ETSI TR 122 988 V13.0.0 (2016-01)

Universal Mobile Telecommunications System (UMTS);
LTE;
Study on alternatives to E.164 for
Machine-Type Communications (MTC)
(3GPP TR 22.988 version 13.0.0 Release 13)

Reference
RTR/TSGS-0122988vd00

Keywords
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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

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 Report (TR) 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 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

There are currently unprecedented demands within the telecommunications industry for E.164 MSISDNs resources and these demands are expected to accelerate in the years to come. Accordingly, some countries and their national regulatory authorities have expressed concerns over the numbering requirements of new services involving Machine Type Communications (MTC) services and their expected rapid growth.

MTC demand is forecast to grow from 50M connections to over 200M by 2013. A large number of these services are currently deployed over circuit-switched GSM architectures and therefore use E.164 MSISDNs although such services do not require 'dialable' numbers, and generally do not communicate with each other by human interaction.

Without technical alternative to using public international numbering resources as addresses, and considering the current forecasts and pending applications for numbers made to numbering plan administration agencies, there is a significant risk that some national numbering/dialling plans will run out of numbers in the near future, which would impact not only these MTC services but also the GSM/UMTS service providers in general.

1 Scope

This document seeks to study and highlight the challenge of using the existing public numbering resources to support Machine Type Communication (MTC) services and proposes that 3GPP develop an alternative to using public numbering resources for MTC communications.

2 References

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

[2] 3GPP TS 41.101: "Technical Specifications and Technical Reports for a GERAN-based 3GPP system".

[3] IETF RFC 3986 "Uniform Resource Identifier (URI): Generic Syntax'.

3 Definitions, symbols 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].

(void)

3.2 Symbols

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

(void)

3.3 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 Use cases

4.1 Use case 1 (Wireless Vending Machines)

4.1.1 Short Description

The Snack Company owns 100,000 snack vending machines in the Tri-City area. Each machine is connected to Snack"s central network via a wireless connection and sends a report of sales every hour. These scheduled reports are staggered so they don"t collide within Snack"s systems. These reports are short bursts of no more than a few hundred bytes of data, and typically take less than 3 seconds to transmit. On occasion, Snack"s network will contact a machine by sending it an SMS, to which the machine sends a response.

Snack would like to add another 250,000 machines across the state, but their wireless service providers cannot provide enough MSISDNs. One provider, however, has implemented SIP capability, and makes available radio modules that use all-IP connections over the radio network. The main benefits to this new service is that each machine is assigned a SIP URI rather than a MSISDN (an alphanumerical SIP URI that doesn"t encapsulate a phone number), and that the service provider expects network loads and costs to decrease by going with all-IP traffic. The service provider"s network can easily handle the traffic load from 350,000 vending machines.

The service provider has assigned Snack its own domain, vending. snack.com, so Snack can assign its own names to the machines. Snack has chosen to use its internal asset numbers for machine names to simplify the mapping from their asset management system to the messaging interface provided by the service provider. Messages are generated by Snack"s system and sent via the Internet to a web service provided by the service provider. The service provider then delivers the messages to the machines using SMS over IP. The machine modules are pre-configured to send scheduled reports to a web service provided by the service provider that transmits them to Snack"s network. All messages are encrypted in transit.

Because the service provider was able to 'recover' 100,000 previously issued MSISDNs, it was able to expand its coverage to wireless service consumers, generating much greater margins in the process.

4.1.2 Actors

- Snack Company
- Its wireless service provider

4.1.3 Pre-Conditions

- The service provider has available to it IP-ready radio modules
- The service provider"s network can support SIP or IMS, and is able to map a SIP URI to an IMSI or IMPI in its HLR or HSS node. The service provider can support SIP URIs with a domain name of <XYZ>vending.snack.com.
- The service provider has a messaging gateway, maybe not much more than a web service
- The radio modules are capable of establishing an IP connection in response to a page over the paging channel

4.1.4 Post-Conditions

- Vending machines transmit sales and trouble reports according to the schedule
- Snack"s network receives and processes the reports
- The service provider"s network supports the traffic load
- Machines are reachable via their SIP URI and the service provider"s message gateway
- The service provider"s experience allows it to lower the price charged to Snack by 25%

4.1.5 Normal Flow

In the course of normal operations, there are three main events for a given vending machine:

1) When it first powers up and registers with the network
2) When it generates and sends a report to the network
3) When the Snack network sends a message to the machine

Each of these events is comprised of a sequence of smaller steps.

Registration:

1) The machine powers up

2) The radio module registers through the GPRSnetwork in the normal way

3) The radio module registers with the SIP server on the service provider"s network. This sets up the mapping between the SIP URI in the HSS and the newly assigned IP address

Note: this would normally require a MSISDN+IMSI (IMSI for authentication and MSISDN generally required in all back-office IT/IS).

Remote-originated messages:

1) The machine 'wakes up' on schedule and establishes a SIP session with the SIP server

2) The machine generates a report as a short message then transmits that to the SIP server as a message payload. If the message is more than 1500 bytes, then concatenated messages are sent.

3) The SIP server acknowledges receipt of the message

4) The machine terminates the SIP session

5) The machine goes back to 'sleep'

Remote-terminated messages:

1) The Snack network generates a message addressed to a specific SIP URI

2) Snack sends the message to the service provider"s message gateway

3) The service provider"s HSS contains the mapping of SIP URI to IMSI or IMPI, and to the currently assigned IP address

4) The service provider pages the machine over the paging channel using the IMSI or IMPI

5) The machine responds by establishing a SIP session with the SIP server

6) The service provider delivers the message to the machine as a message payload

7) The machine responds

8) The machine terminates the SIP session

9) The machine goes back to 'sleep'

4.1.6 Alternative Flows

The messaging interface also allows the machine to send trouble reports that go directly into Snack"s trouble ticketing system. These messages are generated by on-board logic in the machine and sent to a different web service. The steps required to do this are the same as for remote-originated messages described above.

4.1.7 Exceptions

Due to the standard nature of the communications, the main exceptions occur when a message cannot be delivered for some reason. The most common reason, based on early experience, is that the web service Acme occasionally goes down. This is a result of the way Snack"s services are configured and not related to SIP or the service provider"s network. When this happens, the web services on the service provider"s network queue the messages and deliver them in the order they were received when Snack"s services come back online. The service provider has implemented Web Services messaging and security practices.

