ETSI TS 122 368 V10.5.0 (2011-07)

Technical Specification

Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
LTE;
Service requirements
for Machine-Type Communications (MTC);
Stage 1
(3GPP TS 22.368 version 10.5.0 Release 10)

Reference
RTS/TSGS-0122368va50

Keywords
GSM, LTE, UMTS

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 (http://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.

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 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: A MTC Device might also communicate locally (wirelessly, possibly through a PAN, 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 this technical specification.

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

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: 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 optimisations 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 optimised for machine type communications differs from a service optimised 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.)

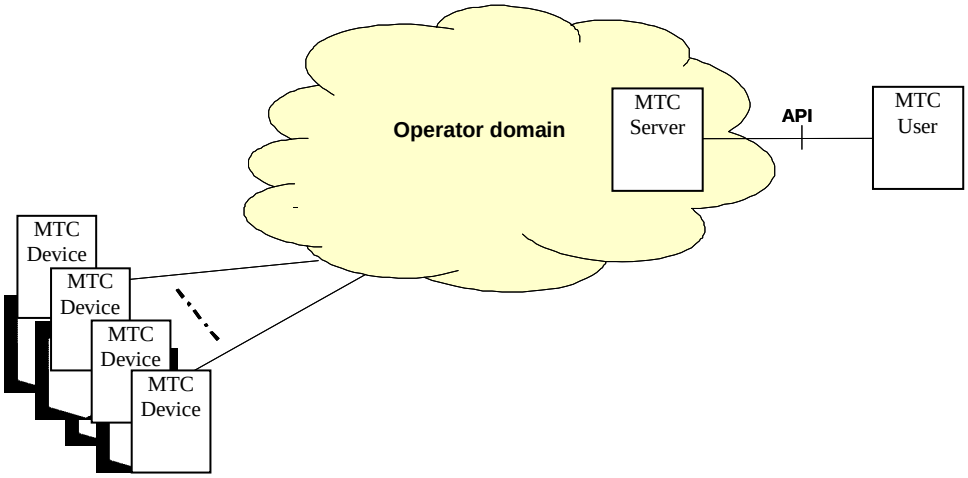

Figure 5-1: Communication scenario with MTC devices communicating with MTC server. MTC server is located in the operator domain.

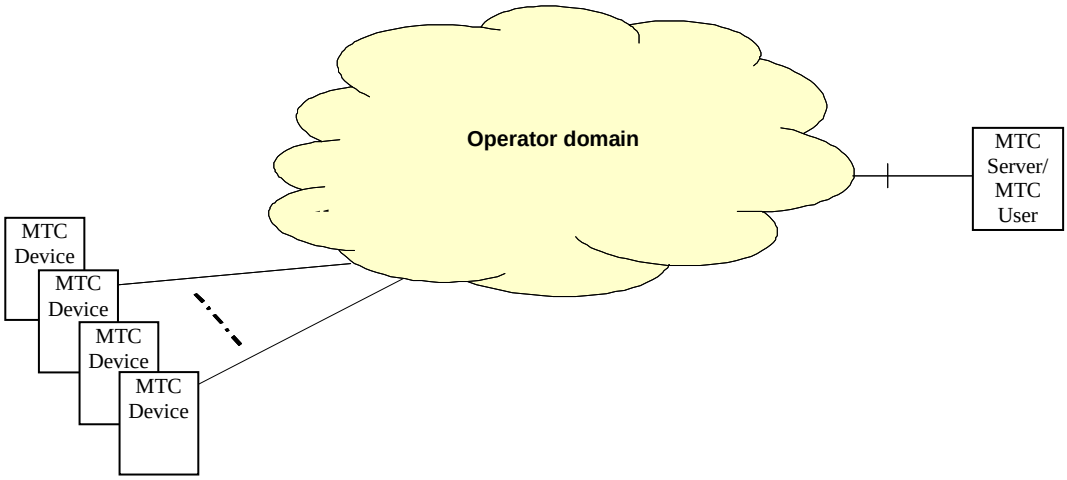

Figure 5-2: Communication scenario with MTC devices communicating with MTC server. MTC server is located outside the operator domain.

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.

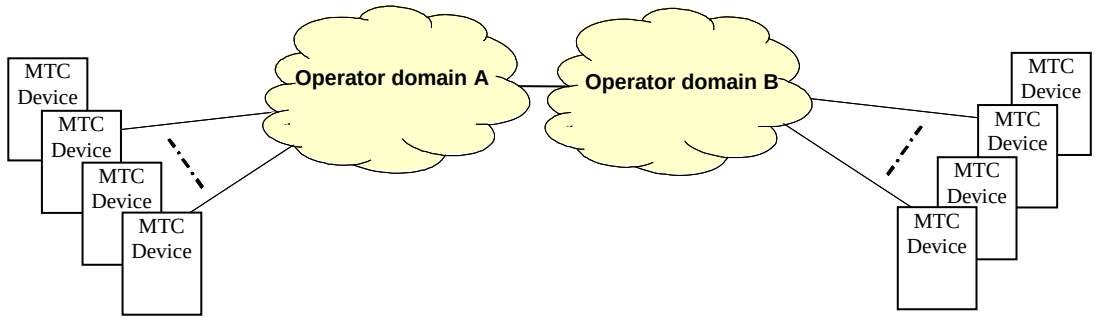

Figure 5-3: MTC Devices communicating directly with each other without intermediate MTC server.

