ETSI TS 122 368 V13.1.0 (2016-03)

Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
Service requirements
for Machine-Type Communications (MTC);
Stage 1
(3GPP TS 22.368 version 13.1.0 Release 13)

Reference
RTS/TSGS-0122368vd10

Keywords
LTE

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification 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

The present document specifies the service requirements for Network Improvements for Machine Type Communications. In particular it will:

- identify and specify general requirements for machine type communications;
- identify service aspects where network improvements (compared to the current human-to-human oriented services) are needed to cater for the specific nature of machine-type communications;
- specify machine type communication requirements for these service aspects where network improvements are needed for machine type communication.

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 22.011: " Service accessibility".

[3] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

[4] ETSI TS 102 690: "Machine-to-Machine communications (M2M); functional architecture".

[5] ETSI TS 102 921: " Machine-to-Machine communications (M2M); mla, dla, and mld interfaces".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] 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].

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 1: A MTC Device might also communicate locally (wirelessly, possibly through a Personal Area Network, or hardwired) with other entities which provide the MTC Device "raw data" for processing and communication to the MTC Server(s) and/or other MTC Device(s). Local communication between MTC Device(s) and other entities is out of scope of the present document.

MTC Feature: MTC Features are network functions to optimize the network for use by M2M applications.

MTC Group: A MTC Group is a group of MTC Devices that share one or more MTC Features and that belong to the same MTC Subscriber.

MTC Server: A MTC Server is a server, which communicates to the PLMN itself, and to MTC Devices through the PLMN. The MTC Server can also have an interface which can be accessed by the MTC User. The MTC Server can:

- Provide services for other servers (e.g. The MTC Server is a Services Capability Server 3GPP TS 23.682 [3] for an Application Server [3]), and/or
- Provide services for applications and can host the application (e.g. The MTC Server is an Application Server [3]).

MTC User: A MTC User uses the service provided by the MTC Server.

MTC Subscriber: A MTC Subscriber is a legal entity having a contractual relationship with the network operator to provide service to one or more MTC Devices.

Note 2: Typically a M2M service provider is the party holding subscriptions in order to provide connectivity between MTC Devices and the MTC Server. In practise certain roles can collapse, e.g. the network operator acts as the same time as service provider.

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].

NIMTC	Network Improvements for Machine Type Communications
MNO	Mobile Network Operator
MTC	Machine-Type Communications

4 Overview of system optimizations for machine-type communications

Machine-type communication is a form of data communication which involves one or more entities that do not necessarily need human interaction.

A service optimized for machine type communications differs from a service optimized for Human to Human communications. Machine-type communications is different to current mobile network communication services as it involves:

a) different market scenarios,

b) data communications,

c) lower costs and effort,

d) a potentially very large number of communicating terminals with,

e) to a large extent, little traffic per terminal.

For the purpose of the present document, the term MTC is used for the purpose to describe use-cases and illustrate the diverse characteristics of machine-type communication services.

The informative annex A gives an overview of MTC use-cases which also illustrate different overload scenarios which will require overload control functions to prevent overload and to differentiate between services offered to different subscribers with different service requirements. In particular, certain MTC services and MTC applications, as exemplified in annex B, are more tolerant and can accept a lower level of performance requirements for its communication services. However, some MTC services will have similar service requirements as current mobile network communication services.

5 MTC communication aspects

5.1 MTC communication scenarios

5.1.1 Introduction

For MTC communication the following communication scenarios can be identified:

a) MTC Devices communicating with one or more MTC Server;

b) MTC Devices communicating with each other.

5.1.2 MTC devices communicating with one or more MTC servers

The network operator provides network connectivity to MTC Server(s). This applies to MTC Server(s) controlled by the network operator (refer to figure 5-1) or to MTC Server(s) not controlled by the network operator (refer to figure 5-2.)

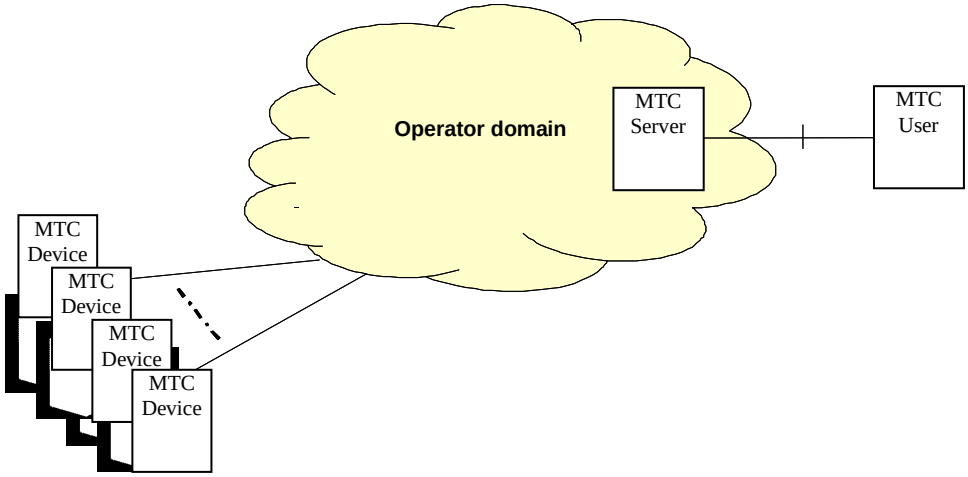

Figure 5-1: Communication scenario with MTC devices communicating with MTC server. MTC server is located in the operator domain.