4.2 Use case 2 (Smart Bridges and Tunnels)

4.2.1 Short Description

The State of California would like to install up to 150,000 sensors on the Golden Gate Bridge to monitor structural elements by measuring displacement, temperature, humidity, and magnetic or ultrasonic resonance. These measures are

used to detect structural deficiencies in the bridge that require attention, perhaps immediate attention. Each sensor takes measurements on a periodic basis, 'wakes up,' and transmits a short burst of data of less than a few hundred bytes to the state"s central system where it is analyzed. On occasion, the state"s system will contact a sensor by sending it an SMS, to which the machine sends a response. Most often, this is a result of the system needing more information based on the report of another sensor nearby. The sensors use an IP data connection.

Due to the expense and time required to install wire-based connections and the advancements in battery technology, the state wants to use wireless network. To avoid having to buy, install, and run its own radio network, the state decides to use a service provided by a mobile network operator. To preserve the limited supply of MSISDNs in the area, one provider, suggests using a SIP capability and has offered to create a domain specifically for the Golden Gate Bridge, goldengate.bridge.ca.net, allowing the state to assign its own names to the sensors. Messages are generated by the state"s system and sent directly to the SIP URI assigned to a sensor when it was configured via a web service gateway offered by the service provider. The service provider then translates the SIP URI into the IP address assigned to the sensor when it first powered up and registered with the network. The sensors are pre-configured to send scheduled reports to a web service provided by the state via the service provider"s messaging gateway. All messages are encrypted in transit.

4.2.2 Actors

- The State of California
- Its wireless service provider

4.2.3 Pre-Conditions

- The service provider"s network can support SIP or IMS, and is able to map a SIP URI to an IMSI or IMPI in its HLR or HSS node. The service provider can support SIP URIs with a domain name of <XYZ>.goldengate.bridge.ca.net.
- The service provider has a messaging gateway, maybe not much more than a web service
- The radio modules are capable of establishing an IP connection in response to a page over the paging channel

4.2.4 Post-Conditions

- Sensors transmit data and trouble reports according to the schedule
- The state"s network receives and processes the reports
- The service provider"s network supports the traffic load
- Sensors are reachable via their SIP URI and the service provider"s message gateway

4.2.5 Normal Flow

In the course of normal operations, there are three main events for a given sensor:

1) When it first powers up and registers with the network
2) When it generates and sends a report to the network
3) When the state"s network sends a message to the sensor

Each of these events is comprised of a sequence of smaller steps.

Registration:

1) The sensor powers up
2) The radio module registers through the GPRSnetwork in the normal way
3) The radio module registers with the SIP server on the service provider"s network. This sets up the mapping between the SIP URI in the HSS and the newly assigned IP address

Remote-originated messages:

1) The sensor 'wakes up' on schedule and establishes a SIP session with the SIP server
2) The sensor generates a report as a short message then transmits that to the SIP server as a message payload. If the message is more than 1500 bytes, then concatenated messages are sent.
3) The SIP server acknowledges receipt of the message
4) The sensor terminates the SIP session
5) The sensor goes back to 'sleep'

Remote-terminated messages:

1) The state"s network generates a message addressed to a specific SIP URI
2) The state sends the message to the service provider"s message gateway
3) The service provider"s HSS contains the mapping of SIP URI to IMSI or IMPI, and to the currently assigned IP address
4) The service provider pages the sensor over the paging channel using the IMSI or IMPI
5) The sensor responds by establishing a SIP session with the SIP server
6) The service provider delivers the message to the sensor as a message payload
7) The sensor responds
8) The sensor terminates the SIP session
9) The sensor goes back to 'sleep'

4.2.6 Alternative Flows

The messaging interface also allows the sensor to send trouble reports that go directly into the state"s trouble ticketing system. These messages are generated by on-board logic in the sensor and sent to a different web service. The steps required to do this are the same as for remote-originated messages described above.

4.2.7 Exceptions

Due to the standard nature of the communications, the main exceptions occur when a message cannot be delivered for some reason. The most common reason, based on early experience, is that the web service the state uses occasionally goes down. This is a result of the way the state"s services are configured and not related to SIP or the service provider"s network. When this happens, the web services on the service provider"s network queue the messages and deliver them in the order they were received when the state"s services come back online. The service provider has implemented Web Services messaging and security practices.

4.3 Use case 3 Implantable Defibrillators

4.3.1 Short Description

Acme Medical Devices has introduced an implantable defibrillator that makes use the GSM network to provide 24 hour access to patient status. These devices are expensive and are reserved for patients with very serious heart rhythm issues or patients who have received a heart transplant. Existing implantable defibrillators require an external transceiver that connects to a wired phone line. By embedding the mobile capability in the device, the expense and inconvenience of the external transceiver is removed. The resulting devices are less expensive and allow the patient more latitude for travel and moving around. Like existing devices, the lithium-ion batteries are charged by induction so no physical contact with the device is required or desired.

The company estimates that 1-2 million devices will eventually be operating within North America, with the potential for as many in Europe.

Regional and national wireless service providers have balked at allowing these devices to connect to their networks. The problem, they say, is that the target markets for these devices are highly concentrated and would strain the numbering resources in a few communities. Roaming is an issue but could be handled with existing business agreements.

A consortium of service providers has proposed adopting SIP URIs as the primary means to address these devices. Acme would be assigned a domain name, and would be free to assign each device a number or name of its choosing. Acme has agreed to manufacture the devices to assume an IP connection, and Acme"s radio module manufacturers have agreed to create modules that open an IP connection in response to a signal over the paging channel.

Future versions of the device may be able to capture location information and transmit that along with other medical data to the nearest emergency call center or public safety answering point, effectively generating an automatic emergency call.

4.3.2 Actors

- Acme Medical Devices Company
- Radio module manufacturers
- Wireless service provider

4.3.3 Pre-Conditions

- Acme"s suppliers provide IP-ready radio modules
- The service providers" networks support SIP or IMS and are able to map a SIP URI to an IMSI or IMPI in their HSS or HLR nodes
- The service providers have messaging gateways that allow Acme or doctors to contact specific devices via IM messages or via SIP over IP

4.3.4 Post-Conditions

- Defibrillators can originate and receive messages over an IP connection
- The service providers" networks support the loads
- Devices are reachable via their SIP URIs and the service provider message gateways
- Patients report increased satisfaction from not having to remain close to home
- The end-to-end system proves more reliable due to the nature of the connections between the old-style devices and the external transceivers.

