European Commission
Information Society and Media

SEVENTH FRAMEWORK PROGRAMME

Large Scale Integrating Project

EXALTED
Expanding LTE for Devices

FP7 Contract Number: 258512

WP7 – Integration & Proof of Concepts

D7.1
Selection of Scenarios for Proof of Concept Testbeds and Specifications for Key Building Blocks Functionalities and Interfaces

Contractual Date of Delivery:	31 August 2011
Actual Date of Delivery:	31 August 2011
Responsible Beneficiary:	TST
Contributing Beneficiaries:	TST, SC, ALUD, UNIS, TUD, CTTC, CEA, VID, GTO
Security:	Public
Nature	Report
Version:	2.0

Document Information

Document ID:	EXALTED_WP7_D7.1_review_EC
Version Date:	30 January 2012
Total Number of Pages:	70
Abstract	This document present the status of WP7 work defining the different testbeds that EXALTED project will perform to demonstrate the novelties introduced by the project.

Authors

Name	Organisation	Email
Juan Rico	**TST**	**jrico@tst.sistemas.es**
Javier Valiño	**TST**	**jvalino@tst.sistemas.es**
Stephan Saur	**ALUD**	**Stephan.Saur@alcatel-lucent.com**
Nhon CHU	**SC**	**nhon.chu@sagemcom.com**
Mohamed Ammari	**SC**	**Mohamed.ammari@sagemcom.com**
Payam Barnaghi	**UNIS**	**p.barnaghi@surrey.ac.uk**
Walter Nitzold	**TUD**	**walter.nitzold@ifn.et.tu-dresden.de**
Jesús Alonso-Zárate	**CTTC**	**Jesus.alonso@cttc.es**
Petros Bithas	**UPRC**	**pbithas@unipi.gr**
Alexandru Petrescu	**CEA**	**alexandru.petrescu@cea.fr**
Patrick Van-Haver	**GTO**	**Patrick.van-haver@gemalto.com**
Eleftheria Vellidou	**VID**	**projects@vidavo.gr**

Approvals

	Name	Organisation	Date	Visa
Internal Reviewer 1	Nemanja Ognjanovic / Bojana Jakovljevic	TKS	16/08/2011	OK
Internal Reviewer 2	Christian Ibars	CTTC	15/08/2011	OK
Technical Manager	Pirabakaran Navaratnam	UNIS	26/08/2011	OK
Project Manager	Djelal Raouf	SC	30/08/2011	OK

Executive Summary

This deliverable presents the work done during the first project year in work package (WP) 7. This document represents a summarization of the development done in defining demonstration activities that are going to be carried out in the EXALTED project.

The work presented in this document is based on the activities developed in other work packages in the project. It analyzes target scenarios and use cases provided by WP2, and the researches done and envisioned in technical WPs, from 3 to 6, each of them focused on different aspects of the overall system architecture proposed by the project.

Three main target scenarios have been defined in EXALTED, namely Intelligent Transportation System (ITS), e-Health and Smart Metering and Monitoring (SMM). Considering those three scenarios, the objective of WP7 is to create demonstrators associated to different use cases, showing the capabilities of the devices, protocols and concepts developed in EXALTED. In this sense, three main testbeds will be created:

- LTE-M based, aiming to demonstrate PHY and MAC layers concepts. This testbed comprises key concepts being developed on WP3. The goal is to demonstrate, in a simplified way, the applicability of envisaged enhancements of LTE, in terms of algorithms and functionalities, in order to be able to handle large amounts of M2M devices.
- Connectivity oriented testbed, focused on demonstrating how EXALTED will perform an end-to-end (E2E) communication between devices and servers. This testbed includes a relative large of heterogeneous devices provided by partners, trying to prove the interoperability and the ability to manage different kinds of devices. Three different networks are envisaged, some of them including just one type of devices and some other comprising heterogeneous devices.
- Device Management testbed, whose goal is to prove how the different elements in the architecture will be controlled. The main goals of this testbed are, apart from E2E connectivity, defining the most appropriate device management protocols to be implemented both on devices and servers and assuring the security that device management protocols imply.

The scope of this document is the definition of each testbed in terms of architecture, functional blocks, interfaces and timeline that can be set at this stage of the project in order to create clear integration plans.

The document is divided into 5 sections. Section 1 introduces the document, and section 2 depicts the scenarios identified by EXALTED, selecting specific use cases within them to be demonstrated by the testbeds. Then the three main testbeds are described, presenting a general overview of each of them. Section 4 is the core of the document, providing a clear specification of each testbed. Finally the conclusions derived from the work done in the WP7 are presented.

Table of Contents

1. Introduction

The research work done in the EXALTED project shall be presented in a tangible way. In this sense, this document aims to create the basis for the demonstration activities that will be carried out in the project. It also contributes to the overall EXALTED project by giving to the public the current status at month 12 of this Work Package (WP).

As a reminder, WP7 is dedicated to prove the EXALTED project concepts, by delivering three testbeds that will demonstrate many concepts and novelties introduced and developed all along the 30 months duration of the EXALTED project.

This public deliverable is the first one of the three expected in WP7. It is oriented toward the selection of use cases and scenarios, their justification and, the specifications of the key building blocks and their interfaces of the three testbeds, while the next two public deliverables will focus on the integration of the building blocks into the final platforms and their final validations on months 24 and 30 of the EXALTED project, respectively.

The preliminary conclusions from the other five work packages that are performed in parallel to this work package mainly focus on the following:

- In WP2, main scenarios, use cases, baseline reference systems and requirements will be described. This information has been included in the first WP2 public deliverable [1]. This is a valuable work for WP7, and the testbed selection should rely on these guidelines provided. Furthermore, some other documents are under development and will be released coinciding with D7.1. WP2 deals with general concepts, the EXALTED architecture and business models, so synergies between these documents and D7.1 are important in order to well define all testbeds.
- WP3 focuses on the new LTE-M network. The preliminary recommendations from WP3 have been developed during this period of the project and will be included in [2] and [3]. These requirements shall be taken into account in the definition process of the testbeds, especially on LTE-M testbed.
- WP4 is related to capillary networks and assuring the E2E (end-to-end) connectivity. First requirements derived from its work have been presented in WP7 by the partners involved in both WPs, and will be considered when introducing all testbeds, with special implications on connectivity oriented and device management ones.
- WP5 deals with security issues, applicable on both LTE-M and capillary networks. The security recommendations introduced by the partners participating in this WP will be integrate in the testbeds, so as to prove all these concepts.
- Finally, WP6 is in charge of device improvement, some of its requirements are included when defining testbeds, especially on the last one, device management testbed.

Given this general project scenario, the focus in D7.1 is on combining, on one hand use cases and scenarios defined in WP2, and on the other hand, all the knowledge provided in terms of technical requirements and recommendations developed in WP3 to WP6, in order to create feasible and comprehensive testbeds that could prove concepts introduced by EXALTED. As all work packages have performed their own preliminary studies, it is possible to introduce a first architecture model for testbeds, trying to include most of the assumptions being made.

The work done on the WP7 first Interim Report (IR7.1) is the basis for this document. Each partner's capabilities and intentions were outlined there, as well as a preliminary architecture based on generic functional blocks. The goal will be the mapping of all partners' capabilities

(in terms of knowledge and hardware/software modules that can be provided) into a more detailed architecture, explaining not only the generic functions that shall be proven, but the real ones enabled by the real devices/modules that are going to be brought by partners.

2. Analysis of Use Cases and Scenarios

2.1 Introduction

Machine-to-machine communications attract more and more attention, offering tremendous opportunities to the saturated telecommunications market, with new services and applications, which open a mass market with a wide range of business opportunities. The vast field of M2M applications and services could change the telecommunications market by allowing carriers to charge based on the type of data, rather than the amount of data.

The telecommunication industry, standardization groups and research organizations have foreseen several use cases, with some of them having attracted particular interest, such as the Smart Metering (end-to-end energy management), which is seen as one of the most important areas for development in 2011, while in some countries such M2M applications are already commercially available. The automotive industry is expected to be another growth area for M2M, with a variety of applications, such as navigation and infotainment, emergency calling and diagnostics, and stolen vehicle tracking and recovery. Another development area is related with e-healthcare applications, including the monitoring of patients.

Despite the fact that some M2M applications have already started to be available commercially, the current cellular networks and architecture are not appropriate for supporting a general flexible framework for M2M communications with a large number of diverse services and applications. This can be also seen by the fact that each commercial M2M application may be implemented through different technologies.

While the number of possible M2M applications and services is limitless, a unified architecture should support them. Moreover, a global standard would result in developers creating millions of applications, with endless possibilities. Towards this concept, GSM and CDMA can handle the bulk of today's low-bandwidth applications, but the amount of information continuing to grow, which will require LTE-based modules which can handle considerably larger amount of data. The powerful advantage of using LTE for M2M communications is that it not only provides high bandwidth when required, but also minimises the network resources required to transmit data.

The EXALTED project aims exactly at advancing towards this conceptual unified architecture by expanding LTE for an architecture, which will support a general framework of M2M applications and services. Supporting M2M communications through LTE is equivalent to realizing specific key requirements, which may be common in different scenarios. The scope of this section is the selection of those use cases and those key requirements whose implementation will demonstrate how LTE can be expanded for supporting M2M communications.

The three main scenarios identified as key ones for EXALTED are described in this section, from the WP7 perspective. From each one, the specific requirements to be demonstrated are pointed out. Then, a selection among the wide range of possible use cases related to the scenario is done, providing a full description of it and reasoning why it is selected.

2.2 Scenario Description

In this section consolidated scenarios coming from use cases identified by D2.1 are presented from the WP7 point of view that is with the testbeds implementation in mind and the EXALTED key techniques to be demonstrated.

2.2.1 *Intelligent Transport System (ITS)*

Intelligent transport systems are expected to play a key role in M2M business market. The envision scenario in this report is the traffic optimization and smart navigation, whose purpose is mainly to supply traffic information to vehicles.
Figure 2—1 presents a rough system architecture. Each vehicle is equipped with an individual device with GNSS capabilities, to gain information necessary for the traffic optimization (position, speed etc).
The base stations collect this information for further off-board processing. The devices at each vehicle may also communicate directly with other devices nearby, aiming at interference and traffic load reduction. Also, smaller autonomous networks may be setup between the devices, communicating with the base station through a gateway.

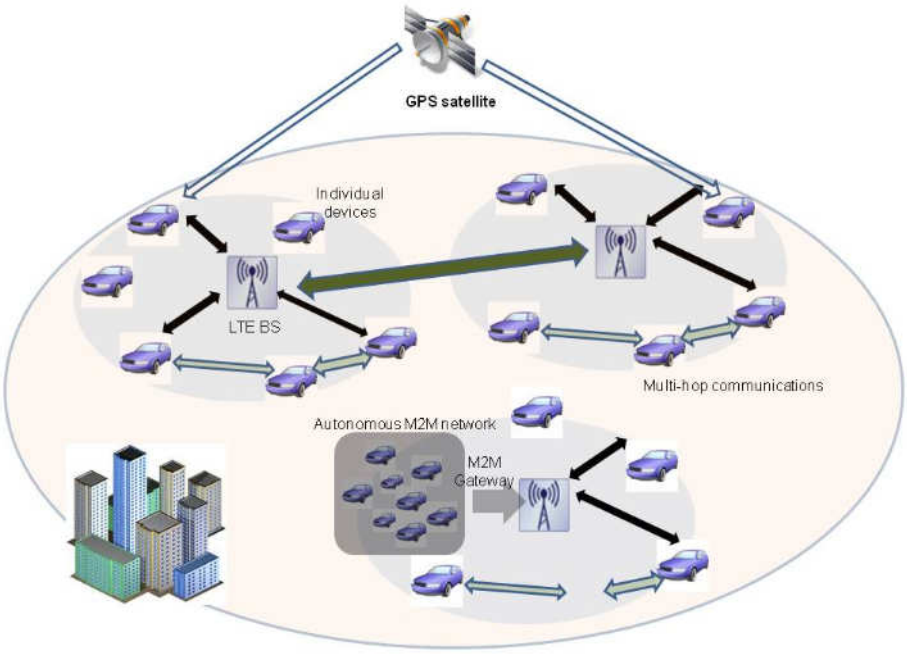

Figure 2—1. The ITS Scenario

This scenario will be used to verify some requirements of EXALTED:

i. *Wide connectivity range*: covering large geographical areas.
ii. *Techniques for large number of devices*: this scenario will serve to study in testbeds:
    a. Multicast and broadcast capabilities.
    b. Advanced scheduling protocols.
    c. Advanced resource allocation techniques.
iii. *High scalability*: new connections should not cause any problems.
iv. *High mobility*: since the devices are attached on vehicles, high mobility is expected.
v. A*utonomy*: the nodes will be able to create independent networks, in order to provide backup connectivity to other nodes. Multi-hop communications may also be used.

2.2.1.1 *Vehicular Communications*

In general, Vehicular Communications can be exemplified by a large number of possible demonstration use cases, because vehicles exchange data for a variety of reasons ranging from paid entertainment to critical collision avoidance, eHealth, and much more. We propose

to focus on one particular vehicular communication scenario: vehicle-to-vehicle-to-infrastructure communications (V2V2I). This scenario will be demonstrated as a prototype on a table, using same hardware equipment as deployed in vehicles. If time and resources allow, three other scenarios are considered:

- Remote monitoring of vehicle data
- Parking time check
- In-vehicle M2M diagnosis.

The technical specifications of the V2V2I IP communications mechanism are developed within WP4. Currently, a number of initial characteristics have been identified, with respect to the addressing architecture, subnet structure, vehicular networks as capillary networks and more.

Car-to-car communications are important for several applications. One potential application is the use of assisted breathalyzer engine ignition. An existing in-vehicle application analyses the driver's breath before allowing local engine ignition; whereas this entirely local decision (breathalyzer connected directly to the ignition lock) a value-added service may consist in transmitting the breathalyzer information to a server notifying in advance the law enforcement agency about potential danger on the road. Not all vehicles have the same communication capabilities: some have subscription-based SIM cards and long-range communication facilities (e.g. LTE-M) whereas others could only benefit from short-range capabilities within unlicensed spectrum. In this landscape, a communication system takes advantage of a nearby "Internet Vehicle"(IV) to give access to a Leaf Vehicle(LV) (Concepts that has been defined in WP4). In the following figure we illustrate a topology for V2V2I communications:

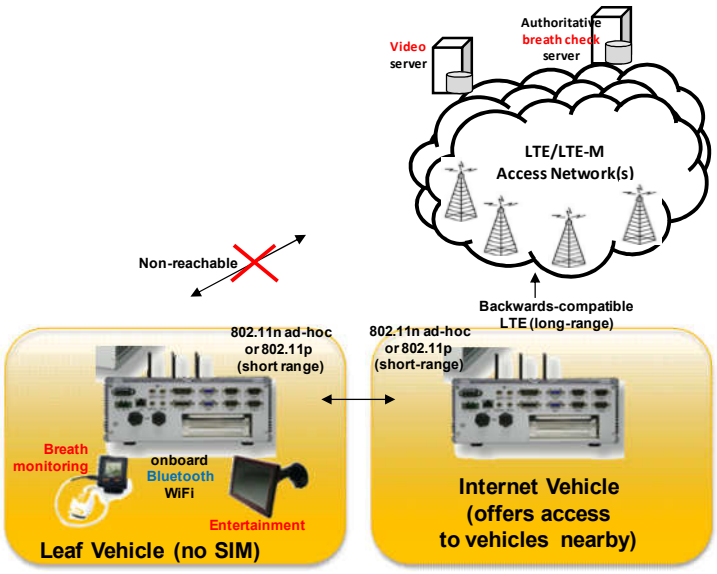

Figure 2—2 Preliminary Demo Concept for ITS

In this figure we depict an LV on the left side, equipped with a breath monitoring device ("breathalyzer") and a brick-class (defined here under on section 4) device offering a number of communication interfaces. This vehicle is not connected to LTE, but connected to an IV which does have a connection to the infrastructure. In the infrastructure, there is an authoritative breath check server.

Another example of use-case in the V2V2I scenario is constituted by vehicle collision detection and avoidance. Pre-collision information is sent instantaneously from the colliding vehicles to other vehicles which may be subject to the shock following wave propagation. Vehicles are connected to the infrastructure with LTE-M and all can receive emergency

information. Further, an enhanced scenario is where vehicles communicate directly and exchange data in a hop-by-hop manner, potentially building a *multi-hop* system. Some vehicles are equipped with a *Gateway* enabled with LTE-M, whereas others use a smaller router using short-range communication. This application will not be implemented in WP7, but the concepts demonstrated are the basis of this scenario.

The following three ITS scenarios will be considered only if time allows.

For remote monitoring of vehicle data, a server in the fixed infrastructure monitors the data emitted by M2M devices deployed in a vehicle. For example, the server may monitor a counter device ("odometer" for path measurement) of a vehicle and alert when a mileage is reached for periodic vehicle safety inspection.

Parking Time Check is an application related to the law enforcement vehicles. A law enforcement vehicle drives along a line of parked vehicles and sequentially queries data from M2M devices deployed in these vehicles. The large vehicle is equipped with a gateway capable to communicate wirelessly directly to the M2M devices of each vehicle: this exchange should be standardized. The communication should be happening even when fixed infrastructure is not available.

The scenario of diagnosis in-vehicle using M2M devices is described as a wireless counterpart to the wired scenario (not implemented here) whereby a technician checks various local points of vehicular health data: fuse state, light bulb state, cable continuity, etc. Use a low-power short-range wireless communication technology to query status data from dedicated M2M devices deployed in a vehicle.

Further information of these scenarios can be found in EXALTED D2.1 document [1].

2.2.2 Smart Metering and Monitoring Scenario

Smart Metering or Advanced Meter Management is more than Automated Meter Reading (AMR). Smart Metering allows for two-way communication between the utility (supplier or DSO (Distribution System Operator)) and the meter. Smart meters are modern, innovative electronic devices capable of offering consumers, suppliers, distribution network operators, generators and regulators a wide range of useful information, enabling the introduction of new enhanced and more effective services. These scenarios are characterizing by providing:

- Accurate measurement of physical parameters, as well as the possibility of acting depending on the value of them. These scenarios cover activities related not only with sensors, but also with actuators.
- A data transmission infrastructure, in EXALTED case, the project aims to adjust the capabilities of LTE networks to M2M particularities.
- The information collected by the sensors will be easily remote accessible. Either directly or through a gateway, each device should provide a method; IP based most of the cases, for accessing them from any location connected to a public network.

Based on the assumptions aforementioned, there exists a plethora of potential applications and use cases associated to this specific scenario. The following sections will offer a deeper insight into their main characteristics, capabilities and the devices involved in each case, focusing on the most interesting ones for being implemented on testbeds.

The selected ones, and the reasons why they have been selected among the wide range of suitable use cases, are the following

- **Energy smart metering.** There are many use cases in smart metering which covers from electricity, water to gas arena, as shown in Figure 2—3. All use cases are relaying on remote resource consumption data collect and on the ability to control devices remotely based on decision flows. Device connectivity is provided through a gateway (energy gateway in the figure), by using this device it is possible to access remotely to all systems integrated, electricity, gas, water, home automation actuators and any device connected to the gateway.

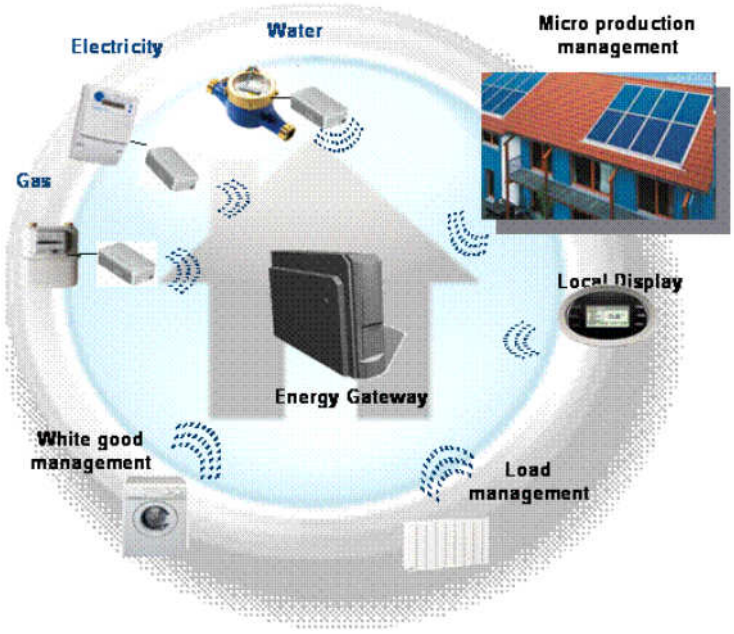

Figure 2—3. Energy gateway ecosystem

(Source: Sagemcom, Energy Department, 2010)

The following benefits are obvious:

- Provide real-time accurate measurements of energy consumption, consumer can therefore adjust consumption behaviours to further save energy
- Provide accurate billing service
- Save supplier's operational cost by eliminating the need to send field technicians to collect data on-site

The selected use case provides further "Green" values by providing a novel procedure to electricity supplier to avoid importing electricity from abroad or starting a fossil fuelled thermal power plant, in case of energy consumption peaks. These temporary electricity consumption peaks can be observed in cold winter, particularly between 6PM to 10PM timeframe, as millions of heaters, ovens, etc are likely to operate at once when households get back to home. Importing energy from abroad or starting an additional power plant to satisfy this instant need has negative impacts on supplier's operational cost and environment.

