ETSI TS 102 689 V1.2.1 (2013-06)

Machine-to-Machine communications (M2M);
M2M service requirements

Reference
RTS/M2M-00001ed121

Keywords
M2M, requirements, service

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

Contents

Intellectual Property Rights

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Machine-to-Machine communications (M2M).

Introduction

Machine-to-Machine (M2M) communications is the communication between two or more entities that do not necessarily need any direct human intervention. M2M services intend to automate decision and communication processes.

The M2M service requirements detailed in the present document enable consistent, cost-effective, communication for wide-range ubiquitous applications. Examples of such applications include: fleet management, smart metering, home automation, e-health, etc.

The present document, together with the architecture specification, TS 102 690 [i.1], forms the basis for the M2M communications detailed technical specifications.

The present document specifies general and functional requirements for M2M communication services.

1 Scope

The present document specifies the M2M service requirements aiming at an efficient end-to-end delivery of M2M services.

It contains the following clauses:

- **General requirements** - describes communications features necessary for the correct establishment of M2M communications.
- **Management** - specifies requirements related to the management modes (malfunction detection, configuration, accounting, etc.).
- **Functional requirements for M2M services** - describes functionalities-related requirements for M2M (data collection & reporting, remote control operations, etc.).
- **Security** - covers the requirements for M2M device authentication, data integrity, privacy, etc.
- **Naming, numbering and addressing** - provides the requirements relating to naming, numbering and addressing schemes specific to M2M.

The M2M requirements in the present document are influenced by the following use cases:

- Smart meter use cases as described in TR 102 691 [i.2].
- eHealth use cases as described in TR 102 732 [i.3].
- Track and Trace use cases as described in annex B.
- Monitoring use cases as described in annex B.
- Transaction use cases as described in annex B.
- Control use cases as described in annex B.
- Home Automation use cases as described in annex B.
- City automation use cases as described in TR 102 897 [i.4].
- Connected consumer used cases as described in TR 102 875 [i.5].
- Automotive use cases as described in TR 102 898 [i.6].
- Smart Grid use cases as described in TR 102 935 [i.10].

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 102 690: "Machine-to-Machine communications (M2M); Functional architecture".

[i.2] ETSI TR 102 691: "Machine-to-Machine communications (M2M); Smart Metering Use Cases".

[i.3] ETSI TR 102 732: "Machine to Machine Communications (M2M); Use cases of M2M applications for eHealth".

[i.4] ETSI TR 102 897: "Machine to Machine Communications (M2M); Use cases of M2M applications for City Automation".

[i.5] ETSI TR 102 875: "Access, Terminals, Transmission and Multiplexing (ATTM); Study of European requirements for Virtual Noise for ADSL2, ADSL2plus and VDSL2".

[i.6] ETSI TR 102 898: "Machine to Machine Communications (M2M); Use cases of Automotive Applications in M2M capable networks".

[i.7] ISO 16750: "Road vehicles -- Environmental conditions and testing for electrical and electronic equipment".

[i.8] ETSI TS 102 412: "Smart Cards; Smart Card Platform Requirements Stage 1 (Release 8)".

[i.9] ETSI TR 102 725: "Machine to Machine Communications (M2M) Definitions".

[i.10] ETSI TR 102 935: "Machine-to-Machine communications (M2M); Applicability of M2M architecture to Smart Grid Networks; Impact of Smart Grids on M2M platform".

3 Abbreviations

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

AEC	Automotive Electronics Council
CO	Connected Object
CPE	Customer Premises Equipment
CPU	Central Processing Unit
EPOS	Electronic Point of Sale
FW	Firmware
HLR	Home Location Register
HLSA	High-Level M2M System architecture
HSS	Home Subscriber Server
HW	Hardware
IMSI	International Mobile Subscriber Identity
ITS	Intelligent Transport System
M2M	Machine-to-Machine (communication)
MNO	Mobile Network Operator
MS	Mobile System
MVNO	Mobile Virtual Network Operator
NAT	Network Address Translator
NFC	Near Field Communication
OAM	Over-The-Air Management
PLC	Power Line Communication

QoS	Quality of Service
RFID	Radio Frequency IDentification
SLA	Service Level Agreement
SW	Software
TrE	Trusted Environment
UICC	Universal Integrated Circuit Card
USSD	Unstructured Supplementary Service Data
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WSN	Wireless Sensor Networks

4 General requirements

General requirements specified below are for the M2M System in general, meaning that not all particular M2M systems or components of these systems need to implement every requirement.

4.1 M2M Application communication principles

The M2M System shall be able to allow communication between M2M Applications in the Network Domain, and the M2M Device Domain, by using multiple communication meansbased on IP Access.

Also a Connected Object may be able to communicate in a peer-to-peer manner with any other Connected Object.

The M2M System should abstract the underlying network structure including any network addressing mechanism used, e.g. in case of an IP based network the session establishment shall be possible when IP static or dynamic addressing are used.

NOTE: Abstraction (e.g. operational environment and topology) of the network can reduce the effort in application development for varying scenarios.

4.2 Message Delivery for sleeping devices

The M2M System shall be able to manage communication towards a sleeping device.

4.3 VOID

4.4 Message transmission scheduling

The M2M System shall be able to manage the scheduling of network access and of messaging.

The M2M System shall be aware of the scheduling delay tolerance of the M2M Application.

4.5 Message communication path selection

Assuming multiple paths are available, the M2M System shall be able to select communication paths, based on e.g. policies or rely on routing mechanisms in case of transmission failures.

4.6 Communication with devices behind a M2M gateway

The M2M System should be able to communicate with Devices behind a M2M gateway.

4.7 Communication failure notification

M2M Applications, requesting reliable delivery of a message, shall be notified of any failures to deliver the message.

4.8 Scalability

The M2M System shall be scalable in terms of number of Connected Objects.

4.9 Abstraction of technologies heterogeneity

The M2M Gateway may be capable of interfacing to various M2M Area Network technologies.

4.10 M2M Service Capabilities discovery and registration

The M2M System shall support mechanisms to allow M2M Applications to discover M2M Service Capabilities offered to them.

Additionally the M2M Device and M2M Gateway shall support mechanisms to allow the registration of its M2M Service Capabilities to the M2M system.

4.11 M2M Trusted Application

The M2M Core may handle service request responses for trusted M2M Applications by allowing streamlined authentication procedures for these applications.

The M2M system may support trusted applications, that are applications pre-validated by the M2M Core.

4.12 Mobility

If the underlying network supports seamless mobility and roaming, the M2M System shall be able to use such mechanisms.

4.13 Communications integrity

The M2M System shall be able to support mechanisms to assure communications integrity for M2M services.

4.14 Device/Gateway integrity check

The M2M System may support M2M Device and M2M Gateway Integrity Validation [i.9].

4.15 Continuous connectivity

The M2M System shall support continuous connectivity, for M2M applications requesting the same M2M service on a regular and continuous basis. This continuous connectivity may be de-activated upon request of the Application or by an internal mechanism in the M2M Core.

