FUTURE COMMUNICATION ARCHITECTURE FOR MOBILE CLOUD SERVICES
Acronym: Mobile Cloud Networking Project No: 318109
Integrated Project FP7-ICT-2011-8 Duration: 2012/11/01-2015/10/31

D2.1

Reference Scenarios and Technical System Requirements Definition

Type	Public
Deliverable No:	D2.1
Workpackage:	WP2
Leading partner:	Portugal Telecom Inovação
Author(s):	Jorge Carapinha, Carlos Parada (Editors), List of Authors overleaf
Dissemination level:	Public
Status:	Final
Date:	01 April 2013
Version:	1.0

List of Authors (in alphabetical order):

Adel Alhezmi	FHG
Almerima Jamakovic	UBERN
Alvaro Rodriguez	STT
André Gomes	UBERN
Andy Edmonds	ZHAW
Bhavin Trivedi	INTEL
Carlos Parada	PTIN
Daniele Stroppa	ZHAW
David Palma	ONE
Elena Demaria	TI
Georgios Karagiannis	UTWENTE
Ivano Guardini	TI
João Soares	PTIN
Jorge Carapinha	PTIN
Lúcio Ferreira	INOV
Luís Correia	INOV
Marc Villinger	SAP
Marco Liebsch	NEC
Marius Corici	FHG
Mónica Branco	INOV
Nicolas Bihannic	FT
Paolo Crosta	ITALTEL
Pedro Neves	PTIN
Plamen Ganchosov	CS
Santosh Kawade	BT
Simone Ruffino	TI
Sina Khatibi	INOV
Steffen Haase	SAP
Tarik Taleb	NEC
Thijs Metsch	INTEL
Thomas Michael Bohnert	ZHAW
Uwe Riss	SAP

Reviewers:

Edmundo Monteiro	ONE
Keith Briggs	BT
Peter Gray	CS
Thomas Bohnert	ZHAW

Versioning and Contribution History

Version	Description	Contributors
0.1	First draft	Jorge Carapinha, Carlos Parada et al.
0.5	Peer review version	Jorge Carapinha, Carlos Parada et al.
1.0	Final version ready for submission	Jorge Carapinha, Carlos Parada et al.

Executive Summary

This report is a public deliverable of the Mobile Cloud Networking (MCN) EU-FP7 Project and provides the results of Task 2.1 “Reference Scenarios and Requirements”, which ran in the first five months of the Project as part of WP2 “Scenarios, Requirements, Business Models, and Overall Architecture”. The basic goals of this task have been the identification and definition of a set of reference scenarios, use cases, stakeholders and, based on those results, the specification of requirements. These results are intended to be used as baseline for the activities to be carried out in the scope of other MCN Work Packages (namely WPs 3, 4 and 5), as well as the other tasks in WP2 (T2.2, T2.3) dealing with business models and overall MCN architecture.

Task 2.1 activities generally followed guidelines from best practices in requirements engineering. The work was carried out in three main stages:

1. Identification of draft scenarios, covering the full spectrum of the project technical domain;
2. Consolidation of the draft scenarios in a smaller set of scenarios, and definition of stakeholders and use cases based on those consolidated scenarios;
3. Specification of requirements organised in four technical domains: Cloud Data Centre Infrastructure and Network Programmability, Access Network Infrastructure Cloud, Mobile Core Network Cloud, IMS/OSS/BSS/VAS as a Service.

This report presents the final results of this activity. It starts by providing the basic terminology used throughout the document and then describes the adopted methodology. The basic stakeholders are presented, with a focus on functional roles and their relationships. A set of five real-life scenarios illustrates the scope of the MCN project and its potential, from a business or social point of view. Finally, an extensive list of requirements is presented, organized in the four technical domains identified above.

Table of contents

List of Figures

List of Tables

List of Acronyms

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorisation, and Accounting
ABC	Always Best Connected
API	Application Programming Interface
ASP	Application Services Provider
BBU	Base Band Units
BS	Base Station
BSS	Business Support System
CAPEX	Capital Expenditure
CDN	Content Delivery Network
CDR	Charging Data Record
CIP	Cloud Infrastructure Provider
COTS	Commercial Off-The-Shelf
CPP	Cloud Product Provider
CPU	Central Processing Unit
CRM	Customer Relationship Management
CSP	Cloud Service Provider
DC	Data Centre
DIP	Data Centre Infrastructure Provider
DoW	Description of Work
DPI	Deep Packet Inspection
DS	Digital Signage
DSN	Digital Signage Network
E2E	End-to-End
EEU	Enterprise End User
EPC	Evolved Packet Core
EPCaaS	EPC-as-a-Service
EPS	Evolved Packet System
EU	End User
FP7	Framework Programme 7
GGSN	Gateway GPRS Support Node
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HSS	Home Subscriber Server
HW	Hardware
IaaS	Infrastructure-as-a-Service
ICN	Information Centric Networking
IEU	Individual End User
IMS	IP Multimedia Subsystem
IMSaaS	IMS-as-a-Service
IP	Internet Protocol
LAN	Local Area Network
LCD	Liquid Crystal Display
LCR	Least Cost Routing
LTE	Long Term Evolution
M2M	Machine to Machine
MCN	Mobile Core Network
MCNC	(EPC) Mobile Core Network over a Cloud infrastructure

MCNP	Mobile Core Network Provider
MCNSP	Mobile Cloud Networking Service Provider
MME	Mobility Management Entity
MNO	Mobile Network Operator
MTC	Machine Type Communication
MVNO	Mobile Virtual Network Operator
NCP	Network Connectivity Provider
O&M	Operation & Maintenance
OPEX	Operational Expenditure
OSS	Operation Support System
OTT	Over-The-Top
PaaS	Platform-as-a-Service
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PGW	Packet Data Network Gateway
PoP	Point of Presence
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
RANaaS	RAN-as-a-Service
RANP	Radio Access Network Provider
RAT	Radio Access Technology
RC	Requirements Cluster
RE	Requirements Engineering
RRH	Remote Radio Head
RSS	Rich Site Summary
SaaS	Software-as-a-Service
SB	Service Broker
SDN	Software-Defined Networking
SDO	Standards Development Organisation
SGSN	Serving GPRS Support Node
SGW	Signalling Gateway
SLA	Service Level Agreement
SSP	Support Systems Provider
SW	Software
TD	Technical Domain
UI	User Interface
UML	Unified Modeling Language
UMTS	Universal Mobile Telecommunication System
UP	Utility Provider
VAS	Value-Added Service
VM	Virtual Machine
VRAN	Virtual Radio Access Network
WP	Work Package
XaaS	Anything-as-a-Service

1 Introduction

1.1 Motivation, Objectives and Scope

Mobile Cloud Networking (MCN) is a European FP7 Large-scale Integrated Project, which aims at investigating, implementing and evaluating the technological foundations for novel mobile network architecture and technologies, leading the way to fully cloud-based mobile communication systems (Mobile Cloud Networking Project, 2012). Additionally, MCN aims at extending cloud computing to support on-demand and elastic provisioning of novel mobile services and providing service orchestration with guaranteed end-to-end SLAs across multiple heterogeneous technological domains – wireless, mobile core and data centres. The objectives of the MCN project and the required advances over the state of the art are very challenging and span a broad range of technical domains.

In addition to the technological aspects, MCN plans to identify and evaluate novel business models to support the exploitation of the mobile cloud in multiple diverse multi-stakeholder scenarios. The MCN architecture will be evaluated in realistic scenarios based on a set of concrete use cases and MCN-enabled applications, taking into account the large ecosystem of involved players. Based on the MCN architecture we expect to find a variety of possible business settings with stakeholders in different roles and the work presented in this report will serve as the basis for further investigations in this direction.

MCN Work Package 2 (WP2) is responsible for the definition of scenarios, requirements, business models and the overall architecture. This report is the first WP2 public deliverable and consolidates the results of activities performed in the scope of Task 2.1 (Reference Scenarios and Technical System Requirements Definition) during the first five months of the project. The basic goal of this task is the establishment of a common ground across all MCN work packages, more specifically:

- The definition of a set of reference scenarios and use cases focused on the delivery of advanced mobile cloud services over heterogeneous mobile radio access networks;
- The identification of the basic set of core stakeholders derived from these reference scenarios;
- The specification of technical and non-technical requirements covering both functional and non-functional aspects of the elastic, flexible and scalable MCN network architecture vision, and including the three basic infrastructure domains (wireless access networks, LTE mobile core network, cloud computing platforms), as well as application and service platforms.

The approach towards the definition of stakeholders, use cases and requirements followed best practices in requirements engineering, namely the *Volere* process, as described in Section 3. Definition of general use scenarios was the first activity carried out by Task 2.1. These scenarios came from the different partners in the project, which provide a representative spectrum of experience regarding the covered areas and provided the starting point for the subsequent phases of the work. A list of requirements structured in four technical domains was compiled to provide guidelines to the system architecture design process.

The results included in this report reflect the work carried out in the initial months of the MCN project. As a result of the iterative strategy followed by the project, it is expected that the feedback generated by Work Packages 3-5, as well as by the work on business models and architecture carried out in Tasks 2.2 and 2.3, will make us revisit some of the requirements specified in this document, or even defining new ones, at a later stage of the project.

These results will be used in the next steps of the project in multiple ways:

- Task 2.2 will build on the initial definition of scenarios and stakeholders provided by this deliverable to further develop business models and business roles and investigate the potential economic implications of the MCN architecture.
- By defining a common set of technical requirements and documenting the specific requirements from different technical domains, this deliverable lays the foundation for the architectural work, to be carried out in the scope of Task 2.3.
- MCN technical Work Packages (namely, WP3, WP4 and WP5) will use the requirements defined in this Deliverable as a general guideline for the design and development of new components.
- WP6 will take the reference scenarios defined in this deliverable as candidate scenarios to be validated and demonstrated in testbeds.

1.2 Structure of the Document

Following this introductory section, the remaining part of the document is structured as follows:

- Section 2 provides the basic terminology used throughout this report. Here we will explain the central terms that stem from the *Volere* process as well as the most fundamental technical terms.
- Section 3 describes the methodology followed in Task 2.1 based on the *Volere* process and explains in which respect we deviated from this process and for which reasons. It specifies the role of scenarios, stakeholders and requirements.
- Section 4 describes the main stakeholders involved in the scenarios identified above, their relationships and the relevant use cases. It includes a selection of stakeholders and an explanation for this selection.
- Section 5 presents a set of use scenarios, which intend to illustrate the scope of the MCN project. Each final scenario contains a use story, as well as a brief description of the contribution that MCN is expected to bring.
- Section 6 provides the set of requirements, structured in four technical domains: Cloud Data Centre Infrastructure and Network Programmability, Access Network Infrastructure Cloud, Mobile Core Network Cloud, IMS/OSS/BSS/VAS as a Service.
- Section 7 summarizes the main conclusions and describes the future work.
- In addition, complementary information is provided in four Appendices, including:
    - The detailed specification of requirements identified in Section 6 (Appendix A);
    - The description of Consolidated Scenarios used to derive requirements, as explained in Section 3 (Appendix A);
    - The list of Draft Scenarios that was initially produced in the first step of the requirements specification process (Appendix C);
    - The *Volere* requirements specification template structure, which complements the information provided in Section 3 (Appendix D).

2 Terminology

In the following we will provide the basic terminology that has been agreed within the project and will be used throughout this deliverable and the project. Although we expect the definition of terms to develop in the course of the project we think that it is advantageous to provide an overview in this first technical deliverable. Even if some of the terms described in this section are not yet extensively used in the description we have included them for the sake of consistency and comprehensibility since some of the often used terms implicitly assume other terms even though these are not explicitly mentioned.

The following terminology does not include the Stakeholders since these are separately explained in Section 4.

- Application Services Provider (ASP),
- Cloud Service Provider (CSP),
- Data Centre Infrastructure Provider (DIP),
- Mobile Cloud Network Service Provider (MCNSP).
- Mobile Core Network Provider (MCNP),
- Mobile Network Operator (MNO),
- Mobile Virtual Network Operator (MVNO),
- Network Connectivity Provider (NCP),
- Radio Access Network Provider (RANP),
- Service Broker (SB),
- Support Systems Provider (SSP) and
- Utility Provider (UP).

In the following we will distinguish between more business-related and more technology-oriented terms and handle both in separate sections.

2.1 Terminology Related to Business Aspects

We start the compilation with the terminology that is related to business aspects of the project. Most of these terms refer to the *Volere* process, on which that MCN Requirements Engineering is based (see Section 3) and which we will also follow later on (see Section 6). A detailed description of the *Volere* process can be found in (Robertson & Robertson, 2012).

Activity

An Activity (or more precisely a business activity) describes what an Actor conducts in the course of a Business Process to bring about a service (or a product). User Stories usually consists of a series of Activities performed by different Actors.

An example for an Activity consists in a customer submitting a purchase order on their mobile device, which is part of a Business Process.

Related Terminology: Actor, Business Process, Service, User Story.

Actor

In Unified Modeling Language (UML) an Actor "specifies a role played by a user or any other system that interacts with the subject" (OMG, 2011). Here the subject means the respective scope of business, which might be a service (or product). Due to this interaction an Actor is affected by this subject and this means that in the case that the actor is a person he or she becomes a Stakeholder for it. Actors mainly occur in User Stories.

An example of an actor is an end user, who applies their mobile device to run an application.

Related Terminology: Activity, Stakeholder, User Story.

Business Event

The term Business Event is characteristic for the *Volere* methodology. The underlying assumption is that "any piece of work responds to things that happen outside it" (Robertson & Robertson, 2012). Usually Business Processes are triggered by Business Events and can be part of User Stories.

An example for a Business Event is a customer searching for a product or service using their mobile device and submits a purchase order from it, starting a Business Process that ends with the provision of a product or service.

Related Terminology: Activity, Business Process, User Story.

Business Process

A Business Process can be characterised as "a series of steps designed to produce a product or service." (Rummler & Brache, 1995). The steps in a Business Process can be Activities or automated operations. The steps in a Business Process consist in Activities referring to the tasks that the Actors perform to provide the intended service (or product).

An example for a Business Process is the series of Activities and operations that a Mobile Virtual Network Operator (MVNO) has to perform in order to setup their own MVNO business offering.

Related Terminology: Activity, Actor, Business Event, Business Use Case.

Business Use Case

"For every Business Event, there is a pre-planned response to it, known as a Business Use Case. The Business Use Case is always a collection of identifiable processes (Business Process), data that is retrieved and/or stored, output generated, messages sent, or some combination of these." (Robertson & Robertson, 2012). It is different to a Use Case that only focuses on the interaction of an Actor (user) with an automated system but does not aim at the entire process.

For example the Business Use Case would describe the Business Event that brings an MNVO to extend their service (e.g., an increased number of service requests) and describes what the MNVO and other players have to do to achieve this goal.

Related Terminology: Actor, Business Event, Business Process, Use Case.

End User

An End User is an Actor, who uses a mobile device or other kind of computer to benefit from some service that is offered through this device. The the MCN context we also use the term End User for organisations (Enterprise End User) inasmuch as they use MCN services. The End User also describes a Stakeholder (see Section 3).

Related Terminology: Actor, Service.

Requirement

With respect to service (and product) development a Requirement describes an individual, specifically documented (functional as well as non-functional) need that this service (or product) has to fulfil. The specification of requirements determines the necessary properties, capabilities, and characteristics of this service or product with respect to the value and utility that it has for the users or customers.

The terminology used to describe Requirements is proposed to follow the IEEE Standards Style Manual[1] (IEEE, 2012):

- The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (shall equals is required to). NOTE — The use of the word *must* is deprecated and shall not be used when stating mandatory requirements; *must* is used only to describe unavoidable situations. The use of the word *will* is deprecated and shall not be used when stating mandatory requirements; *will* is only used in statements of fact.
- The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).
- The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).
- The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

Related Terminology: Business Scenario, Scenario, Use Case.

Scenario

A Scenario is a "breakdown of a Business Use Case" into a list of steps, which can be recognised by Stakeholders. (Robertson & Robertson, 2012). While Use Cases aim at the description of the interaction of Actor with automated systems, Scenarios describe the relationship between different Actors from a more general perspective. In this sense we use the term Scenario in a similar way as it is used in *Volere* (Robertson & Robertson, 2012).

An example for a scenario is the football fan who enters the stadium after he had bought the ticket via his mobile device and uses the connectivity that has been additional service included in the ticket purchase.

Related Terminology: Actor, Business Use Case, Stakeholder, Use Case, User Story.

Service

A Service consists in a series of activities that are provided to a customer to increase the customer's level of satisfaction (Turban, et al., 2002). A service can either be provided by one or more persons or by a technical device. In the latter case we call it an automated service.

---

[1] To minimize ambiguity, and following the *Volere* methodology guidelines, it was decided to avoid any forms except "shall" in the requirements specified in this document.

An example for a service is the provided connectivity in the Scenario example that helps the football fan to have access to the internet during the match.

Related Terminology: Activity, Service Provider.

Service Provider

A Service Provider is a company that offers specific Services on the market.

Related Terminology: Service.

Stakeholder

"A stakeholder in an organisation is (by definition) any group or individual who can affect or is affected by the achievement of the organisation's objectives" (Freeman, 1984). These can be Actors in a Use Case as well as entire organisations, which play certain role in a Scenario. Since Freeman's definition of stakeholders is rather broad we will initially restrict it to organisations that contribute to MCN Scenarios by providing certain functional capacities. This is explained in Section 3 in more detail.

An example for a general stakeholder in the domain mobile connectivity is the government that grants the use of certain frequencies to a telecommunication company. In this deliverable we restricted the considerations to potential business stakeholders providing dedicated, mobile cloud services.

Related Terminology: Activity, Actor, Use Case, User Story, Scenario.

Use Case

A Use Case is the description of specific interactions between one or more Actors and technical devices in connection to service (or product) as described in a Scenario.

An example of a use case is the purchase of a good from a mobile device where the application on the device offers a search functionality to the user that allows her to find the desired product, allows her to put it in her purchase basket, and asks her for some security code before charging her credit card.

Related Terminology: Actor, User Story, Scenario, Stakeholder.

User Story

A User Story is a narrative that explains a Scenario from the perspective of an individual (human) Actor. It provides more context than the Scenario, for example about the motivation of the Actor. A User Story assumes hypothical persons and organisations as representatives for Actors and Stakeholders, respectively.

An example is the story that a football fan, whose name is Frank, goes to the football match of his favourite club every week and wants to know about the matches of other teams during his stay using his mobile device.

Related Terminology: Activity, Actor, User Case, Scenario, Stakeholder.

2.2 Terminology Related to Technology

We start the compilation with the terminology that is related to technological aspects of the project. If we use the term Service in this context we usually mean an automated service.

Cloud Computing

We use the term Cloud Computing to indicate that the described computing resources (i.e., hardware and software) are provided as a service over a network independently of the location of the respective resources. In a loose formulation we say that the respective service runs in the *Cloud*.

Related Terms: Infrastructure as a Service, Platform as a Service, Software as a Service.

Core Network (CN)

A Core Network (also called Network Core) describes the central component of a telecommunication network that enables End Users to access Services via the Access Network. This Access Network can be wireless (Radio Access Network, RAN) or wired. In MCN we assume that the Access Network is a RAN.

Related Terminology: Evolved Packet Core, Radio Access Network, End User.

Evolved Packet Core (EPC)

Evolved Packet Core is a central component in 3GPP’s Core Network architecture.

Related Terminology: Core Network.

Evolved Packet Core as a Service (EPCaaS)

This term describes the virtualisation of the Evolved Packet Core as a Service in the Cloud. This service is provided by on-demand deployment of distributed EPC instances on top of an Infrastructure as a Service on data centres.

Related Terminology: Cloud Computing, Evolved Packet Core, Infrastructure as a Service, Software as a Service.

Hybrid Cloud

A Hybrid Cloud is an integrated Cloud based environment in which an organisation utitises both Private and Public Clouds. An organisation can manage onsite resources while employing remote Cloud infrastructure.

Related Terminology: Cloud Computing, Private Cloud, Public Cloud.

Infrastructure as a Services (IaaS)

The term is used in the context of Cloud Computing in relation to Service Providers of an infrastructure in the form of computational capacities including physical or virtual machines as well as other basic resources.

Related Terminology: Cloud Computing, Platform as a Service, Service Provider, Software as a Service.

Platform as a Services (IaaS)

The term is used in the context of Cloud Computing in relation to Service Providers that offer a computing platform, which can include an operating system, a software development environment, a database, and a web server.

Related Terminology: Cloud Computing, Infrastructure as a Service, Service Provider, Software as a Service.

Private Cloud

A Private Cloud is a (cloud) infrastructure that is exclusively operated for one organisation. However, it does not matter if this infrastructure is operated by this organisation or by a third party.

Related Terminology: Cloud Computing, Public Cloud, Hybrid Cloud.

Public Cloud

Applications, storage and other resources that a Service Provider offers to the public, using a cloud paradigm, are called Public Cloud. Known providers of Public Cloud services are Amazon, Microsoft and Google, which run an infrastructure that is accessible through the internet.

Related Terminology: Cloud Computing, Private Cloud, Hybrid Cloud.

Quality of Service (QoS)

Quality of service is a concept that refers to telecommunications and describes the traffic characteristics with respect to specific quality requirements. Such characteristics might include response time or data loss.

Related Terminology: Service Level Agreement.

Radio Access Network (RAN)

This component of the mobile telecommunication system connects mobile devices such as mobile phones or other remotely controlled machines with the corresponding Core Network.

Related Terminology: Core Network, Radio Access Network as a Service.

Radio Access Network as a Service (RANaaS)

Radio Access Network as a Service aims at the flexible on-demand provision of a RAN service based on cloud-based automatic real-time configuration.

Related Terminology: Infrastructure as a Service, Radio Access Network.

Radio Access Technology (RAT)

Radio Access Technology identifies the technology that is used to implement a Radio Access Network.

Related Terminology: Infrastructure as a Service, Radio Access Network.

Radio Resources

By Radio Resources we mean the resources required for mobile telecommunications based on certain standards such as 3G or LTE.

Related Terminology: Radio Access Network, Virtual Radio Resources.

Service Level Agreement (SLA)

A Service Level Agreement serves as part of a legal framework whereby clear roles and responsibilities are defined.

Related Terminology: Cloud Computing, Quality of Service.

Software as a Service (SaaS)

This term refers to a software distribution model whereby applications are offered by a Service Provider over a network, most typically the Internet. The users neither manage infrastructure nor the platform on which these applications are running.

Related Terminology: Cloud Computing, Infrastructure as a Service, Platform as a Service, Service Provider.

Virtual Radio Access Network (VRAN)

A Virtual RAN provides the capacity (data rate) for virtual connectivity through adaptive allocation of Radio Resources from various Radio Access Technologies resource pools by the means of Virtual Radio Resources.

Related Terminology: Radio Access Network, Radio Resources, Virtual Radio Resources, Radio Access Technology.

Virtual Radio Resources

The outcome of virtualisation techniques on the RAN transforms Radio Resources into Virtual Radio Resources. This enables to offer, on the same physical infrastructure (Physical Radio Access Network), isolated, non-transparent and virtual connectivity to virtual networks.

Related Terminology: Radio Resources, Radio Access Network.

3 Methodology

In order to lay systematic foundations for the Requirements Engineering (RE) process in the MCN project we have decided to refer to *Volere* methodology (Robertson & Robertson, 2012). This methodology appears to be particularly suitable for the MCN project since it can be applied to all development methods including agile approaches as foreseen for the project. Moreover, it provided utmost flexibility since it can be used in combination with most requirements tools and modelling approaches. *Volere* has been used for RE for more than 15 years and is based on experience from a variety of projects (for references see, for example, http://www.volere.co.uk/experience.htm). For the purposes of MCN we have taken the fundamental approach and adapted it to the particular needs of the MCN project where we found it necessary.

In particular the template that *Volere* provides for RE can be regarded as particularly useful and were also used as the basis for the templates used in MCN for this purpose. More precisely, we referred to the information categories specified for RE and selected those that were useful for MCN. From this selection we built a new template to be found in Appendix A. Regarding the structure of Section 3 we start with an overview of the *Volere* process and its fundamental ideas in Section 3.1. In the following Section we provide a reflection on the specific requirements of a research project and the description of the resulting adaptations give before we describe the implications of the differences in Section 3.3 in more detail. Here we refer to specific *Volere* elements that we have applied to the MCN RE process and also explain our particular starting point in implementing the *Volere* process and required adaptations. In Section 3.4 we explain how we kicked off the process by defining first draft scenarios and from where we derived consolidated scenarios as well as relevant stakeholders which evolved from those scenarios, which then formed the basis for the definition of an initial set of business use cases. Finally in Section 3.5 we provide an outlook on how we plan to proceed with these results in a more business-oriented analysis.

3.1 Overview of the *Volere* Methodology

The usual goal of the *Volere* process is the identification of requirements in product development, where it is not relevant which particular development method (e.g., waterfall, scrum etc.) is to be applied. The fundamental idea is to derive the requirements from the specific settings in which the intended product has to fit.

3.1.1 Basic Structure of the *Volere* Process

The *Volere* process is essentiall iterative. The usual starting point is the definition of the project. Most of this definition work for the MCN project has been done in the DoW. Nevertheless we start its description from the perspective of *Volere* before we start with the requirements defining steps.

Project Initiation

This starting poinr, which is called *Project Blastoff* in (Robertson & Robertson, 2012, p. 15), provides the definition of the development project to be started and can be seen as the foundation for the following requirements determination. This definition step specifies which aims are to be achieved from the perspectives of the various involved project stakeholders. In particular it determines what is in the scope of the project and what is outside. Usually it is closely related to the economic situations since these specification are defined under consideration of given business problems or opportunities. The discussion of the project initiation should involve all stakeholders, that is, all parties that are affected by the intended development. This is necessary to ensure that all aspects of the development (i.e., technical, economical, societal, ethical etc.) are considered to avoid later surprises.

In particular the project initiation has to ensure that all participating parties are aware of the defined goal goals and agree on them. This prevents the project member to develop the project into different directions, making contradicting assumptions the goal, which leads to tensions and opposing activities.

Individual stages are explained in the following:

Knowledge Built-up

After the initiation it generally becomes necessary to gather all available information to better understand the nature of the intended product. This process step is called *Trawling for Knowledge* in *Volere* (Robertson & Robertson, 2012, p. 17). We can consider the derivation of requirements as a construction process, which must be based on a solid understanding of the underlying conditions as clues. The specification of these clues is the core of the Knowledge Built-up step. *Volere* provides a number of more fine-grained tools to accomplish this. They will be described in the following.

It also includes a better understanding of the project context or of everything that is affected by the introduction of the new product – this is often related to the stakeholders that were already involved in the previous step.

This collection of information results in the construction of a System Model (see Figure 3-1). This System Model is to help understanding which effects the new product will have in its environment and among its stakeholders.

Business Use Cases

Business Use Cases start with Business Events and describe how the effect of the intended product is expected to be in a business setting when a certain external event (Business Event) occurs. For example, it is described how the Mobile Cloud Networking technology could be used to react to an increased demand of mobile connectivity under certain circumstances (e.g., a sports event). Such Business Event starts a Business Process, in which the new technology is to be used. Making such situation more realistic by introducing concrete situations helps us to better understand the possible implications of the new technologies. Descriptions of this kind are called Business Use Cases, the specification of which includes various means such as the development of Scenarios or User Stories; in Section 0 we will explain in more detail how we apply these tools.

The general goal of this step is the Product Design (see Figure 3-1), in which we develop an idea how the product will be used in a future business context. Furthermore, this step gives us an idea what the product could look like as the basis for the following product construction.

Prototype Development

Although this step is beyond the focus of the development described in the report we want to explain it in some detail as the next step in the *Volere* process. Based on the Product Design sketched before, the actual construction of the product starts including the actual technical development steps (Product Construction in Figure 3-1). In this step it becomes clear whether the intended Business Use Cases can actually be realised, that is, whether we encompass the technical means to implement solutions that can be used to realise them.

In particular in project with extended research phases the first step of Production Construction is usually the development of a prototype. In the case of a research project such as the MCN project we will mainly conclude the project with a prototype (see Section 3.2 for the particular consequences). Nevertheless any kind of solution whether commercial or prototypical will give us feedback about the product and its requirements and might lead to adaptations regarding the latter.

Protoypte Use and Evolution

The final test whether the assumption made regarding de definition of the Business Use Cases were correct can only be obtained from the actual usage of the final product. After a careful development according to the previous steps the use of the product might provide unexpected results, for example, that users apply the product in a different way as originally intended, however, in any case it should avoid that the product is completely incompatible with the user's intentions and wishes.

3.1.2 Reference to the Method Manual

As already indicated in Figure 3-1 the specification of requirements is an on-going process in *Volere* that even involves the final steps of product use. The consequence for every project is that the requirements engineering process is never completely accomplished. Of course this also holds for the MCN project. Beyond these general characteristics of the RE process in general and the *Volere* process in particular – that is rather a lifecycle than a proper process with a clear beginning and an end – we have to deal with the special circumstances of a research project. What this means will be described in the following section.

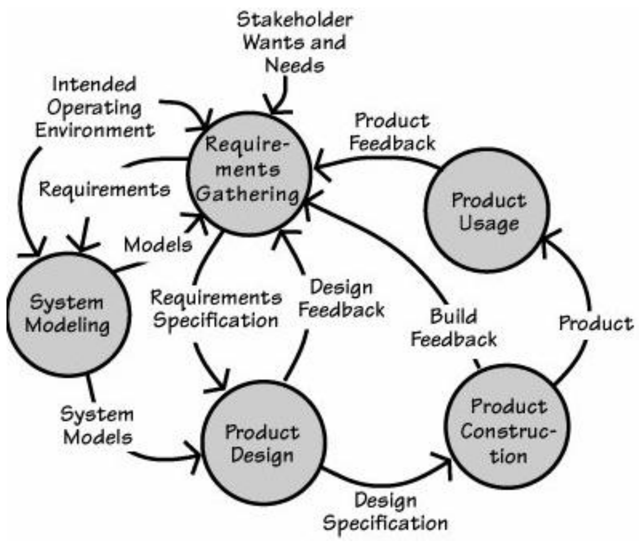

Figure 3-1 Iterative requirements engineering approach - extracted from (Robertson & Robertson, 2006)

The complete *Volere* methodology is described in detail in the book "Mastering The Requirements Process", (Robertson & Robertson, 2006) and (Robertson & Robertson, 2012). This report will only provide excerpts of relevant passages of this book as far as we need them to explain or illustrate how we have applied the suggested templates and structures, and show which MCN-specific adaptions were required. For further details of the *Volere* methodology we refer the reader to this book.

An essential element of *Volere* is the suggested requirements specification template. The structure of this template is provided in Appendix Appendix D.

3.2 Nature and Specific Needs of the MCN Project

Regarding the RE process, we have to bear in mind that MCN is a research project, which aims at disruptive business development by exploring novel technical opportunities that we except to result from the combination of mobile networking and cloud technologies. Due to this setting we do not only have to deal with the fact that the later stages of the requirements specification process (Product Construction and Use in Figure 3-1) cannot yet included in the requirements definition but that also the System Modelling is rather speculative and requires more analysis. We will provide this analysis in the next months of the project and are in a much too early stage to provide reliable information now. Nevertheless, according to the project plan we have started the initial definition of requirements based on the Product Design phase including an analysis of Business Use Cases by scenarios. Otherwise it would not be possible to start the technological research that is required for the realisation of the project now. Although scenarios are provided we should not forget, however, that a thorough analysis of the business context is only due for the upcoming deliverable D2.3 and requires additional work.

Another reason why we could not start with the System Modelling was the fact that the stakeholder identification takes some time and will not be accomplished at this early stage. As we will see in Section 4 we have to deal with a number of potential stakeholders – several do not yet exist at all – that have to be analysed (and/or constructed) in future research. Also here we come to limits regarding the System Modelling.

Due to this "technology-push" nature of the project we started the evaluation of technology-driven scenarios (see Section 0) to provide the input for the technical work packages and scope the future ground for new market solutions first as part of the System Modelling. In fact, the *Volere* methodology gives its users some flexibility in the handling and allows them to start with other stages than the System Modelling if necessary.

