SM-GW to HLR Any Time Modification Request IF used to register the IP-SM-GW for a subscriber in the HLR;

j) clause 11.3.1.1 – for subscriber location and subscriber state information retrieval by CAMEL, MSISDN or IMSI used as subscription identity in gsmSCF to GMLC Any Time Interrogation Request IF used to request information (Mobile Station location) from the GMLC;

k) clause 11.3.3.1 – for subscriber location and subscriber state information retrieval by CAMEL, MSISDN or IMSI used as subscription identity in gsmSCF to HLR Any Time Interrogation Request IF used to request information (any one or more of subscriber state, subscriber location, IMEI (with software version) and MS classmark information for the requested domain) from the HLR;

Editor's Note: Additional dependencies are FFS.

### A.2.11 Other services

1) TS 23066-900 (MNP);

a) Various – describes several alternatives for the realisation of Mobile Number Portability to retain ones MSISDN;

2) TS 23141-900 (Presence Service)

a) clause 6.1.1 – MSISDN can be the contact address attribute of the subscriber;

3) TS 23246-950 (MBMS)

a) clauses 8.2 and 10.3 – MSISDN is passed from SGSN to GGSN and GGSN to MB-SC during MBMS Multicast Service Activation to provide the operator with the ability to associate GPRS location information (i.e. serving network identity) with a user;

4) TS 23240-900 (3GPP GUP)

a) clause B – GUP access for the "PLMN specific user information" by the S-CSCF and AS includes the MSISDN;

b) clause B – GUP access for the "Authorized and subscribed service information for CS & PS" by the MSC/VLR, GMSC, SGSN, GGSN and MMS server includes the MSISDN;

Editor's Note: Additional dependencies are FFS.

## A.3 Impact of MSISDN-less subscriptions for PS only MS/UEs

Editor's Note: analysis is FFS.

# Annex B: Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **Old** | **New** |
| 2009-11 | SA2#76 |  |  |  | Version 0.0.0 Editor's Initial Draft (S2-097387) approved in SA2 #76 | - | 0.0.0 |
| 2009-12 | SA2 #76 |  |  |  | Included approved tdocs in SA2 #76: S2‑097387, S2‑097393, S2‑097481, S2‑097555, S2‑097556, S2‑097563, S2‑097564, S2‑097565, S2‑097570 | 0.0.0 | 0.1.0 |
| 2009-12 | SA2 #76 |  |  |  | Editorial Corrections | 0.1.0 | 0.1.1 |
| 2010-01 | SA2#76 |  |  |  | Editorial Corrections | 0.1.1 | 0.1.2 |
| 2010-01 | SA2 #77 |  |  |  | Included approved tdocs in SA2 #77: S2‑100809, S2‑100814, S2‑100815, S2‑100864, S2‑100865, S2‑100867, S2‑100868, S2‑100872, S2‑100951; Editorial Corrections | 0.1.2 | 0.2.0 |
| 2010-01 | SA2 #77 |  |  |  | The previous version contained a corrupted file. | 0.2.0 | 0.2.1 |
| 2010-03 | SA2 #78 |  |  |  | Restructure TR (all solutions to a new Clause 6) as per S2-101124  Included approved tdocs in SA2 #78: S2-101416, S2‑101450, S2‑101740, S2‑101741, S2‑101742, S2‑101806, S2‑101807, S2‑101808, S2‑101809, S2‑101806, S2‑101810,S2‑101814, S2‑101830, S2‑101831 | 0.2.1 | 0.3.0 |
| 2010-03 | SA2 #78 |  |  |  | Editorial Corrections | 0.3.0 | 0.3.1 |
| 2010-03 | SA2 #78 |  |  |  | Corrected the implementation of S2-101806 | 0.3.1 | 0.3.2 |
| 2010-05 | SA2 #79 |  |  |  | Editorial Corrections, S2-102759, S2‑102894, S2-102903, S2‑102984, S2‑102985, S2‑102986, S2‑102987, S2‑102988, S2‑103088, S2‑103089, S2-103090, S2-103091, S2-103092 | 0.3.2 | 0.4.0 |
| 2010-06 | SA2 #79 |  |  |  | Implementation correction for S2-103089 and S2-102986. Correction to the list of tdocs used to implement version 0.4.0. | 0.4.0 | 0.4.1 |
| 2010-07 | SA2 #79e |  |  |  | Implementation and Rapporteur's merging of approved and endorsed P-CRs: S2-103105, S2-103116, S2-103131, S2‑103132, S2-103136, S2‑103160, S2‑103162, S2‑103168, S2‑103170, S2‑103183, S2‑103184, S2‑103185, S2‑103189, S2‑103206, S2‑103208, S2‑103210, S2‑103211, S2‑103212, S2‑103213, S2‑103214, S2‑103215, S2‑103220, S2‑103223, S2‑103224, S2‑103227, S2‑103228, S2‑103230, S2‑103233, S2‑103234, S2‑103235 | 0.4.1 | 0.5.0 |
| 2010-07 | SA2 #79e |  |  |  | Correction to the listof tdocs used to implement 0.5.0, to the implementation of S2‑103210, S2‑103223 and S2‑103230 additional approved tdocs implemented S2‑103207, S2‑103225 | 0.5.0 | 0.5.1 |
| 2010-09 | SP-49e | SP-100562 | - | - | MCC Update to version 1.0.0 for presentation to TSG SA for information | 0.5.1 | 1.0.0 |
| 2011-02 | SA2 83 |  |  |  | Update the release number to 11. | 1.0.0 | 1.0.1 |
| 2011-03 | SA2 83 |  |  |  | Implementation of S2‑111032, S2‑111218, S2‑111220, S2‑111223, S2‑111225, S2‑111226, S2‑111227, S2‑111228, S2‑111256, S2‑111266, S2‑111268 | 1.0.1 | 1.1.0 |
| 2011-04 | SA2 83 |  |  |  | Correct implementation of S2‑111266, do not implement S2‑111218, editorial corrections of some initial list items. | 1.1.0 | 1.1.1 |
| 2011-04 | SA2 84 |  |  |  | Implementation of S2-112023, S2-112119, S2-112163, S2-112164, S2-112166, S2-112167, S2-112170, S2-112171, S2-112172, S2‑112205, S2-112206 | 1.1.1 | 1.2.0 |