3GPP TR 22.888 V1.0.0 (2013-02)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Study on Enhancements for MTC;
(Release 12)

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 3GPP Organizational Partners and shall not be implemented.
This Report is provided for future development work within 3GPP only. 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

<keyword[, keyword]>

3GPP

Postal address

3GPP support office address

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

Internet

http://www.3gpp.org

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.

© 2013, 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 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

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

Introduction

The Release 10 work item Network Improvements for Machine Type Communications – Stage 1 for NIMTC specified a number of requirements to make the network more suitable for machine type communications. Additional aspects need to be studied before proceeding with their potential inclusion in the normative work.

In the course of the Release 10 work item, it was decided to leave out MTC Device to MTC Device communications from Release 10. This because it was felt it was not possible to do it justice within the Release 10 time frame. Nevertheless, MTC Device to MTC Device communications are expected to become of major importance, especially with consumer devices communicating directly to each other. Therefore, this work item aims to study the network improvements requirements of MTC Device to MTC Device scenarios. A particular aspect of MTC Device to MTC Device scenarios is the identification and functionality needed to set up a connection towards a MTC Device. The IMS domain may provide a solution for this required functionality. In this case the impacts and requirements of MTC on IMS needs to be studied.

Additionally MTC Devices often act as a gateway for a capillary network of other MTC Devices or non-3GPP devices. These gateway MTC Devices may have specific requirements on the mobile network, which have not yet been taken into account in the Release 10 NIMTC work item. Study is needed to determine to what extent improvements are needed and can be specified by 3GPP for MTC Devices that act as a gateway for 'capillary networks' of other devices. Also alignment with what is specified by ETSI TC M2M on this aspect is needed.

Further optimisations may be possible for (groups of) MTC Devices that are co-located. An example of this could be a car with a number of different MTC Devices that always move along together. Optimisations for these kind of scenarios have been suggested, but have not yet been taken into account in the Release 10 NIMTC. Study is needed to determine to what extent network improvements can be specified for co-located MTC Devices.

Because of the different characteristics of Machine-Type Communications, the optimal network for MTC may not be the same as the optimal network for human to human communications. Optimisations of network selections and steering of roaming may be needed. Study is needed to determine to what extent improvements are needed on network selection and steering of roaming for MTC.

Many MTC applications use some kind of location tracking. E.g. the existing LCS framework could be used to provide location information for these kinds of MTC applications. Study is needed to determine to what extent improvements are needed for MTC location tracking.

MTC brings a new concept of a MTC User and MTC Server. So far little attention has been given to service requirements on the communication between the network and the MTC User/MTC Server. Also alignment with what is specified by ETSI TC M2M on that aspect is needed. Study is needed on what kind of service requirements are needed and can be specified by 3GPP.

1 Scope

Objective of this work item is to study additional requirements, use cases and functionality beyond that specified by the Release 10 NIMTC work item on the following aspects:

- network improvements for MTC Device to MTC Device communications via one or more PLMNs.

  NOTE: direct-mode communication between devices is out of scope.

- possible improvements for MTC Devices that act as a gateway for 'capillary networks' of other devices.

  NOTE: capillary networks themselves are out of scope of 3GPP.

- network improvements for groups of MTC Devices that are co-located with other MTC Devices.
- improvements on network selection mechanisms and steering of roaming for MTC devices.
- possible enhancements to IMS to support MTC.
- possible improvements for location tracking of MTC Devices.
- service requirements on communications between PLMN and the MTC User/MTC Server (e.g. how the MTC User can set event to be monitored with MTC Monitoring).
- possible service requirements to optimize MTC Devices.
- possible New MTC Features to further improve the network for MTC.

For each of the aspects above, the Study will need to identify what kind of (if any) impacts there are on 3GPP standards.

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 TR 41.001: "GSM Release specifications".

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

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [x] 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 [x].

MTC Device: A MTC Device is a UE equipped for Machine Type Communication, which communicates through a PLMN with MTC Server(s) and/or other MTC Device(s).

NOTE: MTC Device may communicate with MTC Gateway Device(s) or Local-Access Device(s) using local connectivity.

Local-Access Device: A Local-Access Device is a device in MTC Capillary Network, which has no 3GPP mobile communication capability.

NOTE 1: The Local-Access Device connects to an MTC Gateway Device via local connectivity to communicate through a PLMN with MTC Server(s), other MTC Device(s), and/or other Local-Access Device(s).

NOTE 2: Local connectivity between Local-Access Devices is out of 3GPP scope.

MTC Capillary Network: An MTC Capillary Network is a network of devices that provides local connectivity between devices within its coverage and MTC Gateway Device.

NOTE 1: Typically, examples of MTC Capillary Networks include personal/local area network technologies such as IEEE 802.15, Zigbee, Bluetooth, etc.

NOTE 2: The local connectivity within MTC Capillary Network is out of 3GPP scope.

MTC Gateway Device: An MTC Gateway Device is an MTC device equipped for Machine Type Communication, which acts as a gateway for a group of co-located MTC Devices or to connect MTC Devices and/or Local-Access Devices in an MTC Capillary Network to communicate through a PLMN with MTC Server(s), and/or other MTC Device(s).

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [x] 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 [x].

4 Study area

4.1 Communication via MTC Gateway Device

4.1.1 Scenario and Use-case 1

In this scenario, depicted in Figure 4.1.1-1, the MTC Gateway Device is a kind of MTC Device that has 3GPP mobile communication capability. The devices located at the MTC Capillary Network do not have 3GPP mobile communication capability, i.e. they are Local-Access Devices. They are connected to the MTC Gateway Device via local connectivity technologies such as IEEE 802.15, Zigbee, Bluetooth, etc. The MTC Gateway Device connects via 3GPP Access Networks to the operator network and communicate with the MTC Server(s). Thus the MTC Gateway Device acts as an agent for the Local-Access Devices in the MTC Capillary Network. The Local-Access Devices are not visible to the operator network. The MTC Gateway Device performs procedures such as authentication, authorization, registration, management and provisioning for the Local-Access Devices connected to it using local connectivity mechanisms.

