European Commission
Information Society and Media

SEVENTH FRAMEWORK PROGRAMME

Large Scale Integrating Project

EXALTED

Expanding LTE for Devices

FP7 Contract Number: 258512

WP2 – Business Models, Use cases & Technical Requirements

D2.3
The EXALTED system architecture (Final)

Contractual Date of Delivery:	31 August 2012
Actual Date of Delivery:	31 August 2012
Responsible Beneficiary:	UPRC
Contributing Beneficiaries:	SCET, EYU, ALUD, TKS, CEA, TST, UNIS, CTTC, UPRC, VID
Estimated Person-Months:	29
Security:	Public
Nature	Report
Version:	1.0

Document Information

Document ID: EXALTED_WP2_D2.3.doc
Version Date: 31 August 2012
Total Number of Pages: 61

Authors

Name	Organisation	Email
Athanasios Lioumpas (Editor)	UPRC	lioumpas@unipi.gr
Stephan Saur	ALUD	Stephan.Saur@alcatel-lucent.com
Nemanja Ognjanovic	TKS	nemanjao@telekom.rs
Bernard Hunt	UNIS	b.hunt@surrey.ac.uk
Djelal Raouf	SWIR	draouf@sierrawireless.com
Bruno Corlay	SWIR	bcorlay@sierrawireless.com
Nhon Chu	SC	nhon.chu@sagemcom.com
Juan Rico	TST	jrico@tst-sistemas.es
Javier Valiño	TST	jvalino@tst-sistemas.es

Executive Summary

The purpose of this document is to present the EXALTED system architecture, which supports the enhanced functionalities, protocols and service provisioning developed in the project's technical work packages. The EXALTED project focuses on Machine-to-Machine (M2M) communications, and, as its name implies (ExpAnding LTE for Devices), the natural ecosystem of EXALTED is to be found within the 3rd Generation Partnership Project (3GPP) and Long Term Evolution (LTE) specifications. More specifically, the EXALTED Architecture leverages and enhances the 3GPP Machine Type Communications (MTC) Architecture [1].

Though the focus of EXALTED is on M2M communications, the EXALTED Project couldn't afford to ignore that important initiative to set up a framework for M2M applications which is ETSI M2M [2]. Therefore, the EXALTED Architecture tries to meet the ETSI M2M functional specifications whenever they fall within the EXALTED scope of work. In particular, the EXALTED architecture consists of two so called domains, namely the Network Domain (ND) and the Device Domain (DD).

Since backward compatibility is a major target in EXALTED, the ETSI M2M (Machine-to-Machine) [2] and the 3GPP MTC (Machine-Type Communications) [1] system concepts have influenced the EXALTED architecture. However, in order to achieve the project objectives, several modifications, enhancements and simplifications have been proposed.

The ND comprises the access network, the core network, the M2M service capabilities layer (SCL), the M2M applications, the management functions and the M2M server. The access network in EXALTED is the LTE-M system [3], which is an expanded version of LTE for supporting M2M communications, while the core network is that assumed by 3GPP [1]. The M2M server is a key element in the EXALTED architecture, which offers M2M SC, applications and management functions (Section 3.1). The DD includes also a SCL, the LTE-M enabled devices (i.e. the M2M Gateway and the LTE-M end devices) and the non-LTE-M devices, i.e. the non-LTE-M cluster heads and the non-LTE-M end devices. Moreover, it is possible to for applications to run within the DD (Section 3.1).

This deliverable describes the required functionalities at each of these components regarding the knowledge provided by technical WPs, which are the ones developing the respective algorithms with the required functionality. These functionalities are straightly related with the technical requirements, extracted in previous deliverables based on the use cases of interest. For each requirement or a group of requirements specific solutions were developed by the technical work packages (WP).

Additionally, the interfaces between the components and the layers involved in the protocol stacks are identified. The purpose of interfaces is to enable the signalling exchange between the components on the respective layer in order to provide the support of related services and also to consider dependencies between the components. In a simplified view three types of interfaces are considered: peer-to-peer interfaces characterized by lower layer (L1-L3) protocols, interfaces providing L3 IP connectivity, and, finally, higher layer (L4-L7) interfaces providing E2E connectivity.

Finally, D2.3 will be complemented by D2.4 (to appear) that will describe the EXALTED system concept and its performance.

Table of Contents

Executive Summary ..... **iii**

Table of Contents ..... **iv**

1 Introduction **1**

2 Baseline architectures **2**

2.1 The ETSI M2M architecture **2**
2.1.1 Domains 2
2.1.2 Service Capabilities and Service Capability Layers 3
2.1.3 Reference Points 4
2.1.4 Point of Contact 5
2.1.5 Resources 5
2.1.6 Possible Organization of xSCL 7
2.2 The 3GPP MTC architecture **7**
2.2.1 Network elements 8
2.2.2 Reference points 9
2.3 Beyond the 3GPP and ETSI architectures **9**

3 The EXALTED architecture **11**

3.1 Components of the EXALTED system architecture **12**
3.1.1 ETSI, 3GPP and EXALTED terminology equivalences 13
3.1.2 Components in the ND 14
3.1.2.1 M2M Server 14
3.1.2.2 Evolved Packet Core (EPC) 14
3.1.2.3 LTE-M eNB 15
3.1.2.4 LTE-M relay 17
3.1.3 Components in the Device Domain (DD) 17
3.1.3.1 LTE-M device (LTE-M enabled device) 17
3.1.3.2 M2M Gateway (LTE-M enabled device) 19
3.1.3.3 Non-LTE-M enabled device (non LTE-M enabled device) 21
3.1.3.4 Non-LTE-M Cluster Heads (CHs) (non LTE-M enabled device) 22
3.1.4 Summary of the EXALTED features 22
3.1.4.1 The LTE-M access network 22
3.1.4.2 EXALTED capillary networks and E2E aspects 25
3.1.4.2.1 Innovative functionalities enabled by the Gateway 26
3.1.4.2.2 Innovative functionalities enabled within the capillary network 26
3.1.4.2.3 Device management functionalities 27
3.1.4.2.4 Low cost security 28
3.1.4.2.5 Device self-diagnostic 29
3.2 Interfaces in the EXALTED architecture **30**
3.2.1 Interfaces between EPC components and LTE-M components 34
3.2.2 Interfaces between LTE-M eNB and LTE-M devices/gateways (I-4, I-5) 35
3.2.3 Interfaces between LTE-M components (LTE-M eNB/GW) and capillary networks 36
3.2.4 Other Interfaces (reference points) 40
3.3 Supported communications scenarios in EXALTED **40**
3.3.1 Communication of Devices with Application Servers in the IP network (Type 1) 41
3.3.2 Communication between Devices (Type 2) 44
3.4 Security aspects of the EXALTED architecture **48**

3.4.1 Embedded secure element to create application level security....49
3.4.2 Role of the M2M Gateway in security....49
3.4.3 Key hierarchy....50

4 Conclusion.... 52

Appendix.... 53

A1. EXALTED technical requirements....53

List of Acronyms.... 54

References.... 58

1 Introduction

This document introduces the *EXALTED system architecture*. Previous deliverables related to architecture [3]-[7] aimed to convey to the technical work (related to the LTE-M system, the end-to-end (E2E) connectivity, the security and device improvement) those components and requirements, necessary to realize the EXALTED system concept. Following a thorough investigation of the most emerging M2M applications and use cases, the most critical requirements (e.g. functional requirements, network requirements, and service requirements), were identified towards the development of the necessary corresponding algorithms, procedures and technologies. The system architecture aims to provide a coherent framework, ensuring that all technical innovations are aligned towards a unified system concept, able to achieve the project's objectives. Through an iterative process between the technical innovations and the system architecture, and after cycles of refinements and interactions between contributors covering different parts of the EXALTED system, the final architecture provides a consolidated view of the EXALTED concept.

The work in EXALTED is founded on two existing proposals that are considered as baseline architectures, namely 3GPP MTC [1] and ETSI M2M [2], which are briefly summarized in Section 2. However, for the achievement of the EXALTED objectives, it is not sufficient to adopt ETSI M2M or 3GPP MTC as they are. Note that at the next ETSI M2M meeting plenty of contributions are expected towards the document "TS 101 603 Machine-to-Machine communications (M2M); 3GPP Interworking" aiming to a combined ETSI/3GPP Architectural Model. Given the diversity of requirements between the M2M use cases (i.e. ITS, SMM, E-health), the development of a unified generic and flexible architecture applicable to all type of services has proven to be a great challenge, especially under the prerequisite of the compatibility with the ongoing standardization activities. To this end, influenced by the baseline architectures [2] and [1], the necessary enhancements at the Network Domain (ND) and the Device Domain (DD) were identified, in order to leverage on these standardization efforts and complement them with new sets of features needed to provide cost, energy, and spectrally efficient connectivity to devices.

The working assumption for the EXALTED architecture is that it consists of various *components* characterized by their *functionalities*. A component can either be a physical entity, e.g. a M2M device, or a logical element summarizing certain functions that are in reality distributed at different locations, e.g. the Evolved Packet Core (EPC). Section 3.1 presents all components that build up the EXALTED architecture. The different *interfaces*[1] between these components are identified in Section 3.2 The functionality of a component can be realized by *algorithms*, and interfaces can be implemented with *protocols*. Candidate algorithms and protocols are being developed in the WP3-WP6 and are part of the *EXALTED system concept*. They are exchangeable without impact on the architecture design itself and won't be detailed in this report. The purpose is to define components, their functionality and their interactions. Finally, D2.3 will be complemented by D2.4 (to appear) that will describe the EXALTED system concept and its performance.

[1] The definitions are adopted from the "Vocabulary for 3GPP Specifications" [8]
- **Interface**: the common boundary between two associated systems.
- **Layer interface**: The interface between adjacent layers of hierarchy of layers.
- **Layer**: A conceptual region that embodies one or more functions between an upper and a lower logical boundary within a hierarchy of functions.
- **Physical interface**: The interface between two equipments.
- **Reference point**: A conceptual point at the conjunction of two non-overlapping functional groups
- **Functional group**: A set of functions that may be performed by a single equipment.

2 Baseline architectures

Two baseline architectures are considered for the work in EXALTED, namely 3GPP MTC [1] and ETSI M2M [2]. 3GPP MTC mainly focuses on the communications, while ETSI M2M focuses on the applications. In the following their paradigms and characteristics are briefly summarized. However, the goal of EXALTED is not to simply adopt these architectures, but to establish a complete architecture with additional options. The ETSI and 3GPP architectures are the result of long-lasting efforts, but still some gaps remain. For example, in the 3GPP architecture the E2E aspects of communication between MTC devices and MTC servers, or the functionalities provided by the MTC Server itself are out of scope [1]. On the other hand, ETSI architecture does not specify the Radio Access Network (RAN) that links the DD with the ND [2]. The EXALTED architecture can be considered as an enabler, based on 3GPP MTC, for specific Service Capabilities required by ETSI M2M-based applications.

2.1 The ETSI M2M architecture

This section gives an overview of the ETSI M2M architecture [2]. The main scope of the ETSI architecture is to specify a framework for developing M2M applications with a generic set of capabilities, independently of the underlying network. Its key architectural elements are domains (see 2.1.1), service capabilities (see 2.1.2), reference points (see 2.1.3), point of contact (see 2.1.4), and resources (see 2.1.5) . Beside these key architectural elements, the ETSI M2M architecture also defines procedures for security and bootstrap, which are not described here.
Finally a possible organization of service capabilities is described in section 2.1.6.

2.1.1 Domains

Domains represent scopes to run M2M business applications. Each domain can potentially be operated respectively by a different actor of the M2M market. Depending on the location where these M2M applications reside, two domains have been defined: the ND and the Device and Gateway Domain as shown in Figure 2-1.

- **Network Domain**

The Network Domain is mainly composed of the following elements:

- The Core Network (CN) essentially provides:
  - IP connectivity
  - Interconnection with other networks
  - Roaming with other CNs
  - Service and network control functions
- The Access Network (AN) represents the link, e.g. RAN, to allow an M2M Device or an M2M Gateway to access CN services.

Beside CN and AN, the ETSI M2M architecture defines Network Management functions located in the CN or the AN, and M2M Management functions located at M2M Application level.

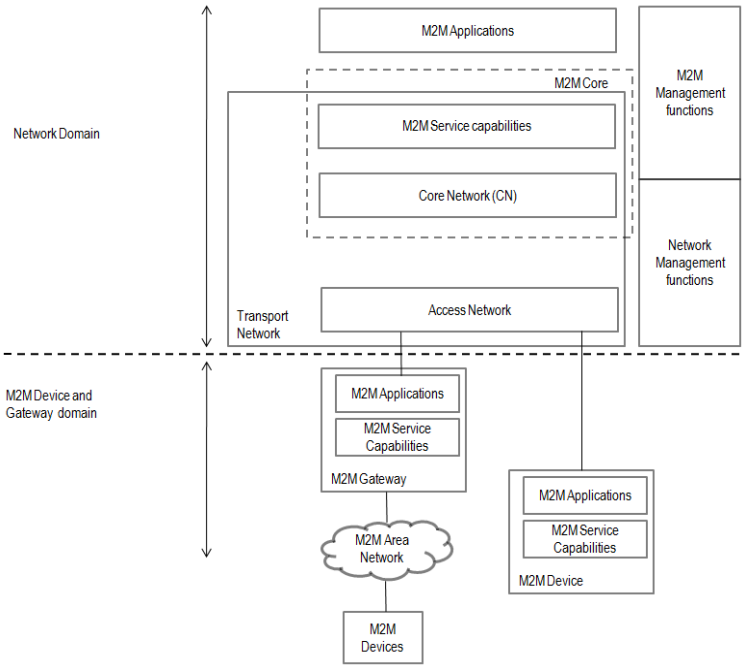

Figure 2-1: High-level view of ETSI M2M architecture [2]

- **Device and Gateway Domain (D/GD)**

The Device and Gateway Domain is composed of M2M Devices and gateways which connect to the ND according to two connectivity models:

- Direct connectivity through the AN
- Indirect connectivity through an M2M Gateway. The M2M Gateway acts as a proxy between M2M Devices and the ND through the AN. The ETSI M2M Functional Architecture document further specifies that an M2M Device can connect to several M2M gateways.

2.1.2 Service Capabilities and Service Capability Layers

M2M Service Capabilities (SC) are functionalities offered to M2M Applications by each domain and shared by different applications. SC can use CN functionalities through a set of exposed interfaces, e.g. existing interfaces specified by 3GPP, 3GPP2, ETSI TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking). SC can also invoke other capabilities. Additionally, SC can interface to one or several Core Networks. Interfaces towards Capabilities in other M2M Service Capabilities Domains are for further study. These functionalities are offered under the form of resources and uniform methods to access these resources. The Service Capability Layer (SCL) exposes these functionalities on Reference Points, described in section 2.1.3. Whenever a feature provided by a domain is directly manipulable by an M2M Application, it should reside in the corresponding SCL. The list of M2M Service Capabilities (SC1 to SC11) is provided in

Table 2.1, while the ETSI's SC (SC1-SC8) functional architecture is depicted in Figure 2-2.

Table 2.1: ETSI M2M Service Capabilities.

SC1	Application Enablement (xAE)	where x : N for Network. G for Gateway D for Device
SC2	Generic Communication (xGC)	
SC3	Reachability, Addressing and Repository (xRAR)	
SC4	Communication Selection (xCS)	
SC5	Remote Entity Management (xREM)	
SC6	SECurity (xSEC)	
SC7	History and Data Retention (xHDR)	
SC8	Transaction Management (xTM)	
SC9	Compensation Broker (xCB)	
SC10	Telco Operator Exposure (xTOE)	
SC11	Interworking Proxy (xIP)	

Not all M2M SCs are foreseen to be instantiated in the different parts of the system.

The M2M SCs above provide recommendations of logical grouping of functions, but does not mandate an implementation for M2M SCs. The M2M SCs are therefore not represented as separate entities in the flow charts. However, the external interfaces are mandated and are required for ETSI M2M compliance.
At the time of the writing of this document, the routing function between SC is not standardized and thus left to the implementation.

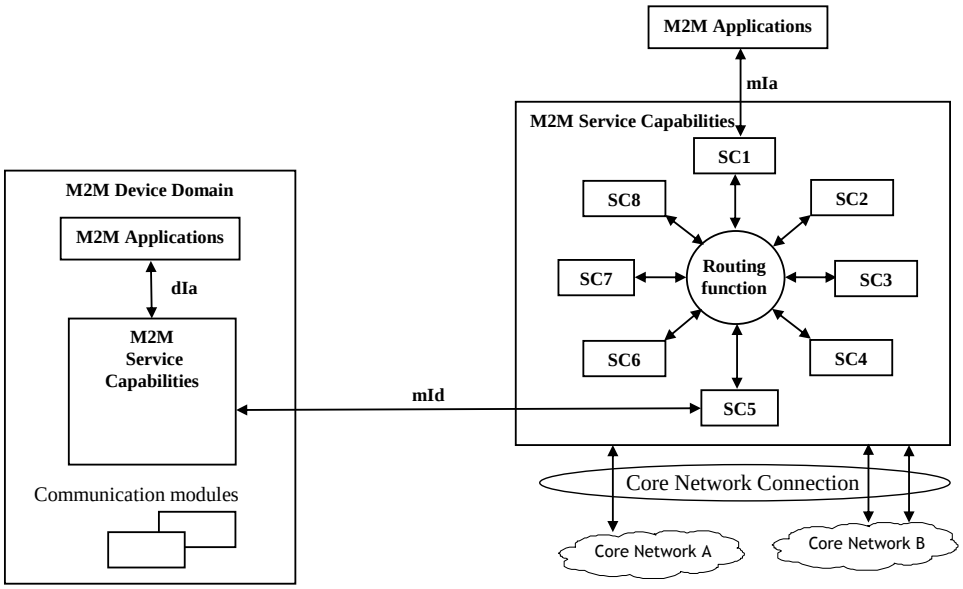

Figure 2-2: ETSI's M2M Service Capabilities functional architecture [2]

2.1.3 Reference Points

Reference points represent open interfaces to which SC are attached. This is illustrated in Figure 2-3. In the following points the reference points *mla*, *mld* and *dla* are explained.

- **mla**
  This reference point exposes SC of the CN to M2M Applications in the Network Domain. More specifically, this reference point establishes an interface between an M2M

Application in the Network Domain and the NAE Service Capability. An M2M Application in ND accesses all network SC through NAE over mIa.

- **mId**
  This reference point allows the communication between Device SCL (DSCL) or Gateway SCL (GSCL) with Network SCL (NSCL) over the Core Network. More specifically, this reference point establishes an interface between a Device or Gateway Service Capability and the NGC Service Capability. A service capability in the DSCL or the GSCL accesses all network SC through NGC over mId.

- **dIa**
  This reference point exposes SC of the M2M Device or M2M Gateway to M2M Applications running in the same device or in the associated Gateway. More specifically, this reference point establishes an interface between an M2M Application in the Device and Gateway Domain and the DAE or GAE Service Capability. An M2M Application in D/GD accesses all device or Gateway SC through DAE or GAE over dIa.

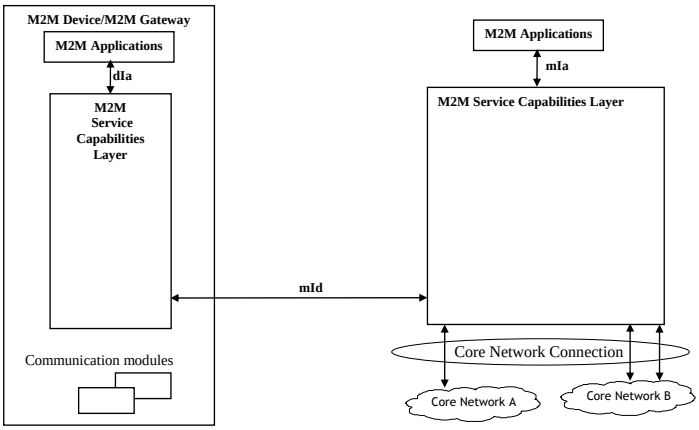

Figure 2-3: ETSI M2M reference points [2]

2.1.4 Point of Contact

In the D/GD, to each application and SCL that may either reside on the Device or in the Gateway is associated a Point of Contact (PoC) which is a set of information needed to reach it from ND. This usually takes the form of an URI encoding the IP address of the Device or the Gateway.
The PoC is maintained in NSCL (via a specific resource, see 2.1.5) and the Device or the Gateway is responsible for keeping the PoC up-to-date.
In a mobility context, the Device or the Gateway may detach then reattach to the cellular network, thus changing the IP address. It must update the PoC in the NSCL as well.