4.3.5 Normal Flow

In the course of normal operations, there are three main events for a given sensor:

1) When it first powers up and registers with the network
2) When it generates and sends a report to the network
3) When the company"s network sends a message to the sensor

Each of these events is comprised of a sequence of smaller steps.

Registration:

1) The devices are powered up and tested in the operating room before implantation
2) The device powers up
3) The radio module registers through the GPRSnetwork in the normal way
4) The radio module registers with the SIP server on the service provider"s network. This sets up the mapping between the SIP URI in the HSS and the newly assigned IP address

Remote-originated messages (Assumes device is registered on the network):

1) The device 'wakes up' on schedule and establishes a SIP session with the SIP server
2) The device generates a report as a short message then transmits that to the SIP server as a message payload. If the message is more than 1500 bytes, then two messages are sent.
3) The SIP server acknowledges receipt of the message
4) The device terminates the SIP session
5) The device goes back to 'sleep'

Remote-terminated messages:

1) The company"s network generates a message addressed to a specific SIP URI
2) The company sends the message to the service provider"s message gateway
3) The service provider"s HSS contains the mapping of SIP URI to IMSI or IMPI, and to the currently assigned IP address
4) The service provider pages the sensor over the paging channel using the IMSI or IMPI
5) The device responds by establishing a SIP session with the SIP server
6) The service provider delivers the message to the device as a message payload
7) The device responds
8) The device terminates the SIP session
9) The device goes back to 'sleep'

4.3.6 Alternative Flows

When a device responds to an event in the patient"s heart, a report is generated an immediately sent to the doctor via the company"s portal. Future versions of the device may use network and/or GPS information to capture location and transmit an emergency call to the nearest emergency call center, either automatically or at the instructions of the patient"s doctor.

4.3.7 Exceptions

The most critical exception occurs when the GSM network is unreachable. The radio modules are built to work on every standard cellular network in either North America or Europe, depending on the model, but there are still areas that do not have access to a network. In those cases, the device will queue up all event reports for transmission when the network is next reachable.

4.4 Use case 4 (Wireless Utility Meters)

4.4.1 Short Description

The Edison Power company installed devices in its serving area to report meter readings at the end of billing cycles each month. Devices can have different billing cycles. Each device is configured to send the meter reading to a pre-

configured Edison Power company server via the wireless connection. The Edison Power company server can also submit a request to an interworking gateway in the wireless service provider network to send a trigger to a specific device to report the meter reading (e.g., when the service is terminated).

The Edison power company uses a device ID in the format of <device-ID>.meter.edisonpower.biz (e.g., a Fully Qualified Domain Name (FQDN)) where the device-ID contains a 10-digit number and each number uniquely identifies a device.

4.4.2 Actors

- Edison Power company
- Its wireless service provider

4.4.3 Pre-Conditions

- The wireless service provider has assigned an IMSI to each device and has provisioned that internal identifier and other information on the relevant network nodes and on each device
- Devices are always powered on and attached to the wireless service provider network once it attaches to the wireless service provider network
- Devices do not have always-on data connections but can listen and receive the trigger from the wireless service provider network
- The wireless service provider network has an interworking gateway that allows the Edison Power company server to submit a trigger request to be sent to a specific device indicated by a device ID in the format of <10-D number>.meter.edisonpower.biz
- The wireless service provider network can map the device ID to the associated IMSI and send a trigger to the associated device
- Each device has been configured to know where to send the meter reading to (e.g., Edison Power company server"s IP address or domain name)

4.4.4 Post-Conditions

- Devices can send the meter reading over the data connection to the Edison Power company server at pre-configured date/time of the month or when receiving a trigger from the Edison Power company server
- The Edison Power company server can submit a trigger request for any device and the wireless service provider network can send the trigger to that device

4.4.5 Normal Flow

Send meter reading:

1) A device detects that it is scheduled to send a report or receives a trigger and takes the meter reading.
2) The device sets up a data connection and sends an IP packet containing its device ID and the meter reading to the Edison Power company server"s IP address.
3) The Edison Power company server acknowledges the successful receipt of the meter reading.
4) The device terminates the data connection.
5) The wireless service provider network removes resources associated with the terminated data connection.

Submit a trigger request:

1) The Edison Power company server determines that it needs to ask a specific device to send the meter reading.

2) The Edison Power company server submits a trigger request for that specific device ID to an interworking gateway in the wireless service provider network.

3) The interworking gateway in the wireless service provider network interrogates with relevant network nodes to authenticate and authorize the request and sends a trigger to the device.

4) The device receives the trigger and invokes the 'Send meter reading' process above to send the meter reading to the Edison Power company server.

4.4.6 Alternative Flows

The wireless service provider network may return a positive indication to the Edison Power company server about the successful delivery of the trigger to the device.

The Edison Power company server can include a command in the response to change the settings (e.g., date/time to report meter reading) at the device when it receives the meter reading from the device.

4.4.7 Exceptions

The device re-sends the meter reading at a configured time later if it cannot communicate with the Edison Power company server or the Edison Power company server indicates an internal problem.

The wireless service provider network may return a negative indication to the Edison Power company server if it fails to deliver the trigger to the device.

4.5 Use case 5 (Wireless Weather Monitors)

4.5.1 Short Description

The WeatherABC company installed devices in the US to collect weather information. Each device is configured to collect the weather information at a pre-configured time interval and send the weather information after N (e.g., 10) measurements to a pre-configured WeatherABC company server via the wireless connection. The WeatherABC company server can also request the wireless service provider network to send a command to a specific device via an interworking gateway in the wireless service provider network to change the configured settings in that device.

The WeatherABC company uses a device ID in the format of <device-ID>@weatherABC.com (e.g., an Network Access Identifier (NAI)) where the device-ID contains a string up to 12 alphanumeric characters and each string uniquely identifies a device.