To avoid this scenario, the system consists in monitoring the global energy consumption. When this latter exceeds a defined threshold, the system will be sending "power cut" orders (based on an algorithm) to selected heaters. Cutting heaters for 10 or 15 minutes does not affect households comfort level. Heaters could be powered off based on a round robin basis so that households are evenly affected in order to prevent the consumption peak to happen. An alternative option is to lower the heating temperature instead of turning the heaters off.

The workflow of this selected use case is described in §2.2.2.1.

- **Hospital Logistics Monitoring.** The logistic monitoring use case is addressed by selecting this scenario. The particular case of Hospitals have been selected as a clear proof of concept can be performed by simulating fluctuations on the stock of medicines (which will be tagged with NFC cards), and how the system can notice them and automatically place orders. Building blocks can be provided by partners without gaps, and the needed knowledge is addressed by some industrial partners offering solutions oriented to this kind of applications.

2.2.2.1 Energy smart metering

This section describes the system and the workflow of the selected novel use case, as described above, for smart metering.

The system is composed of the following components:

1. Energy monitoring central server is connected to the internet. This server manages devices (actuators and smart meters) through gateways.
2. Gateways are connected to the LTE-M network and to the capillary network (e.g. Zigbee) that covers actuators and smart meter
3. Smart meters are connected to the unique gateway in the house (e.g. using Zigbee)
4. Each actuator is linked to a heater. The actuator can turn the heater on or off. This on/off order is sent by the local gateway (e.g. using Zigbee)

The proposed use case supports the workflow as depicted in Figure 2—4:

1. The gateway is reading the smart meter indexes on periodical basis. The retrieved meter index is posted to the central server.
2. The central server gathers metering indexes from all gateway and process the global power consumption. The power cut logic continuously monitors the global power consumption.
3. If the global power consumption exceeds the defined threshold then the central server sends power cut order to actuators to power off heaters. If the global power consumption drops below the threshold then the central server sends power on orders to actuators to resume heaters.
4. Supplier operational staff members can access the control panel of the central server, using a computer connected to the internet. The user can view the current global power consumption, view/edit the threshold, trigger manual a power cut on a selected actuator (heater)

The selected use case fulfils the following requirements:

1. Device management protocol with evidence of small payload. This has positive impact of system scalability and device power consumption
2. Device plug and play mechanism may be demonstrated. This include device bootstrapping

The selected use case can be emulated by the testbed with the following assumptions and limitations:

1. Physical smart meters and heaters may not be available
2. Heaters can be emulated by lamps. Turning the light off is equivalent to turn the heater off.
3. Smart meters can be emulated by sensors (e.g. temperature sensor, accelerometer). High energy consumption can therefore be emulated by heating up the sensor or shaking the accelerometer

Based on these assumptions and limitations, the testbed is further specified in section 4.

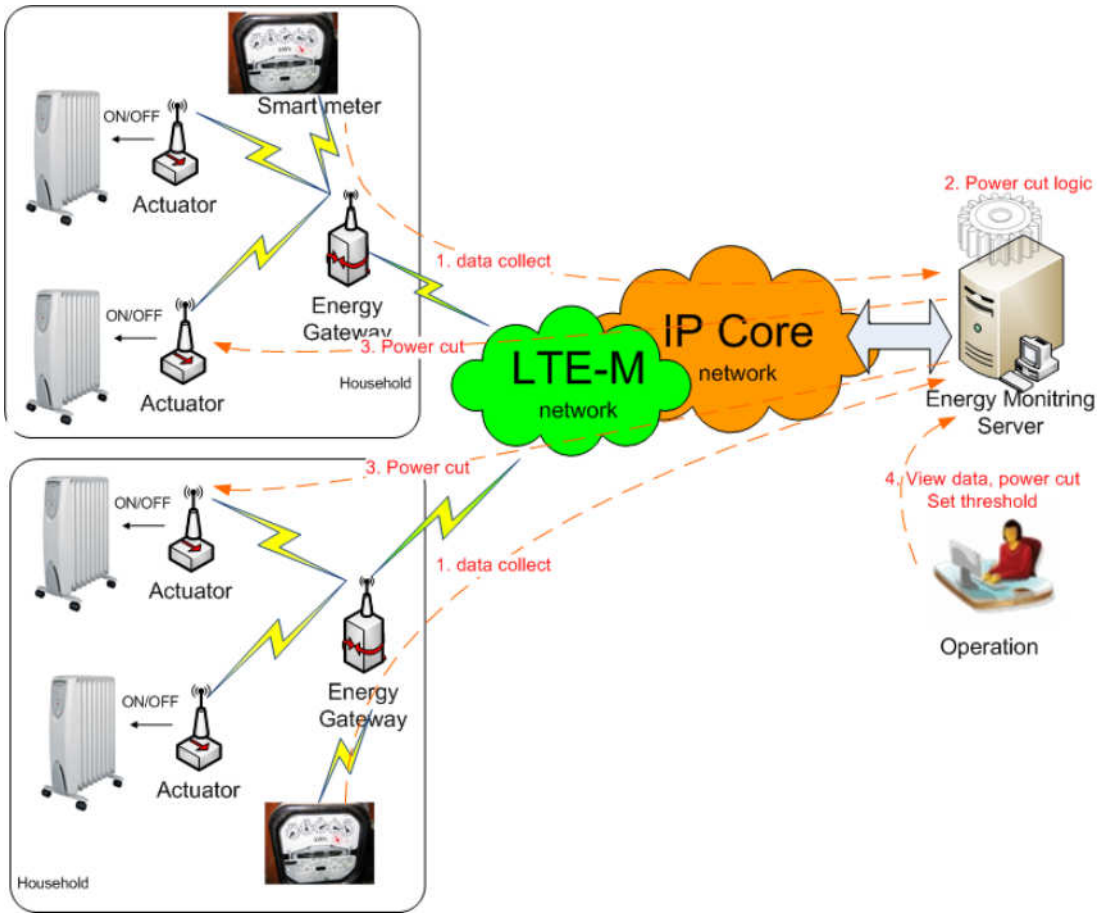

Figure 2—4 Smart metering use case workflow

2.2.2.2 Hospital Logistics monitoring

Current logistics systems in hospital environments are usually supported using large dedicated equipment. Although the automation processes in logistics mean great advance, it is still necessary to consider many other aspects in order to enhance the overall system performance. In this sense, the design of these proprietary systems does not fulfil all the demands of the sector. Scalability has been stated as a key issue to be addressed on these systems, always taking into account other aspects as the cost of the overall system.

The already available smart devices seem to be the optimal solution to this issue. By combining the potential of the already existing solutions, integrating them with multiple heterogeneous communications technologies in a smart low cost device, it is possible to fulfil the requirements imposed by hospital environments and provide flexibility to adapt the system to final user demands

Nowadays taking advantage of the efforts done in the field of M2M communications and the progress done by scientific community towards IoT paradigm, it is possible to create a scalable system based on smart devices. The possibilities offered by the combination of both concepts have been exploited in the system we are proposing.

The scope of the proposed system is to create a platform for improving the performance of current logistic system by exploiting the possibilities of current IT technologies. This proposal combines the benefits of emerging and well proven technologies such as ZigBee, cellular networks and NFC, this heterogeneity represents a huge advance in this kind of

deployments, as it allows spreading the different equipment over the whole area to be monitored and analyzed. Its scope is the optimization of requesting and delivery processes by using simple devices, and forming an autonomous environment.

Additionally, NFC has been implemented for triggering the events generating the messages that have to be sent to the application server.

Figure 2—5 presents the system architecture, with three main components:

- End devices, smart devices forming capillary networks or directly connected to a public network. They generate messages enclosing stock or other relevant information to be analyzed in the application server side in order to perform specific actions.
- Gateways, these are the points that perform the actions needed for connecting external application queries to the different devices inside a capillary network.
- Application server, in this case a Logistics Management Server. Central point of the system that keeps the intelligence makes the decisions and performs actions based on the information received from the various nodes distributed on the hospital, both end devices and the ones in the core network.

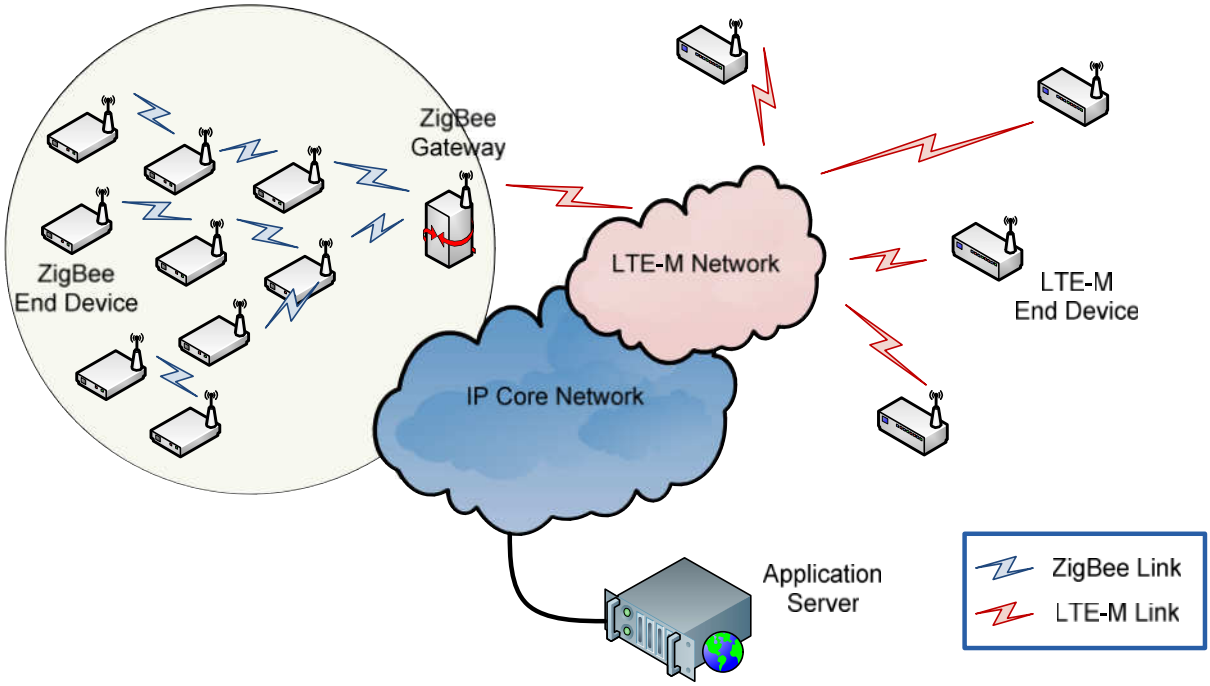

Figure 2—5. Overall System Architecture

The architecture presented is ETSI compliant and the underlying communication technologies do not affect to the concept of the elements composing the overall system. For the LTE-M network emulation, as it could not be possible to build the testbed with this technology, other 3G/3.5G cellular network will be used.

2.2.3 E-Health Scenario

Remote health-care poses a vast range of M2M applications, such as remote monitoring in hospitals, clinics, and patient homes (Figure 2—6), expected to play a key role in the future M2M market. Device internetworking for such medical/healthcare scenarios is particularly important, especially for cases where certain functions have to be performed over large areas, harsh operating conditions, or other restrictions.

Source: ETSI

Figure 2—6. Envisaged application of e-health scenario

Towards the deployment of this kind of M2M application, it is necessary that sensors can be autonomous, thus posing the requirement of extreme energy-efficiency. The patient should not be tied up to recharging all the sensors continuously. In addition, the performance of these systems might be very variable. While some measurements are not time-critical, some other sensors might be able to immediately transmit an alarm when an unexpected event occurs.

The E-healthcare scenario will be used to verify some requirements of EXALTED:

i. *High energy efficiency:* battery life is essential in such applications, since it may be the only source of power for certain applications. Energy efficiency techniques and sleep-methods are important for these scenarios. Alternative power sources, e.g. solar energy or kinetic energy may be also be efficient solutions.
ii. *Continuous connectivity:* for critical applications (e.g. pulse monitoring)
iii. *High reliability:* for critical applications.
iv. *Wide connectivity range:* monitored persons may move to any geographical area.
v. *Possible high mobility* (e.g. monitored patients on a moving vehicle).

2.2.3.1 Envisaged use cases

Europe is an ageing Continent and along with old age chronic conditions such as cardiovascular diseases (CVD), diabetes mellitus type 2 (DMT2) and pulmonary conditions most prominent amongst them Chronic Obstructive Pulmonary Disease (COPD) afflict a geometrically increasing population hence one of the main challenges faced by most National Health Systems is the need for increased efficiency when treating chronic patients. Key element for the so much sought for efficiency is the drastic reduction of the number of unnecessary visits to hospitals without even once jeopardizing the concerned patients' safety.

M2M enabled health care will allow patients to stay at home or move freely out and about with the confidence that they are being monitored from a team of treating physicians at the hospital or at the nearest health care unit. Different measuring sensors placed along the home, inside the car or even worn by the individual will obtain vital data from the patient, such as blood pressure, ECG, temperature, respiratory rate, position, acceleration per axis,

etc. In the case that a critical event occurs, an alarm will be triggered and a treating procedure will be initiated based on the plethora of data accumulated over time.

Towards the deployment of this kind of M2M applications, it is necessary that sensors can be autonomous, thus posing the requirement of extreme energy-efficiency. The patient should not be tied up to recharging all the sensors continuously. In addition, the performance of these systems might be very variable. While some measurements are not time-critical, some other sensors might be able to immediately transmit an alarm when an unexpected event occurs.

As shown in Figure 2—7 of the envisaged application the medical sensors encapsulated in different devices with appropriate user machine interfaces constituting a Personal/Body Area Network (P/BAN) transmit through a short range wireless communication protocol (e.g. Bluetooth) the acquired vital data to a master station equipped with LTE capabilities and from there over internet they are available to a physician.

More or less the same configuration could be used for enhanced mobility i.e. the patient travelling by car and his/her P/BAN transmitting to a master station installed somewhere in the vehicle's console. The only limitation to this variation is imposed by the clinical value of the measurements i.e. while driving it is of no importance to perform oxygen saturation measurements etc.

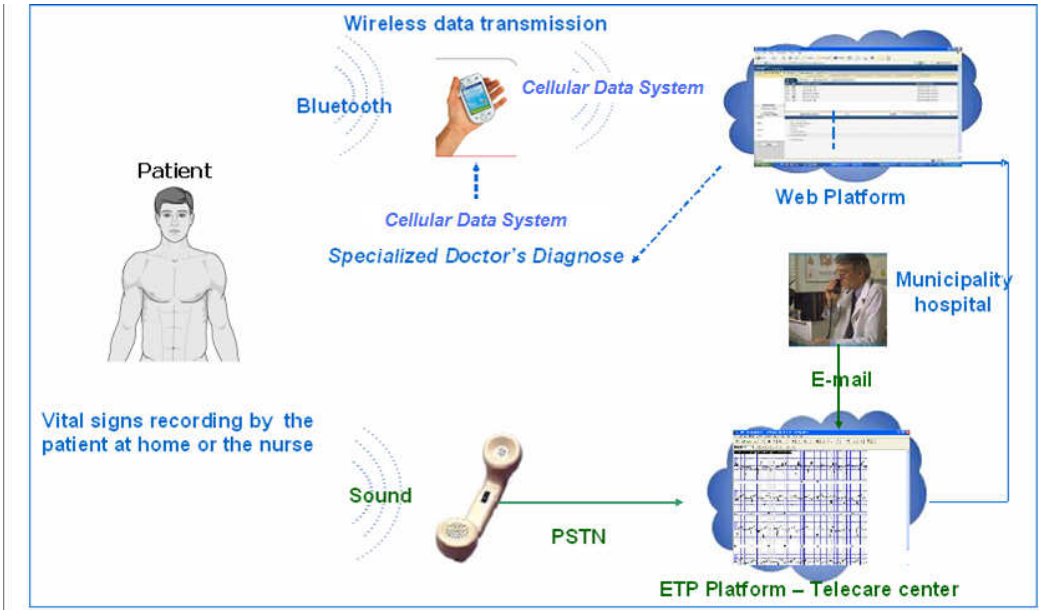

Figure 2—7. Envisaged application of medical sensors encapsulated in different devices

Summing it all up the architecture of the proposed system consists of three main levels:

- Special devices capturing vital signs (ECG, spirometer, oxymeter, blood glucose, blood pressure) using Bluetooth as a capillary network. Under a strict protocol as defined by a physician they provide information on the individual's health status
- Gateways in the form of PDAs gathering all data from the devices through the capillary network and they transmit them to the infrastructure. Communication between the devices and the gateways is bidirectional.
- Telecare server where all the acquired data / vital signs from the individuals are gathered and the physician can monitor their health status hence providing for efficient consultation.

For efficient and reliable use of sensor devices and M2M communications in health care domain, Exalted project will investigate and develop solutions that enable energy-efficient, autonomous and reliable sensor device deployment in medical, patient and elderly care scenarios. The main focus will be on ease of use, autonomous processes, prioritised and emergency communications, event detection, effective M2M communication for the devices and sensors, and intelligent mechanisms to support reliability and consistency for the M2M communications.

3. Testbed Overview

The EXALTED project aims at advancing towards the definition of a conceptual unified architecture that expands the existing LTE architecture in order to support M2M applications and services in an efficient manner. The methodology for achieving this goal includes the implementation of three testbeds, each one dedicated to a different Proof of Concept (PoC) in the broader scope of the project.

This section of the document summarizes the work done so far within WP7 and outlining the scope and special features that they will implement. Each of the three envisaged testbeds is roughly described by its architecture.

3.1 TESTBED 1: LTE-M testbed

With Testbed 1, we will validate LTE-M PHY layer algorithms, namely the LTE-M radio access methods Generalized Frequency Division Multiplexing (GFDM) and Code Division Multiple Access (CDMA) that we also study analytically and with link level simulations in WP3. They are described in [2]. We will demonstrate that the predicted spectral behaviour of the LTE-M waveform that we propose in WP3 can be actually be achieved and that the signal can be decoded successfully after a transmission over a real radio channel. Further we will demonstrate that the effect on the legacy LTE signal utilizing a different part of the same frequency band complies with our simulation analysis in WP3.

Figure 3—1 shows the landscape of the overall EXALTED system architecture and the sub-system (accentuated with a blue shaded ellipse) that will be considered in the LTE-M testbed.

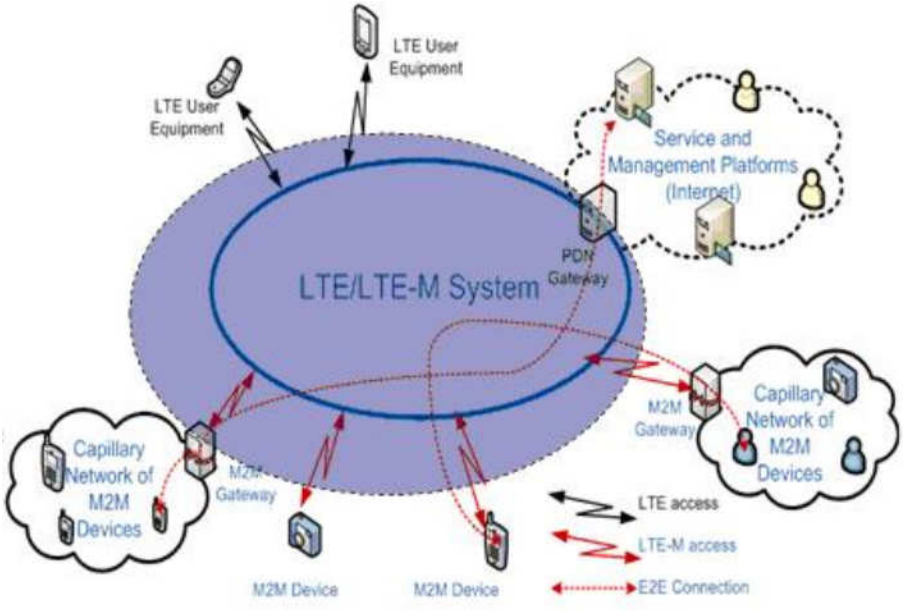

Figure 3—1. Overall EXALTED system architecture and LTE-M radio access (in blue)

For the evaluation in the testbed we will utilize presumably the following Key Performance Indicators (KPI). This list reflects our current knowledge after the first project year and may be subject to future refinements. The achieved measurement results will be compared against analytical assessments and link level simulations in WP3.