3.3 Application of the *Volere* Methodology to MCN

Figure 3-1 displays the elements used for covering and documenting the first phase of the MCN project, which is reflected in this report. It has started with the definition of scenarios and requirements as part of the definition of Business Use Cases and the results are presented in Section 5. It shows the iterative character of the process that oscillates between the explorations of technological feasibility and business requirements and reveals 3 layers:

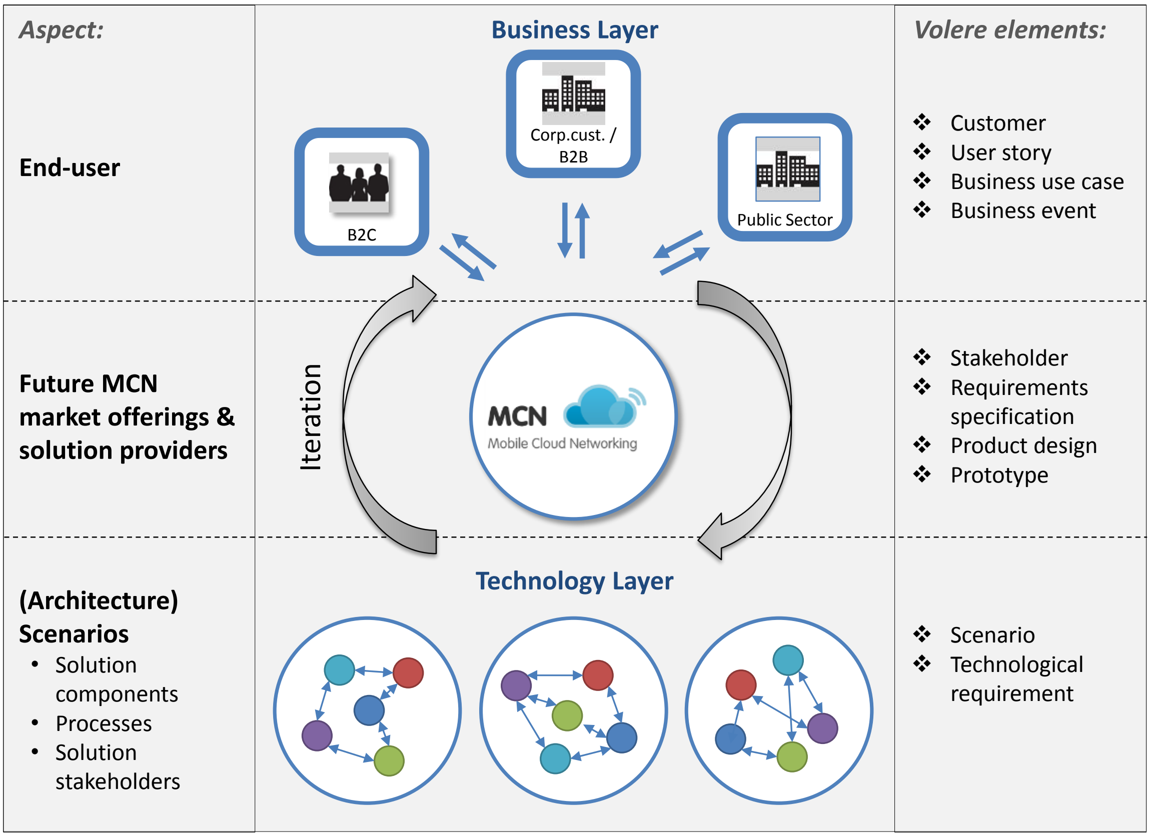

Figure 3-2 MCN requirements engineering approach and link to *Volere* method elements

The first (business) layer (in Figure 3-2 on top) stands for the business context of the product. It requires a thorough understanding of the end-users and their needs as well as of the market players. The second (technology) layer (in Figure 3-2 at the bottom) describes the technical opportunities. These are reflected in the scenario that this deliverables provides. However, as mentioned in the last section these still lack a thorough analysis of the market players. We need these scenarios for the product design and construction but should overemphasise their importance until we have complemented them by a business analysis. The third or middle layer represents the iterative RE process as defined by *Volere* that oscillates between technology-based scenarios and external business demands. In addition, the left hand side of the diagram shows the concepts of the respective layer as we have used them in the first phase of our analysis while the right hand side corresponds to the respective *Volere* elements. The entire process is described in Section 0.

For a definition of the relevant terms for the RE process as displayed in the section on the right hand side of Figure 3-2, please refer to Section 2 Terminology.

3.4 Scenario Analysis Approach

3.4.1 General Process Outline

For the scenario analysis we have applied the following step-by-step approach, as displayed in Figure 3-3:

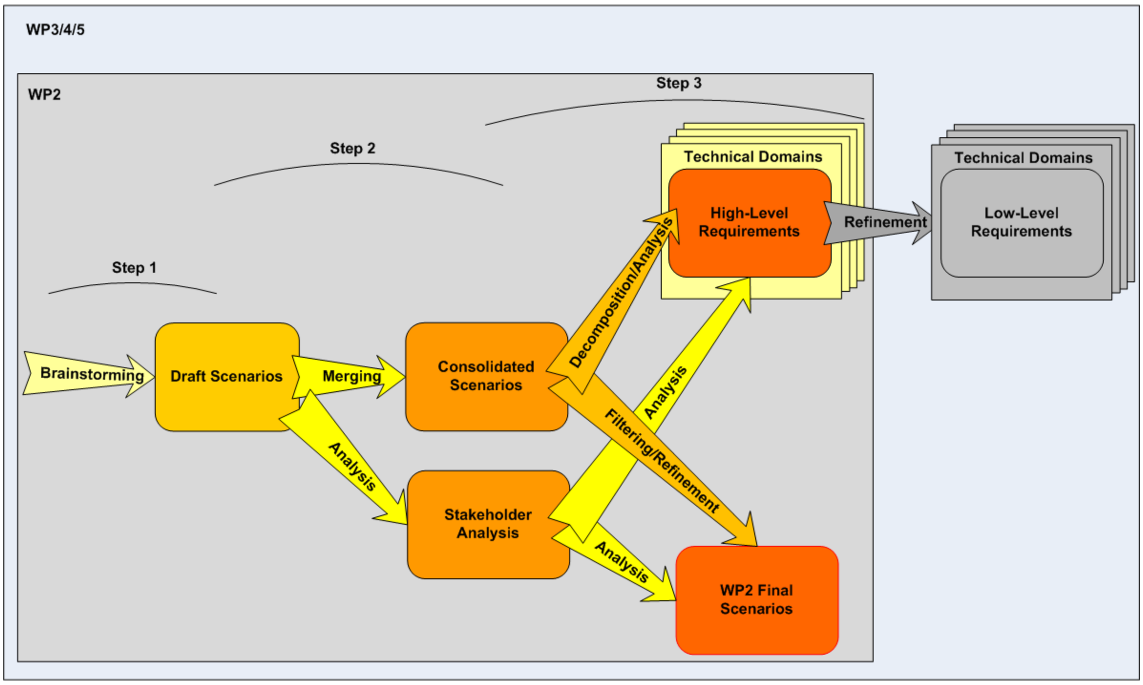

Figure 3-3 Scenario analysis approach

The individual steps in Figure 3-3 are explained in the following paragraphs:

- **Step 1**:

As a first step, all scenarios and use cases proposed by the partners were collected in a brainstorming process. Here, the partners contributed according to their long experience in their respective core domains that cover the relevant markets. The result was a set of **Draft Scenarios**, eventually with many overlapping features and similar functionalities.

- **Step 2**:

In the following we merged these **Draft Scenarios**, in order to obtain a smaller number of **Consolidated Scenarios**, which combines the description of the Draft Scenarios and possesses more distinct features. Furthermore, we determined a set of **Technical Domains** that helped us to focus on specific technical aspects. Hereby the analysis illuminated each scenario from the perspective of every relevant Technical Domain. This ensures completeness with respect to each Technical Domain. At the same time, we performed a **Stakeholder Analysis** with the goal to go beyond mere technical description and to start including business aspects.

- **Step 3**:

Then we deconstructed the **Consolidated Scenarios** in order to derive a set of **Use Cases** per **Technical Domain**. **Use Cases** are providing a clearer specification of the interactions in a given Technical Domain, which comprise a limited and meaningful subset of the Technical Domain features. From the analysis and decomposition of the **Use Cases** we finally derived the **Requirements**. In WP2, only high level **Requirements** will be considered. In addition, based on the **Use Cases** (**Composition**) and the **Stakeholder Analysis**, a small set of **WP2 Final Scenarios** was built (see Section 5). The purpose of these Final Scenarios is to exemplify the major features and capabilities of the overall environment.

- **Step 4**:

Later on and after defining **Use Cases** and high level **Requirements** (under the WP2 scope), we will start an iterative **Refinement** process in order to drill down these high-level **Requirements** into more specific and detailed **Requirements**. This work will be performed in WPs 3/4/5 before starting the implementation.

It has to be emphasized that the full set of features and capabilities will be considered and specified under the WP2 scope, by defining Use Cases and Requirements, as well as representative scenarios. However, WPs 3/4/5 are not expected to take all possible features, capabilities and WP2 requirements into account, but only part of them, according to the project interest. The same rationale applies to the demonstration scenarios that will be defined under the scope of WP6.

3.4.2 Definition of Scenarios

As described in the previous section, the requirements specification process was started by defining a set of Draft Scenarios (DSs). These are listed in Appendix Appendix C. These draft scenarios were later classified, grouped and condensed into 10 Consolidated Scenarios (CSs), listed in Table 3-1 and described in Appendix Appendix B. The mapping of the Draft Scenarios into Consolidated Scenarios is presented in Appendix Appendix C.

Table 3-1 Consolidated Scenarios.

	Title
CS01	RAN on Demand
CS02	Mobile Virtual Resources on Demand
CS03	Machine Type Communication on Demand
CS04	Software-Defined Networking
CS05	Energy saving & fast network reconfiguration
CS06	Scaling the capacity of a virtualized Evolved Packet Core
CS07	Follow-Me cloud & Smart content location
CS08	Digital Signage
CS09	Operational Management & Charging as a Service
CS10	End-to-End Cloud

Also, based on this set of scenarios, a set of Technical Domains (TDs) was defined, and this was later the basis to derive and organize requirements. This set of TDs is thought to cover the key technical areas covered by the MCN project. The list of TDs as follows:

A. Cloud Data Centre Infrastructure and Network Programmability

B. Access Network Infrastructure Cloud

C. Mobile Core Network Cloud

D. IMS/OSS/BSS/VAS as a Service.

3.5 Outlook to Further Work

We have shown how the chosen approach for the identification of requirements is rooted in the *Volere* RE process. Its concentration on the technical feasibility, which has been necessary at the current stage of the process but has to be enlarged in the future, provides a valid starting point for the technical research. The next obvious steps consist in the elaboration of the business-oriented System Modeling that provides the bases for further requirements refinement and opens up opportunities for the identification of new business opportunities.

This will be done in the following phasis of the project that aim at a market and business analysis as part of Task 2.2 in WP2. Here we will incorporate the next steps in the iterative process as described above. As already indicated in Figure 3-1 the respective findings and conclusions from this analysis will be fed back into the requirements engineering process. This will lead to a continuous development of the requirements which have to be checked with respect to this feedback. We do not expect fundamental changes in the technical approach, however, previous discussion have shown that certain details cannot be decided on a merely technical basis, for example, the specific ways of integrating mobile network or cloud technologies, which definitely have to respond to business requirements.

Finally, the work in Task 2.2 will not only lead to an assessment of the developed technology but is also expected to pioneer new business models and in particular business networks, which will be based on the stakeholder analysis that we have started in the following section.

4 Stakeholder Analysis

As discussed in (Robertson & Robertson, 2012), stakeholders play an important role in the *Volere* process of requirements engineering. Here the central insight is that these requirements are fundamentally influenced by the stakeholders' needs. Before we introduce these stakeholders that we regard as particular relevant for the MCN project we first want to clarify how we have actually gone about the stakeholder analysis. Defining the eventual goal of this analysis, we primarily referred to Freeman's stakeholder definition (Freeman, 1984):

> A stakeholder in an organisation is (by definition) any group or individual who can affect or is affected by the achievement of the organisation's objectives.

The main purpose of a stakeholder analysis according to (Freeman, 1984) has been related to the problem of value creation and exchange. The underlying assumption is that analysing the relationship between a business and its stakeholders helps us find out about business opportunities and restrictions, in particular with respect to such innovative technologies as developed in the MCN project, where we cannot yet refer to actual experience. However, it has been observed that this definition is quite broad (Mitchell, et al., 1997), so that its analysis requires some time and poses the question where we should start in a business setting that is so far more imaginative than real.

For this reason we will start our stakeholder consideration with the technological stakes on which the overall architecture of the MCN project is build, as it becomes obvious from the scenario analysis, which we performed. The potential holders of these technological stakes interact with each other (see Figure 4-1 Joint Stakeholder View) and to understand their mutual dependencies is crucial for the later investigation of business opportunities. This does not mean that for a complete stakeholder analysis it is not necessary to go beyond the mere technical description and setting the socio-technical environment aside; it only means that we take the mentioned stakes as starting point for our investigation to understand the basic dependencies. Consequently the current identification only provide a preliminary insight into the stakeholder landscape that we will enlarge in the future where it appears to be necessary. Talking at this stage about stakeholders instead of considering technical components only has the intention to already open up our horizon towards business and social factors, which will definitely influence the MCN technology. Initially, however, we will primarily focus on those stakeholders in the MCN setting who determine the business impact of the solution to be provided. However, we will also look at stakeholders beyond the business realm if these are relevant. This corresponds to previous discussions of stakeholder analysis, which has been tied to enterprise strategy (Freeman, 1984). It mainly concerns the questions what a provider of some technology stands for. Freeman has already discussed the separation of stakeholder analysis regarding the question whether "the discourse of business and the discourse of ethics can be separated" (Freeman 1994 in Freeman et al., 2010) even though the thesis has been criticised. Albeit we regard it as a kind of working hypothesis for the moment that we take as a starting point.

Another problem that we currently face is the link between technical components and (potential) stakeholders. The assumption is that each technical component identified within MCN could in principle be offered by a respective stakeholder. Which technical components are actually suitable for such commercialisation will be the subject of further investigation in Task 2.2. Nevertheless we already took the discussion of use scenarios and requirements for a preliminary identification of potential stakeholders whose possible role will be the subject of further analysis. Starting from such technology-centred perspective we first of all refer to the technical component to identify related stakeholders, inasmuch as they "affect or are affected" by this technology and the organisational entity that develops or runs it.

As introduction to the stakeholder identification we give an overview of the initially identified potential stakeholders. In this section we are mainly focused on functional roles, independently of which business entities play those roles in practice. This means that there might be a one-to-one mapping between stakeholders and business entities, but it might be also the case that the role of multiple stakeholders is played by a single business entity (e.g. the MVNO, to be described in Section 5.1). Different combinations are expected to lead to a rich set of business models, which will be further explored by Task 2.2.

The central stakeholder in the MCN stakeholder analysis is the consumer in the role of an **End User (EU)**. The EU can take the form of an **Individual End User (IEU) -** here we can imagine a person, who possesses a SIM card for her mobile device and makes use of the offering of a service provider; alternatively it can take the form of an **Enterprise End User (EEU)**, which in turn makes use of the MCN services to compose new services and offer these to end users. A typical example of an EEU is a **Utility Provider (UP)**, which offers supplementary utility services by making use of MTC-enabled connectivity via mobile services.

The **Mobile Cloud Network Service Provider (MCNSP)** manages the End User (either IEU or EEU) subscription and appears as provider of the MCN services. In addition, the MCNSP integrates the service components required to build Mobile Cloud Network services to the EU. In summary, the MCNSP includes two basic functions:

1. Integration of the different components required to build the service (radio access network, mobile core, support systems, etc.). These components are provided by stakeholders such as the Radio Access Network Provider (RANP), the Mobile Core Network Provider (MCNP), who could be separate different players, or belong to the same business entity.
2. Handling the final subscription with the end user. Although this is a purely commercial function, it is essential to define the role of the MVNO as a business entity, as will be discussed in the Section 5.1.

In order to be able to offer these mobile services the MCNSP relies on other stakeholders, four of them will be described in the following.

First, the **Radio Access Network Provider (RANP)** is a stakeholder, who represents the entity that provides Radio Access Network (RAN) services to the MCNSP. The RAN functional block provides a spectrum of licensed as well as unlicensed radio resources, which include the Base Station/Access Point functions from given systems (e.g., GSM, UMTS, LTE E-NodeB and WiFi), the controllers of the resources and associated capacity, as well as the backhaul links between them and to some “external” point. The RANP relies on a Cloud Service Provider (CSP) to process information and data.

Second, the **Mobile Core Network Provider (MCNP)** represents a stakeholder, who offers Mobile Core (EPC) services (in the "as a Service" model) to the MCNSP. The Mobile Core functional block includes all EPC components (e.g. MME, PGW, SGW, etc.). The MCNP components run of top of infrastructural resources (IaaS), which are also provided by a Cloud Service Provider (CSP). Any connections, which are required to interconnect the Mobile Core with the RAN or to access the Internet, can be provided by a Network Connectivity Provider (NCP), which we describe later.

Third, the **Support Systems Provider (SSP)** stands for a stakeholder, who offers Operational/Business Support Systems (OSS/BSS) that support the technical as well as the business operations MCNSP. The respective systems are again provided in the "as as Service" model. The Support Systems functional block contains central OSS such as Monitoring and Provisioning services as well as BSS such as Charging, and CRM services. Also the components offered by the SSP run of top of infrastructural resources (IaaS) provided by a Cloud Service Provider (CSP). Any links required to interconnect the Support Systems with the Mobile Core (EPC), the RAN or the MCNSP premises can be also here provided by a Network Connectivity Provider (NCP).

Fourth, the **Application Services Provider (ASP)** describes a stakeholder that offers Application Services (VAS, SaaS, etc.) either directly to the EU or to the MCNSP, which in turn will provide them to the EU. The business relationship between the ASP and the MCNSP depends on the particular type of application service and business model; either the ASP has a contract with the EU or it is the MCNSP who has this contract. In any case it services are made available through the "as as Service" model. ASP applications run of top of infrastructural resources (IaaS/PaaS) provided by Cloud Service Provider (CSP). Also here, any links required interconnecting the Application Services with the Mobile Core (EPC) or the MCNSP premises can be provided by a Network Connectivity Provider (NCP).

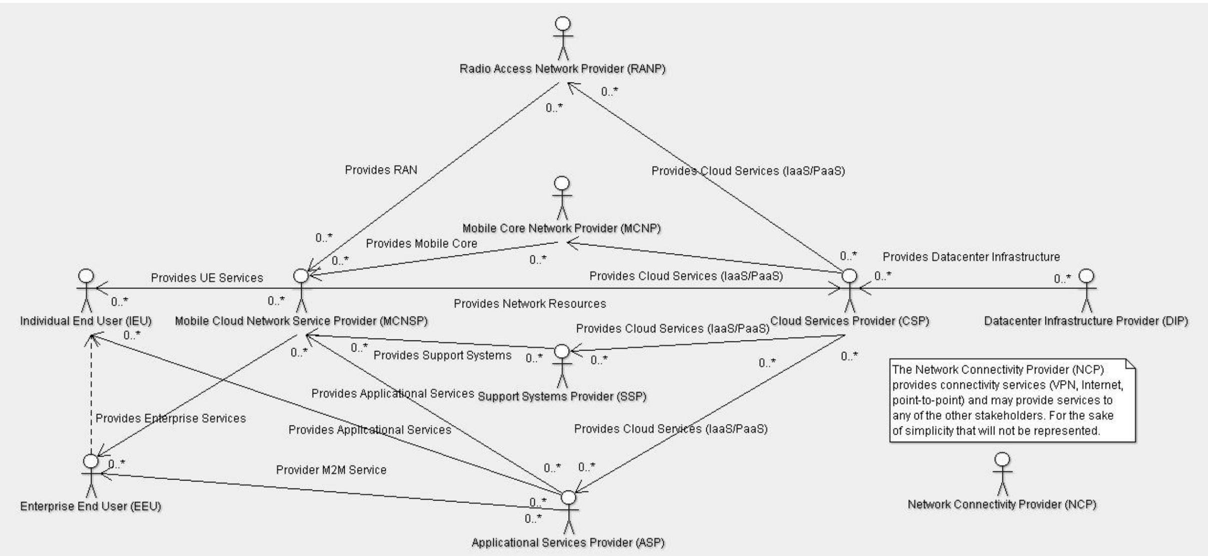

Figure 4-1 Joint Stakeholder View

These four (potential) stakeholders represent the central players in future offering of MCN services. Whether they will appear as independent market actors or whether some of the stakeholder roles are to be merged forming new stakeholders will be subject of further investigation in Task 2.2. In addition, we have already mentioned to other stakeholders that might work together with these 4 providers. We will describe them in the following:

The **Cloud Service Provider (CSP)** is a stakeholder that we already find as successful player in today’s markets (Buyyaa, et al., 2009). CSPs provide virtual infrastructural services based on cloud technologies (e.g., Hypervisors, OpenStack, etc.) to functional block providers such as RANPs, MCNPs, SSPs and ASPs. The virtual resources that they offer support features such as flexibility, on-demand availability, follow-me and other cloud-related features. The CSP does not necessarily own Data Centre infrastructure, so it often needs to contract a Data Centre Infrastructure Provider (DIP).

Any links required to interconnect to its customers can be provided by a Network Connectivity Provider (NCP).

The **Data Centre Infrastructure Provider (DIP)** is a stakeholder that provides Data Centre infrastructure (physical/hardware/network) to the CSPs, which enables the latter to offer a virtual infrastructure to its customers. Again, any links required to interconnect different locations (e.g. Data Centres) can be provided by a Network Connectivity Provider (NCP).

Both the DIP and the CSP can make use of hardware and software offered by the **Cloud Product Provider (CPP)** (not represented in Figure 4-1).

Finally we come to the **Network Connectivity Provider (NCP)** as a stakeholder, which can potentially support any other stakeholder. The links provided by the NCP are typically point-to-point, VPNs, or Internet access. This stakeholder is an abstraction that fills the connectivity gap between two or more geographical points, which require interconnection. This stakeholder allows for splitting up into more fine-grained stakeholder roles, however, considering that this is not the focus of the project, we only assume one NCP for our purposes. The Network Connectivity provider could in turn make use of physical network resources provided by the **Network Infrastructure Provider (NIP)** (not represented in Figure 4-1).

An already established stakeholder that we have not explicitly considered in the previous overview is the Mobile Virtual Network Operator (MVNO), which provides mobile communication services without owning a mobile network infrastructure. This means that in order to provide the respective services an MVNO has to work together with a Mobile Network Operator (MNO) which provides the required infrastructure. A discussion of the relationship between MVNOs and MNOs can be found in (Copeland, 2011). For a discussion of the particular role of MVNOs and MNOs in a concrete scenario, please refer to Section 5.1.3.

It is to be remarked that the relationships between the different stakeholders as depicted in Figure 4-1 are obviously not one-to-one but can actually be multiple, increasing the flexibility in the business network. As a consequence the additional stakeholder role of a **Service Broker** might come into play, however, this is due to further investigation. We only want to emphasise that the described relationships cannot be considered as final in this respect. This also holds for the relationships as such. For example, it might occur that it is not only a MCNSP who makes use of the services offered by an ASP but also vice versa, that is, that ASPs incorporate MCN services in their offerings. Here we additionally see that the distinction between UPs and ASPs is not as strict as Figure 4-1 might suggest. This might also include **Platform Providers**, who might also additionally enter the market as Service Brokers.

As mentioned in the beginning this overview only provides a rough sketch of possible stakeholder constellations, which have to the considered in the future. The following investigation has to define the relationships between these stakeholders in more details as well as the relationships to stakeholders outside this network described in Figure 4-1. In the centre of this investigation will be the possible value propositions of these stakeholders towards each other. However, due to the limited timeframe and the focus on technical requirements it has not been possible to provide such analysis. Nevertheless the stakeholder analysis already opens up an insight into potential business networks which are the final prospect of the MCN project.

5 MCN Scenarios

This section contains a limited set of final scenarios. These final scenarios can be seen as the minimum set of scenarios thought to cover the full scope of the MCN project. They can be seen as a refinement (and a reduced set) of the Consolidated Scenarios, described on section 3. Each final scenarios contains a use story and describes the contribution that MCN is expected to bring to make this scenario possible.

5.1 Cloud-Enabled MVNO

5.1.1 General Background

Mobile Virtual Network Operators (MVNOs) are an important player in the mobile telecommunication industry (voice and data). The number of MVNOs has reached very high numbers and is still steadily rising.

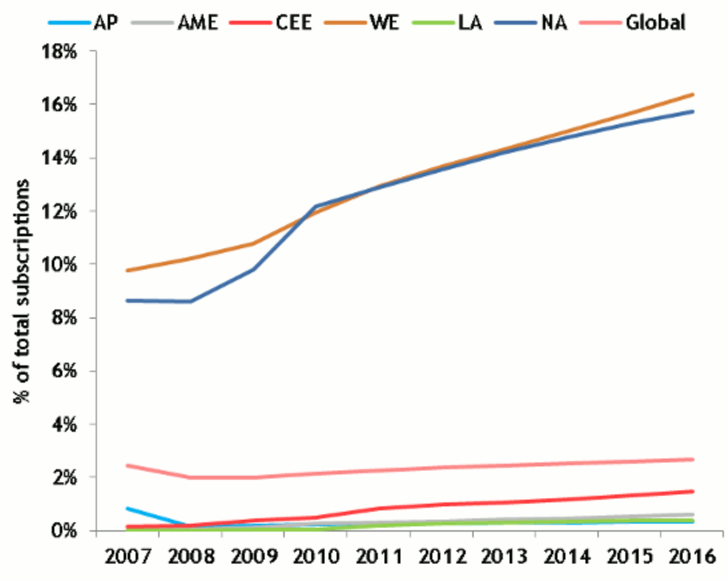

Figure 5-1 MVNO Market Forecast (2007-2016) as a percentage of total mobile subscribers per region (Pyramid Research, 2012)

As shown in Figure 5-1, the number of subscribers per MVNO is expected to keep increasing in the coming years, in particular in the Western European (line WE in the graph above) and North American (line NA in the graph above) markets (Ayvazian, 2012).

MVNOs need to perform different functions that can either be handled in-house by the MVNO itself or outsourced to a Mobile Network Operator (MNO), meaning that MVNOS can adopt different operating models. This combination of different functions varies from simply reselling communication services to the full range of function of an MNO, except the RAN.

Figure 5-2 (Copeland, 2011) shows the range of MVNO operating models. The relationship with MCN stakeholders will be discussed in Section 0.

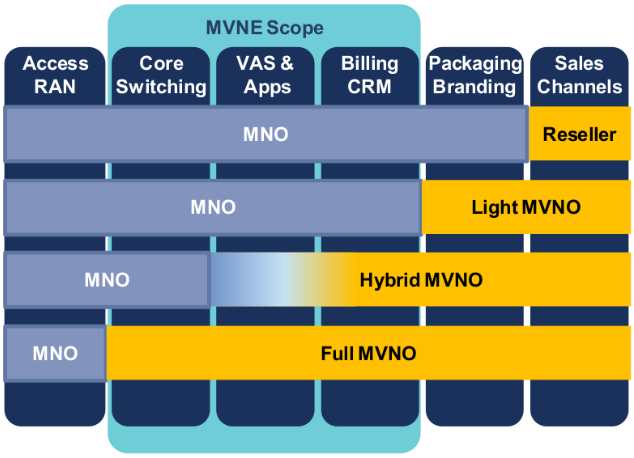

Figure 5-2 MVNO business models (Copeland, 2011)

When an MVNO operates under the light MVNO model only does packaging/branding and relies completely on the Mobile Virtual Network Enabler (MVNE) to provide all required functions. This model is sometimes considered not an MVNO at all.

The hybrid model gives MVNO more flexibility on what equipment and/or service is self-managed by the MVNO and what is hosted by the MNO. Hybrid MVNOs relies on the MVNE to provide at least the Core Switching and Radio Access functionalities, while they own or manage themselves other functions (OSS/BSS, VAS).

Full MVNOs operate in a similar way as the MNOs, i.e. the MVNO runs everything except the spectrum license and the wireless infrastructure. Full MVNOs have the ability to respond to market request, e.g. adding new applications or services, at their own pace, without depending on the MNO. Under this model the MVNO distributes its own SIM cards and manages its subscribers with no intervention from the MNO, allowing the MVNO to maintain control over the user data. Full MVNOs can keep their business information private from the MNO by generating their own charging data records (CDRs) and bill in-house, instead of relying on the MNO's billing records.

An extension of the classic MVNO model is the Multi-MNO model (Copeland, 2011), where the MVNO splits the outsourced services into different functions, e.g. Packet Switching, Content Provider - and sources each function from a different MNO. In this model the MVNO can then utilize its own capabilities and resources and complement them with the best offer available in each area.

In the Multi-MNO model the MVNO signs agreements with several MNOs, but assign each subscriber to only one MNO. Although Multi-MNO MVNOs are able to obtain competitive network charges, the volume discounts decrease since users' traffic is spread across several MNO networks. This model is particular attractive for Light or Hybrid MVNOs wanting to leverage their position as a service brokers to multiple MNOs and create relationships with third party services and content providers.

A further extension of the Multi-MNO model is the 'Always Best Connected' (ABC) model. The idea behind the ABC model resembles the Least-Cost-Routing (LCR) concept in legacy networks, where calls are routed to the network with the lowest associated cost based on time and destination. The ABC model allows MVNOs to choose the best MNO to connect to for each connection, not just each user as in the Multi-MNO model. This can bring to further costs reduction – see (Copeland, 2011) and (Ponce de Leon & Adhikari, 2010).

As mentioned in (Copeland, 2011), both the Multi-MNO model and the ABC model present both technical issues and implementation complexity.

5.1.2 User Story

The Summer Olympics are about to start in Italy and hundreds of thousands of fans are flying in from all over the world. Most of these visitors are expected to stay in Italy for a couple of weeks, or even longer, to support their favourite athletes and also enjoy the lovely Italian food and architecture.

During this time, the Irish airline Shamrock Airlines decides to offer to all its passengers flying to Italy a mobile service, to be able to make calls and surf without incurring into high international roaming charges. Shamrock Airlines doesn't own any infrastructure, but can rely on their own marketing and distribution channels, therefore signs an agreement with one of the main Italian mobile operators, Operator A, to use their mobile network infrastructure, i.e. RAN, Core Switching, OSS/BSS – and therefore being able to operate under the Light MVNO model.

At the same time, given the high number of its existing customers travelling to Italy, a Swiss mobile operator, SwissMobile, strikes a deal with Italian mobile operators Operator A and Operator B to use their access networks (RANs) to offer its customers attractive tariffs to make calls during their stay in Italy. SwissMobile will operate under the Full MVNO ABC model, meaning that it will still retain full control over its customers' data and still operate the network up to the Radio Access point. Also, SwissMobile will be able to choose whether to use Operator A or Operator B Radio Access resources on a per connection basis, depending, e.g., on the used service or location of the subscriber.Shamrock Airlines can tap into this new business opportunity without incurring into high initial investment and without the need to know in advance how many users will take advantage of this new service, as the whole network infrastructure provided by Operator A will be instantiated on-demand. Also, as the request from its customers increases, Shamrock Airlines can ask for more resources from Operator A, which will allocate them dynamically, giving Shamrock Airlines the flexibility it requires.

SwissMobile can easily extend its coverage into a new region without any initial investment or planning. Also, given the on-demand-based agreement with both Italian operators (Multi-MNO model), SwissMobile has the flexibility to dynamically choose the best operator for each connection and is able to keep operational costs down. SwissMobile is also able to add more capacity in a new area on demand as it is needed, and quickly. SwissMobile gets services from both Operator A and operator B via a self-service interface where they supply their billing details. SwissMobile can either use the web user interface or programmatic interface of one of the operators to create an instance of the required services.

Operator A is able to cope with the increased traffic thanks to its cloud-based approach. When additional resources are required Operator A can dynamically instantiate them, and remove them once they are not needed anymore. Upon receiving requests from Shamrock Airlines and SwissMobile, Operator A understands the various components that need to be created to offer the type of service required. For example, Operator A needs to create RAN, EPC and IMS related components, including OSS and BSS elements for Shamrock Airlines, while SwissMobile will only require the Radio Access Nework services. Once these components are created, Operator A needs to suitably configure them so that the end-to-end service is ready for use by Shamrock Airlines and SwissMobile.

5.1.3 Stakeholders

The main stakeholder from an overall perspective is the Cloud-enabled MVNO. However, the MVNO is a particular business entity and thus no stakeholder as they are defined herein. In fact, the exact representation is a very interesting case as it depends and varies with the specific MVNO type.

A **Reseller** or **Light MVNO** (see Figure 5-3) is mostly a consumer, it doesn't consider infrastructure ownership nor operation as a strategic aspect for its business. This type is thus the equivalent of the **Enterprise End User (EEU)**. The Light MVNO provides the classical set of mobile telco services to the End User (EU), most commonly voice, text, data, and to some extent VAS. What the Light MVNO cares for the most is the customer relationship, which it keeps ownership of and maintains the relationship; recall the Enterprise End User is the entity handling the final subscription with the **Individual End User** and so does the Light MVNO. For anything else, in particular the infrastructure ownership and operation it contracts respective providers and consumers respective services.

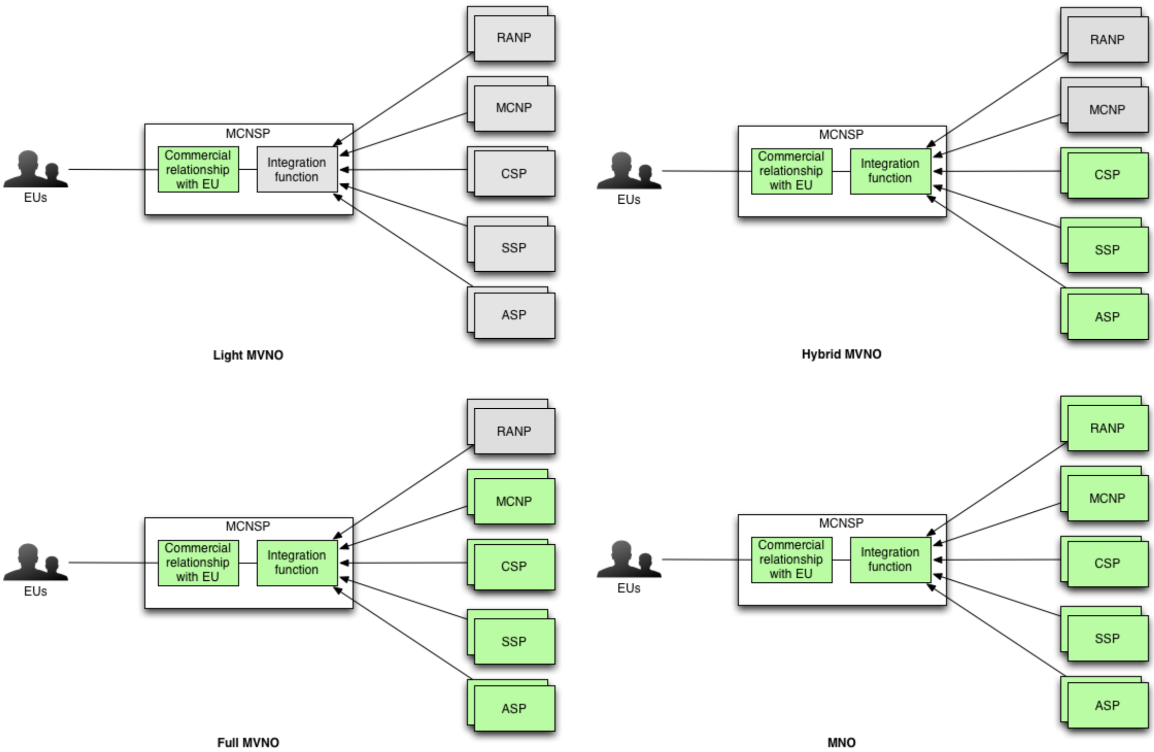

Figure 5-3 MVNO/MNO variants and respective stakeholder roles

In our cloud-based context, the **Mobile Cloud Network Service Provider (MCNSP)** will take a mediating role. In this scenario the MCNSP can be seen purely as an integrator, combining the different components required to build the service and the functions provided by the **Radio Access Network Provider (RANP)**, the **Mobile Core Network Provider (MCNP)**, the **Support Systems Provider (SSP)**, the **Application Services Provider (ASP)** and the **Cloud Services Provider (CSP)**.