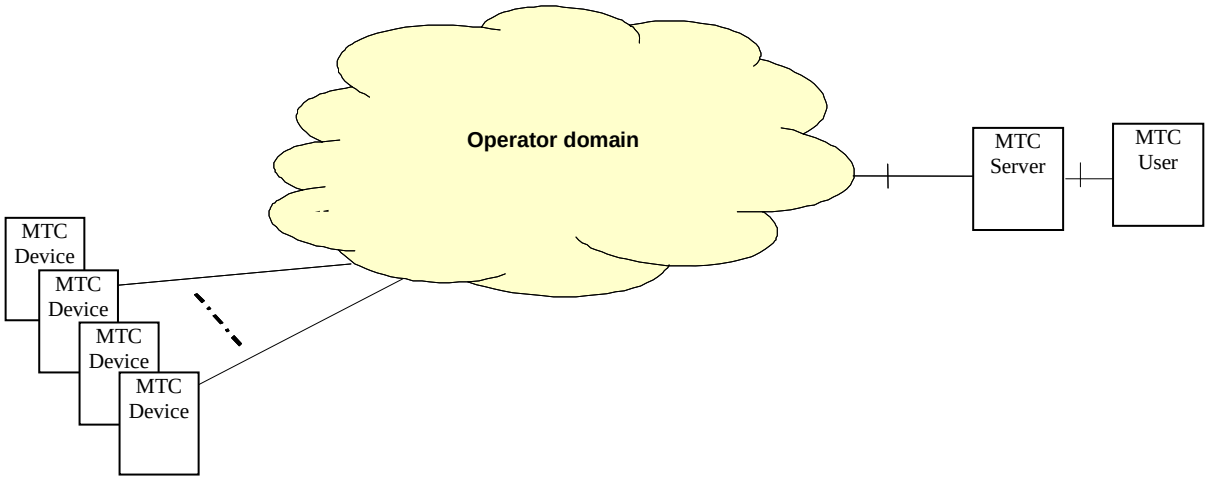

Figure 5-2: Communication scenario with MTC devices communicating with MTC server. MTC server is located outside the operator domain.

The MTC Device and the MTC Server it is communicating with may implement a service enablement framework (e.g. as specified in [4] and [5]) to provide generic functionality for applications. The MTC Device may implement multiple instances of service enablement frameworks, each communicating with a different MTC Server.

Note 1: the standardization of service enablement frameworks is out of scope of 3GPP.

Note 2: as an example, a device can have two (or more) service enablement frameworks, both compliant to the same specific standard or belonging to the same proprietary implementation. Each one has to be peered to a different MTC server.

5.1.3 MTC devices communicating with each other

The communication scenario where the MTC Devices communicate directly without intermediate MTC Server (refer to figure 5-3) is not considered in this release of the specification.

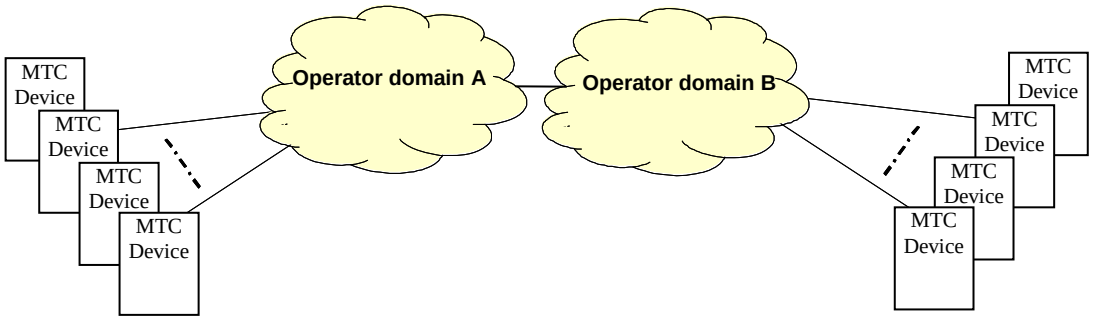

Figure 5-3: MTC Devices communicating directly with each other without intermediate MTC server

5.2 (void)

6 Categories of features for Machine-Type Communications

Machine-Type Communication (MTC) applications do not all have the same characteristics. This implies that not every system optimization is suitable for every MTC application. Therefore, MTC Features are defined to provide structure for the different system optimization possibilities that can be invoked. MTC Features provided to a particular subscriber are identified in the subscription. MTC Features can be individually activated.

The following MTC Features have been defined:

- Low Mobility;
- Time Controlled;
- Small Data Transmissions;
- Infrequent Mobile Terminated;
- MTC Monitoring;
- Secure Connection;
- Group Based MTC Features:
  - Group Based Policing;
  - Group Based Addressing.

7 Service requirements

7.1 Common service requirements

7.1.1 General

The following are MTC common service requirements:

- The network shall enable the network operator to identify per subscription which individual MTC Features are subscribed to by a particular MTC Subscriber.
- The network shall provide a mechanism for the MTC Subscriber to activate or deactivate MTC Features.
- The network shall enable the network operator to identify which individual MTC Features are activated for a particular MTC Subscriber.

Note 1: The activation/deactivation functionality can be provided via a web interface that is outside the scope of 3GPP specifications.

- The network shall provide a mechanism for the network operator to control the addition or removal of individual MTC Features to a subscription (e.g. based on matching or mismatching of MTC Features).
- The network shall provide a mechanism for the network operator to restrict activation of MTC Features (e.g. based on matching or mismatching of MTC Features).
- The network may provide a mechanism for the network operator to allow MTC Devices to override restrictions imposed by a particular MTC Feature.
- The network operator shall be able to restrict the use of a USIM to specific MEs/MTC Devices.
- The network shall provide a mechanism to reduce peaks in the data and signalling traffic resulting from very large numbers of MTC Devices (almost) simultaneously attempting data and/or signalling interactions.
- The network shall provide a mechanism to restrict downlink data and signalling when the network is overloaded.
- The network shall provide a mechanism to restrict access towards a specific APN when the network is overloaded.
- A MTC Device may support the Extended Access Barring (EAB) mechanism defined in TS 22.011 [2].
- A MTC Device supporting the EAB mechanism shall be able to be configured for EAB by the HPLMN.
- The HPLMN shall be able to configure EAB on a MTC Device that supports it.
- Once configured, and upon reception of broadcasted EAB information, the MTC Device shall adhere to the defined EAB mechanisms.

Note 2: The decision of whether a MTC Device is configured for EAB is out of 3GPP scope. In general, MTC Devices considered more tolerant to access restrictions are well suited to be configured for EAB.

- The system shall provide mechanisms to efficiently maintain connectivity for a large number of MTC Devices.
- 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.
- Configuration parameters which are provided in the USIM shall take precedence over parameters provided in the MTC Device if both exist.
- 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)

- The system shall provide mechanisms to lower power consumption of MTC Devices.
- The system shall provide a resource efficient way to support MTC Devices that send or receive data infrequently, i.e. with long periods between data transmissions.
- MTC Devices may or may not be kept attached to the network when not communicating, depending on operator policies and MTC Application requirements.
- MTC Devices may keep their data connection or not keep their data connection when not communicating, depending on operator policies and MTC Application requirements.