- Bit Error Ratio (BER) at the output of the decoder.
- Peak-to-Average Power Ratio (PAPR): Ratio of peak power and average power of the transmitted signal in the time domain.
- Out-of-band radiation (OOB): Power spectral density outside the allocated radio resources.
- Throughput: Number of successfully received bits per time unit in bit/s.

Besides the pure performance analysis of the LTE-M air interface itself, the measurement campaign will also include an assessment of the impact of LTE-M transmissions on legacy LTE users.

As testbed 1 will validate only basic PHY layer functionality within the LTE-M system, a mapping of the testbed set-up to one particular application, service or use case is not possible. The features that we can show with this testbed are comparably valid for all of the use cases explained in section 2.

The following description will give a more detailed insight in the set-up of the testbed, its components and its advantages compared to link level simulations and theoretical analysis done in WP3.

The “classical” approach for the analysis of PHY and MAC functionalities in communication networks is the use of a computer-based link-level simulation chain as shown in Figure 3—2.a. In this figure, it is shown that the transmitting and receiving processes, as well as the low-pass channel response, are simulated by means of software modules. However, in several cases software simulation has its limitations in terms of accuracy (correlation with real world behaviour) and efficiency (e.g., time-cost). For example, the equivalent low pass channel models implemented in C++ or MATLAB [5] consume the majority of the overall computation time in the simulation chain, thus taking a long time to obtain statistically meaningful results.

A possible solution to overcome the high time-cost of software simulation is the use of the Signalion’s ***Hardware in the Loop (HaLo)*** [6]. The use of HaLo makes the simulation much more efficient and reduces the computation time significantly. As it is shown in Figure 3—2.b, the use of HaLo modules simply replaces the software model of the channel by a real radio frequency channel over the air. This second approach will be adopted in EXALTED for testbed 1. The transmitter part is implemented with the customizable HaLo concept while the receiver used for the testbed is a configurable Signalion Sorbas System [7] capable of receiving and storing the transmissions from the channel.

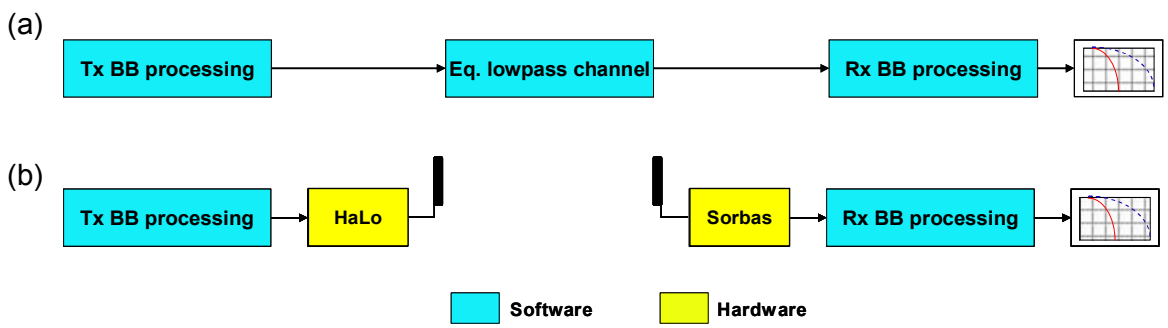

Figure 3—2. Performance evaluation with (a) link level simulation chain and (b) HaLo over the air replacing the software channel model

A detailed description of the testbed is included in Section 4.1 of this deliverable. In that section, the relevant technical requirements extracted from [1], as well as the novelties introduced in this testbed are described. In addition, the general architecture, its building blocks and the interfaces between these functional units are also described in Section 4.1. Finally, an anticipated timeline and the milestones of the testbed implementation conclude that section.

3.2 TESTBED 2: Connectivity Oriented testbed

The purpose of the connectivity oriented testbed is to demonstrate capillary network concepts and E2E connectivity. Capillary networks will be composed by a group of nodes, provided by partners involved in this WP, with limited communication capabilities composing ad-hoc networks and accessing to the core network through a gateway equipped with an LTE-M interface. The concepts that will be proven in this testbed will be further explained in Section 4.2.

The goal of this testbed, as shown in the Figure 3—3, is to demonstrate E2E connectivity between M2M devices, not only belonging to the same capillary network, but also to different ones connected to LTE/LTE-M network.

The specific Proof of Concept tests that will be carried out with the connectivity oriented testbed are subject to the availability of an LTE-M network (or any other suitable cellular network) at the deployment time of the testbed.

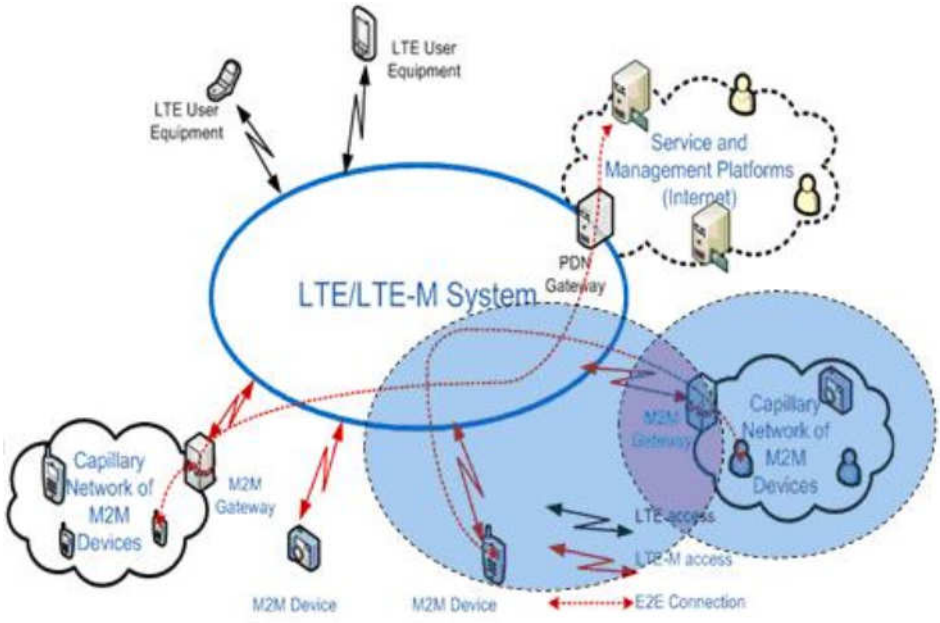

Figure 3—3. Connectivity Oriented testbed overview

Three different application domains with their respective scenarios will be investigated in terms of connectivity and M2M devices characteristics.

Each scenario has its own characteristics and they are summarized here below. Although they were already presented in detail in D2.1 in the section devoted to the description of use cases and business models, the focus herein is on testbed implementation issues and EXALTED key techniques that will be demonstrated. The application areas that are listed below are escorted by a breakdown of characteristics to be demonstrated.

1) Intelligent Transport Systems (ITS)

i. *Wide connectivity range*: covering large geographical areas.
ii. *Techniques for large number of devices*: this scenario will serve to study the following features in the testbeds:
    d. Multicast and broadcast capabilities.
    e. Advanced scheduling protocols.
    f. Advanced resource allocation techniques.
iii. *High scalability*: new connections should not cause any problems.
iv. *High mobility*: since the devices are attached on vehicles, high mobility is expected.
v. Autonomy: the nodes will be able to create independent networks, in order to provide backup connectivity to other nodes. Multi-hop communication may also be used.

2) Smart Metering and Monitoring

i. *High energy efficiency:* battery life is essential in such applications, since it may be deployments remotely controlled aimed to be not visited by human in long periods of time. Energy efficiency techniques and sleep-methods are important for these scenarios. Alternative power sources may be also be efficient solutions.
ii. *Techniques for large number of devices.* Several solutions require large number of monitoring points so the system should allow these kinds of topologies. In order to provide communication capabilities similar to the ITS case, the following characteristics should be considered:
    a. Multicast and broadcast capabilities
    b. Advanced scheduling protocols.
    c. Advanced resource allocation techniques.

3) eHealth

vi. *High energy efficiency:* battery life is essential in such applications, since it may be the only source of power for certain applications. Energy efficiency techniques and sleep-methods are important for these scenarios. Alternative power sources, e.g. solar energy or kinetic energy may also be efficient solutions.
vii. *Continuous connectivity:* for critical applications (e.g. pulse monitoring)
viii. *High reliability:* for critical applications.
ix. Wide connectivity range: monitored persons may move to any geographical area.
x. Possible high mobility (e.g. monitored patients on a moving vehicle).

3.3 TESTBED 3: Device Management testbed

The purpose of the Device Management (DM) testbed is to demonstrate the capability to manage LTE-M enabled devices as well as non-LTE-M enabled devices. The different management actions that will be considered in EXALTED project are covered by the following use cases:

- LTE-M Enabled M2M Device Provisioning on the Device Management Server.
- LTE-M Enabled M2M Device Bootstrapping.
- Sensors/Actuators plug-n-play to the Gateway, association information sent to the Server.
- Sensors data collected and aggregated by the Gateway and then sent to the Server.
- Sensor can be remotely controlled by the Server.
- Device diagnostic can be triggered remotely by the Server.

The testbed should allow the user to perform management of the connected device(s) via a server where various kinds of actions, belonging to the aforementioned use cases, and data exchange connectivity can be performed by using the communication infrastructure developed in the project.

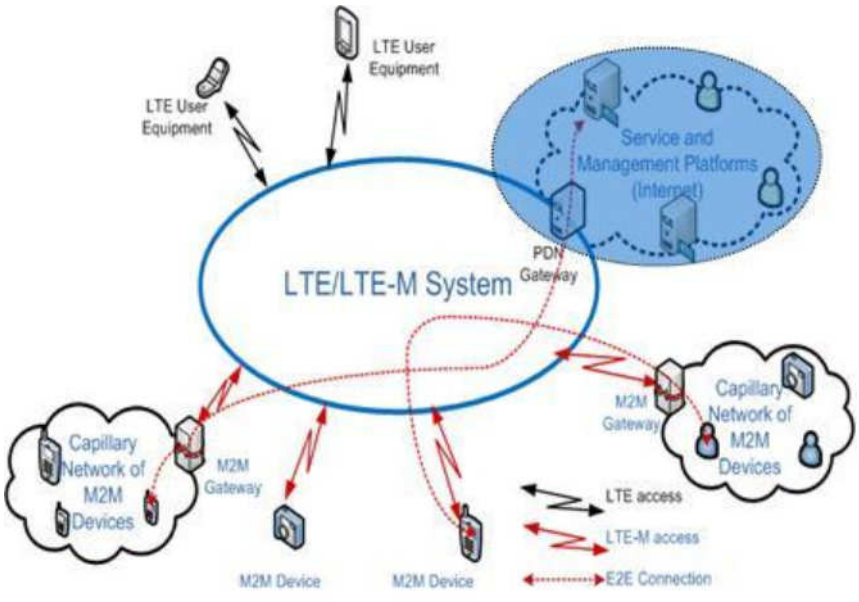

Figure 3—4. Device management testbed overview

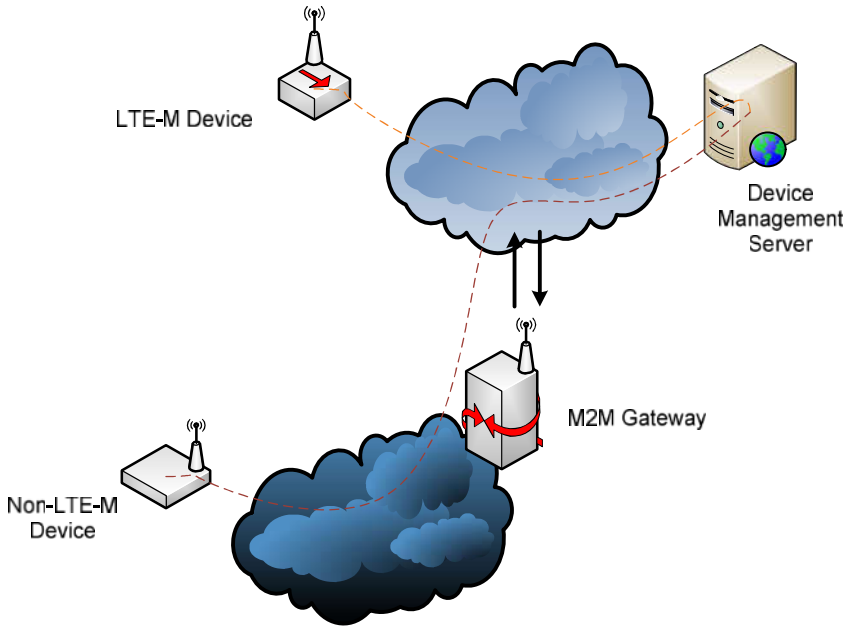

Figure 3—5. Connectivity with Device Management Server in LTE-M Network

The following three scenarios will be demonstrated by the testbed:

1) Connectivity between non-LTE-M devices with the Device Management server, including demonstration of event handling and data exchange between the M2M device and the Device Management server. In this scenario, the Non-LTE_M Device connects through a capillary network to an M2M Gateway that provides connectivity to the LTE-M system.
2) Connectivity between LTE-M device with the Device Management server, where data connectivity is initiated by the Device Management server (push mode)
3) Connectivity between LTE-M device with the Device Management server, where data connectivity is initiated by the LTE-M device (pull mode)

4. Specifications

This section will describe in more detail the testbed definition. It is expected to provide a detailed description of the testbeds that will be implemented, including how the elements that compose them “fit together”, and an application that enforces the position of the novelties developed by EXALTED.

4.1 LTE-M testbed

4.1.1 Requirements and novelties

The novelty of this testbed is primarily to demonstrate the functionality of LTE-M PHY and MAC algorithms that are currently developed in WP3. Therefore, only a small subset of the technical requirements described in D2.1 can be evaluated with the testbed without additional analytical assessment. Those items that have impact on the testbed implementation are summarized in Table 4—1.

Table 4—1: Technical requirements

ID	Title	Priority
FU.2	Efficient spectrum management	Mandatory
SV.1	Overall QoS concept	Mandatory
NT.2	LTE-M backward compatibility	Mandatory
NT.3	Minimum number of modifications in network infrastructure	Mandatory
NT.5	Half duplex transmission mode	Medium
NT.17	Reduced signalling	Mandatory
NF.1	Scalability	Mandatory
NF.2	Energy efficiency	Mandatory

4.1.2 Architecture

As mentioned in Section 3.1, the main benefit of a HaLo-system is the acceleration of the required computation time, because a software based channel model is not needed anymore. Therefore, Figure 4—1 can be seen as the first approach for the architecture of the testbed. We have a transmitter for signal generation and a receiver for signal analysis, both implemented in MATLAB. The HaLo Tx module converts a MATLAB array in a physical transmit signal that propagates over the air. The Sorbas Rx module reconverts the received physical signal to a MATLAB array. In order to prove backward compatibility to LTE, an LTE-Advanced UE will also be included in the testbed. This is possible, because the radio resources can be shared among several users. For example, one part of the frequency band can be utilized for legacy LTE access and the other part for LTE-M. Figure 4—1 illustrates this extension.

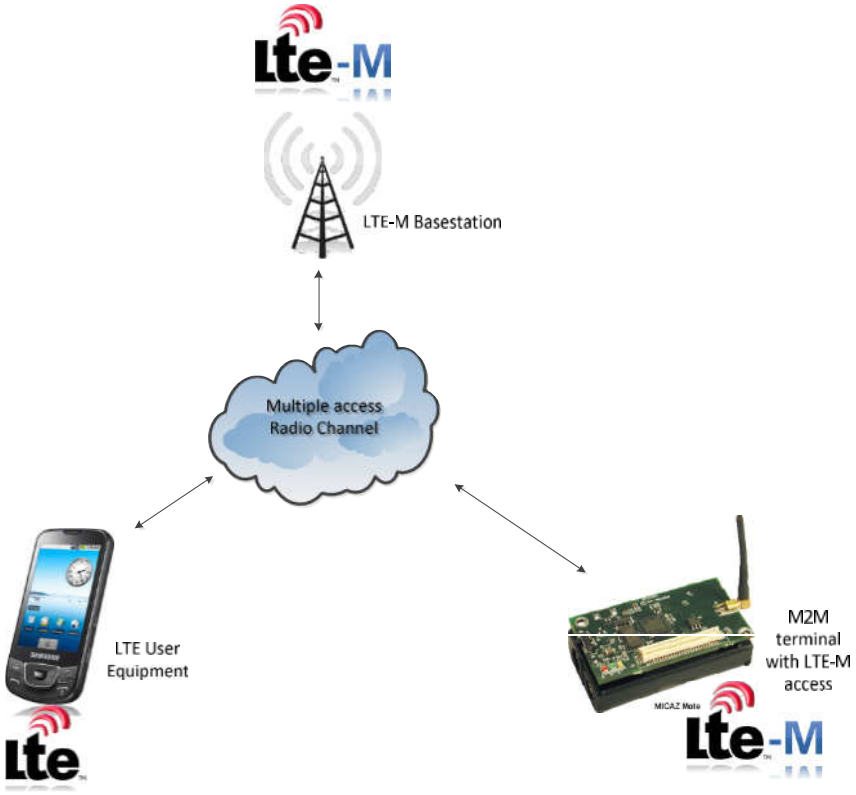

Figure 4—1. Principal LTE-M testbed architecture

Before selecting an LTE-M algorithm to be implemented on the testbed, the following constraints have to be considered:

- Non-real-time capability. As the transmitter and receiver functionality are based on a software model, the signal processing in the testbed is slower than in the real-time, i.e. the processing of an OFDM symbol takes longer than the actual duration of the symbol. This raises constraints for the implementation of some algorithms, in particular if they rely on channel measurements and a respective feedback mechanism.

- Frequency band: The hardware has fixed capabilities of supporting certain frequency bands which results in limited possibilities of communicating to other hardware blocks.

- The memory is limited.

Once a suitable LTE-M algorithm is chosen (e.g. by evaluating a secondary waveform for LTE-M radio access), implementation is done on the HaLo prototyping platform using the MATLAB API. After the implementation of a selected algorithm, the transmission chain between an LTE-M terminal and an LTE(-M) base station and, a UE and an LTE(-M) base station can be setup. The procedure for a validation of the algorithm is a joint reception of the transmissions from the LTE UE and the LTE-M terminal (using e.g. the secondary waveform) at the base station. The received data in a form of baseband samples can then be interpreted offline in a post processing stage that incorporates the MATLAB toolset also on the receiver side. Therefore, the receiver algorithms at the base station can also be implemented keeping in mind the hardware and real-time restrictions. Certain metrics for validation can then be evaluated regarding the specific algorithm, e.g. bit error rate. This is

possible for the secondary system, which is the LTE-M terminal. The primary system which is the LTE(-Advanced) transmission chain can also be evaluated in a similar manner.
The basic testbed setup can be seen in Figure 4—2.

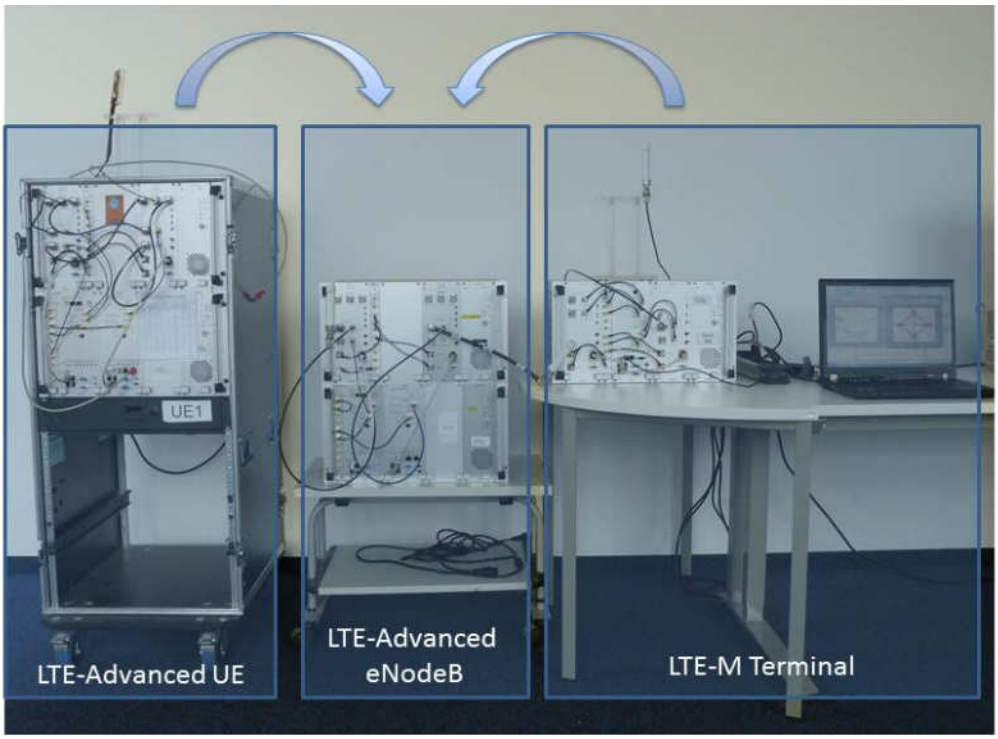

Figure 4—2. Testbed setup within the TU Dresden labs (not all interconnections shown)

4.1.3 Building Blocks

The testbed consists of the following basic components:

- LTE-M terminal, further explained in section 4.1.3.1.
- LTE(-Advanced) UE, depicted in more detail in section 4.1.3.2 .
- LTE-M base station that is an LTE(-Advanced) eNodeB supporting LTE-M, described in section 4.1.3.3.