2.1.5 Resources

Resources are abstract structures residing in the SCL and offering capabilities to M2M Applications and other SC to exchange information. The ETSI M2M architecture promotes a RESTful (Representation State Transfer) architectural concept and applications access to resources over mIa and dIa reference points following REST guidelines. Similarly, DSCL and GSCL access the NSCL over mId reference point following REST guidelines.

It is useful to explain briefly what the REST concept is (see [9] for the complete description). This concept was introduced by Roy Fielding in his doctoral dissertation to explain the underlying concepts of HTTP 1.1 ([10]) to which he was one of the contributors. REST is a client-server architecture based on four fundamental principles:

1. **Resources**. These are abstract entities to identify services offered by the server. Resources must have a precise, invariable semantic and must be named according to Uniform Resource Identifier (URI) schemes (see [11]). When the client accesses a resource on the server, a representation of it is exchanged between the client and the server for data transmission. No “out-of-band” transmission of data, e.g. based on the URI itself and not its representation, is allowed.
2. The client must access the resources via their URI using the **four uniform methods**: CREATE, RETRIEVE (or READ), UPDATE, and DELETE. These methods are commonly denoted **CRUD** after the initials of each of them. Moreover, these methods (except CREATE) must obey to idempotence rules which guarantee that successive calls on the same URI always produce the same effects, i.e. no-side effect on the server are allowed.
3. Interactions between the client and the server must be **stateless**. Each transaction must remain unrelated to the previous one and no state related to the application is stored on the server. This guarantees server scalability and transaction reliability.
4. **A hypermedia engine**. This is actually the most important principle in [9] but also the less well-understood. It means that representations of resources must contain data and (hyper-) links to other URI and resources. Applications navigate through hypermedia instead of calling functions and the navigation is performed according to link semantic. Actually, running an REST application is navigating through the hypermedia engine and the state of the application is the path it follows through hyperlinks.

These principles were enacted in order to guarantee the scalability of the World Wide Web under ever increasing connections ([9]).
Web applications following REST principles must not be tied to specific URI, except maybe the top-level URI to access the service. From the top-level URI, all other URI must be discovered and accessed only through representations. Thus, it is easy to move RESTful web services from one hosting site to another.
Beside HTTP, another promising RESTful protocol, specifically targeting the Internet of Things, is CoAP (Constraint Application Protocol, see [12]).

As an example of ETSI M2M resource, the **container** resource is used to exchange data between applications and/or SCL in a buffered way, allowing one of the parties to not be online at the same time. The ETSI M2M does not specify its implementation, but one can imagine implementing through Device Triggering mechanisms explained in [1].
Another example of ETSI M2M resource is the PoC in the NSCL, described in section 2.1.4.

It is debatable whether the ETSI M2M functional architecture strictly adheres to the REST principles or not. Here are some examples of difference between strict REST and ETSI M2M:

- For efficiency reasons, ETSI M2M introduces two additional methods beside CRUD:NOTIFY and EXECUTE, although they are implemented on CRUD.
- It is not obvious that RETRIEVE, UPDATE, DELETE in ETSI M2M will obey the idempotence rules.
- The hypermedia aspect seems missing in ETSI M2M in the sense that executing an application is not navigating through hyperlinks.

Nevertheless, this kind of issues is not directly relevant to EXALTED.

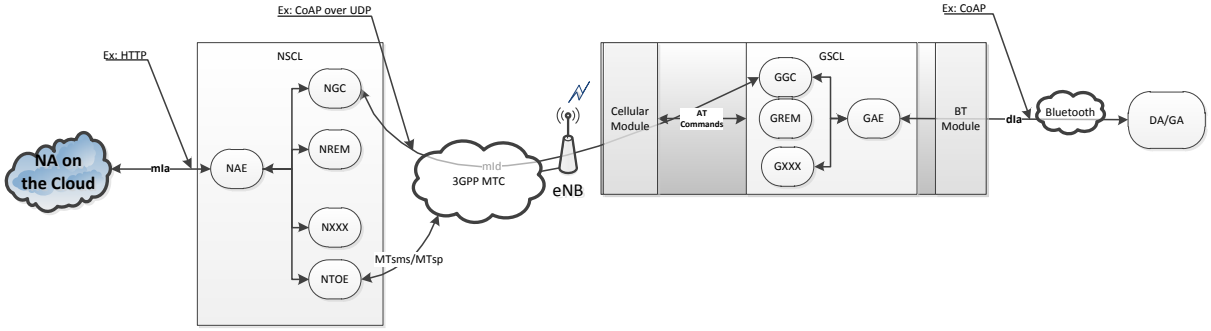

Figure 2-4 Possible Organization of SCL

2.1.6 Possible Organization of xSCL

From the above description of SCL and resources, one can envisage a possible organization of SCL. In this organization, the NAE is nothing more than a Web server offering an HTTP-like interface to NA[2]. Likewise the NGC offers aCoAP-based interface for D/GSCL. NAE and GAE are in charge of routing requested between applications and/or SC.
The NTOE SC is in charge of interworking with the Core Network whenever interworking with Core Network elements is required, e.g. the SMS-SC. In view of section 2.2, the Core Network mentioned in the Figure 2-5 is 3GPP MTC.

2.2 The 3GPP MTC architecture

This section gives a high-level overview of the 3GPP MTC architecture [1]. It considers those architectural enhancements to support a large number of MTC devices in the network and fulfil the MTC service requirements. The MTC Server is an entity which connects to the 3GPP network to communicate with user equipment (UE) used for MTC and nodes in the public land mobile network (PLMN) .

The 3GPP architecture distinguishes two major types of communication models between the MTC device and the MTC server, namely the indirect and the direct model. In the direct model, the MTC Application connects directly to the operator network without the use of any MTC Server, while in the indirect model a MTC server is required, which can be either outside of the operator domain (MTC Service Provider controlled communication), or inside the operator domain (3GPP Operator controlled communication). These two major models can be merged to a hybrid one (Figure 2-5). The MTC Application entities and the reference point API (Application Programming Interface) in the figure are outside of 3GPP scope (see [1]). More specifically:

- The E2E aspects of communication between MTC devices and MTC servers (which can be located outside or inside the network operator's domain) are out of the scope of this study.
- Communication at the application level between the MTC Device and the MTC Application is out of scope of 3GPP standardization.
- The interface between the MTC server and the MTC application is out of the scope of 3GPP. The MTC server communicates with the 3GPP network by means of an interface or set of interfaces.

[2] M2M Application in the Network Domain

- The MTC Application makes use of an MTC Server, again for additional value added services, provided by the 3GPP operator (which becomes a Service Provider). The interface between the MTC Server and the MTC application remains still out of the scope of 3GPP, whilst the communication between the MTC server and the 3GPP network becomes internal to the PLMN.

2.2.1 Network elements

The following 3GPP network elements provide the functionalities to support the Indirect and Hybrid models of MTC. As 3GPP notes, as further development of the MTC architecture takes place, further network elements may be defined in the future.

- MTC-IWF (Inter Networking Functions): The MTC-IWF hides the internal PLMN topology and relays or translates signaling protocols used over MTCsp (see 2.2.2) to invoke specific functionality in the PLMN. Some of the functionalities of the MTC-IWF includes the following [1]:

  - terminates the MTCsp, S6m, T5a, T5b, T4 and Rf/Ga reference points (see 2.2.2).
  - may authenticate the MTC Server before communication establishment with the 3GPP network.
  - may authorize control plane requests from an MTC Server.
  - support the following control plane messaging from an MTC Server.
  - receive device trigger request.
  - support the following control plane messaging to an MTC Server:
  - may report device trigger request acknowledgement.
  - device trigger success/failure delivery report.

- HLR/HSS: HLR and HSS specific functionality to support the Indirect and Hybrid models of MTC. Functionality for triggering includes the following [1]:

  - termination of the S6m reference point where MTC-IWFs connect to the HLR/HSS.
  - stores and provides the mapping/lookup of E.164 MSISDN or external identifier(s) to IMSI, routing information (i.e. serving MME/SGSN/MSC address), configuration information and UE reachability information to the MTC-IWF.

- SGSN/MME: SGSN and MME specific functionality to support the Indirect and Hybrid models of MTC includes the following [1]:

  - SGSN terminates the T5a reference point.
  - MME terminates the T5b reference point.
  - receives device trigger from MTC-IWF and optionally stores it.
  - encapsulates device trigger delivery information in NAS message sent to the UE used for MTC.

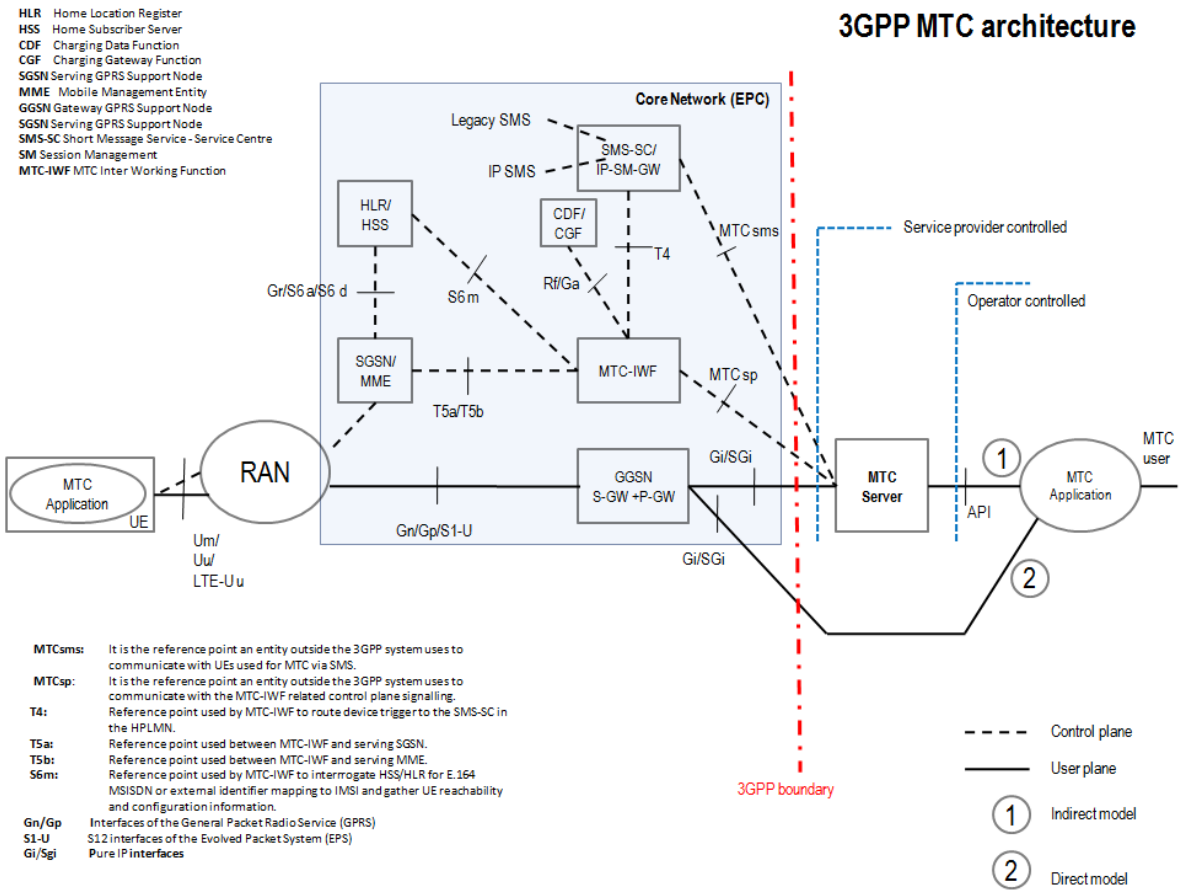

Figure 2-5: High-level view of 3GPP M2M (MTC) architecture [1]

2.2.2 Reference points

The MTC related reference points in the 3GPP architecture are:

MTCsms:	It is the reference point an entity outside the 3GPP system uses to communicate with UEs used for MTC via SMS.
MTCsp:	It is the reference point an entity outside the 3GPP system uses to communicate with the MTC-IWF related control plane signalling.
T4:	Reference point used by MTC-IWF to route device trigger to the SMS-SC in the HPLMN.
T5a:	Reference point used between MTC-IWF and serving SGSN.
T5b:	Reference point used between MTC-IWF and serving MME.
S6m:	Reference point used by MTC-IWF to interrrogate HSS/HLR for E.164 MSISDN or external identifier mapping to IMSI and gather UE reachability and configuration information.

Details for each reference point can be found in [1].

2.3 Beyond the 3GPP and ETSI architectures

Although both ETSI M2M and 3GPP MTC have made significant progress, there are still several gaps with the most important one being the absence of a common approach, since

3GPP MTC mainly focuses on communications, while ETSI M2M focuses on the applications, including service capabilities, security and device management. The two organizations have identified this issue and very recently (June 2012) they initiated a common action, which aims to design the M2M functional architecture that makes use of an IP capable underlying network as the IP network service provided by 3GPP [13]. This action can be considered as an important fact for the EXALTED project, since it is oriented towards the same objective, which is to make 3GPP MTC an enabler for the Service Capabilities required by ETSI M2M-based applications. ETSI Architecture reflects the viewpoint of Service Provider and 3GPP Architecture reflects the viewpoint of Telco.

Moreover, the EXALTED architecture aims to support the enhanced functionalities, protocols and service provisioning developed in WP3–6 coherently through an iterative procedure between those technical WPs and WP2. The EXALTED architecture defines the necessary components, the corresponding functionalities and interfaces, which enhance the M2M communications over the LTE cellular network, through directed innovations, which provide solutions to crucial problems and important advancements with respect to the state of the art. In summary the EXALTED architecture integrates the following key innovations:

- Enhancements in the PHY, MAC and RRC layers, which enable spectrum, energy efficient and cost-effective M2M communications over LTE.
- Those Gateway functionalities for E2E M2M communication between capillary networks and M2M Servers. These functionalities include:
  - Protocol translation.
  - IP/non-IP addressing translation.
  - Data aggregation.
  - Coverage extension.
  - Enhanced MAC for capillary networks (energy and cost efficient).
- Device management functionalities
  - Device MGMT Server.
  - Access to Device MGMT Actions.
  - Lightweight Device MGMT Protocol.
  - Lightweight monitoring.
  - Device MGMT Protocol Translation.
- Low cost security
  - Low overhead Security.
  - Embedded SIM.
  - Sharing Elements.
  - Application Layer Security.

More details about these innovations can be found in subsection 3.1.4, after the presentation of the EXALTED architecture in Section 3.

3 The EXALTED architecture

As discussed in the previous Section, both baseline architectures presented in section 2 are not sufficient to achieve the EXALTED objectives. Therefore, we propose the following specification of the EXALTED architecture. It adopts as much as possible paradigms and terminology of the baseline architectures. The first step towards the EXALTED architecture was the identification of the use cases of interest, taking into account the respective interests of the project's partners and the use cases as seen by ETSI M2M and 3GPP MTC [6], [7]. Based on the analysis of the described use cases, the technical system requirements were identified, in order to ensure an effective E2E system description, able to provide M2M communications over an LTE-based cellular network. These requirements are grouped into the following categories (see Appendix A1 for a brief summary):

- Functional – features of the EXALTED functional elements.
- Service – M2M services offered through LTE-M and the capillary networks
- Network – requirements regarding network infrastructure.
- Non-functional – quality features of the EXALTED system.
- Device – characteristics of end-devices, cluster-heads and gateways.

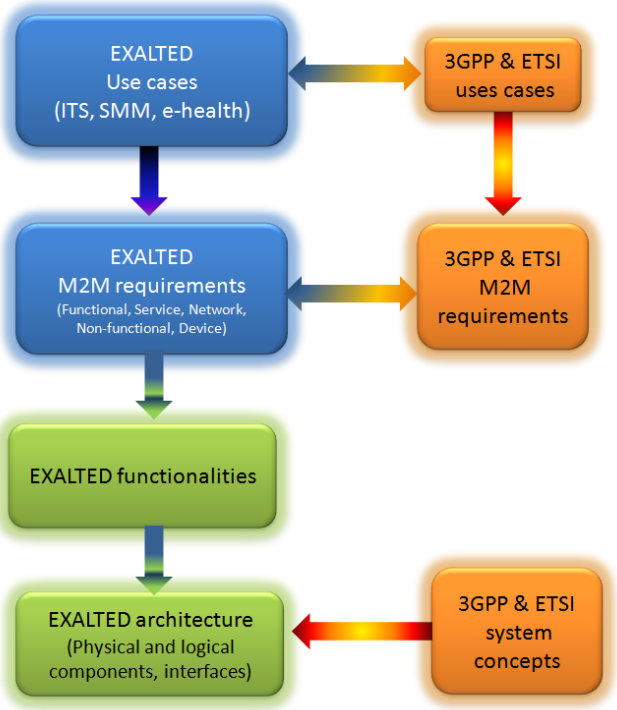

Figure 3-1: Towards the EXALTED architecture

These technical requirements are the basis for identifying the architectural components and the corresponding required functionalities, which ensure that the needed technical requirements are satisfied. For each requirement or a group of requirements specific solutions were developed by the technical work packages (WP3-WP6). An illustration of this logical procedure is shown in Figure 3-1.

3.1 Components of the EXALTED system architecture

In Figure 3-2, the EXALTED architecture is depicted, along with the major innovations compared to the ETSI and 3GPP proposals (green colour), which will be detailed in the following sections. A component is either a physical entity, e.g. an LTE-M device, or a logical element summarizing certain functions that are in reality distributed at different locations, e.g. the Evolved Packet Core (EPC). The Core Network is depicted in more details in Figure 3-2, illustrating the relation with the 3GPP MTC approach and the backward compatibility with LTE. EXALTED has adopted the indirect 3GPP model, which assumes that the MTC Application does not connect directly to the operator network without the use of any MTC Server.

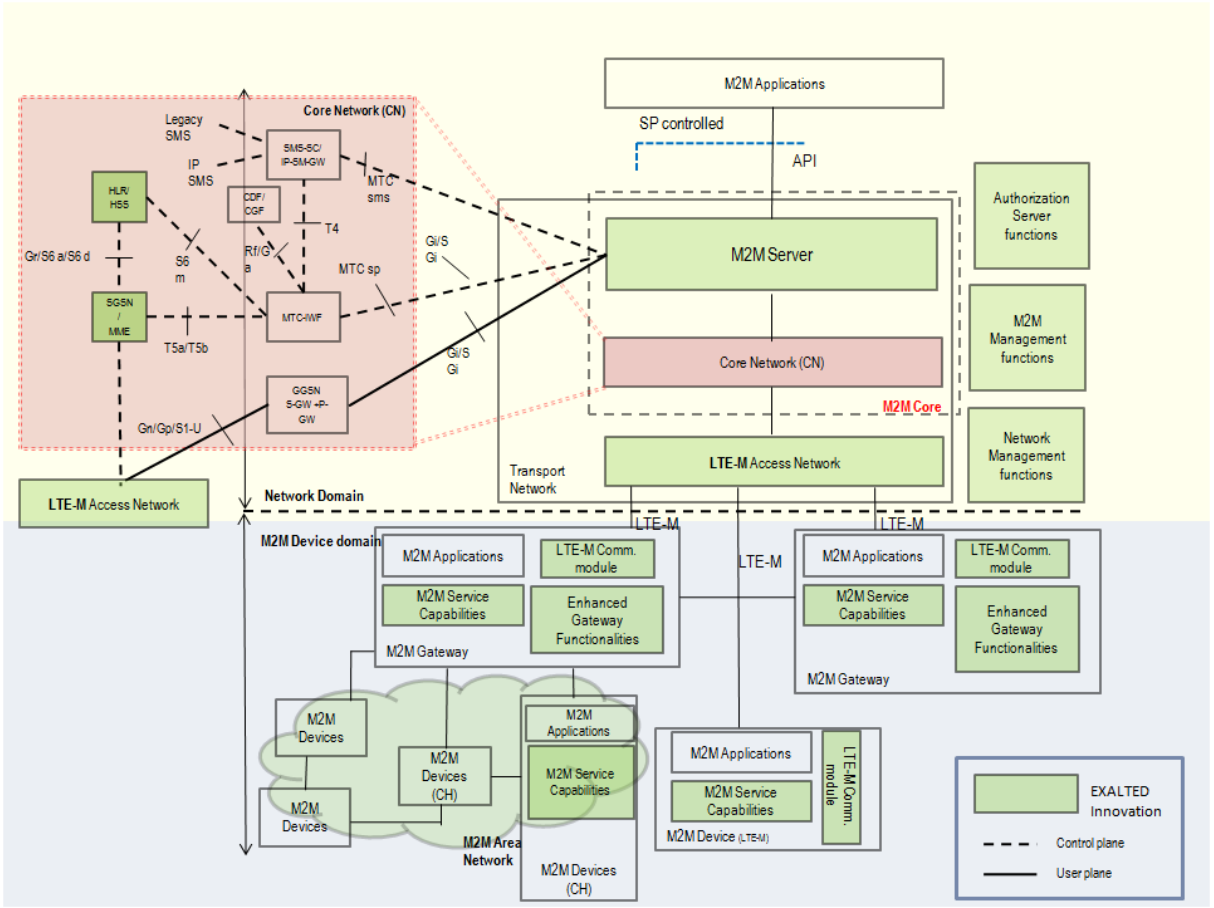

Figure 3-2: Components of the EXALTED architecture

In the following, we classify the EXALTED architecture in two domains, namely, the *Network Domain*, and the *M2M Device and Gateway Domain.*

Network Domain (ND): All components whose functionality is related with the control of applications, security and the management of devices belong to the ND. In EXALTED the wide area Access Network is restricted to the LTE-M/LTE system. Moreover, the EPC responsible for the management of cellular radio network and the eNB in the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) are part of the ND. It is assumed that the application may run on a M2M server accessible from the Internet using the EPC. In the ND reside also the logical components, which are responsible for specific functions, such as the authorization and management of devices and network components.

