3GPP TR 22.868 V8.0.0 (2007-03)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Facilitating Machine to Machine Communication in 3GPP Systems; (Release 8)

The present document has been developed within the 3rd Generation Partnership Project (3GPP ™) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and reports for implementation of the 3GPP ™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords
<keyword[, keyword]>

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Copyright Notification

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

© 2007, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TTA, TTC).
All rights reserved.

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.

1 Scope

The present document identifies potential requirements to facilitate improvements in M2M communication and the more efficient use of radio and network resources.

Special consideration is given to the following areas for optimisation:

- Charging mechanisms
- Addressing
- Types of communication
- Fixed location, low mobility and low activity terminals
- Handling of large numbers of subscriptions and subscriber data within the network
- Handling issues of large number of M2M subscriptions for the user of M2M services
- Impact of optimisations for security resulting from improvement for M2M

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 TS 23.008: "Numbering, addressing and identification, stage 1"

[2] ITU-T Recommendation E.164: "The international public telecommunication numbering plan"

[3] 3GPP TS 22.259: "Service Requirements for Personal Network Management (PNM), stage 1"

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

H2H Human to Human (Communication) the type of communication 3G networks are currently designed and optimised for.

M2M User Legal entity, i.e. company or person that uses M2M terminals, usually the contractual partner for the operator

M2M Terminal A UE specifically adapted to the requirements of M2M

3.2 Abbreviations

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

M2M Machine to Machine (Communication)

4 General

4.1 Overview

It appears that there is market potential for M2M beyond the current "premium M2M market segment" i.e. the market segments that are currently using M2M.

In particular it is possible to identify potential applications for mass M2M service, e.g. consumer products manufacturers could keep in touch with their products after they are shipped – car manufacturers could serve as an example for that.

Another example is in the home environment where remote maintenance of heating and air condition, alarm systems and other applications can also be identified.

In addition to identified applications, it can be expected that if there was an easy to use M2M service offering other applications for M2M would be forthcoming.

At present structures that have been optimally designed for H2H may be suboptimal for M2M and therefore structures designed for M2M need to be investigated.

4.2 Definition of M2M within the context of this study

Machine to Machine (M2M) Communication is seen as a form of data communication between entities that do not necessarily need human interaction. It is different to current communication models as it involves:

- new or different market scenarios
- lower costs and effort
- a potentially very large number of communicating terminals with
- to a large extent little traffic per terminal

This new type of M2M communication may in future become more relevant as

- M2M in GSM/UMTS is a future growth sector in particular in mature markets, and the ubiquitous coverage of mobile networks is one main enabler
- Potential enhancements of 3GPP standards may be a stimulator; as such business could be addressed more cost efficiently.

4.3 Goals of this study

The study shall investigate on the improvements how standards can be enhanced to provide network operators with lower operational costs when offering M2M services.

It shall lower the M2M users' effort associated with handling large M2M groups.

The study shall look at the trade-off between the effort and the benefits associated with the improvements

4.4 Use Cases

M2M bears enormous application diversity, hence it is difficult to devise comprehensive use cases. Areas in which M2M right now is used:

Security	Alarm systems Backup for landline Access control Car/driver security
Tracking & Tracing	Fleet Management Order Management Pay as you drive Asset Tracking Navigation Traffic information Road tolling Traffic optimisation/steering
Payment	Point of sales Vending machines Loyalty concepts Gaming machines
Health	Monitoring vital signs Supporting the aged or handicapped Web Access Telemedicine points Remote diagnostics
Remote Maintenance/Control	PLCs Sensors Lighting Pumps Valves Elevator control Vending machine control Vehicle diagnostics
Metering	Power Gas Water Heating Grid control Industrial metering

In the following a few already existing use cases covering the most important user requirements and the areas of improvement are outlined.

Use Case 1: Pay as you drive (PAYD)

This use case already exists in Italy and also the UK. The idea is not to charge the car driver a fixed premium for the car insurances but to base the premium on the usage of the car instead. For this reason the car is equipped with a M2M terminal, a GPS device and various other sensors that transmit the data to the insurance company. The terminal including the UICC is mounted on the car at a location where tampering with is difficult for the purpose to avoid theft of the UICC or deactivation of the terminal for fraud purposes. For the same reason the insurance company holds the contract with the network operator.