4.1.3.1 LTE-M terminal

LTE-M is being defined during the EXALTED project. Therefore, we cannot use an available commercial terminal in this testbed, but instead we will use the hardware platform described below to validate LTE-M PHY and MAC layer algorithms.

The LTE-M terminal is a vital part of the testbed, as it comprises the functionality of the M2M devices and/or M2M gateways within the scenarios of M2M communication. It includes the interoperability to the LTE-M system, which means interfacing to the air interface of the LTE-M base station.

Within the testbed, this building block is represented by the so-called HaLo platform, which is hardware in the Loop Prototyping & Monitoring Platform that supports diverse transmission modes. It is equipped with a powerful API, written within and for MATLAB to use. For the transmission, the MATLAB offers the interface to the HaLo box on a time sample basis. So within the implemented MATLAB algorithm model the data can be processed in software until real time samples are at hand, i.e. the complete transmit signal processing functionality like

coding, interleaving and modulation is included. The software modules can easily be exchanged, for example modules generating a Generalized Frequency Division Multiplex (GFDM) waveform can be replaced by modules generating Code Division Multiple Access (CDMA) samples. In the testbed, they will be executed on a separate laptop.

By transmitting the samples to the HaLo Box via API (right yellow box in Figure 4—3), the transmission over the channel starts. The sample rate of the system is scalable between 5MHz and 20 MHz (and under restrictions of 40MHz). As the API supports the upload of pre-processed data to the HaLo Box, any real-time ability is not supported. Every upload of data includes a hardware processing delay.

4.1.3.2 LTE Advanced UE

An important ability of the LTE-M system is the backward compatibility to the LTE standard in order not to impact already deployed LTE users. A legacy LTE user requires a high throughput connection to the base station in order to satisfy the QoS needs for services like media streaming and internet access. The LTE UE therefore sets up a connection to the base station using the LTE(-A) radio interface.

Within the testbed this building block is represented by the LTE(-Advanced) UE of the LTE(-Advanced) transmission chain based on the Signalion Sorbas hardware (see further description in Section 4.1.3.3).

4.1.3.3 LTE Advanced eNodeB

The LTE-M/LTE-A base station is the counterpart to the LTE-M terminal and the LTE Advanced UE. It receives the uplink signalling from both LTE-M terminal and LTE Advanced UEs including the payload from M2M terminals, such as measurement data, etc. according to a certain use case like e.g. eHealth.

Within the testbed, this building block is represented by the Sorbas LTE(-Advanced) base station which incorporates a fixed, configurable implementation of the LTE(-Advanced) physical layer. It includes the communication between an LTE Base station (eNodeB) as one building block and an LTE User Equipment (UE) as another building block. The transmission chain can be configured through a software tool provided by Signalion.

The LTE-M base station includes the respective receiving signal processing units like demodulation, deinterleaving and decoding (upper left part of Figure 4—3). Similar as in the transmitter, the individual processing software modules can be exchanged within MATLAB. Hence, the bit error rate performance of different algorithms can be compared. In the testbed, the receiving algorithms and the performance evaluation are executed on a control laptop.

4.1.4 Interfaces

In the following text, the interfaces between the individual components of the testbed are described. As can be seen in Figure 4—3, the building blocks of the testbed are interconnected in a twofold way. One connection contains the control information needed for proper work of the components. In the setup this is accomplished either via Local Area Network (LAN) IP-based connection for the LTE(-Advanced) transmission chain, or Universal Serial Bus (USB) in case of the HaLo Prototyping platform. While the LTE(-Advanced) transmission chain is only configurable, the HaLo Prototyping platform is programmable from a Laptop via USB.

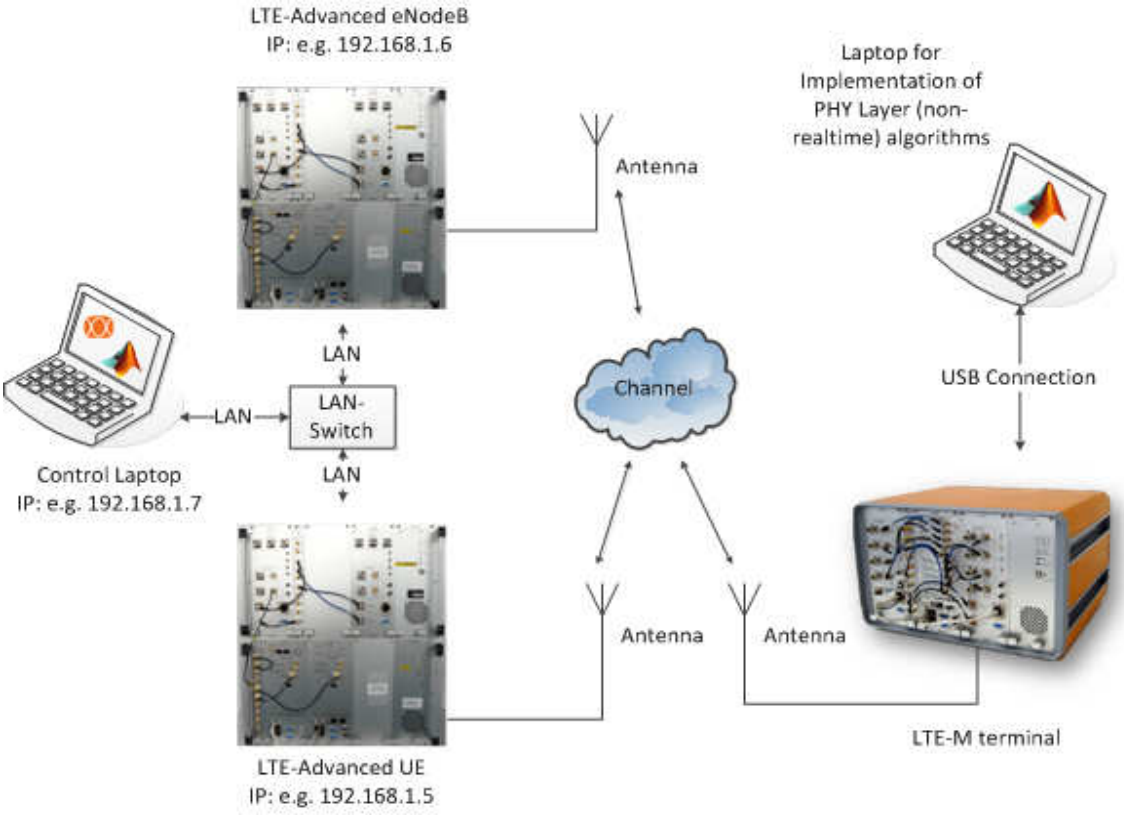

Figure 4—3. Schematic testbed setup with Signalion Hardware

The by far most important interface they all have in common is the LTE-M radio interface, which is the key component of the testbed.

All building blocks of the testbed transmit and receive on the same frequency band, which allows for an integration of the LTE(-Advanced) transmission chain with the HaLo prototyping platform. The data handled on that interface is not derived from higher layers and therefore transmission in the testbed can be handled in an abstract fashion, not related to any use case or scenario.

4.1.5 Timeline and milestones

The first intermediate milestone is the implementation of an LTE-M link-level simulation chain that allows an initial performance assessment of different LTE-M PHY and MAC algorithms. This task has been almost completed. Afterwards, a selection of promising algorithms according to this initial performance assessment has to be done. The selection has to consider also the capabilities and constraints of the testbed. Single software modules, e.g. the coding and decoding, will be extracted from the simulation chain and integrated in the testbed according to the given interfaces. The last milestone, at the end of the EXALTED project, will be the operation of the complete testbed as well as a detailed performance evaluation complemented by analytical assessment. These dates are summarized in Table 4—2.

Table 4—2. Timeline and Milestones for Testbed 1

Milestone	Description	Envisaged Completion
M1.1	Implementation of an LTE-M link-level simulation chain	M12

M1.2	Selection of promising algorithms	M24
M1.3	Set-up of the testbed	M24-M27
M1.4	Operation of the complete testbed and detailed performance evaluation.	M30

4.1.6 Scenario mapping

Requirements from each scenario have been classified and quantified; the ones that fit best with this testbed are listed on the following Table 4—3.

Table 4—3: Requirement quantification from scenarios regarding testbed 1.

M2M Network			**Justification**
Deployment architecture	Device-to-device communication	YES	O4.5 DoW: Design an IP based E2E networking system for M2M communications. Enabling interactions between end M2M devices.
	Infrastructure-to-device communication and vice versa	YES	O4.1 DoW. DM operations requires communication in both directions, being contactable all devices in a capillary network. ETSI requirements for DM.
	Hybrid architecture, devices-to-cluster head	Possible	O4.4 and O4.1 of DoW. Energy optimization approaches focus on clustering as a mean of aggregate traffic reducing overall consumption. Based on this principle it is mandatory to support this communication.
	Note: Testbed 1 doesn't include real devices or infrastructure hardware, but signal generators and signal analyzers, in which the functionality of real devices and infrastructure hardware is partly implemented (only PHY layer). It is a question of configuration, which kind of device is represented. In principle all single-cast communication types in the EXALTED architecture can be realized.		
Communication type	Simplex	For low complex. apps	Do not fulfill ETSI M2M TS102689 Requirements. Require bidirectional communication in order to address DM requirements.
	Peer-to-peer	Possible	Functional Requirement from ETSI TS102689 Req. 6.9 demands path diversity
	Note: Testbed 1 consists of equipment that can either transmit signals or receive signals. It is a unidirectional link to evaluate basic PHY layer algorithms offline (not in real-time)		
Device capabilities	MIMO	POSSIBLE	Low complex MIMO or MISO schemes can be used for range extension. Antennas are available at the base stations anyway.
	Data rate requirements	<10Kbps	• Typical monitoring applications. 1 param, 1 measure/hour, including all layers overhead supposes a data rate of 0.189 bps/ device. • In case of CPL the current requirement is <20Kbps • In case of WMBus EN13757 the current rate is <2.4Kbps
	Bandwidth usage	<50KHz	EN 13757 current implementation gives 12,5KHz of bandwidth.

Miscellaneous	Interference management	YES	Interference management is closely related to energy efficiency, which is one key objective of EXALTED. This is valid for all use cases.

M2M to Gateway			**Justification**
MAC	OFDMA, CDMA, TDMA, Hybrid.	DPCF and PRCSMA	T4.1 defines two novel MAC protocols addressing EXALTED objectives regarding high number of devices, energy efficiency and packet congestion.
	Note: Testbed 1 is not limited to the abovementioned requirements derived from the use cases. Also alternative, not yet commercialized radio access methods like Generalized Frequency Division Multiplexing (GFDM) can be realized.		

Gateway to Infrastructure		**Justification**
Access	LTE-M, GPRS/3G	Current implementation of AMR (Automatic Metering Reading)
	Note: Only a part of the LTE-M PHY layer can be implemented in Testbed 1	

4.2 Connectivity Oriented Testbed

This scenario will be focused on demonstrating the novelties developed in two main fields, on the one hand, the concepts developed within capillary networks, and on the other hand, providing end-to-end connectivity between M2M devices, not only belonging to the same capillary network, but also from different ones connected to the LTE/LTE-M network.

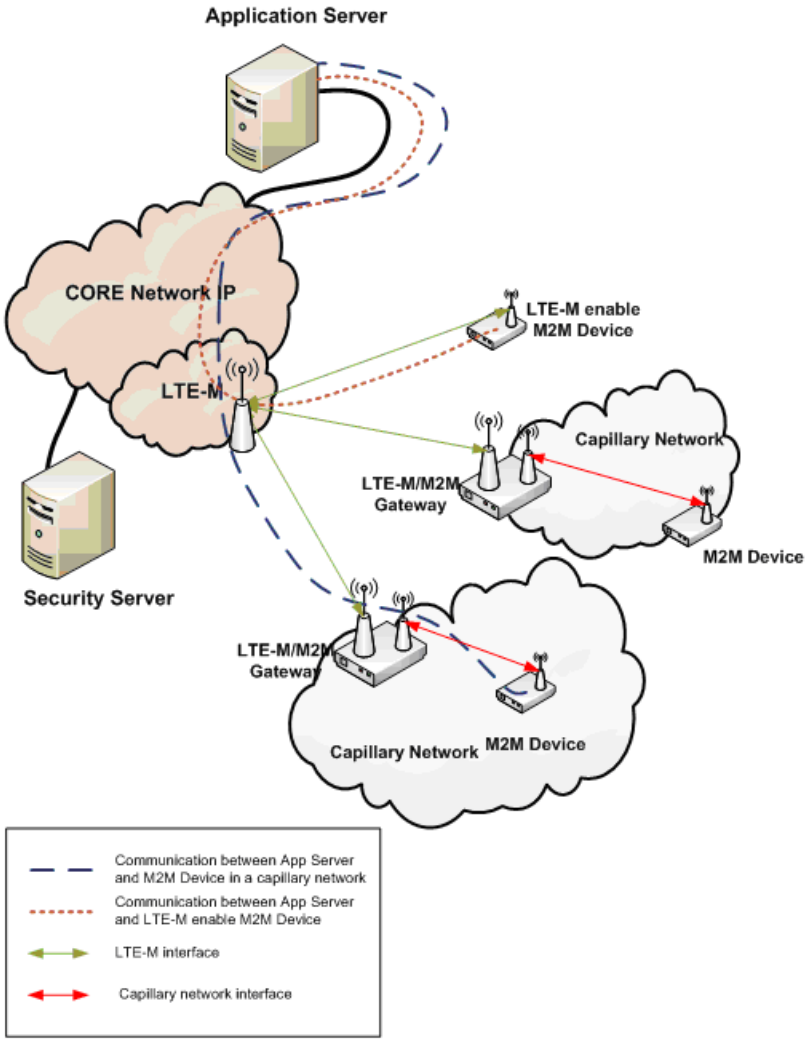

Figure 4—4 Connectivity oriented testbed overall architecture

Figure 4—4 shows the focus on this testbed in the framework of the overall EXALTED architecture. For the definition of building blocks and the testbed itself, it is assumed that the envisaged LTE-M network will be available to be proven by the time the testbeds are deployed. If it is not possible, due to technological or time constraints, some other cellular network will be selected in order to make the PoC tests. The following subsections will describe the different modules that will compose the testbed, the interaction among them, and also all the novelties introduced by EXALTED and demonstrated in this particular testbed.

4.2.1 Requirements and novelties

This Proof of Concept is focused on the provision of E2E connectivity among different entities regardless of their location. There is a set of requirements that this test will fulfil in order to demonstrate the EXALTED project achievements. Table 4—4 and Table 4—5 summarize the challenges that will be addressed.

Table 4—4 General Architectural Requirements

Category	To demonstrate	Impact on testbed
Deployment architecture	Multi-hop	Several devices must be implemented on the testbed, and retransmission between nodes should be proved and tested.
Transmission mode	Half-duplex	Devices integrated in this scenario must be able to both transmit and receive data/commands from the network.
Data Compression	High data compression	Aggregation mechanisms are under study in WP4. If possible, some of them shall be tested with real devices.
Energy efficiency	Energy efficient routing and MAC protocol	The devices integrated on testbeds must be energy aware and low power.
Delay / Real-time interactions	Real-time interactions Delay-tolerant	Depending on the application tested, devices should support both real-time and non real-time operations. If possible, PoC of both applications should be implemented.

Table 4—5 Specific E2E Connectivity Requirements

Category	To demonstrate	Impact on testbed
Addressing scheme / NAT	Flexible addressing schemes, including IP address of connected devices, IP address of groups of , E.164 addresses of connected devices	IP protocols shall be implemented on devices included into this testbed, in order to enable partners' protocol researches. If this is not possible due to constraints on devices, address translations shall be implemented on gateways.
Reliability	Reliable delivery of a message Notification of any failure to deliver the message Notification of failure in demand-response communications between sensor and actuator	Mechanisms in order to assure reliability shall be implemented,
Communication type	End to end communication	As one of the main goals for the testbed, communication among nodes from different environments must be tested.
Mobility	Single user mobility Group mobility	Nodes inside the capillary networks can be mobile. The testbed shall be able to handle this mobility of single nodes or groups of devices.
Security	Trusted communications among the different parties involved in communication process	Implement hardware and software thus allowing secure and protected communication.

In addition to these requirements previously depicted, a subset of the ones identified in [1] is directly applicable into this particular testbed.
Those items that have impact on the testbed implementation are summarized in Table 4—6.

Table 4—6. Technical requirements

ID	Title	Priority
FU.1	Support of large number of devices	Mandatory
FU.3	Support for diverse M2M services	Mandatory
NT.1	Heterogeneous networks	Mandatory
NT.4	Support of multi-hop communication	Medium
NT.5	Half duplex operation of terminals	Mandatory
NT.6	End to end device to device communication	Mandatory
NT.7	Flexible addressing scheme	Mandatory
NT.9	Reliable delivery of a message	High
NT.15	End-to-end session continuity	Mandatory
NT.16	Support for dual stack IPv4/IPv6	Mandatory
NF.1	Scalability	Mandatory
NF.2	Energy efficiency	Mandatory
NF.6	Address space scalability	High
DV.1	Self organized M2M equipments	Mandatory

The main activities to be implemented in this testbed are the following:

- Cooperation of IP and non-IP worlds based on M2M communication paradigm.
- Integration of multiple heterogeneous devices into a single testbed.
- Secure communications in capillary networks.

4.2.2 Architecture

The architecture of this PoC will be based on the available hardware and software that will be provided by partners and will be explained on section 4.2.3. Taking into consideration all the pieces, Figure 4—5 presents the overall architecture that will be implemented.

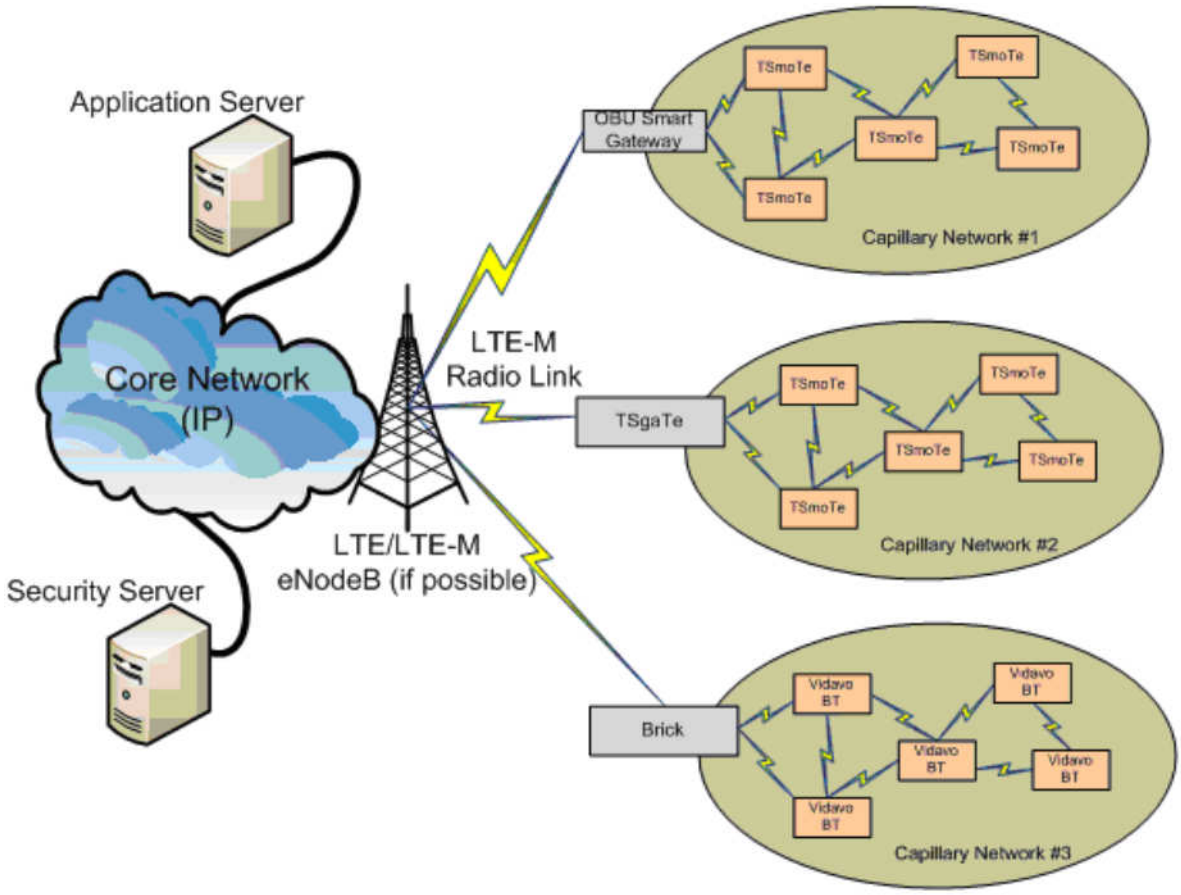

Figure 4—5. Connectivity oriented testbed architecture

The connectivity oriented testbed will create three different capillary networks where developments from different partners will cooperate. These developments will be connected to different servers through the core network by using others access technologies than the ones used by the gateways of the capillary. So the final scope of this architecture will be to prove that different capillary networks, based on different communication technologies, Bluetooth and ZigBee, can operate in the IP world in both ways, from and to public IP addresses.