4.16 Confirm

The M2M System may support mechanisms to confirm messages.

The M2M System shall support the delivery of the confirmation in a time that is configurable e.g. 1 s.

4.17 VOID

4.18 Logging

Messaging and transactions requiring non-repudiation shall be capable of being logged. Important events (e.g. received information from the M2M Device or M2M Gateway is faulty, unsuccessful installation attempt from the M2M Device or M2M Gateway, service not operating, etc.) may be logged together with diagnostic information. Logs shall be retrievable upon request.

4.19 VOID

4.20 Time Stamp

The M2M System shall be able to support accurate and secure and trusted time stamping. M2M Devices and M2M Gateways may support accurate and secure and trusted time stamping.

4.21 Device/Gateway failure robustness

After a non-destructive failure, e.g. after a power supply outage, a M2M Device or Gateway should immediately return in a full operating state autonomously, after performing the appropriate initialization e.g. Integrity Validation [i.9] if supported.

4.22 VOID

4.23 Operator telco capabilities exposure

The M2M interface to the external M2M applications shall enable the exposition of telco operator capabilities (e.g. SMS, USSD, localization, subscription configuration, authentication (e.g. Generic Bootstrapping Architecture), etc.). The service platform shall be able to provide access to non-M2M resources abstracted as M2M resources to provide to the applications a consistent use of the M2M capabilities.(e.g. to send an SMS to common cellular phones).

4.24 Location reporting support

The M2M System shall be able to report M2M Device/Gateway location to M2M applications when this information is available. The location information of the M2M device/M2M gateway may be determined by the underlying network procedures (taking into account relevant privacy/security settings for transfer of such information), by application-level information reported from the M2M device/gateway application, or a combination of both.

4.25 Support of multiple M2M Applications

The M2M System shall support a mechanism to manage a multiple M2M Applications and to provide a mechanism to interact between multiple M2M Applications. This mechanism shall support as following:

- Maintenance of the list of registered M2M Applications.
- Maintenance of registration information of M2M Applications.
- Notification of newly registered M2M Applications towards the subscribing M2M Applications authenticated and authorized for the information exchange.

4.26 Support for subscribing to receive notification

The M2M System shall support a mechanism for allowing applications or Connected Objects to subscribe and being notified of changes.

4.27 Support for optimizing notification

The M2M System may support a mechanism for delaying notifying a Connected Objects.

4.28 Support for store and forward

The M2M System may support a mechanism to manage a remote access of information from other Connected Objects. When supported the M2M system shall be able to aggregate requests and delay to perform the request depending on a given delay and/or category.

5 Management

5.1 Fault Management

5.1.1 Proactive monitoring

The M2M System shall be capable of proactively monitoring the M2M system in order to attempt to prevent and correct errors.

5.1.2 Diagnostics mode

The M2M System shall provide the means to allow diagnostics for M2M Application functioning.

5.1.3 Connectivity test

The M2M System shall support testing the connectivity towards a selected set of Connected Objects (COs) at regular intervals provided the COs support the function.

5.1.4 Fault discovery and reporting

The Connected Object (CO) operational status shall be monitorable, provided the CO supports the function.

5.1.5 Fault Recovery by Remote Management

M2M devices may support remote management for fault recovery e.g. firmware update, quarantine device. After this operation of firmware update, the device may reboot to a known and consistent state.

5.1.6 VOID

5.2 Configuration Management

5.2.1 Pre-provisioning and auto configuration of the M2M Devices and Gateways

The M2M Application or Capabilities in the Service Capabilities shall support autoconfiguration, that is without human intervention, of M2M Device or M2M Gateway when these are turned-on. The M2M Device or M2M Gateway may support autoconfiguration and registration to M2M Application functions.

The M2M System shall support mechanisms to perform simple and scalable pre-provisioning of M2M Devices/Gateways. The pre-provisioning mechanism shall be able to work even when the communication path to the M2M Device/Gateway is absent.

5.2.2 M2M Area Network resilience

An M2M Device or M2M Gateway experiencing a fault shall not affect the normal operation of the M2M Area Network.

5.2.3 Time synchronization

The M2M System should support time synchronization. M2M Devices and M2M Gateways may support time synchronization. The level of accuracy and of security for the time synchronization can be system specific.

5.2.4 Configuration Management

The M2M System and M2M Gateways shall support configuration management (i.e. manageability will depend on the end-system).

5.3 VOID

6 Functional requirements for M2M services

6.1 Data collection & reporting

The M2M System shall support the reporting from a specific M2M Device or M2M Gateway or group of M2M Devices or group of M2M Gateways in the way requested by the M2M Application as listed below:

- a periodic reporting with the time period being defined by the M2M application;
- an on-demand reporting with two possible modes. One is an instantaneous collecting and reporting of data, the other one is a reporting of the data that were pre-recorded at the indicated specific time period;
- a scheduled reporting; or
- an event-based reporting.

6.2 Remote control of M2M Devices

The M2M System shall support the capability for an Application to remotely control M2M Devices that support this capability.

6.3 Group mechanisms

The M2M System shall support a mechanism to create and remove groups, and to introduce an entity into a group, modify the invariants (i.e. characteristics) of the members in a group, remove an entity from a group, list members of a group, check for an entity's membership in a group, search entities in a group, and identify all groups where the entity is a member.

6.4 VOID

6.5 M2M Devices/Gateways type varieties

The M2M System shall be able to support a variety of different M2M Devices/Gateways types, e.g. active M2M Devices and sleeping M2M Devices, upgradable M2M Devices/Gateways and not upgradable M2M Devices/Gateways.

The M2M system should support parameter constrained operations where the parameters are controllable resources like CPU, memory size, battery level, etc.

6.6 Information reception

The M2M System shall support the following mechanisms for receiving information from M2M Devices and M2M Gateways:

- Receiving unsolicited information (passive retrieval).
- Receiving scheduled information.
- Operating particular algorithms for retrieving information (e.g. round robin, random within given time window, round robin groups with random reply in given time window).

6.7 Reachability

The M2M System may be aware of the reachability state of the connected objects.

6.8 Asymmetric flows

M2M Devices and Gateways should support asymmetric flows.

6.9 Paths diversity

The M2M System should support physical paths diversity if required by the M2M Application.

6.10 Heterogeneous M2M Area Networks

The M2M System shall be capable of interfacing heterogeneous M2M Area Networks. This may be achieved at the M2M Gateway.

6.11 Information collection & delivery to multiple applications

The M2M System shall support the ability for multiple M2M Applications to interact with the same M2M Devices simultaneously.

6.12 Management of multiple M2M Devices/Gateways

The M2M Application shall be able to interact with one or multiple M2M Devices/Gateways, e.g. for information collection, control, either directly or through using M2M Service Capabilities.

6.13 M2M Devices/Gateways description

M2M characteristics of the M2M Device/Gateway may be either preconfigured in the M2M System or provided by the M2M Device/Gateway to the M2M System; the characteristics provided by the M2M Device/Gateway take precedence over the preconfigured characteristics.