4.5.2 Actors

- WeatherABC company
- Its wireless service provider

4.5.3 Pre-Conditions

- The wireless service provider has assigned an IMSI to each device and has provisioned that internal identifier and other information on the relevant network nodes and on each device
- Devices are powered off when not collecting weather information
- Devices wake up at certain times to collect weather information or report weather information or listen to incoming commands
- The wireless service provider network has an interworking gateway that allows the WeatherABC company server to submit a command to be sent to a specific device indicated by a device ID in the format of <12-alphanumeric-character string>@weatherABC.com

- The wireless service provider network can map the device ID to the associated IMSI and send a command via signaling to the associated device
- Each device has been configured to know where to send the weather information to

4.5.4 Post-Conditions

- Devices can send the weather information over the data connection to the WeatherABC company server at the pre-configured time interval
- The WeatherABC company server can submit a command for any device and the wireless service provider network can deliver the command to that device
- A device can change the settings according to the command received from the WeatherABC company server via the wireless service provider network

4.5.5 Normal Flow

Send weather information:

1) A device detects that it is to send the collected weather information.
2) The device sets up a data connection and sends an IP packet containing its device ID and weather information to the WeatherABC company server"s IP address.
3) The WeatherABC company server acknowledges the successful receipt of the meter reading.
4) The device terminates the data connection.
5) The wireless service provider network removes resources associated with the terminated data connection.

Submit a command request:

1) The Edison Power company server determines that it needs to ask a specific device to change certain settings.
2) The Edison Power company server submits a command request for that specific device ID to an interworking gateway in the wireless service provider network. The request may include the location of the device and the time to deliver the command to the device (e.g., when the device will wake up to listen to the incoming commands).
3) The interworking gateway in the wireless service provider network interrogates with relevant network nodes to authenticate and authorize the request and deliver the command to the device.
4) The device acknowledges the receipt of the command and changes the settings according to the received command.
5) The wireless service provider network returns a positive indication to the WeatherABC company server about the successful delivery of the command to the device.

4.5.6 Alternative Flows

The device may inform the WeatherABC company server about the successful execution of the received command.

The WeatherABC company server can include a command in the response to change the settings at the device when it receives the weather information from the device.

4.5.7 Exceptions

The device can re-send the weather information at a configured time later if it cannot communicate with the WeatherABC company server or the WeatherABC company server indicates an internal problem or can include the weather information in the next report.

The device may inform the WeatherABC company server if it cannot execute based on the received command

The wireless service provider network returns a negative indication to the WeatherABC company server if it fails to deliver the command to the device.

5 High level Service Aspects

5.1 What are the high level requirements for alternatives to E.164 for machine-type communications?

Any alternative addressing scheme needs to take into account the services provided to the MTC device. There are 3 types of service that need to be considered:

- Voice or video (e.g. portal) service
- SMS service
- Data service

MTC applications have long moved away from using CS services in favour of PS service for MTC so only a very small percentage of newly deployed solutions will be relying on this CS service. However, a significant number of existing MTC applications including some with large infrastructures still rely on CS service including those based on the Circuit Switched Data bearer service. Given this, much less emphasis on solving the MSISDN issue with regard to CS services is required. One of the remaining issues in that respect is that as underlined in the previous section accessing PS service will require authentication to the mobile network, which may directly or indirectly (eg in IS systems) rely on MSISDNs.

SMS is still frequently used by even newly deployed MTC applications, however, MTC applications do not require SMS per se, MTC applications only require a mechanism to send MT messages (to the UEs). SMS is currently used for that purpose. Some applications however do require MO messages (from the UEs) and SMS is used as a wake up mechanism for the UE to trigger such actions. The SMS is sent to trigger the UE to setup a PDP connection to the server (or to re-trigger the connection when this PDP connection is lost) or to trigger device management connection. This requires specialized SMS handling in the UE and MTC Server. Always-on PS connections are rarely used and reasons include:

- lack of publically routable IPv4 address space,
- lack of PS capacity in the CN (e.g. GGSNs),
- lack of PS only network support etc.

Currently device management (e.g. OMA Device Management) also uses SMSs for triggering the device to initiate a PDP connection and contact the device management server. If the device were able to maintain an always-on PS connection, the device management could use an IP method e.g. SIP Invite to initiate a device management session which is supported by popular DM protocols e.g. OMA DM.

There are several scalable options for device identification in the PS domain: SIP URI, FQDN, NAI or IPv6. IPv6 could be used for both device identification and message routing purposes but requires the CN and the MTC Server to support IPv6. Although the deployment of IPv6 in the network is within MNO control, the deployment of IPv6 with an external MTC Server is not so IPv6 is an unlikely solution for the short term given that less than 1% of servers in the world support IPv6 now. SIP URI, FQDN, NAI or a proprietary application level ID does not require IPv6 but does require special clients in the UE and possibly additional services in the CN. Such 'human-readable' formats would probably be preferable to the IPv6 address (hexadecimal format) for device identification if only for reading purposes.

Due to the shortage of publicly routable IPv4 addresses, IPv4 is not a scalable alternative for identification for MTC services. It can however be used for routing if a NAT is used by the CN. However, if a NAT is used, the problem of MT messages needs to be solved without the use of an MSISDN (some solutions have been identified in TR 23.888 and this is currently a requirement already in TS 22.368).

For MTC devices, the requirements for an alternative addressing scheme are provided in the sections below.

5.1.1 Large capacity

The addressing scheme will need to cater for at least two orders of magnitude more than needed for human to human communications. The addressing scheme will need to be able to handle a minimum of 50 billion devices.

It should therefore have a large capacity, be flexible and scalable. It should also be capable of uniquely addressing any MTC device globally.

5.1.2 Compatibility with existing schemes

Any new addressing scheme will need to be compatible with or at least be capable of working with existing schemes including E.164 and E.212 and also IP addressing for data session services. This compatibility of "interworking" with an existing scheme should also have no impact on these "legacy" identification schemes and the associated mechanism (see also 5.1.3) i.e. be backward compatible.

The use of SIP allows MTC devices for any given customer to reside on any operator"s network. Discovery of SIP servers via DNS routing automatically directs the SIP signalling traffic towards the correct network.

IP connections require an open connection between the MTC device and the server. This connection is maintained by the network access hardware, the network adapter in hard-wired device, or the radio in a mobile device. To minimize the power requirements, MTC devices should maintain the connection using network-facing hardware, much like the hardware that today listens for CS signalling.

IPv6-addressing for MTC services diminishes the significant risk that some national numbering and dialling plans will run out of numbers in the near future, especially with the wide introduction MTC services.