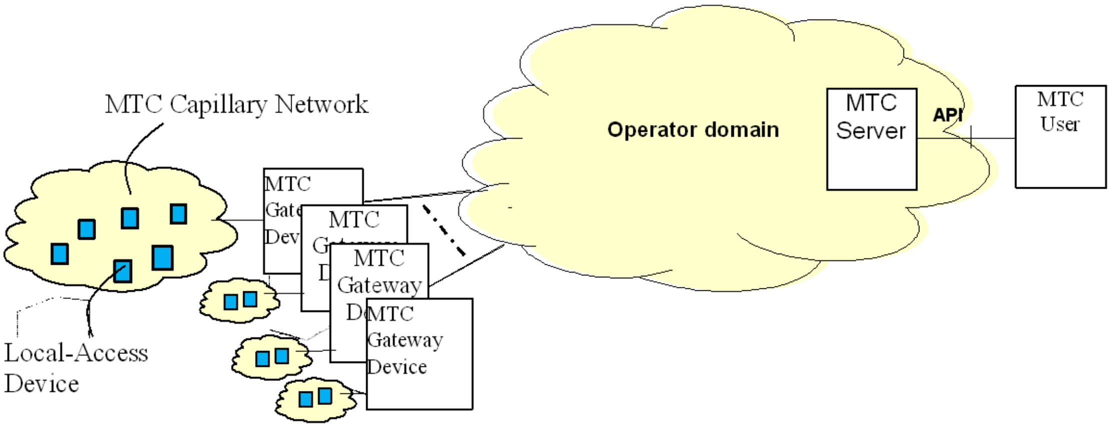

Figure 4.1.1-1: MTC Gateway Device Communication Scenario 1

Use Case 1: Smart Grid

In future smart grid applications, it might be necessary to provide a communications path between the utility and the home appliances through the M2M gateway (ETSI M2M) or communications hub. It is unlikely that each of these home appliances has a UE module installed. It is, however, reasonable to have an M2M gateway or communications hub to be an MTC Device. Hence, in such deployment, the home appliances in the home area network forms a capillary network behind an MTC Gateway Device (e.g. the M2M gateway or communications hub) from 3GPP perspective.

Use Case 2: Automotive

Future vehicles may contain many devices that use machine-type communications. For instance, the navigation unit may need access to real-time traffic information and map updates. An automatic toll-paying device will need to contact relevant authorities for toll payment. The car sensors network will need to communicate with the workshop to report on operating parameters of various parts of the car. A plug-in vehicle will need to communicate with the smart-grid to facilitate demand response kind of applications.

In one deployment model, all these devices may be implemented by a single manufacturer, and thus may communicate using common local area network protocol (e.g. the Controller Area Network), and have only a single MTC Device for access to 3GPP network. Such an MTC Device will become the MTC Gateway Device, providing access for a capillary network of Local-Access Devices in the vehicle.

4.1.2 Scenario and Use-Case 2

In this scenario, depicted in Figure 4.1.2-1, some or all of the devices forming the MTC Capillary have 3GPP mobile communication capability (i.e. MTC Devices) and some of the devices do not have 3GPP mobile communication capability, i.e. they are Local-Access Device. In this case all the devices that are connected to the MTC Gateway use local access. MTC Devices communicating directly with the network use their 3GPP mobile communication capability.

For example, a vehicle installed with an MTC Device of navigation and entertainment function may communicate with MTC Server independently at first to get some location service, entertainment service information. Then it moves into an airport or onto a ferry which deploys an MTC Gateway Device to provide local network connectivity for the devices within its coverage. This MTC Gateway Device may beforehand communicate with and download some useful information such as location, weather, entertainment, flight, etc from the MTC Server the vehicle previously communicated with. The MTC Device can connect to the MTC Gateway Device and fetch the information the driver wants directly from it. It can also request for additional information that the MTC Gateway Device does not provide from the MTC Server via the MTC Gateway Device. When the vehicle moves out of the coverage of the airport or of the ferry, it disconnects from the MTC Gateway Device and re-establishes connection with the operator network to communicate with the MTC Server.

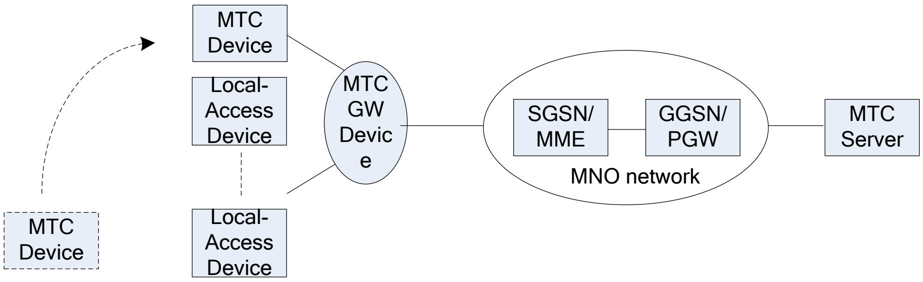

Figure 4.1.2-1: MTC Gateway Device Communication Scenario 2

Use Case: Mobile Rescue Team

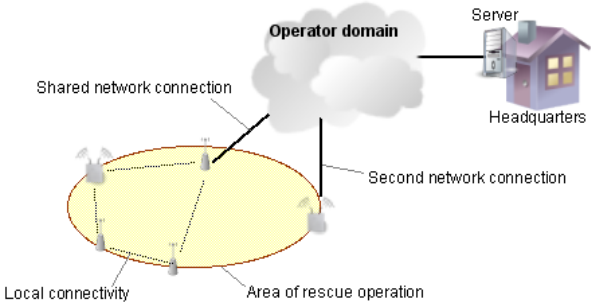

Figure 4.1.2-2A: Mobile Rescue Team

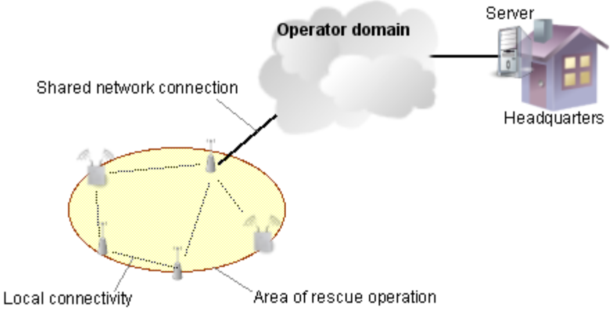

Figure 4.1.2-2B: Mobile Rescue Team

A group of devices (e.g. sensors) may be employed by a mobile emergency resuce team communicating with the rescue headquarter. In most applications, these devices need to communicate among themselves, in addition to communicating with the headquarter server. Hence, once the devices are deployed, a local network connectivity will usually be established among themselves (e.g. using Bluetooth, WiFi, or other local area network technology). With the local network established, it will be more resource efficient for the devices to communicate with the headquarter server via a single network connection through a "group representative"device or MTC Gateway Device (see Figure 4.1.2-2A).