M2M characteristics consist of the static information such M2M capabilities that may be assigned to M2M Devices and Gateways and the dynamic information such as location, state, availability, that may be associated to M2M Devices and Gateways.

6.14 Data store and share

The M2M System shall be able to store data to support the following requirements:

- Provide functionality to store and retrieve data.
- Establish storage policies for stored data (e.g. define maximum byte size of the stored data).
- Enable data sharing of stored data subjected to access control.

7 Security

In this clause we elaborate on the security requirements for the M2M System. We expand on the basic requirements of confidentiality, integrity, authentication, and authorization and provide specific examples of potential threats that the system should be protected against.

7.1 Authentication

The M2M system shall support mutual authentication of the M2M Core and the M2M Device or M2M Gateway, and one-way authentication of the M2M Device or M2M Gateway by the M2M Core. For example mutual authentication may be requested between a service provider and the entity requesting the service. The parties may choose the strength of authentication to ensure appropriate level of security.

7.2 Authentication of M2M service layer capabilities or M2M applications

When there is a request for data access or for M2M Device/Gateway access, the M2M Device or M2M Gateway shall be able to mutually authenticate with the M2M Service Capabilities or M2M Applications from which the access request is received.

7.3 VOID

7.4 Data integrity

The M2M System shall be able to support verification of the integrity of the data exchanged.

7.5 Prevention of abuse of network connection

M2M security solution should prevent unauthorized use of the M2M Device/Gateway.

7.6 Privacy

The M2M System shall be capable of protecting privacy.

7.7 Multiple actors

Multiple actors are involved in the end-to-end M2M service. The M2M System shall allow for such different actors to deliver the service in collaboration, maintaining security of the end-to-end service.

For example, M2M services can involve three different actors contributing to the delivery of the service. The cellular network provider may be separated from the M2M application provider. A third party that may be involved is the M2M operator or mobile virtual network operator (MVNO) that sits between the cellular network operator and the application provider. When an MVNO is involved, it typically plays the role of the network provider as the M2M cellular device's home network is with the MVNO, i.e. MVNO has the HLR/HSS entry for the device.

7.8 Device/Gateway Integrity Validation

The M2M System shall be able to support a mechanism for M2M Device/Gateway Integrity Validation [i.9]. The M2M Device/Gateway may or may not support Integrity Validation. If the M2M Device/Gateway supports Integrity Validation and if the M2M Device/Gateway validation fails, the M2M Device/Dateway shall not be allowed to perform M2M Device/Gateway authentication.

The mechanism for M2M Device/Gateway Integrity Validation may be initiated upon query from the M2M System or may be autonomously started locally by the M2M Device/Gateway at any time.

The M2M System may remotely get the historical log of tamper detection in a M2M Device/Gateway if supported by the M2M Device/Gateway.

7.9 Trusted Environment

M2M Devices/Gateways that require Integrity Validation shall provide a Trusted Environment (TrE) [i.9] for that purpose.

7.10 Security credential and software upgrade at the Application level

Where permitted by the security policy, M2M System shall be able to remotely provide the following features, at the Application level:

- Secure updates of application security software and firmware of the M2M Device/Gateway.
- Secure updates of application security context (security keys and algorithms) of the M2M Device/Gateway.

This functionality should be provided by a tamper-resistant Secured Environment [i.9] (which may be an independent Security Element) in M2M Devices/Gateways supporting this functionality.

8 Naming, numbering and addressing

8.1 Naming

The M2M System should be able to reach the M2M Devices or M2M Gateways using M2M Device Names or M2M Gateway Names respectively.

The M2M System should be flexible in supporting more than one naming scheme.

8.2 Identification

The M2M System should support identification of COs or groups of COs by their names, temporary id, pseudonym (i.e. different names for the same entity), location or combination thereof (e.g. URIs or IMSI).

It shall be possible to reuse names for certain classes of devices or for devices operating in certain (i.e. resource constrained) environments.

8.3 Addressing

The M2M System shall allow flexible addressing schemes, including:

- IP address of CO.
- IP address of group of COs (including multicast address).
- E.164 addresses of CO (e.g. MSISDN).

Annex A (informative): M2M System Overview

A.1 High Level System Architecture

In order to facilitate the understanding of some of the terms used in the present document, figure A.1 provides a High-Level M2M System Architecture (HLSA).

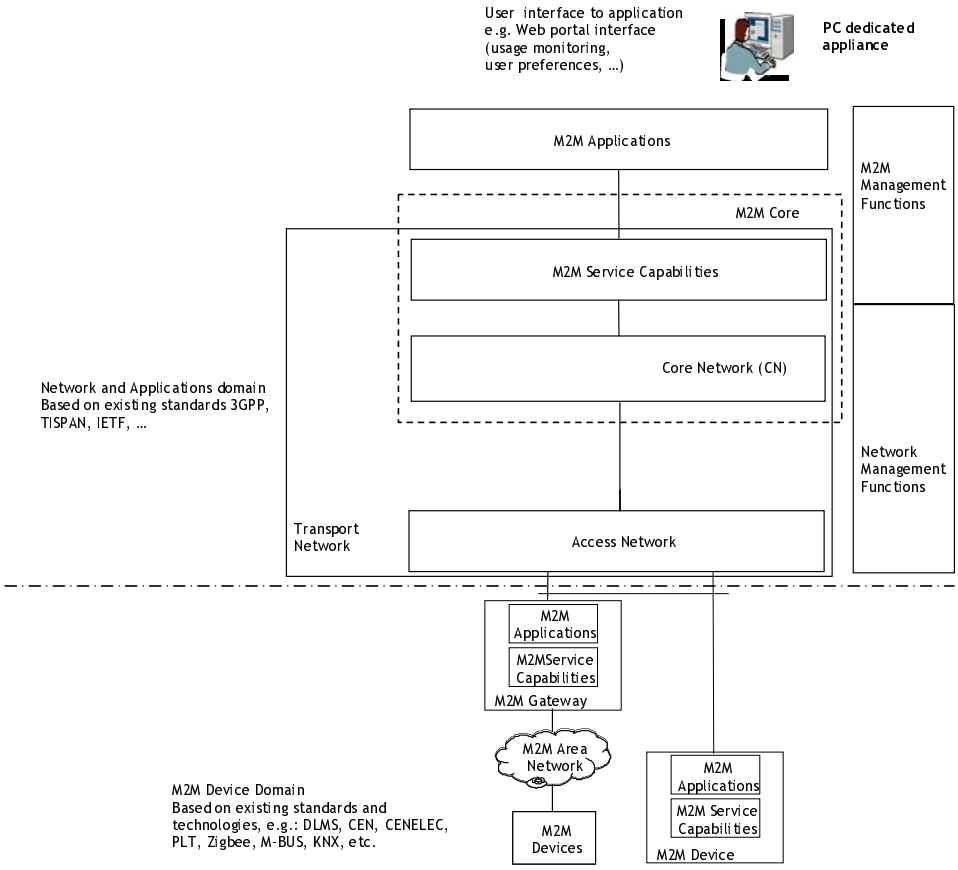

Figure A.1: M2M high level system overview

The M2M system Architecture includes M2M Device domain, and a Network and applications domain. The HLSA is based on existing standards regarding the network domain extended with M2M specificities.