4.2.3 Building Blocks

In order to perform the required testbed and probe the functionalities associated to this particular testbed, the partners involved in EXALTED project provide different hardware and software developments. These elements will be put together in order to create a common

testbed and to prove many different concepts. The sections below will give a deeper insight of each block composing the testbed.

4.2.3.1 LTE-M Network

The access network intended to be created in EXALTED is the LTE-M, an extension of the LTE network adapted to the particularities of M2M communication paradigm. The scope in the project is to use the same infrastructure for providing a more efficient communication link, in terms of resources and costs due to the M2M constraints, very low data rate, cheap devices and long life batteries.

As it will not be possible to use LTE-M connections in the testbed, the demonstration of the communication concepts developed in the project will be performed using other available cellular technologies such as LTE, Universial Mobile Telecommunication System (UMTS), Global System for Mobile communication (GSM), General Packet Radio Service (GPRS), etc.

4.2.3.2 Core IP Network

This block does not represent any novelty introduced by the project, but it is needed in order to assure full compatibility of the developments done in the capillary networks. As part of the communications infrastructure, the core IP network will be used as basis for reaching different devices and servers contributing to the development of a global testbed.

As the focus of EXALTED is to develop an LTE version enhanced for M2M communication, it is necessary to prove the compatibility of the proposed solution with the whole IP system. The underlying IP infrastructure will be used to provide E2E connectivity between an M2M device and the application server regardless of its location, but connected on an IP basis.

4.2.3.3 Capillary Network

Capillary networks are growing in importance nowadays, not only by their number, but also by the number of devices composing them. The type of capillary networks which EXALTED is focused on are characterized by some common aspects:

- **Long term deployment of devices**. Usually the devices deployed in capillary networks are intended to be at the same place for a very long period of time. That means, the design should be done according to this feature, trying to avoid continuous physical operations over the device itself.
- **Low energy constraints**. Tightly related with the previous consideration, the nodes in capillary networks must be low energy devices, not only in computational terms, but also in the transmission mechanisms used to establish communication.
- **Very low data rates**. EXALTED project is based on low rate applications, the ones that are not suitable for the current broadband connections provided by next generation networks.
- **Low cost devices**. One of the most important reasons for envisioning such a huge amount of applications and devices is the cost of them. M2M paradigm is ready to manage with very simple devices and basic communication capabilities. That simplicity should reflected in the final cost of the elements.

The focus in WP7 will be on creating a capillary network capable to demonstrate the concepts developed in the other technical WPs, so as to develop a real implementation, the project will use the different solutions provided by the partners. Thus a combination of hardware and software pieces will build the target testbed. The following subsection will thoroughly describe each of the modules that will be used.

4.2.3.4 Gateways

The topology presented in EXALTED project implies the connection of the core network to the capillary network. The devices in charge to provide this communication link are the M2M Gateways. These devices have, at least, two interfaces, one connected to the access network (LTE-M or equivalent), and other connected to the capillary network.

The behaviour of Gateways implies many different tasks, and the most important are:

- Proxy for protocol translation and traffic aggregation.
- Local and remote Device Management,
- Mobility management.
- Self healing.

The following subsections will present the different options to be used as gateways within this Proof of Concept framework.

4.2.3.4.1 TSgaTe

The TSgaTe [8] has been introduced as a powerful communication platform, integrating multiple interfaces, both wireless and wired ones. Taking the advantage of the multiple communication opportunities, this platform perfectly fits for proving concepts developed within EXALTED framework.

Figure 4—6. TSgaTe device

The main features of the platform are listed below:

- Advanced RISC Machine (ARM) Cortex M3 Processor
- FreeRTOS, the board runs a true real time operating system
- Zigbee Radio based on Digi XBee [9] family devices.
- Faxtrak Global Position System (GPS) IT500.
- Cellular modem, Sagemcom HiLo 2G/3G [10] module to perform cellular communications.
- Integrated Sensors, temperature, humidity and a three axis accelerometer.
- Several Port I/O interfaces for extend sensing and communication capabilities, Inter Integrated Circuit (I²C), Universal Asynchronous Receiver Transmitter (UART) General Purpose Input/Output (GPIO), Analog to Digital Converter (ADC), Ethernet Socket.

In order to manage this Ethernet socket, the software running here will include Transmission Control Protocol (TCP), User Datagram Protocol (UDP), IP, Hypertext Transfer Protocol (HTTP), Internet Control Message Protocol (ICMP) and Dynamic Host Configuration Protocol

(DHCP), by using µIP library, integrated in the device operating system. Taking the advantage of all these features, TSgaTe will be able to handle the communications between nodes in the capillary networks and servers connected at any point in the network. This device is mainly oriented to smart metering applications although, due to its versatility and expansion possibilities, it could be fit in other scenarios.

4.2.3.4.2 CEA Brick with Bluetooth dongle

CEA Brick is an on board unit, which could be easily used in the context of emergency health care provision scenario if placed in an ambulance. The so called brick provides a plethora of communication interfaces to the world outside the vehicle. The devices interacting with it could be standard telemedicine devices for continuous vital signs monitoring, such as blood oxygen saturation levels, a metric very useful for determining respiration capacity even in Intensive Care Units, heart rate, blood pressure meters, electrocardiograph etc. The standard communication protocol for these devices is Bluetooth or Bluetooth Health Device Profile (HDP) widely known as BT-Health (see also par. 4.2.4.2 of this document) for transferring their data to a master station (i.e. CEA brick) and from there to the outer world. In this case Bluetooth could be perceived as the capillary network.

4.2.3.4.3 OBU running UNIS Intelligent Gateway

4.2.3.4.3.1 Description

Sagemcom's On Board Units called OBU in this document are automotive oriented systems able to fit in a vehicle and feature communications through multiple networks.

The board is composed of a processor card running Linux kernel and multiple peripheral accesses. It also embeds a GPS and a 3G M2M module with its SIM access feature and a secure chip element able to provide the PHY layer for the security architecture scenario to be demonstrated.

This system is an ad hoc implementation created for the EXALTED project testbeds and validation platform of some software implementations. The whole system is in around 130mm x 130mm form factor.

This board is intended to be used in multiple scenarios in the testbeds. The goal is to run the UNIS intelligent gateway software on this device. It can be also used as the simple M2M IP device or even be used as a mobile router (for dynamic IP scenario).

Sagemcom will provide an implementation of the device improvement related to the research on device improvement done in Work Package 6. The main contribution is a self-diagnostic module resulting from WP6 T6.3.

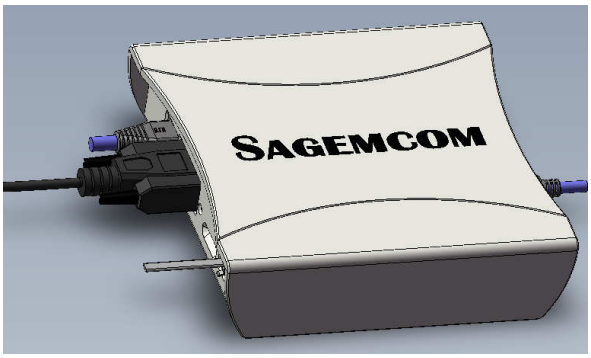

Figure 4—7. On board Unit device

4.2.3.4.3.1.1 As an Intelligent Gateway:

The OBU will be used as an intelligent gateway using the UNIS gateway software development. The gateway is planned to be used in the Testbed 2.

UNIS is designing and implementing an intelligent gateway component for LTE networks to support communications between underlying sensor network and high-level application and service layers. The gateway design and architecture in particular focus on three main aspects: connectivity of heterogeneous resources, information processing and optimization of access and resource usage for resource constrained devices, and provisioning and interaction with network's higher-level and service layers.

The planned architecture for the gateway will be in line with the testbed design and scenarios that will be selected for (and will run on) the testbeds. The communication between the gateway and capillary networks and intelligent decision making within the components will enable the EXALTED components to provide connectivity and interoperability for the underlying heterogeneous networks and at the same time optimize and manage resource access for constraint devices using context-aware and intelligent machine learning mechanisms.

4.2.3.4.3.1.2 As LTE-M device:

The OBU will be used in a common M2M device able to reach and to be reached from the network to exchange data from various measurements without the need of a gateway.
The embedded different sensors will be used to gather physical data to be sent on requests from the application server.

4.2.3.4.3.2 The connectivity of the OBU

The on board unit architecture is based on an integrated system-on-module featuring the following Peripherals:

- 1 UART RS232 1 Mbps.
- 1 Zigbee module.
- 1 I²C will be present on the PCB.
- 1 Controller Area Network (CAN) will be present but buried just in case of need.
- 1 Bluetooth chip embedded.
- 1 Secure Digital Input/output (SDIO) card reader.
- 2 USB (On The Go and Host).
- 1 Serial Peripheral Interface (SPI) for the secure Chip embedded.
- 1 Joint Test Action Group (JTAG) will be present but buried just in case of need.
- 10 GPIO's.
- 1 Ethernet (Redboot access to load Linux OS 128MB NAND + 64MB Secure Digital Random Access Memory (SDRAM)).
- 1 battery 8.25Wh /3.75V.
- 1 RF link with a HiLo 3G Family.
- 1 Subscriber Identity Module (SIM) card reader.
- 1 SIM IC chip embedded.
- 1 RF GPS receiver in the HiLo 3G.
- 1 Digital temperature sensor on I²C or SPI buses.
- 1 Accelerometers on SPI or I²C buses.

Those peripherals are managed by the system-on-module with the following main specification:

- ARM926 400MHz processor with Dry Ice security element.
- 64 Mega-bytes of SDRAM.
- 128 Mega bytes of NAND flash.

- Linux 2.6.

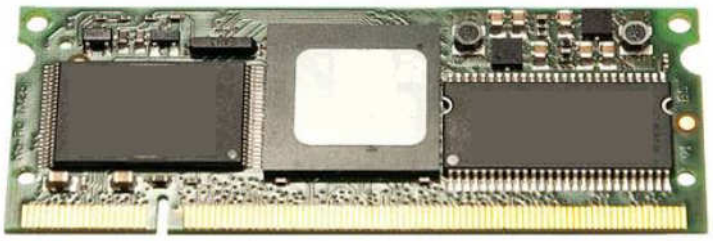

Figure 4—8. System on module unit

4.2.3.5 LTE-M devices

Another category of M2M devices are the ones that can directly communicate to the LTE-M network. They do not have an interface that enable the creation of capillary networks behind it, so they cannot be used as gateways.

In EXALTED Proof of Concept tests, two devices could act as IP LTE-M enabled, a limited version of the aforementioned TSgaTe and the OBU, and both of them are capable to implement different cellular technologies (GPRS, UMTS, LTE...) in order to demonstrate the different concepts developed in the project.

4.2.3.6 Non LTE-M device

These are simple devices with limited capabilities, both in terms of sensing and communication capabilities. They are connected to the core network through the gateway in the capillary network in which they are operating.

The sections below describe the main features and capabilities of the M2M devices that will be used in the Proof of Concept.

4.2.3.6.1 TSmoTe

This device aims to be a flexible and powerful wireless communication platform, with optimized costs and equipped with multiple communication interfaces in order to manage sensors or actuators. In addition to these potential external sensors, it has three built-in sensors on board: temperature, humidity and 3-axis accelerometer. Furthermore, a GPS-enabled daughterboard (integrating Fastrax IT500) is available, enabling it to perform mobile tracking applications. Other expansion interfaces are available as well, including UART, I2C, SPI and CAN bus, apart from analog and digital I/O interfaces.

Finally, the following modules are available for integration: an USB socket, a SD card slot, a SPI Flash memory, a WiFi module (Digi's XBee WiFi), a 2G/3G modems (SAGEM's HiLo), which can be replaced by an LTE-M module if possible, an IEEE802.15.14/ZigBee/DigiMesh module and a Radio Frequency Identification and Near Field Communications (RFID/NFC) interface (NXP's PN532). Envisaged applications cover not only remote sensing, processing and data transmission of data from sensors connected to the device, but also remotely controlled applications supporting management of relays and/or actuators.

Figure 4—9. TSmoTe module

These devices can be connected either through OBU or Intelligent Gateway, or directly to the TSgaTe, providing IP connectivity to the nodes.

4.2.3.6.2 E-Health Telemedicine Bluetooth devices

In the E-Health scenario, a cooperation between the CEA brick and special telemedicine devices takes place in a supposed ambulance environment where the goal is to prepare (i.e. to provide accurate and up to date health information) as best as possible the physicians at the nearest hospital where the patient is destined for, and also to treat the patient in the optimum way during his route to the hospital. In order to achieve those purposes, critical vital signs of the patient should be transferred from the ambulance to the hospital and the resident medical team. The vital signs indicatively include: Electrocardiogram (ECG), blood oxygen saturation level, heart rate, blood glucose etc. The special devices communicate the values captured from the patient's body to the CEA brick via Bluetooth, as the most common, short range wireless protocol.

Some pictures of the devices can be seen on Figure 4—10.

Figure 4—10. Example of Bluetooth devices

4.2.3.7 Application Server

Capillary networks are often associated to application servers that handle the data collection in a remote way. If no application is embedded on nodes or gateways to perform such function, all data collection and storing is done via remote connections to these application servers, located on the core IP network.

Connection between this kind of servers and end nodes should be enabled and proved.

4.2.3.8 Secure element

The hardware secure element will provide to the testbed a flexible connectivity through industry standard serial access buses. With the various functionalities that an LTE-M device could offer, it has been considered a basic architecture around a machine identity module secure core.

The secure element form factor will be packaged into an industrial low pin count form factor able to be soldered on a printed circuit board according to the LTE-M device general purpose logical input/output configuration.

On the hardware side, the secure chip has been chosen to fit with multi-application requirements:

- Standard secure USIM chip architecture;
- Up to 256Kb of non volatile memory with extended life;
- Very large memory endurance in time allowing a large number of cycles for software update;
- Standard telecom qualification: 2G/3G/LTE;
- Well adapted to industrial manufacturing processes and low cost molded technology;
- Configurable interface through dedicated software programming as I2C, SPI or UART communication module.

On the software side, the secure element operating system is Java Card and Global Platform system compliant. In particular, additional specific applications can be developed and uploaded on board in order to demonstrate the LTE-M device EXALTED use-cases.

The secure element form factor and pin out configuration is fully adapted to fit the on-board-units (OBU) system requirements for EXALTED device management testbeds demonstration.

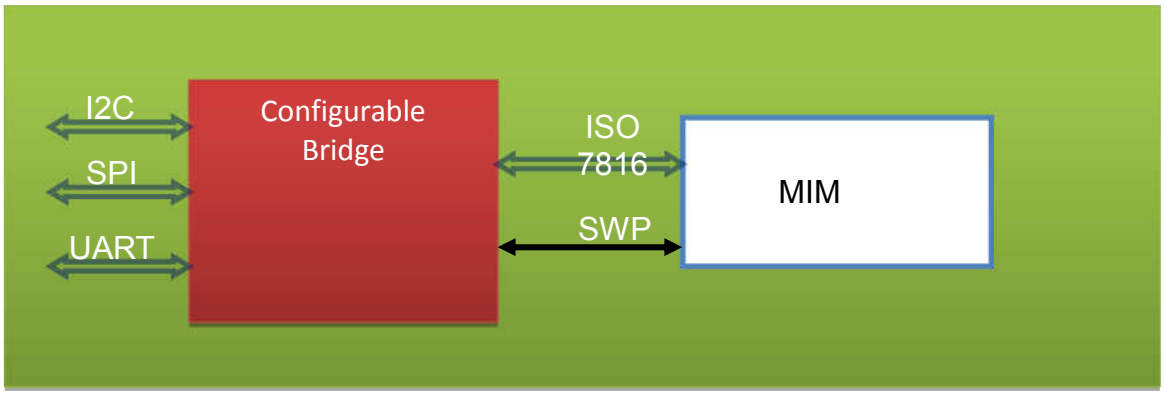

Figure 4—11 Secure element architecture

4.2.3.9 Device summary

In order to provide a clearer view of devices included on this second testbed, Table 4—7 is provided summarizing all equipment envisaged and the partner responsible for its integration.

Table 4—7. Device Summary for Testbed 2.

Device Type	Device Name	Testbed	Partner
Gateways	TSgaTe	2	TST
	CEA Brick	3	CEA
	OBU	1	SC/UNIS
LTE-M Devices	TSmoTe	Any	TST
Non-LTE-M Devices	TSmoTe	1,2	TST
	e-Health devices	3	VID
Security	Secure Element	2	GTO
Server	Application Server	All	All

4.2.4 Interfaces

Once the general architecture and specific functional blocks for connectivity oriented testbed is depicted, the interfaces are presented so as to completely define interactions between nodes from architecture.

Depending on the device, there are three possible interfaces that it may implement: Zigbee, Bluetooth or cellular. This selection will affect the way it could communicate with other elements on the testbed.

4.2.4.1 Xbee Modules

TSgate and TSmoTe devices will implement Zigbee as the wireless interface to communicate within the capillary network. In order to achieve this, they use a Zigbee module provided by DIGI manufacturer, called XBee.

XBee and XBee-PRO 802.15.4 Original Equipment Manufacturer (OEM) RF modules are embedded solutions providing wireless end-point connectivity to devices. These modules use the IEEE 802.15.4 networking protocol for fast point-to-multipoint or peer-to-peer networking. They are designed for high-throughput applications requiring low latency and predictable communication timing.

Its main characteristics can be summarized as follows:

- No configuration needed for out-of-the-box RF communications.
- Common XBee footprint for a variety of RF modules.
- Fast 250 kbps RF data rate to the end node.
- 2.4 GHz for worldwide deployment.
- Sleep modes supported for extended battery life.

Figure 4—12. XBee module

This module (shown in Figure 4—12) will be used for communication of two TSmoTes between themselves, TSmoTes with TSgaTes or TSgaTes between themselves. Digi's proprietary routing protocols are used by default with these modules, but custom ones are possible, enabled by the board's capabilities.

4.2.4.2 The Bluetooth Health Device Profile (HDP)

Bluetooth as a short range wireless technology is very suitable for various medical applications both in-house and in-hospital. Up to a certain point in time Bluetooth enabled systems for medical applications used proprietary implementations and data format. Consequently if these systems were not from the same provider they were non-interoperable creating barriers for the large scale adoption of similar solutions. In 2006 the Medical Working Group (Med WG) of the Bluetooth Special Interest Group (SIG) began defining a specification addressing the needs of the medical community. Under Bluetooth, a profile defines the characteristics and features including function of a Bluetooth system. The end result of this work was the HDP specification that included the Multi-Channel Adaptation Protocol (MCAP) and made use of the Device ID (DI) Profile. The following picture describes the architecture of a Bluetooth system with the HDP and applications:

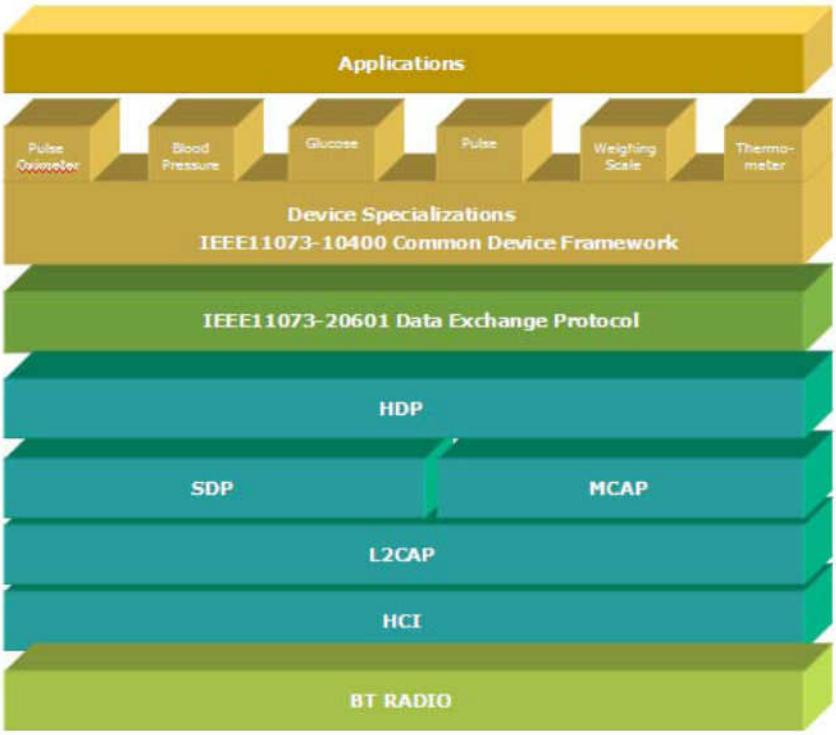

Figure 4—13. Architecture of a Bluetooth system with the HDP and applications

HDP is specialized for health applications and thus has the following advantages over other more generic profiles:

- It provides strong application level interoperability by operating with the ISO/IEEE 11073-20601 Personal Health Data Exchange Protocol.
- Provisions for a standardized method by which the device-type and supported application data-types of a device can be determined wirelessly, using the Bluetooth Service Discovery Protocol (SDP).
- Connection-oriented communication is used in order to ensure more reliable behavior when a *Source* moves out of range or disconnects (either inadvertently or

intentionally), allowing the device to recognize the condition and take appropriate actions.