However, depending on the nature of the emergency situation, different devices may be deployed for different rescue operations. Hence, there is a need for the grouping of devices to be dynamic, i.e. a device may join a group and later leave the group. A device, communicating with the rescue headquarter directly at first, moves into the coverage of the MTC Gateway Device of the local network. It can join this group and connect to this MTC Gateway Device using the local network connectivity. It can communicate with rescue headquarter through this MTC Gateway Device instead of communicating on the original network connection, communicate locally with other rescue device, and obtain some information directly from this MTC Gateway Device instead of downloading from the rescue headquarter (see Figure 4.1.2-2B).

4.1.3 Analysis

4.1.3.1 Model

For the above use cases, the following deployment model exist (refer to Figure 4.1.3-1):

- MTC Gateway Device acts as a gateway and provides connectivity of the devices forming an MTC Capillary Network to the 3GPP access network.
- The MTC Capillary Network may contain MTC Devices.
- The MTC Capillary Network may contain Local-Access Devices.

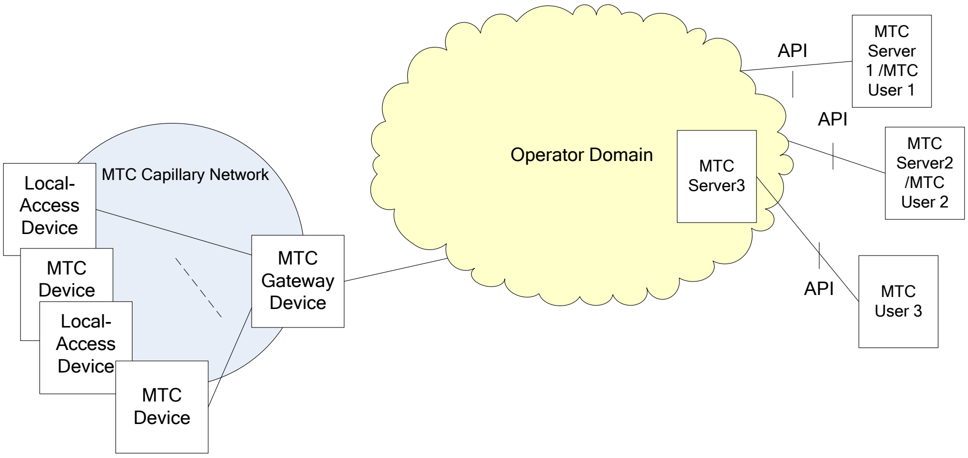

Figure 4.1.3-1: Deployment model with MTC Gateway Device communicating with MTC Server.

4.1.3.2 Addressing

Based on the model above, there is need for devices in a MTC Capillary Network to obtain connectivity via a MTC Gateway Device. In a packet-switched architecture, this is equivalent to the devices in the MTC Capillary Network being able to obtain a routable address through the MTC Gateway Device.

The case of Local Access Devices using non-IP communications within the MTC Capillary Network is not considered.

For IP addressing this means the local access devices be allocated private/public IPv4 addresses or global IPv6 addresses. In the above model, the MTC gateway device is a 3GPP device and is directly connected to the 3GPP network while the local access devices uses non-3GPP access technology (and is thus not "visible" to the 3GPP network),

NOTE 1: "multiple addresses" include e.g. the case of a range of continuous addresses, or multiple prefixes.

NOTE 2: the capillary network related details such as how the capillary network allocates addresses, validate uniqueness among each other, etc are out of scope.

4.2 MTC Device-to-Device Communication

4.2.1 Scenario and Use Case 1: Communicating directly

One MTC device can communicate with another MTC Device directly over 3GPP networks if it knows the IP address or MSISDN of the target MTC device.

Two cases are given to depict this kind of communication:

Case1: For IPv6 based communication, if MTC devices are statically assigned with an IPv6 address, the communication can be established if the IPv6 addresses are known by each side.

Case2: For MSISDN based communication (i.e.SMS), the originating MTC Device should know the MSISDN of the target side.

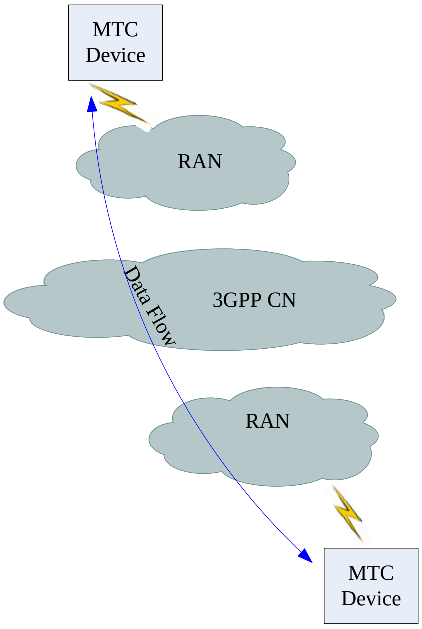

Figure 4.2.1-1: MTC Devices communicating directly with each other

4.2.2 Scenario and Use Case 2: Communicating via MTC Server

In this kind of communication, all data transmission will go through the MTC Server. The MTC Devices do not need to know the routable identifier of each other while the MTC Server possesses or is able to provide mechanisms to find the identifiers (routable or un-routable, e.g. IP address, MSISDN, application layer identifier, etc) of MTC Devices under its control. The originating MTC Device establishes connection with the MTC Server and sends out data, together with the identifier of the target side, to the MTC Server. The type of the identifier is specific to the MTC applications. The MTC Server then finds target MTC Device based on mechanisms such as application layer registration mechanism, downlink addressing mechanism, MTC Device triggering mechanism, etc, and forwards the data to the target MTC Device.

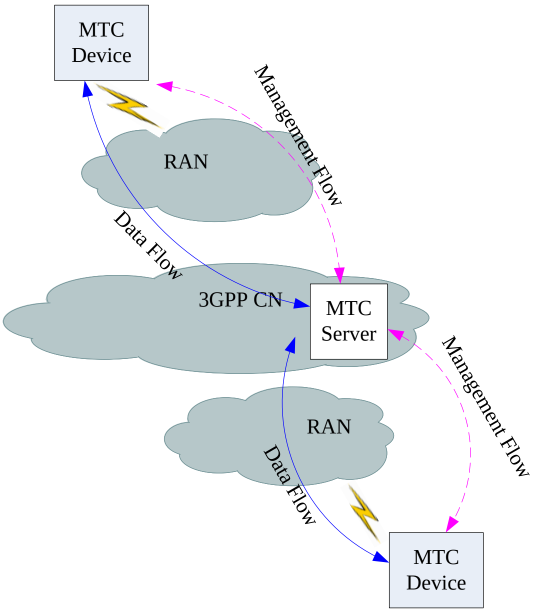

Figure 4.2.2-1: MTC Devices communicating with each other via MTC Server

4.2.3 Scenario and Use Case 3: Communicating with assistance from a Name resolution Function of the network/ the MTC Server

Besides communicating directly and communicating via MTC server, there is another kind of communication between MTC Devices, whose data transmission will go directly to each other, with establishment of data session assisted by a Name Resolution Function of network/MTC Server. A Name Resolution Function can be integrated in the existing network entities, e.g. DNS, etc or in the MTC Server.