Use Case 2: Tracking and Tracing

This scenario is already well known in the area of car rental companies where at least the top class cars are equipped with tracking devices to obtain the car's position e.g. in case of theft. Another use case already in place is tagging very expensive tools and equipment e.g. containers or tools in the building industry or oil industry.

It has to be noted that this is currently applied only to expensive goods where the relation of costs associated with tagging and the handling overhead for the user compared to the value of the product justify this business case for the equipment owner. A user of this type of M2M is facing two major problems, the first problem being the tamper/theft proof terminal including the UICC. Currently this done by constructive measures e.g. by locking the entire M2M module and in some cases even mounting at difficult to reach places. As a matter of fact this makes the whole M2M

application very difficult to handle and thus expensive for the M2M user. The second problem comes from the need of the M2M users to have, depending on the lifetime of their products, a reliable, long term functional and viable M2M application. One aspect of this is the possibility for the M2M user to change the subscription for whatever reason. This is practically impossible with the current solution, esp. when there are substantial numbers of M2M terminals out in the field. This is why there are only few real applications where the products always, frequently, return to the company where, besides others, also maintenance of the M2M equipment - such as checking whether the M2M has been tampered with or swapping UICCs - can be done.

All M2M applications where the product does not return frequently or never cannot be covered if the above mentioned problems are not resolved, thus leaving a large percentage of the market uncovered.

Use Case 3: Metering

A Metering device is usually untouched after installation for at least the next 8 years. Again, the UICC needs to be protected against theft and removal for the purpose cutting the connection to the utility e.g. for fraudulent purposes.

Changing the utility (and probably the operator) causes unprecedented obstacles. This use case requires no mobility as it is being mounted somewhere but requires high flexibility in allocating the M2M terminal in case of utility change and/or mobile network operator change. The most complex case is that the utility customer changes his utility eg from one power supplier to another. This power supplier, however, happens to have a contract with a network operator different than the customer's initial supplier. To resolve that either complex accounting mechanisms need to be put in place or the utility needs to send out a service person. Both ways are very costly and also prone to misallocations.

5 Study Areas

5.1 Types of Communication

There are several different communication models under which M2M will take place, each with different relevance and importance for the M2M market.

In the first step M2M can be restricted to a "many M2M terminals to one server" communication model (N to 1) which is the mode of operation in nearly all M2M applications running already today. A number of terminals communicating with the same server are considered a group, and a M2M user can run many of these groups. The N to 1 communication model can be further restricted in that way that the group of M2M terminals belonging to one M2M user can communicate with one destination server only whose address is supplied by the network. This would greatly reduce the effects of misuse of stolen M2M terminals which are usually unattended to a very large extent. In other words, the network decides on the destination address the M2M data is being sent to.

For the first step, it is also considered sufficient that M2M communication is initiated by the M2M terminals only as most of the M2M scenarios run well with a pull type of communication.

When the market evolves and the need for other types of communications such as M2M terminal to M2M terminal emerges it shall be possible to introduce this later on.

It is understood that current M2M scenarios are mostly based on SMS. This, however, was driven by historical constraints, at that time when the first M2M applications were set up, nothing else, besides CS data was available.

When considering the communication requirements for various types and classes of machine it becomes obvious that no single Teleservice or Bearer Service will satisfy all their individual needs up to now. Also there are multi-function machines that may need to communicate with different servers/terminals, at different data rates, for different tasks. For example, a network of 'printer/fax/scanner' machines might communicate externally via a master machine/server with a gateway terminal (containing a SIM/USIM/ISIM). Existing master 2G/3G capable terminals might request a CS bearer to send a fax, SMS to report a fault, or GPRS/HSUPA to transfer a large graphics file to a manufacturer.

GPRS and UMTS PS should be the preferred way for transferring data as this would simplify terminals and networks (No CS impacts), and thus reduce costs.

This also facilitates simple writing of M2M applications by the M2M users without having to deal with specialised and proprietary SMS interworking, by simply providing e.g. an IP protocol stack. This will open up new market segments as M2M application can use an IP packet service.

Communication scenarios:

It is assumed that two kinds of machines are deployed within this scenario:

- Wireless modulesM2M terminals, connected via a RAN, included in the "machines in the field (e.g. vending machines)" and

- Central servers, located behind the GGSN. These servers may be located as follows:

  - within the operator (MNO) domain, giving the possibility for tight coupling to servers within MNO domain.