Annex B (informative): M2M use cases

B.1 M2M use cases generalized from SCP UICC

The following use cases are generalized from [i.8] UICC for Machine-to-Machine (M2M) applications.

B.1.1 Track and trace use cases

Track and trace use cases are mainly automotive related, but also related to tracking and trace of goods in production environments and retail, e.g. based on RFID technology.

M2M applications within the automotive industry are focused on delivering enhanced security for people (emergency call applications) or assets (theft tracking applications). Fleet management applications focus on increased operational efficiency and increased incremental revenue. These services are broad ranging and include remote diagnostics, navigation systems, pay-as-you-drive (insurance, in-car services), etc.

For use cases in the automotive sector there are common automotive criteria. The Automotive Electronics Council (AEC) was established for the purpose of establishing common part-qualification and quality-system standards directly addressing product reliability. The AEC Component Technical Committee is the standardization body for establishing standards for reliable, high quality electronic components.

The automotive market increasingly requires that semiconductor suppliers provide products compliant to the AEC-Q100 standard and ISO 16750 [i.7] (provides guidance regarding environmental conditions commonly encountered by electrical and electronic systems installed in automobiles) as such the M2M Devices and modules should comply with all these requirements.

Use case - Emergency Call

The in-vehicle emergency call system can save lives by automatically or manually sending the accurate location and driver information to an emergency centre. In this use case, an in-vehicle M2M communication module enables the transfer of emergency call data between the vehicle and an emergency service.

In this use case, a vehicle has a built-in M2M communication module which is connected to sensors that can identify an occurring accident. In case of an accident the module automatically sets up a connection to an emergency centre and sends information about the location, an indication about the level of the accident and maybe other additional information that might be available and evaluated as useful. (These services may be implemented via applications residing inside the M2M module). A key criterion for this use case is that the M2M module and its interfaces are able to survive and operate after a shock caused by an accident. Additionally, the automotive industry has indicated that the size of the M2M module and the ability of the module to communicate whilst in a normal automotive environment, over the expected vehicle lifetime, are important.

Use case - Fleet Management

For this use case, a vehicle has a built-in M2M communication module which is typically owned by a company (not the user). The module collects information, for example: location, timings, traffic jams, maintenance data and transport environmental conditions. This information can be sent by the module via a mobile network to a server application where it can be used to track the vehicle and deliveries.

Using the retrieved information, a server application can effectively optimize the delivery plan and route. The adjusted delivery plan is then sent via the mobile network to the vehicle and appropriate information can be displayed to the driver. Additionally, based on the maintenance related information, maintenance can be planned or remote maintenance performed. In addition, environmental sensors can be used to retrieve information on the storage environment and condition of product being transported.

Key criterion for this use case is the ability of the M2M communication module to communicate whilst in a normal automotive environment, over the expected vehicle lifetime.

Use case - Theft Tracking

Currently, the theft of automobiles is usually prevented in one of two ways, either by deterring the thief with an alarm system or by preventing the engine from starting with an immobiliser system. These systems however can be evaded, for example by quickly disabling or ignoring the alarm system, or transporting the vehicle without the aid of the engine.

In this use case the introduction of M2M allows for the possibility of preventing the theft itself or recovering the vehicle, for example by theft tracking. It is envisioned that the M2M module will allow secure communication over the network to a third party entity.

M2M in this use case will have to function in an extended temperature and humidity range not usual for a terminal. In addition, the connection with the M2M communications module will have to withstand the vibration produced by the engine of the vehicle as well as by the vehicle on the road. To keep M2M module from suffering the same fate as numerous alarm systems, it needs to be protected against theft and misuse, for example through M2M UICC to vehicle and/or communications module pairing.

Another factor in this environment is the often limited space available to conceal or secure the system from theft and misuse, which means that the size of M2M modules should be kept small. In order to make it available to a large segment of the automobile market, in some cases, the M2M module should be integrated in mass produced modules as generally required by the automobile manufacturer groups. As vehicles are built to have a lifetime that may easily extend beyond ten years, but also keeping the costs of maintenance to a minimum, lifetime expectation is also a factor.

B.1.2 Monitoring use cases

M2M applications within this category are either used to monitor and control utilities consumption, or monitor, track and trace persons, animals or assets.

Use case - Metering/Prepaid delivery of utilities (water, gas, electricity)

The utility companies deploy intelligent metering services by installing M2M communication modules on metering devices which can send information automatically or on demand to a server application which can, for example, be used to automatically bill the metered resource. In this use case the purpose is either to improve energy performance and efficiency through the delivery of a much more accurate picture of consumption, efficiency and cost, while also delivering the end user actual usage without human intervention. This in turn provides a positive environmental impact. In the opposite direction information inside the metering device may be securely updated (over the air).

Metering devices are often placed in harsh environments. In many metering devices space is very limited, meaning the size of the M2M communication module needs to be minimized. Metering devices may be produced in high volumes, which require that the M2M modules can be integrated in an industrialised process. As sensitive data might be stored, the modules need to be protected against theft and misuse.

An extension of the above use case for metering of gas, electricity, water, is based on pre-payment. A household can purchase a specific volume of gas, electricity, water, etc. by pre-payment. The information about the purchased volume is securely transmitted (over the air) to the metering device and then securely stored inside the M2M modules. During consumption the actual information about the consumed volume is transmitted to the M2M module. When the purchased volume has been consumed the supply can be stopped.

This use case implies the ability to perform secure transactions between the M2M module and the controlled metering device. This may also include the possibility to securely perform control operations e.g. stopping the delivery.

Use case - Person/Animal protection

In this use case persons and/or animals are equipped with portable devices containing a M2M communication module, and optionally a GPS function, which sends information automatically or on demand to a server application which can monitor the status and positioning of the persons or animals. The purpose is to improve security and/or remotely monitor the status while also being able to track and trace either the person or the animal. These services may be implemented via applications residing inside the M2M module/UICC.

For persons, the typical applications are lone worker, healthcare, elderly or child monitoring. For animals, the typical application is track and trace.

The portable devices are often placed in harsh environments; this means that they are undergoing strong vibrations or even shocks. The space is very limited, meaning the size of the M2M communication module needs to be minimized. As sensitive data might be stored, the module needs to be protected against theft and misuse.

Use case - Object protection

This use case is very similar to the above (persons/animal protection). Objects are equipped with portable devices containing a M2M communication module, and optionally a GPS function, which sends information automatically or on demand to a server application which can monitor the status and positioning of those objects. (These services may be implemented via applications residing inside the M2M module/UICC).

The purpose of this application is to track and trace.

The portable devices are often placed in harsh environments. This means that they are undergoing strong vibration or even shock, extreme temperature, humidity or corrosive environments such as salt water.