In this kind of communication, the MTC Devices may only know the un-routable identifiers of each other (e.g. MSISDN, SIP URI, etc). The types of the identifiers are according to specific applications. These identifiers can not be used to target and route data to the remote communicating MTC Devices directly. Instead, a name resolution function is able to provide mechanisms to find remote communicating MTC Devices under its control. The originating MTC Device queries a name resolution function with the un-routable identifier of the target MTC Device. The name resolution function can then map the identifiers of the target MTC Device provided by the originating MTC Device to the routable identifiers (e.g. IP address for IP communication). After that, through appropriate mechanisms, the name resolution function returns the routable identifiers to the originating MTC Device. By retrieving the routable identifiers (e.g. IP address) of the target MTC Device, the originating MTC device can directly send data to the target MTC Device.

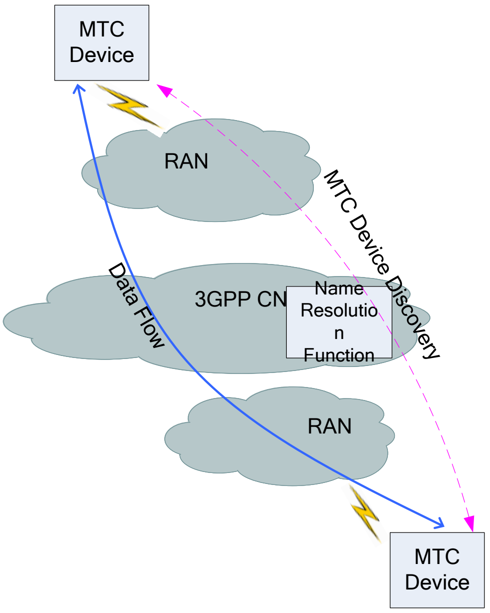

Figure 4.2.3-3: MTC Devices communicating with each other with assistance of network / MTC Server

4.2.4 Scenario and Use Case 4: Group Member Communication

As for MTC Devices belonging to one group, whether they can only communicate with MTC Devices in the same group or they can communicate with MTC Devices of other group depends on different MTC applications in different scenarios.

In most of the scenarios, for security and privacy consideration, (e.g., for home appliances control applications), MTC Devices of one group should be restricted to communicate with those devices not belonging to the same group.

However, there are also scenarios where the communication between MTC Devices of different groups is allowed, e.g., when visiting Bob's home, John may want to utilize Bob's TV, belonging to group A, to receive the pictures or video sending from a monitor in John' home, which belongs to group B.

4.2.5 Scenario and Use Case 5: M2M Communication with Network Coordination

4.2.5.1 General

Communication between MTC Devices may be established directly via the network, or established with the help of an MTC Server. When a MTC Device initiates a communication request to another MTC Device via the network, it may not know the status of the destination MTC Device and the communication may not be established due to various reasons. Similarly, when a MTC Device initiates a communication request to another MTC Device with the help of the MTC Sever, the MTC Server may not know the status of the destination MTC Device and the communication may not be established due to various reasons.

4.2.5.2 Congestion scenario

In the case of MTC Devices establishing communications directly via the network, when the radio access network of the destination MTC Device is congested, the communication is not established and the originating MTC Device receives a feedback from the network to avoid trying further request, which may lead to unnecessary load to network. Similarly in the case of MTC Devices establishing communications with the help of the MTC Server, the MTC Server receives a feedback from the network and the MTC Server can then (via the application layer) notify the originating MTC Device to avoid further communication attempts to the destination MTC Device.

4.2.5.3 Time controlled scenario

In the case of MTC Device establishing communication directly via the network, when the destination MTC Device is subject to the Time Controlled MTC Feature and communication is attempted outside the access grant time interval, the communication is not established and the originating MTC Device receives a feedback from the network to avoid trying further request, which may lead to unnecessary load to network. Similarly, in the case of MTC Device establishing communication with the help of the MTC Server, the MTC Server receives a feedback from the network and the MTC Server can then (via the application layer) notify the originating MTC Device to avoid further communication attempts to the destination MTC Device.

Note: the above two scenarios also apply to MTC Device to MTC Server communication.

4.2.5.4 Synchronized communication scenario

In order to save device battery, MTC Device can be attached to MTC Server and only use the PLMN network when communication is necessary (e.g., at certain scheduled time intervals). To avoid the situation where the destination MTC Device is not attached to the network when the originating entity attempts communication, the MTC Server can synchronize the timing of when MTC Devices are connected to the PLMN network (attached to the PLMN network).

For instance, when the MTC Server determines that it is time for device communication, the MTC Server requests the PLMN network to send triggers to the MTC Device. The MTC Device initiates communication (either directly via the network, or with the help of MTC Server). When the communication is completed, the MTC Server triggers the MTC Devices to disconnect.

4.2.6 Analysis

If one MTC Device wants to communicate with another MTC Device, several kinds of identifiers can be used to target the remote MTC device and route the data to it directly or indirectly, such as IMSI, MSISDN, IP address, or SIP URI etc.

Some kinds of identifiers are routable and can directly target the remote side. By using these kinds of identifiers the originating MTC Device can directly set up communication towards the remote end. For those identifiers which are not routable, the originating MTC Device may request the assistance from the network or the MTC server.

Thus, for this communication scenario the following use cases exist:

a) MTC Devices communicating over 3GPP networks with each other without intermediate MTC Server (refer to figure 4.2.6-1);

MTC Devices can communicate with each other directly;

- Data transmission between MTC Devices can be routed directly to each other, with establishment of data session assisted by a Name Resolution Function on network entities

b) MTC Devices communicating with each other with intermediate MTC Server (refer to figure 4.2.6-2)

- MTC Server(s) can be located outside of the network operator domain;
- MTC Server(s) can be located inside of the network operator domain;
- Data transmission between MTC Devices can be routed to each other via MTC Server(s);
- Data transmission between MTC Devices can be routed directly to each other, with establishment of data session assisted by a Name Resolution Function on the MTC Server.