M2M Device Domain (DD): The DD includes all kind of devices that support one or more applications. The link between DD and ND is the Uu interface defined in 3GPP. However, the used air interface is not LTE, but LTE-M, an autonomous radio access network coexisting with LTE in the same spectrum and specified in [3].

In the following we present the components belonging to the two domains ND and DD and explain those parts of their functionality that will be implemented by EXALTED algorithms. Further it is distinguished between *mandatory* and *optional* functions. The EXALTED architecture shall support the communication between different types of devices and various use cases, and not the complete functionality is required for all of them. Mandatory means that this function must be always implemented, whereas optional means that the function is only required for some of the communication types or use cases. A high-level view of the EXALTED is depicted in Figure 3-3.

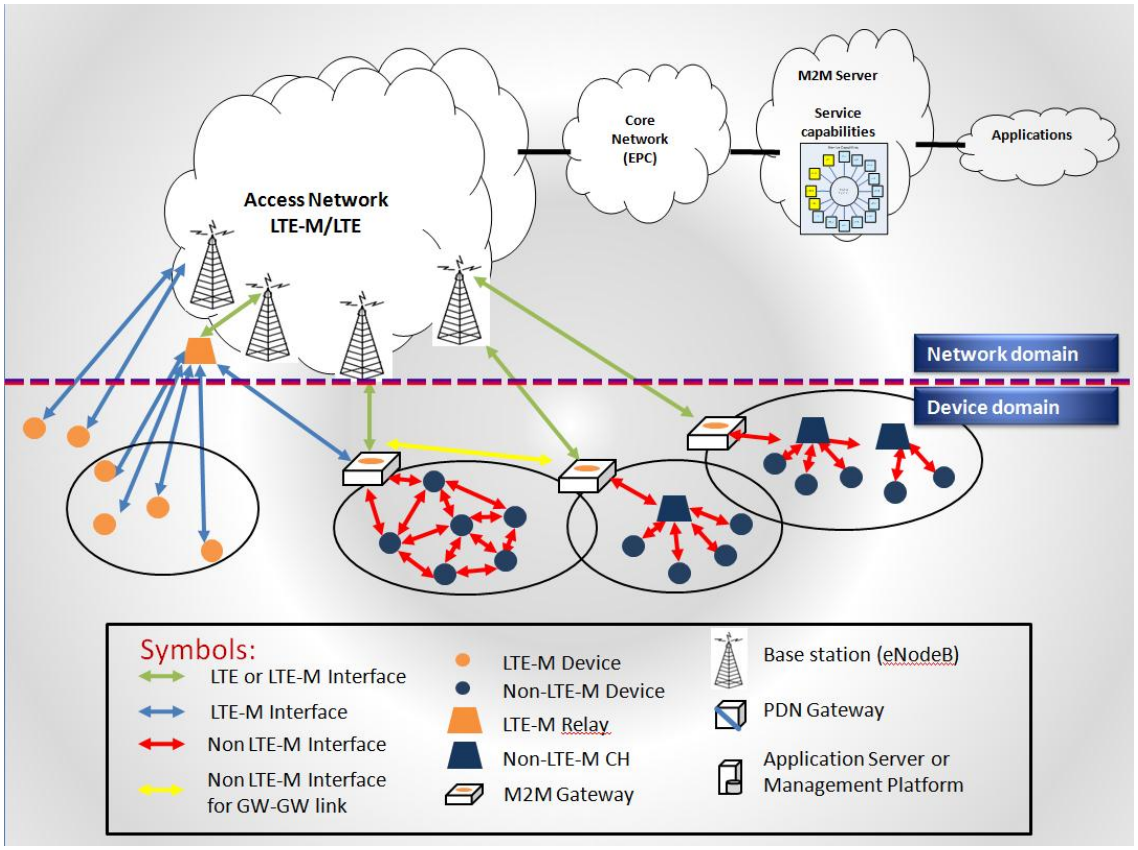

Figure 3-3: Components of the EXALTED architecture

3.1.1 ETSI, 3GPP and EXALTED terminology equivalences

ETSI, 3GPP and EXALTED each follow a slightly different terminology for broadly similar architectural elements. The most important architectural elements from each approach can be found in Table 3-1, with the equivalent EXALTED terminology indicated. It should be noted that the role and functionalities of each element are not necessarily identical across the different architecture, but this table should assist those moving from one architectural description to another.

Table 3-1: Terminology equivalences

3GPP terminology	ETSI terminology	Equivalent EXALTED terminology
MTC Server	M2M Service capabilities (SC)	M2M Server
MTC Application (UE)	M2M Application (Device)	M2M Application (Device)
-	M2M Application (M2M Gateway)	M2M Application (M2M Gateway)
-	-	M2M Application (CH)
MTC User	M2M Device	• LTE-M Device • Non-LTE-M Device
EPC	Core Network (CN)	EPC
RAN	Access Network	LTE-M Access Network
eNB	-	eNB
Relay Node (RN)	-	LTE-M Relay
-	M2M Gateway	M2M Gateway
	M2M Area Network	M2M Capillary Network

3.1.2 Components in the ND

The functionalities of the components in the ND are related with the control of applications, security and the management of devices. Additionally, in the same domain reside those logical components, which are responsible for authorization functions. In the following subsection, the functionalities of the ND components are presented in details.

3.1.2.1 M2M Server

M2M Server is a logical component, i.e. it has not been necessarily implemented on a single equipment. On top of the underlying protocols and technologies, particular M2M Servers communicate with M2M Devices and Gateways that are involved in the same application. Note that the applications may run on any functional element in the DD (i.e. on the M2M Gateway, the M2M Devices, or the CHs). Apart from the application itself, management and control functionality is part of the M2M server, such as Device Management, which uses specifically designed protocol over the same network for communication with Devices and gateways, and servers needed to fulfill the security requirements.

Required Functionalities:

- Execution and control of the application.
- Device management and monitoring.
- Control over all security related aspects.
- Initiation and termination of E2E connectivity[3].

3.1.2.2 Evolved Packet Core (EPC)

The EPC consists of Packet Data Network Gateway (PDN-GW), Serving Gateway (SGW), Mobility Management Entity (MME), Home Subscriber Server (HSS), and Policy Control and Charging Rules Functions (PCRF). EXALTED does not intend to propose any changes in the EPC. Therefore, its functionality is not explained in this report, and it is referred to [14], [15], [16].

[3] The M2M server can initiate a communication link with a device only if it is already registered to the server.

Table 3-2: EPC required functionalities

Required functionalities	Technical requirements	Objective
Host information about devices	- Mobility management (NT.8) - Reduced signaling (NT.17)	Enabler for other solutions
Suspension of T3412 when duty cycle flows through inactivity phase.	- Support of large number of devices (FU.1) - End-to-end session continuity (NT.15) - Reduced signaling (NT.17) - Scalability (NF.1) - Energy efficiency (NF.2) - Congestion control mechanism (NF.5) - Energy efficient duty cycles (DV.3)	Energy efficiency, large number of devices
Accesses information about duty cycling of the LTE-M Device / M2M Gateway		Enabler for the previous solution
Minimization of the number of paging messages sent towards M2M device during the paging procedure	- Mobility management (NT.8) - Reduced signaling (NT.17) - Energy efficiency (NF.2)	Reduction in the network load and signalling in the radio access network

3.1.2.3 LTE-M eNB

LTE-M PHY, MAC and RRC Uplink (UL) and Downlink (DL) algorithms must be implemented at the eNB in order to support respective protocols of the LTE-M Uu interface. The most important functions are: error protection and correction, provision of random access and scheduled access to radio resources in time and/or frequency utilized for the payload and control signalling, transmission of pilot signals for channel estimation, initialization and control of re-transmission processes, connection set-up and finalisation, synchronisation between transmitter and receiver, adaptation of the radio link parameters to the propagation conditions, and support of broadcast und multicast services.

One possible realization option of LTE-M is to provide a radio interface purely consisting of PHY, MAC, and RRC protocols. For this purpose, the IP protocol normally executed between PDN-GW and UE has to be terminated at the eNB, where IP addresses are translated into a local addressing scheme and vice versa.

In the case, where the eNB has a connection to an M2M Gateway, it must be able to aggregate data packets addressed to several Non-LTE-M Devices behind the M2M Gateway into one compound data packet, either the end-devices are IP based or non-IP based.

Table 3-3: eNB required functionalities (Uplink)

Required functionalities	Satisfied technical requirements	Objective
Uplink (from LTE-M Device / M2M Gateway to eNB / Relay)		
Separation of LTE signal and LTE-M signal	- LTE-M backward compatibility (NT.1) - Minimum number of modifications in network infrastructure (NT.3)	LTE/LTE-M coexistence LTE/LTE-M coexistence
GFDM PHY Rx signal processing (inverse to Tx)	- Support of large number of devices (FU.1) - Efficient spectrum management (FU.2) - Support for diverse M2M services (FU.3) - LTE-M backward compatibility (NT.1) - Minimum number of modifications in network infrastructure (NT.3)	
Correlation receiver for CDMA overlay	- Support of large number of devices (FU.1) - Efficient spectrum management (FU.2)	Wide area coverage

Collision recovery Random access retransmission protocol (Rx)	- Support of large number of devices (FU.1) - Efficient spectrum management (FU.2) - High node density (NT.10) - Reduced signaling (NT.17) - Scalability (NF.1)	Energy efficiency, large number of devices
HARQ (Rx)	- Efficient spectrum management (FU.2) - Energy efficiency (NF.2)	Spectrum efficiency
Channel estimation from uplink sounding (TDD)	- Support of large number of devices (FU.1) - Overall QoS (SV.1) - LTE-M backward compatibility (NT.2) - Minimum number of modifications in network infrastructure (NT.3) - Reduced signaling (NT.17) - Energy efficiency (NF.2)	Enabler for other solutions
Antenna selection Energy detection at each antenna element (Signal-plus-Noise)	- LTE-M backward compatibility (NT.2) - Minimum number of modifications in network infrastructure (NT.3) - Energy efficiency (NF.2)	Complexity reduction

Table 3-4: eNB required functionalities (Downlink)

Required functionalities	Technical requirements	Objective
Downlink (from eNB / Relay to LTE-M Device / M2M Gateway)		
Calculate beamforming weights (TDD) Zero forcing beamforming (FDD)	- Support of large number of devices (FU.1) - Overall QoS (SV.1) - LTE-M backward compatibility (NT.2) - Minimum number of modifications in network infrastructure (NT.3) - Reduced signaling (NT.17) - Energy efficiency (NF.2)	Wide area coverage
Scheduling according to delay classes (two options: PS1, PS2)	- Support of large number of devices (FU.1) - Support for diverse M2M services (FU.3) - Overall QoS (SV.1) - LTE-M backward compatibility (NT.2) - Minimum number of modifications in network infrastructure (NT.3) - Real time performance (NF.4)	Large number of devices
Scheduling based on clustering of devices	- Efficient spectrum management (FU.2) - Support for diverse M2M services (FU.3) - Overall QoS (SV.1) - LTE-M backward compatibility (NT.2) - Minimum number of modifications in network infrastructure (NT.3) - Reduced signaling (NT.17) - Real time performance (NF.4)	
Scheduling based on traffic heterogeneity (according to rushing entity classifier)	- Support of large number of devices (FU.1) - Support for diverse M2M services (FU.3) - Overall QoS (SV.1) - LTE-M backward compatibility (NT.2) - Minimum number of modifications in network infrastructure (NT.3) - Real time performance (NF.4)	LTE/LTE-M coexistence
Control of HARQ processes HARQ (Tx)	- Efficient spectrum management (FU.2) - Energy efficiency (NF.2)	Spectrum efficiency
Rateless encoding on BC channel	- Support of large number of devices (FU.1) - Efficient spectrum management (FU.2)	Energy Efficiency,

	- Local and remote device management (FU.5) - High node density (NT.10) - Multicast and broadcast communication (NT.13)	Spectrum efficiency
Packet encoding for broadcast architecture	- Support of large number of devices (FU.1) - Efficient spectrum management (FU.2) - Local and remote device management (FU.5) - Scalability (NF.1) - Reliable delivery of a message (NT.9) - High node density (NT.10) - Multicast and broadcast communication (NT.13) - Efficient provisioning of a set of M2M equipments (SV.3) - Software update over the air (DV.11)	Wide area coverage
Control of energy efficient relaying	- Energy efficiency (NF.2) - Overall QoS (SV.1)	Energy efficiency, wide area coverage
Optimized paging	- Mobility management (NT.8) - Reduced signaling (NT.17) - Energy efficiency (NF.2)	Protocol simplification, turning off devices
Optimized mobility support		
Address mapping function	- Reduced signaling (NT.17)	
Host information about devices	- Mobility management (NT.8) - Reduced signaling (NT.17) - Energy efficiency (NF.2)	Enabler for other solutions

3.1.2.4 LTE-M relay

These elements are similar to 3GPP rel.10 LTE-A Relays. They are used in LTE-M environment for coverage extension and communication with the rest of the network. Both transparent and non-transparent Relays are supported within 3GPP. The required functionalities depend on the relay type (L1, L2, or L3). The LTE-M relays have the very same functionalities as the LTE ones with the additional capability to support the LTE-M interface.

3.1.3 Components in the Device Domain (DD)

In the DD there exist devices that utilize the LTE-M air interface (LTE-M enabled) and devices that do not (non LTE-M enabled). The M2M Gateway has a key role in the EXALTED architecture, because it is the link between the cellular radio network (LTE-M) and connected capillary networks. It enables reliable E2E connectivity between a simple Non-LTE-M Device and the M2M Server, i.e. the application being executed in the internet, which is one of the key objectives in EXALTED.

3.1.3.1 LTE-M device (LTE-M enabled device)

They have LTE-M interface and can access the Network domain, either by directly accessing the LTE-M network, or through an LTE-M Relay. The required functionalities of this component are listed in Table 3-5**:** and

Table **3-6:**.

Table 3-5: LTE-M device required functionalities (Uplink)

Required functionalities	Satisfied technical requirements	Objective
Uplink (from LTE-M Device / M2M Gateway to eNB / Relay)		
GFDM PHY Tx signal processing (up-sampling, pulse shaping, up-conversion)	- Support of large number of devices (FU.1) - Efficient spectrum management (FU.2) - Support for diverse M2M services (FU.3) - LTE-M backward compatibility (NT.1) - Minimum number of modifications in network infrastructure (NT.3)	LTE/LTE-M coexistence
CDMA overlay (multiplication with code sequence)	- Support of large number of devices (FU.1) - Efficient spectrum management (FU.2)	Wide area coverage
Estimation and feedback of CSI, PMI	- LTE-M backward compatibility (NT.2) - Minimum number of modifications in network infrastructure (NT.3) - Energy efficiency (NF.2)	Enabler for other solutions
Perform random access (eventually according to round robin criterion)	- Support of large number of devices (FU.1) - Efficient spectrum management (FU.2) - High node density (NT.10) - Scalability (NF.1) - Reduced signaling (NT.17)	Energy efficiency, large number of devices
Random access retransmission protocol (Tx)		
HARQ (Tx)	- Efficient spectrum management (FU.2) - Energy efficiency (NF.2)	Spectrum efficiency
Spectrum sensing	- Efficient spectrum management (FU.2)	
Energy harvesting	- Energy efficiency (NF.2)	Independence from power supply

Table 3-6: LTE-M device required functionalities (Downlink)

Required functionalities	Technical requirements	Objective
Downlink (from eNB / Relay to LTE-M Device / M2M Gateway)		
HARQ (Tx)	- Efficient spectrum management (FU.2) - Energy efficiency (NF.2)	Spectrum efficiency
Energy detection at each antenna element	- LTE-M backward compatibility (NT.2) - Minimum number of modifications in network infrastructure (NT.3) - Energy efficiency (NF.2)	Complexity reduction
Antenna selection		Wide area coverage
Set-up of semi-static assignment of radio resources	- Support of large number of devices (FU.1) - Reduced signaling (NT.17)	Signaling reduction
Rateless decoding of BC channel	- Support of large number of devices (FU.1) - Efficient spectrum management (FU.2) - Local and remote device management (FU.5) - High node density (NT.10) - Multicast and broadcast communication (NT.13)	Energy Efficiency, Spectrum efficiency
Forwarding or decoding of packets for broadcast architecture	- Support of large number of devices (FU.1) - Efficient spectrum management (FU.2) - Local and remote device management (FU.5)	Wide area coverage

	- Scalability (NF.1) - Reliable delivery of a message (NT.9) - High node density (NT.10) - Multicast and broadcast communication (NT.13) - Efficient provisioning of a set of M2M equipments (SV.3) - Software update over the air (DV.11)	
Address mapping function	- Reduced signaling (NT.17)	Protocol simplification, overhead reduction
Suspension of T3412 when duty cycle flows through inactivity phase.	- Support of large number of devices (FU.1) - End-to-end session continuity (NT.15) - Reduced signaling (NT.17) - Scalability (NF.1) - Energy efficiency (NF.2) - Congestion control mechanism (NF.5)	Energy efficiency, large number of devices

3.1.3.2 M2M Gateway (LTE-M enabled device)

It provides the interconnection between the LTE-X (i.e. LTE/LTE-A/LTE-M) network and the capillary networks (consisting of one or more M2M devices). It can provide various functionalities, such as protocol translation, routing, resource management, device management, data aggregation, etc. In some cases, the Gateway may provide M2M services without requiring accessing the CN. Scenarios, where the access to the CN is not mandatory for providing M2M applications are beyond the scope of EXALTED. EXALTED considers the scenarios where M2M services are provided to the capillary networks, through the LTE-M AN. However, in these scenarios the continuous access to the CN is not mandatory, as long as security or other required operations (e.g. authorization) has been established. It is expected that the M2M Gateway will normally connect to the LTE-X network with a direct radio link. In the case that an M2M Gateway is unable to establish direct connectivity (for example, due to deployment in a remote area without coverage, or due to localised infrastructure failure) connectivity to the LTE-X network may be achieved by hopping via an LTE-M Relay and/or one or more other M2M gateways. The availability of direct M2M Gateway to M2M Gateway links will depend on the capillary radio network interfaces supported within the gateways. Similar to LTE, LTE-M does not support such links. Direct M2M Gateway to M2M Gateway connectivity for the purpose of E2E device to device connection without any LTE-X involvement (e.g. local breakout) is not the primary focus of EXALTED.

The functionalities of the M2M Gateway are the same as those of the LTE-M devices plus some additional ones as listed in Table 3-7.