A long-term solution that depends on a rapid world-wide grow-curve of MTC service deployment is needed and points towards consideration of IPv6 addressing in combination with identifiers defined after, for instance SIP-addresses, URIs/URLs, as the most feasible strategic solution.

Applying specific MTC solutions utilizing IPv6-addressing and corresponding identifiers in core and radio networks is important to properly cover the large capacity of MTC devices deployment expected by year 2013 and extending over and beyond the next two decades.

5.1.3 Impact on existing systems and hardware

The implementation of an alternative MTC addressing scheme should not require significant changes to the existing mobile network radio and core network components (e.g. HLR/VLR). Similarly, significant changes to the USIM should be avoided. It is less important if there have to be changes to the functions of the Mobile Terminal to support a new addressing scheme as for many MTC applications, new, specific devices will probably be produced.

When a SIP-enabled device powers on, it registers its location (IP address) with its network. This location is stored at the HLR/HSS that can respond to the query for the location of an intended device so that inbound packets can be routed to the device. Once registration is complete, the main part of the device may power down, so long as part of the device is listening to the network for 'wake-up' packets, similar to the way GSM devices continue to listen for inbound SMS messages.

5.1.4 Provisioning

It should be possible to use an alternative addressing scheme with minimum change to the MNO"s existing provisioning systems.

5.1.5 Device Identity Portability

'Device identity' portability may need to be supported for MTC Devices in some cases or be irrelevant depending on the applicable national regulatory requirement, (for applicability of number portability to M2M, see ECC report on M2M numbering http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP153.PDF).

5.1.6 Charging

The alternative addressing scheme should be capable of identifying the MTC device for charging without major changes to the Operator billing systems.

5.1.7 Services

The alternative addressing scheme should support all services required by the MTC application including Voice, SMS and Data communication. It should support both Mobile Originated and Mobile Terminated calls/sessions.

5.2 What are the security, reliability, and priority handling requirements for alternatives to E.164 for machine-type communications?

Any alternative addressing scheme should provide the same level of security and reliability as the current addressing schemes. An alternative scheme should support priority handling.

Any alternative addressing scheme should allow the addressing of the MTC device and/or USIM for software updates. This includes new device software (e.g. operating system, applications) and updates to the USIM using the existing remote update mechanisms. It should also allow access for controlling the MTC device (e.g. ability to switch the MTC device on/off, control its use).

5.3 Are there any implications due to roaming?

Roaming must still be supported by any alternative addressing scheme. This includes support of national and international roaming (both persistent and permanent roaming).

5.4 Are there any implications on inter-domain routing?

Call/session routing between networks/operators must still be supported by any alternative addressing scheme to MSISDNs. A large part of MTC devices do need to be addressable from endpoints that do not belong to the same network. This includes support of national and international interconnection.

5.5 Are there any implications to hand-over between access networks?

Handover between access networks (e.g. GSM/GPRS to UMTS) should be possible with any alternative addressing scheme.

6 MMI Aspects

The main point of interface to these machines is through the service provider"s message gateway. The gateway is a web service that accepts SOAP messages addressed to one or more machines. The gateway uses the information in the HSS to translate the SIP URI to the current IP addresses (IPv4 or IPv6) of the machine, then transmit the message payload using SMS over IP or IM paging mode. If the payload is short enough, it can be sent directly in a SIP message. A service provider may choose to put a web site in front of this server to allow human users to manage, manipulate, and send messages or commands to machines. Behind this interface, though, lies the same web service used by the customer"s systems.

7 Charging Aspects

Networks that support IP traffic are already set up to charge for it. Many network operators charge by the megabyte or gigabyte. For MTC communications, the traffic for all of the devices owned by a given customer can easily be collected, rated, and billed in the aggregate or by device. This allows for great flexibility in the possible billing arrangements between customers and service providers. Any new scheme should also make it possible to differentiate between MTC traffic and 'normal' interpersonal calls for charging purposes.

8 Security Aspects

SIP has built-in security, using a three-way handshake (INVITE/OK/ACK) to mutually authenticate sender and receiver. Authentication is done using shared certificates, or using dynamic keys such as those generated by Generic Bootstrap Architecture (GBA) [7]. In addition, many of the parameters to be used for the session are negotiated during this process.

9 Analysis

For future MTC schemes the following schemes could be considered for identification of the MTC device:

Table 9.1: Analysis of the different addressing schemes

	Pros	**Cons**
MSISDN (E.164) with existing number length	- existing number portability mechanism might be used - 'Backward compatible' (current MTC identification scheme) - No impact on billing systems - Potentially compatible with non always on MTC devices	- Numbering plan exhaustion - Impacts for compatibility for interconnection with Internet - Regulation prohibits the use of existing interpersonal number ranges in some territories, (e.g. Netherlands).
MSISDN (E.164) with max length of 15 digits	- No new standards required - Can give a large number of additional MSISDNs - Solution available from ITU-T global resouces.	- May need changes to existing network equipment - May impact some legacy billing systems
IMSI (E.212)	- Widely supported in mobile networks today (but not for session/call routing)	- Impacts networks and billing systems
Other Numbering Plan Indicator as supported by MAP such as Telex or re-use of Spare code as 'M2M'	- Widely supported in 3GPP standards	- Not used (today) for call/session routing - Need to define or redefine a new code point in MAP
Uniform Resource Identifier URI	- URI can be resolved to IP address by DNS - Well know concept on Internet - Widely accepted on Internet - Can be used in conjunction with E.212 - No IMS client needed on UE	- Not used in today"s wireless network as an MTC identifier - May require some Network System upgrades (e.g. HSS) - Requires IT backend support system upgrade (e.g. billing, provision systems)
[SIP] Uniform Resource Identifier sip:MTC@domain	- Potentially backward compatible if a subspace of the MTC URI scheme is used to 'map' E.164 numbers (MSISDNs) - Virtually unlimited space	- Format to be clarified - Requires IT backend support system upgrade (e.g. billing, provision systems)