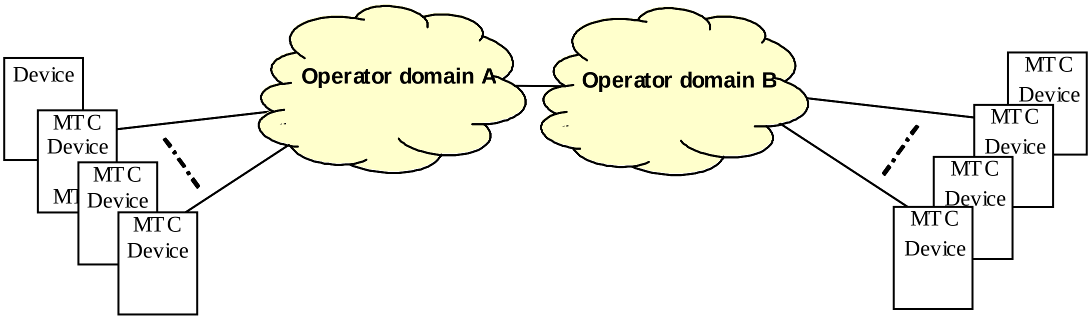

Figure 4.2.6-1: MTC Devices communicating with each other without intermediate MTC server.

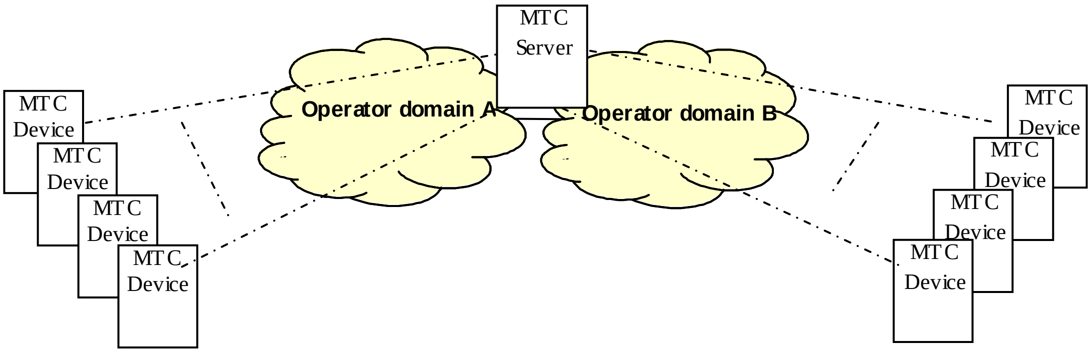

Figure 4.2.6-2: MTC Devices communicating with each other with intermediate MTC Server

4.3 Co-Located MTC Devices

4.3.1 Use Case: Cargo Tracking

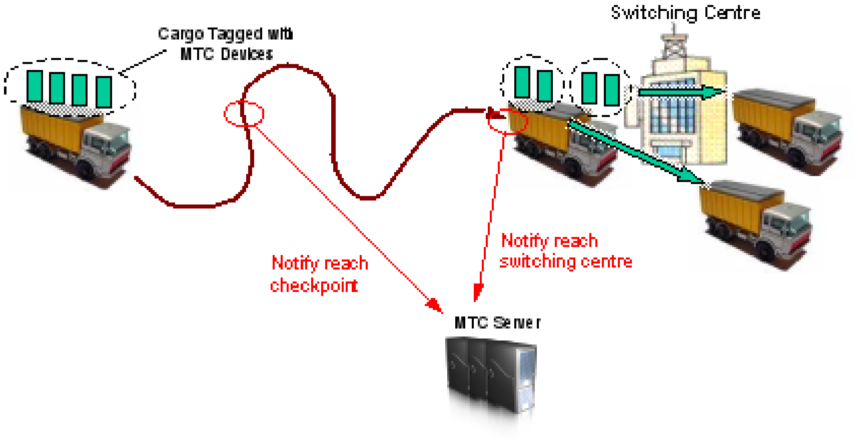

Figure 4.3-1: Cargo Tracking

Courier services may attach communication tags on customer's parcels/cargoes to track the current the location of the cargoes. While transporting, many such cargos may be placed in the same container truck. The courier service company may utilize third-party transport companies such that the cargoes on a single truck may be from different courier services. In addition, in order to optimize transport schedule, a cargo may switch between different container trucks before reaching its final destination. These make it necessary for each customer's cargo to be attached with a separate communication tag. These communication tags are then MTC Devices that will be co-located throughout the duration of the transport. This use case demonstrates the scenario of MTC Devices being co-located temporarily (but may be for a long time).

4.3.2 Use Case: Taxi Fleet Management

There is sufficient interest to employ a MTC Device in a taxi for fleet management. This offers many advantages: call-centres knowing exactly where the taxis are, efficient facilitation of the booking of taxis, and navigation aids can be provided to taxis. However, in many cities, there can be hundreds of taxis concentrated in one location: e.g. train stations, hotels, and tourist attractions. This may place undue stress on the network in order to support hundreds of MTC Devices in a single cell.

4.3.3 Use Case: Multiple applications on a single MTC Device

On MTC Devices various different applications can run concurrently. E.g. a MTC Device can be used to send alarms (e.g. for health reason) and can also contain a tracking application that every 15 minutes sends an update of the geographical location of the MTC Device. Or an MTC Device may need to poll data from the network every 5 minutes, while in the background a firmware update is being downloaded.

The different applications that concurrently run on the MTC Device may have very different characteristics. This makes it difficult to identify which of the existing network improvements may apply to the MTC Device.

4.4 Location Tracking MTC Feature

4.4.1 Use-Case: Checkpoint Reporting

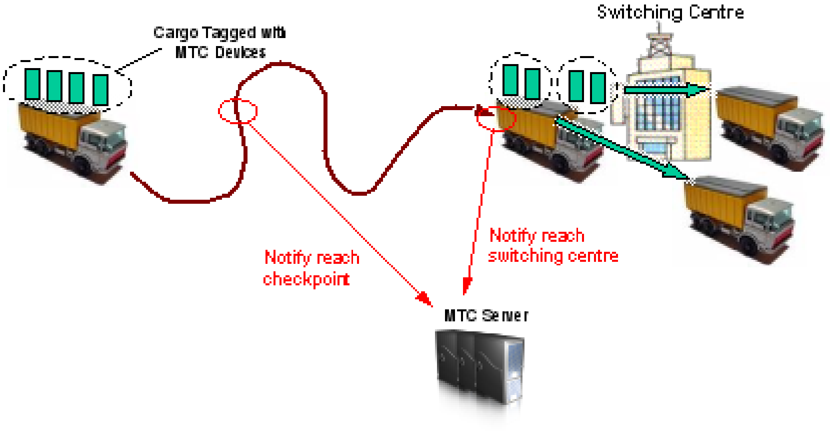

Figure 4.4-1: Cargo tracking via pre-determined checkpoints

Courier services may attach communication tags on customer's parcels/cargoes to track the current location of the items. While on a transport, it is generally not necessary to get accurate location information of each item. There will be pre-determined locations (i.e. checkpoints) where the tags should report their locations to the MTC Server. This checkpoint reporting will enable the courier service company to provide real-time tracking updates to their customer on the delivery status of the cargoes/parcels. Also, the MTC Server would like to know when the parcels/cargoes arrive in a switching centre, so that possible transfers of parcels/cargoes to achieve the most efficient/speedy delivery can be determined. When the network operator provides the service of tracking the MTC Devices, it removes the need for communication tags to contain GPS units, making it an attractive solution to MTC Customers.