The space is also very limited, meaning the size of the M2M communication module needs to be minimized. In many cases the device should be small enough to be hidden.

As sensitive data might be stored, the module needs to be protected against theft and misuse.

B.1.3 Transaction use cases

Use case - PoS Terminals (Point of Sale Terminals)

Today most Point of Sales terminals are connected via a wired connection. For the use in locations like bars, restaurants, etc. this means they are mounted or placed at a fixed position, and the person who wants to perform a transaction needs to go to the location of the PoS terminal. This causes inconveniences for the sales person/waiter as well as for the customer. In the case of remote located PoS terminals, e.g. parking meters, ticketing machines, etc. these require a wired connection which is often difficult and costly to be installed and may also be exposed to damages. Another option is to connect PoS terminals via a (local) wireless connection which imposes some security constraints.

The introduction of the M2M modules into this environment allows additional possibilities for applications, as M2M communication modules can be installed into wireless PoS terminals, street parking and ticketing machines, etc. to provide communication for credit or debit card on-line transactions. The use of a M2M communication module can offer a secure communication channel.

Typically these devices including the M2M communication module will need to pass specific security requirements for financial transactions.

B.1.4 Control use cases

Use case - Controlling vending machines

Today, vending machines are placed in various locations like e.g. inside office buildings, public buildings, public outside places, railway stations, etc. The re-filling and maintenance of vending machines is today done by dedicated personnel who have to visit the vending machines at regular intervals to check the fill-levels, re-fill the machines, perform maintenance and identify damages or malfunction.

The introduction of M2M into this environment allows additional possibilities for optimization of the operation of vending machines. By allowing access to a (mobile) telecommunication network, the M2M modules can be used by a built-in M2M communications module to provide authenticated information about the current status of the vending machine via the network to a background service. Via this connection it is possible to transmit information about the current fill-levels, maintenance status, possible damages, malfunctions, etc. Additionally it is possible to transmit updates of e.g. pricing information or perform remote maintenance. This way the vending machines need only to be visited as required.

Use case - Controlling production machines

Today, production machines are placed normally inside production facilities which, depending on these facilities may expose the production machine to harsh environments. The repair and maintenance of production machines is today done by dedicated personnel who have to visit the production machines at regular intervals to repair, perform maintenance and identify damages or malfunction.

The introduction of M2M into this environment allows additional possibilities for optimization of the operation of production machines. By allowing access to a mobile telecommunication network, the M2M modules can be used by a built-in M2M communications module to provide authenticated information about the current status of the production machine via the network to a background service. Via this connection it is possible to transmit information about the current maintenance status, possible damages which may lead to malfunctions, etc. Additionally it is possible to transmit updates of e.g. updated software or perform remote maintenance, e.g. via Over-The-Air functionality. This way the production machines need only to be visited as required.

B.2 Compensation use cases

B.2.1 Utility account management for prepaid

A consumer, with a prepaid arrangement, receives an indication (e.g. on the Local display) that his prepaid account is soon exhausted. Thus, he initiates a refill of the account, e.g. via the Local display, a home-banking application or the mobile phone. The mechanism involved apply a trusted third party (e.g. a bank or a credit card company) to verify and carry out the refilling of the account.

B.2.2 Micro compensation for sensor readings

A service provider offering sensor readings of the water temperature at attractive sea locations for bathing charges 1/50 EURO for each reading. The compensation scheme requires computerized micro-payment to be applied in order to be cost effective.

B.2.3 Additional areas of applicability

- In transport/logistics where e.g. a driver can register delivered goods and receive payment.
- EPOS applications.
- NFC payments e.g. via the MS.

All these areas benefits from electronic compensation capabilities.

B.2.4 Service capabilities and primitives

Settlement and compensation is part of the Management domain. The following high level primitives may be used for settlement between any pair of objects (i.e. the compensator and the compensated). It is a precondition for the settlement that the object has a valid account and relation with a mutually trusted broker (e.g. a bank).

- CommitValue (Object-ID Vendor, Currency currency, Integer Devidedby, Object-ID Broker).
- Settle (Object-ID Vendor, Integer Amount, Object-ID Broker).

B.2.5 Example micro compensation scheme

A candidate compensation scheme implementing the above service primitives may be based on the following micro-compensation scheme. A significant benefit of micro-compensation over macro-compensation is the flexibility in allowing any granularity of value in the transaction.

An object generates a hash chain of length N by applying a hash function N times to a random secret value PN, the root of the hash chain, to obtain a final hash P0, the anchor of the hash chain. The object commits to the chain by digitally signing the anchor with the private key. For each payment, the object releases a pre-image of the last hash value. For example, the object releases the hash value P1 for the first payment. The receiver of the payment can apply the same hash function to the value P1 to obtain the anchor P0. Since the hash function is one-way, only the object could have generated the hash value. The object commits to the anchor of the chain P0, the length of the chain, the value of each hash, and the vendor at which he/she wishes to spend the chain. Prior to payment, the object forwards the commitment to the vendor, who can verify its authenticity (e.g. offline). For each micro-payment, the object releases the next (number of) payment hash(es) in the chain. The vendor can redeem the hashes at the Broker with whom the object has an account at a later date, by presenting the highest payment hash along with the signed commitment. (There exist optimizations to this scheme.)

The following service primitive initiates the acquirement of Length number of tokens (returned in Tokens), each valued and honoured by Vendor (e.g. via a macro transaction):

- Buy-Tokens (Object-ID Broker, Integer Length, Integer Value, Object-ID Vendor, Hash P0).

The Commit-Token is used to initiate compensation, and it allows the Vendor to verify the validity of the tokens via the Broker:

- Commit-Token (Object-ID Vendor, Object-ID Broker, Integer Length, Integer Value, Hash P0).

Explicit micro-compensation is made by invoking the primitive:

- Submit-Tokens (Object-ID Vendor, Integer Length, Hash Tokens []).

Length number of tokens is transferred to the Vendor.

The Submit-Tokens functionality may be integrated in other primitives, e.g. in the Messaging primitives.

The Vendor applies the following primitive for redeeming the tokens (e.g. macro-payment):

- Redeem-Token (Object-ID Broker, Hash Tokens []).

B.3 Home Automation use cases

M2M communications may play a major role in houses, where automation of some processes appear essential in many home-related sectors such as comfort, health, security, energy efficiency, etc.

Deployment of Home Automation involves service requirements that can be derived from the description of some associated use cases, as below.

B.3.1 Energy efficiency at home

The purpose of this use case is to use M2M communications to optimize the use of energy in a house. For example, some occupancy sensors will be used in order to get the information about whether there is somebody or nobody in a room. In case nobody is in anymore, the lights will automatically be switched off. This basic example can be extended to other types of sensors in different rooms of the house to control the energy consumption from different equipments. The sensors and actuators are connected either wirelessly or via wires (e.g. via PLC) to an M2M gateway. By getting the data from the various sensors (e.g. measure of the electricity consumption of the heater, presence detection, outside temperature sensor), the M2M gateway can send the appropriate orders (e.g. to switch off the heater in a room or in the whole house) to the actuators depending on the local context information (e.g. nobody in the house any more for a while). The M2M system thus allows reducing energy consumption by automatically adapting the use of the house equipment to the local parameters.