7.1.2 MTC Device triggering

The requirements related to MTC Device triggering include the following:

- The network shall be able to trigger MTC Devices to initiate communication with the MTC Server based on a trigger indication from the MTC Server.
- The system shall provide a mechanism such that only trigger indications received from authorized MTC Servers will lead to triggering of MTC Devices.
- Upon receiving a trigger indication from a source that is not an authorized MTC Server, the network shall be able to provide the details of the source (e.g. address) to the MTC User.
- The system shall provide a mechanism to the MTC User to provide a set of authorized MTC Server(s).
- Upon receiving a trigger indication, if the network is not able to trigger the MTC Device, the 3GPP system may send an indication to the MTC Server that triggering the MTC Device has been suppressed.

Note: Suppression of triggering could be due to system conditions such as network congestion.

- A MTC Device shall be able to receive trigger indications from the network and shall establish communication with the MTC Server when receiving the trigger indication. Possible options may include:
  - Receiving trigger indication when the MTC Device is not attached to the network.
  - Receiving trigger indication when the MTC Device is attached to the network, but has no data connection established.
  - Receiving trigger indication when the MTC Device is attached to the network and has a data connection established.

7.1.3 Addressing

The system shall provide mechanisms, according to operator policy, where an MTC Server can send a mobile terminated message to the MTC Device. Scenarios include:

- The MTC Server is located in the public IPv6 address space. The MTC Device is assigned a public IPv6 address by the MNO.

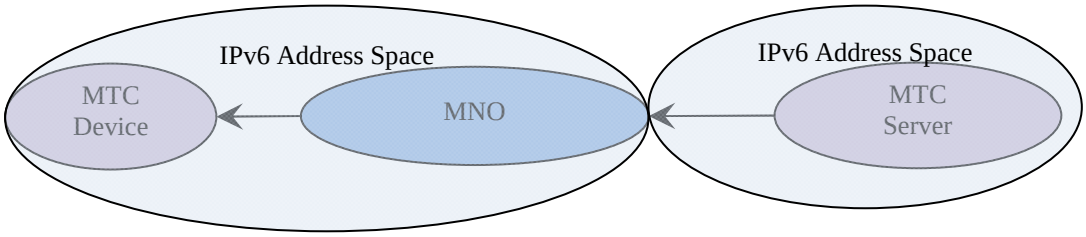

Figure 7-1: MTC server and the MTC Device in the public IPv6 address space

- The MTC Server is located in a public IPv4 address space; the MTC Device is assigned a private IPv4 address by the MNO.

  Alternatively, the MTC Server is located in a private IPv4 address space and is assigned a private IPv4 address by the MNO; the MTC Device is assigned a private IPv4 address by the MNO corresponding to the same IPv4 address space as the MTC Server.

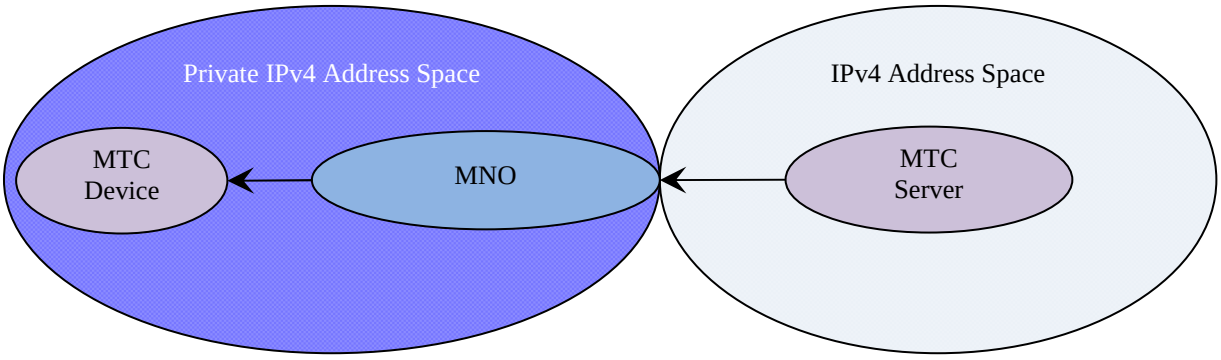

Figure 7-2: MTC Server in a public or private IPv4 address space, MTC Device in a private IPv4 address space

7.1.4 Identifiers

The requirements for MTC related to identifiers include the following:

- The system shall be able to uniquely identify the ME;
- The system shall be able to uniquely identify the MTC Subscriber.

Note 1: The two requirements above also apply to human-to-human communications. However, for Machine-Type Communications identifiers will have to be able to cater for a number of identifiers at least two orders of magnitude higher than for human-to-human communications.

- In order to use MTC triggering, the system shall support association between an MTC Device identity and one or more Service Enablement Framework individually.

Note 2: The Service Enablement Framework server in the network needs to associate its peer Service Enablement Framework client on the MTC Device with the external identifier of the MTC Device. Preconfiguration of the association is sufficient when the Service Enablement Framework knows the MTC Device identities in advance to the starting of the service, but this does not match all the relevant scenarios of service deployment.

- The system shall provide mechanisms for the network operator to efficiently manage numbers and identifiers related to MTC Subscribers.

7.1.5 Charging requirements

The core network shall be able to:

- count MTC Feature activation / de-activation.

- collect charging data with a granularity (e.g. in time or location) that can identify the use of network resources when used outside the limits of subscription or MTC Feature, e.g. time window, location, or can identify when the MTC Device is overriding other restrictions (e.g. low priority).

- count particular Monitoring events.

Note: The above charging requirements apply to off line charging only.

7.1.6 Security requirements

The security requirements for MTC include the following:

- MTC optimizations shall not degrade security compared to non-MTC communications

7.1.7 Remote MTC device management

The operator shall be able to manage MTC Devices using existing mechanisms (e.g. OMA DM)

7.2. Specific service requirements – MTC Features

7.2.1 Low Mobility

The MTC Feature Low Mobility is intended for use with MTC Devices that do not move, move infrequently, or move only within a certain region.

For the Low Mobility MTC Feature:

- The network operator shall be able to change the frequency of mobility management procedures or simplify mobility management per MTC Device.

- The network operator shall be able to define the frequency of location updates performed by the MTC Device.

7.2.2 Time Controlled

The MTC Feature Time Controlled is intended for use with MTC Applications that can tolerate to send or receive data only during defined time intervals and avoid unnecessary signalling outside these defined time intervals. The network operator may allow such MTC Applications to send/receive data and signalling outside of these defined time intervals but charge differently for such traffic.