The **Hybrid** and **Full MVNO** are entirely different case. These two types do indeed consider infrastructure, platform, application, and ultimately service ownership strategically important and do operate them, with different technical perimeter. This indeed means that these two types of MVNOs may incorporate several roles:

- **EEU** since they maintain the business relationship with the IEE,

- **MCNSP** since they do orchestrate/integrate the various pieces
- **MCNP** (Full MVNO), SSP (Hybrid and Full MVNO), ASP (Hybrid and Full MVNO)

Although these two functions, i.e. integration and customer management, have traditionally been played by the same business entity (usually referred to as the MNO), the possibility to decouple them in two independent actors paves the way to the emergence of the Cloud-enabled MVNO. In the minimal scenario, the role of the Cloud-enabled MVNO is limited to a purely business function (Reseller, Light MVNO, as defined in Section 5.1.1, Figure 5), but it can also include other functions. Figure 5-3 below illustrates the multiple variations of the MVNO, according to the stakeholder roles that it accommodates. A detailed description of the EEU, the MCNSP and other relevant stakeholders is provided in section 4.

This scenario brings the following benefits to the MVNO:

- Reduced initial investment (CAPEX) and operational costs (OPEX) thanks to the on-demand allocation of resources.
- Lowered risks related to planning, thanks to service elasticity and scalability.
- Expand into new markets and regions and explore new business opportunities.

5.1.4 MCN Contribution and Innovations

The main contribution from the MCN project will be to enable the Cloud Computing principles, i.e. on-demand, elasticity, pay-as-you-go – for all technology domains and for all MVNO models (Light, Hybrid, Full MVNO). From a technology perspective this means:

- Cloud-enabled Radio Access Network (RAN) (in MCN referred to as Wireless Cloud);
- Cloud-enabled Mobile Core, i.e. Elastic EPC/EPCaaS;
- Cloud-enabled IMS (IMSaaS);
- Cloud-enabled management in the Operation Support System (OSS);
- Cloud-enabled Rating, Charging, Billing and SLA management in the Business Support System (BSS).

Today, MVNOs faces high investment (CAPEX) into systems and significant operational costs (OPEX). Also, by committing to comprehensive wholesale agreements, that includes determine in advance the number of users they would like to serve and fixing the region where they will offer their services, current MVNOs undertake high risk and operate with limited flexibility.

Thanks to the elasticity, on-demand and pay-as-you-go Cloud Computing principles the Cloud-enabled MVNO will be able to take advantage of a lower investment (CAPEX) into systems, depending on the MVNO model – Light, Hybrid or Full, and also lower operational costs (OPEX). The Cloud-enabled MVNO will be more flexible thanks to on-demand-based wholesale agreements and elastic service availability and scalability. Moreover, new business opportunities will open to the Cloud-enabled MVNO in terms of extending its coverage and tapping into new markets. The MobileCloud Networking project will also address the issues with the implementation complexity of the Multi-MNO and ABC models.

Note: the actual service provided by a Cloud-enabled MVNO is exactly the same as a classical one – voice, text, data. Besides running on top of a cloud foundation it uses standard / classical mobile Telco systems.

5.1.5 Challenges

The following technical challenges will have to be addressed to enable this scenario:

- MVNOs rely on the Mobile Cloud Network Service Provider (MCNSP) to provide services and resources required to operate. How are these services and resources provided? What new interfaces need to be defined?
- How is the MVNO going to be billed for the services/resources utilized? Is it going to be a pay-per-resource model, i.e. the billable item is, for example, an instance of EPC - pay per user, meaning that the MVNO will be charged per user roaming in the MNO network, no matter how many resources are being used - or pay per service, i.e. pay for each service being used, e.g. RAN-as-a-Service or Billing-as-a-Service?
- What model is the MVNO going to use to bill its customers? How can the current pay-as-you-go and flat fee models be further enhanced to reflect the elasticity and on-demand Cloud Computing characteristics? This issue is already partially addressed in (Ponce de Leon & Adhikari, 2010).
- Given the different billing model, how are the Service Level Agreements (SLAs) between the MVNO and the MNO defined?
- In case of Multi-MNO model (with or without ABC) the MVNO will need to manage multiple SLAs and different billing interfaces and presents them to the customer as if they were one. How can this be achieved if, for example, the MVNO is billed with different models, i.e. pay-per-resource and pay-per-user, from the MNOs?
- How can a Light MVNO switch to the Hybrid MVNO or Full MVNO model? And vice versa, i.e. from Hybrid MVNO to Light MVNO model? What are the requirements and restrictions for such upgrades/downgrades?
- Can an adequate level of security and isolation for data records be guaranteed? Meaning that two MVNOs that use the services from the same MNO, i.e. potentially using the same resources, will not be able to access or interfere with each other data.

5.2 Cloud-optimized MNO operations

5.2.1 General Background

Nowadays, the network of a mobile operator is typically built relying on a variety of network appliances. These include the network entities that implement the Evolved Packet Core (EPC) (e.g. MME, SGSN, PDN/Serving Gateway, GGSN and HSS), the surrounding platforms used to control and charge the services offered to the end users (e.g. Deep Packet Inspection (DPI), Legal Interception, Operation & Maintenance (O&M), online/offline charging systems), as well as the infrastructure needed to deliver services going beyond pure connectivity (e.g. application servers, IMS).

All these entities are based on custom hardware and need to be statically provisioned and configured. The resulting network configuration is mostly static and does not feature any cloud-principle, like elasticity or on-demand. The network is typically dimensioned based on the load foreseen in the peak hours and updating it, e.g., to increase the network capacity or enable new functions, requires the deployment of new equipment in specific network sites. Hence, the operation of such a static network is a costly, cumbersome and time-consuming process.

The "cloudification" of the EPC, and of the aforementioned surrounding platforms, creates the opportunity for the mobile operator to move to a completely different network paradigm, where the network functions that used to be implemented on physical boxes deployed in specific Points of Presence (PoPs) become workloads running on top of a cloud infrastructure. The workloads instantiated in the cloud are not statically bound to a specific location, but can be transparently moved between servers located in the same Data Centre, or across Data Centres, without causing any service disruption to the end users. In addition to the obvious advantage of reducing the heterogeneity of deployed hardware, through the re-use of industry standard servers, storage and switching, this approach allows to move from today's mostly static deployments to highly dynamic network implementations, where the network topology, configuration and dimensioning can be changed over time depending on a variety of factors.

5.2.2 User Story

The Summer Olympics are about to start in Italy and hundreds of thousands of fans are flying in from all over the world. Most of those visitors are expected to stay in Italy for a couple of weeks or even longer, to support their favorite athletes and also enjoy the lovely Italian cuisine and architecture.

One of the main Italian mobile operators, Best Mobile, decides to collaborate with an Italian broadcasting company to launch a service allowing the fans to use their smartphone or tablet to retrieve real-time statistics and/or replies of the most interesting sport events. Since the application server is located in Italy, for inbound roamers the service is offered relying on local breakout roaming, meaning that the PDN Gateway is provided by the Italian operator.

The service is a real success. The number of customers using it goes far beyond the initial expectations of Best Mobile, causing very high peaks of traffic during the most interesting sport events. Such peaks of traffic are promptly detected by the mobile operator's O&M systems and, since the EPC is implemented "as a Service" on top of a cloud infrastructure, Best Mobile's cloud orchestration platform automatically reacts to the unexpected traffic growth instantiating additional PDN Gateways. Moreover, since the O&M systems detect that most of the traffic is originated by customers located inside, or around, the Olympic Stadium, the additional PDN Gateways are instantiated in a Data Centre nearby that area, in order to optimize traffic routing. This network reconfiguration is completely transparent to the customers who continue to enjoy the service with no interruptions and have no idea of what happened behind the scenes.

The statistics collected by Best Mobile's O&M systems show that the traffic pattern generated by the customers is periodic and mostly predictable: the traffic load rapidly ramps up in the evening, while the main sport events are taking place at the Olympics Stadium, and is much lower during the rest of the day. As such, during off-peak hours the cloud orchestration platform automatically concentrates the PDN Gateway instances on a smaller number of physical servers, in order to free up unused capacity and achieve energy saving.

The Summer Olympics proceed pretty well: the customers are very satisfied with the experienced quality of service and at the same time Best Mobile is experiencing very high network efficiency and low operational costs. What makes Best Mobile particularly satisfied is the fact that all the required network reconfigurations are triggered and enforced automatically by the cloud orchestration platforms, with very little involvement of Best Mobile's personnel.

Unfortunately, during one of the main events of the Summer Olympics, the men's 100 metres final, an unforeseen situation arises: the network of another Italian operator, Fancy Telecom, experiences a sudden failure, causing lack of service in the area around the Olympic Stadium. As a result, all the inbound roamers who were connected to Fancy Telecom's network, simultaneously reselect Best Mobile, causing a storm of attach requests towards Best Mobile's MMEs. Potentially, such storm of requests can overload the available MMEs, and the interfaces to the HSS, with very high chances to seriously deteriorate the user experience of the customers. But, once again, Best Mobile's O&M systems detect the unexpected increase of signaling and the cloud orchestration platform automatically instantiates additional MMEs to deal with it. The extra MMEs are then released when Fancy Telecom's network is restored and a big chunk of inbound roamers go back there.

At the end of the Summer Olympics many visitors, instead of immediately leaving Italy, decide to take the chance to visit some of the most famous Italian cities, like Rome, Florence and others. Best Mobile, that had foreseen such a situation in advance, extends the service launched during the Olympic events providing additional content, such as tourist guides and maps of Italian attractions. The PDN Gateway instances that had been allocated nearby the Olympic Stadium, where most of the customers used to be concentrated, are automatically spread over the Italian territory to better support foreign visitors during their tours.

At the end of summer, after most of the visitors have left Italy, all the extra resources, such as the extra PDN Gateways instances, are released, so that the correspondent CPU, memory and/or transmission capacity can be used for other services implemented in Best Mobile's Data Centre(s).

5.2.3 Stakeholders

The main stakeholder for this scenario is the Mobile Core Network Provider (MCNP), which provides the Evolved Packet Core (EPC) using the "as a Service" model, meaning that EPC functional entities, such as MME, PDN/Serving Gateway, HSS, etc., are implemented as workloads instantiated on a cloud infrastructure. The cloud infrastructure is provided by the Cloud Service Provider (CSP).

The End User (EU) is the customer that subscribes for mobile connectivity services, and eventually application services such as IMS or others, with the MCNSP. MCNSP, MCNP and CSP may be the same business entity or different business entities.

This scenario brings the following benefits to the MCNP:

- Shorter time to market by minimizing the typical network operator cycle of innovation. Enabling new network features, or simply increasing the capacity allocated to an already supported network function, does not require the deployment of dedicated network appliances.
- Reduced power, space and operational expenses. This mostly comes from the fact that a large variety of network and/or application functions can be implemented re-using industry standard servers, storage and switching. Moreover the possibility of running production, test and reference facilities on a common infrastructure provides much more efficient test and integration, reducing development costs.

- Increased flexibility, meaning that the network configuration, dimensioning and/or topology can be adjusted in real-time, or near real-time, to better fulfil the customer's expectations and/or to optimize the network operation.
- Reduced equipment costs through consolidating equipment and exploiting the economies of scale of the IT industry.

Even though this scenario mostly deals with optimizing the mobile network operation, and hence is particularly relevant for the MCNP, it also brings advantages for the EU in terms of improved quality of experience. For example, relying on cloud technologies, and in particular the ability to migrate Virtual Machines (VMs) between physical servers located in the same, or different, Data Centre(s), a virtualized PDN/Serving Gateway could be easily and transparently relocated, so that to keep it as close as possible to the EU's point of attachment and minimize the end-to-end user plane latency. Finally, in this scenario also the CSP can take advantage from the dynamic workload placement, to fully utilize its data centre infrastructure.

5.2.4 MCN Contribution and Innovations

It is anticipated that, once enabled, the "cloudification" of the EPC will be exploited by the mobile operator in a variety of ways, such as those briefly described in the following:

- The resources allocated to a specific network entity (e.g. MME, DPI, etc.), or even to a certain set of functions implemented by a network entity (e.g. mobility management, session management), can be scaled up and down depending on the actual offered load. As an example, if in a certain geographical area the number of customers faces a sudden increase, e.g. due to an event attracting a lot of people in the same location, the operator can allocate more MMEs and PDN/Serving Gateways in that area, and then release those extra resources as the offered load decreases, so that the correspondent CPU, storage, and transmission capacity can be used for other purposes. Moreover, if most of the customers showing up in a certain location do not move, the operator can allocate more resources to session management and constrain the amount of resources reserved for mobility management, so that to achieve very fine-grained resource control and minimize the amount of unused CPU, storage and/or transmission capacity.
- Relying on the combination of Software-Defined Networking (SDN) and workload orchestration in the cloud, those functions that deal with user traffic processing and which are typically computational-heavy (like DPI, firewalling, parental control and video compression) can be placed on the routing path only for the customers, the APNs and/or the specific IP flows that actually require advanced user plane traffic handling. In all other cases user-plane traffic can be routed to the destination network directly, bypassing any intermediate function.
- Reduced energy consumption can be achieved by exploiting power management features in standard servers and storage, as well as workload consolidation. For example, relying on virtualisation techniques it would be possible to concentrate the workload on a smaller number of servers during off-peak hours (e.g. overnight) so that all the other servers can be switched off or put into an energy saving mode. This is expected to be a very effective way to achieve energy saving because the load in a mobile operator's network, in terms of number of connected customers, signaling overhead and traffic, varies quite a lot during the day. As such, the CPU, memory and transmission capacity required to handle the network load during peak hours are much higher than those needed in other periods of time.

- If a major failure affects one or more nodes of a cloud infrastructure (servers, switches, storage, etc.), or an entire Data Centre, thanks to the recovery techniques supported in a virtualized environment, a new backup node (or a set of nodes) can be spawned in the same Data Centre, or in another Data Centre (self-healing). The workload is moved onto the spare capacity, minimizing user sessions loss.
- The mobile network configuration and topology can be automatically updated, in a near-real time fashion, depending on the actual traffic and/or mobility patterns, the number of customers showing up in a specific location and/or network segment, etc. Doing so the mobile operator has the chance to optimize the network operation and improve the user experience of its customers (self-optimisation). For example, if most of the customers served by a certain PDN Gateway instance are located in a specific geographical area, the correspondent workload could be moved onto a server that is topologically close to that area, in order to achieve better usage of the transmission capacity in the operator's network and also ensure lower user plane latency.
- Separated network instances can be allocated on-demand in the cloud and then used for specific services (e.g. machine-to-machine) or sold to third parties (e.g. MVNOs).

5.2.5 Challenges

The following technical challenges and open questions will have to be addressed in order to enable this scenario:

- What is the reference architecture for the cloud-based mobile network operator? Should we assume that the functional entity instances (e.g. MME, PGW, etc.) to be moved across servers and/or DCs to achieve workload consolidation, network optimisation and/or fault tolerance are implemented as separate Virtual Machines (VMs), or are there other options? How is the terminal-related context information handled? Is the terminal-related context information locally stored on each VM or is it kept in a centralized database? Should we aim at deactivating some network node instances during off-peak hours? Are there any impacts on the gateway and/or node selection mechanisms that 3GPP has standardized for the EPC? Do we need to define a load balancer for user-plane traffic and related signaling?
- Can this approach provide carrier-grade performance (e.g. in terms of network reliability, throughput, delay)?
- In which scenarios and under which assumptions can workload consolidation during off-peak hours provide substantial energy savings compared to simply relying on the power management features supported by standard servers and storage?
- Does it make sense to enforce workload consolidation across different DCs? As an example, is it a valid scenario that during off-peak hours multiple PGW instances that used to be distributed across several DCs are concentrated on a few servers located in a single DC?
- How do we select the servers and/or DC(s) where multiple PGWs, SGWs, MMEs, etc. should be concentrated during off-peak hours to achieve workload consolidation?
- How can we minimize the signaling overhead required to enforce real-time, or near real-time, network re-configuration, e.g. to achieve energy saving or to optimize the network operation?

- How can we ensure that dynamic network re-configuration via workload migration does not cause service disruption of active sessions?
- How can we achieve data traffic re-routing in case a PDN/Serving Gateway is moved to a different server, potentially located in a different DC?
- What are the conditions which trigger workload migration? Is it only triggered in certain time windows pre-configured by the operator (e.g. during off-peak hours, that are most often well known), or can we trigger workload consolidation dynamically, based on the actual measured load on the servers in the DCs?
- Once workload consolidation has been carried out, what are the mechanisms for restoring the original configuration as the network load increases?
- Different delay constraints may demand different technologies to accomplish scale-out/in or migration. Objective is minimized service disruption and maximum system stability.

5.3 Machine-to-Machine / Machine-type Communication Mobile Cloud

5.3.1 General Background

Recently, we can observe a tremendous interest among Utility Providers (e.g., gas, electricity, water utility providers) to reduce their operational cost by means of Machine Type Communications (MTC) (or Machine to Machine (M2M)) devices. Indeed, rather than contracting a firm to manually collect meter readings or have the consumers provide meter information through mail or phone, Utility Providers may use MTC devices and have them automatically provide the current meter readings through a mobile network infrastructure. MTC devices can be smart sensors, actuators, or smart meters. Each MTC device is normally equipped with a SIM card that enables it to connect to a mobile operator network. Depending on the MTC application, MTC devices are usually used to gather specific measurements at a given periodicity (e.g., at the end of every month, at the end of every year, etc.).

5.3.2 Use Story

A central heating company supplies several houses in the region of Twente, the Netherlands. This supplier would like to automatically read out user data from the heating radiators in order to calculate correct billings for this service on an individual usage basis. To accomplish this, the company wants to utilize small devices that are attached to the radiators. These devices, log usage data over a certain timespan and then transmit usage data directly to the company's databases and business information systems, respectively, through the mobile network.

To exploit MTC, the Utility Provider, which in this context is an instantiation of an Enterprise End User, has to, currently, partner with a mobile network operator. The operator may usually charge a fixed average amount of Euro per month and per MTC device to its consumers. Note however, that some consumers with specific profiles, e.g., consuming energy mostly during the night, might be charged with an amount lower than this fixed average amount of Euro per month. Depending on the MTC application/service, the Utility Provider may need to deploy a potentially high number of MTC devices (e.g. millions of devices). With the current pricing model, such a Utility Provider has to pay a significantly large amount of Euros per month, given the fact that such MTC devices connect to the mobile network only at low frequency (e.g., once a month) and most importantly for a very short time (i.e., only for several seconds at the end of each month for sending measurements about the gas/electricity/water consumption).

The Utility Provider decides to reduce these MTC related prices, including the reduction of the charging bill to its consumers, and therefore it decides to partner with the newly established Mobile Cloud Network Service Provider (MCNSP). The prices can be reduced by requesting from the MCNSP to deploy a short-term configuration of a mobile network having a lifetime for only the time to collect measurements from the deployed MTC devices and to send them to adequate MTC servers.

5.3.3 Stakeholders

The main stakeholder associated with this scenario is the Enterprise End User, which in this scenario is represented by the Utility Provider, is able to provide utility services to its consumers (in this scenario considered as being the End Users). Another stakeholder that partners with the Utility Provider is the MCNSP. The MCNSP provides services to the Utility Provider, including Connectivity and Application Services, both based on cloud infrastructures, which are only charged for the time that they are being used (i.e., Pay as you Go concept).

The End Users, i.e., the consumers of the Utility Provider, benefit from the deployment of this scenario by a (significant) reduction of their energy bill needed to be paid to the Utility Provider. Moreover, since the smart meter readings will be automated, consumers will benefit by not having to worry communicating the smart meter readings by mail or phone to the Utility Providers.

5.3.4 MCN Contribution and Innovations

The MCN contributions and innovations will allow an Utility Provider to partner with an MCNSP and to request the deployment of a short-term configuration of a MTC mobile network. These contributions and innovations are briefly described below:

- The MTC mobile network (on the cloud) will be dynamically and on-demand created, allowing stakeholders, like Utility Providers to create and use the mobile network whenever they need it and for the time they need it. The lifetime of this MTC mobile network will be for only the time needed to collect measurements from the deployed MTC devices and to send them to adequate MTC servers. Allocating resources from the cloud and running mobile network functions there for a very short time is certainly less costly than paying MTC device subscription fees (for the multitude of MTC devices) to a traditional mobile operator. In particular, this mobile network can be proactively enabled (e.g. through an interface available on the O&M system), but also reactively enabled in case of for example, increase/decrease of the number of consumers.
- Dynamic adaptation of the topology and architecture of the MTC mobile network (RAN and EPC) will be enabled in order to optimize its operation by providing the ability to initiate and use mobile network instances and resources when needed and for the time that they are needed. This can be proactively enabled (e.g. through an interface available on the O&M system), but also reactively activated, in case of for example, increase/decrease of the MTC devices and load.
- Network elasticity will be supported, with scaling out/in of EPC virtual instances, in order to cope with the variability of the number of consumers and of the MTC traffic load. The support

of network elasticity optimizes the usage of system resources by allocating only the needed resources, being able to scale in/out the allocated CPU, memory and network capacity to follow the variations of the MTC traffic load. The scaling out/in of EPC virtual instances can be manually triggered by the network administator (e.g. through an interface available on the O&M system), but it can also be automatically activated in case of MTC load increase/decrease.

- The collection and dissemination of the MTC measurements will be balanced over time. Load balancing is necessary since usually all MTCs belonging to multiple Utility Providers are reporting in bursts. In this way the MCNSP provider is able to provide different MTC mobile networks to different Utility Providers and to perform MTC load balancing over time among these different MTC mobile networks. The MCNSP provider is in this way enabled to charge the use of resources depending on the network load.
- The SLA and charging models used between the Utility Provider and the MCNSP provider will be optimized in order to take into account conditions and overall costs thresholds. By having a clear definition of the SLA and charging models the Utility Provider can specify the conditions and the overall costs threshold (maximum amount of financial resources) that is willing to pay for the use of the MCNSP service (access and use of the MTC devices).

5.3.5 Challenges

The Utility Providers will benefit from the ability to obtain rapid, flexible, and elastic network configurations for accessing and collecting information from MTC devices, significant cost reduction and short time to market solutions. In addition, since they become the owner of their respective "virtual mobile networks", they will be able to have a certain level of control on the efficiency of communications among their MTC devices and MTC servers. For the MCNSP provider, it is expected to directly and strongly enter into a new end-to-end value chain, generating important revenue streams with this particular scenario, as it offers the ability to host and dynamically deploy 3rd party MTC services.

This can be realised by supporting the following technical challenges:

- Which technical solutions can be deployed in order to initiate and use mobile network instances and resources when needed and for the time that they are needed? These technical solutions will allow the MTC mobile network (RAN and EPC) to be dynamically and on-demand created and disposed.
- How can allocated resources, such as CPU, memory and network capacity scale in/out in order to follow the variations of MTC traffic load? The answer to this question will optimize the operation of the MTC mobile network (RAN and EPC) by dynamically adapting its topology and architecture.
- Should the increase/decrease of MTC traffic load control the scall in/out of allocated resources in real time?
- How load predictions schemes can be used to optimize the process of scaling in/out RAN and EPC instances? Load prediction can provide the ability to the the virtualized RAN and EPC to scale in/out before the actual actual load changes.

- How and when should the MTC measurements be monitored, collected and processed in order to initiate/maintain EPC topological changes? Such MTC measurements could be monitored, collected and processed on an event basis, e.g., alarm, or in a periodic basis, when charging and billing related information needs to be processed.
- How can the MTC traffic load generated by different MTC mobile networks be balanced over time? The MCNSP provider is then able to provide different MTC mobile networks to different Utility Providers and to perform MTC load balancing over time among these different MTC mobile networks.
- How and which conditions and overall costs threshold can be applied in order initiate, configure and maintain SLA and charging models? The answer to this question will optimize the operation of SLA and charging models that are e.g., used between an Enterprise End User and the MCNSP provider.

5.4 MCN-enabled Digital Signage

5.4.1 General Background

A Digital Signage (DS) system is a network of customizable displays that can be controlled electronically using a computer, allowing content to be changed remotely for well targeted messaging. DS architecture is formed by two main components:

- DS Central Server: a server where multimedia contents are uploaded. It also hosts an application frontend to schedule and set up playlists and monitor the network to ensure that everything works well. Authentication is also done in the Central Server. When a request is made to the Central Server, it is performed in the security context of a specific user or DS player. The Central Server also keeps track of the resources usage of each user to support the billing service.
- DS Player: is usually composed by a PC and a screen (LCD TV, videowall, video projector, etc). It can play different type of contents (Video, audio, images, RSS, flash, web) and it also reports back to the central server its status and the contents played. It can also receive real time events from different sources (camera, sensors, etc) that will dynamically change contents in real time

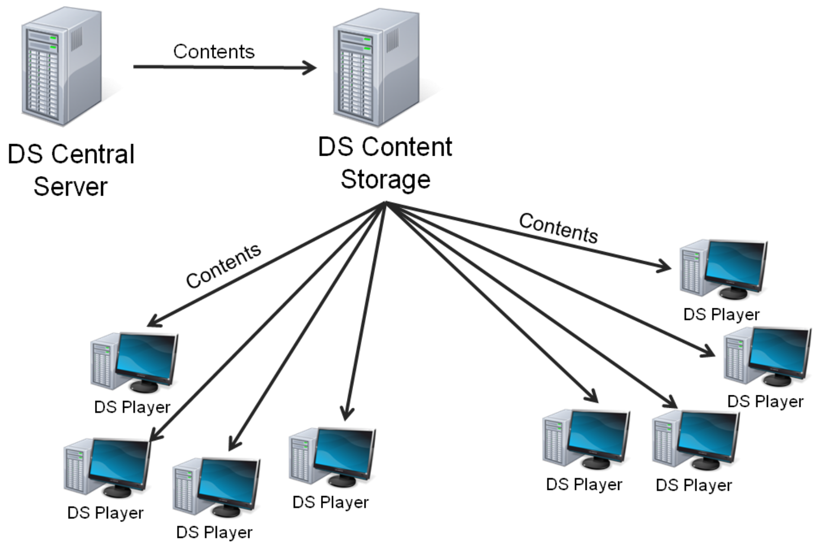

Figure 5-4 Conventional Content Distribution

The DS central server receives data reports from the DS players with information related to two main issues, what contents have been played and when they have been played and information related to the sensors that the DS players have and produce the real time events. This data is stored and it can be processed offline (statistics information).

A DS Network deployment is based on geographically distributing DS players over a certain area (e.g. a building, many different company locations) during a certain time period. The DS players must have a network link to synchronize with the DS central server and download the schedules, the playlists and the multimedia contents needed.

5.4.2 User Story

A Gastronomy Tour is going to take place in Spain. The tour is composed by 6 events of 1 week duration allocated in 6 different cities. At each event, different companies and manufacturers will show their products and information presenting the local gastronomy. The organizer of the Tour is planning to deploy a Digital Signage Network (DSN) for each event. Every company participating on the fair will be able to upload their contents (products portfolio, company information, prices list) to the DSN so that they can be displayed on the LCD screens that will be installed in the venues of the tour and on the outskirts of each venue. The companies' contents will be mixed with some multimedia contents related to the cities that are hosting the event, as a tourism guide. The DS players will also be equipped with small cameras to act as a sensor for obtaining demographic data from the people who are watching the players. The data obtained from the cameras will be the trigger for displaying contents depending on how many people is watching the player and if they are male or female. This data will also be sent to the DS Central Server to be processed offline.

To achieve this kind of deployment, the DS service provider needs to deploy an efficient network infrastructure (Ethernet LAN or WIFI for example) and an Internet connection service with high capacity for each venue for the synchronisation (multimedia contents, schedules and playlists) between each of the DS players and the DS central server. In most cases this is very expensive and also a hard job (manage different services contracts with different vendors), even more for a temporary event. Even the costs can vary from one city to another.

The DS provider will also have to provide a DS Central Server and a Content Storage to control and monitor all the DS players deployed in each venue of the fair and to store all the contents uploaded by the different companies participating on the fair. The DS central server will also receive the reports form the DS players, with the summary of what contents have been played and when, and the information from the demographic detection. This data will be merged and processed in the DS central server so the users will be able to measure the effectiveness of their contents. With this architecture, two types of computation are considered:

- Offline computation: is made in the DS central server. The stored data from all the DS players is merged and processed and it can be presented as statistics through the user interface.
- Online computation: is made in the DS players. It is related to how the DS players respond to the interactive events in real time. In this case the online computation is based on the demographics detection and the response of the DS players to this events with the triggered contents.

The DS provider could hire compute, storage and network resources from a cloud service provider. The resources hired will have to be enough for: storing all the multimedia contents of all the participants and answer all the requests from the users (Web based frontend) and the DS players (API). The Central Server throughput will also have to be enough for the peaks of traffic during the DS Players contents download process as all the DS players of a venue will have to download a huge amount of data at the same time. The service contracted for hosting the DS Central Server must be very reliable as it is a key component of the DS Network, if The DS Central Server goes down, no contents can be downloaded, no schedules can be set and no monitoring data can be collected from the DS players.

From the customer's point of view, it would be really useful to be able to have an on-demand, pay-per-use DS service (DS Server and DS Players) and the connectivity service in the same package. And there is where the Mobile Cloud Networking (MCN) technology becomes crucial.

5.4.3 Stakeholders

In this scenario, the main stakeholder is the DS Service Provider (Application Services Provider) that deploys and provides the DS Network ready to use for the End User (DSN Customer). The DS Provider should make an agreement with the Mobile Cloud Network Service Provider (MCNSP) for offering the connectivity service along with the DS service. In addition, the DS provider could also use other Value Added Services (VAS) from the MCNSP like the Rating, Charging, Billing and SLA management services. The expenses of deploying a network infrastructure would be reduced.

The Cloud Service Provider (CSP) enables the DS provider (ASP) to instantiate the DS network on top of the cloud infrastructure. This service could also be offered by the MCNSP along with the connectivity service.

The main benefits for the DS provider in this scenario are:

- Improve the Digital Signage service by offering it along with the connectivity service for the DS players.
- Increase the elasticity of the service by being able to adapt storage, compute and network resources in real time depending on the requirements (higher bandwidth only during the traffic peaks for example).

- Reduce the latency between the DS players and the DS Central Server by migrating a subset of the server functions to a location near to the DS players. This improves the contents download process of the DS players and also generates faster responses from the server to the interactive events captured by the DS player sensors.
- Increase the reliability and availability of the DS Central Server as it can be distributed by migrating the resources.
- Improve the DS Experience for the potential targets by using the network information provided by the MCNSP (location, network load level) for triggering new interactive events.
- Accuracy on the charging and billing services as the user would only pay for the resources he has used.
- Reduce the expenses of deploying a physical network infrastructure for each event.

5.4.4 MCN Contribution and Innovations

The main MCN contributions and innovations derived from this scenario are the following:

- Instantiating network services on-demand in the cloud for specific events. The DS provider could contract the MCN Service Provider for providing a flexible connection service for each venue of the event.
- All the resources needed for offering the DS service could be scaled up or down depending on what is required in a certain moment. If more storage space is needed for the multimedia contents, the DS provider could allocate more storage resources to those contents. The same happens with the network capacity if there is a traffic peak due to many DS players downloading contents at the same time.
- Regarding the elasticity concept, the Offline computation can be highly improved applying new processing algorithms, despite the computational or storage resources they need. Either, a new computation layer can be added in the data centre where data can also be stored now to distribute the Online computation that is done in the DS players.
- Locating a subset of the functionality and the multimedia contents in the Data Centre, near the user, thanks to the virtualisation technology. As depicted in Figure 5-5, by locating content caches near the users, the download time of the multimedia contents is considerably reduced and also the use of the network becomes more efficient.