In such a use case, the abstraction of the heterogeneous technologies used by the sensors and actuators is performed in the M2M gateway, which treats all the data received, merges them with other context information and sends appropriate orders to the actuators as a result of the treatment.

Sensors and actuators that are deployed in houses are expected to use low power consuming technologies (especially those sensors and actuators used for energy efficiency objectives!) so that the end-user do not need to replace their batteries before a long time. This is also needed for practical reasons when sensors or actuators are installed in some places with difficult access.

This use case also relates to the energy monitoring, by informing the customer on his energy consumption, in a global or a detailed (equipment by equipment) way, with possible remote access to be aware of this consumption even when the end-user is not at home. It may also alert the user of any detected anomaly compared to the usual consumption, so that any leak can be managed in due time.

B.4 Other use cases

Other relevant use cases are relevant to justify some generic requirements for M2M services. Some of these use cases are mentioned hereafter.

B.4.1 Data from Wireless Sensor Networks

This is a general use case for Wireless Sensor Networks (WSN) that can be considered as sources of large amount of data that has to be frequently stored in a persistent repository.

Raw sensor data is usually post-processed by some applications and the resulting aggregated data is then stored in another repository.

Both raw and aggregated sensor data are made available to many consuming applications that are able to access to it.

Also WSN sensor management is provided by maintaining sensor's databases for information like: manufacturer, model, type of measurements, hardware version, software version, etc.

Annex C (informative): Security aspects

C.1 Trusted and secure Environment

Some M2M devices typically operate unmanned and unguarded by humans and thus are subject to increased levels of security threats, such as physical tampering, hacking, unauthorized monitoring, etc. Terminals may also get geographically dispersed over time. Such M2M devices should therefore provide adequate security to detect and resist attacks. Devices may also need to support remote management including firmware updates to correct faults or recover from malicious attacks.

Some M2M Equipments (M2Mes) are typically required to be small, inexpensive, able to operate unattended by humans for extended periods of time, and to communicate over the wireless area network (WAN) or WLAN. M2Mes are typically deployed in the field for many years, and after deployment, tend to require remote management of their functionality. It is likely that M2Mes will be deployed in very large quantities, and many of them will also be mobile, making it unrealistic or impossible for operators or subscribers to send personnel to manage or service them. These requirements introduce a number of unique security vulnerabilities for the M2Mes and the wireless communication networks over which they communicate.

The Third Generation Partnership Project (3GPP) Security Workgroup (SA3) has collected categories of vulnerabilities:

1) physical attacks including the insertion of valid authentication tokens into a manipulated device, inserting and/or booting with fraudulent or modified software (reflashing), and environmental/side-channel attacks, both before and after in-field deployment;

2) configuration attacks such as fraudulent software update/configuration changes; misconfiguration by the owner, subscriber, or user; and misconfiguration or compromise of the access control lists;

3) protocol attacks directed against the device, which include man-in-the-middle attacks upon first network access, denial-of-service (DoS) attacks, compromising a device by exploiting weaknesses of active network services, and attacks on over-the-air management (OAM) and its traffic;

4) attacks on the core network, the main threats to the mobile network operator (MNO), include impersonation of devices; traffic tunneling between impersonated devices; misconfiguration of the firewall in the modem, router, or gateways; DoS attacks against the core network; also changing the device's authorized physical location in an unauthorized fashion or attacks on the network, using a rogue device;

5) user data and identity privacy attacks include eavesdropping user's or device's data sent over the access network; masquerading as another user/subscriber's device; revealing user's network ID or other confidential data to unauthorized parties.

Following are some references to the security requirements from the discussions when elaborating M2M specifications:

- As per M2M functional architecture document (TS 102 690 [i.1]), M2M devices provide secure transmission of messages. Security sensitive functions should be executed from within a secure environment. Also, in order to ensure that the message is secure, the executables providing the cryptographic security and the transmission of the messages should be integrity checked before being executed. Such an integrity check has to be performed in a secure execution environment which resists malicious attacks and unauthorized access.

- The devices should support accurate and secure time synchronization. In order to ensure that such synchronization software is secure, the software should execute in a secure environment and should be integrity checked and validated before it is executed.

- The M2M device should support secure and traceable compensation and micro-compensation. In order to ensure that the software/firmware necessary to generate the compensation information and the cryptographic keys necessary for authentication and compensation are integrity verified and secured, the integrity check of the firmware has to be executed in a secure and trusted environment in the M2M device. The secure environment should provide secure storage to store the necessary keys and data. Such secure storage has to be inaccessible to unauthorized users.

- As per the M2M smart metering use case TR 102 691 [i.2], the smart metering provider can initiate or the M2M device has the ability to report the security status of the device. Such monitoring and reporting software should be secured from malicious modifications and therefore execute in a secure environment.

In addition, Application in M2M devices that generate measurements or information which is accountable and billable, or M2M Devices that require device integrity validation, should provide a trusted secure execution environment or trusted platform for executing applications that require high-security execution environments. Therefore these M2M Devices are expected to provide a trusted and secured execution environment. Such a TrE would provide secure storage and resist malicious and unauthorized access. It would also be integrity checked and validated before it is started or executed by a hardware root of trust.

The TrE can be a logically separate entity within the M2ME, containing all necessary resources to provide a trustworthy environment for the execution of software and storage of sensitive data. The TrE is expected to provide isolation of software and stores data by separating them from the rest of the M2ME, thus protecting from unauthorized access. The TrE is expected to provide a trust anchor, which would be secured against tampering by hardware security measures. In particular, it is expected to provide the root of trust (RoT) for secure operation. The RoT is expected to be an immutable part of the TrE, which would secure internal operation and would be able to expose properties, or the system's identity, to external entities. Based on the RoT, the TrE would perform a secure start-up process ensuring that the TRE reaches a determined trustworthy state.

As an example, the TrE can be built from an irremovable and immutable hardware based Root of Trust by way of secure boot process. The secure boot process would include checks, performed by the Root of Trust, of the integrity of every loaded or started component of TrE, and would also include checks, performed by the TrE after it has started, of every loaded or started component of the M2M device other than the RoT or the TrE. The TrE can store at least one cryptographic key that is physically bound to the M2M device. The TrE can use such key to authenticate the TrE to the M2M system and also to protect the confidentiality and integrity of communication messages for device integrity checking and validation between the M2M device and the M2M system.

Annex D (informative): Rationale texts related to some of the Requirements

During elaboration of the present document, contributions for requirements were proposed with rationale texts justifying the need for these requirements. After editing v0.3.1 of the present document it was decided to delete all rationale texts in order to have requirements texts clearly appeared. Yet some of these rationale texts can help for a better understanding of the initial context under which a requirement was proposed. Thus they are copied back in this informative annex.