For the Time Controlled MTC Feature:

- The network operator shall be able to reject access requests per MTC Device (e.g. attach to the network or set up a data connection) outside a defined access grant time interval.

Note 1: The Time Controlled MTC Feature does not affect the MTC Server to send trigger indications to the MTC Device.

- The network operator shall be able to allow access (e.g. attach to the network or set up a data connection) outside a defined access grant time interval and charge this differently.

- The network shall reject access requests per MTC Device (e.g. attach to the network or set up a data connection) during a defined forbidden time interval (e.g. to allow maintenance of a MTC Server).

- The local network shall be able to alter the access grant time interval based on local criteria (e.g. daily traffic load, time zones). The forbidden time interval shall not be altered.

Note 2: It is assumed that an access grant time interval will not overlap a forbidden time interval.

Note 3: "Local network" can refer to a VPLMN in roaming case, or to the local part of a large RPLMN (e.g. that spans across multiple time zones).

- The network shall be able to restrict the duration of access by terminating access (e.g. detach or disconnect a data connection) after a defined access duration.

Note 4: The defined access duration (e.g. 10 minutes) is pre-agreed between the network operator and the MTC Subscriber, and is typically long enough to ensure the completion of normal communication between MTC Device and MTC Server.

- The MTC Device may disconnect immediately when it finishes its communications with the MTC Server before wait until the end of the access duration.

- The network shall communicate the (altered) access grant time interval and the access duration to the MTC Device.

- The network may communicate the (altered) access grant time interval and the access duration to the MTC Server/MTC User.

Note 5: It is desirable that access of MTC Devices with the same access grant time interval is distributed across this interval in a manner to reduce peaks in the signalling and data traffic.

7.2.3 Void

7.2.4 Void

7.2.5 Small Data Transmissions

The MTC Feature Small Data Transmissions is intended for use with MTC Devices that send or receive small amounts of data.

For the Small Data Transmissions MTC Feature:

- The system shall support transmissions of small amounts of data with minimal network impact (e.g. signalling overhead, network resources, delay for reallocation).

- Before transmission of small amount of data, the MTC Device may be attached or detached to/from the network.

Note 1: "Transmission" implies either sending or receiving small amount of data.

- The 3GPP system shall be able to count the number of small data transmissions per subscription e.g. for charging or statistical purposes.

Note 2: observed size of many of the instances of data exchanges is on the order of 1K (1024) octets

Note 3: Charging and accounting of small data transmissions between operators can be done on a bulk basis.

7.2.6 Void

7.2.7 Infrequent Mobile Terminated

The MTC Feature Infrequent Mobile Terminated is intended for use with MTC Devices that mainly utilize mobile originated communications.

For the Infrequent Mobile Terminated MTC Feature:

- The network operator shall be able to reduce the frequency of mobility management procedures per MTC Device.
- The network shall be able to maintain information on when the MTC Device is not reachable for mobile terminated communications. The network shall not trigger the MTC Device when it is known to be unreachable, and instead may inform the MTC Server that the MTC Device is not reachable.

Note: With the Infrequent Mobile Terminated MTC Feature, the network operator should be able to minimize mobility management due to MTC Device movement .

7.2.8 MTC Monitoring

The MTC Feature MTC Monitoring is intended for monitoring MTC Device related events.

For the MTC Monitoring MTC Feature:

- The system shall provide mechanisms to detect the following events:
  - behaviour which is not aligned with activated MTC Feature(s)
  - change of the association between the ME and the USIM
  - loss of connectivity. The maximum time between the actual loss of connectivity occurred and the loss of connectivity detected shall be configurable per subscription.
  - communication failure events of the UE visible to the network (e.g. for troubleshooting)
  - change of the location (geographical position and/or point of attachment in the network) of the MTC Device.

Note 1: Loss of connectivity means it is no longer possible to establish signalling between the MTC Device and the network.

Note 2: The maximum detection time is on the order of 1 minute to 1 hour.

- The MTC Subscriber shall be able to define which of the above events will be detected.
- Upon the above event detection, the network shall be able to:
  - provide a warning notification to the MTC Server;
  - limit the services provided to the MTC Device (e.g. reduce allocated resource).
- The MTC User shall be able to define what occurs when an event is detected.
- The MTC Device shall be able to transfer other event notification to the MTC Server where the event detection is out of 3GPP scope, for example, the loss of signal reception, notification when the MTC Device power level is lower than a threshold.

Note 3: Loss of signal reception refers to a situation when a MTC Device can no longer receive the network which could be due to interference (e.g. from a jammer or other source) or other reasons.

7.2.9 Void

7.2.10 Secure Connection

The MTC Feature Secure Connection is intended for use with MTC Devices that require a secure connection between the MTC Device and MTC Server/MTC Application Server.

For the Secure Connection MTC Feature:

- The network operator shall be able to efficiently provide network security for connection between MTC Device and a MTC Server or between MTC Device and a MTC Application Server in case there is a direct connection with the MTC Application Server. This applies even when some of the devices are roaming i.e. connected via a VPLMN.

7.2.11 Void

7.2.12 Void

7.2.13 Void

7.2.14 Group Based MTC Features

7.2.14.1 General

A Group Based MTC Feature is a MTC Feature that applies to an MTC Group.

- The system shall be optimized to handle MTC Groups. The system shall provide a mechanism to associate an MTC Device to a single MTC Group.
- Each Group Based MTC Feature is applicable to all the members of the MTC Group.
- An MTC Group shall be identified uniquely across 3GPP networks.

Note 1: With Group Based MTC Features, each MTC Device is visible from the 3GPP Network perspective.

Note 2: MTC Features that are not Group Based MTC Features can also be applied to MTC Group members.

Note 3: An MTC Device can belong to more than one MTC group, but policy conflicts need to be avoided through administrative means.

7.2.14.2 Group Based Policing

The MTC Feature Group Based Policing is intended for use with a MTC Group for which the network operator wants to enforce a combined QoS policy.

For the Group Based Policing MTC Feature:

- A maximum bit rate for the data that is sent/received by a MTC Group shall be enforced.

Note: Policy control could be static to reduce complexity. In this case, static means that the policy for a specific MTC Group is fixed for the group and does not change due to dynamic conditions.

7.2.14.3 Group Based Addressing

MTC Feature Group Based Addressing is intended for use with a MTC Group for which the network operator wants to optimize the message volume when many MTC Devices need to receive the same message.