Table 3-7: M2M Gateway additional required functionalities

Required functionalities	Satisfied technical requirements	Objectives
Address Translation Mechanism for capillary networks	- Network initiated packet-data communication (FU.4) - Heterogeneous networks (NT.1) - End to end device to device communication (NT.6) - Protocol translation at the Gateway (DV.7) - Information routing at the Gateway (DV.8)	Connection/transmission integrity across aggregation points through IP based E2E networking system

Dynamic Aggregator selection	- Traffic aggregation (NT.11) - Energy efficiency (NF.2)	Traffic aggregation
Dynamic Cluster-Head selection- DISC	- Heterogeneous networks (NT.1) - Support of multi-hop communication (NT.4) - Flexible addressing scheme (NT.7) - High node density (NT.10) - Traffic aggregation (NT.11) - Self-diagnostic and self-healing operation (NT.12) - Reduced signaling (NT.17) - Scalability (NF.1) - Energy efficiency (NF.2) - Support of large number of devices (FU.1) - Support for diverse M2M services (FU.3) - Network initiated packet-data communication (FU.4) - Local and remote device management (FU.5) - Unique identity for devices (FU.6) - Efficient provisioning of a set of M2M equipments (SV.3) - Delegation and distribution of functionality (SV.5)	Connection/transmission integrity across aggregation points through Traffic aggregation
Data Compression Strategy	- Support of large number of devices (FU.1) - Location information (DV.4) - Protocol translation at the Gateway (DV.7) - End-to-end QoS system (NT.14) - End-to-end session continuity (NT.15)	Efficient and consistent IPv6 Packet mapping
Payload Reduction	- Energy efficiency (NF.2) - Reliable delivery of a message (NT.9) - Multicast and broadcast communication (NT.13)	Compatibility with existing hardware Energy efficiency Efficient and consistent IPv6 Packet mapping
Device Management Protocol Translation	- Local and remote device management (FU.5) - Unique identity for devices (FU.6) - End to end device to device communication (NT.6) - Multicast and broadcast communication (NT.13) - Protocol translation at the Gateway (DV.7) - Remote configuration (DV.10) - Software update over the air (DV.11)	Device management architecture. Addressability and security Traffic aggregation
Self Diagnostic	- Support of large number of devices (FU.1) - High node density (NT.10) - Self-diagnostic and self-healing operation (NT.12) - Multicast and broadcast communication (NT.13) - End-to-end QoS system (NT.14) - Reduced signaling (NT.17) - Scalability (NF.1)	Device / node monitoring mechanism Reliable devices
Addressing and Routing Mechanism (ARM)	- Support of large number of devices (FU.1) - Local and remote device management (FU.5) - Unique identity for devices (FU.6) - Heterogeneous networks (NT.1) - Support of multi-hop communication (NT.4) - End to end device to device communication (NT.6) - Mobility management (NT.8) - Self-diagnostic and self-healing operation (NT.12) - End-to-end session continuity (NT.15) - Information routing at the Gateway (DV.8)	Device management architecture. Addressability and security IP based E2E networking system
MIMO Capabilities	- Support of large number of devices (FU.1) - Traffic aggregation (NT.11) - Reduced signaling (NT.17)	Energy efficiency Connection/transmission integrity across

		aggregation points through
Device selection		Minimization of complexity and feedback signalling
Channel estimation		
Feedback Capabilities		
Scheduling capabilities	- Support of large number of devices (FU.1) - Overall QoS (SV.1) - Support of multi-hop communication (NT.4) - Traffic aggregation (NT.11)	Optimization of resource utilization Energy efficiency
Beacon transmission capabilities		
Mediated Gossiping Mechanism	- Support of large number of devices (FU.1) - Local and remote device management (FU.5) - Traffic aggregation (NT.11) - Multicast and broadcast communication (NT.13) - Extensibility and adaptability (NF.3) - Information routing at the Gateway (DV.8)	Traffic aggregation
Single Hop Communication, Payload Reduction	- Energy efficiency (NF.2) - Reliable delivery of a message (NT.9) - Multicast and broadcast communication (NT.13)	Compatibility with existing hardware Energy efficiency Efficient and consistent IPv6 Packet mapping
Single Hop Communication, Decentralized Source Coding	- Support of large number of devices (FU.1) - Location information (DV.4) - Protocol translation at the Gateway (DV.7) - End-to-end QoS system (NT.14) - End-to-end session continuity (NT.15)	Efficient and consistent IPv6 Packet mapping

3.1.3.3 Non-LTE-M enabled device (non LTE-M enabled device)

These devices do not have an LTE-M interface, but form capillary network(s) using other network access technologies, such as Zigbee, and IEEE 802.11x. They can access the Network domain through a M2M Gateway, and run M2M applications locally (Table 3-8).

Table 3-8: Non LTE-M device required functionalities

Required functionalities	Technical requirements	Objective
Dynamic Cluster-Head selection-DISC	Same as in Table 3-7.	Connection/transmission integrity across aggregation points through Traffic aggregation
Decentralized Source Coding (DSC) techniques	- Support of large number of devices (FU.1) - Location information (DV.4) - Protocol translation at the Gateway (DV.7) - Reliable delivery of a message (NT.9) - High node density (NT.10)	Efficient and consistent IPv6 Packet mapping
Payload Reduction	Same as in Table 3-7.	Compatibility with existing hardware Energy efficiency Efficient and consistent IPv6 Packet mapping

Self Diagnostic	Same as in Table 3-7.	Device / node monitoring mechanism Reliable devices
StateLess Address Auto Configuration	Same as in Table 3-7 (ARM)	Device management architecture. Addressability and security IP based E2E networking system
Memory capabilities	- Support of large number of devices (FU.1) - Overall QoS (SV.1) - Support of multi-hop communication (NT.4) - Traffic aggregation (NT.11)	Optimization of resource utilization Energy efficiency Traffic aggregation

3.1.3.4 Non-LTE-M Cluster Heads (CHs) (non LTE-M enabled device)

They can be considered as M2M devices with some additional capabilities (Table 3-9). Like regular M2M Devices, they are also part of capillary networks and the communication from a regular M2M Device may be directed through and managed by a CH. The functionalities of a CH may include data aggregation, device management, routing, etc. Unlike an M2M Gateway, a CH will not perform protocol translation. Most of the functionalities of CHs are protocol specific, and depend on the particular protocol running in the capillary network.

Table 3-9: Non LTE-M CH additional required functionalities

Required functionalities	Technical requirements	Objective
Dynamic Aggregator selection	See Table 3-7.	Traffic aggregation
Dynamic Cluster-Head selection- DISC		Connection/transmission integrity across aggregation points through Traffic aggregation
Self Diagnostic		Device / node monitoring mechanism Reliable devices
Channel state information		Minimization of complexity and feedback signalling
Feedback		
Mediated Gossiping Mechanism		Traffic aggregation

3.1.4 Summary of the EXALTED features

The required functionalities at each EXALTED component are related with the corresponding solution or group of solutions, which are detailed in the project's technical WPs (WP3-WP6). Figure 3-4 illustrates the main innovations developed within the EXALTED system, compared to the ETSI and 3GPP proposals. These innovations are the following:

3.1.4.1 The LTE-M access network

The cellular network is a major part of the EXALTED architecture. A detailed discussion why the existing specification of LTE cannot meet the stringent technical requirements with respect to an efficient support of a multitude of short messages within the architecture is presented in [17] In the following the most important arguments are briefly summarized.

Small data transmission in M2M: The majority of M2M applications transmit and receive only very small amounts of data. The aim is to transmit these short messages with very efficient resource usage, in particular with respect to the control channels. The current LTE specification was mainly designed for broadband applications with reasonable control information overhead to achieve the required high peak data rates and high mobility support. The ratio between payload size and control information becomes inacceptable, if the same specification is applied to short messages. This is further emphasized by the fact that we expect a significantly higher number of machine devices in one cell compared to legacy LTE UEs. Hence, in LTE-M we envisage a reduction of signalling overhead.

Radio access: When in active mode, LTE devices use scheduled radio resources to transmit data. These resources are used in time and frequency and are utilized exclusively by a device to which they were allocated, hence, collisions cannot happen. The drawback is that scheduling information has to be distributed among all active devices in a cell, and that these devices have to listen to the control channel and to decode the information in order to know which resources they may utilize. This basic LTE system design paradigm is well-thought-out as long as the amount of data to be transmitted is big and the number of devices small. But in EXALTED the opposite situation is assumed: A big number of devices sending only small messages. One basic means is be the application of random access. But this alternative has a disadvantage as well: Without assignment of dedicated radio resources, collisions can occur and messages can be lost. The challenge is to find a trade-off.

Device cost issues: Wide area M2M networks currently utilize the Global System for Mobile Communications (GSM) because their coverage is almost ubiquitous and the cost is sufficiently low. However, operators wish to reduce the number of supported radio access technologies in order to simplify maintenance of deployed hardware. Moreover, it is desirable to reuse GSM spectrum for LTE because this technology is verifiably much more spectrum efficient. One crucial challenge for this migration is the manufacturing cost of the device. The cost of a LTE device is much higher than for a GSM device. One focus is therefore the provision of means to reduce the cost of a LTE-M device to the level of GSM. Possible solutions are: Reduction of bandwidth, reduction of data rates, reduction of transmit power, half-duplex operation, and the usage of only one single RF chain in the machine device.

Network overload issues: One of the key working assumptions in EXALTED is the support of a big number of M2M devices in one cell. Even if these devices are in idle mode most of the time, an external event could wake them up and let them connect or attach. The current LTE system is not prepared for such an overload situation, in particular the Mobility Management Entity (MME) and the Packet Data Network Gateway (PGN) may be vulnerable. Protection algorithms are being specified in LTE-M that firstly prevent the network from a collapse, and secondly guarantee the QoS of the M2M application that has caused the massive device triggering.

Low mobility support: LTE air interface is not optimized for low resource utilization for short transactions, and for low device power consumption, since M2M devices in LTE are treated in the same manner as other mobile subscribers (human), although their way of working and communication patterns are quite different. In LTE various radio measurements are performed to ensure best connection quality as the terminal is moving around. These procedures are relatively complex, use huge amount of radio resources and have significant impact on energy consumption. Actually, these procedures are necessary in the case of

standard mobile terminals (phones), while for the case for many M2M terminals this is just an unnecessary overhead, since large number of M2M devices will be at fixed locations and will throughout their lifetime use one or two radio cells and consequently will not require nor use fast handovers.

Paging of M2M devices: In LTE, when M2M device is in the idle mode, monitoring paging channel takes up substantial amount of time and consumes significant amount of energy. For mobile phones this is necessary to ensure quick response in case of incoming calls, while for M2M devices it is an overhead as the majority of traffic is terminal initiated or at least it is possible to tolerate delay in answering the incoming calls. To cope with this issue, for M2M devices should be possible to avoid monitoring paging and/or to increase the paging cycle (Discontinuous Reception (DRX) cycle), which is explored in EXALTED.

Device duty cycling: In some important scenarios, such as smart metering or monitoring, M2M devices need not be powered continuously. Hence, to save energy, a duty cycling mechanism for M2M devices based on T3412 timer suspension (both at the device and at the MME) to sustain the EPS bearer over the inactive phase is added to the existing LTE standards.

Addressing schemes of M2M devices: IP headers, even if header compression techniques such as Robust Header Compression (ROHC) are used, present significant overhead for M2M applications with small payload. A mechanism is required to reduce overhead of the application layer addressing for M2M devices in an LTE-M system.

In the following, the key features of LTE-M are briefly summarized and it is clarified how they fulfill the initial design objectives. Details and a first performance assessment can be found in the EXALTED project report D3.3 [3].

The approach of EXALTED is to define a communication system for M2M that coexists with LTE in the same frequency band and that can reuse existing hardware and network infrastructure as much as possible. To achieve this objective, an LTE-M downlink super frame structure based on the Multimedia Broadcast / Multicast Service (MBMS) over Single Frequency Network (MBSFN) repeat pattern was proposed, which occupies single subframes solely for LTE-M. Within these resources several Physical Channels are defined for different purposes like the transmission of data to one particular device, exchange of control information and distribution of broadcast messages. In the uplink a joint LTE/LTE-M shared channel is proposed, and it is up to the scheduler in the eNodeB how to allocate these resources advantageously. One particular solution that aims at the coexistence of both systems is the usage of Generalized Frequency Division Multiplexing (GFDM) in the uplink instead of Single Carrier Frequency Division Multiple Access (SC-FDMA). GFDM benefits from the fact that it can flexibly occupy very small spectrum junks without affecting the surrounding LTE users.

A lot of EXALTED solutions benefit from the basic idea to register information about the LTE-M devices and M2M gateways and their respective capabilities at the Home Subscriber Station (HSS). Examples are the differentiation whether or not a device supports IP, whether a device is mobile or installed at a fixed location, which type of traffic it causes and to which delay class it belongs. Such information is primarily exploited to simplify the Radio Resource Control (RRC) protocols. Obvious examples are paging and mobility management. Moreover the Medium Access Control (MAC) scheduling of the devices can be optimized based on their priority, and three different proposals are being investigated in EXALTED showing significant gains with respect to the overall Quality of Service (QoS), in particular if the number of devices is big.

Signaling reduction is a promising means to save energy, but also to increase the number of short messages that can be handled simultaneously. The main approach for the uplink is the definition of a suitable combination of random access and scheduled access. The Physical MTC Random Access CHannel (PMRACH) allows the transmission of both control information and payload. It is proposed to apply mechanisms to force the arrival distribution of PMRACH usages being flat over time in order to minimize the probability of collisions. Moreover, a scheme for collision recovery is investigated that enables the eNodeB to partially recover packets involved in collisions. Hence, the energy consumption for retransmissions in the device is reduced and the overall spectral efficiency is improved. All these ideas can be complemented by spectrum sensing before the transmission of a message on the PMRACH. However random access solely is not sufficient. Therefore it is proposed to optimize scheduled access on the Physical MTC Uplink Shared CHannel (PMUSCH) by utilizing semi-static resource allocations for devices that transmit messages of the same size in a regular time grid. The amount of control information to be exchanged between device and eNodeB is considerably reduced. Signalling reduction and protocol simplification are means to achieve energy efficiency provided by the specification of LTE-M. This can be complemented by generic concepts like energy harvesting, which can be applied in power limited devices in order to extend their battery lifetime.

Another key objective is the provision of sufficient LTE-M coverage. In particular for power limited isolated devices, maybe installed in the basement of buildings or at other shadowed locations, this is a critical issue. Several concepts address this challenge. Firstly, a Code Division Multiple Access (CDMA) overlay is proposed, and it is shown that the Signal-to-Noise power Ratio (SNR) at the receiver can be increased. Also multiple antenna schemes aim at an improvement of the link robustness, either through beamforming techniques or through a Multiple Input Multiple Output (MIMO) scheme that is characterized by a considerable complexity reduction at the device. Further, an energy efficient relaying concept and a collaborative broadcast architecture based on network coding are analyzed and their special benefits for M2M communications are demonstrated.

Low Density Parity Check (LDCP)-like rateless coding for multicasting and optimized retransmission schemes are proposals that primarily aim at spectrum efficiency, with the additional assumption that a big number of LTE-M devices are connected. In both schemes the basic idea is to transmit an optimal amount of redundancy, which is barely sufficient for a successful reception of the information. In LTE this flexibility is missing.

Cost efficiency is inherently included in almost all of the proposals mentioned above. Furthermore, the conceptual LTE-M framework considers mechanisms that support cost efficiency, e.g. the reduced transmission bandwidth compared to LTE. Another solution is the definition of a device class with reduced performance requirements. This supports the design of devices with only one Radio Frequency (RF) chain, which is of course cheaper than a device that must be equipped with two or more RF chains to fulfill the requirements. Half-duplex operation is a further approach to reduce the cost, and this mode is foreseen in the specification of LTE-M.

As a summary, it is claimed that all LTE-M design objectives are sufficiently addressed, and a first performance assessment [3] clearly suggests that EXALTED makes good progress towards the achievement of these objectives.

3.1.4.2 EXALTED capillary networks and E2E aspects

Besides the LTE-M access network, EXALTED introduces several innovation for providing M2M services to devices with no direct access to LTE-M. For these type of scenarios, the

M2M Gateway plays a catalytic role. In the following, a summary of these innovations is presented.

3.1.4.2.1 Innovative functionalities enabled by the Gateway

The Gateway enables the integration of heterogeneous end devices into capillary networks and the connection of these capillary networks to the LTE cellular networks. This allows M2M servers to have a global reach and coverage of end devices and to provide services beyond those which could be provided within a M2M LAN. The integration of heterogeneous end devices allows optimal support of a wide range of scenarios, where very specific requirements on device characteristics such as size, cost, physical resilience and battery life could not be met by a single type of device or wireless standard.

The key functionalities which support the integration actions of the Gateway are protocol translation and address translation [19]. By protocol translation we refer to the support of multiple radio access technologies (RATs) at the Gateway In particular, the LTE networks use IP addressing to identify end devices but some capillary network access systems do not use IP addressing. Address translation allows non-IP end devices to be visible to and addressable by the LTE network and the M2M servers.

Other benefits enabled by the Gateway include improved energy efficiency, increased numbers of devices supported within the system, and improved spectral efficiency. Data aggregation and compression within the Gateway enables data to or from a large number of devices to be consolidated into a reduced size transmission between the Gateway and the LTE network [21]. This effectively increases the number of devices which can be served by the LTE network and increases the spectral efficiency of the backhaul link. Aggregation and compression can apply not only to "user" data, but also to control signalling and feedback, and device management messages [18], [20]. Since IP addressing has significant overheads, particularly for the small data packets typically encountered in M2M applications, the ability to translate between IP and non-IP addressing brings benefits in terms of both energy efficiency and spectrum efficiency for the capillary network and end-devices [19]. Mobility estimation at the Gateway improves radio resource management and hence spectral efficiency and capacity by predicting and more efficiently tracking the mobility of end-devices [18].

3.1.4.2.2 Innovative functionalities enabled within the capillary network

Innovative functionalities within the capillary network allow for increased radio coverage extension and energy efficiency. Distributed data aggregation, compression and coding techniques allow end-devices to reduce the amount of data they need to send, or even to not send data at all, whilst still providing the M2M server with all the required information from the network of devices as a whole. This can bring significant energy efficiency and battery life benefits for the end devices [21].

New MAC design and clustering techniques allow devices to group together and relay data transmissions to the Gateway [18], [20]. By forming clusters, the energy required in the network for longer range transmissions can be reduced, and techniques to adapt the assignation of the cluster head roles within the capillary network allow the energy drain to be managed across end-devices to provide the optimal network lifetime, and also the increase the coverage area of the network. This approach also reduces the occurrence of data bottlenecks at the Gateway, which can increase the capacity of the network and the number of devices which can be supported.

Provision for capillary network to capillary network to infrastructure allows for support of important scenarios where a capillary network cannot directly connect to the LTE network, for example in the case of different capability vehicular networks, remote locations and situations where the infrastructure is incapacitated. Key functionalities here relate to IP addressing, address translation and routing, which solve the issues of addressing M2M Devices deployed in capillary networks, the Cluster Head M2M Devices and the M2M Gateways [19].

3.1.4.2.3 Device management functionalities

The following device management functionalities are introduced by EXALTED:

- Lightweight Device Management Protocols [20]: OMA-DM v1.x compliant Lightweight Device Management solution supports usual device management functions such as Provisioning, Device configuration, Firmware/Software update, Diagnostic and Monitoring. This lightweight solution aims to reduce the payload footprint by 85% and to lower the encoding complexity while maintaining backward compatibility with the widely deployed OMA-DM v1.x specifications on over 1.4 billion of mobile devices. This approach enables operators to reuse existing OMA-DM v1.x servers to manage constrained M2M devices. Existing OMA-DM Management Objects can also be reused. This solution contributes to enhance the Scalability, Energy efficiency and to further reduce the cost of devices.

  Device Management over CoAP: Simple device management operation like change of configuration of a device, remote control of device (e.g. turn light ON/OFF), reporting a monitoring event or value (e.g. battery level) can usually be accomplished by sending a pair of key-value, where the key can be represented by a resource, and the value reflects the actual command (e.g. 1 for ON and 0 for OFF). In addition, any other device management procedure that includes more complex scenarios (i.e. update of device software/hardware) can be also employed by using CoAP protocol, to manage a device as well as a group of devices. The CoAP protocol can be utilized for these operations due available multicast requests, header option fields and the simple congestion control mechanism that are applicable for the remote monitoring and the diagnostic of the devices. In order to employ CoAP for device management, protocol features are mapped with required device management procedures and DM module based on REST is defined.

- Lightweight monitoring: There are two basic needs derived from EXALTED's goals in conflict when talking about monitoring. On one hand, device management and monitoring of M2M devices require complex algorithms and high payloads, so as to assure proper behaviour. This situation is due to the fact that actual monitoring systems are conceived for conventional and non power constrained equipment. On the other hand, EXALTED must deal with devices with lower power and fewer resources that the ones present on conventional monitored devices. Thus, there is the need of evaluating a trade-off between these two aspects. This way, the proposed approach is to select simpler file transmission mechanisms, and Gateway delegated IP communications in case the node is not IP enable.

- Low cost devices are mostly small and constrained. They have very limited resources such as CPU, memory, battery. Low cost devices are not able to support the following required services, as various protocols must be embedded in devices e.g. device

management protocol, File Transfer Protocol (FTP), MQTT for messaging, self-diagnostic communication protocol, etc
- Mobility management of capillary devices
- Multicasting and broadcasting message to capillary devices
- Data collect and uploading sensor data to M2M server
- Device control, triggering actuators
- Device Self-diagnostic and self-healing
- Device to device messaging

The proposed service extension approach only relies on the lightweight device management protocol to support the above services on low cost devices [20]. This resource saving solution also reduces the complexity, thus the cost of the device; aspects such as communication concurrency, multiple protocol-related security credentials are no longer needed.