D.1 Rationale texts for some of the Requirements of clause 4

D.1.1 Related to clause 4.1

M2M application in the Network and Applications Domain should be able to initiate communications with the M2M Device even when dynamic addressing is used at the network layer.

Some M2M Applications may require a peer-to-peer communication between objects, e.g. between a gateway and an actuator for local processing e.g. in a home automation context. Thus, communication flows between these objects should be supported.

D.1.2 Related to clause 4.2

Battery operated M2M Devices may have long sleep times.

M2M Applications should be able to send a message to a sleeping M2M Device, as an example, and have it delivered to the device by the network when the device is awake. The application should not be burdened with keeping track of when the device is awake, especially for devices behind a gateway, for example behind a Zigbee coordinator.

D.1.3 Related to clause 4.3

Some M2M Applications in the Network and Applications Domain require the same message to be delivered to a number of M2M Devices. The delivery may be implemented through a combination of unicast and multicasts depending on the access network types.

D.1.4 Related to clause 4.4

In many M2M applications there is generally a flexibility in when the data is collected from the M2M Device or pushed into the M2M Device. For example, in smart metering it may be sufficient to get a meter reading once every hour and that could be any time within each hour. The M2M System will benefit from being able to schedule the data transmission when the network is least congested as this can reduce the communication costs.

D.1.5 Related to clause 4.5

In some M2M applications the M2M Device may be able to communicate over multiple access technologies such as wireline and wireless with different time-dependent communication costs. M2M Applications will thus benefit from appropriate route selection.

D.1.6 Related to clause 4.6

M2M applications should be able to communicate with devices behind a Network Address Translator (NAT) entity. For example, in the case of home sensor networks the sensors and sensor coordinator are behind a home gateway.

D.1.7 Related to clause 4.7

Sometimes the message that an application wants the network to delivery cannot be delivered within the time frame specified because of e.g. some network node failure. In such cases M2M Applications in the Network and Applications Domain should receive notification about communication-related failures.

D.1.8 Related to clause 4.8

The M2M System should be designed to achieve both scalability and minimalism in terms of system resource usage. The number of sensing nodes, controllers and actuators (i.e. objects) e.g. deployed in the urban environment in support of some applications is expected to be very high (i.e. in the order of 10^2 to 10^7).

D.1.9 Related to clause 4.13

Not all M2M applications may have to rely on integrity of the transmitted information. On the other hand, integrity of information delivered with M2M services might be very important for other M2M applications.

D.1.10 Related to clause 4.15

Some M2M applications might request the same M2M service on a more regular and continuous bases. In that case it would be good if the network could establish a persistent connectivity that will persist beyond the point in time when a individual transmission of information is completed. This persistent connectivity could be disabled once the network is requested by the requesting source to do so or until a timer expires. On the other hand M2M applications might use M2M services very infrequent and irregular without any possibility to predict how soon a M2M service would be needed again after a first request. In that case the network would need to know that the connectivity can be removed after transmission of information is completed after an individual request.

D.1.11 Related to clause 4.20

M2M communication such as generating information of high value used for billing may require time stamping. For such communications, a secure and trusted time stamp needs to be generated that can be used in the network and the device.

D.2 Rationale texts for some of the Requirements of clause 5

D.2.1 Related to clause 5.1.3

Testing the connectivity towards certain COs (as agreed with the customer) at regular intervals is in demand for more application areas. The test may be initiated by an application or by the CO and the events where connectivity is not verified is logged and reported.

D.2.2 Related to clause 5.1.5

M2M devices may be in the field, operational for many years. Some devices may operate in areas where it is difficult to physically access the device. For example, M2M sensors mounted in harsh environments, or M2M devices for geo tracking. Such devices are difficult to service by human intervention. Since the M2M devices are projected to exist in large numbers, if the M2M device experiences a fault, then remote management of such devices provides for prolonged service life. Such faults can be caused for example, by harsh environment, system failure and security breach. It is therefore proposed that M2M devices may support remote management or device remediation. In such a management process, the device may be able to obtain firmware updates by connecting with a management server securely. After application of the firmware udpate, the device may reboot to a known and consistent state.

D.2.3 Related to clause 5.2.1

M2M services typically involve a large number of M2M Devices generally sending a small amount of data each. The revenue per M2M Device is generally small for any of the players in the value chain. Thus it is important to minimize expenses incurred in deploying and maintaining these devices. One of the key steps in the deployment of M2M Devices is their provisioning in the appropriate data bases of the network and application provider. In particular, provisioning of keys or other information for the security solution should be simple and scalable. The provisioning process cannot assume that the M2M Device will be turned-on at a known pre-arranged specific time. Devices may be turned-on temporarily at the manufacturing site for testing but then subsequently turned-off until deployment. It can be installed at one time but then the communication may only be established later. Thus it is not possible to predict a particular time for a provisioning process to be executed.

D.2.4 Related to clause 5.2.2

The network should be able to repair connectivity as objects die out and new ones are put in place. New objects may also be installed just to increase the reliability and performance of the network. The change should be localized, and not visible all around the network. The time interval for repairing the network may be relatively long, as in the bootstrapping phase.

D.2.5 Related to clause 5.2.3

In order to make accurate measurements from multiple M2M Devices at the exact same instance in time, time synchronization with accuracy in the order of milliseconds is needed, possibly over a larger physical area. Hibernating objects may require even higher synchronization needs in order to maintain efficient intermittent connectivity.

D.2.6 Related to clause 5.2.4

Management, e.g. of Customer Premises Equipment (CPE), field devices including M2M Device domain elements and objects is key to service offerings and operational efficiency.

D.3 Rationale texts for some of the Requirements of clause 6

D.3.1 Related to clause 6.1

Depending on the M2M application, data collection may be needed in different ways. For example a smoke alarm information should be delivered as soon as detected, whereas the energy consumption at home may be required only sometime. The M2M System should support the different ways of delivering the data in time.

D.3.2 Related to clause 6.3

A key design element is the Group. It is an architectural construct which may be used for large scale and wide distribution networks and offers a generic grouping and partitioning mechanism. Such a mechanism can provide increased functionality and management of unresolved problems in current networks. The rationale is that virtually any horizontal slice through the current Internet structure reveals a loosely coupled federation of separately defined, operated, and managed entities. It is natural to think of each of these entities as existing in a group of the network, with each group having coherent internal technology and policies, and each group managing its interactions with other groups of the net according to some defined set of rules and policies. A group is an entity that encapsulates and implements scoping, grouping, subdividing, and crossing boundaries of sets of entities. In network systems, these functions are used for a variety of purposes including scaling, heterogeneity, security, billing, performance, trust management, and so on. It is shown that we can separate mechanism from purpose, by providing a single highly optimized and reusable generic mechanism to serve a number of purposes.