For the Group Based Addressing MTC Feature:

- The network shall provide a mechanism to send a broadcast message within a particular geographic area, e.g. to wake up the MTC Devices that are members of that MTC Group; only MTC Devices of the target group configured to receive the broadcast message will recognize it.

Note 1: The geographic area for the broadcast may be a cell sector, a cell or a group of cells.

Note 2: Verification of receipt of a broadcast message is not necessary.

Annex A (informative): Use cases

Addressing from a centralized entity Use Case

Metering devices are typically monitored and controlled by a centralized entity outside or inside the network operator system. Due to the need for centralized control, the centralized entity will inform or poll the metering device when it needs measurement information rather than the metering device autonomously sending measurements. Depending on the nature of the metering application, low latency responses are sometimes required (metering for high pressure pipelines for example). To accomplish this, the centralized entity will need to inform the metering device when it needs a measurement. Typically due to the limitation of IPv4 address space, the metering terminal is behind a NAT (Network Address Translator) where it is not assigned a routable IPv4 address.

Theft /Vandalism Vulnerable MTC Application Use Case

In contrast to the traditional H2H devices, which are carefully held and protected by a person, MTC Devices are often located in remote areas and ideally are untouched after installation for many years. The remote locations make these devices more susceptible to tampering by unauthorized persons. The tampering of the MTC Device is often accompanied by damage to the metering device. The network has security mechanisms for protection for this type of activity which may not be effective for MTC Devices. The network can not prevent it but can detect it as early as possible in order to deactivate the ME's service and the related USIM. In addition, often theft/vandalism vulnerable MTC Devices are stationary after initial installation and activation. The stationality of the MTC Device can be utilized to improve the detection of theft. If a known stationary devices moves, it can be concluded that the MTC Device has been stolen and thus the account deactivated.

Time Controlled MTC Application Use Case

For some MTC applications the actual time at which communication takes place is less important, but low communication costs are extremely important. A network operator can offer low communication fees for this type of applications by allowing communication to take place during low traffic time periods only. Possibly the network operator may want to dynamically adjust these time periods based on the actual network traffic load at a specific time.

Radio Network Congestion Use Case

Radio network congestion because of mass concurrent data transmission takes place in some MTC applications. One of the typical applications is the bridge monitoring with a mass of sensors. When a train passes through the bridge, all the sensors transmit the monitoring data almost simultaneously. The same thing happens in hydrology monitoring during the time of heavy rain and in building monitoring when intruders break in. The network should be optimized to enable a mass of MTC Devices in a particular area to transmit data almost simultaneously.

Core Network Congestion Use Case

With many MTC applications, a large number of MTC Devices is affiliated with a single MTC User. These MTC Devices together are part of a MTC Group. The MTC User associated with the MTC Group owns a MTC Server which is connected to the PS network of a mobile network operator via an Access Point Name (APN) using the Gi interface. The MTC Devices in the MTC Group communicate with this MTC Server.

Typically, the MTC Devices in the MTC Group are scattered over the network in such a way that the data simultaneously sent by the MTC Devices in any particular cell is limited and will not cause a radio network overload. Despite this, 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 between mobile core network and MTC Server where the data traffic related to MTC Group is aggregated. Preferably, a network operator and the MTC User have means to enforce a maximum rate for the data sent/received by the MTC Group.

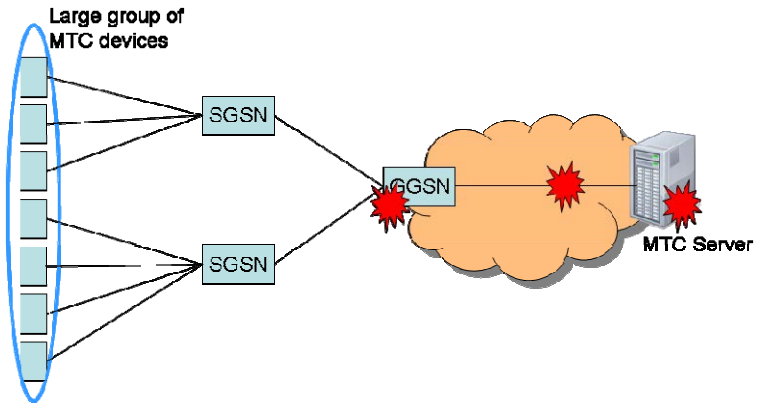

Figure A-1: Congestion in mobile core network and on the link between mobile core network and MTC Server

Signalling Network Congestion Use Case

Congestion in the signalling network is caused by a high number of MTC Devices trying almost simultaneously: (1) to attach to the network or (2) to activate/modify/deactivate a connection. In a 3GPP system supporting MTC applications such an overload of the network can be caused by e.g. many mobile payment terminals that become active on a national holiday or by high numbers of metering devices becoming active almost simultaneously after a period of power outage. Also some MTC applications generate recurring data transmissions at precisely synchronous time intervals (e.g. precisely every hour or half hour). Preferably, the 3GPP system provides means to the network operator and MTC User to spread the resulting peaks in the signalling traffic.

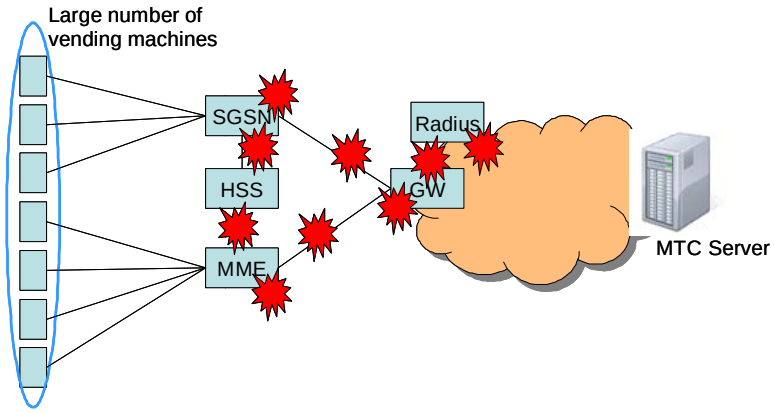

Figure A-2: Signalling network congestion

Access Control with billing plan Use Case

In some configurations, it may be necessary to restrict the access of a UICC that is dedicated to be used only with machine-type modules associated with a specific billing plan. It should be possible to associate a list of UICC to a list of terminal identity such as IMEISV so that if the UICC is used in an other terminal type, the access will be refused.
See the following configuration:

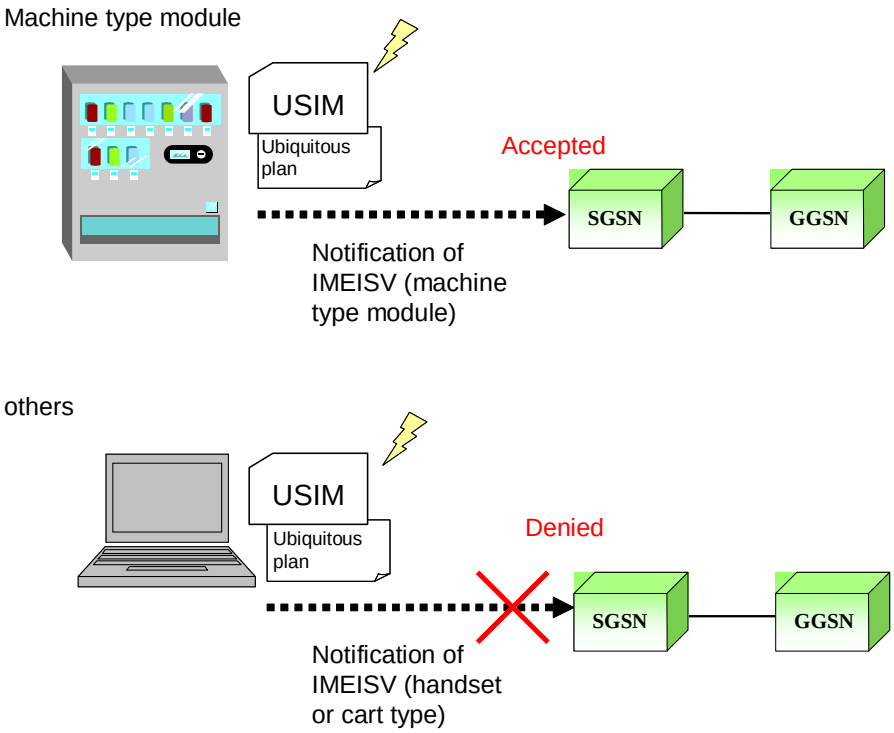

Figure A-3: Access Control with billing plan

Extra Low Power Consumption Use Case

For high mobility case, tracking MTC devices such as animal tracking MTC devices in natural world with high mobility require extra low power consumption because it is almost impossible to replace the battery or recharge the battery for animal tracking MTC device. Compared to the tracking devices installed in the cars and trucks because cars and trucks could generate electricity by themselves, extra low power consumption for these MTC devices is required.

For cargo tracking, the cargo with a tracking MTC device could move very fast such as on a train or lorry and could stand still such as in the dock before loading or unloading. It is not desired to either change its battery or replace battery during the transport period, so extra low power consumption MTC devices are also required.

For prisoner tracking MTC devices are already used by police, prisoners will not cooperate with police and would wish the MTC devices have flat batteries; therefore, extra low power consumption feature is required for these MTC devices. For the tracking MTC devices of elder people who have memory problem, children or pets, even the batteries of these MTC devices could be replaced or charged, however, considering the worst scenario – if they are missing, it requires the MTC devices with extra low power consumption and long working time in order to find them.

For low mobility case, the gas meter MTC devices must be battery powered. Extra low power consumption for gas MTC devices is much more critical than electricity meters.

Extra Low Power Consumption with Time Controlled MTC Devices Use Case

Time Controlled MTC Devices which send or receive data only at certain pre-defined periods may be operated in one or more modes that minimize power consumption.

An MTC Device may be operated in a mode where it is expected to receive non-periodic messages (e.g. emergency messages or notifications of altered access period as with the MTC Feature Time Controlled outside the time controlled periods. The MTC Device should minimize power consumption while in a mode to support this.

If the application requires the MTC Device to send or receive data within pre-defined periods and receive non-periodic messages outside these periods, operation at the lowest possible power consumption level to extend battery life should be achieved.

End-to-end security for roaming MTC devices

An MTC Application communicates with a large number of MTC Devices that are located globally and may or may not be mobile. Examples of such devices are mobile navigation systems and payment terminals. Connectivity for the MTC Devices is provided by a single network operator that uses its roaming agreements to connect MTC Devices that are not within range of its own network.

From the perspective of the operator of the MTC application its MTC Server and the domain of its network operator are part of a trusted domain. However, the domain of the roaming operator are not seen as part of the trusted domain, as is depicted in the figure below.

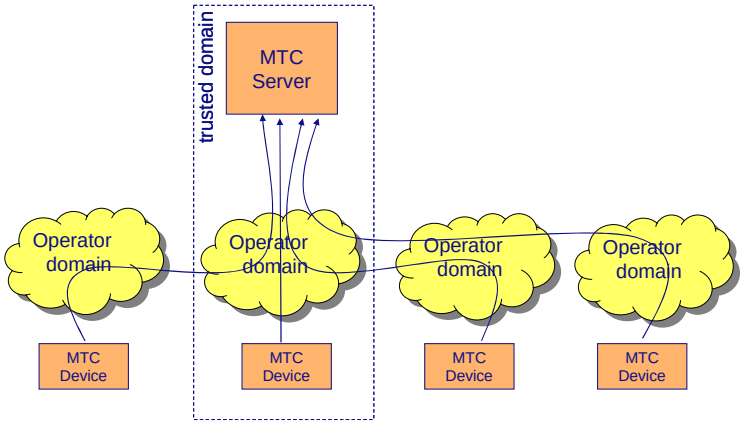

Figure A-4: End-to-end security for roaming MTC devices

The operator of the MTC application therefore requires end-to-end security for messages exchanged between MTC application and MTC Devices. The network operator does not have control over the security features in the domain of the roaming operators. Furthermore, for efficiency reasons the roaming operators may decide on a local breakout to for instance the Internet for MTC traffic in which case the information partly travels over the Internet. The network operator needs to satisfy the MTC application owner's end-to-end security requirement without relying on network security alone.

Annex B (informative): Examples of MTC applications

Some examples of machine-type communication applications are listed in the following table. This list is not exhaustive and is intended to be indicative of the scope of machine-type communication applications.