4.5 Core Network Node Selection

4.5.1 Use Case: Dedicated M2M Core Network (Nodes)

With M2M services being deployed extensively in the future, the performance of existing operator networks may not be able to keep up with the requirements of M2M in many aspects, such as bandwidth, signalling processing capabilities, etc., without affecting the H2H communications. It seems quite possible that a dedicated core network or at least some core network nodes that are exclusively used by the M2M services will emerge.

For example, in many MTC applications, a large number of MTC Devices affiliated with a single MTC User may connect to a single MTC Server which is connected to the PS network of a mobile network operator via an Access Point Name (APN) using the MTCi interface. When a high number of MTC Devices are sending/receiving data simultaneously, data congestion may occur in the mobile core network or on the link connecting to the MTC Server. To avoid potential impacts brought by the M2M applications on the data traffic, as a first step of dedicated M2M core network, an M2M dedicated GGSN can be introduced, as illustrated in Figure 4.5-1.

Moreover, an M2M service operator could have its own or leased core network, sharing the costly wireless access infrastructure with other operators for better resource utilization. This deployment may require the radio network decide to which core network it will deliver the signalling and data traffic, as illustrated in Figure 4.5-2. Furthermore, if more solutions are introduced in SA2, it's possible not only to differentiate between M2M core network and H2H core network, but also between different M2M core networks. The advantage of dedicated core network is obvious in that the possible congestion due to large number of MTC devices accessing the network in parallel will not result in endangering H2H communication.

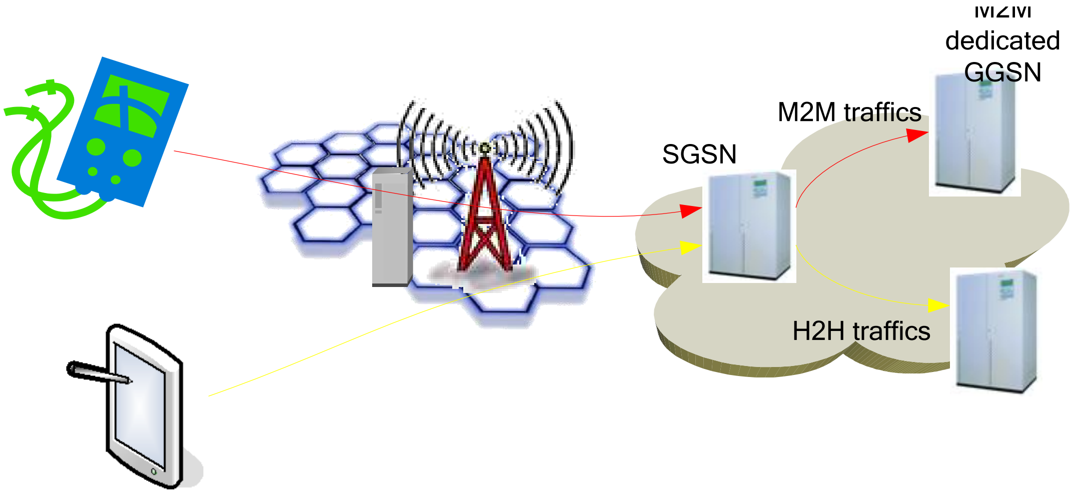

Figure 4.5-1 M2M dedicated core network node

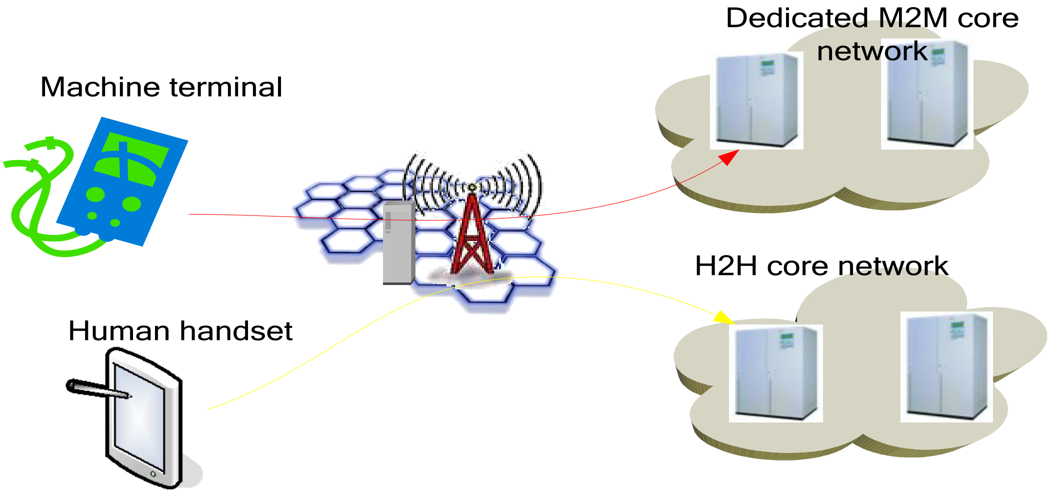

Figure 4.5-2 M2M dedicated core network

4.6 Reusing 3GPP of the IP Multimedia Subsystem Communication capabilities

4.6.1 Scenario and Use Case 1: Surveillance

In this Use Case, a House is equipped with surveillance sensors e.g. surveillance cameras, motion sensors, fire alarm, temperature etc. that are directly connected or connected via an MTC Gateway Device over fixed or mobile access towards a Security Control Center (SCC) via a 3GPP CN using IP Multimedia Subsystem.