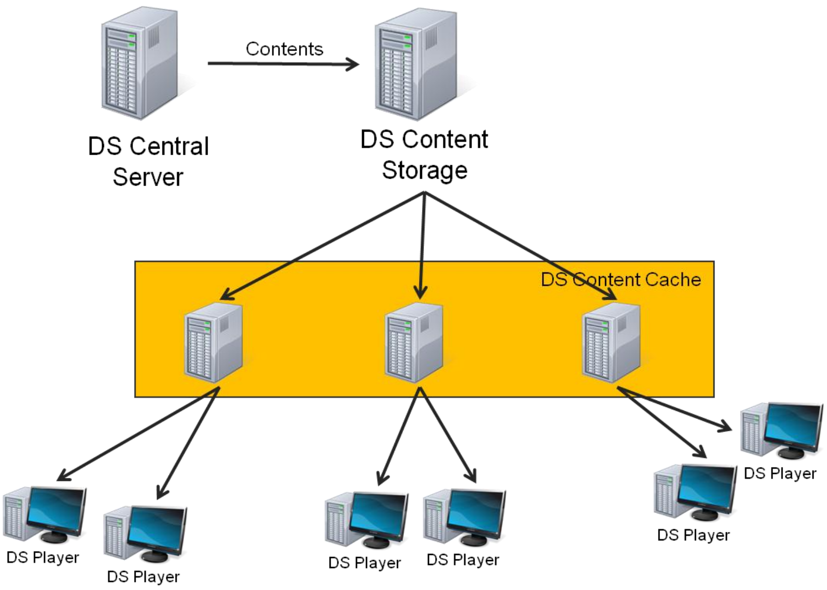

Figure 5-5 "On-the-border" content distribution

- Providing certain end-to-end QoS / QoE parameters, combined with the "on-the-border" contents concept, offers new business cases to the DS provider. Content Delivery Networks (CDNs) could be used for providing contents to the DS players for example.
- Providing information from the network enables the possibility for the DS players to dynamically change and adapt the contents displayed. For example with the location information de the DS player may trigger new contents depending on where it is. Another case would be if the load of the network is high, the DS player could ask for videostreams with a lower bitrate.
- Thanks to instantiating the DS service in the cloud, the Ds Central Server and the contents can be distributed so in the case an instance goes down it can be quickly recovered and instantiated again. This issue makes the DS service more robust and reliable.

5.4.5 Challenges

The Digital Signage Network Provider must adapt the DS Network solution to take advantage of the MCN potential. These are the following challenges to accomplish this:

- Develop a service orchestrator entity that keeps track of the state of the DS service and allocates and disposes service instances as needed, based on the monitoring information obtained from the controllers of the different resources.
- Create a content manager that will manage the storage resources, it will scale up and down the storage space whenever is needed.
- In the case of distributed services, where many instances are deployed, mechanisms to balance the workload between different instances must be developed.
- Define mechanisms to decide when and where to locate content caches and subsets of the DS central server functionality to reduce the latency between the DS players and the DS central server.

- Be able to define definite QoS/QoE levels that can be directly translated into QoS/QoE requirements for the network service (EPC for example).
- Create an interface that can provide real time information of the system status for triggering new contents in the DS players. For example, when a DS player changes its location or is in movement, the location detection must be fast enough to permit the DS player to adapt its scheduled playlist.
- The resources migration mechanism must be transparent for the user and the service mustn't be interrupted by the migration process.
- Track of the used resources (compute, storage, network), even if they are distributed, is needed for charging the user just for the resources used.

5.5 End-to-End Mobile Cloud

5.5.1 General Background

In Mobile Cloud Networking, there are wide and varied ranges of possible services that can be offered to a potential service owner. Key to providing these services to the ASP in an integrated and uniform fashion is the MCNSP that provides end-to-end (E2E) services. An E2E service is a service that comprises of sub-services that are combined together with additional logic and configuration in order to offer out as a new service offering. This is very much similar to how web service composition or mash-ups are offered.

Typically in Mobile Cloud Networking, there are 3 main service domains (RAN, Core Network & Data Centre). Within each there is one or more services that can be combined with each other or with services from different domains. It is the MCNSP that is responsible for combining and integrating these sub-services. An example of this would be the combination of: a Wireless service (RAN domain), an EPC service (Core Network domain) with Compute and Storage services (Data Centre Domain). This service itself would likely need to have additional support services (such as OSS and BSS) added in order to be a complete service. Other potential services that can be combined include an IMS service and a CDN service. For the purposes of this scenario a fictitious partnership is described. A mutual partnership between network operators and Cloud service providers (for example CloudSigma & Italtel) is formed to leverage each other's resources. This partnership will be the business realisation of "Cloud and Network convergence" or as noted in the MCN DoW "Extend[ing] the Concept of Cloud Computing beyond data centres towards the Mobile End-User."

Each stakeholder will profit from this mutually leveraging each other's strategic assets. Essentially this will allow for new business revenues because of the number and size of the customers. The goal is to offer their combined services in a new "Mobile Cloud Networking End-to-End Cloud" offering. This offering will be offered to service consumers in an on-demand, dependable and billable way.

The network providers have large untapped networking resources and licences for network frequencies, which could be used (multiplexed) by any of their customers. These network resources are geographically distributed, fast, and able to deal with large amounts of customers.

On the other hand the Cloud Service Providers are experts on using and optimising the utilisation within the data centres. Currently they mainly offer Compute and Storage as a Service. But more and more CSPs start to offer other Services on the PaaS layer as a Service. However the network providers do not have the expertise the offer out Cloud services as a commodity to service consumers.

The CSPs do not have the large resources of the Network providers and the captive audiences. So if both combine forces the CSP can deploy services on all available/suitable network provider infrastructures. The network provider is able to offer cloud service to the service consumers now. The service consumer of those services power/run OTT services. Together they can offer capabilities like a RAN as a Service.

5.5.2 User Story

CleverDev is a software service development company operating as a startup wishing to offer new higher level services to enterprise customers.

One of the services that CleverDev wishes to offer is an enterprise collaboration suite that has messaging (both instant message and email), collaborative document editing, presentation sharing and desktop sharing. Many companies offer such integrated suites of tools however, none of them provide an essential piece, especially to mobile and remote working “road warriors”. This piece is the access from the user’s mobile device (any device with wireless capabilities) to an IP-based network. Generally what happens today is that a collaboration suite provider, such as webex.com or gotomeeting.com, provides the services and high quality connection access to those services. In the case of CleverDev their application requires a varied set of cloud-based services. In order to operate all their services they require compute service capabilities implemented as VMs. To persist their data they will need two types of storage services: block and object storage. The block storage is used to persist their mysql database files safely. The object storage is used to persist files (e.g. presentations, documents, images etc.).

So that all these services are connected a set of virtual networks are required. A simple logical configuration of 2 networks is planned: a network that hosts the publically accessible services (e.g. web servers, desktop streaming servers) and then a private network that hosts internal database services and others that are not appropriate to be externally exposed.

Key to CleverDev’s service offering is that the user has a high experience in terms of performance. What this means is that there should be no perceivable degradation in servicing the user for example: when a user requests a file it should begin downloading quickly and at maximum speed, when the user is viewing another presentation or desktop there should be no apparent lag when the presenter changes from one slide to another. As such control of network parameters such as latency and bandwidth are very important for delivering a quality service.

To address these issues, CleverDev aims to use a content distribution service to bring static content (e.g documents, presentations, images) closer to the end user based on their geographic location (approximated by IP address range). To ensure a suitable response time from the services, CleverDev wishes to use a combination of load-balancers and geographically located services. Purpose of the load balancers are to route user traffic to the closest available service (IP approximation).

CleverDev are very much aware that there is massive growth in mobile applications and although they still see the traditional desktop-bound user as an important market segment, they wish to offer the very same experience to mobile device user market segment. It is here where a large challenge arises.

With existing cloud services is has been possible to provide consistent user experience but only where the access to services has been over fixed network infrastructure (either physical or virtual). This has been possible due to the easy access to the required network services. Now when we consider mobile access there is significantly reduced access to the required wireless network services. This is because currently today mobile access technologies are not commonly offered as on-demand services as VMs are by the likes of Amazon. It is exactly these wireless networking services that CleverDev needs to ensure the same service to both its desktop and mobile users.

CleverDev wants to provide their services but in a true end-to-end service offering. This means that service access must also include wireless access to the collaboration services. That connectivity to those services must be specified with QoS/QoE depending on the type of customer is being serviced by CleverDev. Today this cannot be achieved, however with the advent of Mobile Cloud Networking technology it can. In doing so new innovative services can be provided to end users and ease the service procurement process for enterprises.

However CleverDev does not own their own physical infrastructure to realize their service offering. It so needs to leverage (e.g. lease) the infrastructure of one or more providers. Other service providers which offers connectivity services can offer these features for CleverDev. CleverDev decides to use UrNet as they're offering the right set of services and at the right price. This allows CleverDev to add more capacity (quickly) on demand as it is needed. If needed, UrNet allows CleverDev to add new services in order to extend their service offering. CleverDev gets the UrNet service via a self-service interface where they supply their billing details. CleverDev can either use the web user interface or programmatic interface of UrNet’s service to create an instance of the service.

When UrNet receives the request from CleverDev, UrNet understands the various components that need to be created and orchestrated to offer back the service instance to CleverDev. In this case UrNet needs to create compute, storage (block & object), CDN, RAN, EPC and IMS related components, including OSS and BSS elements. When these components are created, UrNet needs to suitably configure them so that the full end-to-end service is ready for use by CleverDev. This essentially means that the (inter)networking required to connect all services is carried out. UrNet is something similar to CleverDev as they do not own physical infrastructure, however UrNet was created by people that understand how to create, orchestrate and configure both cloud and telco-type services. In order for UrNet to assemble the correct service for CleverDev, they create the necessary services on partner providers that offer individual compute, storage, RAN, EPC, IMS and other services.

5.5.3 Stakeholders

The stakeholder to begin with for this Scenario is the **Application Service Provider (ASP)**, who offers services to its service consumers (as **IEU**). The ASP provides services to service consumers on higher layers in a dependable, billable, on-demand manner. In our scenario above the ASP is a developer wishing to offer a suite collaboration services. The ASP requires foundational services in order to provide its services. In order to get these services the ASP uses the facilities and services of the MCNSP. The **MCNSP** acts as an entity that integrates and orchestrates a suite of complimentary services that it can then offer back to prospective users, in our case an ASP. Behind the MCNSP are the service providers. These are providers or particular services and in MCN, these are the **CSP**, **MCNP**, **SSP** and **RANP**. The **CSP** provides services such as compute, storage (block and object) and basic networking services. The **MCNP** provides important networking services that are in this user story’s case predominantly wireless networking services, which are managed through an EPC software stack. In order to enable the MCNP, it may be required that mobile wireless access networks be provided as services. This is what the **RANP** provides in this case. Finally, the **SSP** is the provider that can bring the necessary authentication, monitoring and billing, rating and charging services that are needed in the user story.

The benefits for key stakeholders in this scenario are:

- The ASP can develop new applications based on the services offered to him, especially the new network capabilities brought by MCN (EPCaaS). This will allow for the creation of new applications from which Mobile End-Users can benefit in that they will use services provided by the ASP that are more tailored to their needs and are more cost-effective.
- Other stakeholders offering services similar to this can also make use of the network capabilities which are exposed 'as a Service'.
- In general, the benefit is greater to the NCP than the CSP. This is natural as telcos have to catch up with the cloud computing ecosystem and as telcos generally own the physical infrastructure they are in an advantageous position.
- New revenue streams for CSP in providing their MCN-enabled management software, running NCP workloads on their infrastructure.
- The NCP has the ability to offer new on-demand OTT services to end users, maximise infrastructure utilisation, offer cloud services closer and more cheaply to end users.
- This scenario enables to build MVNO/MNO services (e.g. leveraging EPCaaS) by offering RANaaS and supporting services such as compute and storage.
- New revenue streams for CSP and DIP in providing their MCN-enabled management software, running NIP workloads on their infrastructure.
- The MCNSP becomes a critical entity as through the use of the cloud controller it can not only offer the services that ASPs need but also as a value added reseller. Going one step further it can become a market place, so long as it can capture the market of ASPs and provide the technical means to access and use services through a common interface.

5.5.4 MCN Contribution and Innovations

This scenario is challenging in the requirements it places upon the resulting MCN software framework. Overall what will result will be “telco grade” cloud services that have low latency, are dependable and minimise downtime. In detail, some of the main contributions and innovations arising from MCN and this scenario will be:

- Develop a cloud controller that will be able to (inter)network related instantiated services through orchestration techniques.
- Extend current APIs and/or frameworks (e.g. OCCI, OpenStack) so that a user can list and specify the geographic region or regions where their services should be deployed in.
- Define or extend APIs so that QoE and QoS requirements upon networking services can be easily specified.
- Develop a monitoring service that can be used and integrated with all services that has a well defined interface, offered to standardisation bodies, that allows monitoring metrics to be enabled or disabled and/or customised (update period, granularity etc.).
- Extensions to current cloud computing SDO specification, especially in the area of networking and/or new service types to be considered (e.g. wireless as a service).

- Develop a content distribution service that not only distributes static content such as images but one that can distribute the load on a service (a dynamic entity) to the instance that is geographically most close to the requesting entity.
- Create a billing, rating and charging service that can not only integrate with service providers such as the MCNSP but also to service developers like the ASP. The definition of the interface to such a service would make for a useful contribution to SDOs. This service should be built upon the monitoring service that MCN will deliver upon and in doing so be used in both telco and cloud computing technology domains.
- Implement and/or extend an existing AAA solution that can both integrate with existing technologies in the telco domain (e.g. EPC) and also with services in the cloud computing domain (e.g. OpenStack).
- Expose the services used within MCN upon a platform as a service (PaaS) technology. This would entail extending an existing PaaS so that it could instantiate the various services used within MCN. Having the platform enabled with these services would be just one of the steps needed. Another important step would be to expose the services through software libraries that developers of the PaaS service could program their applications against. For this various software APIs would be defined and their implementations would call out to the services where appropriate or needed.

5.5.5 Challenges

For the user story and the innovations as described above the following challenges will need to be solved.

- How to enable end-to-end (inter)networking between all services instantiated, even across multiple service providers;
- How to provision compute and storage services based on geographic requirements;
- How to ensure that the (inter)networking between all services are compliant to QoS/QoE requirements set by the service requestor;
- How to specify the network QoS/QoE when requesting a network-type service instance;
- How to ensure that the virtualisation technology employed by each service provider will provide a similar performance (e.g. response time, latency, bandwidth) as current non-virtualised technologies;
- How to consistently monitor provisioned service instances from different providers in a efficient and common fashion;
- How to enable particular monitoring metrics that are important to me and disable other unimportant metrics;
- How to enable alerting on selected metrics using simple rules;
- How to discover new services and new service providers;
- How to request a composite service and have its constituent services correctly (inter)networked;

- How to request multiple different service type instances using a common interface;
- How can a service provider offer the services of another provider but through its interface;
- How to have an easy to use wireless network service instance that is created in geographic regions of my selection? That service should be easy to integrate with my existing traditional wired networking service infrastructure. It should also be scalable depending on the number of my customers;
- How to have an easy to use multimedia (voice, text, image, video) service that is compliant to mobile phone standards (e.g. 3GPP). This service should be easy to manage and configure. The service should also scale according to the number of users consuming it;
- In order to distribute content closer to my end-users an easy to use content distribution service is needed. This should easily integrate with existing storage services and should allow me to redirect end-users to compute services that are geographically closer;
- As a service developer, I will be billed by my service provider. As a service developer I will have a number of customers. As such I will need a billing, rating and charging service so that I can charge (possibly with discounts) and bill my customers;
- As there will be customers using the developed service, those user will need to authenticate themselves in order to access those services. The same applies for the application developer as they too will need to authenticate themselves to the service provider. A service should be provided in order to authenticate both types of actors;
- With all the services that a MCNSP could potentially offer, how could a new or existing platform as a service provider integrate and offer those services upon its platform.

6 Requirements

6.1 Requirements Methodology Outline

This section outlines the methodology used for the specification of requirements. The starting point is material available in D2.1 Methodology. In order to allow a productive work, the derivation of requirements followed a well-known process and used well-known table templates. This section describes both briefly.

Figure 6-1 generally outlines the process to derive Requirements.

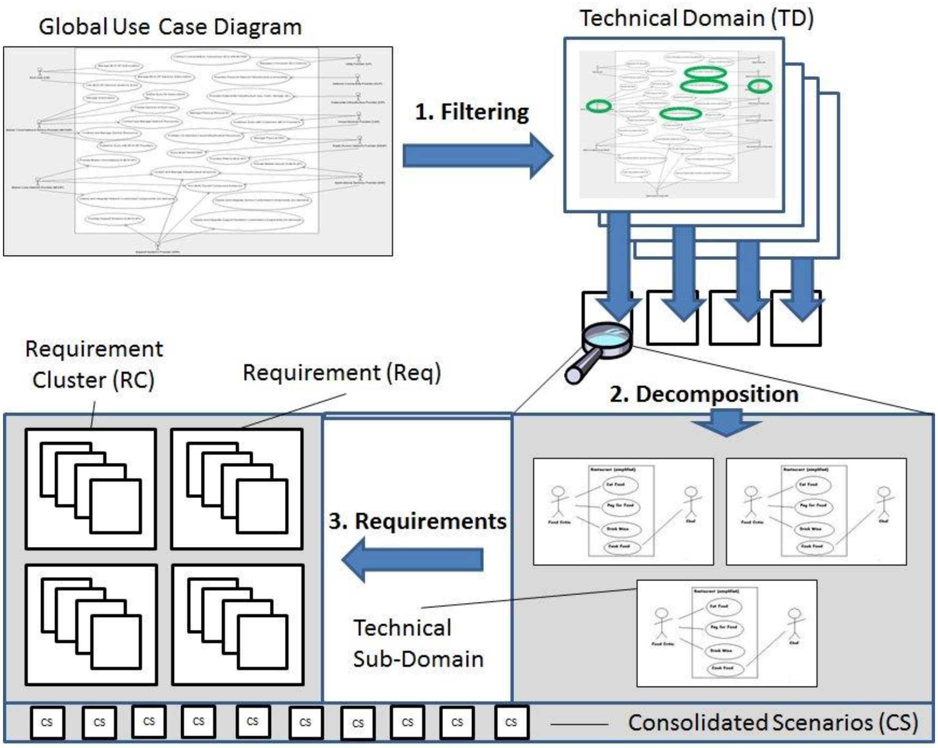

Figure 6-1 Requirements process

The process started by considering the Global Use Case Diagram. This diagram resulted from the global view of all stakeholders and their main functions (at very high level) for all Consolidated Scenarios (see section 3).

The first step was to filter (Filtering) from the Global Use Case Diagram, which stakeholders and Use Cases (bubbles) are relevant for a particular Technical Domain (TD). This step created four different views of this Global Diagram: the Global Technical Domain Diagrams. From this point on, the process evolved in four fully independent threads: one for each Technical Domains (TD). To each TD a team was assigned including specialists in each of these areas.

In the second step, Technical Domain teams analysed the Global TD Diagrams and decomposed them into multiple sub-domains, if considered helpful. In that case, each sub-domain generated a more focused and detailed set of UML Use Case Diagram (Decomposition).

In the third step, Technical Domain teams looked into Consolidated Scenarios (CS) (or even at Draft Scenarios (DSs), if needed), the DOW, or other relevant source of information and identified Requirements within the specific boundaries of that Technical Domain.

In the fourth step, a list of detailed requirements was derived and fully specified.

As a final step, each Technical Domain team had a look into all other TDs, in order to align Requirements, ensuring that all are following a common language and editorial style. At the same time, this was the appropriate moment to reach dependencies between TDs. This final point was essential to come up with coherent and integrated overall results.

It should be noted that basis for requirements was the Consolidated Scenarios (see Appendix B), not the Final Scenarios. As a matter of fact, Consolidated Scenarios provide the technical content that enables a realatively straightforward derivation of requirements. On the contrary, the Final Scenarios, although quite aligned with the Consolidated Scenarios, are meant to provide a prosaic description and a high-level business-oriented vision, with the technical aspects considerably diluted, thus obviously not so adequate to derive technical requrements.

6.2 Specification of Requirements

The specification of requirements has been organized in four major technical domains:

A. Cloud Data Centre Infrastructure and Network Programmability
B. Access Network Infrastructure Cloud
C. Mobile Core Network Cloud
D. IMS/OSS/BSS/VAS as a Service

The requirements are classified in two basic groups – functional and non-functional. Functional requirements specify what the system must do, or the actions it must perform to satisfy the fundamental reasons for its existence. Non-functional requirements specify system properties such as performance, reliability, security, usability or operating environment. Non-functional requirements do not alter the essential functionality of the system (Robertson & Robertson, 2012).

For each TD, requirements were organized in clusters, according to the functionality or properties tha they address. This typically includes:

- Functional requirements regarding desired behaviours of the system.
- Requirements addressing provisioning capabilities.
- Requirements regarding monitoring capabilities.
- Requirements addressing properties such as reliability, availability, robustness, resiliency and redundancy.
- Requirements regarding system performance
- Requirements regarding system security
- Other requirements, which do not fit into any cluster above, e.g. backward compatibility – standardisation bodies (e.g., 3GPP) requirements are considered as requirements to be fulfilled by the proposed solutions within MCN.

In the following sections, the requirements related to each of these Technical Domains are identified. The detailed specification of requirements is presented in Detailed Requirements Specification. The fields used to specify requirements follow the *Volere* guidelines with minor adaptations and simplifications (appropriate for high level Requirements).

In order to uniquely identify Requirements, the notation Req-X.YYY has been used, where:

- X identifies the Technical Domain: (A, B, C or D, as above).
- YYY identifies the requirement within a specific Technical Domain.

6.2.1 Domain A: Cloud Data Centre Infrastructure and Network Programmability

This Technical Domain includes all the features regarding the cloud infrastructure implementation in the Data Centre. That includes typical cloud capabilities like virtualisation, elasticity, on-demand provisioning, etc. It also includes features regarding Network Programmability.

Figure 6-2 depicts the UML Use Case Diagram that supports the Domain A perspective.

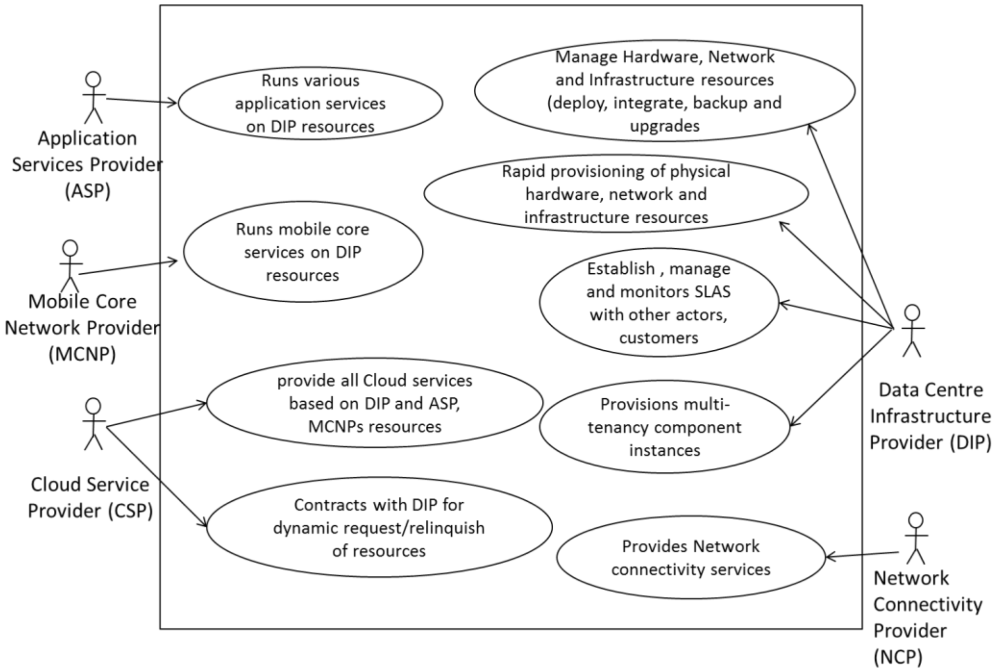

Figure 6-2 Technical Domain A Use Case diagram

Table 6-1 presents Technical Domain A requirements. The full specification of these requirements can be found in Appendix A.

Table 6-1 Technical Domain A Requirements

Requirement ID	Name	Description
Req-A.001	Virtualisation	The functionality for EPC and Mobile cloud shall be virtualizable
Req-A.002	Elasticity	The cloud shall be elastic, i.e. shall be able to scale horizontally
Req-A.003	On Demand Scaling	Cloud shall be able to scale on demand i.e., on rapid timescales
Req-A.004	Network Programmability	Networking among the system components shall be changeable

Requirement ID	Name	Description
		dynamically
Req-A.005	Load balancing	The Cloud shall be able to balance load among different nodes
Req-A.006	Multitenancy	Multiple instances of the software shall be able to run on each single physical node
Req-A.007	Energy efficiency	Energy efficiency shall be supported
Req-A.008	Configuration and management of virtual machines and their addressing	Configuration and management of virtual machines and their addressing shall be supported to manage software-based functional blocks, as they can be virtually run from different locations and hardware.
Req-A.009	Dynamic adaptability of topological / architectural changes	Dynamic adaptability of topological/architectural changes shall be supported
Req-A.010	Dynamic migration of virtualized functions	Dynamic migration of virtualized functions shall be supported
Req-A.011	Retrieving/providing the topological location of Data Centres	Retrieving/providing the topological location of Data Centres shall be supported
Req-A.012	Dynamic placement of instances within a Data Centre	Dynamic placement of instances within a Data Centre shall be supported
Req-A.013	Upgrading the location information of the instances (e.g., after migration) running on Data Centres	Upgrading the location information of the VM instances (e.g., after migration) running on Data Centres shall be supported
Req-A.014	Set-up a proper inter-Data Centre or inter-server (i.e., intra-Data Centre) connectivity	Set-up a proper inter-Data Centre or inter-server (i.e., intra-Data Centre) connectivity shall be supported
Req-A.015	Adaptation of address and identification information for migrated instances	Adaptation of address and identification information for migrated instances shall be supported
Req-A.016	Inter-working with transport network to enforce rules for traffic indirection	Inter-working with transport network to enforce rules for traffic indirection shall be supported
Req-A.017	Dynamic Resource Allocation	Various resources shall be dynamically allocated by cloud controller as per loading conditions
Req-A.018	Supporting IaaS interfaces	New IaaS interfaces shall be supported to allow interoperability of equipment, preserving investments.
Req-A.019	Allocate new Virtual Machines	The system shall be able to create and allocate Virtual Machines as per functional requirements
Req-A.020	Modify existing Virtual Machines	The system shall be able to modify existing Virtual Machines
Req-A.021	Dispose Virtual Machines	The system shall be able to dispose existing Virtual Machines
Req-A.022	Create Storage Resources	The system shall be able to allocate new storage resources
Req-A.023	Modify Storage Resources	The system shall be able to modify storage resources
Req-A.024	Dispose Storage Resources	The system shall be able to release storage resources
Req-A.025	Create Network Resources	The system shall be able to allocate new network resources
Req-A.026	Modify Network Resources	The system shall be able to modify network resources
Req-A.027	Dispose Network Resources	The system shall be able to release network resources
Req-A.028	Data collection from Nodes	There shall be a mechanism to collect data from individual nodes and send it back to collector node
Req-A.029	Data Aggregation and processing	All monitoring data shall be gathered and processed
Req-A.030	SLA monitoring support	Monitoring data shall be checked against SLA requirements to determine a possible violation

Requirement ID	Name	Description
Req-A.031	Monitoring of the location of workloads	Monitoring of the location of workloads in real-time (or near-real-time) shall be supported
Req-A.032	Monitor VMs (location, resources)	Monitor VMs (location, resources) shall be supported
Req-A.033	Monitoring of load in VMs	Monitoring of load in VMs shall be supported
Req-A.034	Monitoring of service quality	Monitoring of service quality shall be supported
Req-A.035	Monitoring of system stability	Monitoring of system stability shall be supported
Req-A.036	Process load statistics and compute scale-out/in prediction scheme	Process load statistics and compute scale-out/in prediction scheme shall be supported
Req-A.037	Identification of unloaded/overloaded VMs	Identification of unloaded/overloaded VMs shall be supported
Req-A.038	Robustness	The Cloud Data Centre shall have a robust, resilient architecture in line with standard industry requirements
Req-A.039	High availability	The data centre shall ensure high availability i.e., high uptime and low recovery time
Req-A.040	Fault Tolerance	Individual nodes going down should not affect the functionality of the whole Data Centre
Req-A.041	Reliable migration of virtualized functions	Reliable migration of virtualized functions shall be supported
Req-A.042	SLA support	Cloud infrastructure shall support the SLA requirements for performance
Req-A.043	Scaling performance	The system shall be able to scale dynamically to meet the loading conditions.
Req-A.044	Traffic latency in Data Centre	The traffic latency in the Data Centre shall be minimized below agreed SLA requirements
Req-A.045	Scalable and seamless migration of instances within one Data Centre	The scalable and seamless migration of instances within one Data Centre shall be supported
Req-A.046	Scalable and seamless migration of instances between different Data Centres	The scalable and seamless migration of instances between different Data Centre shall be supported
Req-A.047	Prioritised handling of traffic within a Data Centre	Different levels of priority on handling traffic within a Data Centre shall be supported
Req-A.048	Security Control	The system shall meet security requirements: confidentiality, privacy, authentication, access control, integrity, availability, non-repudiation, auditability.
Req-A.049	Secure communication between nodes	The communication between cloud nodes has to be encrypted
Req-A.050	Different levels of privacy	Different levels of privacy depending on supported services shall be supported
Req-A.051	Facilitate fast deployment	Fast deployment shall be supported
Req-A.052	Compatibility with Legacy system	Compatibility with Legacy systems shall be supported

6.2.2 Domain B: Access Network Infrastructure Cloud

This Technical Domain includes all the features regarding the cloud infrastructure implementation in the access network (particularly in wireless environments). That includes the sharing of wireless nodes, backhaul links, etc. The service can be provided according to different schemes for QoS differentiation, according to traffic type and SLA contract. In Figure 6-3 the use-case supporting the Domain B is drawn. From this use-case, requirements were derived. The associated requirements are listed in the Sections below and the detailed specification of each requirement available in Appendix A.2.

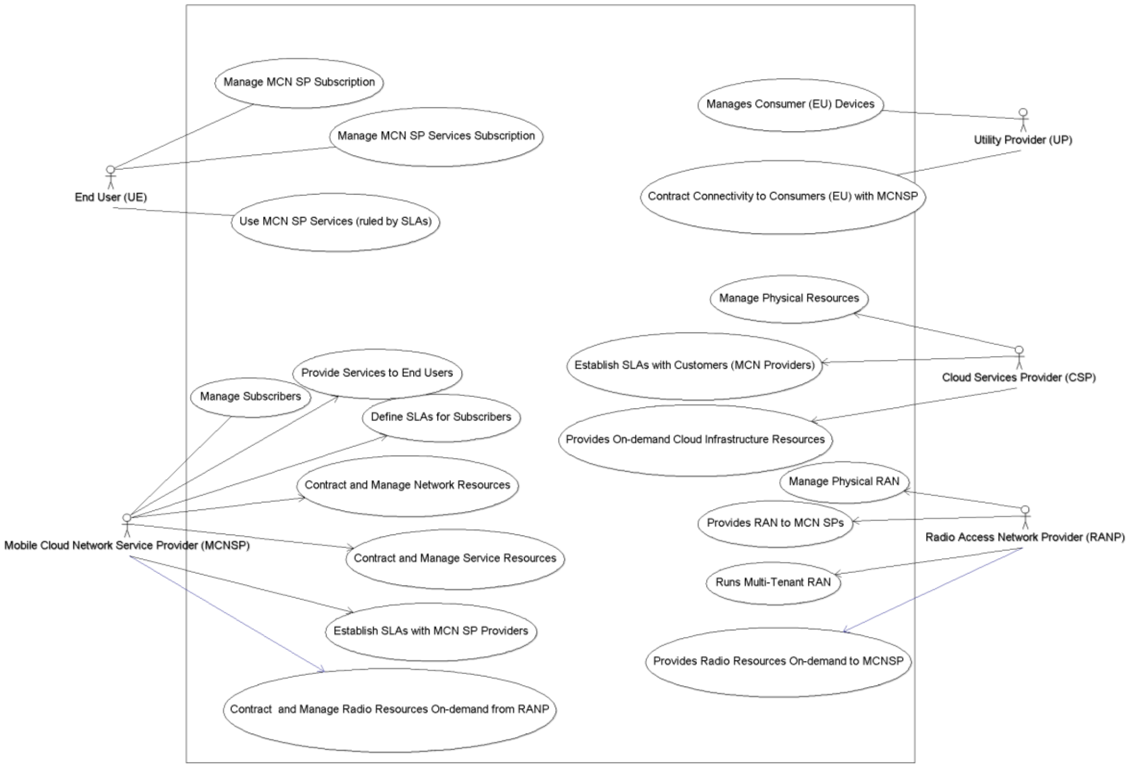

Figure 6-3 Technical Domain B Use Case Diagram.

Table 6-2 presents Technical Domain B requirements. The full specification of these requirements can be found in Appendix A.