Service Area	MTC applications
Security	Surveillance systems Backup for landline Control of physical access (e.g. to buildings) Car/driver security
Tracking & Tracing	Fleet Management Order Management Pay as you drive Asset Tracking Navigation Traffic information Road tolling Road traffic optimization/steering
Payment	Point of sales Vending machines Gaming machines
Health	Monitoring vital signs Supporting the aged or handicapped Web Access Telemedicine points Remote diagnostics
Remote Maintenance/Control	Sensors Lighting Pumps Valves Elevator control Vending machine control Vehicle diagnostics
Metering	Power Gas Water Heating Grid control Industrial metering
Consumer Devices	Digital photo frame Digital camera eBook

Annex C (informative): Change history

TSG SA#	SA Doc.	SA1 Doc	Spec	CR	Rev	Rel	Cat	Subject/Comment	Old	New	WI
SP-47	SP-100192	-	22.220	-	-	-	-	Raised from v1.2.2 to v.2.0.0 for approval	1.2.2	2.0.0	NIMTC
SP-47	-	-	22.220	-	-	-	-	Raised from v.2.0.0 to v.10.0.0 after approval of SA#47	2.0.0	10.0.0	NIMTC
SP-48	SP-100400	S1-101157	22.368	0001	2	Rel-10	F	Deletion of section 5.2	10.0.0	10.1.0	NIMTC
SP-48	SP-100400	S1-101158	22.368	0003	2	Rel-10	F	Clarification of PAM	10.0.0	10.1.0	NIMTC
SP-48	SP-100400	S1-101138	22.368	0005	1	Rel-10	F	CR to TS22.368 Clarification of Location Specific Trigger	10.0.0	10.1.0	NIMTC
SP-48	SP-100400	S1-101139	22.368	0006	1	Rel-10	F	CR to TS22.368 Clarification of Infrequent Transmission	10.0.0	10.1.0	NIMTC
SP-48	SP-100400	S1-101159	22.368	0009	3	Rel-10	F	Clarification of Requirements for Time Controlled MTC Feature	10.0.0	10.1.0	NIMTC
SP-48	SP-100435	S1-101143r	22.368	0010	2	Rel-10	F	Clarification and completion of PAM requirements	10.0.0	10.1.0	NIMTC
SP-48	SP-100400	S1-101142	22.368	0011	1	Rel-10	F	Clarification of local network in Time Controlled	10.0.0	10.1.0	NIMTC
SP-48	SP-100400	S1-101077	22.368	0013	-	Rel-10	F	Correction of missing changes to clause 7.2.2	10.0.0	10.1.0	NIMTC
SP-48	SP-100400	S1-101078	22.368	0014	-	Rel-10	F	Correction of terminology	10.0.0	10.1.0	NIMTC
SP-48	SP-100400	S1-101080	22.368	0015	-	Rel-10	F	Clarification of "may" in clause 7.2.2	10.0.0	10.1.0	NIMTC
SP-48	SP-100400	S1-101083	22.368	0017	-	Rel-10	F	Correction of MTC User shall in 7.2.8	10.0.0	10.1.0	NIMTC
SP-49	SP-100579	S1-102258	22.368	0023	1	Rel-10	F	Simplification of Mobile Originated Only feature	10.1.0	10.2.0	NIMTC
SP-49	SP-100579	S1-102259	22.368	0024	1	Rel-10	F	Simplification of Infrequent Mobile Terminated feature	10.1.0	10.2.0	NIMTC
SP-49	SP-100579	S1-102260	22.368	0025	1	Rel-10	F	Clarification of MTC Monitoring feature	10.1.0	10.2.0	NIMTC
SP-49	SP-100579	S1-102264	22.368	0029	1	Rel-10	F	Clarification of Group Based MTC Features	10.1.0	10.2.0	NIMTC
SP-49	SP-100579	S1-102280	22.368	0038	2	Rel-10	F	Clarification of subscription	10.1.0	10.2.0	NIMTC
SP-49	SP-100579	S1-102281	22.368	0018	2	Rel-10	F	Clarification on MTC Server relationship to network operator	10.1.0	10.2.0	NIMTC
SP-49	SP-100579	S1-102282	22.368	0027	2	Rel-10	F	Clarification of Location Specific Trigger	10.1.0	10.2.0	NIMTC
SP-49	SP-100579	S1-102287	22.368	0034	1	Rel-10	F	MTC Group Features definition clarification	10.1.0	10.2.0	NIMTC
SP-49	SP-100579	S1-102288	22.368	0035	1	Rel-10	F	MTC Infrequent Transmission clarification	10.1.0	10.2.0	NIMTC
SP-49	SP-100579	S1-102289	22.368	0036	1	Rel-10	F	MTC Secure Connection	10.1.0	10.2.0	NIMTC
SP-49	SP-100579	S1-102290	22.368	0037	2	Rel-10	F	MTC Time Controlled clarification	10.1.0	10.2.0	NIMTC
SP-50	SP-100798	S1-103312	22.368	0049	2	Rel-10	F	NIMTC Terminology	10.2.0	10.3.0	NIMTC
SP-50	SP-100798	S1-103311	22.368	0051	2	Rel-10	B	Clarification of data delay in case of Overload	10.2.0	10.3.0	NIMTC
SP-50	SP-100801	S1-103209	22.368	0045	1	Rel-11	C	Clarification on the requirements of Low Mobility MTC Feature	10.2.0	11.0.0	SIMTC
-								LTE logo changed into LTE Advanced logo	11.0.0	11.0.1	-
SP-51	SP-110162	S1-110427	22.368	0069	2	Rel-11	A	MTC charging requirements in Rel-11	11.0.1	11.1.0	NIMTC
SP-51	SP-110162	S1-110411	22.368	0071	-	Rel-11	A	Clarification of EAB	11.0.1	11.1.0	NIMTC
SP-51	SP-110167	S1-110429	22.368	0058	3	Rel-11	B	Additional security for MTC Triggering requirements	11.0.1	11.1.0	SIMTC
SP-51	SP-110167	S1-110414	22.368	0059	2	Rel-11	B	Suppress MTC device triggering	11.0.1	11.1.0	SIMTC
SP-51	SP-110167	S1-110420	22.368	0080	2	Rel-11	B	MTC - IMS Service Layer Capabilities	11.0.1	11.1.0	SIMTC
SP-52	SP-110374	S1-111026	22.368	0075	-	Rel-11	F	Correction of charging requirements	11.1.0	11.2.0	SIMTC
SP-52	SP-110374	S1-111036	22.368	0072	-	Rel-11	B	MTC - IMS Service Layer Capabilities	11.1.0	11.2.0	SIMTC
SP-52	SP-110374	S1-111304	22.368	0091	-	Rel-11	F	Clarification of MTC Device management requirement	11.1.0	11.2.0	SIMTC
SP-52	SP-110374	S1-111328	22.368	0088	1	Rel-11	F	Clarification of MTC identifier to	11.1.0	11.2.0	SIMTC