- Management of capillary devices deployed behind M2M Gateway, which includes:
  - Self-organized capillary devices and network clustering
  - Mobility management of capillary devices
  - Multicasting and broadcasting message to a group of capillary devices

  Clusters in capillary network are formed dynamically. This self-organizing capability aims to optimize energy consumption. As the battery level of a cluster head is getting low, the cluster can be reformed by electing another cluster head [20].
  Mobility management of capillary devices is handled at the application level over the device management protocol [20]. Upon attachment of a device to the M2M Gateway, this latter update the local device inventory which serves to manage groups and provides routing information. If required, the Gateway can automatically register the new device member to M2M server, so that network initiated command can be issued towards to this device through the gateway. Server initiated command helps the device to further save energy as the polling frequency can be lowered thus lengthen device's idle cycle. The inventory and registration process are also applied whenever a device is detached.
  Multicast and broadcast offload the traffic on the LTE-M link; the spectrum efficient is therefore enhanced. As such, M2M Server can target a group of devices by sending one message to the M2M Gateway, over the proposed lightweight device management protocol. This latter fans the command out to devices belonging to the targeted group [20].
- Device-to-Device messaging can be leveraged to distribute the application logic at the device and gateway level [20]. For instance, sensors data can be posted to a gateway over the lightweight device management protocol, upon data analysis by the distributed application logic, the gateway may trigger application specific actions to actuators. Given the anticipated massive number of devices not being attended by human, the automation of application logic with a distributed approach contributes to enhance the scalability of EXALTED.

3.1.4.2.4 Low cost security

- Low overhead Security: The security protocol used to protect data shall not compromise the energy efficiency of the device and must induce the minimal extra electrical consumption. The size of the payload will inflate due the security requirement but this increase must be restricted to a minimum because not only it means bigger buffers to process the messages but also more electrical energy required.
- Embedded SIM: A hardware component must bring to devices both the intrinsic security features of the SIM and the flexibility of an SPI bus. The operating system of the SIM has been improved over the years and enables a high security for a minimal economical cost and a minimal energy consumption. Involved entity is the device.

- Sharing Secure Elements
- Application Layer Security: considering how critical are the data exchanged between devices and M2M server a flexible security layer must enable applications to protect their data according to the security requirements. This feature is optional. Applications may decide to protect against unsolicited data modifications thanks to the integrity mechanism provided by the security layer or to use ciphering to protect the confidentiality of the data. Entities involved by the security layer are the device and the M2M server.

3.1.4.2.5 Device self-diagnostic

Device self-diagnostic [5] is a mechanism that aims at addressing device reliability as well as the continuity of the service provided by the device. It is also a flexible and updatable service that runs locally in the device or the gateway and applies programmable logic to a device context in order to produce a status of the device and, if necessary, triggers a reaction to this status (issuing notifications, initiating self-healing procedure, etc.). The self-diagnostic service in the device can also serve as a basic pattern to build a virtual observation network of devices with a tree network topology. The result is an efficient mechanism to produce network diagnostic offloading radio resource usage to the capillary network, thus preserving the radio resources of the main LTE/LTE-M link since only the initial network status request and the answer are transmitted. Yet, every device is addressed in a process that is also very scalable as the number of addressed devices does not impact the main LTE/LTE-M radio link.

The self-diagnostic mechanism in EXALTED and its extension to network diagnostic exhibit the following key features:

- An architecture design that matches very well the capillary network architecture that EXALTED considers in the Device Domain.
- A hierarchical approach for the description of arrangement of peripherals, components and functionalities in the devices and the gateways.
- A participation to better global energy efficiency and better spectral efficiency thanks to the hierarchical approach to the virtual observation network. Each node behaves like an aggregator (typically a cluster head) for the diagnostics resulting from subnodes, minimizing both transaction messaging and its associated signalization over LTE-M.
- A scalable approach resulting from the hierarchical architecture of the virtual observation network: addition of new devices to the device network does not hamper LTE-M connectivity. Transaction messaging remains the same regardless of the number of devices in the observation network.
- Flexibility in the architecture of the virtual observation network: dynamic reconfiguration is possible in order to bypass a failing aggregation node or to adapt changing environment, elements of cognitive networks can be applied to drive this dynamic reconfiguration.
- A standard, flexible and scalable interface to the diagnostic of a component.
- A logical integration to device management enabled by the common use of Management Objects.
- The virtual observation network enables integration to the EXALTED network monitoring mechanism.

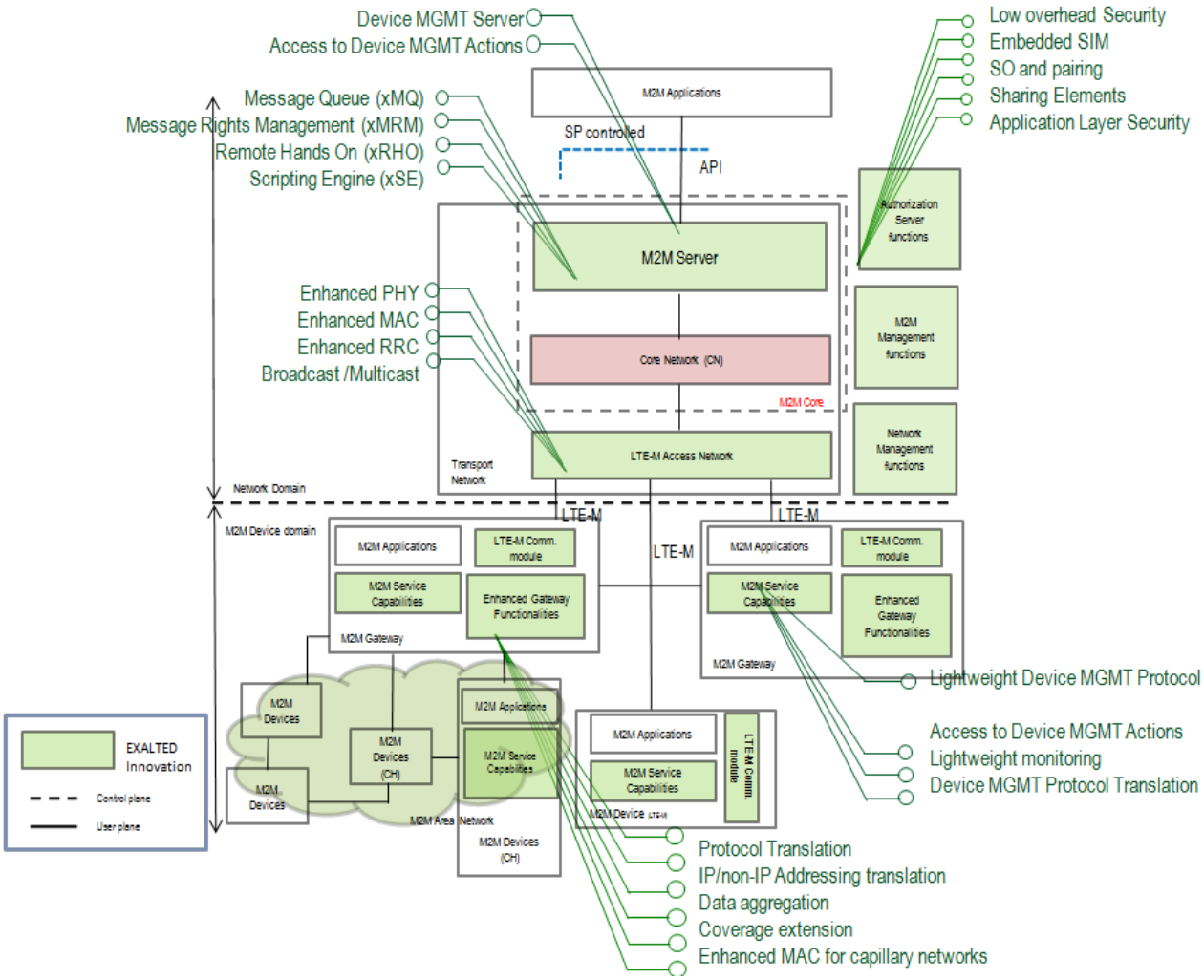

Figure 3-4: Summary of the EXALTED key functionalities

3.2 Interfaces in the EXALTED architecture

In this section the interfaces between the physical and logical components in the EXALTED architecture are identified. Each component is capable of specific functionalities, as discussed in the previous subsection (Section 3.1). The different *interfaces* between these components are identified in this Section. An interface can embrace several layers, e.g. peer-to-peer (lower layers) or end-to-end (higher layers). The functionality of a component can be realized by *algorithms*, and interfaces can be implemented with *protocols* (Figure 3-5).

Generally, we distinguish between higher layer (L4-L7)[4] interfaces providing E2E connectivity, and lower layer interfaces. The latter can be separated further in interfaces including L3 IP connectivity and Peer-to-Peer (P2P) L1-L3 interfaces without IP, which include PHY, MAC, RLC, PDCP and RRC. This principle is shown in Figure 3-6.

[4] Refers to an IP E2E connection.

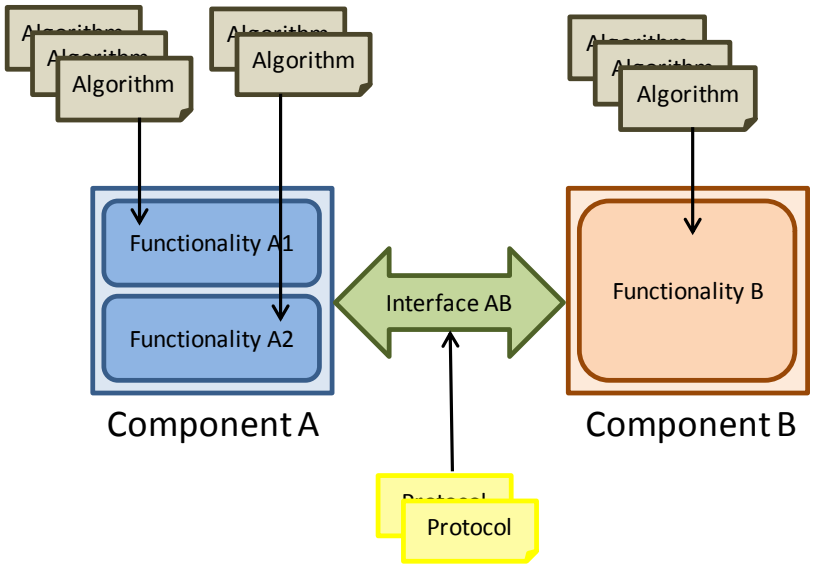

Figure 3-5: Definition of the terminology used in the EXALTED system

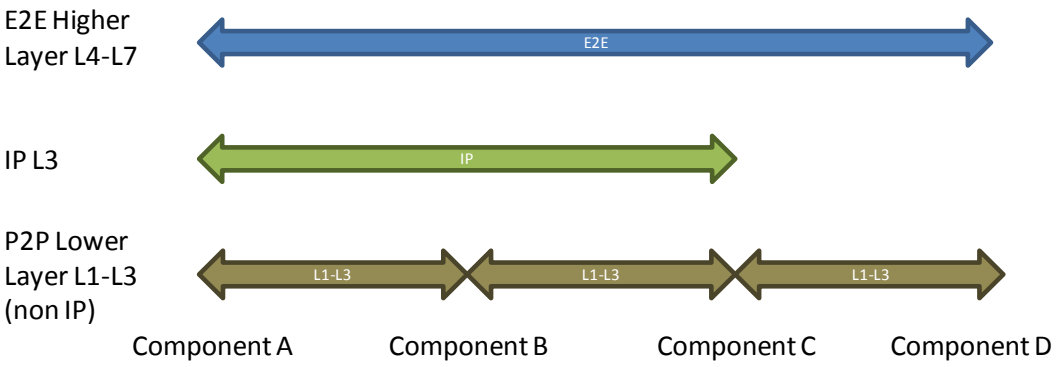

Figure 3-6: Classification of interfaces

In this example we have

- One E2E interface between components A and D
- One IP interface between components A and C
- Three P2P interfaces, namely between components A and B, components B and C, and components C and D.

Component D does not support IP, i.e. one of the mandatory functions of component C must be the translation of the IP address to a local addressing scheme used between C and D.

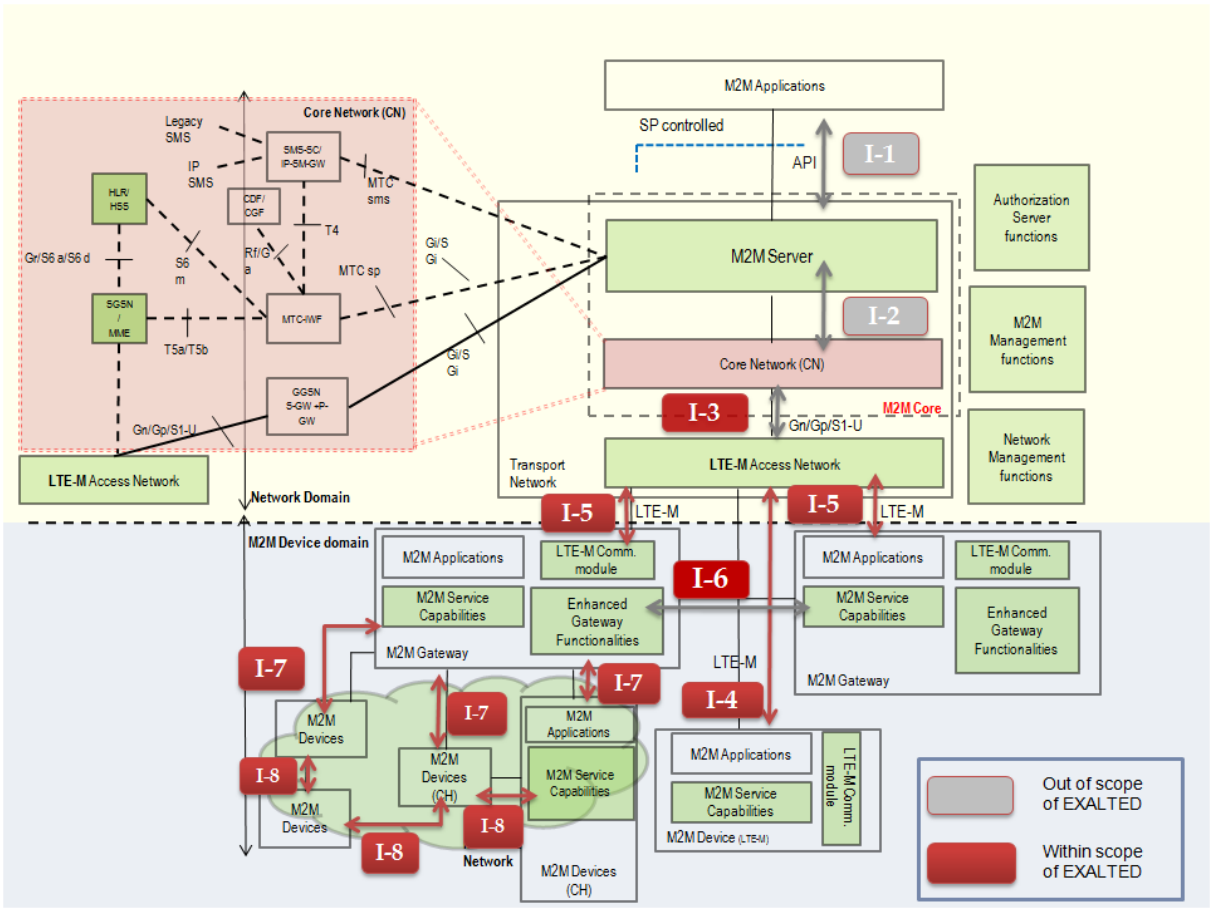

Figure 3-7: Logical relationship between components in the EXALTED system architecture

The L1-L3 protocols can change from hop to hop, e.g. LTE-M between B and C and Zigbee between C and D.

In the following this principle is mapped to the EXALTED architecture and its components. Firstly, Figure 3-7 shows the horizontal view of the interfaces, i.e. the logical relationship between the components. The interfaces relevant for the work in EXALTED are labelled with I-1 to I-8. Some interfaces are out of the EXALTED scope, i.e. the API interface, I-1, and the interface between the M2M Server and the Core Network, I2. In other words, it is assumed that the access to the end Application is possible as long as the access to the Core Network is available through the LTE-M Access Network. However, EXALTED considers also scenarios where the continuous access to the CN is not mandatory, as long as security or other required operations (e.g. authorization) has been established

Reflecting the key use cases (ITS, SMM and eHealth), the EXALTED architecture must support different types of E2E connections. These are:

- E2E connectivity between a M2M server and a LTE-M enabled end device.
- E2E connectivity between a M2M server and a non-LTE-M enabled end device located in a capillary network.
- E2E connectivity between two end devices over the ND
- E2E connectivity between non-LTE-M devices within the DD, either in the same, or in two different capillary networks.

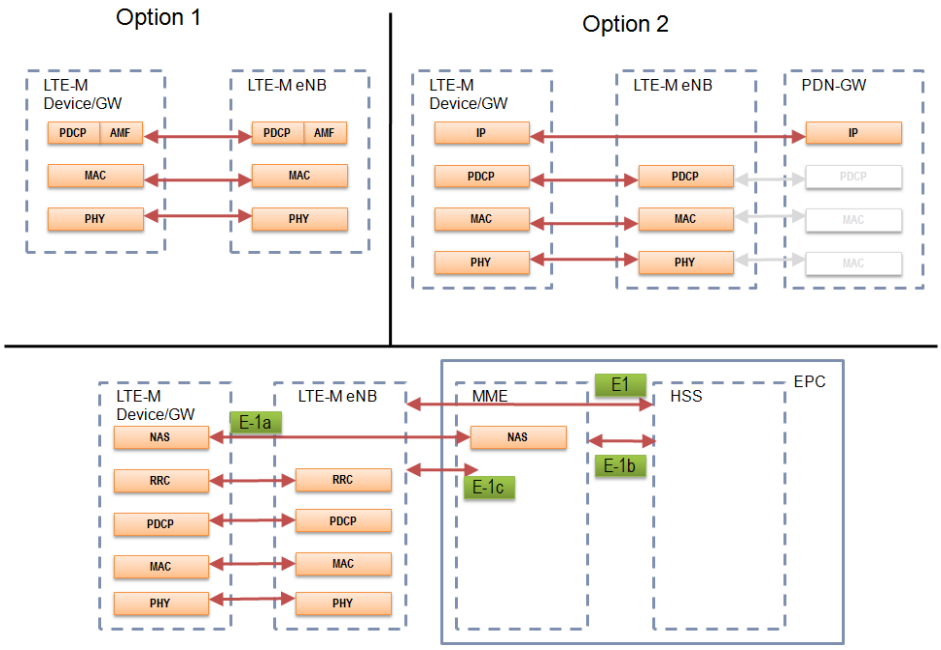

Figure 3-8: Logical interfaces between the different components within the LTE-M system

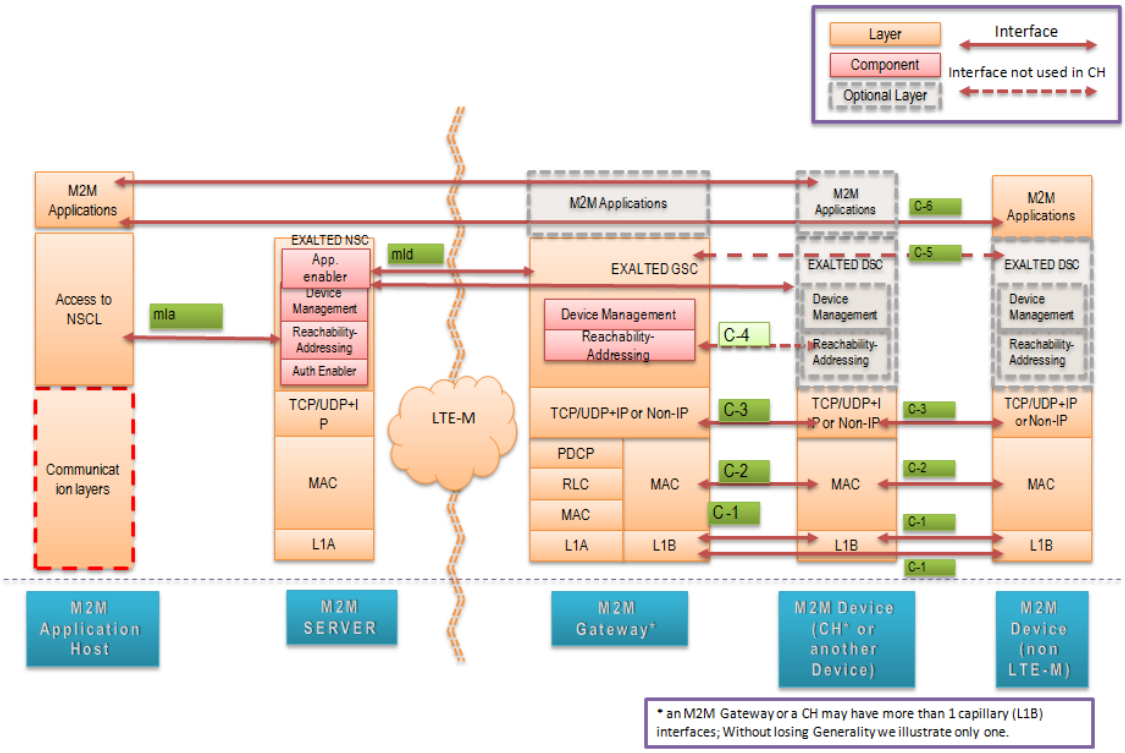

Figure 3-9: E2E logical interfaces of the EXALTED system

Figure 3-8 depicts the logical interfaces between the different components within the LTE-M system, which are detailed in 3.2.1 and 3.2.2. In short, these interfaces describe the interaction between the EPC and the LTE-M eNB and the LTE-M devices (i.e. LTE-M end devices or M2M gateways), in order to provide those functionalities, necessary for the M2M communications, such as the reduction of the information exchanged between the EPC and

the LTE-M eNB, enhanced PHY or MAC functionalities (e.g. reduction of complexity, M2M scheduler, etc.). Moreover, Figure 3-9, illustrates the E2E logical interfaces (e.g. between an end device and the M2M Server), with the corresponding functionalities and protocols being described in 3.2.3 and 3.2.4.