Overall Bluetooth Health Device Profile, in combination with the IEEE 11073 Specifications, provides a robust, standards based framework to allow interoperability between Bluetooth Health Devices.

4.2.4.3 Cellular Interface

For the time being, it is not possible to determine which cellular network technology could be used on EXALTED's testbeds. As LTE-M is being specified during the project, commercial devices will not be available, just simulations and testbed implementations (see section 4.1) will be performed by some partners. Hence, it is clear that using it for the other testbeds will not yet be possible.

Given this fact, a range of cellular network options are still available to be integrated on the testbeds. If time and state of the art technology by the time testbeds are integrated permit, LTE interfaces will be considered to be implemented. But, as it is not possible to assure it right now, GPRS/3G interfaces are also proposed as cellular interfaces as further alternatives.

Those are the ones already implemented on some devices planned to be integrated on testbeds.

4.2.5 Timeline and milestones

In order to properly plan testbeds, it is important to define timelines and milestones to guide and schedule the process of integrating heterogeneous devices/modules.

Even though the project is on early stages, and it is difficult to fix deadlines for milestones, an initial approach will be provided in order to schedule and plan all needed steps .

As this particular scenario is made up of three different capillary networks, a subset of milestones will be defined for each of them, and the deadlines may vary depending on the amount of effort needed to combine different partners' contributions:

Table 4—8. Milestones for capillary networks

Milestone	Description	Envisaged Completion
M2.1	Fully operative capillary network. Enabled communications between M2M nodes and Gateways.	M15
M2.2	Enabled communications between nodes and application server on the core network.	M22
M2.3	E2E communication. Capillary network cooperation.	M27
M2.4	Validation of the concepts demonstrated in the testbed	M30

For the first and the third network (OBU+TSmoTes and CEA Brick + VID modules), as they comprise devices from several partners, integration is not immediate, so it will need some time to adjust cooperation between them. On the other hand, Network 2 only implements TST devices, so integration and first network deployment are easier.

Once these milestones are achieved, it is needed to implement the secure layer on the top of communications. In order to perform such task, it is needed to set some extra milestones:

Table 4—9. Milestones for security implementation

Milestone	Description	Envisaged Completion
M2.5	Secure element integration on M2M devices	M20
M2.6	Delegation of secure mechanisms to Security Server.	M27

4.2.6 Scenario mapping

Requirements from each scenario have been classified and quantified; the ones that fit best with this testbed are listed on the following table:

Table 4—10. Requirement quantification from scenarios regarding testbed 2.

M2M Network			Justification
Deployment architecture	Device-to-device communication	YES	O4.5 DoW: Design an IP based E2E networking system for M2M communications. Enabling interactions between end M2M devices.
	Infrastructure-to-device communication and vice versa	YES	O4.1 DoW. DM operations requires communication in both directions, being contactable all devices in a capillary network. ETSI requirements for DM.
	Hybrid architecture, devices-to-cluster head	Possible	O4.4 and O4.1 of DoW. Energy optimization approaches focus on clustering as a mean of aggregate traffic reducing overall consumption. Based on this principle it is mandatory to support this communication.
Communication type	Simplex	For low complex. apps	Do not fulfill ETSI M2M TS102689 Requirements. Require bidirectional communication in order to address DM requirements.
	Half-duplex	YES	Compliant with ETSI M2M TS102689 requirements
	Full-duplex	Improbable	Extra complexity level not mandatory for being compliant with ETSI requirements
	Peer-to-peer	Possible	Functional Requirement from ETSI TS102689 Req. 6.9 demands path diversity
	Multi-hop	YES	Wireless mesh technologies demands this connectivity. In order to cover larger areas without increasing transmission power in devices.
	Multicast	YES	ETSI M2M TS102689 Requirement 6.3 Functional requirements Group Mechanisms
Network partitioning	Clustering	YES	O4.4 DoW: Traffic aggregation point architectures to support reduced traffic load.
	Cluster-head selection	YES	O6.1 DoW: Energy-efficient devices. Distributing the cluster head role among several nodes increases the energy efficiency of the whole network.

Devices' transmission range	Device to gateway	< 200m	• @2.4 GHz 1mW 100 m LOS, 30m NLOS. For single hop communications. Max number of hops 255. – Typical values extracted from Digi XBee modules • Existing solutions that use PLC with Prime / OFDM protocol can push the range to 1000m between the device and the gateway (data concentrator)
	Device to cluster head	< 200m	
	Device to Base station	N/A	
	Device to device	< 200m	
Device capabilities	Data rate requirements	<10Kbps	• Typical monitoring applications. 1 param, 1 measure/hour, including all layers overhead supposes a data rate of 0.189 bps/ device. • In case of PCL the current requirement is <20Kbps • In case of Wireless M-Bus EN13757 the current rate is <2.4Kbps
	Processing capabilities	Very Low	8bit PIC can handle the operations required for SMM applications. http://code.google.com/p/xbee-arduino/
	Power consumption	<0.1mW	• This parameter is highly dependent on duty cycling techniques implemented. Consumption can be estimated based on: sleep time, wake time, sleep current, TX current, RX current. It is not possible to provide exact figures to this params due to the variety of the values it allows. By the way, typical deployments are below 0.1mWatts. • The next generation of Smart metering solutions for water and gas requires a battery lasting at least 20 years..
	Bandwidth usage	<50KHz	EN 13757-4 current standard gives 12,5KHz of bandwidth.
Miscellaneous	Self-organized network	YES	Bootstrapping and routing protocols within the capillary networks allow the attachment of new devices once the network has been deployed.

M2M to Gateway			**Justification**
Type of Gateway	Heterogeneous Interfaces	YES	Data concentrator.
Resources management		YES	Clustering allow resource management.
Number of aggregation points		<5 per 100 devices or dynamic range	Smart metering scenarios do not require large amount of aggregation points, but other ones (e.g. monitoring) may need dynamically adjusted aggregation points.
Networking	IP v4, IP v6, non IP	YES	Non-IP supported on very low complexity nodes within the capillary network, and dual stack compatibility envisaged for LTE-M enabled and Gateways.

4.3 Device Management testbed

The testbed will be focusing on the following aspects:

- Device Management (DM) protocols, as defined in WP4 task T4.3, allowing the Device Management server to exchange messages with LTE-M enabled gateways and LTE-M devices. The low-cost and lightweight aspects of the proposed protocols are important. The testbed will demonstrate the small footprint of the message payload and low-processing power to implement the protocol in the gateway and the device.
- Security related to the proposed Device Management protocols
- End-to-end communications. Relying on the Device Management protocols, the testbed will demonstrate DM Server to end-Devices functionalities required in selected scenarios.

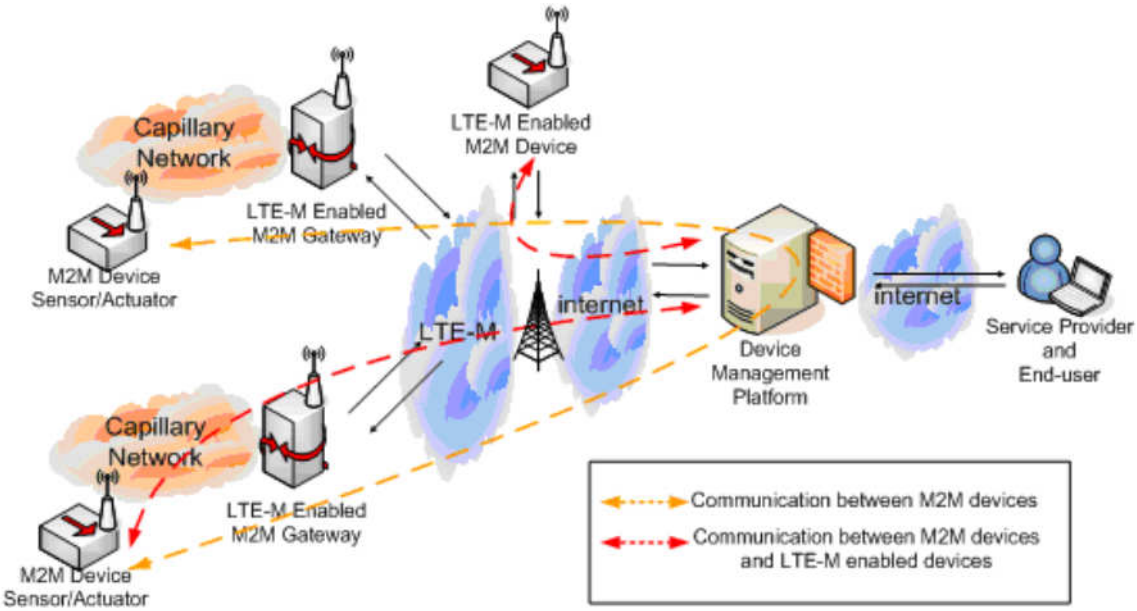

Figure 4—14. Device Management testbed

Figure 4—14 shows an overview of this testbed. End-to-end communication paths between different building blocks are depicted in dotted lines.

This testbed is composed of 6 building blocks:

1. Device Management Server, comprised in Services and Management platform
2. Security entity, comprised in Services and Management platform
3. Service Provider User Interface
4. LTE-M network and Core network
5. LTE-M gateway & LTE-M devices
6. M2M devices (non LTE-M devices)

LTE-M network will not be available to run on this testbed. Other cellular network can be used to perform the device management scenarios. As the device management protocol is not dependent to LTE-M network, the novelties can still be demonstrated using LTE, 3G or GPRS network.

Due to time constraints and the focus of this testbed, only a limited set of device management functionalities will be implemented and demonstrated. In addition, the overall

architecture of the testbed does not reflect the E2E system architecture as recommended in other documents of the project.

4.3.1 Requirements and novelties

Device management requirements have been identified and described in WP4 framework.

As this testbed aims to demonstrate some key features and novelties, only a limited set of requirements will be implemented. These requirements are summarized in the table below (Table 4—11).

Table 4—11. Requirements addressed by Device Management Testbed

Category	To demonstrate	Impact on testbed
Deployment architecture	Multi-hop. Device Management messages & commands can be relayed to/from end-devices	The proposed DM protocols must be implemented on LTE-M enabled gateway and devices in the capillary network.
Addressing scheme / NAT	Device Management server shall be able to send notifications and commands to end-devices (not reachable via IP address) located behind a NAT.	The proposed DM procedure and protocol must be implemented in gateway. Where DM transparent, proxy or adaptive mode must be supported.
Device/Gateway Configuration	DM server to retrieve current device configuration of end-device. Then server has the ability to push new configuration to end-devices	Software update for gateway and devices may not be demonstrated. On the DM point of view, software update is a particular configuration scenario.
Device/Gateway Data Collect	DM server to collect and store data sent by end-devices	Need to define type of data to be tracked
Device/Gateway Alarms	DM server is able to collect Alarms fired by end-devices	End-devices shall implement the alarms notification, using the proposed DM protocol, for send alarms (device discovery or device self diagnostic faults)
Device/Gateway Remote Diagnostic	DM server can initiate a diagnostic command on a selected end-devices, and collect diagnostic results	Remote Diagnostic execution command must be defined in the proposed Management Objects. Either the device is woke up and execute the commands or the device includes a wake up mechanism to be in wake mode ready to be reach by the DM
System Security	Authentication & challenge mechanism shall be in place for the DM protocol	Need to define test cases to showcase the authentication failure/challenge/retry
Reliability	Reliable delivery of a message, in terms of data integrity and message exchange mechanism	Need to define test cases to show case the data integrity issue/auto fix and communication issue (disconnection) during message exchange
Scalability	The proposed Device Management protocol is lightweight compared to other industry well known protocols.	Need to define comparison scope and metrics (e.g. payload)

In addition to these requirements previously depicted, subsets of the ones identified on EXALTED D2.1 document are directly applicable into this particular testbed.
Those items that have impact on the testbed implementation are summarized in Table 4—12.

Table 4—12. Technical requirements

ID	Title	Priority
FU.5	Local and remote device management	High
FU.7	Security and provisioning	Mandatory
SV.3	Efficient provisioning of a set of M2M equipments	Mandatory
SV.6	Security	Mandatory
NT.1	Heterogeneous networks	Mandatory
NT.6	End to end device to device communication	Mandatory
NT.12	Self-diagnostic and self-healing operation	Medium
NF.1	Scalability	Mandatory
DV.1	Self organized M2M equipments	Mandatory

DV.2	Reliable M2M equipments	High
DV.9	M2M equipment wake-up	Mandatory
DV.10	Remote configuration	Mandatory
DV.11	Software update over the air	Mandatory

The key novelty is the small data footprint involved in the device management procedures. The size of payloads and device management procedures has direct impact on device's power/resource consumption, and on the system scalability.

4.3.2 Building Blocks

Connectivity Oriented testbed and Device Management testbed share the same building blocks. This subsection describes the three following building blocks with a focus on device management: Device Management Server, Service Provider User Interface and LTE-M enabled gateway/device. The other building blocks are described in section 4.2.

In this section, each building block will be described as well as the main functions and the functional architecture related to device management.

4.3.2.1 Device Management Server

This is a central server that interfaces with LTE-M enabled M2M devices. This server acts as a middleware between the managed devices and the service providers.

Task 4.3 will be proposing a lightweight Device Management protocol to align to EXALTED's low-cost device vision. The proposed protocol will be derived from an existing standard.
The device management testbed will be implementing this proposed protocol.

4.3.2.1.1 Main Functions

The main functions that will be performed by the Device Management server are the following:

- Persistence of the managed Devices information in the database.
- Authenticate Devices (devices connecting to the server).
- Retrieve the list of Devices attached to a Gateway.
- Retrieve Device's current state and attributes.
- Update the database.
- Apply new configuration to selected Devices.
- Trigger a remote Device Diagnostic.
- Enable user (Service Provider and end-user) to manage Devices:
    - create, view, update and delete Devices,
    - view Devices states and attributes,
    - set new configuration,
    - trigger Remote Device diagnostic,
    - remotely control Devices (e.g. turn light on/off, etc…).

4.3.2.1.2 Functional architecture

The Device Management building blocks will be built for the testbed with the following components:

- PC with an Internet access with a public IP address (through a DSL line).
- Web server hosted on the aforementioned PC (e.g. Tomcat).
- DM protocol, specified by Task 4.3, implemented as a Java Servlet 1. This servlet interacts with the device, retrieve and persist device data into database.
- Simple database, e.g. MySQL.

- Java Servlet 2, able to send a Notification to device through a Web services of the operator. This servlet can also receive ACK from the notification server (from operator)
- Java Servlet 3, serving the user interface and relays user command onto DM protocol.

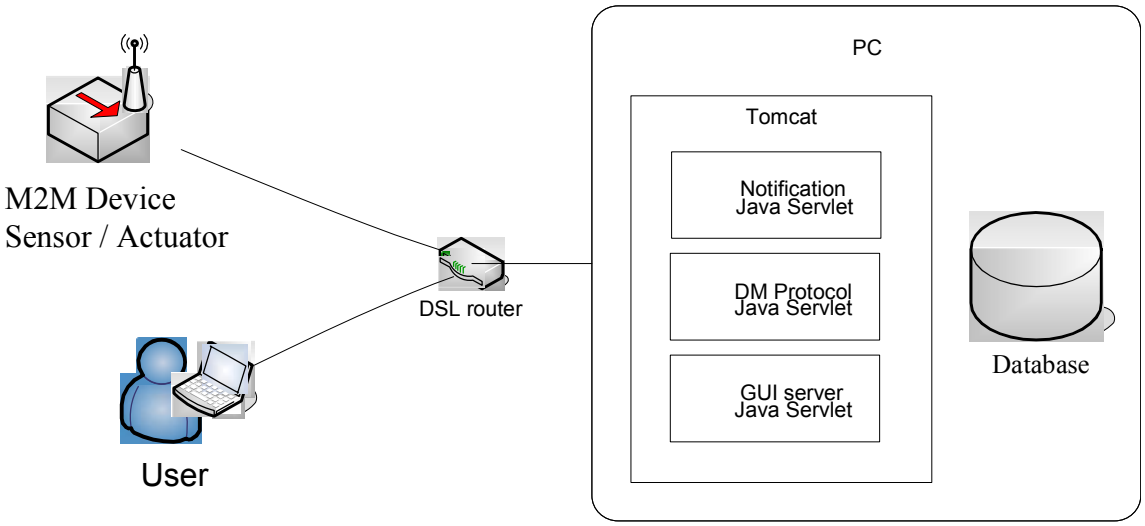

Figure 4—15. Device Management building block Functional Architecture

The Figure 4—15 introduces the different actors and elements taking part in the functional architecture of the device management scenario.

4.3.2.2 User Interface

This user interface enables service provider and end-user to remotely control the Devices.

4.3.2.2.1 Main Functions

The main functions that users can perform are:

- Provision additional LTE-M enabled devices into the Server.
- Bootstrap LTE-M enabled devices.
- View status and attributes of managed devices.
- Trigger Device Diagnostic actions.
- Trigger an action on the device (e.g. get data, turn on/off…).

4.3.2.2.2 Functional architecture

The User Interface sub-system will be built for the testbed with the following components:

- Client PC with Internet browser and an Internet access (e.g. DSL line).
- The GUI client component is a RIA (Rich Internet Application).
- The GUI client component is hosted on DM server. It will be loaded into Client PC's web browser and executed.

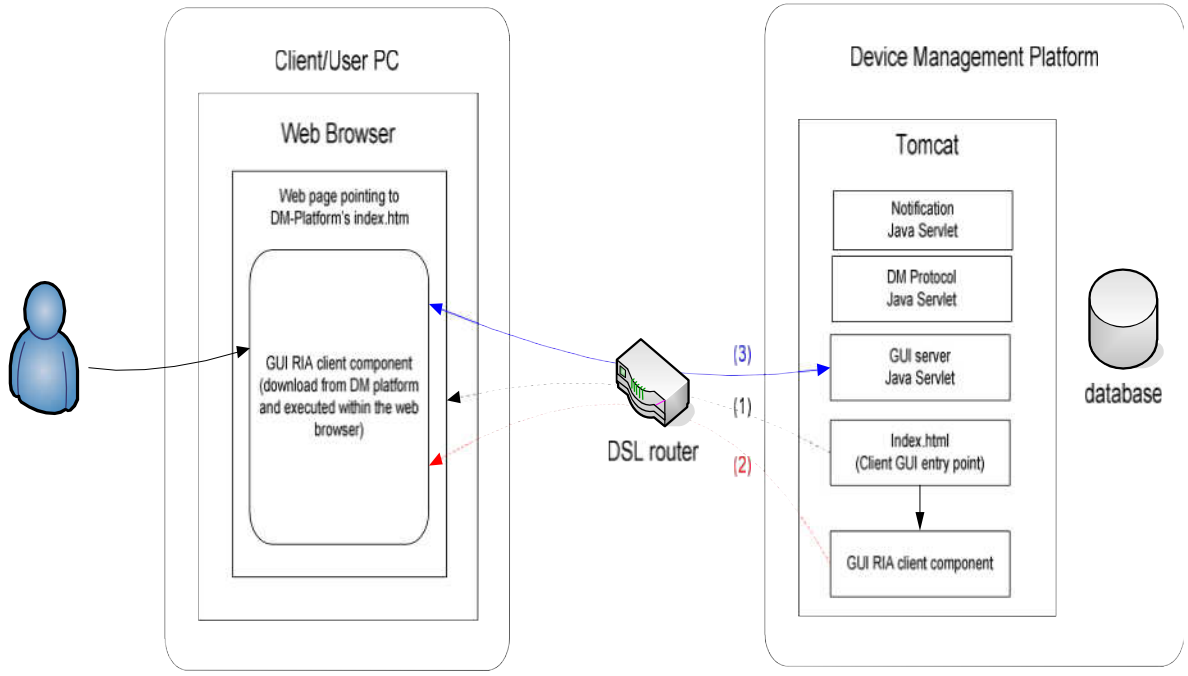

Figure 4—16. User Interface sub-system Functional Architecture

4.3.2.3 LTE-M enabled Device or Gateway

LTE-M enabled Device or M2M Gateway both share the same Device Management services. Therefore the Device Management functionalities, interfaces and data flows of the device and gateway are merged into this single section.