								aligning it with MTC Group feature			
SP-52	SP-110374	S1-111329	22.368	0083	2	Rel-11	B	New Requirements for MTC Monitoring Feature	11.1.0	11.2.0	SIMTC
SP-52	SP-110374	S1-111373	22.368	0092	2	Rel-11	A	Correction of SIMTC requirements to define the precedence for NAS configuration parameters in case they are defined in the device and in the USIM	11.1.0	11.2.0	SIMTC
SP-52	SP-110374	S1-111374	22.368	0078	2	Rel-11	C	MTC Device Trigger and Time Controlled MTC Feature	11.1.0	11.2.0	SIMTC
SP-52	SP-110374	S1-111375	22.368	0081	3	Rel-11	F	Clarification on MTC User	11.1.0	11.2.0	SIMTC
SP-52	SP-110374	S1-111377	22.368	0089	2	Rel-11	F	Clarification of requirements for MTC	11.1.0	11.2.0	SIMTC
SP-52	SP-110374	S1-111379	22.368	0079	3	Rel-11	C	Introduction of new scenarios for IP addressing	11.1.0	11.2.0	SIMTC
SP-53	SP-110578	S1-112334	22.368	0095	3	Rel-11	F	Clarification to small data transmissions requirement	11.2.0	11.3.0	SIMTC
SP-53	SP-110578	S1-112335	22.368	0103	2	Rel-11	C	Clarification of MTC Small Data	11.2.0	11.3.0	SIMTC
SP-53	SP-110578	S1-112336	22.368	0101	1	Rel-11	B	Location Monitoring Requirement for MTC Monitoring Feature	11.2.0	11.3.0	SIMTC
SP-53	SP-110578	S1-112337	22.368	0096	2	Rel-11	F	Correction of offline MTC Device Triggering	11.2.0	11.3.0	SIMTC
SP-53	SP-110578	S1-112338	22.368	0108	1	Rel-11	D	Editorial CR on offline MTC Devices	11.2.0	11.3.0	SIMTC
SP-53	SP-110578	S1-112339	22.368	0098	2	Rel-11	C	MTC Group-Based Addressing	11.2.0	11.3.0	SIMTC
SP-53	SP-110578	S1-112412	22.368	0099	3	Rel-11	F	MTC Small Data Transmissions	11.2.0	11.3.0	SIMTC
SP-53	SP-110651	S1-112169	22.368	0106	2	Rel-11	F	CR to 22.368 - Moving "Network provided destination for uplink data" requirement from 22.368 into 22.101	11.2.0	11.3.0	SIMTC
SP-53	SP-110651	S1-112171	22.368	0107	2	Rel-11	F	CR to 22.368 - Moving PS-Only requirements from 22.368 into 22.101	11.2.0	11.3.0	SIMTC
SP-55	SP-120103	S1-120334	22.368	0120	3	Rel-11	F	Security to MTC server and MTC application	11.3.0	11.4.0	SIMTC
SP-56	SP-120289	S1-121376	22.368	0126	1	Rel-11	F	Clarify restricting use of a USIM to specific MEs/MTC Devices	11.4.0	11.5.0	SIMTC
SP-56	SP-120289	S1-121447	22.368	0128	4	Rel-11	F	MTC Server Definition	11.4.0	11.5.0	SIMTC
SP-56	SP-120288	S1-121457	22.368	0130	5	Rel-11	F	MTC Device Power Level Monitoring	11.4.0	11.5.0	TEI11
SP-56	SP-120289	S1-121458	22.368	0131	4	Rel-11	F	Connection Error Codes for Troubleshooting Requirement	11.4.0	11.5.0	SIMTC
SP-57	SP-120524	S1-122513	22.368	0133	2	Rel-12	F	Clarification of MTC Charging Requirements wrt on line/off line	11.5.0	12.0.0	MTCe-SRM
SP-57	SP-120533	S1-122516	22.368	0127	7	Rel-12	C	External identifier availability	11.5.0	12.0.0	MTCe-SIMSE
SP-57	SP-120533	S1-122435	22.368	0132	1	Rel-12	B	MTC Device and MTC Server relation with Service Enablement Frameworks	11.5.0	12.0.0	MTCe-SIMSE
SP-58	SP-120868	S1-124465	22.368	0144	-	Rel-12	C	Removal of requirement to be able to count for device initiated signalling	12.0.0	12.1.0	MTCe-SRM
SP-58	SP-120868	S1-124489	22.368	0139	2	Rel-12	C	Clean-up of Location specific trigger Requirement	12.0.0	12.1.0	MTCe-SRM
SP-58	SP-120868	S1-124512	22.368	0145	2	Rel-12	C	Moving MTC Feature Infrequent Transmission into a generic requirement	12.0.0	12.1.0	MTCe-SRM
SP-58	SP-120868	S1-124488	22.368	0136	2	Rel-12	C	Clean-up of Time Tolerant Requirement	12.0.0	12.1.0	MTCe-SRM
SP-59	SP-130104	S1-131289	22.368	0146	2	Rel-12	C	Clarification and merge of Mobile Originated Only and Infrequent Mobile Terminated	12.1.0	12.2.0	MTCe-SRM
SP-59	SP-130104	S1-131290	22.368	0147	2	Rel-12	C	Moving MTC Priority Alarm into a generic requirement	12.1.0	12.2.0	MTCe-SRM
SP-59	SP-130109	S1-131302	22.368	0148	2	Rel-12	D	Clarification of requirements for the support of multiple service enablement frameworks	12.1.0	12.2.0	MTCe-SIMSE
SP-62	SP-130593	S1-135102	22.368	0151	-	Rel-12	F	Removal of group based charging requirements	12.2.0	12.3.0	MTCe-SRM
SP-64	-	-	-	-	-	-	-	Rel.13 version created to keep text applicable to Rel-13 only,	12.3.0	13.0.0	-

								removed in the Rel-12 version 12.4.0 by CR0153r1			
SP-66	SP-140751	S1-144352	22.368	155	-	Rel-13	F	Align the MTC monitoring requirements with Service Exposure requirements	13.0.0	13.1.0	TEI13

History

Document history		
V13.1.0	March 2016	Publication