3.2.1 Interfaces between EPC components and LTE-M components

As discussed, EXALTED does not intend to propose any changes in the EPC, in terms of architectural changes. However, some new functionalities are introduced in the EPC, which are necessary for supporting M2M communications over LTE. These functionalities are mostly related with the management of the information exchanged between the LTE-M eNB and the EPC, taking into account the special requirements of the M2M devices (e.g their duty cycles). In the following tables, the functionalities of each component and the relative protocols are presented. Details for the following functionalities and the algorithms that realize them can be found in [3].

3.2.1.1 Interface E1: EPC (HSS) ⇔ LTE-M eNB

Functionalities of EPC (HSS)	**Functionalities of LTE-M eNB**	**Interface**
Host information about devices. Registering information about terminals	Access to information about devices	Interface E1 **Protocol**: An expansion of existing protocols, with new fields that allow recording more detailed information about terminals (users) beside existing in HSS.

3.2.1.2 Interface E-1a: EPC (MME) ⇔ LTE-M Device/M2M Gateway

Functionalities of EPC (MME)	**Functionalities of LTE-M device/GW**	**Interface**
Maintenance of the EPS bearer during duty cycling. Suspension of T3412 when duty cycle flows through inactivity phase.	Maintenance of the EPS bearer during duty cycling. Suspension of T3412 when duty cycle flows through inactivity phase.	Interface E-1a **Protocol**: Both the device or gateway and the MME suspend T3412 at the same time.

3.2.1.3 Interface E-1b: EPC (MME) ⇔ EPC (HSS)

Functionalities of EPC (MME)	**Functionalities of EPC (HSS)**	**Interface**
Maintenance of the EPS bearer during duty cycling. Suspension of T3412 when duty cycle flows through inactivity phase.	Maintenance of the EPS bearer during duty cycling. Suspension of T3412 when duty cycle flows through inactivity phase.	Interface E-1b An expansion of existing protocols, with new fields describing the duty cycling of the devices.

3.2.1.4 Interface E-1c: LTE-M eNB ⇔ EPC (MME)

Functionalities of LTE-M eNB	Functionalities of EPC (MME)	Interface
Adaptive paging	Minimization of the number of paging messages sent towards M2M device during the paging procedure	Interface E-1c **Protocol**: In adaptive paging algorithm MME sends commands to eNodeBs for paging of end device, but based on the paging tables on MME, these paging commands are sent to a reduced number of eNodeBs, so eNodeB is not aware of these algorithms. The same protocol (communication with eNodeB) is used as in LTE, the difference is that paging commands will be sent to fewer eNodebs.

3.2.2 Interfaces between LTE-M eNB and LTE-M devices/gateways (I-4, I-5)

The interfaces I-4 and I-5 (Figure 3-7) are the major interfaces in EXALTED and provide the connectivity between any LTE-M enabled device (end device or M2M Gateway) and the LTE-M eNB or LTE-M relay. These interfaces involve the PHY, MAC and RRC layers and introduce several innovations, which aim to expand the LTE radio access interface for supporting M2M. The algorithms and protocols in these interfaces result in improved spectrum and energy efficiency, wide area coverage and the support of a large number of M2M devices. Details for these solutions are given in the respective WPs. Details for the following functionalities and the algorithms that realize them can be found in [3].

Functionalities of LTE-M eNB	Functionalities of LTE-M devices/GW	Interface
Separation of LTE signal and LTE-M signal (UL)		**LTE-M PHY**
Correlation receiver for CDMA overlay (UL)	CDMA overlay (multiplication with code sequence) (UL)	**LTE-M PHY**
GFDM PHY Rx signal processing (inverse to Tx) (UL)	GFDM PHY Tx signal processing (up-sampling, pulse shaping, up-conversion) (UL)	**LTE-M PHY**
	CSI estimation process Algorithm: Feedback of CSI, PMI (UL) (see D3.3 [3], section 3.2.1)	**LTE-M PHY**
HARQ (Rx) (UL) HARQ (Tx) (DL) Control of HARQ processes (DL)	HARQ (Tx) (UL) HARQ (Rx) (DL)	**LTE-M PHY**
	Spectrum sensing (UL)	**PHY**

- Channel estimation from uplink sounding (TDD) (UL) - Calculate beamforming weights (TDD) (DL) - Zero forcing beamforming (FDD) (DL)	HARQ (Tx) (UL) HARQ (Rx) (DL)	**LTE-M PHY**
Antenna selection	- Energy detection at each antenna element - Antenna selection	**LTE-M PHY**
Energy detection at each antenna element		**LTE-M PHY**
Energy Harvesting	Energy Harvesting (UL)	**PHY**
-Collision recovery (UL) -Rateless encoding on BC channel (DL)	- Perform random access (eventually according to round robin criterion) (UL) - Rateless decoding of BC channel (DL)	**LTE-M MAC**
Random access retransmission protocol (Tx)	- Random access retransmission protocol (Tx) (UL) - Set-up of semi-static assignment of radio resources	**LTE-M MAC**
- Scheduling according to delay classes (two options: PS1, PS2)	CSI estimation	**LTE-M MAC**
- Scheduling based on clustering of devices - Scheduling based on traffic heterogeneity (according to rushing entity classifier)	Scheduling algorithm for heterogeneous traffics	**LTE-M MAC**
Packet encoding for broadcast architecture (DL)	Forwarding or decoding of packets for broadcast architecture (DL)	**LTE-M PHY**
- Optimized paging - Optimized mobility support	Monitoring paging channel and mobility support	**LTE-M RRC**
Address mapping function	Address mapping function	**LTE-M PDCP**

3.2.3 Interfaces between LTE-M components (LTE-M eNB/GW) and capillary networks

The communication between LTE-M based components and the capillary networks is very important, since it enables devices (usually low cost, low energy) with no direct access to the LTE-M access network, to get M2M services. Details for the following functionalities and the algorithms that realize them can be found in [4], [5], [18], [19], [20], [21].

3.2.3.1 Interface I-6: M2M GW ⇔ M2M GW

The communication between M2M gateways may find applications to scenarios where an M2M Gateway loses connection with the LTE-M eNB (e.g. due to severe channel conditions).

In that case, the M2M Gateway may retrieve connections through an adjacent MM Gateway with connection to a LTE-M eNB.

Functionalities of M2M GW (A)	Functionalities of M2M GW (B)	Interface
Addressing and Routing Mechanisms	Addressing and Routing Mechanisms	**-Neighbour Discovery Protocol** **-Dynamic Host Configuration Protocol** **- Mobile IP Protocol**

3.2.3.2 Interface I-7: M2M GW ⇔ non LTE-M CH

As mentioned, the functionalities of a CH may include data aggregation, device management, routing, etc. Unlike an M2M Gateway, a CH will not perform protocol translation. The CH requires a connection to a M2M Gateway in order to reach the LTE-M access network.

Functionalities of M2M GW	Functionalities of non LTE-M CH	Interface
Multihop Communications	Multihop Communications	**IEEE 802.15.4 (C-1 interface)**
Network Initialization and Control	Network Initialization and Control	**DISC (C-1 interface)**
Self Diagnostic Manager	Self Diagnostic Module Self Diagnostic Agent	**Self Diagnostic. SDM protocol over IEEE 802.15.4 (C-4)**
MIMO capabilities: - Beamforming - Device selection - Zero forcing with user selection	Channel station information, feedback	**Decentralized Source Coding (C-1 interface)**
Self-organization and pairing in capillary networks - use of group pairing / key distribution scheme, and Secure Elements to verify pairing / group set-up with M2M Service Provider (or M2M Application Provider)		
Sharing Secure Elements - reuse to secure a group of devices, sharing a eUICC (via a "hub")		

3.2.3.3 Interface I-7: M2M GW ⇔ non LTE-M device

The non LTE-M devices are able to connect to the M2M Gateway using different air interfaces (e.g. ZigBee, 802.11, etc). In order for the device to reach the LTE-M access network, specific functionalities are necessary for the Gateway as already discussed.

Functionalities of M2M GW	Functionalities of non LTE-M device	Interface
Multihop Communications	Multihop Communications	**IEEE 802.15.4 (C-1)**
Network Initialization and Control	Network Initialization and Control	**DISC (C-1)**
- Data Aggregation -Single Hop Communication	Data Aggregation	**Decentralized Source Coding (C-1)**
Device Management Protocol Translation	Device Control and Management	**Device Management.** **IEEE 802.15.4 (C-4)**
Self Diagnostic Manager	Self Diagnostic Module Self Diagnostic Agent	**Self Diagnostic. SDM protocol over IEEE 802.15.4**
- Single Hop Communication	Energy-efficiency message exchanges	**PHY (C-1)**
Addressing and Routing Mechanisms	Stateless Address Auto Configuration	**Neighbour Discovery Protocol**
- MIMO capabilities Selection diversity	Channel station information, feedback	**PHY (C-1)**
- MIMO capabilities Selection diversity	Channel station information, feedback	**PHY (C-1)**
Scheduling capabilities: Based on channel non idle counter Beacon transmission capabilities	- Memory capabilities - feedback	**Based on 802.15.4 (C-2**
Cooperative MAC protocol for high number of devices (DPCF) Capillary network based on 802.11 or 802.15.4	Two available interfaces: LTE-M and capillary network based on 802.11 and/or 802.15.4 **Algorithm**: Capillary network based on 802.11 or 802.15.4	**MAC (C-2)**
Cooperative ARQ	- Broadcast of retransmission request in case of error - Cooperative Retransmission upon request from Gateway	**(MAC)** **based on CSMA (C-2)**
Self-organization and pairing in capillary networks - use of group pairing / key distribution scheme, and Secure Elements to verify pairing / group set-up with M2M Service Provider (or M2M Application Provider)		
Device Management - use of Gateway to translate existing DM protocol		

into capillary protocols; convergence of DM protocol and usage protocol for low end devices; device management by managing Secure Element (use SE provisioning protocol)		
Sharing Secure Elements - reuse to secure a group of devices, sharing a eUICC (via a "hub")		
Gateway-assisted pairing methods in capillary network - Gateway as trusted group leader; Gateway as aggregator; Gateway as mediator between LAN and WAN side of network Infrastructure-assisted bootstrap in and between capillary networks - single capillary device connected to guest network; secured communication between capillary devices using the WAN; aggregation of capillary networks		

3.2.3.4 Interface I-8: non LTE-M CH ⇔ non LTE-M CH

This interface enables the coverage extension of the capillary network through the communications to the M2M Gateway by multiple hops between CHs.

Functionalities of non LTE-M CH (A)	**Functionalities of non LTE-M CH (B)**	**Interface**
- Energy-efficiency message exchanges - Device Control and Management- Data Aggregation	- Energy-efficiency message exchanges	**IEEE 802.15.4**
Self Diagnostic Manager	Self Diagnostic Module Self Diagnostic Agent	**Self Diagnostic. SDM protocol over IEEE 802.15.4**

3.2.3.5 Interface I-8: non LTE-M device ⇔ non LTE-M device

The non LTE-M devices within a capillary network can communicate with each other, making it possible for a device to reach the M2M Gateway through multi-hops.

Functionalities of non LTE-M device (A)	**Functionalities of non LTE-M device (B)**	**Interface**
Self Diagnostic Manager	- Self Diagnostic Module - Self Diagnostic Agent	**Self Diagnostic. SDM protocol over IEEE 802.15.4**

Cooperative ARQ	- Broadcast of retransmission request in case of error - Cooperative Retransmission upon request from Gateway	**(MAC)** **based on CSMA**
Cooperative ARQ	Listen, Store and Retransmit data packets from other non LTE-M device	**(MAC)**

3.2.4 Other Interfaces (reference points)

Functionalities of Subscription Manager	**Functionalities of eUICC (RAM/RFM/profile loader)**	**Interface**
Embedded Secure Elements and remote provisioning - reduced distribution and activation costs; multi-application UICC		

Functionalities of M2M Server	**Functionalities of M2M GW**	**Interface**
Self-organization and pairing in capillary networks - use of group pairing / key distribution scheme, and Secure Elements to verify pairing / group set-up with M2M Service Provider (or M2M Application Provider)		
Device Management - use of Gateway to translate existing DM protocol into capillary protocols; convergence of DM protocol and usage protocol for low end devices; device management by managing Secure Element (use SE provisioning protocol)		
Sharing Secure Elements - reuse to secure several communication layers (network access, M2M service layer, application layer)		

Functionalities of Auth. Server		**Interface**
Application Layer Security Model - end to end data encryption, managed by Authorization Server; extension of ETSI M2M bootstrapping model.		

3.3 Supported communications scenarios in EXALTED

The design of the EXALTED architecture took into account the required communications scenarios, necessary for supporting the envisioned use case. The communication between the elements can be one of the following two general types, with their corresponding communication modes:

- **Communication of Devices with Application Servers in the IP network** (Type 1)
- **Communication between Devices** (Type 2)

Communication between Devices and Application Servers embedded within Devices are covered by Type 2 communications.

The term Device refers to any of the entities in the Device Domain (M2M Devices, M2M Gateways, Relays, Cluster Heads). The term Application Server refers to any type of servers used in the system (M2M applications, Device Management, Security…).

3.3.1 Communication of Devices with Application Servers in the IP network (Type 1)

In this communication type, the following communication modes are available:

A. **LTE -M Device ↔ Application Server**: This is the simplest mode of communication (**Figure 3-10**), where the application data is directly encapsulated into the LTE-M protocol stack, and forwarded over the LTE-M network from a Device to a Server, and vice versa.

B. **LTE-M Device ↔ LTE-M Relay ↔ Application Server**: In this type of communication (**Figure 3-11**), the application data is directly encapsulated into the LTE-M protocol stack by the Device, and the LTE-M Relay forwards the data over the LTE-X network to the Application Server. The equivalent process occurs in the other direction.

C. **M2M Gateway ↔ Application Server**: This is a similar case to communication mode A. It an application is running on an M2M Gateway, it communicates directly with the Application Server over LTE-M network (**Figure 3-12**).

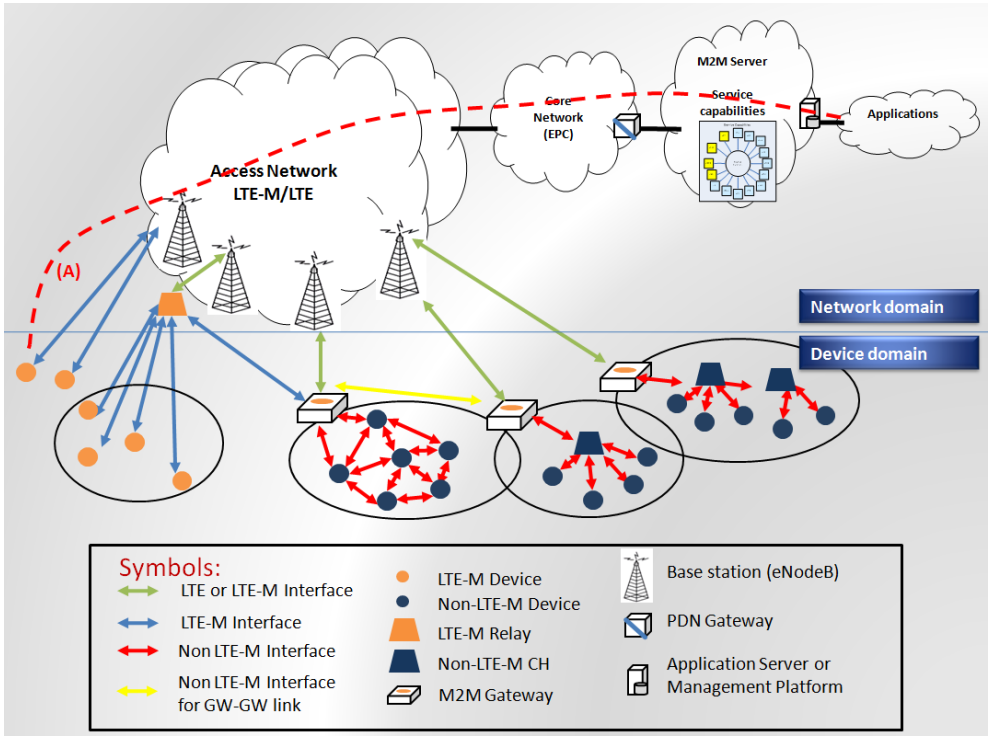

Figure 3-10: LTE-M Device – Application Server communication

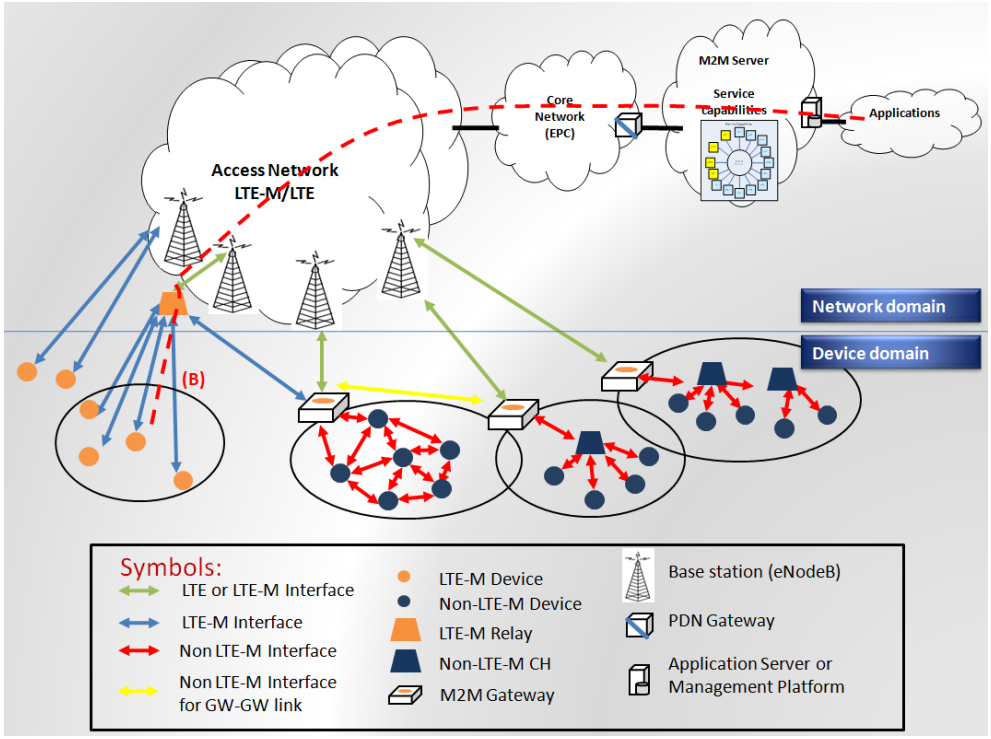

Figure 3-11: LTE-M Device – LTE-M Relay – Application Server communication

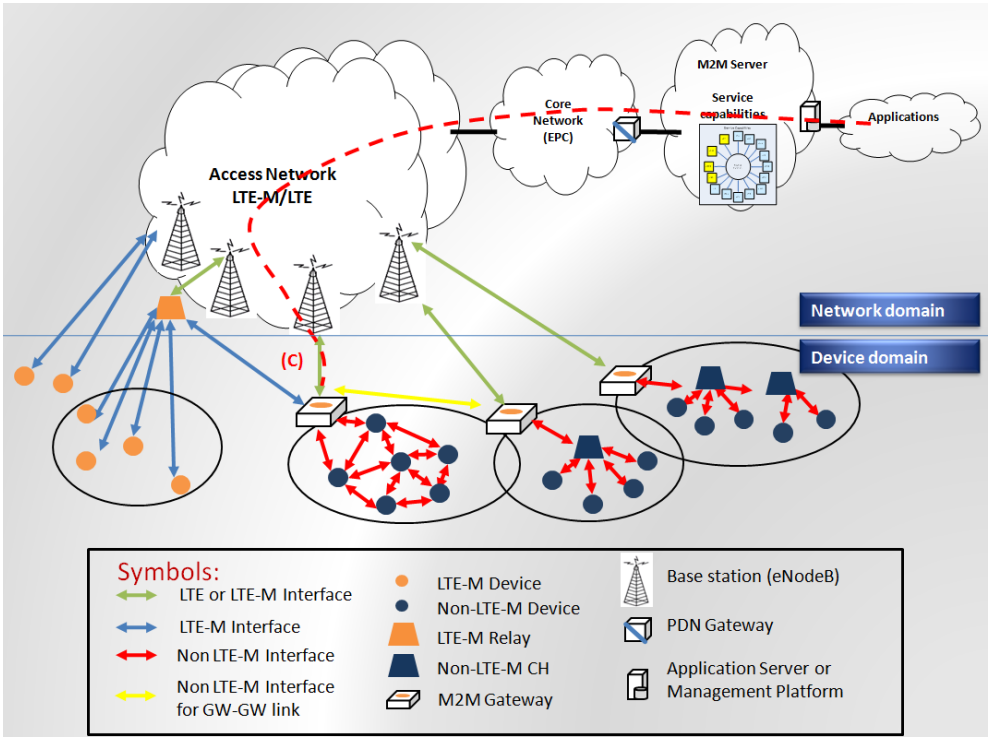

Figure 3-12: M2M Gateway – Application Server communication

D. **Non-LTE-M Device ↔ M2M Gateway ↔ Application Server**: In this case the M2M Device is part of a capillary network that is not LTE-M, and the access to the LTE-M network is realized through an M2M Gateway. The application data is sent by the M2M Device to the M2M Gateway, which performs protocol translation from the capillary network protocol to the LTE-M protocol stack and vice versa. The application data is extracted and re-encapsulated by the M2M Gateway. This scenario corresponds to different topologies in capillary networks, some of which are presented on **Figure 3-13**.