4.3.2.3.1 Main Device Management (DM) Functions

- Receive notification from DM server
- Authenticate the notification
- Establish DM session with DM server
- Post device data (configuration, status, attributes) to DM server
- Receive DM commands from DM server
- Execute DM commands
- Ability to execute auto-diagnostic
- Relay DM command to Capillary Device (not LTE-M enabled)
- The above Relaying function requires a mapping mechanism in order to identify and address a particular device
- Relay and Post execution results to DM server

4.3.2.3.2 Functional architecture

The LTE-M enabled Gateway sub-system could be built for the testbed with the building blocks as depicted below :

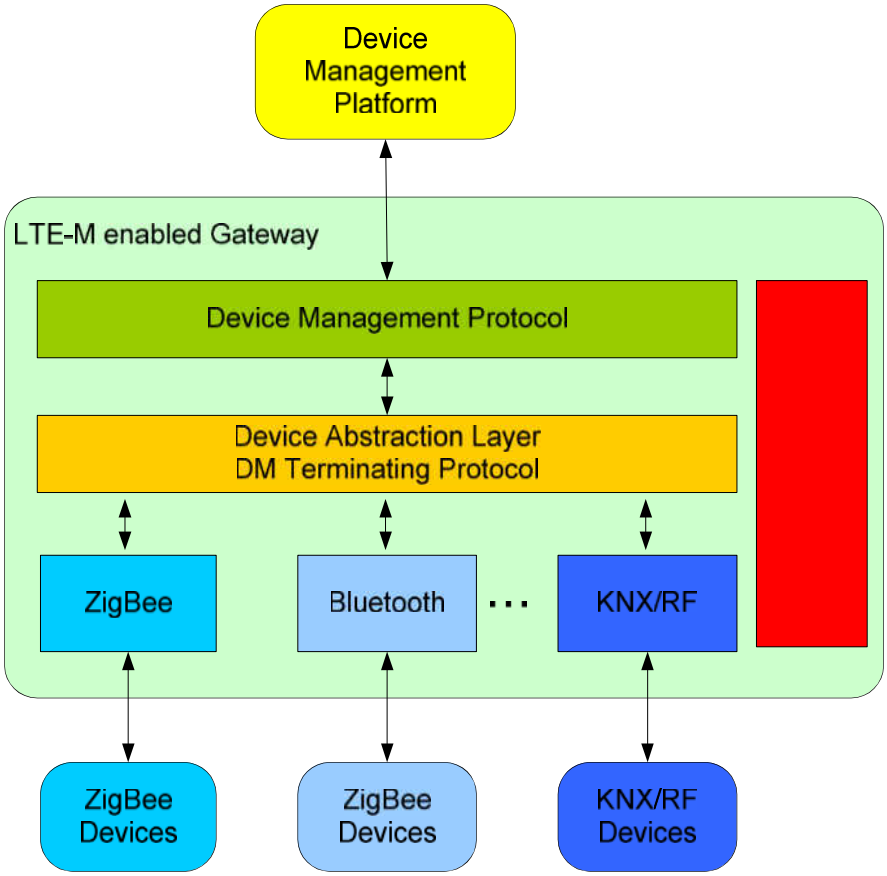

Figure 4—17. LTE-M enabled Gateway Functional Architecture

4.3.3 Interfaces

The Device Management Server has 3 interfaces:

- Graphical User Interface (GUI), to enable the user to manage Devices,
- Core network, to gain access to operator's Web services (e.g. send SMS),
- Device Management Protocol over http/https, to communicate with Devices.

The GUI has 2 interfaces:

- User interface,
- DM server interface.

LTE-M enabled device/gateway has at least 1 DM interfaces:

- DM server; both device and gateway are interfacing with DM server;
- Capillary device; LTE-M enabled gateway interacts with capillary devices.

4.3.4 Data Flows

1) Data flows between DM server and the GUI
    - GUI → DM Server
        - Device Management commands applied to Management Objects. The basic commands are create, get, update, delete, execute.
        - Commands are transmitted to the DM Server over HTTP-GET.
    - DM Server → GUI
        - HTTP response.
        - Array of Devices along with the current states and attributes.
        - This data is transmitted to the GUI as XML format in the response.

2) Data flows between DM server and Core Network
   - DM Server → Core Network
     - Notification data in order to wake-up device (if needed).
     - Notification data contains targeted device information and security elements.
     - The Notification could be a SMS or a TBD LTE-M notification mechanism.
     - Notification data is transmitted to Core Network using TBD Web Services over HTTP.
   - Core Network → DM Server
     - Acknowledgement of the requested notification. Returned over the HTTP response along with error code.
     - Error, Status and progress of the notification request, returned to DM server over HTTP GET, as call-back.

3) Data flows between DM server and LTE-M enabled device
   - LTE-M enabled device → DM server
     - Security elements and session setup data.
     - List of devices attached to the gateway.
     - Identity, states and attributes of each attached device.
     - Execution results of a previous DM command issued by DM Server.
     - Above data is sent to DM server using the DM protocol defined in T4.3 over HTTP-POST.
   - DM server → LTE-M enabled device
     - Security elements and session setup data.
     - Device Management commands.
   - Above data is sent to LTE-M enabled device using the DM protocol defined in Task 4.3 over HTTP response

4) Data flows between LTE-M enabled Gateway and Capillary Device
   - LTE-M enabled Gateway → Capillary Device (M2M Device)
     - Pairing data (association phase of a device to a gateway).
     - DM commands. The original DM commands received from the DM server are formulated under DM protocol. These commands must be "translated" to the legacy capillary commands and sent over the device native wireless technology.
   - Capillary Device (M2M Device) → LTE-M enabled Gateway
     - Pairing data (association phase of a device to a gateway).
     - Device data (configuration, status, attributes). This data is sent to the gateway using the device native wireless technology and protocol.

4.3.5 Device Management Procedures

This section describes the procedures used in this testbed to fulfil key device management functionalities.

4.3.5.1 Device Registration

The registration procedure consists of providing a list of managed devices onto DM Server. Access will be denied to unregistered devices attempting to connect to the DM Server.

The Service Provider shall have the ability to register gateway/device to the DM Server. The following information is required during this registration:

- Device/Gateway unique ID – International Mobile Equipment Identify (IMEI).
- Device/Gateway security element (secret, default nonce). Secret and default are embedded in the device at manufacturing.
- Initial software version.

Note that the above registration data set has been intentionally reduced for the testbed. In the full product, other information shall be included in this registration procedure, such as customer ID, further device information, etc.

The Service Provider shall submit the above registration data set to DM Server by the way of the User Interface building blocks. The User Interface shall provide controls to manage (create, read, update, delete) the registration data on the DM Server. The testbed will only provide a manual registration procedure, whilst automated and secured registration process is used in production.

4.3.5.2 Device Provisioning

Device Provisioning procedure consists of assigning connectivity settings to pre-registered devices. These settings, also known as bootstrap information, will be sent to device for activation.

The user (customer) shall have the ability to provision the pre-registered devices.

The following information is required during the provisioning procedure:

- Information for the network to identify the device (e.g. MSISDN) or similar information to enable the network to send a notification message to the device.
- Connectivity information for a device to attach to the LTE-M network, to obtain an IP address, and to establish a default EPS bearer or dedicated EPS bearer.
- URL of the DM Server, so the device knows where to make connect to.
- Server credentials, so the device can authenticate the DM Server.
- Security element, information used for the next connection to DM Server.

The User shall submit the above provisioning data set to DM Server by the way of the User Interface building blocks. The User Interface shall provide controls to manage (create, read, update, delete) the provisioning data on the DM Server. The testbed will only provide a manual provisioning procedure, whilst automated and secured provisioning process is used in production.

4.3.5.3 Device Bootstrapping

Device Bootstrapping procedure consists of sending the provisioned settings (Device Provisioning) to managed devices. This bootstrap data as defined in the previous sub-section shall be sent to the device via a notification message. As the result of the bootstrap, the LTE-M enabled device has all the necessary information to attach and to register to the LTE-M network, and is able to connect to the DM Server. Other device configuration can also be applied at bootstrap, this testbed only limits to the connectivity settings.

The DM Server shall use the provisioned information (Device Provisioning) to create and to send an SMS to the device. This testbed use SMS as a notification message. Other types of notification messages are being considered in WP3.

The SMS shall contain the data as listed in Device Provisioning. The binary format of this SMS will be defined at a later stage.

The SMS shall also contain a ServerDigest, calculated as defined in Server Authentication procedure.

In the testbed, DM Server interfaces with an SMS Broker in order to send the SMS to the targeted device.

The SMS creation and sending by the DM Server shall be triggered by the user via a Device Bootstrapping button on the user interface.

4.3.5.4 Device Wake-up notification

Device Wake-up action is initiated by DM Server and consists of sending a notification message to the device. The intent of this message is to send a request to the device to connect to DM Server as soon as possible. To be energy and cost efficient, the device may not connect to the DM Server on a regular basis. In this case, the wake-up notification is used to trigger the device to establish a connection with the server.

In the testbed, DM Server interfaces with an SMS Broker in order to send the SMS to the targeted device. For simplicity of the testbed, the wake-up message has the same message format as the device bootstrap notification message.

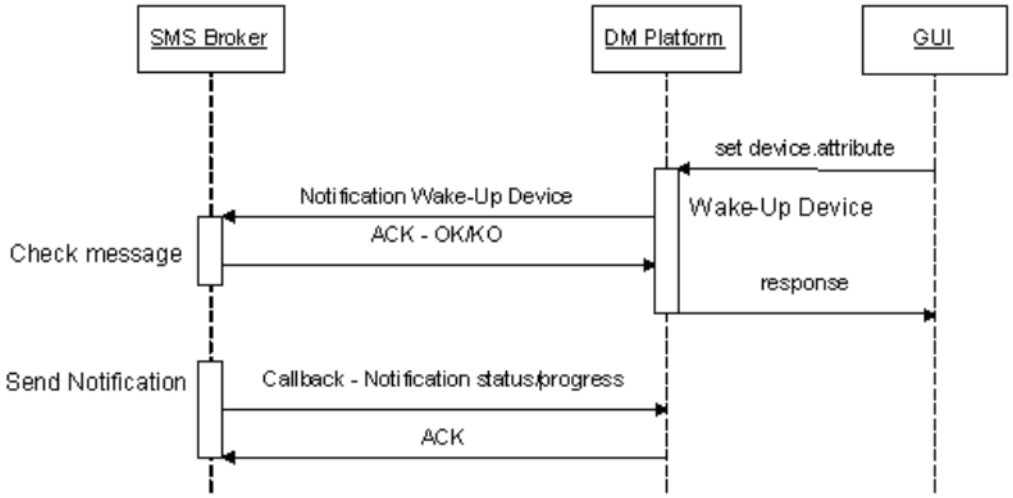

Figure 4—18. Wake-up notification procedure between DM server and SMS Broker

4.3.5.5 Server Authentication

This procedure shall be implemented in the device in order to authenticate the sender upon messages reception. This procedure provides a server authentication at the protocol level.

DM Server calculates a digest as follow:

ServerDigest1 = H(B64(H(IMEI:secret)):cnonce1:B64(H(content)))

Where H is the MD5 hashing function, B64 is Base64, secret is the secret of the device (refer to Device Provisioning), IMEI of the device (refer to Device Provisioning), cnonce1 is the client nonce (number used once) as stored on the server and, content is the body of the message payload
The Server Digest is located in the header of the message being sent to the device.

Upon reception of the message from DM Server, the device authenticates the DM Server by comparing the DeviceDigest1 to ServerDigest1. If they match, the server is authenticated and the device processes the message. If they don't match, the message is ignored by the device.

DeviceDigest1 = H(B64(H(IMEI:secret)):cnonce2:B64(H(content)))

Where H is the MD5 hashing function, B64 is Base64, secret is the secret of the device (refer to Device Provisioning), IMEI of the device (refer to Device Provisioning), cnonce2 is the client nonce (number used once) as known by the device, content is body the incoming message payload

At the very first time (device out of box), cnonce2 is set to the default nonce (factory setting). On the DM Server, cnonce1 is also set to the default nonce. This latter is defined during the Device Provisioning procedure. Therefore, the cnonce1 and cnonce2 are identical at the first message exchange, which leads to server authentication success.
Note that the secret is never transmitted.

The device shall use this procedure upon receiving messages over the Device Management protocol and notification messages (e.g. SMS).

4.3.5.6 Client Authentication

This procedure shall be implemented in the DM Server in order to authenticate the sender upon messages reception. This procedure provides a client authentication at the protocol level.

Device calculates a digest as follow:

DeviceDigest2 = H(B64(H(IMEI:secret)):snonce1:B64(H(content)))

Where H is the MD5 hashing function, B64 is Base64, secret is the secret of the device (refer to Device Provisioning), IMEI of the device (refer to Device Provisioning), snonce1 is the server nonce (number used once) as known by the device, content is body the message payload

The DeviceDigest2 is located in the header of the message being sent to the DM Server.

Upon reception of the message sent from the Device, DM Server authenticates the sender by comparing the DeviceDigest1 to ServerDigest2. If they match then the device is authenticated, the server processes the message. If they don't match then the server shall challenge the device.

ServerDigest2 = H(B64(H(IMEI:secret)):snonce2:B64(H(content)))

Where H is the MD5 hashing function, B64 is Base64, secret is the secret of the device (refer to Device Provisioning), IMEI of the device (refer to Device Provisioning), snonce2 is the server nonce (number used once) as stored on the server, content is body the incoming message payload

At the very first time (device out of box), snonce1 is set to the default nonce (factory setting). And on the DM Server, snonce2 is set to the default nonce. This latter is defined during the Device Provisioning procedure. Therefore the snonce1 and snonce2 are identical at the first message exchange, which leads to client authentication success.

Note that the secret is never transmitted.

The DM Server shall use this procedure upon receiving messages over the Device Management protocol.

4.3.5.7 Device Management Session

Device Management session shall always be initiated by the device, to post data to the DM server or either upon receiving a notification message (bootstrap or wake-up) from the DM server.
The session is composed of 2 phases:

1) Setup phase, where the client authentication and server authentication are performed, as described in 4.3.5.5 and 4.3.5.6. The device includes authentication information in the request. If the client is authenticated by the DM server, this latter sends server credentials along with initial Device Management commands back to the client.
2) Management phase starts once the server is authenticated by the device. In the new request, the device starts sending responses with respect to the DM commands issued by the server (e.g. current device configuration, status). The server retrieves and stores the information, and can issue new DM commands in the response message. The device makes new request to the DM server as long as the response from the DM server contains DM commands. The session is ended whenever the DM server responses with an empty message.

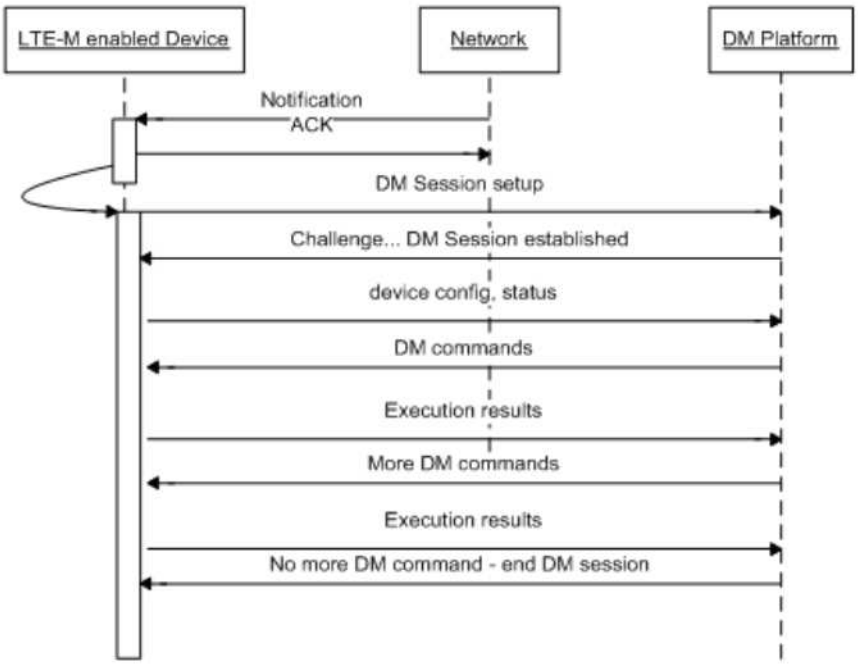

Figure 4—19. Device Management Session

4.3.5.8 Management Objects

Device attributes and properties are exposed via Management Objects. Each device contains a management tree. This latter organizes all available management objects in the device as a hierarchical tree structure where all nodes can be uniquely addressed with a Uniform Addressed Identifier (URI). Attributes can be represented in nodes and are accessible via the URI.

DM Server also contains a copy of the management tree for every device. The management tree can be changed based on User actions applied to the device, or changed by the device based on device's actual status or attributes.

Attributes have properties stating the access rights for the device and for the DM server. For example, device ID is read-only. The device temperature is read-only for the server whilst the device has read/write access to this attribute.

DM commands are exchanged between DM server and device over DM sessions. Each DM Command is specified by a method, an URI and potentially, a value.

The key methods are: Get, Replace, Add, Delete, Exec, Alert.

The number of DM commands is issued by the server based on the management objects trees difference in the device and in the server. This operation is a tree alignment process, also known as data synchronization.

The Management Objects and methods will be defined in further stages of EXALTED project and included in future reports.

4.3.5.9 User controls

Users (Service provider or end user) can interact with the DM server by the way of the User Interface building block. The GUI reads the management object tree of a selected device in the DM Server, and displays the attributes (value of nodes) on the GUI. The figure below depicts 2 user operations:

- Get an updated list of devices along with their attributes.
- Modify an attribute of the device.

The first operation does not create pending DM command, as this operation does not affect the device.

In the second operation, the user is altering the attribute1 of the device xyz. This change creates a pending action on the DM server. This action will be transmitted to the device xyz as a DM command with a "replace" method. Upon receiving this DM command, the device will be replacing the value of the attribute1 by the user defined value.

This user-defined action can only be transmitted over a DM session initiated by the device. Therefore, in order to apply urgent actions on device, DM server can send Wake-up notification message to targeted device in order to trigger an immediate DM session.

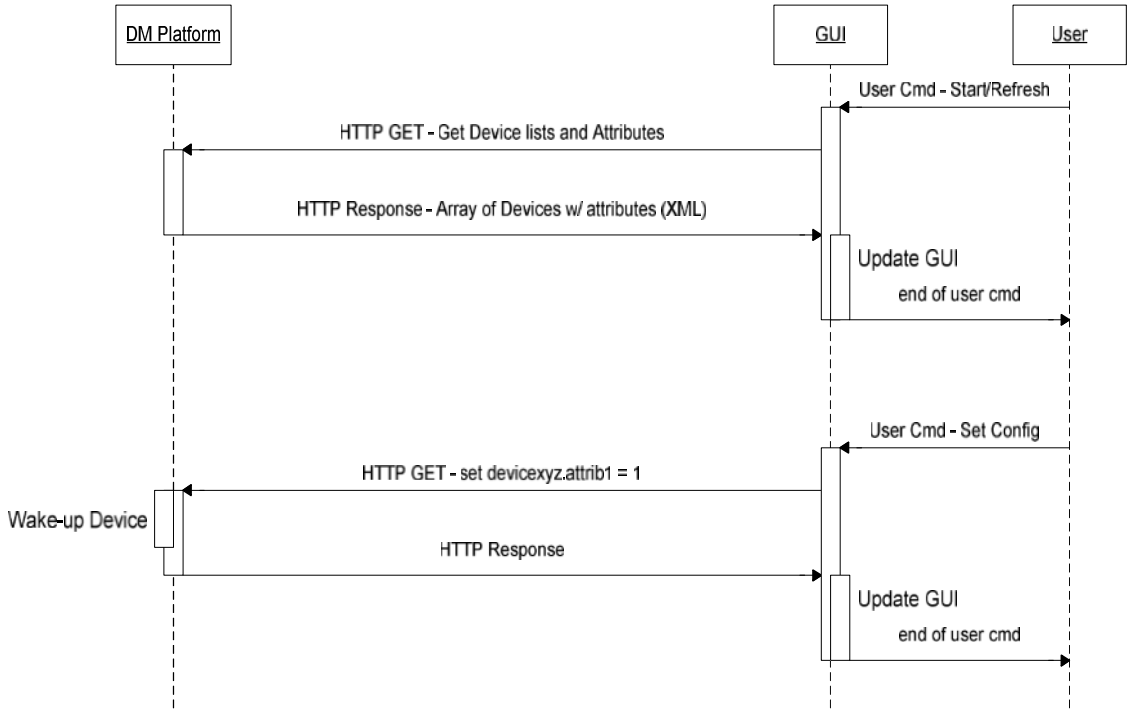

Figure 4—20. User interaction with devices

4.3.6 End-to-end Activities Flow

This section provides an end-to-end sequence activities involved by all sub-systems. Such overview is detailed for few use cases:

1) Supporting new device.
   This use case is necessary in all scenarios. The following flows are depicted in the below activities diagram :
   - At power up, a new device attaching to a new gateway.
   - Upon successful device pairing, the gateway connects to the DM server.
   - As the gateway is not provisioned in the Server, the connection is denied.
   - User provides provisioning information related to the gateway to be supported by the server.
   - DM Server preserves provisioning information into local database.
   - The new gateway makes a new attempt to establish a DM session with the server.
   - As the new gateway has been provisioned previously, the DM session is established upon successful device authentication.
   - The new gateway sends gateway info (configuration, status, attributes) along with all attached devices info to DM server.
   - DM server updates the database with Gateway data.