		- Requires SIP stack in device
TEL Uniform Resource Identifier (URI) **a. Containing an E.164 number (e.g., tel:+1-571-434-1234 or tel:434-1234;phone-context=+1-571)**	- Backward compatible with E.164 numbers (MSISDNs) - No billing system impacts	- Need ENUM to translate MSISDN to URIs then IP address(es). - Relies on E.164 - Numbering plan exhaustion
b. Containing a private number (e.g., tel:1234;phone-context=example.com)	- No E.164 resource consumption - IMS may support routing of this type of TEL URI - The private number may be carried in the revised MSISDN parameter with the addition of a new numbering plan indicator if the phone-context content identifies a specific numbering plan - Virtually unlimited address space	- Not used in today"s mobile networks as a device identifier - No end-to-end support for private number in TEL URI - Need a new code point in MAP to extend the original MSISDN parameter to non-E.164 numbers to carry the private number - Require system upgrades - Require IT backend support system upgrades (e.g., billing, provisioning systems)
Domain name MTCidentifier.example.com (FQDN)	- Potentially backward compatible if a subspace of the MTC URI scheme is used to 'map' E.164 numbers (MSISDNs) e.g. on a dedicated DNS 'root' e.g. MTC-root.net) - Virtually unlimited space	- Format to be clarified - Resolution infrastructure is necessary (DNS) - Dynamic DNS updates for MTC devices are not trivial - Impacts billing systems
Network Access Identifier (NAI), e.g. MTCid@example.com	- Widely used in packet domain that uses RADIUS or DIAMETER (e.g., when communicating with external AAA servers) - Virtually unlimited address space - Potentially backward compatible if a subspace of the MTC NAI scheme is used to 'map' E.164 numbers (MSISDNs) eg <MSISDN>@example.com	- Format to be clarified - Require some system upgrades (e.g. HSS) - Resolution infrastructure may be necessary (DNS) - Dynamic DNS updates for MTC devices are not trivial - Requires IT backend support system upgrade (e.g. billing, provision systems)
***IP address v4**	- Generally supported in packet domain	- Not suitable as public identifier but only as routing identifier -
***IP address v6**	- Virtually unlimited address space	- Not suitable as public identifier but only as routing identifier

* This table does not intend to indicate the IP addresses can be used directly as MTC device identifiers.

* This table does not intend to indicate the IP addresses can be used directly as MTC device identifiers.

Note1: The above solutions are not necessarily exclusive and some of these solutions may share the same underlying identification scheme. For example using the same scheme MTCid@domain is used by both SIP URIs and NAI.

Note 2: The MSISDN can carry the IMSI when the numbering plan indicator has the value of '0110'. In most places, the MSISDN means the E.164 number; however, the 4th and 7th row in the table above discuss the use of 'other numbering plan indicator' in the MSISDN parameter to carry the 'new' MTC identifier.

9.1 MSISDN (E.164) with existing number length

As an addressing mechanism, MSISDNs work very well. They are the current primary means for addressing MTC devices, and will remain so in the near term. The E.164 number scheme is distributed geographically, with each country or region (e.g. North America) controlling how the numbers are allocated within their borders. In many regions, new numbers will become increasingly scarce. The United States has already enacted rather drastic measures to conserve these numbers to enable the supply to last long enough to get an alternative into place.

Current billing systems are typically oriented around MSISDNs, often using them as the primary keys to identify an account. Given the current situation, continuing to use MSISDNs has no impact on existing billings systems. The same is true of network switches.

Dynamic pooling of existing MSISDNs may be used to address MTC devices. This overcomes issues arising from MSISDN scarcity. It also reduces the impact of mass MTC wake-up on the network, from a network protection perspective. Billing is not impacted as the legacy IMSI can be used to identify the device for charging purposes.

The use of ITU-T E.164 International Network country calling codes (e.g. 882 and 883) with existing interpersonal MSISDN ranges can also be used to overcome MSISDN shortage for MTC device addressing.

In some territories new regulation has been enforced which prohibits the use of MSISDNs from existing interpersonal number ranges for MTC services, (e.g. Netherlands).

9.2 MSISDN (E.164) with max length of 15 digits

The looming scarcity of E.164 numbers is the sole reason they are not suitable in the long term. Some regions can extend the size of their MSISDNs which will get them through approximately 2016-2018. For example, North America cannot extend the length of its MSISDNs, but expect that conservation measures will work through the mid-term.

One alternative to the current scheme is to extend the length of the MISISDN to 12 or 15 digits. This alternative is attractive in some regions. In others, such as North America, the entire network and switching scheme is built around a 10-digit MSISDN, and the costs to extend to 12 or more digits likely exceeds $100 billion.

9.3 E.212 Numbers (IMSI)

E.212 numbers (IMSIs) also serve as an effective addressing scheme as they are guaranteed to be unique to each device. However, their primary purpose is for authenticating devices as they connect to the network via the radio link (RAN) and this argues against making them public addresses. Current networks use the IMSI to address messages to the device. One function of the HLR is to translate the publically known MSISDN into a privately known IMSI.

In addition, the IMSI is not generally accessible when the device is connected over the Internet (i.e. not through the GGSN). To use an IMSI as an address in this situation, the domain name services (DNS) of the MNO would have to translate the IMSI into an IP address. This translation could be done by the HLR, and may actually be done in some cases.

Using E.212 numbers may require modifications to existing billing systems.

E.212 numbers are also geographically distributed, but within a region, each service provider is assigned a set of 10-digit IMSIs. Because these 10-digit ranges are not shared like they are for MSISDNs, the pool of available IMSIs is much larger. However, some service providers in some regions are running low on IMSIs and have had to request a second or third range tied to a new service provider code.

9.4 Other Numbering Plan Indicator in MAP

3GPP TS 29.002 defines a set of numbering plan identifiers, including their current assignments. E.164 and E.212 are two of these plans, and each are assigned a code in bits 1-4 of the Mobile Application Part (MAP) defined in the TS. Three of the codes are currently marked as spare, and two others are marked as reserved for numbering plans that are

now obsolete (e.g. X.121 for data numbering and F.69 for Telex numbering). Assigning any one of the spare or obsolete codes for use by M2M numbering would effectively create a very large pool of numbers for MTC devices, which means this alternative meets the large capacity requirement.

Because this alternative makes use of the existing framework, it is compatible with existing schemes. Because M2M numbers would be from a different numbering plan, however, it is likely that issues will arise around billing systems and cross-domain interconnection. Current billing systems that rely on MSISDNs would have to be modified to recognize the fact that some numbers that look like MSISDNs are not. Network switches may also have to be modified. Further it is not possible for a device on one numbering plan to access a device on another as there is no way to specify the target numbering plan in the outbound call. This would effectively make all machine type communications a closed system, and fails to meet inter-domain routing requirements, and may also negatively affect portability and provisioning.