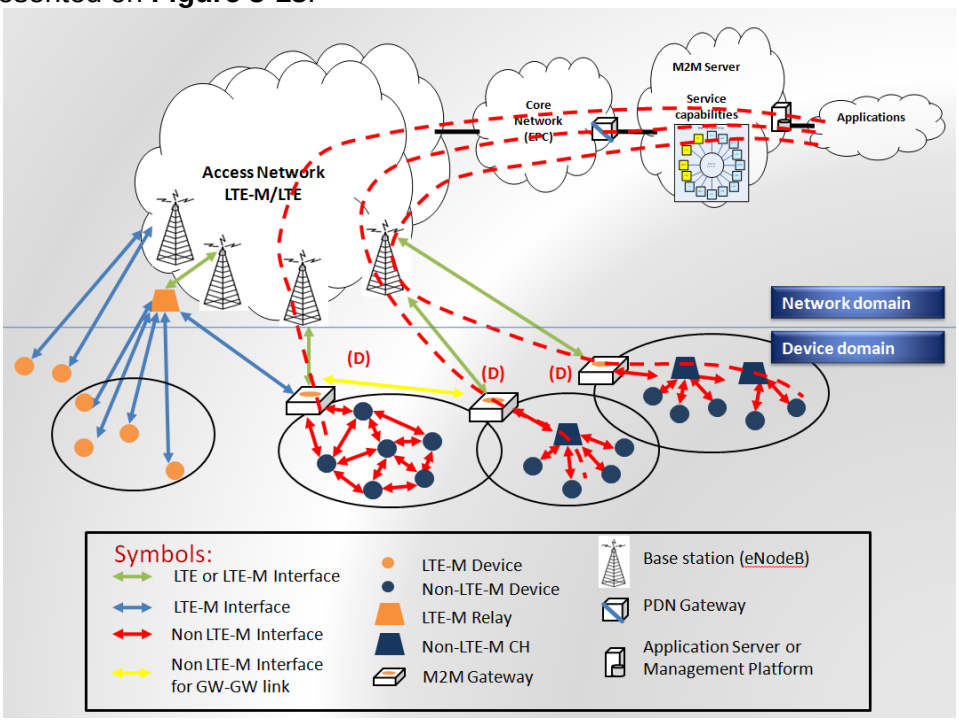

Figure 3-13: Non-LTE-M Device – Application Server communication

E. **Non-LTE-M Device Group ↔ Application Server**: It corresponds to broadcast/multicast traffic (not shown in figure for the sake of clarity) to a group of Non-LTE-M devices. Application data is encoded using network coding.

As a general note, more than one LTE/LTE-M networks may be used for the communication with the Application Server, and proper inter-networking procedures between different operators occurs.

3.3.2 Communication between Devices (Type 2)

In this communication type, the following communication modes are available (see Figure 2.2):

A. **LTE-M Device ↔ LTE-M Device over LTE-M network**: LTE-M Devices or LTE-M Gateways (case **A1**) communicate over the Base Station(s) and the LTE-M Transport and Core network. For the sake of clarity it is not shown on the **Figure 3-14**, but each PDN connection must be terminated at the PDN Gateway, so a Device-to-Device communication actually consists of 2 steps: Device-to-PDN Gateway and PDN Gateway-to-Device communication.

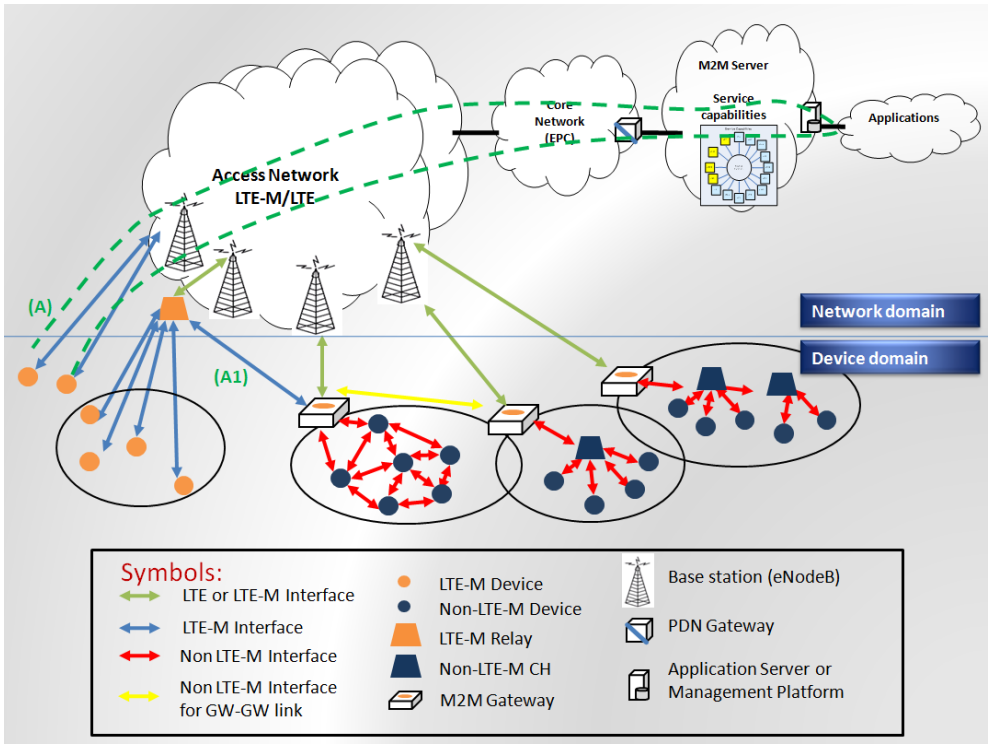

Figure 3-14: LTE-M Device ↔ LTE-M Device over LTE-M network

B. **LTE-M Device (standalone) ↔ LTE-M Device in a capillary network**: LTE-M Devices communicate over LTE-M network and PDN Gateway, and the LTE-M Relays forward data to/from LTE-M devices which it is in charge of (**Figure 3-15**).

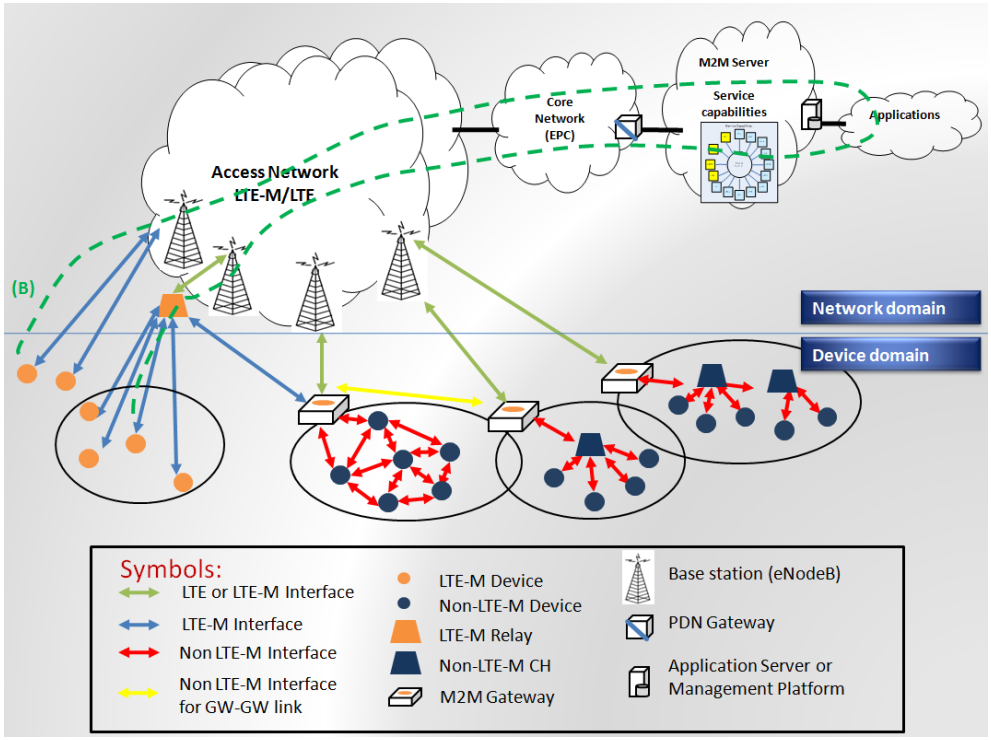

Figure 3-15: LTE-M Device ↔ LTE-M Device in a capillary network

C. **LTE-M Device ↔ LTE-M Device in the same capillary network**: Since each communication between LTE-M Devices must be established via the LTE-M network and PDN Gateway, devices in an LTE-M capillary network cannot communicate directly (**Figure 3-16**).

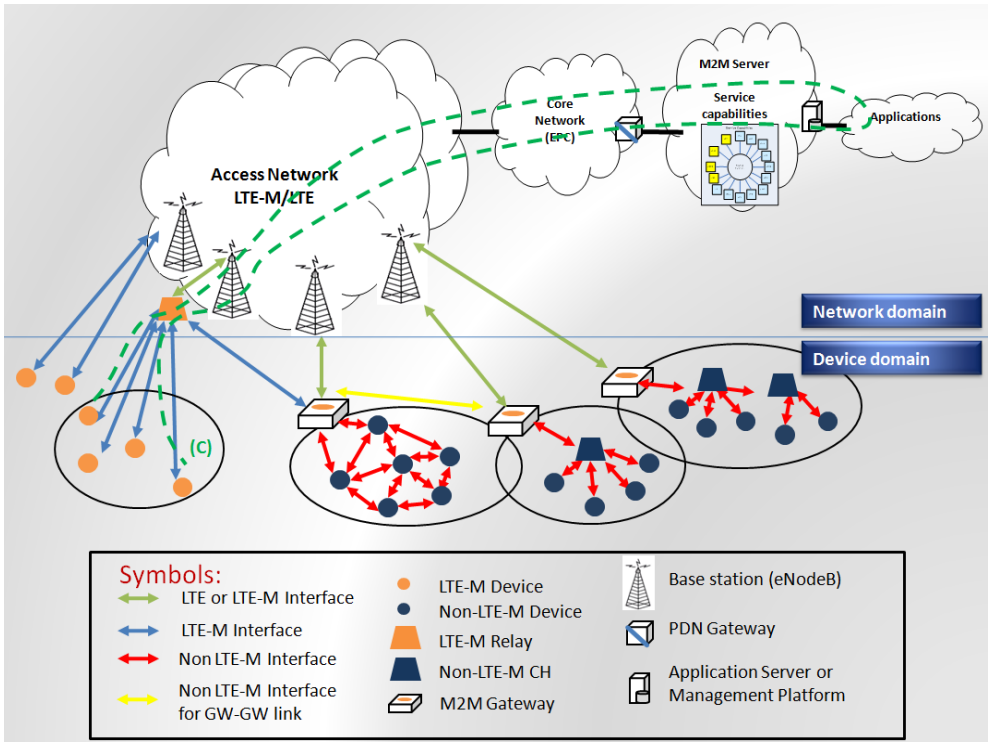

Figure 3-16: LTE-M Device ↔ LTE-M Device in the same capillary network

D. **Non-LTE-M Device ↔ Non-LTE-M Device in the same capillary network**: In this simplest case devices exchange information directly, i.e. the network is not aware of it. This type of communication is possible only if the capillary network protocol allows it. It can work between Devices (case **D1**), Device and CH (case **D2**), or two CHs (case **D3**) (**Figure 3-17**).

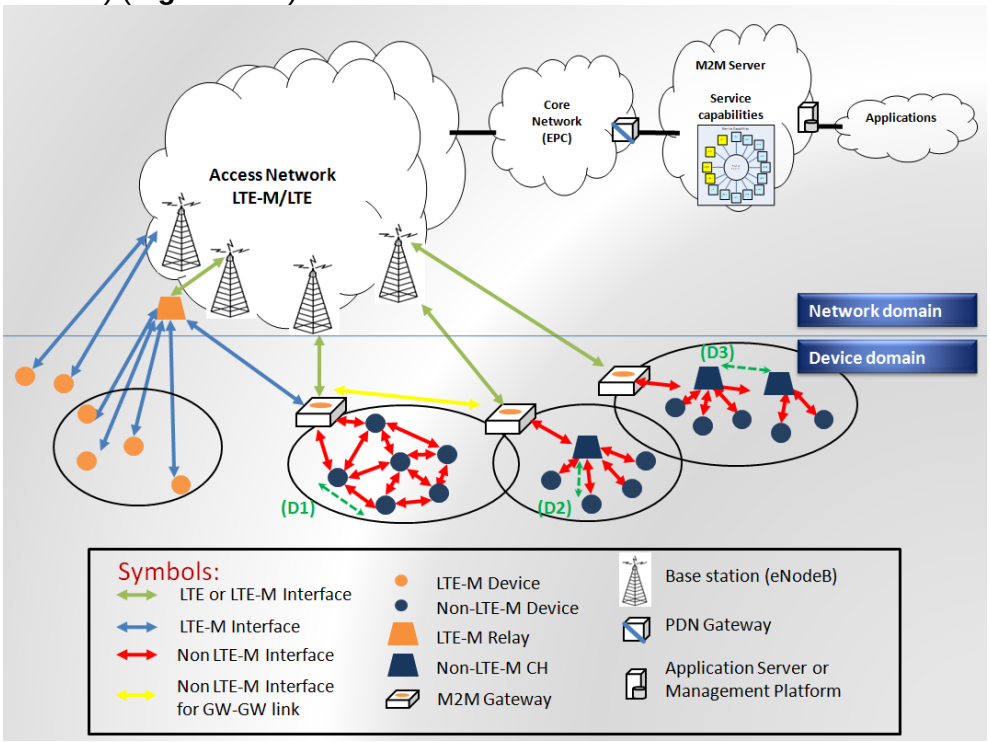

Figure 3-17: Non-LTE-M Device ↔ Non-LTE-M Device in the same capillary network

E. **Non-LTE-M Device ↔ Non-LTE-M Device in different capillary networks**: This is the most complex case of Device-to-Device communication. Devices exchange application data, but since they are not in the same capillary network they must forward the information to their M2M Gateways, which perform the protocol translation, route the traffic (over the LTE-M network, i.e. the PDN Gateway is included) to the receiving M2M Gateway, who then again translates the information to the destination device (**Figure 3-18**).

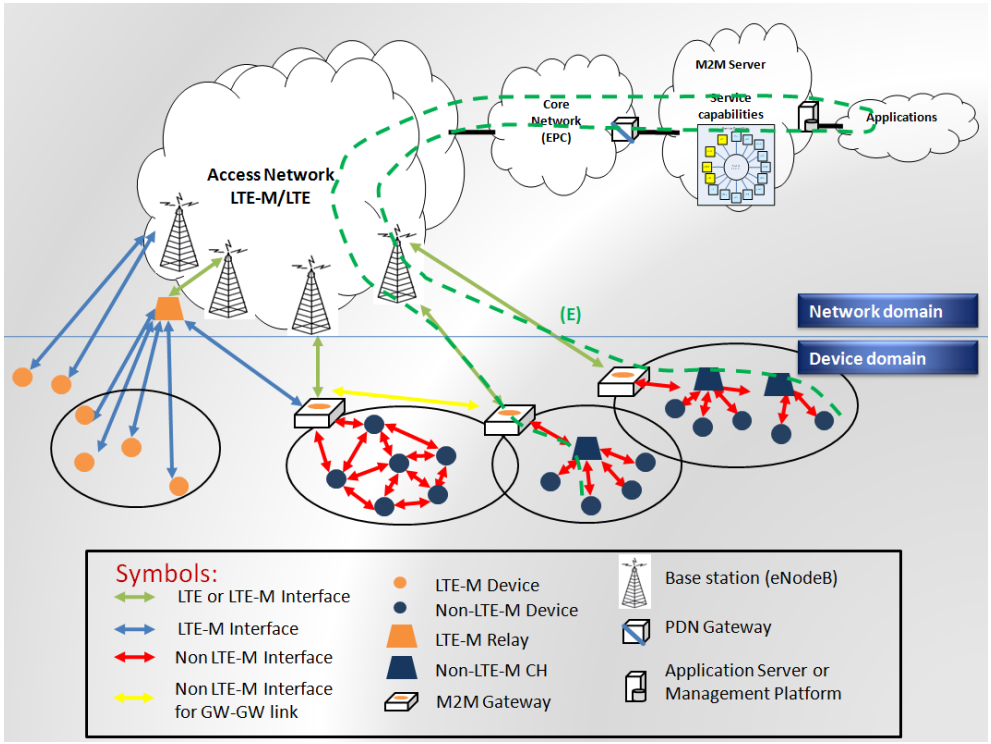

Figure 3-18: Non Non-LTE-M Device ↔ Non-LTE-M Device in different capillary networks

F. **Non-LTE-M Device Group**: It corresponds to broadcast/multicast traffic between a group of Non-LTE-M devices (**Figure 3-19**).