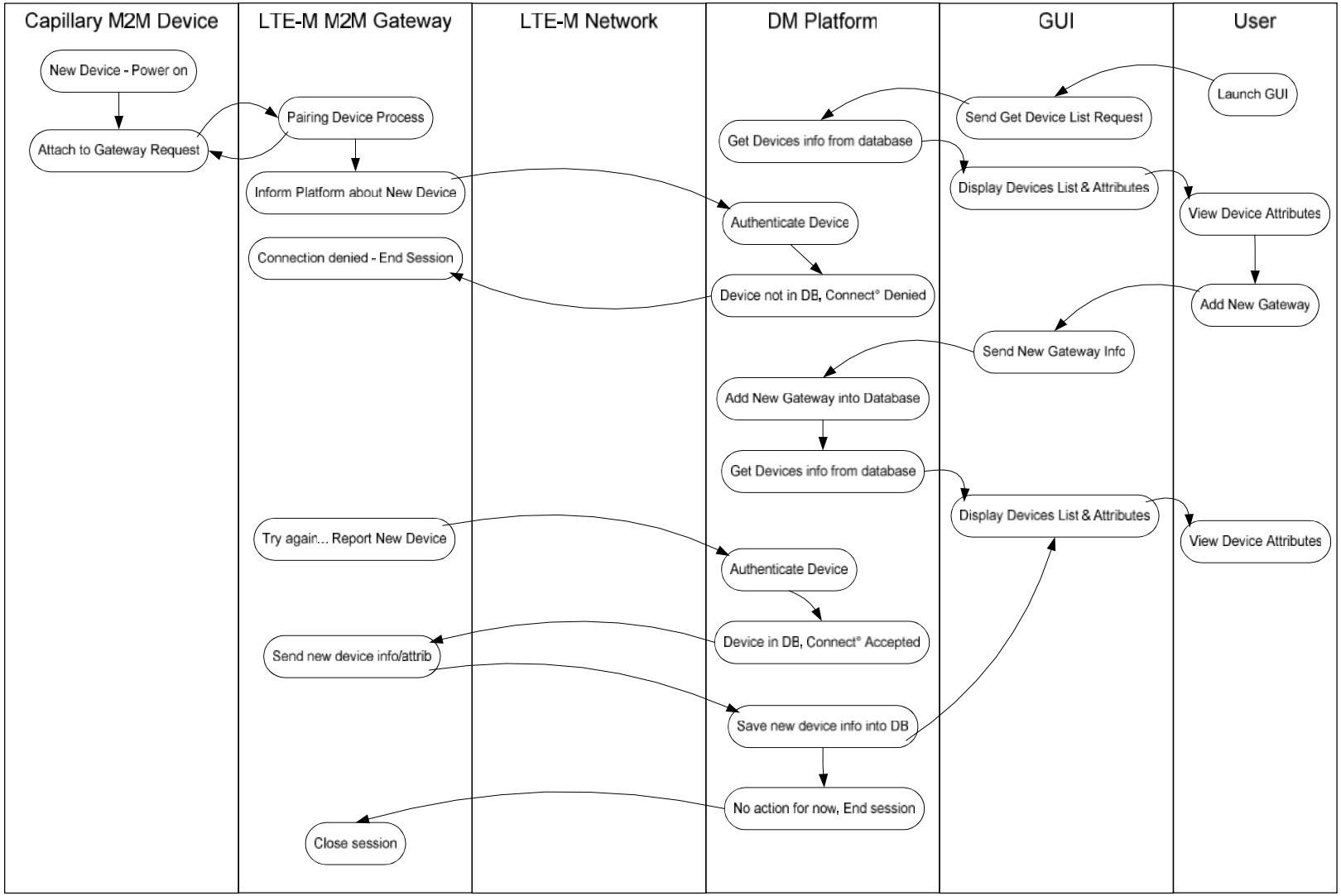

Figure 4—21. Activities diagram for use case: Supporting New device

2) Changing an attribute of a selected Device.
   This use case can demonstrate Industrial Remote Control scenario (e.g. remotely turn on/off engine, street lights...). This use case encloses several functions such as:
   - Retrieve devices list along with device status and attributes from database.
   - Preserve the new device attribute as defined by the user.
   - Create notification message with embedded secure elements. This can be a bootstrap message.
   - Interaction with the network to send notification.
   - Setup connection request from device/gateway, including authentication and challenge. Device authentication is based on information provided at the Device Provisioning phase. Must be performed over the DM protocol.
   - Retrieve current devices info (configuration, status, attributes) from gateway, and update the DM server database.
   - Synchronize the device attribute defined by the user: if current attribute is different than the one defined by the user, then create DM command in order to change the attribute in the device.
   - Send the DM command to the targeted Device over the DM protocol.

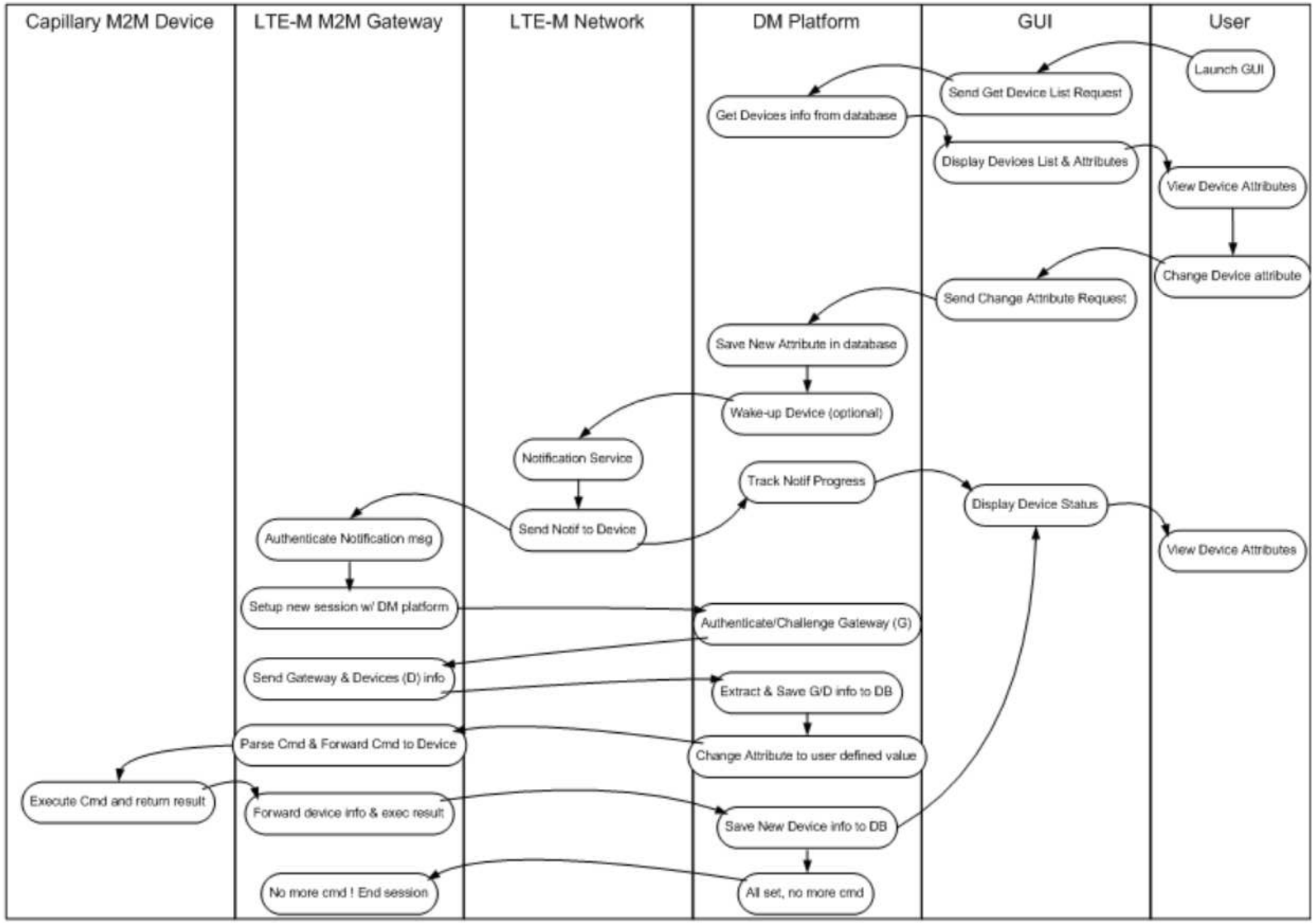

Figure 4—22. Activities diagram for use case: Device Provisioning and Device Authentication

Identified activities will be studied and detailed in the next report D7.2.

4.3.7 System Scalability

The key novelty is the small data footprint involved in the device management procedures. The sizes of payloads and device management procedures have direct impact on device's power/resource consumption, and on system scalability.

The proposed device management protocol and procedures will be benchmarked against a reference standardised protocol (e.g. OMA-DM or TR-069). Thus, the gain in term of footprint and procedures can be highlighted. This comparison will provide indication on the system scalability improvement.

More information on the scalability specification will be provided in D7.2.

4.3.8 Timeline and milestones

This section describes the development plan for Device management testbed.

Table 4—13.Milestones for Device management testbed

Milestone	Description	Envisaged Completion
M3.1	Initial proposal of DM protocol & Management Objects (MOs)	M19
M3.2	Architecture reviewed based on DM protocol & Management Objects revisions	M20
M3.3	Start development – development version of DM session & security	M20
M3.4	Mock-up of user interface	M21
M3.5	Finalized Architecture and all DM goals (protocol, MOs, procedures)	M24
M3.6	Integration with device	M25
M3.7	Continuous integration and Validation process with partners	M26-M30
M3.8	Fully implemented testbed	M30

4.3.9 Scenario mapping

As device management testbed is an application conceived to be implemented over the same hardware used by connectivity oriented testbed, the same parameters depicted in Table 4—10 are as well applicable to this case.

In addition to that parameters, some extra ones can be fixed regarding pure device management needs, and they are listed on the following table.

Table 4—14. Requirement quantification from scenarios regarding testbed 3.

Device Management		Justification
Protocols	Message size < OMA-DM v1.3	Low-cost devices are mostly Constrained devices. They are battery-operated and have limited resources such as memory footprint, processing capability.
	Transmitted message size < OMA-DM v1.3	
	Lightweight message encoding scheme < OMA-DM v1.3	

	Scalability	The number of M2M devices is expected to much larger than mobiles devices.

5. Conclusions

This document reflects the initial steps done in the creation of different testbeds that will be further used for demonstrating the technical achievements of EXALTED project. The project uses three main scenarios so as to fulfil the complete set of researches done in the technical WPs. In order to provide as much details as possible, the document has gone through the initial steps based on expected individual contributions and the envisioned technical developments that will be performed within EXALTED framework.

EXALTED has identified three target scenarios defined as a part of the work done in WP2. Those are:

- Intelligent Transportation Systems - communication of vehicles and transport infrastructure with ITS application servers, which controls parameters such as transportation time, traffic collision avoidance, on-board safety, fuel consumption, and many others.
- Smart metering and monitoring - very applicable use case of industrial, environmental, energy, and other types of monitoring.
- E-Health - a relationship between a healthcare organization and a patient, established through the M2M communication.

These scenarios have been used as the reference for defining a set of requirements detected by the technical WPs of the project that should be achieved during the development of the project and that could be demonstrated as a part of the activities to be done in this WP.

Taking into consideration all the initial information collected, it is necessary to include the different constraints detected at different levels. They are summarized in the following lines:

- Technological constraints:
  - There is no LTE-M core network, so only a subset of LTE-M concepts can be tested.
  - Due to logistics constrains, some of the simulation equipments cannot be displaced.
  - The study of the LTE-M physical layer is crucial but is also complex; hence it is more convenient to study it separately from the other aspects.
  - LTE networks might not be deployed at the time and location of the experimentation.
- Financial constraints:
  - There is no financial, realistic possibility to handle more than a dozens of devices.
  - We cannot develop a complete LTE-M protocol stack nor modify an existing LTE stack, given the available human resources.

Considering the aforementioned concepts and constraints, EXALTED project proposes three main testbeds for demonstrating different concepts:

- **LTE-M Architecture Scenario**. This scenario focuses its effort in demonstrating aspects related to the PHY and MAC layers of the LTE-M System Architecture.
- **Connectivity oriented scenario**. The scope of the verifications developed within this scenario is to demonstrate packet data continuity among nodes regardless their position in the network.

- **Device Management Scenario**. This scenario demonstrates the different device management protocols including security considerations, also using the capabilities offered by the previous scenario.

At this stage of the project we are able to present the key building blocks that will compose each of the testbeds and the interfaces that will connect those blocks. The Table 5—1 summarizes the blocks identified currently.

Table 5—1. Key building blocks of each scenario

Scenario	Block	Description
LTE-M Architecture	LTE-M Base Station	Performs communications between LTE terminals to the network.
	LTE User Equipment	Check backwards compatibility of LTE-M solution.
	LTE-M Terminal	Check the validity of the developed specific LTE-M protocols.
Connectivity oriented	LTE-M Network	Access to the core network. Emulated in this scenario.
	Core IP Network	Main Internet Network, accessible to M2M nodes via the LTE-M cellular network.
	Capillary Network	Group of nodes that are connected to the LTE-M network through a Gateway.
	Gateway	Interconnects LTE-M and Capillary network worlds.
	LTE-M enable device	Devices that can be directly connected to the LTE-M network. They are IP-enabled.
	M2M device	Devices that need a Gateway to access to the public network.
	Device management server	Server located on the core IP network in charge of managing M2M devices.
	Secure element	Specific security module embedded on M2M devices, that allows them to authenticate and communicate in a secure way.
Device Management (apart from the ones present on Connectivity oriented scenario)	User Interface	Allows service provider and end-user to remotely control the devices.
	LTE-M enable device/Gateway	Devices/Gateways directly connected to the LTE-M network.
	M2M Device	Devices that need a Gateway to reach the LTE-M network.

In order to integrate together all these blocks, coming from the different partners contributions, the following Table 5—2 milestone and deadline will be followed..

Table 5—2. Overall Milestones and deadlines.

Testbed	Milestone	Description	Envisaged Completion
1	M1.1	Implementation of an LTE-M link-level simulation chain	M12
	M1.2	Selection of promising algorithms.	M24
	M1.3	Set-up of the testbed	M24-M27
	M1.4	Operation of the complete testbed and detailed performance evaluation.	M30
2	M2.1	Fully operative capillary network. Enabled communications between M2M nodes and Gateways.	M15

	M2.2	Enabled communications between nodes and application server on the core network.	M22
	M2.3	E2E communication. Capillary network cooperation.	M27
	M2.4	Validation of the implemented concepts	M30
	M2.5	Secure element integration on M2M devices	M20
	M2.6	Delegation of secure mechanisms to Security Server.	M27
3	M3.1	Initial proposal of DM protocol & Management Objects (MOs)	M19
	M3.2	Architecture reviewed based on DM protocol & Management Objects revisions	M20
	M3.3	Start development – Mock-up of DM session & security	M20
	M3.4	Mock-up of user interface	M21
	M3.5	Finalized Architecture and all DM goals (protocol, MOs, procedures)	M24
	M3.6	Integration with device	M25
	M3.7	Continuous integration and Validation process with partners	M26-M30
	M3.8	Fully implemented testbed	M30

Finally, considering the complementarities presented in the last two scenarios, both of them could be integrated into a single testbed that may integrate all the concepts aimed to be demonstrated.

List of Acronyms

Acronym	Meaning
3G	Third Generation
3GPP	3rd Generation Partnership Project
ACK	Acknowledge
ADC	Analog to digital converter
AMR	Automated Metering Reading
API	Application Programming Interface
ARM	Advanced RISC Machine
CAN	Controlled Area Network
CDMA	Code division multiple access
COPD	Chronic Obstructive Pulmonary Disease
CVD	Cardiovascular Diseases
DAC	Digital to Analog Converter
DHCP	Dynamic Host Configuration Protocol
DI	Device Identifier
DM	Device Management
DMT2	Diabetes Mellitus Type 2
DSL	Digital Subscriber Line
DSO	Distribution System Operator
E2E	End to end
ECG	Electrocardiogram
ETSI	European Telecommunications Standards Institute
EXALTED	Expanding LTE for Devices Project
GFDM	Generalized Frequency Division Multiplexing
GPIO	General Purpose In/Out
GPRS	General packet radio service
GPS	Global Positioning System
GSM	Global System for Mobile
GUI	Graphical User Interface
HDP	Health Device Profile
HLR	Home Location Register
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
HW	Hardware
I/O	In/Out
I2C	Inter-Integrated Circuit
ICCID	International Circuit Card ID
IF	Intermediate Frequency
IG	Intelligent Gateway
IMEI	International Mobile Equipment Identity

IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IR	Internal Report
ITS	Intelligent Transportation System
ITU	International Telecommunication Union
JTAG	Joint Test Action Group
LAN	Local Area Network
LTE	Long Term Evolution
LTE-A	Long Term Evolution Advanced
LTE-M	Long Term Evolution Network with M2M enhancements
M2M	Machine to Machine
MAC	Media Access Control
MCAP	MultiChannel Adaptation Protocol
MedWG	Medical Working Group
MIMO	Multiple-Input, Multiple Output
MISO	Multiple-Input, Single Output
MSISDN	Mobile Station Integrated Services Digital Network
MTC	Machine type communication
NAT	Network Address Translation
NFC	Near Field Communication
OBU	On Board Unit
OEM	Original Equipment Manufacturer
OFDMA	Orthogonal Frequency-Division Multiple Access
OS	Operating System
P/BAN	Personal/Body Area Network
PC	Personal Computer
PHY	Physical Layer
PoC	Proof of Concept
RF	Radio Frequency
RFID	RF Identification
RIA	Rich Internet Application
RRM	Resource Radio Management
SC-FDMA	Single Carrier Frequency Division Multiple Access
SDIO	Secure Digital I/O
SDRAM	Secure Digital Random Access Memory
SIG	Special Interest Group
SIM	Subscriber Identity Module
SIMO	Single-Input, Multiple Output
SISO	Single-Input, Single Output
SMS	Short Message Service
SPI	Serial Peripheral Interface
SW	Software
TBD	To Be Determined
TCP	Transmission Control Protocol
TMSI	Temporary Mobile Subscriber Identity

UART	Universal Asynchronous Receiver-Transmitter
UDP	User Datagram Protocol
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
URI	Uniform Addressed Identifier
USB	Universal Serial Bus
WCDMA	Wideband Code Division Multiple Access
WP	Work Package
WWRF	Wireless World Research Forum
XML	Extensible Markup Language

References

[1] FP7 EXALTED: “D2.1 - Description of baseline reference systems, scenarios, technical requirements & evaluation methodology,” project report, May 2011.

[2] FP7 EXALTED: “D3.1 - First report on LTE-M algorithms and procedures” project report, September 2011.

[3] FP7 EXALTED: “D3.2 - Study of commonalities and synergies between LTE-A and the heterogeneous network” project report, September 2011.

[4] FP7 EXALTED: “D6.1 - Optimizing a Linux Operating System for M2M devices” project report, May 2011.

[5] MATLAB, Mathworks product. http://www.mathworks.com/products/matlab/

[6] Signalon HaLo. http://www.signalion.com/33-0-HaLo-awarded.html

[7] Signalon Sorbas. http://www.signalion.com/143-0-Signalion-Sorbas-eNodeB-test-products-provide-dual-mode-support-for-3GPP-LTE-FDD--TDD-.html

[8] TSmarT platform. http://www.tst-sistemas.es/en/products-2/tsgate

[9] Digi Xbee Zigbee module. http://www.digi.com/products/wireless-wired-embedded-solutions/zigbee-rf-modules/zigbee-mesh-module/

[10] Sagemcom Hilo 3G module. http://www.sagemcom.com/index.php?id=1415&L=0