9.5 Generic Uniform Resource Identifier (URI)

Not all MTC applications in Internet environment require SIP stack to communicate with each other. Traditional IP socket type of connectivity will serve MTC just as well. To facilitate human readability in MTC development and deployment, Uniform Resource Identifier (URI) can be used as generic identifier. URI enables interaction between resources over Internet using specific protocols (e.g. HTTP).

Detailed URI format can be found in [3]

9.5.1 SIP Uniform Resource Identifier (URI)

SIP URIs resemble email addresses in format and style. This makes the domain of possible URIs virtually infinite. Further, only the domain part of the URI needs to be an entry in the DNS, reducing the amount of data in the DNS. Only the domain part of the URI needs to be managed by the MNO. It is possible for a large customer to use their own domain, allowing the customer to assign their own addresses. The customer domain may be shared amongst different MIOs, in which case the user part and the domain part together need to be used to find the MNO. Finally, the resemblance between SIP URIs and email addresses makes them usable by humans.

The primary benefit of using SIP URIs is not the URI or their management; it is the use of SIP that provides the most benefit. The 3GPP SIP based IMS standard provides for a number of built in functions, including session management, authentication, push-to-talk, conferencing, instant messaging, and paging. Included in these functions is the necessary infrastructure to support SMS over IP. None of the other alternatives offer these functions.

Because SIP is a standard protocol operating at level 5, applications developed to run at levels 6 and 7 will work on any device and over any network.

SIP URI can also contain MSISDN (e.g. sip:+<MSISDN>@domain.com;user=phone).

9.5.2 TEL Uniform Resource Identifier (URI)

TEL URIs are also identifiers used by the Session Initiation Protocol (SIP). Same as SIP URI, it is created by IETF for the purpose of carrying the telephone number (e.g., caller usually uses a phone number instead of a SIP URI). TEL URI can carry an E.164 number or a private number.

TEL URI can carry an E.164 number in two forms without or with the 'phone-context' (e.g., 'tel:+1-571-434-1234' or 'tel:434-1234;phone-context=+1-571). When carrying an E.164 number, the TEL URI is equivalent to an MSISDN so has dependency to MSISDN. TEL URIs can be translated to URIs then IP addresses by using ENUM.

TEL URI can also carry a private number belonging to a domain indicated in the 'phone-context' (e.g., tel:1234;phone-context=example.com). 3GPP may specify a unique domain name such as 'mtcid.3gppnetwork.org' so that the identifier in 'mtcid' uniquely identifies a specific MTC device served by the 3GPP systems, or another global standards body may specify a unique domain name for MTC device identifiers. In either case, a non-E.164 numbering plan indicator could be associated with this domain name and the private number in the TEL URI can be carried in the MSISDN parameter as described in subclause 9.4.

9.6 Fully Qualified Domain Name (FQDN)

The domain name scheme basically assigns fully qualified domain name (FQDN) to every device and is the current means by which every server on the Internet and most private networks are addressed This is not necessarily an issue as it works very well with the current IP network infrastructure. However, it places a huge burden on the DNS servers. The mapping of every FQDN to an IP address (either v4 or v6) requires an entry in the DNS database. Using FQDNs to address MTC devices would cause an increase of FQDNs There are no capacity issues with using FQDNs.

Using domain names will require modifications to most existing billing systems. As each MTC device will likely continue to have an IMSI, existing networks should not be affected. Authentication may be affected if the device connects to the network over a link that is not on the radio network. This will likely require some intelligence, such as Generic Bootstrap Architecture (GBA) to reside on the MTC device. Provisioning will take on characteristics of server provisioning in a data center as each MTC device will have what amounts to a server profile.

9.7 IPv4 Address

IPv4 addresses are not considered suitable as public identifiers, but only as routing identifiers.

Today, IPv4 addresses are the primary means for routing packets to any device connected to the Internet. IPv4 addresses are used within nearly every internal IP network as well (some network operators have transitioned to IPv6, but most are either in process or not yet starting that process). Every MTC device would need to be assigned a permanent IP address under this scheme. As an address resource, IPv4 addresses are even more scarce than MSISDNs and in some countries, it may not be possible to allocate IPv4 addresses to MTC devices due to the exhaustion of IPv4 address.

IP address conservation measures for years in an effort to continue to use IPv4 addresses. One consequence of these conservation efforts is the prevalent use of dynamic IP address assignment by network operators. This goes for MNOs as well as wired IP network operators. The very existence of network address translators (NATs) is due to these IP conservation efforts.

IPv4 addresses will work as an addressing mechanism for MTC devices, but only in the near term. Their scarcity argues against using them much longer than that. Further, IP addresses as a public address has proven to be less than friendly to human users, as anyone who has maintained an IP routing table can attest.

In addition, the use of IP addresses only works through level four of the OSI network model. Session management and authentication tools at level 5 need to be provided by the network or device operator. Standards exist for these upper levels, but using IP addresses to identify devices does not take advantage of them.

9.8 IPv6 Address

IPv6 addresses are not considered suitable as public identifiers, but only as routing identifiers.

IPv6 addresses offer the huge advantage over IPv4 as not being a scarce resource. It is possible to assign every device currently connected to the Internet and every device expected to be connected in the future (well beyond the 50 billion devices expected in the next 20 years) a permanent IPv6 address. But, in existing 3GPP systems, one of the obstacles to use of an IPv6 address as a routing identifier is the difficulty to allocate permanent IPv6 addresses to MTC devices. When MTC devices are moving, the IPv6 addresses allocated from MNO may be changeable. It may be required to allocate permanent IPv6 address even though MTC devices are moving. In some use cases, MTC devices may not move permanently or may move only within small area, it is possible to allocate permanent IPv6 addresses. Although the basic length of an IPv6 address is longer than that of an IPv4 address and IPv6 addresses are even less friendly than IPv4 addresses, the compression scheme and the usage of DNS may mitigate the disadvantage of IPv6 addresses. Besides, in PS mobile network, for the interworking with the Internet and private managed IP networks, IPv6 addresses may provide the efficient address scheme.

IPv6 addresses also have the same disadvantages of IPv4 when it comes to higher level functionality. Specifically, session management and authentication functionality would have to be provided by either the MNO or the device owner. Failure to use standards at this level will inhibit the interoperability of the device, especially when transferring the device from one network to another.

