Small cEllS coordinAtion for Multi-tenancy and Edge services

Grant Agreement No.671596

Topic: H2020-2014-ICT-14
Advanced 5G Network Infrastructure for the Future Internet
Research and Innovation Action

Deliverable D3.4

CESC Small Cell prototype and PoC

Document Number:	H2020-5GPPP-GA No.671596/WP3/D3.4/*31.06.2017*
Contractual Date of Delivery:	*30.06.2017*
Editor:	Alan Whitehead - IP.Access Ltd.
Work-package:	WP3
Distribution / Type:	Public (PU) / Report (R)
Version:	1.0
Total Number of Pages:	63
File:	*SESAME_Deliverable 3.4_v1.0_Final*

Abstract

This document describes the SESAME Small Cell Prototype and Proof of Concept (PoC) demonstrations.

This SESAME CESC Cluster architecture melds together the currently disparate worlds of the traditional small cell RAN infrastructure, the current trends in IT virtualisation and SDN in data centres, the design of Mobile Edge Computing environments, and the growing emphasis of how these are applied in a telecoms environment using NFV approaches. To date, most of the NFV considerations have been towards the core network functions, despite the base station functions being within the NFV remit, but within SESAME they are firmly applied within the RAN, and form the basis of the overall architecture.

This architecture forms the basis of the work of WP3 to develop a Proof-of-Concept demonstrator of the SESAME concepts, how Self-X features may be used in a SESAME environment, and how the virtualisation of radio resources may be used to further enhance the ability to slice the CESC resources between the tenant operators.

This report details those aspects of the SESAME architecture that have been implemented by the Proof-of-Concept demonstrator. It discusses and concludes on the success of these various aspects and indicates where further work is required to achieve a commercially deployable system.

5G-PPP Disclaimer:
This *Deliverable* has been prepared by the 5G Initiative, via an inter 5G-PPP project collaboration. As such, the contents represent the consensus achieved between the contributors to the report and do not claim to be the opinion of any specific participant organisation in the 5G-PPP initiative or any individual member organisation of the 5G-Infrastructure Association.

Version History

Version	Date	Comments, Changes, Status	Authors, contributors, reviewers
0.1	20.06.2017	Initial draft	Alan Whitehead (IPA)
0.2	28.06.2017	Added content from CNET	Leonardo Goratti (CNET)
0.3	29.06.2017	Added content to appendices	Alan Whitehead (IPA)
0.4	30.06.2017	Added citations and cross-references	Alan Whitehead (IPA)
0.5	04.07.2017	Incorporated CNET updates	Alan Whitehead (IPA)
0.6	06.07.2017	Internal revision of the document	Athanassios Dardamanis (SMNET)
1.0	07.07.2017	Full conceptual and editorial review by OTE – Document ready for submission to the Commission	Ioannis Chochliouros (OTE)

Contributors

First Name	Last Name	Partner	Email
Leonardo	Goratti	CNET	lgoratti@fbk.eu
David	Brock	IPA	David.Brock@ipaccess.com
Alan	Whitehead	IPA	Alan.Whitehead@ipaccess.com
Shah Nawaz	Khan	CNET	s.khan@fbk.eu
Cristina	Costa	CNET	ccosta@fbk.eu
Roberto	Riggio	CNET	rriggio@fbk.eu
Tejas	Subramanya	CNET	t.subramanya@fbk.eu
Supreeth	Herle	CNET	s.herle@fbk.eu
Ioannis	Giannoulakis	NCSRD	giannoul@iit.demokritos.gr
Athanassios	Dardamanis	SMNET	adardamanis@smart.net.gr
Ioannis	Chochliouros	OTE	ichochliouros@oteresearch.gr

Glossary

Acronym	Explanation
3GPP	Third Generation Partnership Project
5G	Fifth Generation of Mobile Communications
AP	Access Point
API	Application Protocol Interface
APN	Access Point Name
ARQ	Automatic Repeat ReQuest
AS	Access Stratum
BF	Broadband Forum
CESC	Cloud Enabled Small Cell
CESCM	Cloud Enabled Small Cell Manager
CM	Configuration Management
CN	Core Network
CP	Control Plane
CPE	Customer Premises Equipment
CPU	Central Processing Unit
C-RAN	Cloud RAN
CU	Centralized Unit
CWMP	CPE WAN Management Protocol
DB	DataBase
DC	Data Centre
DL	Downlink
DP	Data Plane
DPI	Deep Packet Inspection
DU	Distributed Unit
E2E	End-to-End
eNB	ENodeB
EPC	Evolved Packet Core (network)
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FAP	Femto Access Point
FDD	Frequency Division Duplex
FDMA	Frequency Division Multiple Access
FM	Fault Management
FT	File Transfer
FW	FireWall
G-PDU	GTP PDU
GA	Grant Agreement
GbE	gigabit Ethernet
GPRS	Generalised Packet Radio Service
GTP	GPRS Tunnelling Protocol
GTP-U	GTP User Plane
GUI	Graphics User Interface
GW	GateWay
GWCN	GateWay Core Network
H2020	Horizon 2020
HARQ	Hybrid Automatic Repeat ReQuest
HeNB	Home eNodeB
HeNB-GW	Home eNodeB Gateway
HSS	Home Subscriber Server
HTTP	HyperText Transfer Protocol