Table 6-2 Technical Domain B Requirements

Requirement ID	Name	Brief Description
Req-B.001	Seamless mobility	The network shall support seamless handover between heterogeneous wireless access technologies.
Req-B.002	Application mappings	The system shall be able to map applications into different service classes.
Req-B.003	Self-organisation	The system shall be able to configure itself in a self-organised way.
Req-B.004	Infrastructure sharing	The system shall be able to share network elements among operators (e.g., antennas, backhaul links, BBU-pools) to provide wireless connectivity to its end-users.
Req-B.005	Heterogeneity	The system shall be able to provide end-users connectivity via multiple wireless access technologies (e.g. 2G, 3G, 4G and WiFi).
Req-B.006	Interoperability	The system shall support interoperability between the available heterogeneous wireless access networks and legacy mobile core networks.
Req-B.007	Resource Allocation On-demand	The system shall be able to allocate physical resources on-demand.
Req-B.008	Elasticity	The system shall be able to dynamically variate the allocated resources within one or multiple wireless access technologies to meet variable offered traffic and SLA contracts.
Req-B.009	Energy-efficiency	The system shall be able to allocate resources energy-efficiently to guarantee a given performance
Req-B.010	RANaaS	The system shall be able to offer RAN as a Service (RANaaS).
Req-B.011	Load balancing	The system shall be able to balance load within components of the same or various wireless access technologies (e.g., antenna, BBU).
Req-B.012	Components connectivity	The system shall guarantee connectivity between network components (e.g., BBU-RRH connectivity).
Req-B.013	Manageability	The cloud controller shall be able to dynamically configure and manage any component of the network.
Req-B.014	Topology knowledge	The system shall be able to provide static/dynamic information on the topology and characteristics of its participants of the RAN.
Req-B.015	SLA support	The system shall support a Service Level Agreement (SLA) with monitoring facilities.
Req-B.016	Traffic pattern	The system shall be able to estimate geographic and temporal offered traffic distribution.
Req-B.017	Location and Movement of End Users in order to initiate/maintain RAN topological changes	The system shall be able to monitor and process the location and movement of End Users used to initiate/maintain RAN topological changes.
Req-B.018	Robustness	The system shall be robust to changes, their impact in the performance of the network being minimised.
Req-B.019	Resiliency	The system shall be resilient to changes, their impact in the performance of the network being minimised.
Req-B.020	Redundancy	The components shall be redundant, existing other ones that may immediately substitute them when needed.

Req-B.021	Connection minimum capacity	Connectivity between network nodes (e.g., BBU-RRH link) should support a minimum requested capacity.
Req-B.022	Connection maximum delay	Connectivity between network nodes (e.g., BBU-RRH link) should support a maximum requested delay.
Req-B.023	Support of Authentication, Authorisation, Accounting, Confidentiality and Integrity	The system shall have the capability of supporting Authentication, Authorisation, Accounting, Confidentiality and Integrity.
Req-B.024	Different level of privacy depending on supported services	The system shall be able to support different levels of privacy depending on the supported services.
Req-B.025	Cost efficiency	Cost-efficient services and applications from the user perspective (e.g., usage of free connectivity vs. paid one).
Req-B.026	Time efficiency	The services and applications shall be time efficiently provided to users.
Req-B.027	Legacy support	The system shall be able to support legacy technologies (2G, 3G).

6.2.3 Domain C: Mobile Core Network Cloud

This Technical Domain includes all the features regarding the implementation of an EPC Mobile Core Network over a Cloud infrastructure, which is referenced in this section with the acronym MCNC. Figure 6-4 depicts the reference use case diagrams for this domain and the relationships between all relevant stakeholders, in particular, the relationship between MCSNP and CSP.

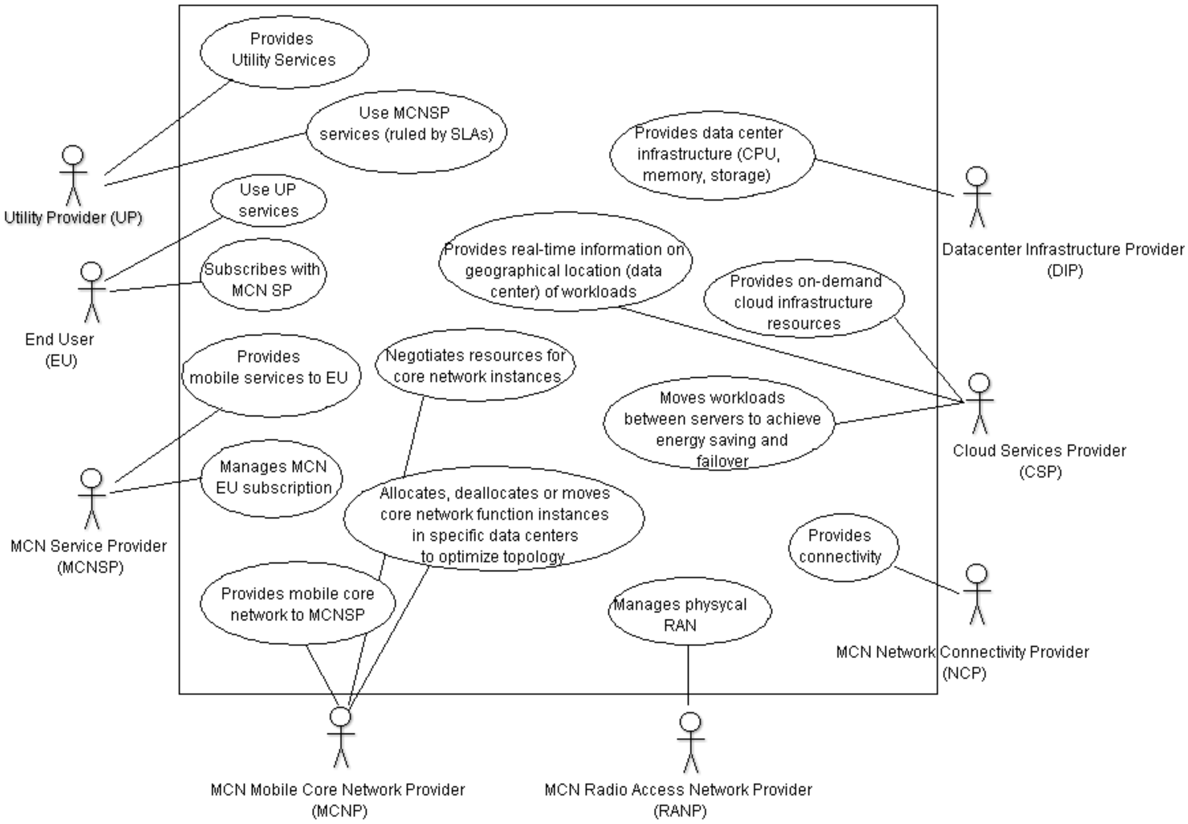

Figure 6-4 Technical Domain C Use Case Diagram

Table 6-3 presents Technical Domain C requirements. The full specification of these requirements can be found in Appendix A.

Table 6-3 Technical Domain C Requirements

Requirement ID	Name	Brief Description
Req-C.001	Dynamic and on demand creation of mobile network	The system shall support dynamic and on demand creation of a mobile network (RAN and EPC)
Req-C.002	Dynamic adaptation to topological/architectural changes	The system shall support dynamic adaptability to topological/architectural changes
Req-C.003	Elasticity	The system shall support network elasticity, with scaling out/in of EPC virtual instances, to cope with the variability of number of users, traffic load and user mobility
Req-C.004	Energy efficiency	The system shall be able to exploit cyclical traffic patterns to optimize energy consumption
Req-C.005	Scalable distributed mobility management	The system shall support scalable distributed mobility management solutions within the same/ across different MCNC
Req-C.006	Scalable service continuity	The system shall support scalable service continuity solutions within the same/ across different MCNC
Req-C.007	MTC load balancing	The system shall support MTC load balancing over time
Req-C.008	Optimisation of SLA and charging models	The system shall optimize SLA and charging models in order to take into account conditions and the overall costs thresholds (maximum amount of financial resources) that a Utility Provider is willing to pay for the access and use of the MTC devices
Req-C.009	Charging based on network volume and time of the day	The system shall support charging based on network volume and time of the day
Req-C.010	Mapping EPC functions	The system shall support the mapping of EPC function instances to VMs
Req-C.011	EPC virtual instances management	The system shall support for flexible, dynamic, fast and scalable allocation, de-allocation and management of EPC function instances
Req-C.012	VM migration together with its EPC instances to distribute load between VM host systems	The system shall support the complete Migration of an EPC instance to a different host, possibly located in a different Data Centre, in case of host system load
Req-C.013	Aggregation and migration of EPC instances to enable VM host shutdown	The system shall support complete Migration of an EPC instance to a different VM host, possibly located in a different Data Centre, to aggregate multiple EPC instances on few VM host systems and save power by shutting down some host systems
Req-C.014	Partial migration of EPC instances	The system shall support partial migration of an EPC instance in case of overloaded EPC instance (temporarily distribute subscriber context between multiple EPC instances of the same type and ID)
Req-C.015	RAN topology exposure	The system shall enable the retrieving/providing of the topological information of the physical RAN (i.e. location of eNBs)
Req-C.016	Data centre topology exposure	The system shall enable the retrieving/providing of the topological location of the Data Centres

Requirement ID	Name	Brief Description
Req-C.017	Topology-driven EPC instance placement	The system shall support the placement of instance(s) into the global topology picture (Data Centre selection)
Req-C.018	Location of EPC instances update	The system shall update the location information for the EPC function instances (e.g. after a migration)
Req-C.019	Maintain large- and small-scale connectivity for EPC virtual instances migration	The system shall support the set-up of proper inter-DC or inter-server (i.e., intra-DC) connectivity for EPC virtual instances migration
Req-C.020	Suitable Identifier and Address handling for migrated EPC virtual instances	The system shall support adaptation of address and identification information for migrated EPC virtual instances
Req-C.021	Backward compatible traffic indirection	The system shall support inter-working with transport network to enforce rules for traffic indirection, to keep traffic routing consistent even in case of migration of EPC virtual instances
Req-C.022	O&M API for MCNC controller	The system shall provide simple APIs for O&M for MCNC controller
Req-C.023	Interfaces for service and cloud layer	The system shall support of interfaces to communicate with service and cloud layer
Req-C.024	Configuration and addressing of EPC function instances	The system shall support configuration of the virtual EPC function instances and their addressing
Req-C.025	Monitor, collect and process MTC measurements in order to initiate/maintain EPC topological changes.	The system shall monitor, collect and process MTC measurements on an event and periodic basis that can be used to initiate/maintain EPC topological changes.
Req-C.026	Real-time location monitoring of EPC virtual instances	The system shall monitor the location of virtual EPC function instances in real-time (or near-real-time)
Req-C.027	Real-time load monitoring in virtual EPC instances	The system shall monitor in real time the load in virtual EPC function instances
Req-C.028	EPCaaS service quality monitoring	The system shall monitor the service quality
Req-C.029	MCNC system stability monitoring	The system shall monitor the MCNC system stability
Req-C.030	Load monitoring for statistics motivated scaling	The system shall monitor and process load statistics and compute scale-out/in prediction scheme
Req-C.031	VM Host (running EPC instances) –level observation of low/high load	The system shall be able to identify unloaded/overloaded VM host systems running virtual EPC function instances
Req-C.032	System announcement of EPC updates	The system shall support the announcement of birth/death event of virtual EPC function instance(s) to the relevant EPC functions (enable/disable selection)
Req-C.033	Location and Movement of End Users in order to initiate/maintain EPC topological changes	The system shall be able to monitor and process the location and movement of End Users used to initiate/maintain EPC topological changes

Requirement ID	Name	Brief Description
Req-C.034	High reliability of virtual EPC	The system shall support high reliability and robustness for the Soft-EPC (transient failures, node failures)
Req-C.035	Reliable scaling of EPC function instances	The system shall handle of scaling in/out without downtime or user experience degradation
Req-C.036	Upgrades with no downtime	The system shall support incremental software/release upgrades on virtual EPC function instances shall be possible without downtime
Req-C.037	Reliable migration of virtualized EPC network functions	The system shall support reliable migration of virtual EPC function instances
Req-C.038	Reliable distributed mobility management	The system shall support reliable distributed mobility management solutions within the same/ across different MCNC
Req-C.039	Reliable service continuity	The system shall support reliable service continuity solutions within the same/ across different MCNC
Req-C.040	MCNC UP latency	The EU traffic latency in the MCNC (i.e. the latency of a EU packet measured between the ingress and the egress point in the virtualized infrastructure within the MCNC) shall be minimized
Req-C.041	MCNC CP latency	The response time of a virtualized function (i.e. MME, PGW) hosted in the MCNC for processing Control Plane traffic shall be minimized
Req-C.042	Seamless migration of EPC function instances	The system shall support scalable and seamless migration of a EPC function (i.e. MME, PGW) hosted in the MCNC between different physical servers
Req-C.043	Near-real time elasticity	The system shall support of near-real time network elasticity, i.e. the increase/decrease of allocated resources for EPC functions should follow the increase/decrease of load in near-real time.
Req-C.044	Seamless distributed mobility management	The system shall support seamless distributed mobility management solutions within the same/ across different MCNC
Req-C.045	Seamless service continuity solutions	The system shall support seamless service continuity solutions within the same/ across different MCNC
Req-C.046	Authentication, Authorisation, Confidentiality and Integrity	The system shall support Authentication, Authorisation, Confidentiality and Integrity
Req-C.047	Different priority levels	The system shall support different levels of privacy depending on the supported services, e.g., IMSaaS, DSNaaS
Req-C.048	Compatibility and Legacy support	The system shall support compatibility with Legacy system supporting a smooth migration path
Req-C.049	User mobility and bandwidth availability prediction algorithms	The system shall support accurate user mobility and bandwidth availability prediction algorithms
Req-C.050	Fast deployment	The system shall facilitate fast deployment
Req-C.051	COTS hardware support	MCNC shall be able to run on COTS hardware, to possibly exploit economies of scale inside Data Centres and thus reducing CAPEX
Req-C.052	Interworking with legacy EPC	The additional operations required by MCNC enhancements on existing EPC components and O&M shall be minimized

Requirement ID	Name	Brief Description
Req-C.053	Compliant to 3GPP TS.22.101	The systems shall be compliant to requirements defined in 3GPP TS 22.101
Req-C.054	Compliant to 3GPP TS.23.401	The systems shall be compliant to 3GPP TS 23.401

6.2.4 Domain D: IMS/OSS/BSS/VAS as a Service

This Technical Domain includes all the features regarding the implementation of IMS (IP Multimedia Subsystem), OSS (Operational Support Systems), BSS (Business Support System) or VAS (Value Added Services) platforms over a Cloud infrastructure. That includes the implementation of platforms of those areas over a Cloud Infrastructure. Examples:

- IMS - IP Multimedia Subsystem
- OSS - Operational Support Systems (Monitoring, Provisioning, SLA Mgm, etc.)
- BSS - Operational Support Systems (Charging/Billing, CRM, Catalogs, etc.)
- VAS - Value Added Services (Location, M2M, Digital Signage, AAA, etc.)

Figure 6-5 depicts the UML Use Case Diagram that supports the Domain D perspective.

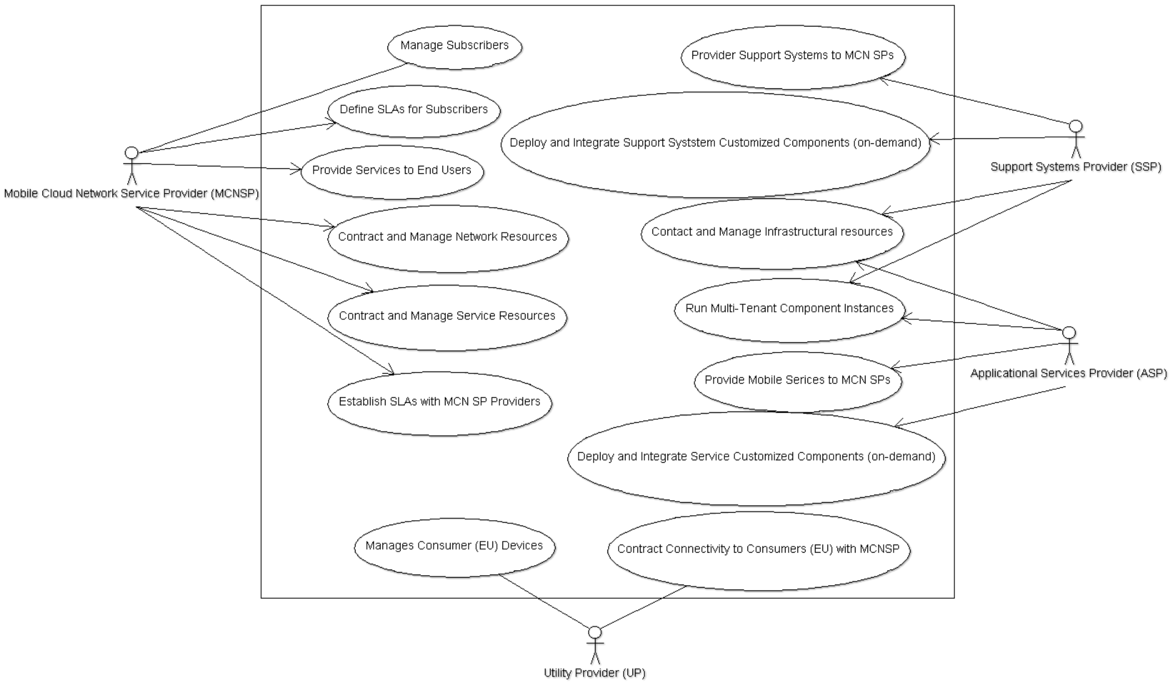

Figure 6-5 Technical Domain D Use Case Diagram

Table 6-4 presents Technical Domain D requirements. The full specification of these requirements can be found in Appendix A.

Table 6-4 Technical Domain D Requirements

Requirement ID	Name	Brief Description
Req-D.001	Get location information	The system shall provide the location information of an user
Req-D.002	Provide connectivity information	The system shall provide connectivity information
Req-D.003	Provide SLA thresholds	The system shall provide SLA thresholds information
Req-D.004	Create and manage end-to-end SLAs	The system shall create and manage end-to-end SLAs
Req-D.005	Support end-to-end Rating and Charging	The system shall support end-to-end Rating and Charging
Req-D.006	Create content cache	The system shall be able to create content caches
Req-D.007	Reallocate content cache	The system shall be able to reallocate content caches taking into account the geographical proximity of users and amount of video traffic associated with them
Req-D.008	Support end-to-end QoS/QoE	The system shall be able to provide end-to-end QoS/QoE support
Req-D.009	Create mobility gateways	The system shall be able to create mobility gateways
Req-D.010	Locate mobility gateways	The system shall be able to locate mobility gateways
Req-D.011	Support Follow-me cloud services	The system shall be able to support Follow-me cloud services
Req-D.012	Support IMS (IP Multimedia Services) services	The system shall be able to support IMS services
Req-D.013	Support DSN (Digital Signage Network) services	The system shall be able to support DSN services
Req-D.014	Support service continuity	The system shall be able to support the continuity of a service when a user roams either within one administrative domain operated by one MCNSP, or between two or more administrative domains operated by different MCNSPs
Req-D.015	Support pay as you go services	The system shall be able to support pay as you go services, where the End User pays only for the time that is using the provided service
Req-D.016	Support communication support for services	The system shall be able to support communication support for supported services
Req-D.017	Support cooperation with social networking services	The system shall be able to support cooperation of social networking services with apps to generate large user generated content
Req-D.018	Create and manage Follow-me cloud service instances	The system shall be able to create and manage Follow-me cloud service instances
Req-D.019	Create and manage IMS service instances	The system shall be able to create and manage IMS service instances
Req-D.020	Create and manage DSN service instances	The system shall be able to create and manage DSN service instances
Req-D.021	Provision a Cloud Storage Manager	The system shall be able to provision a Cloud Storage Manager
Req-D.022	Provision a Container Manager	The system shall be able to provision a Container Manager
Req-D.023	Provision a Resources Orchestrator	The system shall be able to provision a Resources Orchestrator
Req-D.024	Provision a QoS/QoE manager	The system shall be able to provision a QoS/QoE manager
Req-D.025	Provision a Mobility Support Manager	The system shall be able to provision a Mobility Support Manager
Req-D.026	Provision a ICN Resources Manager	The system shall be able to provision a ICN Resources Manager
Req-D.027	Provision a Mobile Content Delivery Networks (Mobile	The system shall be able to provision a Mobile Content Delivery Networks (Mobile CDN) resources Manager

Requirement ID	Name	Brief Description
	CDN) resources Manager	
Req-D.028	Provision a Services Manager	The system shall be able to provision a Services Manager, such as an IMS, DSN and Follow-me cloud services manager
Req-D.029	Provision a SLA manager	The system shall be able to provision a SLA manager
Req-D.030	Provision a Rating/Charging manager	The system shall be able to provision a Rating/Charging manager
Req-D.031	Get Follow-me cloud service instances status	The system shall be able to get the status of the Follow-me cloud service instances
Req-D.032	Get Follow-me cloud service instances utilisation	The system shall be able to get the utilisation of the Follow-me cloud service instances
Req-D.033	Get IMS service instances status	The system shall be able to get the status of the IMS service instances
Req-D.034	Get IMS service instances utilisation	The system shall be able to get the utilisation of the IMS service instances
Req-D.035	Get DSN service instances status	The system shall be able to get the status of the DSN service instances
Req-D.036	Get DSN service instances utilisation	The system shall be able to get the utilisation of the DSN service instances
Req-D.037	Get utilisation of the Cloud Storage Manager	The system shall be able to provision a Cloud Storage Manager
Req-D.038	Get utilisation of the Container Manager	The system shall be able to provision a Container Manager
Req-D.039	Get utilisation of the Resources Orchestrator	The system shall be able to get the utilisation of the Resources Orchestrator
Req-D.040	Get utilisation of the QoS/QoE manager	The system shall be able to get utilisation of the QoS/QoE manager
Req-D.041	Get utilisation of the Mobility Support Manager	The system shall be able to provide information about the Mobility Support Manager utilisation
Req-D.042	Get utilisation of the ICN Resources Manager	The system shall be able to provide the utilisation of the ICN Resources Manager
Req-D.043	Get utilisation of the Mobile Content Delivery Networks (Mobile CDN) resources Manager	The system shall be able to provide utilisation of the Mobile Content Delivery Networks (Mobile CDN) resources Manager
Req-D.044	Get utilisation of the Services Manager	The system shall be able to provide information about the utilisation of the Services Manager, such as an IMS, DSN and Follow-me cloud services manager
Req-D.045	Get utilisation of the SLA manager	The system shall be able to provide information about the utilisation of the SLA manager
Req-D.046	Get utilisation of the Rating/Charging manager	The system shall be able to provide the utilisation of the Rating/Charging manager
Req-D.047	Reliable migration of Follow-me cloud service instances	The system shall support a reliable migration of Follow-me cloud service instances
Req-D.048	Reliable migration IMS service instances	The system shall support a reliable migration of IMS service instances
Req-D.049	Reliable migration of DSN service instances	The system shall support a reliable migration of DSN service instances
Req-D.050	Reliable support of services	The system shall support reliable IMS, DSN and Follow-me cloud services
Req-D.051	Reliable support of SLA provisioning	The system shall support reliable SLA provisioning
Req-D.052	Reliable support of rating and charging provisioning	The system shall support reliable support of rating and charging provisioning
Req-D.053	Seamless service continuity	The system shall support seamless service continuity solutions

Requirement ID	Name	Brief Description
	solutions	
Req-D.054	Support of different levels of QoS/QoE signalling and provisioning	The system shall support different levels of QoS/QoE signalling and provisioning
Req-D.055	Application expected response time	The system shall guarantee that the applications' specific expected time interval is complied.
Req-D.056	Application maximum delay	The system shall guarantee that applications support a maximum requested end-to-end delay.
Req-D.057	Application maximum jitter	The system shall guarantee that applications support a maximum requested jitter.
Req-D.058	Application minimum data rate	The system shall guarantee that applications support a minimum requested data rate.
Req-D.059	Application maximum loss rate	The system shall guarantee that applications support a maximum requested packet loss rate.
Req-D.060	Application maximum error rate	The system shall guarantee that applications support a maximum acceptable error rate.
Req-D.061	Support of Authentication, Authorisation, Accounting, Confidentiality and Integrity	The system shall support of Authentication, Authorisation, Accounting, Confidentiality and Integrity
Req-D.062	Different level of privacy depending on supported services	The system shall support different level of privacy depending on supported services
Req-D.063	Support of user friendly management and monitoring tools	The system shall support user friendly management and monitoring tools
Req-D.064	User friendly, easy-usage and simplicity of interfaces and APIs	The system shall support user friendly, easy-usage and simplicity of interfaces and APIs
Req-D.065	Compatibility with Legacy system supporting a smooth migration	The system shall support compatibility with Legacy system supporting a smooth migration

7 Conclusions and Future Work

The goal of this report has been to provide the groundwork for the research in the upcoming months of the project. We started this foundation in Section 2 with the compilation of the basic terminology to be used throughout the project. This terminology was divided into two groups according to the two main fields of work, that is, one related to business and usage and another related to technologies. These to fields of work will be brought together in the project by an agile (iterative) development process that is based on the *Volere* methodology.

This particular method applied in the project and derived from *Volere* has been described in Section 3. There we have emphasised that both technology and business consideration play crucial roles for the realisation of the project goal. Due to the demand that the development work is to start in Month 4 of the project we have first concentrated on the technology side, which is clearly based on networking and cloud computing, while the business side appears to be more speculative at the current stage. Nevertheless the chosen methodology will centrally include the business side that amalgamate both sides in the course of the project. The *Volere* process will provide the basis for this endeavour.

Based on this agreed proceeding we started in Section 4 with the definition of 5 well-chosen scenarios that had been elaborated from initially 40 draft scenario. The selection of these scenarios aimed at 2 different goals. First, they should cover all relevant aspects of the previous 40 scenarios with respect to technology. Second, they should present the project target in a comprehensive way avoiding overemphasising certain areas, for which we had a large number of scenarios, by the identification of the central research directions that we had discussed at the project meeting in Palermo.

From these scenarios (presuming the knowledge of the 40 draft scenarios) we have derived two kinds of first results. On the one hand, we came up with a number of stakeholders, which are related to technological components, however, with a potential for economic exploitation. This means that the distinction of stakeholders primarily results from possible interfaces that allow for the identification of separated offerings. Due to this selection scheme these stakeholders only provide a selection of all possible stakeholders but we can see them as the most fundamental ones for later business purposes. These stakeholders were presented in Section 4. They will provide the basis for further investigations on the economic perspective of the mobile cloud in Task 2.2.

On the other hand, we derive technical requirements. To ensure that all technological aspects are completely reflected in the requirements, we had introduced 4 technical domains: (A) Cloud Data Centre Infrastructure and Network Programmability (related to WP3), (B) Access Network Infrastructure Cloud (related to WP3), (C) Mobile Core Network Cloud (related to WP4) and (D) IMS/OSS/BSS/VAS as a Service (related to WP5). Since these technical domains are related to individual work package, the proceeding has ensured that each of these work packages could identify relevant requirements for their specific work, which will then be taken as basis for the research in these work packages.

Moreover, the conducted analysis will be taken as starting point for the following discussion of the overall MCN architecture, which will be done in Task 2.3 and assessed against the identified requirements. It is important to note that the requirements identified in this report will be tracked throughout the course of the entire project, however, this does not means that they are fixed once and forever. At this point we want to reemphasise that the MCN project has been conceptualised as agile. This is a necessary aspect since we have already mentioned that the business analysis is still at a starting point and that it connection to the technological analysis according to the *Volere* process is still due in main points. As a consequence this might mean that some of the requirements identified in this report could be dropped if their economic relevance appears to be insignificant while other not yet explicated requirements can come to the fore. However, this will be carefully examined and documented.

References

3GPP, 2013. TS 22.101 V12.4.0 Technical Specification Group Services and System Aspects (Release 12), s.l.: s.n.

3GPP, 2013. TS 23.401 General Packet Radio Service (GPRS) enhancements for E-UTRAN access (Release 12), s.l.: s.n.

Ayvazian, B., 2012. Market Opportunities for B2C Fourth-Generation MVNOs, s.l.: Heavy Reading.

Buyyaa, R. et al., 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. s.l., s.n.

Copeland, R., 2011. Modelling multi-MNO business for MVNOs in their evolution to LTE, VoLTE & advanced policy. Berlin, s.n.

Freeman, R. E., 1984. Strategic Management: A Stakeholder Approach. Pitman, Boston, Toronto: s.n.

IEEE, 1998. IEEE Guide for Developing System Requirements Specifications, s.l.: s.n.

IEEE, 2012. 2012 IEEE Standards Style Manual, s.l.: s.n.

Mitchell, R. K., Agle, B. R. & Wood , D. J., 1997. Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts. The Academy of Management Review, 2(4).

Mobile Cloud Networking Project, 2012. Mobile Cloud Networking (MCN) Project. [Internett]
Available at: https://www.mobile-cloud-networking.eu/
[Funnet 15 3 2013].

OMG, 2011. Unified Modeling Language, version 2.4.1, s.l.: s.n.

Ponce de Leon, M. & Adhikari, A., 2010. A User Centric Always Best Connected Service Business Model for MVNOs. Waterford, s.n.

Pyramid Research, 2012. Romania Courts MVNOs. [Internett]
Available at: http://www.pyramidresearch.com/points/print/120221.htm
[Funnet 01 04 2013].

Robertson, S. & Robertson, J., 2006. Mastering the Requirements Process: Getting Requirements Right. 2nd edition red. s.l.:Addison Wesley Longman.

Robertson, S. & Robertson, J., 2012. Mastering the Requirements Process: Getting Requirements Right. 3rd edition red. s.l.:Addison-Wesley Longman.

Rummler, G. A. & Brache, A. P., 1995. Improving Performance: How to manege the white space on the organizational chart. San Francisco: Jossey-Bass.

Turban, E. et al., 2002. Electronic Commerce 2002: A Managerial Perspective. 2nd Edition red. s.l.:Prentice Hall.

Wireless Inteligence, u.d. Analysis: The MVNO model, global footprint and outlook. [Internett]
Available at: https://wirelessintelligence.com/analysis/2012/05/the-mvno-model-global-footprint-and-outlook/
[Funnet 11 03 2013].

Yrjo, R. & Rushil, D., 2011. Cloud Computing in Mobile Networks – Case MVNO. Berlin, s.n.

Appendix A. Detailed Requirements Specification

This Appendix provides the detailed specification of the requirements associated with each Technical Domain. It is based on the *Volere* requirements template (Robertson & Robertson, 2012). It includes the following fields:

- **Name**: Name of the requirement
- **Description**: Short statement of the intention of the requirement.
- **Rationale**: Justification of the requirement
- **Dependency**: List of other requirements that have some dependency on this one
- **Conflict**: Other requirements that cannot be implemented if this one is
- **Fit Criterion**: Measurement of the requirement such that it is possible to test if the solution matches the original requirement
- **Type**: Functional, Non-functional or Other
- **Severity**: Mandatory, optional or conditional.