  - connected externally similar to a PDN connection (Packed Data Network as in GPRS standardisation), i.e. with a dedicated connection from GGSN (APN) to the server(s) of the machine operator and thus also routing and access control possibility at GGSN.

  - within general Internet, accessible via PDN (and ISP), i.e. without dedicated connection to the server(s) of the machine operator, but transport over the public Internet.

Scenario 1: Many wireless modules communicating with one central server

This scenario applies when one machine operator has many machines at various locations and wants to communicate with these machines in an intermittent way. One Wireless module communicates with one server only. The machines shall be distinguishable from each other, i.e. outgoing messages (as seen by the central server) are not "broadcast", and incoming messages are bound to the particular machine the message was sent from.

Scenario 2: Many wireless modules communicating with many servers

A machine operator may deploy many servers for local diversity or load distribution. This is an extension of scenario 1. The MNO may provide access control to separate the different machine operators' realms.

Scenario 3: Many wireless modules communicating with each other

This scenario is not seen within the scope of 3GPP's work on M2M as the relevant applications only seem to involve module-to-server communication. (FFS)

Further study should determine the relevant communication scenarios. It may be beneficial to limit the scope of M2M communication for the sake of reduced complexity and increased security, but, on the other hand, care should be taken not to exclude relevant scenarios.

5.2 Handling large numbers of terminals

5.2.1 Considerations on handling large numbers of terminals for the Network Operator

Subscription and subscriber management seem to contribute to the inability to provide attractive offerings. For example, requiring the operator to deal with each and every M2M terminal individually - instead of handling the M2M user owning "N" terminals in one step - is considered at least suboptimal. Also, M2M terminals may remain stationary in many applications, thereby reducing the network load and possibly allowing optimisations.

In order to save network signalling overhead for mobiles that are non-stationary and need not to be reachable i.e. use mobile originated traffic only the suppression of location update traffic should be studied.

Furthermore mobility could be de-activated for certain kinds of terminals e.g. mobiles that are stationary.

5.2.2 Considerations on handling large numbers of terminals for the M2M User

The following user requirements can be deduced from the use cases:

- Tamper Save/Theft proof terminal including a UICC

- Possibility to change subscription out in the field e.g. after contract expiry without human intervention
- Possibility to allocate the terminals at initial power up to a network operator without human intervention

5.2.3 Subscription Handling

One of the perceived obstacles to M2M market growth is the difficulty for the M2M operator to change the subscription. Currently, such a change would involve physical maintenance work on all machines in the field, which is seen prohibitive. Therefore, alternatives to realise a dynamic provisioning of USIM/ISIM parameters to a large number of M2M terminals within a short timeframe should be investigated (e.g. UICC OTA update of the MNO data, and transfer of the access right between MNOs). Depending on the business cases deployed in future, the machine operator may have the advantage that he can more easily change the MNO. This may be seen as a disadvantage for the MNO, but on the other hand the MNO may also have the benefit that new customers may switch more easily to his service. In general it is expected that the market for M2M communication may grow faster if the machine operators have more chances to select their favourite operator knowing that they are not tied to this operator forever.

5.2.4 Machine Network Management (MNM)

Many of the ideas being developed for Personal Network Management (PNM) (TS 22.259 [3]) and Network Composition (NC) might also be applied to machine network management (MNM) communications. Like humans, machines may also need to communicate in different ways at different times, between themselves and with remote peers. Standardising MNM procedures, and aligning them with PNM, NC and similar specifications, could lead to improve efficiency through optimised communication and better bearer/bandwidth usage, especially for networked machines belonging to a single or partner entity. In addition to industrial and office machines, example networks would include CCTV surveillance cameras, vending machines, gaming and internet access terminals in a shopping mall, or on a train, or perhaps a home network comprising phones, PCs, PDAs, TV set-top box, alarms, domestic appliances, etc.

Depending on the communication task, machines might communicate, via non 3GPP access technology, to the master machine (containing a SIM/USIM/ISIM) or obtain authorisation from the master machine to communicate directly e.g. using the 3G or fixed NGN network, with an external entity.