HTTPS	HyperText Transfer Protocol Secure
HW	Hardware
ICT	Information and Communication Technology
ID, id	Identifier
IP	Internet Protocol
IRP	Integration Reference Point
IS	Information Service
IT	Information Technology
KVM	Kernel-*based* Virtual Machine
Light DC	Light Data Centre
LTE	Long Term evolution
µs	micro-server
MAC	Medium Access Control (layer of the protocol stack)
MEC	Mobile Edge Computing
MIB	Management Information Base
MIMO	Multi-Input Multi-Output
MME	Mobility Management Entity
MNO	Mobile Network Operator
MOCN	Multi-Operator Core Network
MRI	MEC-RAN Information
NAS	Non-Access Stratum
NFV	Network Function Virtualisation
NFVO	NFV Orchestrator
NMS	Network Management System
NNSF	NAS Node Selection Function
NO	Network Operator
NOS	Network Orchestration System
OAI	Open Air Interface
OFDMA	Orthogonal Frequency Division Multiple Access
OS	Operating System
PC	Personal Computer
PCRF	Policy and Charging Rules Function
PDCP	Packet Data Convergence Protocol (layer of the protocol stack)
PDU	Protocol Data Unit
PGW	Packet GateWay
PHY	Physical (layer of the protocol stack)
PLMN	Public Land Mobile Network
PM	Performance Management
PNF	Physical Network Function
PoC	Proof of Concept
PPP	Public Private Partnership
PRB	Physical Resource Block
QAM	Quadrature Amplitude Modulation
QCI	QoS Class Identifier
QoS	Quality of Service
QPSK	Quadrature Phase-Shift Keying
RAB	Radio Access Bearer
RAN	Radio Access Network
REST	Representational State Transfer
RIA	Research and Innovation Action
RLC	Radio Link Control (layer of the protocol stack)
RNIS	Radio Network Information Service
RR	Round Robin (scheduling)
RRC	Radio Resource Control (layer of the protocol stack)

RRM	Radio Resource Management
RX	Receiver
S1	The 3GPP S1 Interface between an eNodeB and an MME
S1-Flex	A 3GPP S1 feature in which an eNodeB has S1 interfaces to multiple MMEs
SC	Small Cell
SCF	Small Cell Forum
SC-FDMA	Single-Carrier Frequency Division Multiple Access
SCNO	Small Cell Network Operator
SCP	Secure, Contain, Protect
SCTP	Stream Control Transmission Protocol
SDN	Software-Defined Networking
SDR	Software-Defined Radio
SecGW	Security GateWay
SFTP	SSH File Transfer Protocol
SGW	Serving GateWay
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SON	Self-Organizing Network
SS	Solution Set
SSCP	Systems Security Certified Practitioner
SSH	Secure Shell
SW	Software
TB	Transmission Block
TCP	Transmission Control Protocol
TDD	Time Division Duplex
TEID	Tunnel End-point Identifier
TLS	Transport Layer Security
TOF	Traffic Offload Function
TOFS	Traffic Offloading Service
TP	Transmission Protocol
TR	Technical Report
TU	Transcoding Unit
TTI	Transmit Time Interval (1ms in LTE)
TX	Transmitter
UDP	User Datagram Protocol
UE	User Equipment
UL	Uplink
USRP	Universal Software Radio Peripheral
VA	Video Analytics
VIM	Virtual Infrastructure Manager
VM	Virtual Machine
VNF	Virtual Network Function
VNFM	Virtual Network Function Manager
VSCNO	Virtual Small Cell Network Operator
vTU	virtual Transcoding Unit
WAN	Wide Area Network
WP	Work Package
XML	eXtensible Mark-up Language

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1. Deliverable outline

The target of the SESAME PROJECT is to design and develop a novel 5G platform based on small cells (SCs), featuring multi-tenancy between network operators (NOs), and also attach to them edge cloud capabilities to be offered to both the network operators and the mobile users. Thus, the key innovations proposed by SESAME focus on the novel concepts of a multi-operator (multi-tenancy) enabling framework and also on providing an edge-*based*, virtualised execution environment.