A.1 Technical Domain A Requirements

Req-A.001

Name	Virtualisation
Description	The functionality for EPC and Mobile cloud shall be virtualizable
Rationale	Its basis for functioning cloud
Dependency	-
Conflict	-
Fit Criterion	The same functionality should be able to run on a VM and tested.
Type	Functional
Severity	Mandatory

Req-A.002

Name	Elasticity
Description	The cloud shall be elastic, i.e. shall be able to scale horizontally
Rationale	Cloud computing requirement
Dependency	-
Conflict	-
Fit Criterion	Scaling tests should be passed based on predetermined loads (tbd)
Type	Functional
Severity	Mandatory

Req-A.003

Name	On demand scaling
Description	Cloud should be able to scale on demand i.e., on rapid timescales
Rationale	Functional Requirement
Dependency	-
Conflict	-
Fit Criterion	Verify that cluster is able to scale at the user request
Type	Functional
Severity	Mandatory

Req-A.004

Name	Network Programmability
Description	Networking among the system components shall be changeable dynamically
Rationale	It ensures the flexibility to route packets dynamically, making the system compatible to ever changing routing rules
Dependency	-
Conflict	-
Fit Criterion	Routing tests to be performed with different configuration to verify this works
Type	Functional
Severity	Mandatory

Req-A.005

Name	Load Balancing
Description	The Cloud shall be able to balance load among different nodes
Rationale	Load Balancing is vital to insure QoS
Dependency	-
Conflict	-
Fit Criterion	Tests with varying load and corresponding monitoring data is needed to verify this.
Type	Functional
Severity	Mandatory

Req-A.006

Name	Multitenancy
Description	Multiple instances of the software shall be able to run on each single physical node
Rationale	To enable running of heterogeneous virtualized software on any given node
Dependency	-
Conflict	-
Fit Criterion	Test runs should allow running of several different components on a single node
Type	Functional
Severity	Mandatory

Req-A.007

Name	Energy efficiency
Description	Energy efficiency shall be supported
Rationale	If the load patterns are cyclical, e.g. load differs from daytime to nighttime, energy can be saved by scaling the capacity in and switching off pysical Data centre servers on which virtual instances are no more deployed.
Dependency	-
Conflict	-
Fit Criterion	Verify whether the excess Data centre servers are switched off with no loss of functionalities.
Type	Functional
Severity	Mandatory

Req-A.008

Name	Configuration and management of virtual machines and their addressing
Description	Configuration and management of virtual machines and their addressing shall be supported to manage software-based functional blocks, as they can be virtually run from different locations and hardware.
Rationale	The number of active virtual machines can be possibly high, running from different locations and generic hardware. There should be a way to automatically configure and manage the virtual machines with a meaningful set of parameters, including their IP addresses and interfaces.
Dependency	-
Conflict	-
Fit Criterion	Verify whether the virtual machines and their addressing can be configured and managed
Type	Functional
Severity	Mandatory

Req-A.009

Name	Dynamic adaptability of topological/architectural changes
Description	Dynamic adaptability of topological/architectural changes shall be supported
Rationale	The dynamic adaptation of the topology and architecture of the cloud computing platform optimizes the operation of the platform by providing the ability to initiate and use instances and resources when needed and for the time that they are needed.
Dependency	-
Conflict	-
Fit Criterion	Verify whether the dynamic adaptability of topological/architectural changes is supported
Type	Functional
Severity	Mandatory

Req-A.010

Name	Dynamic migration of virtualized functions
Description	Dynamic migration of virtualized functions shall be supported
Rationale	If virtual instances are migrated to another server, possibly located in another Data Centre, for an autonomous decision taken by the Cloud, the change of location should be advertised to the cloud controller.
Dependency	-
Conflict	-
Fit Criterion	Verify whether the dynamic migration of the virtualized functions is supported
Type	Functional
Severity	Mandatory

Req-A.011

Name	Retrieving/providing the topological location of Data Centres
Description	Retrieving/providing the topological location of Data centres shall be supported
Rationale	The topological information of Data centres is needed in order to define, when needed, at which location the necessary virtual machines can be migrated,
Dependency	-
Conflict	-
Fit Criterion	Verify whether the topological location of Data centres can be retrieved.provided
Type	Functional
Severity	Mandatory

Req-A.012

Name	Dynamic placement of instances within a Data Centre
Description	Dynamic placement of instances within a Data Centre shall be supported
Rationale	The dynamic placement of instances within a Data centre is needed in order to scale up and down the provided computing, storge and network resources by a Data centre.
Dependency	-
Conflict	-
Fit Criterion	Verify the dynamic placement of instances within a Data Centre can be realized.
Type	Functional
Severity	Mandatory

Req-A.013

Name	Upgrading the location information of the instances (e.g., after migration) running on Data Centres
Description	Upgrading the location information of the VM instances (e.g., after migration) running on Data Centres shall be supported
Rationale	After the migration of the virtual instances it is required that their location is upgrated, such that they can be contacted when needed.
Dependency	-
Conflict	-
Fit Criterion	Verify that the location information of the virtual instances is upgraded after their migration
Type	Functional
Severity	Mandatory

Req-A.014

Name	Set-up a proper inter-Data Centre or inter-server (i.e., intra-Data Centre) connectivity
Description	Setting up a proper inter-Data Centre or inter-server (i.e., intra-Data Centre) connectivity shall be supported
Rationale	The connectivity between servers within a Data Centre and between Data Centres is required for the support of the services provided by the Data Centres.
Dependency	-
Conflict	-
Fit Criterion	Verify whether the connectivity within a Data Centre and between Data Centres is properly set-up.
Type	Functional
Severity	Mandatory

Req-A.015

Name	Adaptation of address and identification information for migrated instances
Description	Adaptation of address and identification information for migrated instances shall be supported
Rationale	After migration the address and identification information of the instances might change. Therefore it is needed to adapt this information after migration.
Dependency	-
Conflict	-
Fit Criterion	Verify whether the address and identification information of instances is adapted after migration.
Type	Functional
Severity	Mandatory

Req-A.016

Name	Inter-working with transport network to enforce rules for traffic indirection
Description	Inter-working with transport network to enforce rules for traffic indirection shall be supported
Rationale	In situations that the traffic needs to be redirceted it is needed rules should be enforced to realize this. This can only be provided by inter-working with the transport network.
Dependency	-
Conflict	-
Fit Criterion	Verify whether the enforced rules for traffic indirection are able to successfully redirect the traffic on the transport network.
Type	Functional
Severity	Mandatory

Req-A.017

Name	Dynamic Resource Allocation
Description	Various resources shall be dynamically allocated by cloud controller as per loading conditions.
Rationale	Services will be able to be supported only if Cloud Data Centre resources are able to allocate where they are needed and whenever they are needed.
Dependency	-
Conflict	-
Fit Criterion	Verify whether the cloud Data Centre resources are correctly allocated by the cloud controller.
Type	Functional
Severity	Mandatory

Req-A.018

Name	Supporting IaaS interfaces
Description	New IaaS interfaces shall be supported to allow interoperability of equipment, preserving investments.
Rationale	Uper cloud service layers, e.g., PaaS, EaaS, RaaS, can only use the services provided by the IaaS services via unified interfaces to allow interoperability of equipment, preserving software investments.
Dependency	-
Conflict	-
Fit Criterion	Verify whether the interfaces between IaaS and upper cloud service layers are provided.
Type	Functional
Severity	Mandatory

Req-A.019

Name	Allocate new Virtual Machines
Description	The system shall be able to create and allocate Virtual Machines as per functional requirements
Rationale	Virtual Machines are created to host different IaaS services
Dependency	-
Conflict	-
Fit Criterion	Verify if the virtual machine is created
Type	Functional
Severity	Mandatory

Req-A.020

Name	Modify existing Virtual Machines
Description	The system shall be able to modify existing Virtual Machines
Rationale	Regarding the concepts of elasticity, the virtual machines can be modified
Dependency	-
Conflict	-
Fit Criterion	Verify if the modifications to the virtual machine are executed
Type	Functional
Severity	Mandatory

Req-A.021

Name	Dispose Virtual Machines
Description	The system shall be able to dispose existing Virtual Machines
Rationale	In order to release IaaS resources virtual machines can be disposed
Dependency	-
Conflict	-
Fit Criterion	Verify if the virtual machine has been deleted
Type	Functional
Severity	Mandatory

Req-A.022

Name	Create Storage Resources
Description	The system shall be able to allocate new storage resources
Rationale	Regarding the elasticity concept this requirement enables the system to create new IaaS storage resources
Dependency	-
Conflict	-
Fit Criterion	Verify if the IaaS storage resources are created
Type	Functional
Severity	Mandatory

Req-A.023

Name	Modify Storage Resources
Description	The system shall be able to modify storage resources
Rationale	Regarding the concepts of elasticity, the IaaS storage resources can be modified
Dependency	-
Conflict	-
Fit Criterion	Verify if the modifications to the IaaS storage resources are executed
Type	Functional
Severity	Mandatory

Req-A.024

Name	Dispose Storage Resources
Description	The system shall be able to release storage resources
Rationale	In order to free resources, IaaS storage resources can be disposed
Dependency	-
Conflict	-
Fit Criterion	Verify if the IaaS storage resources are released
Type	Functional
Severity	Mandatory

Req-A.025

Name	Create Network Resources
Description	The system shall be able to allocate new network resources
Rationale	Many different services require network resources that have to be provided by IaaS
Dependency	-
Conflict	-
Fit Criterion	Verify if new network resources are provided
Type	Functional
Severity	Mandatory

Req-A.026

Name	Modify Network Resources
Description	The system shall be able to modify network resources
Rationale	Network resources can be modified to adapt to new requirements
Dependency	-
Conflict	-
Fit Criterion	Verify if network resources are modified
Type	Functional
Severity	Mandatory

Req-A.027

Name	Dispose Network Resources
Description	The system shall be able to release network resources
Rationale	Network resources can be released if they are not needed.
Dependency	-
Conflict	-
Fit Criterion	Verify if network resources are released.
Type	Functional
Severity	Mandatory

Req-A.028

Name	Data collection from Nodes
Description	There shall be a mechanism to collect data from individual nodes and send it back to collector node
Rationale	This forms the basis of monitoring and SLA support
Dependency	-
Conflict	-
Fit Criterion	Verify that individual node monitoring is working and nodes are reachable through collector node
Type	Functional
Severity	Mandatory

Req-A.029

Name	Data Aggregation and processing
Description	All monitoring data shall be gathered and processed
Rationale	This forms basis of monitoring and SLA support
Dependency	-
Conflict	-
Fit Criterion	Verify that nodes are reachable through collector node and data aggregation/processing works as intended
Type	Functional
Severity	Mandatory

Req-A.030

Name	SLA monitoring support
Description	Monitoring data shall be checked against SLA requirements to determine a possible violation
Rationale	Business Requirement
Dependency	-
Conflict	-
Fit Criterion	Set different SLA requirements and send different monitoring data (simulation) to the collector node to see SLA flagging works correctly
Type	Functional
Severity	Mandatory

Req-A.031

Name	Monitoring of the location of workloads
Description	Monitoring of the location of workloads in real-time (or near-real-time) shall be supported.
Rationale	The location of the generated traffic needs to be monitored in order to support the dynamic adaptation of the required virtualized resources.
Dependency	-
Conflict	-
Fit Criterion	Verify whether the location of the generated traffic is monitored.
Type	Functional
Severity	Mandatory

Req-A.032

Name	Monitoring VMs (location, resources)
Description	Monitoring of VMs (location, resources) shall be supported
Rationale	To operation of the virtual machines needs to be monitored, in order to measure its correct functionality, its location and used resources.
Dependency	-
Conflict	-
Fit Criterion	Verify whether the virtual machines are monitored.
Type	Functional
Severity	Mandatory

Req-A.033

Name	Monitoring of load in VMs
Description	Monitoring of load in VMs shall be supported.
Rationale	The utilisation of a VM can only be known if the load in VMs is monitored.
Dependency	-
Conflict	-
Fit Criterion	Given a virtual machine id, the system is able to return its utilisation level
Type	Functional
Severity	Mandatory

Req-A.034

Name	Monitoring of service quality
Description	Monitoring of service quality shall be supported
Rationale	Monitoring of service quality is essential to fulfil SLAs
Dependency	-
Conflict	-
Fit Criterion	Verify that the relevant parameters of service quality are adequately monitored in multiple scenarios.
Type	Functional
Severity	Mandatory

Req-A.035

Name	Monitoring of system stability
Description	Monitoring of system stability shall be supported.
Rationale	In order to monitor the system, it must be able to report its stability
Dependency	-
Conflict	-
Fit Criterion	Verify if the system reports its availability
Type	Functional
Severity	Mandatory

Req-A.036

Name	Process load statistics and compute scale-out/in prediction scheme
Description	Process load statistics and compute scale-out/in prediction scheme shall be supported
Rationale	The prediction schemes can operate accurately only if the monitored load statistics are used to scale-out/in the predicted resources.
Dependency	-
Conflict	-
Fit Criterion	Verify if the load statistics are monitored and used to control the prediction scheme.
Type	Functional
Severity	Mandatory

Req-A.037

Name	Identification of unloaded/overloaded VMs
Description	Identification of unloaded/overloaded VMs shall be supported.
Rationale	The system is able to monitor the VM in order to identify whether a VM is loaded or unloaded.
Dependency	-
Conflict	-
Fit Criterion	Verify if the loaded/unloaded state of a VM is monitored.
Type	Functional
Severity	Mandatory

Req-A.038

Name	Robustness
Description	The Cloud Data Centre shall have a robust, resilient architecture in line with standard industry requirements.
Rationale	Reliability requirement. The Cloud Data Centre should have a robust, resilient architecture inline with standard industry requirements
Dependency	-
Conflict	-
Fit Criterion	Verify that the functionality of the system remains unaffected after sending erroneous information to the co-ordinator node
Type	Non-Functional
Severity	Mandatory

Req-A.039

Name	High availability
Description	The data centre shall ensure high availability i.e., high uptime and low recovery time.
Rationale	Ensures QoS and SLA support. The data centre should ensure high availability i.e., high uptime and low recovery time
Dependency	-
Conflict	-
Fit Criterion	Test the efficiency of the system under peak loads
Type	Non-Functional
Severity	Mandatory

Req-A.040

Name	Fault Tolerance
Description	Individual nodes going down shall not affect the functionality of the whole Data Centre.
Rationale	Ensures QoS and SLA support, even when individual nodes are going down.
Dependency	-
Conflict	-
Fit Criterion	Verify that system keeps functioning after taking down random nodes in the cluster
Type	Non-Functional
Severity	Mandatory

Req-A.041

Name	Reliable migration of virtualized functions
Description	Reliable migration of virtualized functions shall be supported.
Rationale	The virtualized functions need to be migrated ensuring high reliability.
Dependency	-
Conflict	-
Fit Criterion	Verify the migrated functions are migrated reliably.
Type	Non-Functional
Severity	Mandatory

Req-A.042

Name	SLA support
Description	Cloud infrastructure shall support the SLA requirements for performance
Rationale	Business Requirement
Dependency	-
Conflict	-
Fit Criterion	Verify that SLA requirements are satisfied by running loads similar to production loads on the test system
Type	Non-Functional
Severity	Mandatory

Req-A.043

Name	Scaling performance
Description	The system shall be able to scale dynamically to meet the loading conditions.
Rationale	Business Requirement
Dependency	-
Conflict	-
Fit Criterion	Verify that new nodes are able to come up when load increases within the time stipulated by the SLA
Type	Non-Functional
Severity	Mandatory

Req-A.044

Name	Traffic latency in Data Centre
Description	The traffic latency in the Data Centre shall be minimized below agreed SLA requirements
Rationale	The latency of the traffic within the Data Centre needs to be minimized in order to optimize the communication procedures within the Data Centre.
Dependency	-
Conflict	-
Fit Criterion	Verify whether the latency of traffic within the Data Centre is minimized.
Type	Non-Functional
Severity	Optional

Req-A.045

Name	Scalable and seamless migration of instances within one Data Centre
Description	The scalable and seamless migration of instances within one Data Centre shall be supported
Rationale	The migration of instances within the Data Centre needs to be done in a scalable way and in such a way that the user does not experience any service quality degradation.
Dependency	-
Conflict	-
Fit Criterion	Verify the instances are migrated within the Data Centre seamlessly.
Type	Non-Functional
Severity	Mandatory

Req-A.046

Name	Scalable and seamless migration of instances between different Data Centres
Description	The scalable and seamless migration of instances between different Data Centre shall be supported
Rationale	The migration of instances between Data Centre needs to be done in a scalable way and in such a way that the user does not experience any service quality degradation.
Dependency	-
Conflict	-
Fit Criterion	Verify the instances are migrated between different Data Centres seamlessly.
Type	Non-Functional
Severity	Optional

Req-A.047

Name	Prioritised handling of traffic within a Data Centre
Description	Different levels of priority on handling traffic within a Data Centre shall be supported.
Rationale	Traffic belonging to certain services, or users can require different treatment/forwarding priority than traffic belonging to other services or user.
Dependency	-
Conflict	-
Fit Criterion	Verify whether different levels of handling traffic within a Data Centre is supported.
Type	Non-Functional
Severity	Mandatory

Req-A.048

Name	Security Control
Description	The system shall meet security requirements: confidentiality, privacy, authentication, access control, integrity, availability, non-repudiation, auditability.
Rationale	The system meets generic security requirements such as confidentiality, privacy, authentication, access control, integrity, availability, non repudiation, auditability, etc
Dependency	-
Conflict	-
Fit Criterion	Verify that basic security testing in the system passes
Type	Non-Functional
Severity	Mandatory

Req-A.049

Name	Secure communication between nodes
Description	The communication between Cloud nodes shall be encrypted.
Rationale	Security Requirement
Dependency	-
Conflict	-
Fit Criterion	Verify that data being sent to different nodes in the cluster is encrypted by sniffing out sample packets from inter-node communication
Type	Non-Functional
Severity	Mandatory

Req-A.050

Name	Different levels of privacy
Description	Different levels of privacy depending on supported services shall be supported.
Rationale	Not all the services require the same level of privacy, thus the system should have the possibility to provide different privacy levels.Verify that the system offers different levels of privacy
Dependency	-
Conflict	-
Fit Criterion	Verify that different levels of privacy can be supported.
Type	Non-Functional
Severity	Optional

Req-A.051

Name	Facilitate fast deployment
Description	Fast deployment shall be supported.
Rationale	The developed system can be succesfully exploitated only when its fast deployment can be facilitated.
Dependency	-
Conflict	-
Fit Criterion	Verify whether facilities for fast deployment are available.
Type	Non-Functional
Severity	Optional

Req-A.052

Name	Compatibility with Legacy system
Description	Compatibility with Legacy systems shall be supported.
Rationale	The developed systems shall be able to cooperate with existing Legacy systems and support a smooth migration path.
Dependency	-
Conflict	-
Fit Criterion	Verify whether the developed system is compatible with Legacy sustems.
Type	Other
Severity	Optional

A.2 Technical Domain B Requirements

Req-B.001

Name	Seamless mobility
Description	The network shall support seamless handover between heterogeneous wireless access technologies.
Rationale	This is an inherent capability of wireless systems, enabling users to move freely, and have seamless connectivity through the best available wireless access technology.
Dependency	-
Conflict	-
Fit Criterion	Verify if the user manages to seamlessly handover between wireless access technologies.
Type	Functional
Severity	Mandatory

Req-B.002

Name	Application mappings
Description	The system shall be able to map applications into different service classes.
Rationale	Guarantee that communication requirements of applications are adequately supported by the underlying system. For example, a voice application must be mapped into a service class that guarantees low delays.
Dependency	-
Conflict	-
Fit Criterion	The application must be adequately supported by the communication system.
Type	Non-Functional
Severity	Mandatory

Req-B.003

Name	Self-organisation
Description	The system shall be able to configure itself in a self-organised way.
Rationale	This enables to have autonomous configuration, optimisation and healing of the system.
Dependency	-
Conflict	-
Fit Criterion	If changes occur in the network, the system shall react and self-configure itself.
Type	Functional
Severity	Mandatory

Req-B.004

Name	Infrastructure sharing
Description	The system shall be able to share network elements among operators (e.g., antennas, backhaul links, BBU-pools) to provide wireless connectivity to its end-users.
Rationale	This has the advantage (in terms of CAPEX and OPEX) of sharing network elements within MVNOs and MNOs which do not own an infrastructure in a certain geographical area.
Dependency	-
Conflict	-
Fit Criterion	Verify that the system is able to share network elements within various MNOs and MVNO.
Type	Functional
Severity	Mandatory

Req-B.005

Name	Heterogeneity
Description	The system shall be able to provide end-users connectivity via multiple wireless access technologies (e.g. 2G, 3G, 4G and WiFi).
Rationale	Due to the diversity of wireless access technologies, heterogeneity shall be supported by abstracting and virtualizing the base infrastructure in wireless, mobile core, and data centres.
Dependency	-
Conflict	-
Fit Criterion	Heterogeneity shall be enabled through multi-technology support.
Type	Functional
Severity	Mandatory

Req-B.006

Name	Interoperability
Description	The system shall support interoperability between the available heterogeneous wireless access networks and legacy mobile core networks.
Rationale	Due to diversity of deployed networks, Cloud RAN should be able to interact with other legacy mobile core networks.
Dependency	-
Conflict	-
Fit Criterion	Interoperability among other legacy mobile core networks must be supported.
Type	Functional
Severity	Mandatory

Req-B.007

Name	Resource Allocation On-demand
Description	The RANP shall be able to allocate virtual-radio resources and processing ones on-demand, as an answer to a specific request by the MCNSP.
Rationale	On-demand resource provisioning (virtual-radio and processing ones) by RANP improves the performance of the services provided by MCNSP in addition to a more efficient usage of resources (only allocating the needed resources, and being able to request new tenants at runtime).
Dependency	-
Conflict	-
Fit Criterion	Verify that if the MCNSP requests virtual-radio resources and processing ones, the RANP automatically provides them.
Type	Functional
Severity	Mandatory

Req-B.008

Name	Elasticity
Description	The system shall be able to dynamically variate the allocated resources within one or multiple wireless access technologies to meet variable offered traffic and SLA contracts.
Rationale	Elasticity improves the usage of system resources by allocating, at each time instant, only the needed resources, being able to adapt dynamically to variations of needs.
Dependency	Req-A.002, Req-A.003
Conflict	-
Fit Criterion	Verify that if there is an increase/decrease of needed resources, the system reacts and increases/decreases the allocated ones.
Type	Functional
Severity	Mandatory

Req-B.009

Name	Energy-efficiency
Description	The system shall be able to allocate resources energy-efficiently to guarantee a given performance.
Rationale	This guarantees that resources are energy-efficiently allocated and used.
Dependency	Req-A.007
Conflict	-
Fit Criterion	Verify that if the energy-consumption of a given resource is decreased, the performance is not anymore guaranteed.
Type	Functional
Severity	Mandatory

Req-B.010

Name	RANaaS
Description	The system shall be able to offer RAN as a Service (RANaaS).
Rationale	This enables to offer RANaaS to MNO or MVNOs which do not have the infrastructure. It can be provided through RAN virtualisation or through RAN sharing.
Dependency	-
Conflict	-
Fit Criterion	Verify that an MVNO is able to have a dedicated RAN to provide wireless connectivity to its end-users.
Type	Functional
Severity	Mandatory

Req-B.011

Name	Load balancing
Description	The system shall be able to balance load within components of the same or various wireless access technologies (e.g., antenna, BBU).
Rationale	This enables to allocate resources to components depending on their load. If the load increases on a given component, part of its load is moved (balanced) to another component of the same or different wireless access technology.
Dependency	Req-A.005
Conflict	-
Fit Criterion	Verify that, if the load on a given component exceeds its capacity, the system allocates the load to another component.
Type	Functional
Severity	Mandatory

Req-B.012

Name	Components connectivity
Description	The system shall guarantee connectivity between network components (e.g., BBU-RRH connectivity).
Rationale	This enables to balance load between antennas and BBUs.
Dependency	-
Conflict	-
Fit Criterion	Verify if a given RRH is able to be linked to any BBU.
Type	Functional
Severity	Mandatory

Req-B.013

Name	Manageability
Description	The cloud controller shall be able to dynamically configure and manage any component of the network.
Rationale	This enables to control any component of the network, essential to be able to allocate resources elastically and on-demand.
Dependency	-
Conflict	-
Fit Criterion	Verify if all components may be configurable remotely by the cloud controller.
Type	Functional
Severity	Mandatory

Req-B.014

Name	Topology knowledge
Description	The system shall be able to provide static/dynamic information on the topology and characteristics of its participants of the RAN.
Rationale	This enables to allocate resources on-demand, based on the needs, and improve the overall performance of the network.
Dependency	-
Conflict	-
Fit Criterion	Verify if the system triggers a notification when a given node appears or disappears, together with information on available links.
Type	Functional
Severity	Mandatory

Req-B.015

Name	SLA support
Description	The system shall support a Service Level Agreement (SLA) with monitoring facilities.
Rationale	This enables to guarantee SLAs to users, by the monitoring of specific aspects that define it.
Dependency	-
Conflict	-
Fit Criterion	Verify that, when a given agreed resource is not guaranteed anymore, a trigger notifies the responsible network component, so that it can correct the situation.
Type	Functional
Severity	Mandatory

Req-B.016

Name	Traffic pattern
Description	The system shall be able to monitor geographic and temporal offered traffic variations.
Rationale	The geographic and temporal monitoring of traffic is a capability that may improve the performance of the system, by dynamically adapting the allocated resources.
Dependency	-
Conflict	-
Fit Criterion	Verify that traffic variations are notified to specific network elements.
Type	Functional
Severity	Mandatory

Req-B.017

Name	Location and Movement of End Users in order to initiate/maintain RAN topological changes.
Description	The system shall be able to monitor and process the location and movement of End Users used to initiate/maintain RAN topological changes
Rationale	It is important that the system is aware when and where users are located and moving. This can be used to initiate/maintain RAN topological changes.
Dependency	-
Conflict	-
Fit Criterion	Verify whether the location and movement of End Users is monitored.
Type	Monitoring
Severity	Mandatory

Req-B.018

Name	Robustness
Description	The system shall be robust to changes, their impact in the performance of the network being minimised.
Rationale	This guarantees that any change or fault in the network is solved, guaranteeing that the impact in the performance of the network will be minimised as much as possible.
Dependency	Req-A.038, Req-A.039, Req-A.040
Conflict	-
Fit Criterion	Verify that, if a component has an error, the network is capable of minimising the impact in the performance of the network.
Type	Non-Functional
Severity	Mandatory

Req-B.019

Name	Resiliency
Description	The system shall be resilient to changes, their impact in the performance of the network being minimised.
Rationale	This guarantees that any change or fault in the network is corrected, guaranteeing that the impact in the performance of the network will be minimised as much as possible.
Dependency	-
Conflict	-
Fit Criterion	Verify that facing an unexpected behavior, the network is capable of minimising its impact in the network performance.
Type	Non-Functional
Severity	Mandatory

Req-B.020

Name	Redundancy
Description	The components shall be redundant, existing other ones that may immediately substitute them when needed.
Rationale	This guarantees that the functionalities of the network are guaranteed, even if the component that performs them has a fault, minimising situations where the functionality is "down" as much as possible.
Dependency	-
Conflict	-
Fit Criterion	Verify that, if a component has an error, the network is capable of recurring to another node to perform the functionality, minimising the impact in the performance of the network.
Type	Non-Functional
Severity	Mandatory

Req-B.021

Name	Connection minimum capacity
Description	The system shall guarantee that the connectivity between network nodes (e.g., BBU-RRH link) supports a minimum requested capacity.
Rationale	The minimum supported capacity within links is guaranteed, enabling adequate operation of the network.
Dependency	-
Conflict	-
Fit Criterion	The capacity shall be measured, and be guaranteed that it is above the established minimum value.
Type	Non-Functional
Severity	Mandatory

Req-B.022

Name	Connection maximum delay
Description	The system shall guarantee that the connectivity between network nodes (e.g., BBU-RRH link) supports a maximum requested delay.
Rationale	The maximum supported delay within links is guaranteed, enabling adequate operation of the network.
Dependency	-
Conflict	-
Fit Criterion	The delay shall be measured, and be guaranteed that it is below the established maximum value.
Type	Non-Functional
Severity	Mandatory

Req-B.023

Name	Support of Authentication, Authorisation, Accounting, Confidentiality and Integrity
Description	The system shall have the capability of supporting Authentication, Authorisation, Accounting, Confidentiality and Integrity.
Rationale	Authentication, Authorisation, Accounting, Confidentiality and Integrity are some of the most common and most important features for any telecommunications system.
Dependency	Req-A.048, Req-A.049
Conflict	-
Fit Criterion	Verify that the necessary interfaces for Authentication, Authorisation, Accounting, Confidentiality and Integrity are implemented.
Type	Non-Functional
Severity	Mandatory

Req-B.024

Name	Different level of privacy depending on supported services
Description	The system shall be able to support different levels of privacy depending on the supported services.
Rationale	The system should have the possibility to provide different privacy levels, as not all the services require the same level of privacy.
Dependency	-
Conflict	-
Fit Criterion	Verify that the system offers different levels of privacy.
Type	Non-Functional
Severity	Mandatory

Req-B.025

Name	Cost efficiency
Description	The services and applications shall be cost efficiently provided to users.
Rationale	This guarantees that, if a free wireless access technology (e.g., WiFi) is available to provide the same service as another one (e.g., LTE), then it shall be used.
Dependency	-
Conflict	-
Fit Criterion	Verify that, among the wireless technologies supporting a given service, the cheapest one is used.
Type	Non-Functional
Severity	Mandatory

Req-B.026

Name	Time efficiency
Description	The services and applications shall be time efficiently provided to users.
Rationale	This guarantees that, if a faster wireless access technology is available to provide the same service as another one, then it shall be used.
Dependency	-
Conflict	-
Fit Criterion	Verify that services and application respect the associated maximum time thresholds.
Type	Non-Functional
Severity	Mandatory

Req-B.026

Name	Legacy support
Description	The system shall be able to support legacy wireless access technologies (2G, 3G).
Rationale	Within a heterogeneous panoply of deployed and operating wireless access networks, mobile operators will be needed to be able to support all of them.
Dependency	-
Conflict	-
Fit Criterion	Verify if the system is able to transparently move users to legacy networks when needed.
Type	Other
Severity	Mandatory

A.3 Technical Domain C Requirements

Req-C.001

Name	Dynamic and on demand creation of mobile network
Description	The system shall support dynamic and on demand creation of a mobile network (RAN and EPC)
Rationale	The dynamic and on demand creation of a mobile network allows stakeholders, like Utility Providers to create and use a mobile network whenever they need it and for the time they need it.
Dependency	-
Conflict	-
Fit Criterion	Dynamic and on on demand creation of a mobile network can be proactively enabled (e.g. through an interface available on the O&M system), but also reactively enabled in case of for example, increase/decrease of the number of Utility Consumers.
Type	Functional
Severity	Mandatory

Req-C.002

Name	Dynamic adaptation to topological/architectural changes
Description	The system shall support dynamic adaptability to topological/architectural changes
Rationale	The dynamic adaptation of the topology and architecture of the mobile network (RAN and EPC) optimizes the operation of the mobile network by providing the ability to initiate and use mobile network instances and resources when needed and for the time that they are needed.
Dependency	Req-A.003, Req-A.002, Req-A.009
Conflict	-
Fit Criterion	Dynamic and on on demand creation and adaptation of mobile network can be proactively enabled (e.g. through an interface available on the O&M system), but also is reactively activated in case of for example, increase/decrease of the MTC devices and load.
Type	Functional
Severity	Mandatory

Req-C.003

Name	Elasticity
Description	The system shall support network elasticity, with scaling out/in of EPC virtual instances, to cope with the variability of number of users, traffic load and user mobility
Rationale	Elasticity optimizes the usage of system resources by allocating only the needed resources, being able to scale in/out the allocated CPU, memory and network capacity to follow the variations of load.
Dependency	Req-A.002
Conflict	-
Fit Criterion	Scaling can be manually triggered by the network administator (e.g. through an interface available on the O&M system), but also is automatically activated in case of load increase/decrease
Type	Functional
Severity	Mandatory

Req-C.004

Name	Energy Efficiency
Description	The system shall be able to exploit cyclical traffic patterns to optimize energy consumption
Rationale	If the load patterns are cyclic, e.g. load differs from daytime to nighttime, energy can be saved by scaling the capacity in during off-peak hour and switching off pysical servers on which virtual EPC function entities are no more deployed.
Dependency	Req-A.007
Conflict	-
Fit Criterion	Virtual functional entities are consolidated on a smaller number of physical servers and servers exceeting the required capacity are switched off (or put into some kind of energy saving mode) with no loss of functionalities. Moreover there shall be a way to describe energy saving activation criteria (e.g. at what time-of-day can energy saving start, for what EPC instances, how long it should last, what are the topological constraints, etc.)
Type	Functional
Severity	Mandatory

Req-C.005

Name	Scalable distributed mobility management
Description	The system shall support scalable distributed mobility management solutions within the same/ across different MCNC
Rationale	The current LTE mobility management solutions are centralized mobility anchor solutions. In order to optimize the mobility management solutions, i.e., decrease the load on the EPC and increase the user perdormance a scalable distributed management solution is needed, where the mobility anchor is placed as much as possible close to the location of a user that is roaming within the same or accross different MCNCs.
Dependency	-
Conflict	-
Fit Criterion	Distributed management solutions should be scalable and make use of mobility and bandwidth availability prediction mechanis in order to acquire and estimate the required information about where and when users are roaming and how much traffic they are generating. The distributed management solution can use LTE/IETF based approaches and/or make use of the virtualisation of the EPC mobility management functionalities, such as the P-GW, S-GW and MME.
Type	Functional
Severity	Mandatory

Req-C.006

Name	Scalable service continuity
Description	The system shall support scalable service continuity solutions within the same/ across different MCNC
Rationale	When users are roaming within the same/ across different MCNC should be able to exploitate a service in a similar way.
Dependency	-
Conflict	-
Fit Criterion	A service should be able to successfully run even when users are roaming within the same/ across different MCNC.
Type	Functional
Severity	Mandatory

Req-C.007

Name	MTC load balancing
Description	The system shall support MTC load balancing over time
Rationale	Currently MTC measurements are often collected and disseminated at the same time. Solutions need to be supported in order to balance the collection and dissemination of the MTC measurements over time.
Dependency	-
Conflict	-
Fit Criterion	The MTC load balancing solutions should not affect the accuracy of the collected and disseminated MTC measurements.
Type	Functional
Severity	Mandatory

Req-C.008

Name	Optimisation of SLA and charging models
Description	The system shall optimize SLA and charging models in order to take into account conditions and the overall costs thresholds
Rationale	SLA and charging models can be optimized by taking into account conditions and the overall costs thresholds (maximum amount of financial resources) that e.g., a Utility Provider is willing to pay for the access and use of the MTC devices
Dependency	Req-A.030
Conflict	-
Fit Criterion	Conditions and overal cost thesholds need to be defined and used in order to optimiza SLA and charging models. It should be possible to verify whether these conditions and cost thresholds are accurately used by the SLA and charging models.
Type	Functional
Severity	Mandatory

Req-C.009

Name	Charging based on network volume and time of the day
Description	The system shall support charging based on network volume and time of the day
Rationale	It should be possible to charge based on network volume and based on the time of the day that e.g., MTC measurements are collected and disseminated.
Dependency	Req-A.028, Req-A.029
Conflict	-
Fit Criterion	Verify whether charging is performed based on network volume and based on the time of the day that e.g., MTC measurements are collected and disseminated.
Type	Functional
Severity	Mandatory

Req-C.010

Name	Mapping EPC functions
Description	The system shall support the mapping of EPC function instances to VMs
Rationale	At deployment time, a translation/mapping shall be performed between the number and type of functional EPC function entities and a certain number and type of Virtual Machines, which will be activated in the Cloud. The mapping criteria shall be sufficiently flexible and expressive
Dependency	-
Conflict	-
Fit Criterion	A adequate number of VMs is spawned, according to the defined mapping rules defined
Type	Functional
Severity	Mandatory

Req-C.011

Name	EPC virtual instances management
Description	The system shall support for flexible, dynamic, fast and scalable allocation, de-allocation and management of EPC function instances
Rationale	The operator only needs to specify the number, type and configuration of EPC function instances it wants. The EPC funtion instances are then activated automatically exploting the Cloud infrastructure. Moreover, the operator should be able to manage the lifecycle of an virtual EPC function instance in a programmatic way, i.e. using an API
Dependency	Req-A.008, Req-A.017-027
Conflict	-
Fit Criterion	The lifecycle of vityual EPC function instances is centrally and programmatically operated through an User Interface and/or API
Type	Functional
Severity	Mandatory