5.2 (void)

6 (void)

7 Service requirements

7.1 Common service requirements

7.1.1 General

The following are MTC common service requirements:

- 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 [x]
- 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: 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 operator shall be able to reduce the frequency of mobility management procedures.
- Configuration parameters which are provided in the USIM shall take precedence over parameters provided in the MTC Device if both exist.

7.1.2 (void)

7.1.3 (void)

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

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

7.1.5 Charging requirements

No MTC specific charging requirements have been identified in this release.

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 management of MTC Devices should be provided by existing mechanisms (e.g. OMA DM)

7.2. Specific service requirements – MTC Features

7.2.1 (void)

7.2.2 (void)

7.2.3 (void)

7.2.4 (void)

7.2.5 (void)

7.2.6 (void)

7.2.7 (void)

7.2.8 (void)

7.2.9 (void)

7.2.10 (void)

7.2.11 (void)

7.2.12 (void)

7.2.13 (void)

7.2.14 (void)

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 locales make these devices more susceptible to tampering by unauthorised 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.

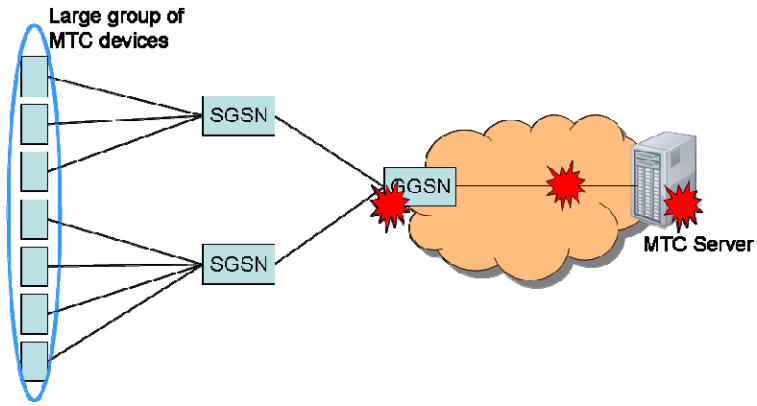

Figure A-1: Congestion in mobile core network and on the link between mobile core network and MTC Server

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.

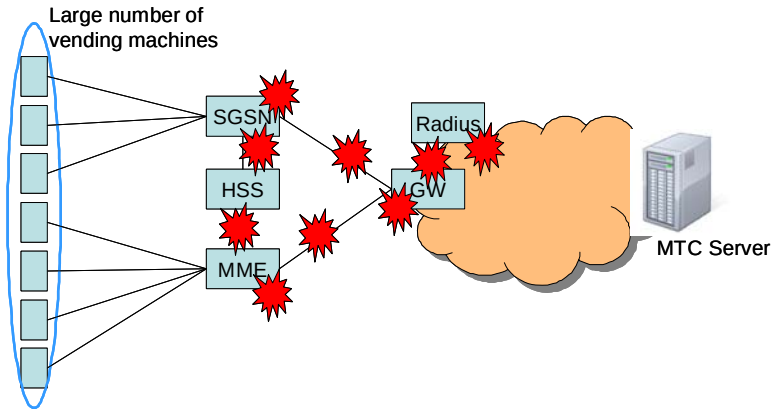

Figure A-2: Signalling network congestion.

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:

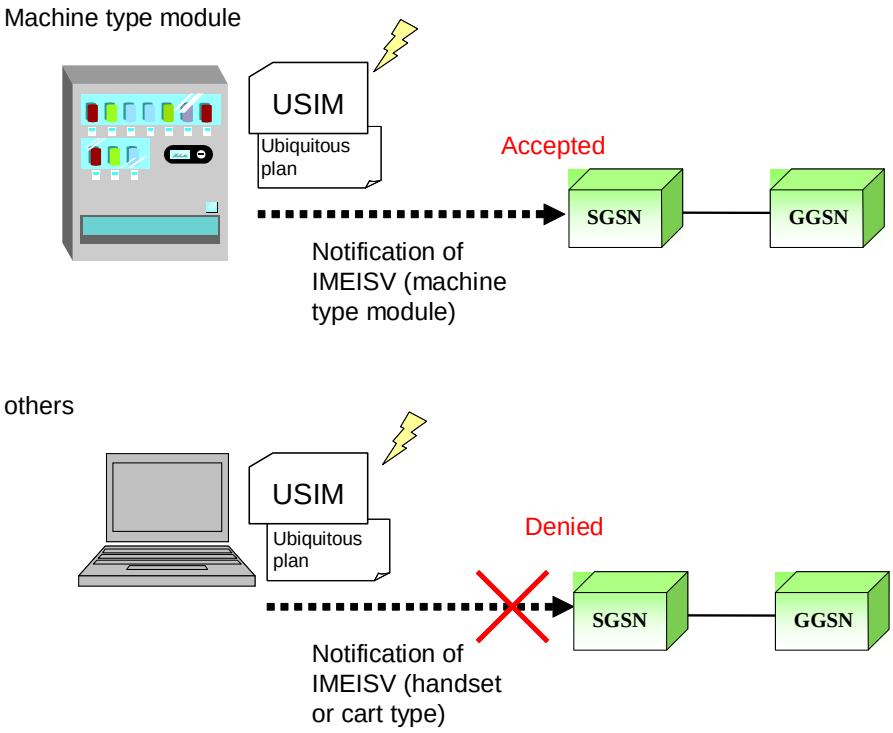

Figure A-3: Access Control with billing plan

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.

Location Specific MTC Devices Trigger Use Case

MTC Devices are generally programmed to autonomously set up a connection to report an event. However, in some implementations it is required that MTC Devices are triggered by the M2M application e.g. by sending them a SMS. In the future millions of this type of MTC Devices will be deployed, while it may be desirable from a M2M application perspective to poll only a sub-set of the MTC Devices in a specific area. For example, during a storm a water authority wants to get status information of dike sensors in a specific area. It is then required that only sensors in that specific area are triggered.

As for several M2M applications the MTC Devices are at fixed locations, which are well known by the M2M application owner, it is a waste of network resources to store the location information of these MTC devices in the network. Also scalability issues will come in play if millions of terminals need to be polled in a relative short time.

A more efficient and scalable polling mechanism is required to trigger M2M devices based on location information provided by the application or user, to subsequently set up a data or other type of connection e.g. a SMS, PDP context to the network.

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.

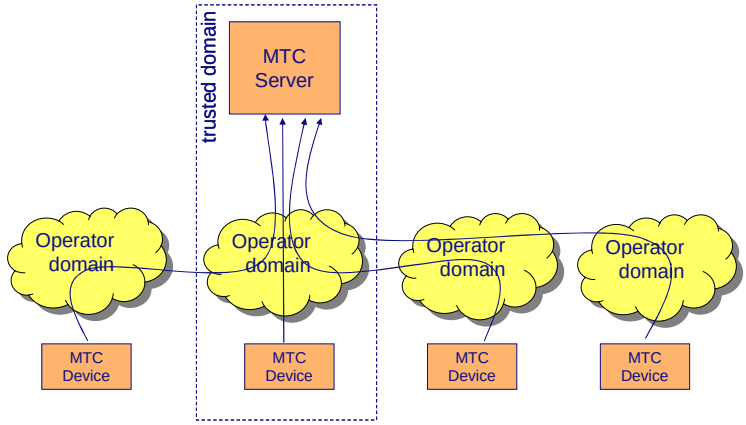

Figure A-4: End-to-end security for roaming MTC devices

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 optimisation/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-100861	S1-103226	22.368	0046	2	Rel-10	F	Alignment with Stage 2	10.2.0	10.3.0	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
-								LTE logo changed into LTE Advanced logo	10.3.0	10.3.1	-
SP-51	SP-110162	S1-110364	22.368	0064	1	Rel-10	F	SA2 Alignment for MTC Time Tolerant Feature	10.3.1	10.4.0	NIMTC
SP-51	SP-110162	S1-110374	22.368	0067	1	Rel-10	F	MTC charging requirements in Rel-10	10.3.1	10.4.0	NIMTC
SP-51	SP-110162	S1-110410	22.368	0070	1	Rel-10	F	Clarification of EAB	10.3.1	10.4.0	NIMTC
SP-52	SP-110370	S1-111306	22.368	0074	1	Rel-10	F	Removal of Rel-10 MTC Charging requirements	10.4.0	10.5.0	NIMTC
SP-52	SP-110370	S1-111309	22.368	0093	-	Rel-10	F	Deletion of requirement on MTC USIM for Release 10	10.4.0	10.5.0	NIMTC
SP-52	SP-110370	S1-111372	22.368	0090	2	Rel-10	F	Correction of NIMTC requirements to define the precedence for NAS configuration parameters in case they are defined in the device and in the USIM	10.4.0	10.5.0	NIMTC

History

Document history		
V10.4.0	May 2011	Publication
V10.5.0	July 2011	Publication