Benefits include:

- Reduced number of subscriptions
- Reduced number of network authentication
- Subscription independent machine replacement/upgrades
- Easier subscription upgrade and portability
- Communication task prioritisation
- Data aggregation and multiplexing e.g. over HSDPA/HSUPA
- Better QoS e.g. optimum location of master machine/terminal
- Continuation of high-speed data link to sub-optimal locations using M2M single or multi-hop Bluetooth/WiFi /cable
- Efficient network management
- Ad-hoc and potentially self repairing network
- Optimised routing
- Consolidated charging and billing

Drawbacks include:

- Non-3GPP entities having access to the 3GPP network
- A potentially reduced security of the 3GPP network if the security level of the slave-master machine communication is lower than the usual 3GPP security.

5.3 Considerations on Charging

The communication behaviour of large numbers of terminals also aggravates the efforts for charging in the network. When the traffic volume may vary by several orders of magnitude, e.g. ranging from few bytes once a year to a few kilobytes every minute the traditional charging record generation effectively stops the widespread use of M2M. Especially charging, as it is designed today, in creating detailed charging records, causes unnecessary overhead in creating at least 10 - 100 times longer CDRs than the payload for every few bytes transaction.

Charging record generation as it is done today was designed for the highly regulated H2H market. It should not be applied for M2M. It is considered sufficient to apply per group counters counting the traffic to and from the servers at the network boundary. Detailed tracking of traffic behaviour per terminal should be handled at the M2M user's server(s) if required.

What is additionally required is to take care of M2M terminals usually tied to one location. To enable the operator to provide suitable service offerings for these types of terminals some per group counter should be established counting mobility related network load, i.e. counting the location update traffic. It has to be noted that location update traffic caused by restructuring of the network needs to be taken into account by the network operator.

5.3.1 Use of Machine Class Subscription Identifiers

In order to differentiate machine to machine communications for optimised mobility management, call routing, security and charging purposes, consideration should be given to the use of machine type subscription identifiers. It is envisaged that several types of M2M communication subscriptions/tariffs could be offered by network operators, based perhaps on different classes of machine e.g. always on high security alarm systems and surveillance camera networks, single point of sale card readers, fixed location machines. The subscription information, including the machine class/ terminal type identifier would be distributed to the responsible network elements handling the M2M communication.

5.3.2 Fixed Location, low mobility and low activity terminals

Many alarm systems and other fixed geographic location terminals generate very low volumes of chargeable traffic . To be able to offer attractive tariffs in these business sectors, there is a need to reduce or eliminate completely some of these signalling overheads. Even in the case of fixed location machines that generate large volumes of chargeable traffic, it is still desirable to minimise signalling due, in particular, to unnecessary periodic location updates. For static terminals, depending on terminal type, it should be possible to selectively extend the periodic time to 255 (deci-hours), or to instruct individual terminals not to make periodic location updates. Alternatively, to make use of off peak traffic periods, low activity terminals might be instructed to perform a location update at some future date and time e.g. 1st February at 02:45:30, rather than at set periodic intervals.

Terminals intended for M2M communications should not need to support unnecessary functionality and should be provisioned accordingly. This might include a dedicated M2M APN but not any unnecessary services like voice mail or customer care messages that cannot be used by the machine or a maintenance engineer.

Ideally, for any given terminal type, it should be possible to optimise mobility management, re-authentication, subscription maintenance and other operational costs. There are several ways that this might be done but in most cases there is a need to differentiate between mobile UEs, fixed location and low activity terminals. By identifying the subscription and terminal type, e.g. machine to machine subscription, low activity, fixed geographic location terminal, in the subscriber information held in the HLR/HSS, and distributed to the MSC-VLR and SGSN, mobility management and other costs may be reduced.

In addition to reducing the signalling overhead and operational costs, minimising MM and GMM signalling also helps to reduce cell congestion.

Further consideration should also be given to the purging of low usage terminals subscription information from the VLR/SGSN, especially for MO only terminals e.g. domestic alarms. In this case the HLR/HSS would be expected to retain a record of the last reported location and timestamp, received from the VLR/SGSN, when the temporary subscriber information was purged.

5.4 Considerations on Security

5.4.1 Denial of Service

The expected large number of terminals and the automated nature of traffic seem to be more prone to Denial of Service Attacks (DoS). These attacks can be either caused deliberately or by bad M2M application design.