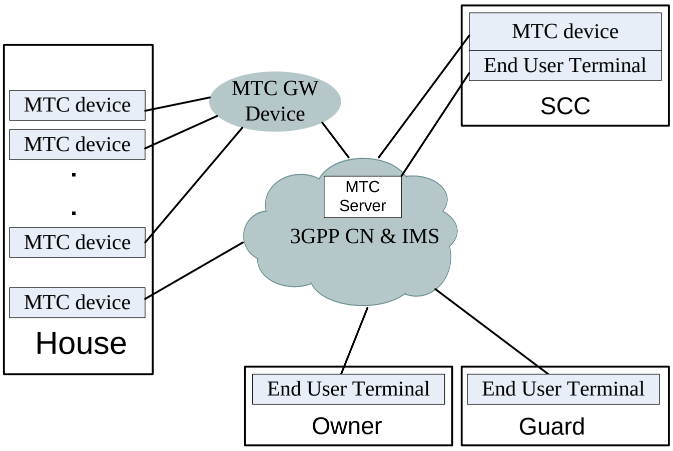

Figure 4.6.1-1: MTC devices communication via 3GPP CN IMS with 3GPP devices

When an alarm is triggered the SCC is notified by for instance using IMS messaging procedures that relies on secure routing, authentication, and priority. The SCC will verify that the alarm was not triggered by mistake by contacting the owner of the house using procedures that relies on secure routing and the possibility to add multimedia capabilities.

-The Security Control Center "calls" up the surveillance cameras to get a better view of the situation using procedures that rely on secure routing and authentication of SCC with the possibility to set up video media (and other multimedia) using QoS, Priority, and NAT traversal of media.

The SCC will further notify a "guard" of the situation using procedures for secure routing with the possibility to additional multimedia, priority, and QoS. The Security Control Center may also directly transfer the surveillance media to the guard, using additional procedures for Inter-UE transfer (transfer media session from SCC to Guard). The guard can then directly view the area, and access the local MTC devices.

4.6.2 Scenario and Use Case 2: eHealth

In this Use Case, a person is equipped with a health sensor that are directly connected over fixed or mobile access towards an eHealth Center (eHC) via a 3GPP CN using IP Multimedia Subsystem.

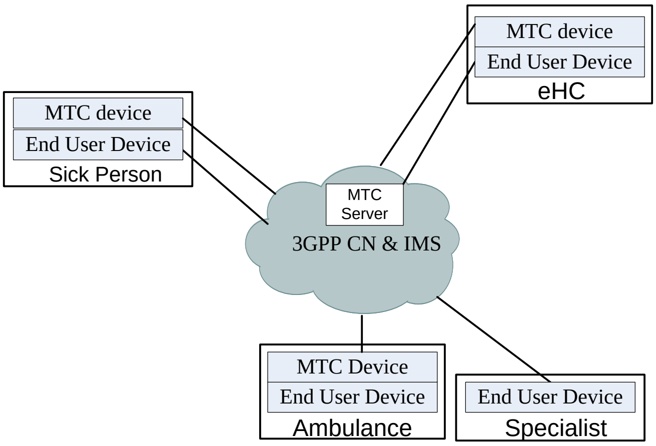

Figure 4.6.2-1: MTC devices communication via 3GPP CN IMS with 3GPP devices

When a health sensor alarm is triggered, the eHC is notified by for instance using IMS messaging procedures that relies on secure routing, authentication, QoS, and priority. The eHC will set up a voice connection towards the person that relies on procedures for secure routing and priority. The eHC will also set up a voice conference and include the person and a specialist (including all three parties). The eHC may directly transfer the sensor data to the specialist using additional procedures for Inter-UE transfer (transfer of media session from eHC to the specialist). The specialists can then directly view and manipulate the sensor.

The eHC will send an ambulance and connect the ambulance into the conference using procedures for secure routing and priority. The eHC may transfer the sensor data to the ambulance using the additional procedures Inter-UE Transfer (transfer of media session from the specialist to the Ambulance).

4.7 MTC Device-to-Server Communication

4.7.1 Access via IMS

This section addresses the access of MTC devices to application server logic hosted in the network, specifically for the case in which the service logic is accessible through an IMS control layer.

Although many MTC applications need only low data rates, some applications will require the use of multi-media. An example is a surveillance camera that will transmit simultaneous video, audio and other data (e.g. temperature). Other MTC applications may require the use of Presence information to determine when to send information to another device.

These, more complex applications will need to connect to an entity of an operator service layer via the IP multimedia core network subsystem (IMS). Such an entity may include interaction with existing service layer elements (both Application servers as well as Service Enablers). The requirement is for the MTC Device to interact with one or several Application Servers or Enablers in order to provide information for other services. Such services may be located either in the operator domain or in external domains. No additional Application Server or Enabler should be required to deploy this capability.

The high level requirements are the following:

- The network shall provide mechanisms to handle MTC Devices and applications on MTC Devices registering on the IP multimedia core network subsystem and accessing its capabilities including interaction with IMS application servers/enablers.

- The network shall allow a resource efficient registration of MTC Devices and applications on MTC Devices on the IP multimedia core network subsystem (e.g. no need of a permanently assigned ID per MTC Device).

Additional supporting requirements are the following:

- If an MTC device has an IMS identity preconfigured, the registration to the IMS control layer shall be fully standard.

- If an MTC device does not have an IMS identity preconfigured, the MTC device shall be able to request for one to the IMS control layer via secure mechanisms

NOTE: The HSS may use wildcarded identities for this purpose.

- If the MTC device does not have an IMS identity preconfigured and has requested for one to the IMS control layer via secure mechanisms, the registration to be performed with such identity shall be fully standard.

The following subsections provide additional details and potential particular solutions for such requirements.

4.7.2 Example of Scenario and Use Case 1: IMS Enabler, Client with IMS credentials

In this type of communication, the MTC Device has an IMS identity, provisioned at the HSS, and therefore the standard registration procedure in the IMS domain is used. The service profile of the MTC Device identity will be configured to guarantee that the signalling generated at the MTC Device will reach the specific Application Server or IMS Enabler.