There may be some use cases where the session management and other functions provided by SIP are not required. In these cases, it is sufficient to use IPv6 addresses to address specific devices. Doing so requires the assignment of

permanent IP addresses, but the large domain of IPv6 makes this practical as well as possible. It does preclude the dynamic assignment of IP addresses, but this may or may not be an issue. It is likely, however, that functionality provided by network operators and/or device owners will not be transferrable to other networks. Further, the software required to provide this additional functionality is likely as not to require more room than the standard SIP stack.

9.9 Network Access Identifier (NAI)

NAI (RFC 4282) has been widely used in packet access networks that use RADIUS or DIAMETER for Authentication, Authorization and Accounting. It usually has a user part and a domain part where the domain part contains a FQDN (e.g., MTCid@example.com).

The NAI scheme has a domain part that may be associated with the serving 3GPP system or with the service provider or could be specific to 3GPP or a global standard, and the user part would contain a device identifier that is unique within the domain indicated by the domain part.

10 Conclusion

This Technical Report (TR) on Study on Alternative to E.164 for Machine type communication identified different alternative solutions that can be used in combination for today or future to meet M2M needs.. Which solution(s) and migration scenario(s) to adapt is dependent on operator policies and/or regulatory requirements. It is possible that solution sets 1, 2 and 3 may co-exist.

Solution Set 1 – No change to existing MSISDN numbering plan

The current solution is to use the numbering formats (defined in E.164) that exist for interpersonal services (e.g. mobile services) also for MTC.

Solution Set 2 – Expansion or minimal change to the current MSISDN numbering plan

One solution for number shortage is to define M2M dedicated ranges that are spare today (and not assigned) with the maximum length permitted by Recommendation E.164 (i.e. 15 digits).

Normally this solution does not need any change in the standards , but it requires a revision of the different national numbering plans and can impact on existing network relying on closed numbering plans..

Other solutions based on existing MSISDN ranges, such as dynamic pooling of MSISDNs, or the use of E.164 International Network country calling codes in conjunction with existing interpersonal MSISDNs, can also be used to offset E.164 number shortage.

An alternative solution for number shortage is to use a different Numbering Plan Indicator as already supported by MAP. This will require little or no change to the standards but is a change of use so it may affect equipment in the field. This will also require either changes to the current management policies both within operators and between them or the creation of a new MTC specific numbering plan.

Solution Set 3 – New Identifiers

Another solution is to use PS mobile IP network for MTC. The requirement becomes how to identify a specific device in a PSmobile network The identifier used in mobile IP network and in current Internet is in the form of URI that is than mapped into IP address to perform the effective routing of the communication. URIs, NAIs and FQDNs are IP-friendly device identifiers that can be used for the MTC devices.

SIP URIs are identifiers used by the Session Initiation Protocol (SIP) created by the IETF. There is no theoretical limit to the number of SIP URIs that can be created. This solution requires an IP capable mobile network.

TEL URIs are regularly used in the IMS networks but introduce a dependency between the URI and the MSISDN. Using a TEL URI would therefore suffer from the same limitations as continued use of MSISDN.

The use of generic URI, SIP URI and TEL URI as MTC identifier may require update of 3GPP specifications and may need an upgrade of mobile operators" PS networks.

The NAI, FQDN and some non-SIP URIs can be used for devices that only receive mobile-terminated communications from their MTC servers. Those identifiers can be mapped to their associated IMSI.

11 Potential requirements for alternatives to E.164 for machine-type communications

The following are potential requirements identified in this Technical Report for which normative requirements may be added to normative Technical Specifications.

Mid Term

- Support PS Only subscriptions without an assigned MSISDN (already a requirement in TS 22.368)
- Support new SMSC interface which uses an alternate ID field from MSISDN

Longer Term

- Efficiently support MT IP messages (such that SMS is not required)

Annex A:
Additional Definitions (Informative)

Addressing: Addressing is a means for a sender of a message or a call to identify the recipient. The message or call is handed over to a network which then makes use of identification and routing mechanisms in order to deliver the message or terminate a call. Addressing and Numbering are often used interchangeably, but they are not exactly the same thing. Numbering is a subset of addressing. A SIP URI is an address, but it is also potentially an identifier. A device needs not be aware of an address assigned to it by the network (a SIP URI is just an address in this case).

Identifier: An identifier is a tag or label assigned by a network to a particular device to allow the device to communicate with a network or for a network to identify a specific device. GSM devices are assigned a number of identifiers, including the IMSI. A SIP URI could be used as an identifier, especially if the device knows it and it is used as part of the network authentication process.

Numbering: Numbering is a specific form of addressing that uses E.164 or E.164-like number sequences to address a message for or a call to a recipient. The number assigned to a device is used only by senders trying to reach the device, but is often confused as an identifier for the device itself. In reality, the device may have no knowledge of the number or numbers assigned by the network to address messages destined for the device.

Routing: Routing is information that is used to reach the device in the network. The structure of an IP address very clearly demonstrates this, as do the country code, area code, and prefix information in an E.164 phone number. Each portion of the address or number helps the network identify hierarchical components that progressively narrow down to reach a single device.

Annex B:
Change history

Change history											
TSG SA#	**SA Doc.**	**SA1 Doc**	**Spec**	**CR**	**Rev**	**Rel**	**Cat**	**Subject/Comment**	**Old**	**New**	**WI**
SP-56	SP-120292	S1-121385	22.988	0001	2	Rel-12	F	Additions to MSISDN and IMSI sections	12.0.0	12.1.0	FS_AMTC
SP-56	SP-120292	S1-121208	22.988	0002	-	Rel-12	F	Update of requirement section	12.0.0	12.1.0	FS_AMTC
SP-57	SP-120535	S1-122007	22.988	0003	1	Rel-12	F	Add NAI analysis	12.1.0	12.2.0	FS_AMTC
SP-57	SP-120535	S1-122008	22.988	0004	1	Rel-12	F	Correct and add additional analysis on tel URI	12.1.0	12.2.0	FS_AMTC
SP-57	SP-120535	S1-122009	22.988	0005	-	Rel-12	F	Correct error in SIP URI example	12.1.0	12.2.0	FS_AMTC
2015-12								Updated to Rel-13 by MCC	12.2.0	13.0.0	

History

Document history		
V13.0.0	January 2016	Publication