A DoS attack is always possible in mobile networks, irrespective of the kind of service offered. The easiest way would be jamming of the radio interface, but more sophisticated attacks are also possible, e.g. with an overload of bogus authentication or mobility management messages. Thus the aim of M2M security is not to open additional channels for DoS attacks. The same applies for degradation of service which may be seen as a weaker form of DoS.

As often, attacks depend a lot on particular properties of a system, a detailed discussion of DoS attacks must be done after selection of a particular architecture for M2M.

5.4.2 Adaptation of Level of Security

In order for the overall risk to remain manageable, there needs to be a finely tuned balance between security provisions on the user side and those in the network: it may be possible to adapt security on the user side for M2M communication to a certain extent, but this would then have to be compensated for by access restrictions on the M2M user enforced in the network. Some of these access restrictions could be realised by dynamically configurable packet filters.

It may be considered whether additional security measure at the application layer may allow to somewhat adapt security at the link or network layer. However, it is questionable whether a requirement on the M2M operator to introduce and manage additional security at the application layer would lead to the cost saving required for a M2M mass market. A re-use and enhancement, where necessary, of the widespread GERAN/UTRAN technology also for security for M2M communication seems the more promising approach.

5.4.3 Security for unattended M2M devices

In contrast to the traditional ME, which is carefully held and protected by a person, the M2M terminals will be placed in more or less accessible locations, and may be tampered with by unauthorised persons. Furthermore, theft or fraudulent modification of an M2M terminal may not be detected and reported as quickly as this is the case for personally owned and held ME. Fraud targets could both be the M2M user (e.g.: fraudster suppresses payment messages) or the PLMN operator (fraudster uses M2M device or its UICC for theft of service). Therefore, requirements for device-based security measures need to be studied. The related work 3GPP TR 33.905 "Recommendations for Trusted Open Platforms" may be relevant for M2M.

One major challenge is to secure the UICC in such a way that it is not trivial to tamper with or steal. On the other hand making the UICC completely theft proof challenges the flexibility for the M2M administrator/end-user to change subscription if that is desired. To get this contradictory issue solved might be a key factor to open up e.g. Telematics business for mobile industry players.

Furthermore, the M2M ME and the system attached to it (or surrounding it, e.g. a vending machine) often represent a single functional entity. Therefore, the interface between the M2M ME and its surroundings are security-relevant. It must be decided whether this interface is in scope or out of scope of 3GPP standardisation. Regardless of the decision, interface security must be addressed to fulfill the M2M user's security requirements

5.5 Considerations on Addressing

5.5.1 Addressing in the CS and PS domain

There are several possibilities which kind of connectivity is needed for M2M terminals – originating, terminating, CS, PS (GPRS), IMS etc. This requires different identities.

- IMSI: Required to access a 3GPP network, provides the possibility to perform a CS or GPRS attach and such to send short messages.

- IMSI + MSISDN: provides the possibility to originate and terminate CS calls as well as to receive short messages.
- IMSI + IP address: provides IP connectivity after PDP Context Activation
- IMSI + IMPI + IMPU: provides possibility to originate and terminate IP multimedia sessions via the IMS.

5.5.2 Addressing based on IMSIs

IMSI based addressing provides only limited connectivity in the current systems but could serve as first step to remotely activate a UE, i.e. to initiate a PDP context activation on network request.

According to TS 23.003[1] the maximum length of a IMSI is 15 digits, consisting of the Mobile Country Code (MCC) with 2 digits, the Mobile Network Code (MNC) with 2 to 3 digits and the Mobile Subscriber Identification Number (MSIN) with up to 10 or 9 digits respectively. In theory this would provide the possibility for addressing up to 10 billion different terminals within one mobile network.

However in practice this may collide with existing IMSIs of the operators. So it seems likely to be necessary for operators to apply a separate MNC for M2M communication which enables the use of nearly all possible numbers.

5.5.3 Addressing based on MSISDNs

According to TS 23.003 [1] and the ITU-T Recommendation E.164 [2] the maximum length of a MSISDN is 15 digits, consisting of the Country Code (CC), National Destination Code (NDC) and Subscriber Number (SN). Although the length of the CC and NDC may differ in various countries the majority of the SNs is around 10 digits long. Again, this would provide the possibility for addressing up to 10 billion different terminals.

Due to existing numbering plans the real number is much more limited. A possible way to use nearly the full possible range is to apply a separate NDC for M2M communication.