Deliverable D2.2 [1] presented the overall design and specification of the SESAME system architecture. Deliverable D2.3 [2] built on this, with a more detailed specification of the CESC components and deliverable D3.1 [3] "crystallised" these elements into a design for the Small Cell Prototype and PoC.

This report forms the Deliverable D3.4. It reports upon the status of the PoC demonstration system and the aspects of the design that it implements. Next, the relative success of the demonstrator is assessed against the original design objectives and any areas for further consideration are so identified. Finally, a brief conclusion summarises the overall success of the PoC demonstrator, what lessons have been learned and what further work is required in order to achieve a commercially deployable system.

1.2. Definitions of Terms and SESAME concepts

At this point, it is useful to provide definitions of terms and processes which will be used later in this document to describe the SESAME main concepts.

- **Small Cell (SC):** Does not change in the context of SESAME.
- **Execution infrastructure, micro-server (μs):** Specific hardware that is placed inside (probably) the Small Cell and provides processing power (and also maybe some memory and storage capabilities).
- **CESC (Cloud Enabled Small Cell):** The Small Cell device which includes a micro-server in hardware form.
- **Cluster of CESCs:** A group of CESCs that are collocated, exchange information and are properly coordinated. As a trivial case, one CESC can be called as a CESC cluster.
- **Light Data Centre (Light DC):** The hardware entity composed by the micro-servers of the CESCs forming a cluster.

The figure below (as in the subsequent section 1.3) provides an overview of SESAME CESC Cluster from a physical system perspective.

1.3. An Introduction to LTE Architectural Elements

In LTE, the Evolved Packet System (EPS) consists of the Evolved Packet Core (EPC) and the Evolved Universal Terrestrial Radio Access Network (E-UTRAN). Figure 1-2 shows the main components of the EPS together with their relevant interfaces. A detailed description of the EPS focusing mainly on E-UTRAN, can be found in [4], and more on the EPC can be found in [5].