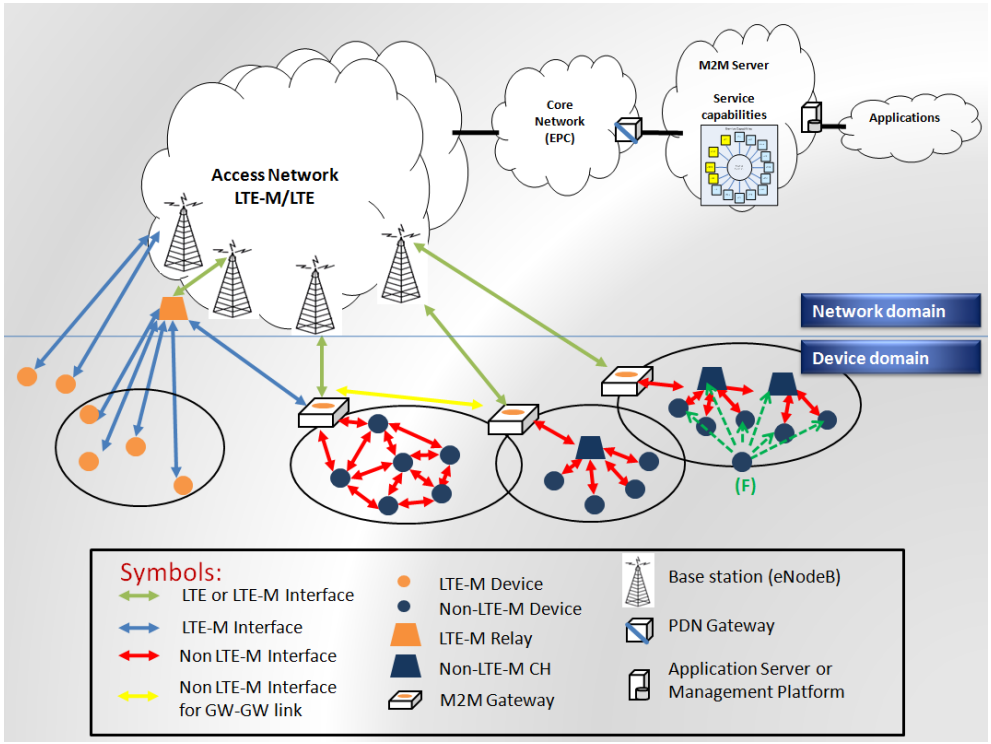

Figure 3-19: Non-LTE-M Device Group

3.4 Security aspects of the EXALTED architecture

The EXALTED security architecture is closely related to the existing LTE security model. There are several security aspects considered in LTE and LTE-M:

- **Network access security**: This concerns protection of the vulnerable radio interface. The 3GPP EPS/LTE standard provides the following features to mitigate against network access security threats:
  - Mutual authentication and key agreement: Mutual authentication is performed between the UE and MME using authentication vectors provided by the HSS. The authentication protocol is an enhanced version of the 3G AKA protocol used in UMTS.
  - Confidentiality and integrity protection of RRC signaling: NAS signaling security is established at initial attach using the NAS security mode command procedure. The procedure determines which cryptographic algorithms and keys should be used to encrypt and integrity protect subsequent NAS signaling messages.
  - Confidentiality and integrity protection of NAS signaling: RRC signaling security is established at transition to active mode using the RRC security mode command procedure. The procedure determines which cryptographic algorithms and keys should be used to encrypt and integrity protect subsequent RRC signaling messages.
  - Confidentiality protection of user traffic: LTE user traffic can be confidentiality protected, but not integrity protected, over the radio interface. User traffic encryption is established at transition to active mode using the RRC security mode command procedure. The procedure determines which cryptographic algorithms and keys should be used to encrypt and integrity protect user traffic.
  - Identity and location confidentiality: Identity and location confidentiality over the radio interface in LTE are achieved in a similar way to GSM and UMTS. In particular, temporary identifiers called GUTIs are generally used instead of the permanent IMSI when the user needs to be identified on the radio interface

- **Backhaul security**: Architectural changes compared to UMTS mean that the backhaul link is more vulnerable to attack and needs dedicated protection.
- **eNodeB security**: Architectural changes compared to UMTS combined with a trend towards smaller cells deployed in more vulnerable locations mean that more attention needs to be given to securing the eNodeB against physical and logical attack.
- **Core network security**: While the access network deserves special attention with respect to security, it is important that the security requirements concerning the core network are not neglected. The access network in LTE deserves special attention with respect to security due to the nature of the radio interface, the placement of eNodeB in untrusted locations, and the untrusted nature of the backhaul link. However, the core network should not be neglected as far as security is concerned since this is where traffic is concentrated, so a successful attack on the core network is potentially much more devastating than an attack on the access network. While it may not be cost effective to protect all LTE core network interfaces, some particularly sensitive interfaces may need to be encrypted and authenticated using IPsec or TLS. In addition, interfaces with roaming partners, interconnect partners and other third parties may also need to be encrypted and authenticated. The 3GPP standard specifies profiles of IPsec and TLS for protecting core network interfaces that need protection. These profiles should be used where possible.

The LTE-M security architecture will be closely based on LTE, largely as this is a proven standardized design, inherited from previous generations of standards (GSM and 3G) with

many enhancements over the years. In particular, the LTE/3G/GSM authentication and key agreement model (involving the SIM card or UICC as a secure element) is very robust, and highly regarded by mobile operators: operators are unlikely to accept anything radically different.

LTE-M may in fact use the USIM as its Network Access Application (NAA); i.e. use the same application that is already used in LTE and 3G networks, and can also be used in 2G mode on GSM networks. This would have big compatibility advantages in the case of LTE-M devices which are also capable of accessing legacy networks. It could also have significant cost advantages, since UICCs with USIMs are already ordered en masse for existing mobile networks, so the starting cost would be lower than with a brand new NAA. Yet the USIM is also adaptable for future uses, since the same basic key agreement model can be used with a variety of key hierarchies (the hierarchies for 3G and LTE are quite different for instance, and LTE-M may also need to be different again, as may an application layer key hierarchy – see Section 3.5.3).

LTE-M is likely to need some optimisations to the UICC form factor (e.g. embedded UICC) to allow for the fact that many LTE-M devices cannot conveniently take a removable smart card, or the card cannot be conveniently swapped in the field. There are also likely to be some optimisations to the back-end key management to minimize overall costs of managing the UICC.

3.4.1 Embedded secure element to create application level security

The ETSI M2M group has proposed an architecture relying upon a hierarchy of keys which are used for different levels of authentication and authorization. This hierarchy involves 3 levels of keys:

- The root key initially provisioned in the devices and in the authentication server side;
- The service key derived from the root key;
- The application key derived from the service key.

There is one root key for each provisioned M2M device credentials. The root key may be stored in a secure element and the perspective of using the same secure element in a low cost M2M device to perform both network authentication and bootstrap application level security seems pretty attractive.

3.4.2 Role of the M2M Gateway in security

Since one of the goals of EXALTED is to make possible low cost M2M communications, the M2M Gateway could play an essential role to enable this to happen by aggregating together the communications originating from many devices located behind it in such a way that the presence of this possibly large number of devices behind the gateway will become transparent from the network, same as NAT gateways are used in the IP world to enable multiple IP devices to communicate on the internet.
Some of the communication scenarios involve the use of a gateway for communication from a LAN onto a wide area network, and the gateway device has an LTE-M radio. In the case the secure element in the gateway may be used for delegated authentication, relieving the load upon the network side. Many implementations would have a single device acting as both gateway and hub, but not all. For instance there might be an “indoor” device which acts as an authentication hub, and a set of “outdoor” sensor devices. For reasons of radio efficiency it is then better to make one (or more) of the outdoor devices act as a communications gateway. Architectures with one authentication hub but multiple gateways/exit points in a LAN also need to be considered.

From the security perspective the gateway can lower the cost of M2M communication in 2 ways:

- The network need not be involved in the Authentication of leaf M2M devices the traffic of which transit by the gateway. Instead the gateway, using a suitable “re-delegation” scheme should be able to authenticate leaf devices using “local” authentication schemes.
- When a large number of devices are involved, Point to point challenge response authentication may become heavy. Broadcasting mechanisms could be very useful to enable low overhead simultaneous authentication of a large number of devices. Unlike challenge/response schemes, Broadcasting does not require a response from the leaf devices. Instead a single challenge is sent simultaneously to all devices via the broadcast channel. Each of the leaf devices receives and processes silently the challenge in order to derive one or multiple key that will be subsequently used in data communications. Only those devices having successfully processed the challenge will be able to communicate with others.

3.4.3 Key hierarchy

The use of symmetric keys for data protection is often used in conjunction with key diversification mechanisms to derive one or more keys from a common root secret value. Such practices may prevent an attacker who obtains a derived key from learning useful information about either the root secret value or any of the other derived keys.
In our case the key diversification mechanisms proposed serve the purpose of enforcing the notion of device ownership and also enable a same device to protect different data streams it may transmit or receive.

The proposed hierarchy of keys to meet those goals is defined as follows:

1. The **root** key or the **device** key: This key is generated at device manufacturing time and is uniquely associated with a specific device. It can be implemented using a signed certificate stored inside the device, or by embedding inside the device a simple symmetric key. The root key is used only in bootstrapping the definition of an owner key. The lifetime of the root key is equal to the lifetime of the device.
2. The **owner** key: This key defines the ownership of a particular device by a specific user or legal entity. It is also used to define the enrolment of the device owner with the Identity provider. This enrolment will be performed in an enrolment phase where the device owner will register his device (referenced with the root key). The device root key will be used to protect the provisioning of the owner key inside the device. At the end of the enrolment phase, the identity provider and the device share a common secret: the owner key. This key will be used to authenticate the device registering in the network, but also for further key diversification operations. The lifetime of the user key is equal to the lifetime of the device ownership by that user. A cession or transmission of the device to another user will lead to the generation of another user key.
3. The **scope** keys: M2M devices commonly act as data senders or receivers. One single device may also possibly transmit or receive different data types that may require distinct data protections. For example, a sensor may transmit different types of measurements (i.e. pressure and temperature), requiring distinct access rights. Also, distinct privileges may be required to receive the data stream emitted by an M2M device and send remote control commands to that device. A data scope is a specific data type sent or received by a device. A key is associated to each scope. Also, the same data stream may be exposed as distinct scopes, for business reasons. For example, a device may deliver some data which may be received by parties using distinct subscription rates. In this case, the same data stream may be transmitted more than once, protected with different scope keys. Scope keys are defined statically. They do not need to be changed as long

as the data scopes do not change and the device ownership does not change The owner key is used to protect the transmission of each scope key on the device. But scope keys are not only shared between the device and the identity provider. They are also distributed to each party authorized to use the device according to a particular scope. For very simple devices, the notion of scope may be created using a proxy gateway that would split and re-encode the data streams as appropriate.

4. The **scope session keys**: The registration of the device to the network gives way to the generation of a temporary session key per scope, which will be valid only for the duration of the session. It is this session key that will be used to encrypt the data stream. Each session scope key is provisioned in the device, protected by the corresponding scope key.
5. The **network session** key(s): the owner key, scope keys and scope session keys are keys shared between the device and the identity provider. The network session key in contrast is shared between the device and the network service provider. It serves the purpose of protecting the exchanges between the device and the closest service gateway. Two distinct schemes will be described for the definition of the network session key: The first one relies on the distribution of credentials directly from the network service provider to the M2M device, the other on a authentication by delegation where the network service provider delegate the device authentication and session key generation to the identity provider.

4 Conclusion

The natural ecosystem of EXALTED is to be found within the 3GPP LTE specifications, with the main scope being to leverage and enhance the 3GPP MTC Architecture. Although the focus of EXALTED is on M2M communications, the ETSI M2M system has been also taken into account, and the ETSI M2M functional specifications are met whenever they fall within the EXALTED scope of work. The EXALTED architecture covers a wide area of communication scenarios between end-devices and M2M servers, or between end-devices through the LTE-M access network, with the main objective being to provide an architecture which supports efficient and cost-effective wireless M2M communications. Moreover, it covers all the technical requirements, derived from the use cases and scenarios and the ones derived during the work progress and refinements.

The EXALTED architecture consists of two elements, namely components and interfaces. Components can be either physical entities, e.g. devices, or the logical combination of functions, e.g. EPC and M2M server. All components are characterized by their functionality, which can be either mandatory or optional. Algorithms realizing these functions are considered to be exchangeable and not part of the architecture. In the style of [2], it is distinguished between device domain (DD) and network domain (ND). Section 3.1 provides a summary of all relevant components and their functionality as far as considered in EXALTED

The interaction between components is controlled by interfaces. They can be grouped in two main categories, namely peer-to-peer lower layer interfaces and end-to-end higher layer interfaces. In section 3.2 all interfaces are identified and classified. The purpose of an interface is to support appropriate signalling exchange on the respective layers between the components at both of its ends in order to provide the related services. Interfaces are realized by protocols. Apart from IP, which is one the basic working assumptions in EXALTED, it is left to WP3-6 how the protocols are specified. The EXALTED architecture will serve as the basis for the overall system concept evaluation and final alignment of all the technical solutions.

Appendix

A1. EXALTED technical requirements

Table A 1 gives a coherent view of all technical requirements in EXALTED derived from the three key use cases *Intelligent Transportation System*, *Smart Metering and Monitoring*, and *E-healthcare*, but valid for other M2M applications as well. Details can be found in the public deliverable [6].

Table A 1: Summary of technical requirements in EXALTED

ID	Title	Priority	Dependencies
FU.1	Support of large number of devices	Mandatory	NT.10
FU.2	Efficient spectrum management	Mandatory	
FU.3	Support for diverse M2M services	Mandatory	
FU.4	Network initiated packet-data communication	Mandatory	
FU.5	Local and remote device management	High	
FU.6	Unique identity for devices	High	NT.16
FU.7	Security and provisioning	Mandatory	
SV.1	Overall QoS	Mandatory	NT.14, NF.5
SV.2	Allow multiple service providers on M2M devices	Low	SV.3, NF.3
SV.3	Efficient provisioning of a set of M2M equipments	Mandatory	NF.1, NT.13, DV.1, DV.10
SV.4	Change of subscription	Mandatory	SV.3
SV.5	Delegation and distribution of functionality	Mandatory	NT.4
SV.6	Security	Mandatory	
NT.1	Heterogeneous networks	Mandatory	
NT.2	LTE-M backward compatibility	Mandatory	
NT.3	NT.3 – Minimum number of modifications in network infrastructure	Mandatory	NT.2
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.4
NT.7	Flexible addressing scheme	Mandatory	NT.3
NT.8	Mobility management	Mandatory	
NT.9	Reliable delivery of a message	High	
NT.10	High node density	Medium	NF.6
NT.11	Traffic aggregation	Medium	
NT.12	Self-diagnostic and self-healing operation	Medium	DV.1
NT.13	Multicast and broadcast communication	Mandatory	
NT.14	End-to-end QoS system	Mandatory	NT.6, NT.8
NT.15	End-to-end session continuity	Mandatory	NT.6, NT.8, NT.9
NT.16	Support for dual stack IPv4/IPv6	Mandatory	NT.7
NT.17	Reduced signaling	Mandatory	DV.3
NF.1	Scalability	Mandatory	NF.6
NF.2	Energy efficiency	Mandatory	DV.3, DV.9
NF.3	Extensibility and adaptability	Medium	
NF.4	Real time performance	Medium	
NF.5	Congestion control mechanism	Low	
NF.6	Address space scalability	High	
NF.7	Control signaling integrity protection and encryption	Mandatory	
NF.8	Service provisioning for MNO/SP customers	Mandatory	SV.3
NF.9	Roaming support	Mandatory	NT.8
DV.1	Self organized M2M equipments	Mandatory	
DV.2	Reliable M2M equipments	High	
DV.3	Energy efficient duty cycles	Mandatory	NF.2
DV.4	Location information	High	

DV.5	Location locked M2M equipments	High	
DV.6	Gateway detection and registration	Mandatory	NT.13
DV.7	Protocol translation at the Gateway	Mandatory	NT.1
DV.8	Information routing at the Gateway	Mandatory	NT.1
DV.9	M2M equipment wake-up	Mandatory	
DV.10	Remote configuration	Mandatory	NT.12
DV.11	Software update over the air	Mandatory	

List of Acronyms

Acronym	Meaning
3GPP	3rd Generation Partnership Project
AC	Access Network
AE	Application Enablement
API	Application Programming Interface
ARM	Addressing and Routing Mechanisms
ARQ	Automatic Repeat Request
CB	Compensation Broker
CDMA	Code Division Multiple Access
CDF	Charging Data Function
CGF	Charging Gateway Function
CH	Cluster Head
CoAP	Constraint Application Protocol
CS	Communication Selection
CN	Core Network
C-RNTI	Cell Radio Network Temporary Identifier
DA	Data Aggregation or Device Application (context dependant)
DC	Data Collection
DCM	Device Control and Management
DCS	Data Compression Strategy
D/GD	Device and Gateway Domain (in ETSI M2M)
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
DMPT	Device Management Protocol Translation
DRX	Discontinuous Reception cycle
DSC	Decentralized Source Coding
DSCL	Device Service Capability Layer
E2E	End-to-end
EE	Energy-efficiency message exchanges
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GA	Gateway Application (M2M Application on the M2M Gateway)
GC	Generic Communication
GD	Gateway Domain
GFDM	Generalized Frequency Division Multiplexing
GGSN	Gateway GPRS Support Node
GSCL	Gateway Service Capability Layer
GSM	Global System for Mobile Communications
GUTI	Globally Unique Temporary Identity
GW	Gateway
HARQ	Hybrid Automatic Repeat Request
HDR	History and Data Retention
HSS	Home Subscriber Server
HLR	Home Location Register
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISDN	Integrated Services Digital Network
(N/G/D)IP	(Network/Gateway/Device) Interworking Proxy

ITS	Intelligent Transport System
LDPC	Low Parity Density Check
LTE	Long Term Evolution
LTE-A	Long Term Evolution – Advanced
LTE-M	Long Term Evolution for Machines
M2M	Machine-to-Machine
MAC	Medium Access Control
MBMS	Multimedia Broadcast / Multicast Service
MBSFN	Multimedia Broadcast / Multicast Service Single Frequency Network
MGM	Mediated Gossiping Mechanism
MHC	Multihop Communications
MIMO	Multiple Input Multiple Output
MIP	Mobile IP Protocol
MME	Mobile Management Entity
MNO	Mobile Network Operator
MQTT	Message Queue Telemetry Transport
MSISDN	Mobile Subscriber ISDN Number
MTC	Machine Type Communications
MTC-IWF	MTC Inter Working Function
NA	Network Application (M2M Application in ND)
NAA	Network Access Application
NAS	Non Access Stratum
ND	Network Domain
NDP	Neighbour Discovery Protocol
NIC	Network Initialization and Control
NSCL	Network Service Capability Layer
OMA-DM	Open Mobile Alliance - Device Management
PDN	Public Data Network
PGN	Packet Data Network Gateway
PLMN	Public Land Mobile Network
PoC	Point of Contact
PR	Payload Reduction
PMRACH	Physical MTC Random Access CHannel
RAN	Radio Access Network
RAR	Reachability, Addressing and Repository
RAT	Radio Access Technology
REM	Remote Entity Management
REST	REpresentational State Transfer
RLC	Radio Link Control
RRC	Radio Resource Control
SC	Service Capabilities
ROHC	Robust Header Compression
SC-FDMA	Single Carrier Frequency Division Multiple Access
SCL	Service Capabilities Layer
SEC	SECurity
SDA	Self Diagnostic Agent
SDM	Self Diagnostic Module
SDMGR	Self Diagnostic Manager
SE	Secure Element
SGSN	Serving GPRS Support Node
SHC	Single Hop Communication
SIM	Subscriber identity module
SLAAC	StateLess Address Auto Configuration
SM	Session Management

SMM	Smart Metering and Monitoring
SMS-SC	Short Message Service - Service Centre
SP	Service Provider
SPI	Serial Peripheral Interface
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TM	Transaction Management
TOE	Telco Operator Exposure
UE	User Equipment
UICC	Universal Integrated Circuit Card
UL	Uplink
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
UTRAN	Universal Terrestrial Radio Access Network
WP	Work Package

References

[1] 3GPP TR 23.888 V1.6.1, "System Improvements for Machine-Type Communications," Release 11, February, 2012.
[2] ETSI TS 102 690 V1.1.1, "Machine-to-Machine communications (M2M); Functional architecture," October, 2011.
[3] FP7 EXALTED consortium, "D3.3 – Final report on LTE-M algorithms and procedures", project report, July 2012.
[4] FP7 EXALTED consortium, “D6.2 – Final specification of the energy-efficiency implementation”
[5] FP7 EXALTED consortium, “D6.3 – Final specification of the reliable device implementation”, project report, February 2012.
[6] FP7 EXALTED consortium, "D2.1 – Description of baseline reference systems, scenarios, technical requirements & evaluation methodology", project report, May 2011.
[7] FP7 EXALTED consortium, “D2.2 – Impact of use cases on business model”, project report, August 2011.
[8] 3GPP TR 21.905 10.3.0, "Vocabulary for 3GPP Specifications," Release 10, March, 2011.
[9] Fielding, Roy Thomas (2000): "Architectural Styles and the Design of Network-based Software Architectures", Doctoral dissertation, University of California, Irvine.
[10] IETF RFC 2616: "Hypertext Transfer Protocol -- HTTP/1.1".
[11] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".
[12] https://datatracker.ietf.org/doc/draft-ietf-core-coap/
[13] ETSI, TS 101 603 V0.0.1, "Machine-to-Machine communications (M2M); 3GPP Interworking, " Draft, June, 2012.
[14] 3GPP TS 23.002: "Network Architecture".
[15] 3GPP TS 23.401: "GPRS enhancements for E-UTRAN access".
[16] 3GPP TS 23.402 "Architecture enhancements for non-3GPP accesses".
[17] FP7 EXALTED consortium, "D3.1 – First report on LTE-M algorithms and procedures, August 2011.
[18] FP7 EXALTED: "D4.1 - M2M Packet Data Protocols between LTE-M and Capillary Networks", project report, June 2012.
[19] FP7 EXALTED: "D4.2 - IP Networking System for M2M communications for EXALTED use cases", project report, June 2012.
[20] FP7 EXALTED: “D4.3 – Device Management”, project report, October 2012, to appear.
[21] FP7 EXALTED: "D4.4 - Traffic Aggregation", project report, October 2012, to appear.