D.3.3 Related to clause 6.4

For mission-critical applications, support of QoS is mandatory. The following service parameters are relevant in a resource-constrained network, non exhaustive list:

- Data bandwidth - the bandwidth might be allocated permanently or for a period of time to a specific flow. Some flows may also share bandwidth in a best effort fashion.
- Latency - the time taken for the data to transit the network from the source to the destination. This may be expressed in terms of a deadline for delivery.
- Transmission phase - process applications can be synchronized through coordinated transmissions.
- Precedence and revocation priority - Networks may have limited resources that can vary with time. This means the system can become fully subscribed or even over subscribed. System policies determine how resources are allocated when resources are over subscribed. The choices are blocking and graceful degradation.
- Transmission priority - the means by which limited resources within objects are allocated across multiple services. For transmissions, an object has to select which packet in its queue will be sent at the next transmission opportunity. Packet priority is used as one criterion for selecting the next packet. For reception, an object has to decide how to store a received packet. The objects are usually memory constrained and receive buffers may become full. Packet priority is used to select which packets are stored or discarded.
- Reliability - Data provided for further processing should be transported in a reliably as if one part of the whole data set is lost, the entire sampled data may be useless.
- Path capabilities - The path recovery scheme might be different depending on the role of the failed path.

D.3.4 Related to clause 6.5

The network should support different object types, e.g. active objects and sleeping objects. Also some devices include Low performance tiny objects, small memory sizes, low-performance processors, low bandwidth, high loss rates, etc. The functionality requirements for M2M Devices should fit within limited hardware configurations.

Handling sleeping objects is a critical requirement, as objects might stay in sleep-mode for most of the time. Time synchronization is important for efficient forwarding of packets. Connectivity should be reliable despite unresponsive objects due to periodic hibernation.

The network should support parameter constrained operations where the parameters are controllable resources like CPU, memory size, battery level, etc.

The M2M System should save power consumption for these un-powered M2M Devices. Powered objects should assist the un-powered objects or take care of more functionalities than un-powered objects.

D.3.5 Related to clause 6.7

Due to external factors or programmed disconnections, an object can be in several states of connectivity, ranging from "always connected" to "rarely connected".

D.3.6 Related to clause 6.8

Data flows between objects are not necessarily symmetric. In particular, asymmetrical cost and unidirectional routes are common for published data and alerts, which represent a significant part of the M2M Device traffic. The reporting of the data readings by a large amount of spatially dispersed nodes towards a few Gateways will lead to highly directed information flows. Downloading (e.g. new functionality) to objects will similarly result in asymmetries in the downstream direction.

D.3.7 Related to clause 6.9

Different services categories have varying service requirements, and it is often desirable to have different paths for different data flows, even between the same two endpoints. For example, alarm or periodic data from A to Z may require path diversity with specific latency and reliability. A file transfer between A and Z may not need path diversity, but high data rate.

D.3.8 Related to clause 6.10

The M2M System architecture should support interfacing of existing and evolving access technologies, wired and wireless, including low power home networks for short range wireless communications. The interfacing of diverse technologies may require gateway functionality that may be provided by network operators.

D.3.9 Related to clause 6.11

In some cases, some different M2M Applications can use the same M2M Devices. A use case of this scenario: when a traffic accident happens, the damaged vehicle reports the information to both the health service centre and the insurance company. So the M2M System should be able to support the M2M Devices reporting data to one or multiple applications.

D.3.10 Related to clause 6.12

Usually an M2M Application has more than one M2M Devices served to provide M2M services to customers. Examples include Intelligent Transport Systems and Smart Metering Systems both supporting a large number of M2M Devices.

D.4 Rationale texts for some of the Requirements of clause 7

D.4.1 Related to clause 7.1

The back-end server that is collecting data from an M2M Device should be assured that the data is coming from a legitimate and correct device. In the absence of such an authentication it is possible for some devices to pretend as other devices in the network and upload data. For example, in the smart metering service where meter data is collected from the various meters, a deviant home owner might alter the meter identification so that it appears as a neighbor's meter to the server there by avoiding paying for use of electricity.

Such an authentication procedure can also help eliminate inadvertent errors such as multiple devices being set to the same identity as in the case where a sensor identity is set by dip switches.

D.4.2 Related to clause 7.2

Devices can be hijacked by adversaries for the data they provide or for their actuation capabilities by pretending to be the back-end application server. A scenario where such an attack could be some economic value to the adversary is remote control of home automation devices such as alarms and garage door openers. By pretending to be the network based home automaton server miscreants can deactivate the alarm and open doors to enter the house. Thus the device should authenticate the server before accepting any data such as commands or management related updates.

D.4.3 Related to clause 7.3

In many M2M applications the data collected from the M2M Devices are sensitive in nature. For example, in a child tracking application it should not be possible for unauthorized persons to acquire information about the location of the child. Thus the M2M security solution should be such that it is not possible to acquire information about the data collected by eavesdropping at any point in the network.

D.4.4 Related to clause 7.4

Adversaries may benefit from modifying the data transferred from the device to the back-end application server or vice versa through man-in-the middle attacks. It should thus be possible to verify the integrity of data transferred between the entities.

D.4.5 Related to clause 7.5

Unlike in the case of consumer electronic devices, in many cases M2M Devices are owned by the application providers and deployed in premises that are not constantly physically monitored or protected. For example, in the case of smart metering, the meters are typically owned by the utility companies and deployed in homes and small business locations. These devices are thus more susceptible to theft. Misuse of stolen communication modules found in these devices for the purpose of regular internet communication such as web browsing should not be allowed.

D.4.6 Related to clause 7.6

In many applications transmission of the actual identity of the device unencrypted is not acceptable since the device and or it usage can be tracked by adversaries eavesdropping on the network. Identity is valuable information as it can be correlated with other data such as the location of network elements from which this identity information is retrieved to discern some patterns.

D.4.7 Related to clause 7.8

M2M Devices typically will be deployed in the field, unguarded and unmonitored by humans or other means. Many M2M Devices will also handle value-added, confidential data for applications that have security implications for the respective M2M market sectors (e.g. smart metering, sensor networks, traffic cameras, ITS devices, etc.). Many such devices may also be implemented on platforms with open interfaces, for causes such as cost reduction, increased functionality and flexibility and ease-of-development. However, all of the above factors mean that tampering of the HW, FW or SW of M2M Devices is a real security concern. An attacker, for example, may be able to use capillary networks and rogue gateways or even on-device interfaces to inject malware or otherwise tamper with the M2M Device, causing damage and harm to the stakeholders. This vulnerability is of special concern for M2M Devices which can connect autonomously to the Internet via public communications networks.

D.4.8 Related to clause 7.10

The number of M2M services, and use case scenarios, is expected to grow over time. Additionally some M2M services may have long product and service life cycles, e.g. smart meters. Security experts and cryptographers often discover new attacks on systems. This coupled with the constant improvements in computing capabilities, often force security managers to upgrade key lengths and modify security policies. In some instances there may be a need to upgrade algorithms. In some other instances, there may be a need to distribute security patches to address vulnerabilities in protocols and applications that are not known at the time of installation. More generally, operators as well as M2M application providers may discover new needs to update service and security policies over a period of time.

History

Document history		
V1.1.1	August 2010	Publication
V1.2.1	June 2013	Publication