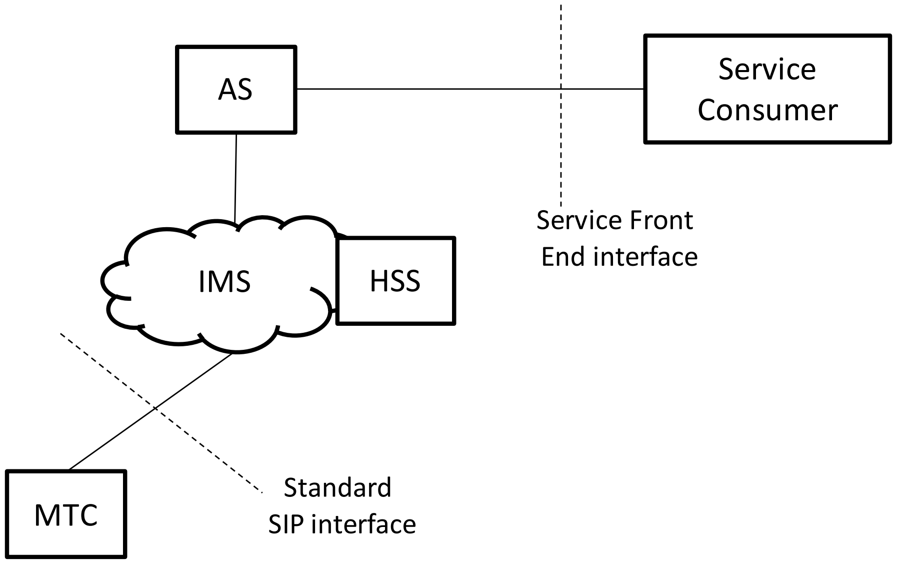

Figure 4.7.2-1: MTC Devices communicating with IMS application Server or Enabler. MTC device has IMS identity.

4.7.3 Example of Scenario and Use Case 2: IMS Enabler, Client with no IMS credentials

In this type of communication the MTC Device has no IMS credentials, no Public and no Private User Identity that can be used for registration purposes. In addition, the HSS will have no identity provisioned associated to the MTC Device.

The MTC Device may require access to multimedia services only rarely in situations with low probability. Each low-probability access to IMS will require the completion of a registration onto the IMS domain to access the capabilities located in the IMS Service Layer.

In order to meet the requirement of a large number of MTC devices that need to access the IMS in an efficient way, an Authentication Gateway is defined.

The Authentication Gateway has standard connectivity with the MTC Device, over a protocol other than SIP. The Authentication Gateway also has an interface with the HSS.

- The interface between the MTC Device and the Authentication Gateway needs to support authentication and authorization mechanisms to guarantee the secure validation of the MTC identity. This may require of additional elements to store the identities of the existing MTC Devices. Such MTC identities are not IMS identities.
- The interface between the Authentication Gateway and the HSS needs to support credential retrieval procedures in order to reserve those at the HSS and deliver those to the MTC server via the Authentication Gateway via the interface established with the MTC Device.
- Such IMS identities retrieved from the HSS by the Authentication Gateway may have subscriber profiles associated.
- Once the MTC Device gets standard IMS identities, the MTC can start a standard IMS registration procedure in order to establish a connection with the specific Application Server or Enabler.

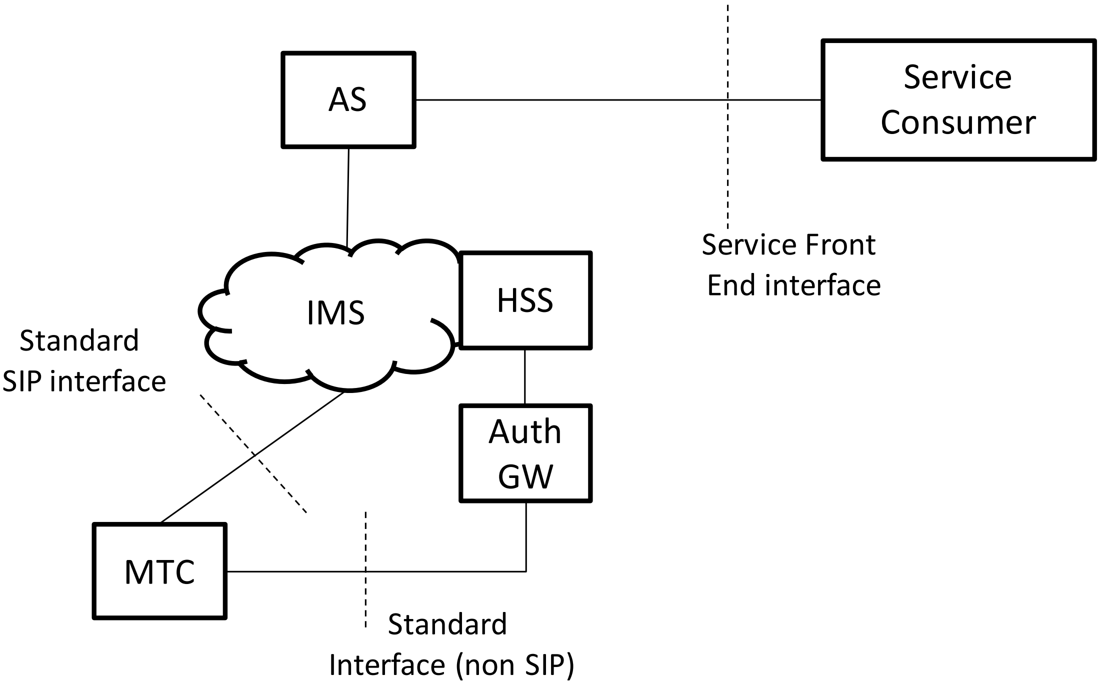

Figure 4.7.3-1: MTC Devices communicating with IMS application Server or Enabler. MTC device has no IMS identity and gets credentials via an Authentication Gateway

5 Possible requirements

The system shall be able to provide MTC Device connection status information to the authorized MTC server.

6 Conclusion and recommendations

This document analyses several use cases.

No consensus has been achieved to specify requirements generated from the use cases.

Annex <A>:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2010-08					*Draft skeleton for review*		*0.0.0*
2010-08					*Inclusion of agreements done in SA1#51: S1-102279, S1-102274, S1-102275, S1-102276, S1-102277, S1-102278*		*0.1.0*
2010-11					*Inclusion of agreements done in SA1#52:, S1-103212, S1-103213, S1-103216, S1-103221*		*0.2.0*
2010-11					*Inclusion of agreements done in SA1#52:, S1-103230, S1-103316*		*0.3.0*
2011-02					*Inclusion of agreements done in SA1#53: S1-110377*		*0.4.0*
2011-02					*Inclusion of agreements done in SA1#54: S1-111037, S1-111314*		*0.5.0*
2012-02					*Inclusion of agreements done in SA1#57: S1-120333*		*0.6.0*
2012-05					*Inclusion of agreements done in SA1#58: S1-121421*		*0.7.0*
2013-01					*Inclusion of conclusion section done in SA1#61: S1-131209 and editorial modifications (changed cover page to indicate Release 12, changed smart quotes to straight quotes, corrected punctuation, deleted Editor's notes)*		*0.8.0*
2013-01					*Editorial changes in SA1#61: removal of empty section 5 and 6*		*0.8.1*
2013-02					*Editorial changes by MCC for presentation for one-step-approval to SA#59*	*0.8.1*	*1.0.0*