On protocol level within mobile networks even longer MSISDNs – up to 20 digits in national or international format - are supported.

5.5.4 Addressing based on IP address or IMPU

After establishment of IP connectivity the use of private or public IPv4 or IPv6 addresses is possible, the registration to the IMS enables addressing via SIP URIs or tel URIs. This provides a nearly unlimited number of addresses.

5.5.5 Conclusions concerning addressing

The limiting factor in addressing is the IMSI: Dependent on the length of the MNC only 9 or 10 digits are available for use within one network identified by one MNC. Furthermore it is the pre-requisite to access the 3GPP system via the CS or PS system. The use of additional MNCs may be restricted by regulatory authorities.

For this reason alternative addressing solutions based on IP addresses should be studied.

Depending on the assumptions made in the section on charging (ie. to base charging on per group counters) the need to individually identify a M2M terminal seems not to be given from the network's point of view. It is assumed that the M2M user, in any case, will have some identification of M2M terminals on application layer. Hence, it should be studied whether authenticating the terminal by just identifying the group it belongs to brings any benefit in facilitating M2M. But it should be studied whether problems may arise when a terminal does not have a unique identity in GPRS: on the one hand, the current mobility management procedures may need to be updated (which may be a serious impact, ffs), on the other hand, it may be desirable to be able to identify a rogue or misbehaving terminal and take it out of service, rather than disabling the entire group. But then it may be possible to use a unique identity of a terminal in GPRS and use a group identity only for charging purposes, i.e. CDRs would be generated only for the group.

For example, many machines could communicate via a master machine/terminal containing a SIM/USIM. As with Personal Network Management (PNM), Machine Network Management (MNM) this would allow a single subscription (MSISDN/Public Address) to serve many devices with Private Addresses. The benefits of such a system are described in section 5.1.2.

Backwards compatible extension of the IMSI address range might also be considered. Special MNC/MCC/MSIN, which are transparent to legacy systems, could trigger a further validation check of the M2M address part of the IMSI.

6 Possible Requirements

Based on the use cases in clause 4 and considerations in clause 5 following possible requirements can be identified:

- De-activation of mobility signalling for stationary terminals
- Optimised mobility signalling for low mobility and low activity terminals
- Possibility to instruct individual/group of terminal types e.g. static, low mobility, low activity terminals, not to perform any periodic location updates, and optionally location updates due to movement between LA/RAs.
- Possibility to instruct individual/groups of terminal types to perform a location update at a specific date and time
- Purging of subscriber data from VLR/SGSN for low activity / MO only terminals
- Tamper Save/Theft proof terminal including a UICC
- Possibility to change subscription out in the field e.g. after contract expiry without human intervention
- Possibility to allocate the terminals at initial power up to a network operator without human intervention
- Re-use of PNM mechanisms for M2M communication
- Possibility to define groups and to have group counters to count the traffic to and from the servers at the network boundary
- Per group counters to count location update traffic
- Add a terminal type identifier to the subscription information to facilitate mobility management and charging
- Overcoming the limitations of the IMSI range by alternative addressing solutions
- To simplify terminals and networks and thus reduce costs the CS should not be impacted and preferably PS should be used.

Annex A:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
24.10.05	SA1#30	S1-05973			Input proposal	0.0.0	0.1.0
28.10.05	SA1#30	S1-051147			Implementing comments received at SA1#30	0.1.0	0.2.0
15.02.06	SA1#31	S1-060277			Implementing comments received at SA1#31	0.2.0	0.3.0
29.06.06	SA1#33	S1-060923			Implementing comments received at SA1#33	0.3.0	0.4.0
11.09.06	SA1-AH	S1-061077			Implementing comments received at SA1#34 Ad-Hocs Based on the 1.0.0 version that will go to SA#33 for information	1.0.0	1.1.0
23.10.06	SA1#34	S1-061313			Implementing comments received at SA1#34	1.1.0	1.2.0
31.01.07	SA1#35	S1-070252			Implementing comments received at SA1#35	1.2.0	1.3.0
31.01.07	SA1#35	S1-070292			Raised to version 2.0.0 for approval at SA #35	1.3.0	2.0.0
31.01.07	SA1#35	S1-070298			Raised to version 2.0.1 for approval at SA #35 and to correct editorials.	2.0.0	2.0.1