Req-C.012

Name	VM migration together with its EPC instances to distribute load between VM host systems
Description	The system shall support the complete Migration of an EPC instance to a different host, possibly located in a different Data Centre, in case of host system load
Rationale	Resource requirements of virtual machines, which run on a single host system, may increase dynamically, hence the host system may not stand the aggregated load anymore. Distribution of load by moving selected VMs to a different host system can distribute load between multiple host systems. This avoids the host system becomes a bottleneck in meeting the resources demand of locally running VMs.
Dependency	-
Conflict	-
Fit Criterion	Loaded host systems or the controller/monitoring functions have means to offload VMs to a different host machine. An appropriate control API must be provided by the cloud control functions. After completed VM migration, load on the previuosly overloaded host system must have decreased.
Type	Functional
Severity	Mandatory

Req-C.013

Name	Aggregation and migration of EPC instances to enable VM host shutdown
Description	The system shall support complete Migration of an EPC instance to a different VM host, possibly located in a different Data Centre, to aggregate multiple EPC instances on few VM host systems and save power by shutting down some host systems
Rationale	Peak busy hours may require ad-hoc instantiation of additional EPC functions. As shut down of these instances cannot easily be accomplished, e.g. due to remaining subscriber states on these instances, cloud EPC operation can be optimized by aggregating VMs with low load to a few host systems. Such aggregation is accomplished by means of VM migration. After shutdown of host systems, which offloaded all VMs, overall power consumption should decrease.
Dependency	-
Conflict	-
Fit Criterion	Power consumption of a data centre decreases after VM aggregation and host system shutdown.
Type	Functional
Severity	Mandatory

Req-C.014

Name	Partial migration of EPC instances
Description	The system shall support partial migration of an EPC instance in case of overloaded EPC instance (temporarily distribute subscriber context between multiple EPC instances of the same type and ID)
Rationale	Unexpected and spontaneous increase of load in a particular VM may require immediate reaction and offload to avoid negative impact to system stability. Load can be distributed between multiple VMs, each running an instance of the same EPC component. Traffic to this EPC component must be dispatched accordingly between the multiple VMs.
Dependency	-
Conflict	-
Fit Criterion	After completed partial VM migration, load on the VM must have decreased and the system must have recovered from instability.
Type	Functional
Severity	Mandatory

Req-C.015

Name	RAN topology exposure
Description	The system shall enable the retrieving/providing of the topological information of the physical RAN (i.e. location of eNBs)
Rationale	The MCNC controller must know the geographical distribution of the eNBs to take optimized decisions on placement and relocation of EPS virtual instances.
Dependency	Req-B.014
Conflict	-
Fit Criterion	RAN topology is available as input to the MCNC controller via an interface
Type	Functional
Severity	Mandatory

Req-C.016

Name	Data centre topology exposure
Description	The system shall enable the retrieving/providing of the topological location of the Data Centres
Rationale	The MCNC controller must know the geographical distribution of the macro/mini Data centres on which the Cloud runs, to take optimized decisions on placement and relocation of EPS virtual instances.
Dependency	Req-A.010, Req-A.011
Conflict	-
Fit Criterion	Data centres topology is available as input to the MCNC controller via an interface
Type	Functional
Severity	Mandatory

Req-C.017

Name	Topology-driven EPC instance placement
Description	The system shall support the placement of instance(s) into the global topology picture (Data Centre selection)
Rationale	To optimize performance, especially in terms of latency of both control and user plane, it should be possible to place the virtual EPC function instances in a specific Data Centre, based on the topological information of both eNBs and Data centres
Dependency	Req-A.012
Conflict	-
Fit Criterion	Placement of EPC instances is performed depending on topological information of RAN and Data centres
Type	Functional
Severity	Mandatory

Req-C.018

Name	Location of EPC instances update
Description	The system shall update the location information for the EPC function instances (e.g. after a migration)
Rationale	If a virtual EPC funtion instance is migrated to another Data Centre, for an autonomous decision taken by the Cloud, e.g. load balancing or reaction to a failure, the change of location should be advertised to the MCNC controller. This is to allow the MCNC controller to always have up to date information for running its algorithm
Dependency	Req-A.010
Conflict	-
Fit Criterion	A migration of one or more EPC function instances triggers an update towards the MCNC controller
Type	Functional
Severity	Mandatory

Req-C.019

Name	Maintain large- and small-scale connectivity for EPC virtual instances migration
Description	The system shall support the set-up of proper inter-DC or inter-server (i.e., intra-DC) connectivity for EPC virtual instances migration
Rationale	Connections with VMs must not break after migration, independent of whether a VM has been migrated to a different host system within the same or in a different data centre. Even though connection endpoints may have different characteristics, such as topologically incorrect IP addresses, traffic routing to and from the migrated VM must be ensured.
Dependency	-
Conflict	-
Fit Criterion	Communication with an EPC instance is maintained after migration. The transport network has means to identify associated traffic of the migrated EPC instance and enforce appropriate forwarding policies.
Type	Functional
Severity	Mandatory

Req-C.020

Name	Suitable Identifier and Address handling for migrated EPC virtual instances
Description	The system shall support adaptation of address and identification information for migrated EPC virtual instances
Rationale	After migration of a VM and the associated EPC instance, the 3GPP specific idnetifier of the instance (e.g. MME identifier) as well as network-level addressing information, such as IP addresses, may not be updated and remain the same as before migration. The MCN must provide means to allow continuation of communication with a migrated EPC instance even if IP addresses turn into topologically incorrect IP addresses or identifiers are not updated.
Dependency	-
Conflict	-
Fit Criterion	Communication between a migrated EPC instance and in particular legacy EPC components must continue. Communication, addressing and identification must not break due to the migration of an EPC instance. Communication must be possible even if EPC instances do not update addressing or identification information.
Type	Functional
Severity	Mandatory

Req-C.021

Name	Backward compatible traffic indirection
Description	The system shall support inter-working with transport network to enforce rules for traffic indirection, to keep traffic routing consistent even in case of migration of EPC virtual instances
Rationale	The requirement about the continuity of communication with migrated EPC instances implies the introduction of a level of indirection to enable traffic routing without relying on the correctness of the IP address information in associated IP packets. Such technology for indirection must not assume re-engineering of the complete transport network but must be compatible with the exsting (legacy) transport network to a large amount.
Dependency	-
Conflict	-
Fit Criterion	Communication with migrated EPC instances continues while some network segments or routing domains between the communicating EPC endpoints are based on legacy technology, such as IP or MPLS routers.
Type	Functional
Severity	Mandatory

Req-C.022

Name	O&M API for MCNC controller
Description	The system shall provide simple APIs for O&M for MCNC controller
Rationale	The MCNC should expose simple yet powerful API towards the O&M system, which provides a way to both configure the MCNC controller and to retrieve statistics and counters from it
Dependency	-
Conflict	-
Fit Criterion	An external O&M system can interact with the MCNC with an API
Type	Functional
Severity	Optional

Req-C.023

Name	Interfaces for service and cloud layer
Description	The system shall support of interfaces to communicate with service and cloud layer
Rationale	The EPCaaS layer needs to be able to communicatie with the service (IMSaaS, DSNaaS) and cloud layer (IaaS) using specified interfaces.
Dependency	-
Conflict	-
Fit Criterion	Verify whether interfaces between service and cloud layer are available.
Type	Functional
Severity	Mandatory

Req-C.024

Name	Configuration and addressing of EPC function instances
Description	The system shall support configuration of the virtual EPC function instances and their addressing
Rationale	The number of active EPC instances can be possibly high. Hence, once they are activated, there shall be a way to automatically configure the EPC virtual instances with a meaningful set of parameters. These are both 3GPP specific parameters (e.g. identifiers, like the GUMMEI or timers) and IP addresses of their interfaces.
Dependency	Req-A.008, Req-A.015
Conflict	
Fit Criterion	Virtual EPC funtion instances and their interfaces are automatically configured, so that the operator will not need to configure them manually
Type	Functional
Severity	Mandatory

Req-C.025

Name	Monitor, collect and process MTC measurements in order to initiate/maintain EPC topological changes.
Description	The system shall monitor, collect and process MTC measurements on an event and periodic basis that can be used to initiate/maintain EPC topological changes.
Rationale	The MTC measurements need to be monitored, collected and processed on an event basis, e.g., alarm, or in a periodic basis, when charging and billing related information needs to be processed. These MTC measurements can be used to initiate/maintain EPC topological changes.
Dependency	-
Conflict	-
Fit Criterion	Verify if the MTC measurements can be monitored, collected and processed on an event and periodic basis.
Type	Functional
Severity	Mandatory

Req-C.026

Name	Real-time location monitoring of EPC virtual instances
Description	The system shall monitor the location of virtual EPC function instances in real-time (or near-real-time)
Rationale	In order to maintain accurate EPC topology information, the system should be able to monitor in real time (or near real time) the location of EPC instances.
Dependency	Req-A.031
Conflict	-
Fit Criterion	Verify whether the location of the EPC virtual instances is real time (or near real time) monitored
Type	Functional
Severity	Mandatory

Req-C.027

Name	Real-time load monitoring in virtual EPC instances
Description	The system shall monitor in real time the load in virtual EPC function instances
Rationale	Distribution of VMs to reduce load on a particular host system requires means to monitor load and resources utilisation with the accuracy of a host system.
Dependency	Req-A.033
Conflict	-
Fit Criterion	The monitoring function allows retrieving information about host system load
Type	Functional
Severity	Mandatory

Req-C.028

Name	EPCaaS Service quality monitoring
Description	The system shall monitor the service quality
Rationale	Service quality needs to be monitored and matched against contrainst values to identify te demand for optimisation.Migration of EPC instances may be motivated not only by local load on the host system, but in bypassing congestion in the transport network which enabled connectivity between the two EPC instances.
Dependency	Req-A.032
Conflict	-
Fit Criterion	Initiation of optimisation, e.g. load distribution, in case of low service quality. Decisions to move EPC instances to a different host system or data centre due to network load to improve e.g. end-to-end communication characteristics must be possible according to available graphs on load or congestion situation in the network.
Type	Functional
Severity	Mandatory

Req-C.029

Name	MCNC System stability monitoring
Description	The system shall monitor the MCNC system stability
Rationale	System stability, e.g. system stalling or message loss, needs to be monitored and matched against contrainst values to identify te demand for optioimisation.
Dependency	Req-A.032
Conflict	-
Fit Criterion	Initiation of optimisation, e.g. load distribution, in case of experienced system instability
Type	Functional
Severity	Mandatory

Req-C.030

Name	Load monitoring for statistics motivated scaling
Description	The system shall monitor and process load statistics and compute scale-out/in prediction scheme
Rationale	Repeated or scheduled events allow the generation of statistics and support the predicion of high load and associated demand for scale-out. Such predicion schemes allow scaling with low latency constraints, as the EPC has sufficient time to instantiate required EPC functions and announce the availability of these functions to the network.
Dependency	Req-A.036
Conflict	-
Fit Criterion	In-time instantiation of new ECP functions to allow distribution of load
Type	Functional
Severity	Mandatory

Req-C.031

Name	VM Host (running EPC instances) –level observation of low/high load
Description	The system shall be able to identify unloaded/overloaded VM host systems running virtual EPC function instances
Rationale	Administrative settings of attributes, which represent high/low load thresholds, allows automatic initiation of scale-out and scale-in when load exteeds a threshold or drops below the threshold respectively.
Dependency	Req-A.037
Conflict	-
Fit Criterion	Results in balanced system load. Avoid overloaded as well as underloaded EPC instances.
Type	Functional
Severity	Mandatory

Req-C.032

Name	System announcement of EPC updates
Description	The system shall support the announcement of birth/death event of virtual EPC function instance(s) to the relevant EPC functions (enable/disable selection)
Rationale	Instantiation of new and unique (unique EPC identifier) EPC instances or shut down of such instance must be announced to the remaining EPC to make new functions selecible and to remove functions, whcih have been shut down, from the list of available functions.
Dependency	-
Conflict	-
Fit Criterion	The EPC must have an accurate picture of available EPC functions.
Type	Functional
Severity	Mandatory

Req-C.033

Name	Location and Movement of End Users in order to initiate/maintain EPC topological changes.
Description	The system shall be able to monitor and process the location and movement of End Users used to initiate/maintain EPC topological changes
Rationale	It is important that the system is aware when and where users are located and moving. This can be used to initiate/maintain EPC topological changes.
Dependency	Req-B.017
Conflict	-
Fit Criterion	Verify whether the location and movement of End Users is monitored.
Type	Functional
Severity	Mandatory

Req-C.034

Name	High reliability of virtual EPC
Description	The system shall support high reliability and robustness for the Soft-EPC (transient failures, node failures)
Rationale	Currently deployed EPC solutions offer very high reliability, achieved with heavy HW redundancy. The Soft-EPC should aim at the same level of carrier-grade reliability. It should do this handling both transient failures of both EPC function instances and physical servers and permanent server failures.
Dependency	Req-A.032, Req-A.038-041
Conflict	-
Fit Criterion	No downtime experienced, no impact on user experience when a failure occurs both at VM or at server level
Type	Non-Functional
Severity	Mandatory

Req-C.035

Name	Reliable scaling of EPC function instances
Description	The system shall handle of scaling in/out without downtime or user experience degradation
Rationale	In case of scaling in/out the virtual EPC function instances, there should not be service interruption. Scaling should be a transparent operation for the end users
Dependency	Req-A.002, Req-A.003
Conflict	-
Fit Criterion	No downtime experienced, no impact on user experience when scaling in/out
Type	Non-Functional
Severity	Mandatory

Req-C.036

Name	Upgrades with no downtime
Description	The system shall support incremental software/release upgrades on virtual EPC function instances shall be possible without downtime.
Rationale	Since in MCNC there will be possibily many virtual EPC function instances providing the same function, is should be possible to perform SW upgrades on a subset of the VMs and continiung in an incremental way, not affecting the live service provided to the end user
Dependency	Req-C.024
Conflict	-
Fit Criterion	SW upgrades on one or more virtual EPC function instances are possible without downtime
Type	Non-Functional
Severity	Mandatory

Req-C.037

Name	Reliable migration of virtualized EPC network functions
Description	The system shall support reliable migration of virtual EPC function instances
Rationale	In order to support EPCaaS services to work fluently, the migration of virtual ized EPC network functions must be very reliable
Dependency	Req-C.012-014
Conflict	-
Fit Criterion	There must be a high percentage of successful migrations of virtualized EPC network functions
Type	Non-Functional
Severity	Mandatory

Req-C.038

Name	Reliable distributed mobility management
Description	The system shall support reliable distributed mobility management solutions within the same/ across different MCNC
Rationale	The developed distrinuted mobility management solutions need to operate reliably in such a way that the end user will not experince any signifficant service quality degradation when it roams within the same/ across different MCNC.
Dependency	Req-C.005
Conflict	-
Fit Criterion	There must be a high percentage of successful distributed mobility management operations/actions when an end user roams within the same/ across different MCNC.
Type	Non-Functional
Severity	Mandatory

Req-C.039

Name	Reliable service continuity
Description	The system shall support reliable service continuity solutions within the same/ across different MCNC
Rationale	The developed service continuity solutions need to operate reliably in such a way that the end user does not notice any difference in the service exploitation while roaming within the same/ across different MCNC.
Dependency	Req-C.006
Conflict	-
Fit Criterion	There must be a high percentage of successful service continuity operations/actions when an end user roams within the same/ across different MCNC.
Type	Non-Functional
Severity	Mandatory

Req-C.040

Name	MCNC UP latency
Description	The EU traffic latency in the MCNC (i.e. the latency of a EU packet measured between the ingress and the egress point in the virtualized infrastructure within the MCNC) shall be minimized
Rationale	The cloud-based MCNC should not worsen the latency of the user traffic with respect to the latency of a hardware-based, currently deployed solutions
Dependency	Req-A.044, Req-A.046, Req-A.047
Conflict	-
Fit Criterion	Latency of user packets into the MCNC is minimized
Type	Non-Functional
Severity	Optional

Req-C.041

Name	MCNC CP latency
Description	The response time of a virtualized function (i.e. MME, PGW) hosted in the MCNC for processing Control Plane traffic shall be minimized
Rationale	The performance of the MCNC with respect to the Control Plane processing can be expressed with the latency added by the MCNC in responding to a control message coming from the RAN or other external platform (e.g PCRF). This latency should be minimized, showing a optimal use of computing resources provided by the Cloud
Dependency	Req-A.044, Req-A.047
Conflict	-
Fit Criterion	Latency of control packets into the MCNC is minimized
Type	Non-Functional
Severity	Optional

Req-C.042

Name	Seamless migration of EPC function instances
Description	The system shall support scalable and seamless migration of a EPC function (i.e. MME, PGW) hosted in the MCNC between different physical servers
Rationale	There should be no downtime and ideally no packet loss when an active EPC virtual instance is migrated to a different server. This is particular important in case of SGW/PGW, since they handle user traffic
Dependency	Req-A.045, Req-A.046
Conflict	-
Fit Criterion	No downtime when migrating a EPC virtual instance on a different server
Type	Non-Functional
Severity	Optional

Req-C.043

Name	Near-real time elasticity
Description	The system shall support of near-real time network elasticity, i.e. the increase/decrease of allocated resources for EPC functions should follow the increase/decrease of load in near-real time.
Rationale	It is not strictly necessary to perform scaling in/out of the MCNC in real time, with a very fine time granularity. The capacity allocated MCNC should follow the demand in near-real time, also to avoid ping-pong effects (i.e. a VM is allocated for adding capacity and deallocated immediately after because a few users left the network)
Dependency	-
Conflict	-
Fit Criterion	Scaling is performed at coarse time intervals
Type	Non-Functional
Severity	Optional

Req-C.044

Name	Seamless distributed mobility management
Description	The system shall support seamless distributed mobility management solutions within the same/ across different MCNC
Rationale	The developed distrinuted mobility management solutions need to operate in such a way that the end user will not experince any signifficant service quality degradation when it roams within the same/ across different MCNC.
Dependency	Req-C.005
Conflict	
Fit Criterion	Verify whether the end user does not experience any signifficant service quality degradation when it roams within the same/ across different MCNC.
Type	Non-Functional
Severity	Optional

Req-C.045

Name	Seamless service continuity solutions
Description	The system shall support seamless service continuity solutions within the same/ across different MCNC
Rationale	The developed service continuity solutions need to operate in such a way that the end user does not notice any difference in the service exploitation while roaming within the same/ across different MCNC.
Dependency	Req-C.006
Conflict	
Fit Criterion	Verify whether the end user does not does not notice any difference in the service exploitation while roaming within the same/ across different MCNC.
Type	Non-Functional
Severity	Optional

Req-C.046

Name	Authentication, Authorisation, Confidentiality and Integrity
Description	The system shall support Authentication, Authorisation, Confidentiality and Integrity features/interfaces associated with the communication support of the EPCaaS users, e.g. an Application Provider, or an Utility Provider.
Rationale	Authentication, Authorisation, Confidentiality and Integrity are security features/interfaces that need to be supported in any telco system. They are strictly needed to provide fundamental security features like: access control, non-repudiation and auditability. In particular, these AAA, confidentiality and integrity features/interfaces should be used to support the communication procedures associated with the EPCaaS users, e.g. an Application Provider, or a Utility Provider.
Dependency	Req-A.048, Req-A.049
Conflict	-
Fit Criterion	Verify that the necessary interfaces for Authentication, Authorisation, Confidentiality and Integrity are implemented.
Type	Non-Functional
Severity	Optional

Req-C.047

Name	Different priority levels
Description	The system shall support different levels of privacy depending on the supported services, e.g., IMSaaS, DSNaaS
Rationale	Not all the services, e.g., IMSaaS, DSNaaS, require the same level of privacy, thus the system should have the possibility to provide different privacy levels to the EPCaaS users.
Dependency	Req-A.050
Conflict	-
Fit Criterion	Verify that the system offers different levels of privacy
Type	Non-Functional
Severity	Optional

Req-C.048

Name	Compatibility and Legacy support
Description	The system shall support compatibility with Legacy system supporting a smooth migration path
Rationale	The developed systems needs to be able to cooperate with existing Legacy systems and support a smooth migration path.
Dependency	-
Conflict	-
Fit Criterion	Verify whether the developed system is compatible with Legacy sustems.
Type	Non-Functional
Severity	Mandatory

Req-C.049

Name	User mobility and bandwidth availability prediction algorithms
Description	The system shall support accurate user mobility and bandwidth availability prediction algorithms
Rationale	The operation of the virtualized EPC depends severely on the accuracy of the developed user mobility and bandwidth availability prediction algorithms.
Dependency	-
Conflict	-
Fit Criterion	Verify whether the developed user mobility and bandwidth availability prediction algorithms operate accurately.
Type	Non-Functional
Severity	Mandatory

Req-C.050

Name	Fast deployment
Description	The system shall facilitate fast deployment
Rationale	The developed system can be succesfully exploitated only when its fast deployment can be facilitated.
Dependency	-
Conflict	-
Fit Criterion	Verify whether facilities for fast deployment are available.
Type	Non-Functional
Severity	Optional

Req-C.051

Name	COTS hardware support
Description	MCNC shall be able to run on COTS hardware, to possibly exploit economies of scale inside Data Centres and thus reducing CAPEX
Rationale	Leveraging economies of scale of the Cloud is essential for reducing the cost of an EPC solution. This will be only possible if the MCNC can run on “standard” COTS hardware, e.g. x86 platform, not requiring any hardware customisation.
Dependency	-
Conflict	-
Fit Criterion	MCNC runs on X86 servers
Type	Non-Functional
Severity	Mandatory

Req-C.052

Name	Interworking with legacy EPC
Description	The additional operations required by MCNC enhancements on existing EPC components and O&M shall be minimized
Rationale	If an operator runs a MCNC and a legacy EPC of the same or of a different vendor the two networks shall not only interwork, but also the O&M of the operator should not notice any difference between managing the MCNC and managing the legacy EPC.
Dependency	-
Conflict	-
Fit Criterion	No MCNC-specific configuration/operation is needed on the legacy EPC or on the O&M system
Type	Non-Functional
Severity	Mandatory

Req-C.053

Name	Compliant to 3GPP TS.22.101
Description	The systems shall be compliant to requirements defined in 3GPP TS 22.101 (3GPP, 2013)
Rationale	The developed system must be compatible with legacy systems. This can partially be realized by supporting the requirements of 3GPP TS 22.101.
Dependency	-
Conflict	-
Fit Criterion	Verify if systems comply to the requirements defined in 3GPP TS 22.101.
Type	Other
Severity	Mandatory

Req-C.054

Name	Compliant to 3GPP TS.23.401
Description	The systems shall be compliant to requirements defined in 3GPP TS 23.401 (3GPP, 2013)
Rationale	The developed system must be compatible with legacy systems. This can partially be realized by supporting the requirements of 3GPP TS 23.401.
Dependency	-
Conflict	-
Fit Criterion	Verify if systems comply to the requirements defined in 3GPP TS 23.401.
Type	Other
Severity	Mandatory

A.4 Technical Domain D Requirements

Req-D.001

Name	Get location information
Description	The system shall provide the location information of a user
Rationale	This requirement enables to know the location of any user of the network. This information can be used to dynamically provision network/compute/storage resources or as an information event for other services.
Dependency	-
Conflict	-
Fit Criterion	Verify if the system returns the correct location of a network user.
Type	Functional
Severity	Mandatory

Req-D.002

Name	Provide connectivity information
Description	The system shall provide connectivity information
Rationale	The connectivity info is used to ensure the best QoS/QoE and attempt to avoid SLA violations with preventive measures
Dependency	-
Conflict	-
Fit Criterion	Verify that, given a user, the connectivity information is returned
Type	Functional
Severity	Mandatory

Req-D.003

Name	Provide SLA thresholds
Description	The system shall provide SLA thresholds information
Rationale	The SLA thresholds will be used to check SLA violations
Dependency	-
Conflict	-
Fit Criterion	Given an SLA the thresholds are returned
Type	Functional
Severity	Mandatory

Req-D.004

Name	Create and manage end-to-end SLAs
Description	The system shall create and manage end-to-end SLAs
Rationale	SLAs are created to establish thresholds in an end-to-end connectivity service
Dependency	-
Conflict	-
Fit Criterion	Verify that the SLAs are created and can be modified (managed)
Type	Functional
Severity	Mandatory

Req-D.005

Name	Support end-to-end Rating and Charging
Description	The system shall support end-to-end Rating and Charging
Rationale	This requirement will provide information about the use of the resources and how to charge for it
Dependency	-
Conflict	-
Fit Criterion	The system will return the rating and charging info from a service given
Type	Functional
Severity	Mandatory

Req-D.006

Name	Create content cache
Description	The system shall be able to create content caches
Rationale	By creating content caches the contents downloading process is improved
Dependency	-
Conflict	-
Fit Criterion	Verify that the content cache is created
Type	Functional
Severity	Mandatory

Req-D.007

Name	Reallocate content cache
Description	The system shall be able to reallocate content caches taking into account the geographical proximity of users and amount of video traffic associated with them
Rationale	By locating content caches taking into account the geographical proximity of users and amount of video traffic associated with them the contents downloading is improved
Dependency	-
Conflict	-
Fit Criterion	Given a new location, the system must reallocate the content cache in the new location
Type	Functional
Severity	Mandatory

Req-D.008

Name	Support end-to-end QoS/QoE
Description	The system shall be able to provide end-to-end QoS/QoE support
Rationale	Some services require specific QoS/QoE values to be offered
Dependency	-
Conflict	-
Fit Criterion	Verify if the system provides the QoS/QoE established
Type	Functional
Severity	Mandatory

Req-D.009

Name	Create mobility gateways
Description	The system shall be able to create mobility gateways
Rationale	This requirement enables the system to offer the network connectivity as a service
Dependency	-
Conflict	-
Fit Criterion	Verify if the mobility gateway is created
Type	Functional
Severity	Mandatory

Req-D.010

Name	Locate mobility gateways
Description	The system shall be able to locate mobility gateways
Rationale	Regarding the flexibility concept, the system must be able to reallocate mobility gateways
Dependency	-
Conflict	-
Fit Criterion	Given a new location, the system must locate the mobility gateway in it
Type	Functional
Severity	Mandatory

Req-D.011

Name	Support Follow-me cloud services
Description	The system shall be able to support Follow-me cloud services
Rationale	The Follow-me cloud support is based on the capacity on migrating resources and services from one location to another
Dependency	-
Conflict	-
Fit Criterion	The interfaces to support the Follow-me cloud services are created
Type	Functional
Severity	Mandatory

Req-D.012

Name	Support IMS (IP Multimedia Services) services
Description	The system shall be able to support IMS services
Rationale	The support for the IMS services is based on implementing the interfaces between the IMSaaS and the cloud controller to deploy new resources and services on demand
Dependency	-
Conflict	-
Fit Criterion	The interfaces to support the IMS services are created
Type	Functional
Severity	Mandatory

Req-D.013

Name	Support DSN (Digital Signage Network) services
Description	The system shall be able to support DSN services.
Rationale	DSN services are based on content location, content cache and service deployment on-demand
Dependency	-
Conflict	-
Fit Criterion	Interfaces for the DSN services are implemented
Type	Functional
Severity	Mandatory

Req-D.014

Name	Support service continuity
Description	The system shall be able to support the continuity of a service when a user roams
Rationale	The system shall be able to support the continuity of a service when a user roams either within one administrative domain operated by one MCNSP, or between two or more administrative domains operated by different MCNSPs
Dependency	-
Conflict	-
Fit Criterion	The service is offered without interruption even if the end-user is roaming
Type	Functional
Severity	Mandatory

Req-D.015

Name	Support pay as you go services
Description	The system shall be able to support pay as you go services, where the End User pays only for the time that is using the provided service
Rationale	Every service shall be paid only for the time and for the resources used
Dependency	-
Conflict	-
Fit Criterion	The charging for the services used by the end-user must be related to the time the service has been used
Type	Functional
Severity	Mandatory

Req-D.016

Name	Support communication support for services
Description	The system shall be able to support communication support for supported services
Rationale	All the different services offered have communications requirements to be fulfilled
Dependency	-
Conflict	-
Fit Criterion	All the communications requirements derived from services are fulfilled
Type	Functional
Severity	Mandatory

Req-D.017

Name	Support cooperation with social networking services
Description	The system shall be able to support cooperation of social networking services with apps to generate large user generated content
Rationale	It would be easier for the users to insert contents to the system if there is an interface to do so from the apps where they generate the contents
Dependency	-
Conflict	-
Fit Criterion	Social Networking services must enable users to generate content
Type	Functional
Severity	Mandatory

Req-D.018

Name	Create and manage Follow-me cloud service instances
Description	The system shall be able to create new and manage Follow-me cloud service instances
Rationale	In order to provide Follow-me cloud services the system must have the capability of deploying and managing Follow-me cloud service instances
Dependency	-
Conflict	-
Fit Criterion	Verify if the system creates and manages new Follow-me cloud service instances
Type	Functional
Severity	Mandatory

Req-D.019

Name	Create and manage IMS service instances
Description	The system shall be able to create and manage IMS service instances
Rationale	In order to provide IMS services the system must have the capability of deploying and managing IMS service instances
Dependency	-
Conflict	-
Fit Criterion	Verify if the system creates and manages IMS service instances
Type	Functional
Severity	Mandatory

Req-D.020

Name	Create and manage DSN service instances
Description	The system shall be able to dispose existing Virtual Machinescreate and manage DSN service instances
Rationale	In order to provide DSN services the system must have the capability of deploying and managing DSN service instances
Dependency	-
Conflict	-
Fit Criterion	Verify if the system creates and manages DSN service instances
Type	Functional
Severity	Mandatory

Req-D.021

Name	Provision a Cloud Storage Manager
Description	The system shall be able to provision a Cloud Storage Manager
Rationale	The Cloud Store Manager must be available to all the components that need cloud storage services
Dependency	-
Conflict	-
Fit Criterion	Verify if the Cloud Store Manager is correctly provided
Type	Functional
Severity	Mandatory

Req-D.022

Name	Provision a Container Manager
Description	The system shall be able to provision a Container Manager
Rationale	The Container Manager must be available to all the components that need to create / edit / destroy containers
Dependency	-
Conflict	-
Fit Criterion	Verify if the Container Manager is correctly provided
Type	Functional
Severity	Mandatory

Req-D.023

Name	Provision a Resources Orchestrator
Description	The system shall be able to provision a Resources Orchestrator
Rationale	Resources Orchestration is needed to control the efficient use of resources and the usage of the system
Dependency	-
Conflict	-
Fit Criterion	Verify if the Resources Orchestrator is correctly provided
Type	Functional
Severity	Mandatory

Req-D.024

Name	Provision a QoS/QoE manager
Description	The system shall be able to provision a QoS/QoE manager
Rationale	The QoS/QoE manager is in charge of configuring the system to provide some certain QoS/QoE levels
Dependency	-
Conflict	-
Fit Criterion	Verify if the QoS/QoE manager is correctly provided
Type	Functional
Severity	Mandatory

Req-D.025

Name	Provision a Mobility Support Manager
Description	The system shall be able to provision a Mobility Support Manager
Rationale	The mobility support manager is important to facilitate the actions needed to support mobility
Dependency	-
Conflict	-
Fit Criterion	Verify if the Mobility Support Manager is correctly provided
Type	Functional
Severity	Mandatory

Req-D.026

Name	Provision a ICN Resources Manager
Description	The system shall be able to provision a ICN Resources Manager
Rationale	The ICN Resources Manager must control where the contents must be located to provide download efficiency
Dependency	-
Conflict	-
Fit Criterion	Verify if the ICN Resources Manager is correctly provided
Type	Functional
Severity	Mandatory

Req-D.027

Name	Provision a Mobile Content Delivery Networks (Mobile CDN) resources Manager
Description	The system shall be able to provision a Mobile Content Delivery Networks (Mobile CDN) resources Manager
Rationale	The Mobile CDN resources manager controls the resources needed to provide a mobile cdn service
Dependency	-
Conflict	-
Fit Criterion	Verify if the Mobile Content Delivery Networks (Mobile CDN) resources Manager is correctly provided
Type	Functional
Severity	Mandatory

Req-D.028

Name	Provision a Services Manager
Description	The system shall be able to provision a Services Manager, such as an IMS, DSN and Follow-me cloud services manager
Rationale	The Services Manager will control the lifecycle of services provided by the system
Dependency	-
Conflict	-
Fit Criterion	Verify if the Services Manager is correctly provided
Type	Functional
Severity	Mandatory

Req-D.029

Name	Provision a SLA manager
Description	The system shall be able to provision a SLA manager
Rationale	The SLA manager will control how SLA are created / modified / destroyed
Dependency	-
Conflict	-
Fit Criterion	Verify if the SLA Manager is correctly provided
Type	Functional
Severity	Mandatory

Req-D.030

Name	Provision a Rating/Charging manager
Description	The system shall be able to provision a Rating/Charging manager
Rationale	The Rating/Charging manager will control the tasks and resources needed to provide Rating/Charging manager
Dependency	-
Conflict	-
Fit Criterion	Verify if the Rating/Charging is correctly provided
Type	Functional
Severity	Mandatory

Req-D.031

Name	Get Follow-me cloud service instances status
Description	The system shall be able to get the status of the Follow-me cloud service instances
Rationale	To monitor the Follow-me cloud service instances created the system must report their status
Dependency	-
Conflict	-
Fit Criterion	Given a Follow-me cloud service instance, the system returns its status
Type	Functional
Severity	Mandatory

Req-D.032

Name	Get Follow-me cloud service instances utilisation
Description	The system shall be able to get the utilisation of the Follow-me cloud service instances
Rationale	To monitor the Follow-me cloud service instances created, the system must report the level of utilisation
Dependency	-
Conflict	-
Fit Criterion	Given a Follow-me cloud service instance, the system returns its utilisation level
Type	Functional
Severity	Mandatory

Req-D.033

Name	Get IMS service instances status
Description	The system shall be able to get the status of the IMS service instances
Rationale	To monitor the IMS service instances created, the system must report their status
Dependency	-
Conflict	-
Fit Criterion	Given an IMS service instance, the system returns its status
Type	Functional
Severity	Mandatory

Req-D.034

Name	Get IMS service instances utilisation
Description	The system shall be able to get the utilisation of the IMS service instancesThe
Rationale	To monitor the IMS service instances created, the system must report the level of utilisation
Dependency	-
Conflict	-
Fit Criterion	Given an IMS service instance, the system returns its utilisation level
Type	Functional
Severity	Mandatory

Req-D.035

Name	Get DSN service instances status
Description	The system shall be able to get the status of the DSN service instances
Rationale	To monitor the DSN service instances created the system must report their status
Dependency	-
Conflict	-
Fit Criterion	Given a DSN service instance, the system returns its status
Type	Functional
Severity	Mandatory

Req-D.036

Name	Get DSN service instances utilisation
Description	The system shall be able to get the utilisation of the DSN service instancesThe
Rationale	To monitor the DSN service instances created, the system must report the level of utilisation
Dependency	-
Conflict	-
Fit Criterion	Given a DSN service instance, the system returns its utilisation level
Type	Functional
Severity	Mandatory

Req-D.037

Name	Get utilisation of the Cloud Storage Manager
Description	The system shall be able to provide information about the Cloud Storage Manager utilisation
Rationale	To monitor the cloud Store Manager provided, the system must report its status
Dependency	-
Conflict	-
Fit Criterion	Given the Cloud Storage Manager id, the system returns its status
Type	Functional
Severity	Mandatory

Req-D.038

Name	Get utilisation of the Container Manager
Description	The system shall be able to provide information about the Container Manager utilisation
Rationale	To monitor the Container Manager provided, the system must report its status
Dependency	-
Conflict	-
Fit Criterion	Given a Container Manager id, the system returns its status
Type	Functional
Severity	Mandatory

Req-D.039

Name	Get utilisation of the Resources Orchestrator
Description	The system shall be able to get the utilisation of the Resources Orchestrator
Rationale	To monitor the Resources Orchestrator provided, the system must report its status
Dependency	-
Conflict	-
Fit Criterion	Given a Resources Orchestrator id, the system returns its status
Type	Functional
Severity	Mandatory

Req-D.040

Name	Get utilisation of the QoS/QoE manager
Description	The system shall be able to get utilisation of the QoS/QoE manager
Rationale	To monitor the QoS/QoE manager provided, the system must report its status
Dependency	-
Conflict	-
Fit Criterion	Given a QoS/QoE manager id, the system returns its status
Type	Functional
Severity	Mandatory

Req-D.041

Name	Get utilisation of the Mobility Support Manager
Description	The system shall be able to provide information about the Mobility Support Manager utilisation
Rationale	To monitor the Mobility Support Manager provided the system must report its status
Dependency	-
Conflict	-
Fit Criterion	Given a Mobility Support Manager id, the system returns its status
Type	Functional
Severity	Mandatory

Req-D.042

Name	Get utilisation of the ICN Resources Manager
Description	The system shall be able to provide the utilisation of the ICN Resources Manager
Rationale	To monitor the ICN Resources Manager provided, the system must report its status
Dependency	-
Conflict	-
Fit Criterion	Given a ICN Resources Manager id, the system returns its status
Type	Functional
Severity	Mandatory

Req-D.043

Name	Get utilisation of the Mobile Content Delivery Networks (Mobile CDN) resources Manager
Description	The system shall be able to provide utilisation of the Mobile Content Delivery Networks (Mobile CDN) resources Manager
Rationale	To monitor the Mobile Content Delivery Networks (Mobile CDN) resources Manager provided the system must report its status
Dependency	-
Conflict	-
Fit Criterion	Given a Mobile Content Delivery Networks (Mobile CDN) resources Manager id, the system returns its status
Type	Functional
Severity	Mandatory

Req-D.044

Name	Get utilisation of the Services Manager
Description	The system shall be able to provide information about the utilisation of the Services Manager, such as an IMS, DSN and Follow-me cloud services manager
Rationale	To monitor the Services Manager provided, the system must report its status
Dependency	-
Conflict	-
Fit Criterion	Given a Services Manager id, the system returns its status
Type	Functional
Severity	Mandatory

Req-D.045

Name	Get utilisation of the SLA manager
Description	The system shall be able to provide information about the utilisation of the SLA manager
Rationale	To monitor the SLA Manager provided the system must report their status
Dependency	-
Conflict	-
Fit Criterion	Given a SLA Manager id, the system returns its status
Type	Functional
Severity	Mandatory

Req-D.046

Name	Get utilisation of the Rating/Charging manager
Description	The system shall be able to provide the utilisation of the Rating/Charging manager
Rationale	To monitor the Rating/Charging manager provided, the system must report its status
Dependency	-
Conflict	-
Fit Criterion	Given a Rating/Charging manager id, the system returns its status
Type	Functional
Severity	Mandatory

Req-D.047

Name	Reliable migration of Follow-me cloud service instances
Description	The system shall support a reliable migration of Follow-me cloud service instances
Rationale	To permit the Follow-me cloud service instances work fluently, the migration of service instances must be very reliable
Dependency	-
Conflict	-
Fit Criterion	There must be a high percentage of successful migrations of Follow-me cloud service instances
Type	Non-Functional
Severity	Mandatory

Req-D.048

Name	Reliable migration IMS service instances
Description	The system shall support a reliable migration of IMS service instances
Rationale	To permit the IMS service instances work fluently, the migration of service instances must be very reliable
Dependency	-
Conflict	-
Fit Criterion	There must be a high percentage of successful migrations of IMS service instances
Type	Non-Functional
Severity	Mandatory

Req-D.049

Name	Reliable migration of DSN service instances
Description	The system shall support a reliable migration of DSN service instances
Rationale	To permit the DSN service instances work fluently, the migration of service instances must be very reliable
Dependency	-
Conflict	-
Fit Criterion	There must be a high percentage of successful migrations of DSN service instances
Type	Non-Functional
Severity	Mandatory

Req-D.050

Name	Reliable support of services
Description	The system shall support reliable IMS, DSN and Follow-me cloud services
Rationale	To be able to provide IMS, DSN and Follow-me cloud services the system must implement at least the mandatory interfaces of each service
Dependency	-
Conflict	-
Fit Criterion	All necessary interfaces for IMS, DSN and Follow-me cloud are implemented
Type	Non-Functional
Severity	Mandatory

Req-D.051

Name	Reliable support of SLA provisioning
Description	The system shall support reliable SLA provisioning
Rationale	SLA provisioning must be reliable for being able to check SLA violations anytime
Dependency	-
Conflict	-
Fit Criterion	There must be a high percentage of successful SLA provisions
Type	Non-Functional
Severity	Mandatory

Req-D.052

Name	Reliable support of rating and charging provisioning
Description	The system shall support reliable support of rating and charging provisioning
Rationale	Rating and Charging provisioning must be reliable to support the pay-for-use and pay-as-you-go concepts
Dependency	-
Conflict	-
Fit Criterion	There must be a high percentage of successful Rating and Charging provisions
Type	Non-Functional
Severity	Mandatory

Req-D.053

Name	Seamless service continuity solutions
Description	The system shall support seamless service continuity solutions
Rationale	The users doesn´t have to notice any difference in the service exploitation while roaming
Dependency	-
Conflict	-
Fit Criterion	Service performance doesn´t change while roaming
Type	Non-Functional
Severity	Mandatory

Req-D.054

Name	Support of different levels of QoS/QoE signalling and provisioning
Description	The system shall support different levels of QoS/QoE signalling and provisioning
Rationale	The system must implement interfaces to provide different QoS/QoE levels and support its signalling
Dependency	-
Conflict	-
Fit Criterion	Verify that the system provides different QoS/QoE levels and signalling
Type	Non-Functional
Severity	Mandatory

Req-D.055

Name	Application expected response time
Description	The system shall guarantee that the applications' specific expected time interval is complied.
Rationale	Application specific expected time interval between the instant a request is sent by an user and the instant at which the response is received.
Dependency	-
Conflict	-
Fit Criterion	The application expected response time shall be measured, and be guaranteed that it is below the established maximum value.
Type	Non-Functional
Severity	Mandatory

Req-D.056

Name	Application maximum delay
Description	The system shall guarantee that applications support a maximum requested end-to-end delay.
Rationale	The maximum supported applications' end-to-end delay is guaranteed, enabling adequate end-user experience.
Dependency	-
Conflict	-
Fit Criterion	The end-to-end delay shall be measured, and be guaranteed that it is below the established maximum value.
Type	Non-Functional
Severity	Mandatory

Req-D.057

Name	Application maximum jitter
Description	The system shall guarantee that applications support a maximum requested jitter.
Rationale	The maximum supported applications' jitter is guaranteed, enabling adequate end-user experience.
Dependency	-
Conflict	-
Fit Criterion	The jitter shall be measured, and be guaranteed that it is below the established maximum value.
Type	Non-Functional
Severity	Mandatory

Req-D.058

Name	Application minimum data rate
Description	The system shall guarantee that applications support a minimum requested data rate.
Rationale	The minimum supported applications' data rateis guaranteed, enabling adequate end-user experience.
Dependency	-
Conflict	-
Fit Criterion	The jitter shall be measured, and be guaranteed that it is above the established minimum value.
Type	Non-Functional
Severity	Mandatory

Req-D.059

Name	Application maximum loss rate
Description	The system shall guarantee that applications support a maximum requested packet loss rate.
Rationale	The maximum supported applications' packet loss rate is guaranteed, enabling adequate end-user experience.
Dependency	-
Conflict	-
Fit Criterion	The packet loss rate shall be measured, and be guaranteed that it is below the established maximum value.
Type	Non-Functional
Severity	Mandatory

Req-D.060

Name	Application maximum error rate
Description	The system shall guarantee that applications support a maximum acceptable error rate.
Rationale	The maximum acceptable applications' jitter is guaranteed, enabling adequate end-user experience.
Dependency	-
Conflict	-
Fit Criterion	The error rate shall be measured, and be guaranteed that it is below the established maximum value.
Type	Non-Functional
Severity	Mandatory

Req-D.061

Name	Support of Authentication, Authorisation, Accounting, Confidentiality and Integrity
Description	The system shall support of Authentication, Authorisation, Accounting, Confidentiality and Integrity
Rationale	Authentication, Authorisation, Accounting, Confidentiality and Integrity are some of the most common and most important features for any telco system
Dependency	-
Conflict	-
Fit Criterion	Verify that the necessary interfaces for Authentication, Authorisation, Accounting, Confidentiality and Integrity are implemented
Type	Non-Functional
Severity	Mandatory

Req-D.062

Name	Different level of privacy depending on supported services
Description	The system shall support different level of privacy depending on supported services
Rationale	Not all the services require the same level of privacy, thus the system should have the possibility to provide different privacy levels
Dependency	-
Conflict	-
Fit Criterion	Verify that the system offers different levels of privacy
Type	Non-Functional
Severity	Mandatory

Req-D.063

Name	Support of user friendly management and monitoring tools
Description	The system shall support user friendly management and monitoring tools
Rationale	The more user friendly the managing and monitoring tools are the easier it will be for anyone to get information
Dependency	-
Conflict	-
Fit Criterion	Verify that the management and monitoring tools are user friendly
Type	Non-Functional
Severity	Mandatory

Req-D.064

Name	User friendly, easy-usage and simplicity of interfaces and APIs
Description	System shall support user friendly, easy-usage and simplicity of interfaces and APIs
Rationale	The system needs to have easy-to-use APIs and interfaces to facilitate the integration process to multiple services and resources
Dependency	-
Conflict	-
Fit Criterion	Verify the user-friendly, easy-usage and simplicity of interfaces and APIs
Type	Non-Functional
Severity	Mandatory

Req-D.065

Name	Compatibility with Legacy system supporting a smooth migration
Description	The system shall support compatibility with Legacy system supporting a smooth migration
Rationale	To monitor the virtual machines created the system must report their status
Dependency	-
Conflict	-
Fit Criterion	Given a virtual machine id, the system returns its status
Type	Other
Severity	Mandatory

Appendix B. Consolidated Scenarios

This Appendix provides description of the defined Consolidated Scenarios is provided.

B.1 Consolidated Scenario 1 - RAN on Demand

Mobile operators are engaged in cost-reduction initiatives targeting every part of the mobile network, from the price of base station equipment to the cost of backhaul. Radio Access Network (RAN) sharing is an option to alter the cost structure of the mobile industry. MCN Radio Access Network Provider (RANP) serves Mobile Virtual Network Operators (MVNOs) and/or Mobile Network Operator (MNOs), with on-demand, dynamic and elastic RAN-as-a-Service (RANaaS). RANaaS is built based on services received from Cloud Infrastructure Provider (CIP) and Network Infrastructure Provider (NIP). RANP allocates resources based on Service Level Agreement (SLAs) with each client.

Clients (MNOs or MVNOs) using RANP services can configure the RAN. Configuration is restricted to the provider capabilities, e.g., more/less radio resources, radio coverage, more or less fronthaul/backhaul resources, being automatic and real-time. RANP is also able to propose optimal configuration, based on real measurements (Self Organizing Networks). Using Cloud-based RAN (C-RAN), RANP is able to dynamically configure physical resources, e.g. Remote Radio Heads (RRHs) and Base Band Units (BBUs), to serve busy hours or temporally high load situations.

B.2 Consolidated Scenario 2 - Mobile Virtual Resources on Demand

Today's Mobile Core platforms (EPC) are based on statically provisioned, tailor-made infrastructure, which usually leads to overprovisioning and sub-optimal efficiency of resources. Taking advantage of modern and efficient cloud technologies, this scenario considers the deployment of on-demand distributed Mobile Core instances, relying on the elastic IaaS service model. Enabling on-demand and automated instantiation of Mobile Core instances - MNRoD (Mobile Network Resources on-demand) - and re-designing Mobile Core components to fully exploit the "as-a-Service" concept constitute complex technical challenges.

MNOs are the most obvious player that may offer such services (although many other may come in). MNOs can use the Mobile Core as a Service model for its own operations, benefiting from the increasing flexibility of bandwidth that can provide to its end customers. On the other hand, MNOs may sell Mobile Core services to other parties, typically MVNOs (although many other entities may apear, like other MNOs, content service providers, etc.). Using the EPC as a Service model, the MNO is able to allow MVNO customers to request resources like bandwidth, Core Network computation and storage capabilities, content delivery capabilities for streaming services, among others.

Other End User Services like IMS, or Support Systems such as Billing or Provisioning can also be provided in the cloud, benefiting of the same advantages of flexibility and on-demand paradigm. These kind of services are able to fully provide to MVNOs all necessary packages to composes services to be delivered to its subscribers.

Any important issue here is to ensure the compatibility between the traditional components (EPC, IMS, etc.) and the cloud-based components. MNOs/MVNOs will move to the cloud gradually, so it must be ensured full compatibility, allowing hybrid scenarios, by mixing traditional and cloud-based components. This feature is a MUST.

Another important issue here is a clear definition of SLAs and charging models. SLAs must clearly define service classes (static and dynamic guarantees of resources, best effort, etc.). Charging models must be able to monetize the resources really used by MVNOs, either statically or dynamically provisioned, considering potential different costs.

This model allows MNOs and MVNOs to benefit. - MNOs are able to better manage and change resources allocated to MVNOs according to predefined SLAs and business models. - MVNOs are able to improve QoE, since they are able to dynamically request resources, according to their particular (and variable) needs. - MVNOs/otherMNOs are able to buy extra capacity for peak situation (e.g. Christmas) without CAPEX increase (and consequent misuse in normal situations).

B.3 Consolidated Scenario 3 - Machine Type Communication on Demand

Today some utility providers use Machine Type Communications (MTC) (or Machine to Machine (M2M)) devices such as smart sensors, actuators, smart meters to gather specific measurements at a given periodicity (e.g., at the end of every month, at the end of every year, etc.). Other utility providers are accessing such MTC devices to also configure them.

However, the access, dissemination and retrieval of information to/from such MTC devices can be expensive, since the Mobile Operator (Mobile Network Operator / Mobile Virtual Network Operator) may need to allocate a significant number of RAN and EPC resources for a relatively short amount of time. The utility provider, which in this situation can be considered as being an MCN end user, may (1) request from MVNO to access, disseminate and /or retrieve information, only at durations of time when the overall costs of these services are lower than a certain agreed amount (SLA agreement), (2) request from the MVNO the creation of a mobile network (RAN and EPC) on the cloud that will be functional only for the duration that MTC devices need to be accessed and used.

An important issue here is that MVNO must be able to dynamically and on demand request the creation of a mobile network (RAN and EPC). This means that the MVNO should be able to create and manage the MCN mobile network resources in a flexible, dynamic, reliable and scalable way. Furthermore, the MVNO should be able to perform load balancing over time and that they are also able to charge the use of resources depending on the network load.

Another important issue is the clear definition of the SLA and charging models. SLA must specify the conditions and the overall costs threshold (maximum amount of financial resources) that an MCN end user (i.e., utility provider) is willing to pay for the use of the MCN service (access and use of the MTC devices).

The most obvious players are the utility providers, and the utility consumers that can be seen as MCN end users, and the MVNOs. The MVNOs can be represented by a combination of stakeholders and in particular, MCN Service Provider that provides the Mobile connectivity to the utility providers, Value Added Services / Applications Provider (VASAP) that provides MTC services to the end user, RAN providers (RANP), Mobile Core Network Providers (MCNP), Network Infrastructure Provider (NIP) that can provide the MTC devices, the Cloud Infrastructure Provider (CIP) that provides the cloud infrastructure adn the MCN Cloud Services Provider (CSP) that provides the cloud services.

This model allows utility providers, utility consumers (i.e., MCN end users), MNOs and MVNOs to benefit. In particular, end users (utility providers) will benefit from the point of flexible configuration for accessing and collecting information from MTC devices, significant cost reduction and short time to market solutions. MVNOs and other MNOs are able to by capacity for peak situations (i.e., only when the MTC devices need to be accessed or configured) without CAPEX increase (and consequent misuse in normal situations). Furthermore, MVNOs will be able to charge the use of their managed RAN and EPC resources depending on the network load.

B.4 Consolidated Scenario 4 - Software-Defined Networking

The following scenario describes how Software Defined Networking (SDN) can help overcome limits of traditional Mobile Networks. Traditional Mobile Networks suffer from several limitations related to data traffic management like inflexible and expensive equipment, complex routing protocols and complex configuration settings. In simple terms, LTE networks work in following way:

- UE (User Equipment) makes a request to connect/update. The request goes to BSS (Base Station).
- The request is forwarded to SGW (Service Gateway) which is local Mobility Anchorpoint for intel BSS handover. SGW forwards it to PGW (Packet Data Network Gateway).
- The PGW is connected to the Internet, and performs several checks and logs before making Internet accessible to user. Basically it includes Policy Control and Billing functions.

Since the PGW has to make all the QoS checks, monitoring and updates, that makes its job more and more complex as the data users and rates increase. PGW is the single gateway performing all the validations and updates. Centralizing data plane functions has following drawbacks: 1) It introduces scalability challenges 2) It makes configuration harder since thousands of parameters have to be tuned 3) It makes equipment expensive (~ $6M for Cisco's packet gateway).

Using SDN can eliminate aforementioned limitations and add the possibility for several value added services. Following is how SDN can work with Mobile Networks. Instead of having a PGW to do all the routing work, SDN approach divides virtualized Radio Hardware and Packet forwarding hardware each having their own Call Agent to perform requests. The SDN controller consists of a Network Operating System(NOS) running a collection of application modules, such as radio resource management, mobility management, and routing. The handling of individual packets often depends on multiple modules. For example, the flow of traffic through the network depends on the subscriber’s location (determined by the mobility manager) and the paths between pairs of network elements (determined by infrastructure routing), and traffic monitoring and packet scheduling depend on the policy and charging rule function. As such, the NOS should support composition to combine the results of multiple modules into a single set of packet-handling rules in each switch. Below is a diagram of such system.

Proposed benefits of SDN are:

- Flexible policy implementation per subscriber basis in real time.
- Cost savings due to use inexpensive network switches instead of sophisticated hardware.
- Elimination of scalability challenges faced by traditional PGWs.
- Support for real time deep packet inspection.
- Greater degree of fault tolerance.

B.5 Consolidated Scenario 5 - Energy saving & fast network reconfiguration

The load in a mobile operator’s network, in terms of number of connected customers, signalling overhead and traffic, varies quite a lot during the day. As such, the CPU, memory and transmission capacity required to handle the network load during peak hours are much higher than those needed in other periods of time. The virtualisation of the Evolved Packet Core, and in particular of core network entities like MME, SGSN and the PDN/Serving Gateway, creates the opportunity for the network operator to achieve reduced energy consumption by exploiting power management features in standard servers and storage, as well as workload consolidation. For example, relying on virtualisation techniques it would be possible to concentrate the workload on a smaller number of servers during off-peak hours (e.g. overnight) so that all the other servers can be switched off or put into an energy saving mode.

Moreover the possibility to transparently move workloads between servers located in the same Data Centre, or across Data Centres, can be exploited by the mobile operator also for other purposes, that go far beyond pure energy saving. These include the possibility to promptly trigger a network reconfiguration as a way to react to a failure or just to optimize the network operation:

If a major failure affects one or more nodes of a cloud infrastructure (servers, switches, storage, etc.), or an entire Data Centre, thanks to the recovery techniques supported in a virtualized environment, a new backup node (or a set of nodes) can be spawned in the same Data Centre, or in another DC. The workload is moved onto spare capacity, with no user sessions loss.

The mobile network configuration and topology can be automatically updated, in a near-real time fashion, depending on the actual traffic and/or mobility patterns, on the number of customers showing up in a specific location and/or network segment, etc.

B.6 Consolidated Scenario 6 - Scaling the capacity of a virtualized EPC

Virtualisation of the EPC mandates suitable solutions to scale to different load situations. The technical approach and details to enable scalability can differ in dependency of time constraints as well as the location, where load is being experienced. Load can be predictable (scheduled fare/festival events, well known peak hours, statistics) or unpredictable and immediate. Load can be experienced in the cloud infrastructure provider’s network, servers/hardware or in VMs and associated instances of EPC components (e.g. MME, PGW).

Predictable load variations imply lower time constraints as compared to sudden and unpredictable increase in load. Unexpected load increase may cause bottleneck or even impact service/system stability. This scenario considers the following approaches to adopt to load in consideration of different delay constraints:

- Low time constraints: Instantiation of additional EPC component (carries unique identifier). New instance is announced to the EPC to make it available and selectable. Load can be distributed between multiple EPC components by appropriate selection functions.
- Strong time constraints: Instantiation of the same EPC component (represents a duplicate of an existing EPC component). Load of a single EPC component can be distributed between multiple instances of the same EPC component.
- Migration of an EPC component’s instance between host servers (within or beyond Data Centres).

The following administrative instances can detect/predict load variations and initiate scaling: Data Centre Infrastructure Provider, Cloud Infrastructure Provider, Mobile Cloud Network Service Provider, Mobile Connectivity Service Provider.

B.7 Consolidated Scenario 7 - Follow-Me cloud & Smart content location

An end user that can be a customer with digital safe services (personal data) or an enterprise employee, must be able to run any service/application (e.g., flight reservation and booking, running demos that require online and Internet support) and access their personal/business data while roaming. For that it needs to receive:

(1) high quality, fast, reliable and secure communication support for their service/application, and
(2) pay only for the time that they are using a communication infrastructure.

A Mobile Operator on the other hand wants to make its services more attractive to its frequently traveling subscribers by lowering roaming costs. This can be done when the mobile operator has the possibility to create on demand an own vPLMN (visited Home Public Land Mobile Network) or, if it MCN capable, expand its own hPLMN (home PLMN) into a visited country, instead of paying fees to roaming partners (other Mobile Operators) in that country. In those cases, the Mobile Operator may also act as a MVNO in order to take benefits from RAN resources that are owned by its local Mobile Operator partner. Another possible business model is for the Mobile Operator to set a partnership with a Cloud Service Provider that has a worldwide footprint. In that case, the Cloud Service Provider is supporting the service by providing compute and storage facilities. Furthermore, an Mobile Operator desires to create its own decentralized content distribution network to cache popular videos for its users, and align the CDN operation, such as caching strategies and request routing, with its technology for distributed mobility management (DMM).Caches should be placed on cloud on strategic data centre places, taking into account the geographical proximity of users to these Data Centres but also the amount of video traffic associated with them! In addition, such content distribution network should cooperate with social networking services and provide support for the most popular apps that generate large User Generated Content (UGC) by providing assets like:

(1) storing efficiently these contents within the network data centre, and
(2) allocating the right network resources to deliver those UGC traffic partners. In the last case an assumption is made that the UGC is stamped as being non premium, and obviously emergency calls have higher priority than UGC videos.

There are several important issues that are related to this consolidated scenario. These are mainly structured around the roaming scenario, and in particular that:

(1) end users should receive high quality, fast, reliable and secure communication support for their service/application,
(2) end users should pay only for the time that they are using a communication infrastructure,
(3) mobile operator should operate a decentralized network and provide caches of contents and local mobility gateways which should be placed on strategic data centre places, taking into account the geographical proximity of users to these data centres but also the amount of video traffic associated with them,
(4) mobile operator should provide cooperation with social networking services in order to provide support for the most popular apps that generate large User Generated Content (UGC) by providing assets like: (i) storing efficiently these contents within the network data centre and (ii) to allocate the right network resources to deliver those UGC traffic partners, under assumption that the UGC is considered as being non premium and emergency calls have higher priority than UGC videos.

Moreover, there are several other issues related to the mobility scenario:

(1) end users should have fast handover procedures between different cells, and
(2) mobile operator should have mechanisms to predict user mobility and user behaviour. Furthermore, mobile operators should have mechanisms to enable runtime relocation of local mobility gateways and local content caches to keep content delivery paths short.

This model allows End Users, who can be personal/individual and/or business consumers/subscribers as well as mobile operators, to benefit from the performance and financial point of view when using Follow-me-Cloud and Service/content services.

In this scenario, the MCN Cloud Services Provider and the MCN Value Added Services/Application Provider (which can be a Content Provider, an SaaS provider or an IMSaaS provider) play a significant role. The Cloud Services Provider and the Value Added Services/Application Provider, that are used to run a service/application, need to support the migration of the Virtual Machines to other parts of the Cloud Infrastructure(s) in such a way that neither the service/application nor the End Users are aware of this migration. In particular, the Cloud Services Provider needs to make the migration of the Virtual machines possible, while the Value Added Services/Application Provider needs to support (in terms of what/when/where) the migration of the service/application or the content, in a seamless way to the End User. This can be accomplished by using Software-Defined Networking (SDN) and/or Information Centric Networking (ICN).

B.8 Consolidated Scenario 8 - Digital Signage

A typical Digital Signage (DS) system is composed of two main components:

- Digital Signage Server: The DS Server performs as a content storage system and also as a coordinator for the distributed DS players (scheduling, supervision, etc.).
- Digital Signage Players: The DS players play the multimedia contents which are downloaded from the DS server. They also may perform an event detection process to adapt its playlist to the context.

A DS deployment is based on distributing digital signage over a certain area. The digital signage players will download the playlists and the required multimedia contents from the DS server and start playing them.

A usual situation for a DS provider is to have to deploy a DS system for temporary event. In this case, many DS players must be installed and they need a network connection to download the multimedia contents from the DS server as fast as possible. A conventional network infrastructure deployment may be expensive and inefficient. A DS provider would need an on-demand network communication services to provide the DS players the capacity to download the multimedia contents from the DS content provider as fast as possible. In addition, multimedia contents should be located as near as possible to the players (cloud content storage).

Another point of action of a DS provider is to enrich the set of events that produce the DS players to react changing their played content. Information from the network could be used to adapt the contents played on the DS players. For example, if the network is overloaded, an over-the-top DS player could react asking for contents with lower bitrates. Another example would be if the DS player is moving (in a bus or a train), it could react to its location.

B.9 Consolidated Scenario 9 - Operational Management & Charging as a Service

Telecommunication network architectures are defined in terms of functional entities each devoted to implement well defined tasks. Non-functional requirements impose high availability (99,999%), low latency and high quality in media management. Telco Operators are familiar with this pure functional model but had to cope with the available technology. Therefore, during the years telco networks has been implemented by carrier-grade available legacy hardware equipment specialized to provide high performing signalling and media management. Extending network performance or introducing new functionalities yield to the deployment of one or more new hardware equipment, thus resulting in slow modification of network infrastructure.

Virtualisation techniques and availability of high performing COTS servers are enabling the introduction of cloud computing as an alternative model for Telco networks deployments. Therefore, cloud concepts such as on-demand, elasticity, pay-as-you-go can now be considered in the design of Telco networks deployments. The base of the novel telco network can now be a cloud infrastructure providing computational resources, network connection and storage for all the needs of signalling, media and operational management. On top of this infrastructure is instantiated the telco specific functional entities, providing the cloud telco platform. The next layer uses these functional entities for building the specific service or application layer where the communication service is end-to-end provided to the operator's customers. Finally the OSS/BSS layer provides operation, management and business services completing this picture and allowing effective network operation, service provisioning and customer's charging.

The novel architecture already described can bring to new business models with a multitude of actors. Business models are beyond the scope of this description. For our objectives it is important to stick that each layer can potentially be implemented by a different actor. The new system architecture is now highly dynamic and reconfigurable, requiring real-time dynamic adaptation of the management systems and procedures. Therefore, traditional FCAPS management is now strictly influenced by cloud computing on-demand, elasticity, pay-as-you-go properties.

B.10 Consolidated Scenario 10 - End-to-End Cloud

A NIP-CIP mutual partnership (e.g. CloudSigma & Italtel) is formed to leverage each other’s resources and offer their combined services through a MCN Cloud Service Provider. This partnership will be the business realisation of “Cloud and Network convergence” or as noted in the MCN DoW “Extend[ing] the Concept of Cloud Computing beyond data centres towards the Mobile End-User.” The goal of this scenario is to describe data centre resources (managed by CIP, located centrally or distributed) offered to end users through a NIP and RAN resources “cloudified” by a CIP and offered out by the NIP. With the partnership in place and a MCN cloud service provider presented, the technical realisation of a combined NIP/CIP’s full end-to-end cloud-enabled stack. Each stakeholder will profit from this mutually leveraging each other strategic assets. Owing to combining (partnership) and increased customer base (greater profit too) the cloud stack should be suitably optimised.

Appendix C. Draft Scenarios

As explained in Section 3, the requirements specification process started by collecting a set of Draft Scenarios, which were grouped in a smaller set of Consolidated Scenarios in a later stage.

The following table shows the correspondence between Consolidated Scenarios (CS), Technical Domains (TD) and Draft Scenarios. Note that some Draft Scenarios are related to more than one Technical Domain.

CS	TD	Draft Scenario
CS04	A	Use of SDN to define custom data plans
		Use of SDN to set priority levels for different web services
CS10		The End-To-End Mobile Cloud
		Back end as a service on top of IaaS
		New generation of Telco infrastructure
		MVNO&MNO stock exchange with federated MVNO cloud
CS01	B	Shared access network infrastructure
		RAN on-demand with legacy third core networks
		RAN on-demand with legacy own core networks
		RAN and/or Core and/or Service Platforms on-demand with own or third partners
		Dynamic Resources Management Based on Spatial and Temporal Load Variations
		Quick Deployment of flexible Mobile Communication Infrastructure
CS05		Energy saving
		Fast Network reconfiguration for disaster recovery or maintenance/repair operations
		Power reduction by means of EP instance aggregation and host system shutdown (EPC focus)
CS06	C	Scaling (out) capacity of Evolved Packet Core instances; low time constraints
		Scaling (out) capacity of Evolved Packet Core instances; strong time constraints
CS02		Mobile Core as a Service
		Mobile Network Resources on-demand
		Enhanced wholesale offer as an implementation of Mobile Network Resources on-demand
		Various Types of MVNO - Guaranteed and Best Effort
		Compatibility between current EPC deployments and MCN concepts
		Offload Network as a Service
		Runtime Mobility Gateway (and Serving Point) Relocation
		Integrated Corporate Mobile Networking
CS03		Machine-to-Machine traffic management
		The Vehicle-to-Vehicle
		Cost Limited Network
		MTC EPC as a Service
CS05		Energy saving
		Fast Network reconfiguration for disaster recovery or maintenance/repair operations

CS	TD	Draft Scenario
		Power reduction by means of EP instance aggregation and host system shutdown (EPC focus)[1]
CS07	D	Travelling
		New application storage and processing services for better QoE (especially latency) in roaming cases
		Smart ingestion and distribution of UGC
		Follow-me Cloud
		visted Home Public Land Mobile Network as a Service
		MOBILE CDN as a Service
		Localized Digital Retail/Services
CS08		Follow Me Digital Signage
		Digital Signage Network as a Service
CS09		Operational Management as a Service
		Charging as a Service

Appendix D. *Volere* requirements specification template structure

As explained on Section 3, the *Volere* process was used as the main reference for specification of requirements. This Appendix provides the basic components of the *Volere* template (Robertson & Robertson, 2012).

Project drivers:

- The Purpose of the Product
- Client, Customer and other Stakeholders
- Users of the Product

Project constraints:

- Mandated Constraints
- Naming Conventions and Definitions
- Relevant Facts and Assumptions

Functional requirements:

- The Scope of the Work
- The Scope of the Product
- Functional and Data Requirements

Non-functional requirements:

- Look and Feel Requirements
- Usability Requirements
- Performance Requirements
- Operational Requirements
- Maintainability and Portability Requirements
- Security Requirements
- Cultural and Political Requirements
- Legal Requirements

Project issues:

- Open Issues
- Off-the-Shelf Solutions
- New Problems
- Tasks
- Cutover
- Risks
- Costs
- User Documentation and Training

- Waiting Room
- Ideas for Solutions