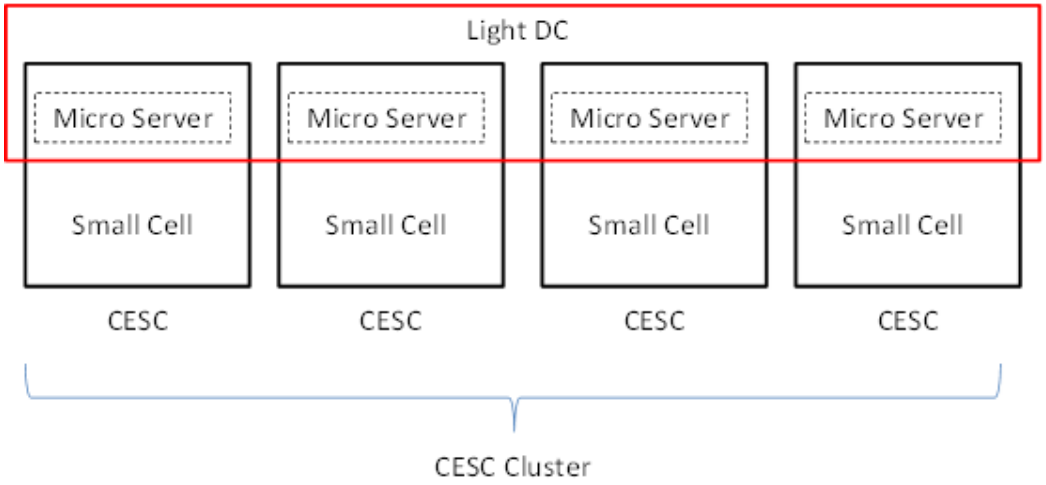

Figure 1-1: Conceptual view of SESAME CESC Cluster components

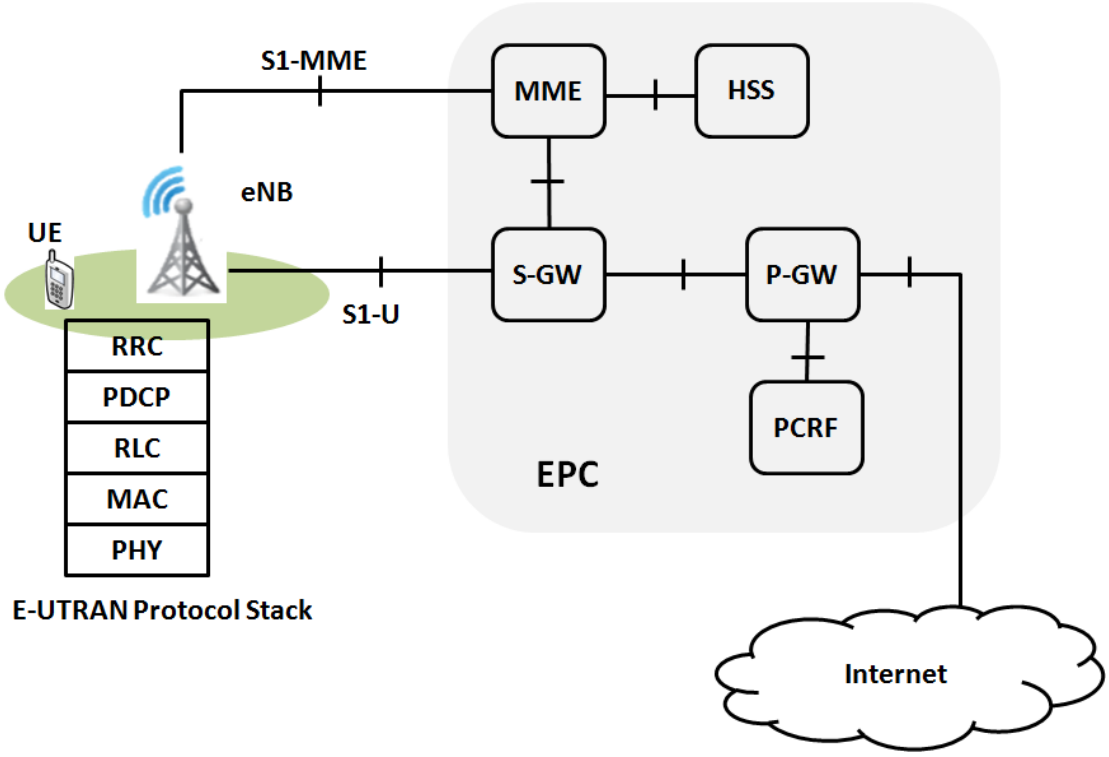

Figure 1-2: LTE Network Architecture

The EPC is composed primarily of the Mobility Management Entity (MME), the Home Subscriber Server (HSS), the Packet Gateway (PGW), the Serving Gateway (SGW), and the Policy and Charging Rules Function (PCRF). In brief, these different entities serve the following purposes:

- *MME*: This entity operates in the Control Plane (CP) and handles signalling related to mobility of the User Equipment (UE) and security. Furthermore, it is responsible for tracking and paging the UEs in idle mode, and is the termination point of the Non-Access Stratum (NAS) signalling.
- *HSS*: This is mainly a database (DB) containing user-*related* and subscriber-*related* information, and is involved in call and session setup, user authentication, and service authorisation.
- *PGW*: This is the interconnection point between the mobile network and the public Internet. IP traffic addressed to UEs is encapsulated at this stage by the GPRS Tunnelling Protocol (GTP) and is sent over the GTP User-plane (GTP-U) tunnel.
- *SGW*: This entity is the interconnection between the radio access network and the EPC and it is responsible for routing GTP-U packets between the PGW and the eNodeB. GTP-U packets received from the PGW are sent to the SGW and then to the eNodeB serving the particular destination UE, and vice-versa. In addition, it is also the "anchor point" for the GTP-U tunnel during intra-LTE mobility (i.e. handover).
- *PCRF*: This entity is responsible for flow charging, and for the authorisation of QoS resources

At the air interface between the UE and the eNodeB, the E-UTRAN protocol stack is as shown in Figure 1-2. In particular, the protocol stack includes the Radio Resource Control layer (RRC), the Packet Data Convergence Protocol (PDCP) layer, the Radio Link Control (RLC), the Medium Access Control (MAC), and the Physical Layer (PHY).

- *RRC*: This layer operates in the control plane and is responsible for Layer 3 functions such as sending NAS and AS information. It is involved in establishment, maintenance and configuration of the RRC connections. The RRC layer is also involved in mobility, measurement reports of the UE, and QoS and security key management,
- *PDCP*: This layer operates in the user plane, and is part of Layer 2. It is mainly responsible for ciphering, integrity protection, and in-sequence delivery of data units. The PDCP is also involved in header compression, and in data forwarding and integrity during intra-LTE handover.
- *RLC*: This layer also operates in the User-Plane as part of Layer 2. It is responsible for error correction through Automatic Repeat Request (ARQ), and the concatenation and segmentation of data units.
- *MAC*: This layer also operates in the User-Plane as part of Layer 2. It is mainly responsible for multiplexing together the data to and from multiple UEs, together with that of the System Information Broadcast, Paging, etc., and assembling them into Transmission Blocks (TBs) to be transmitted over the PHY. It is associated with the Dynamic Resource Allocation function, commonly referred to as the MAC Scheduler, which schedules the data over the available Physical Resource Blocks (PRB) according to different scheduling policies. It schedules resources every Transmission Time Interval (TTI), which lasts one millisecond. The MAC layer is also responsible for error correction using Hybrid ARQ (HARQ).
- *PHY*: This constitutes Layer 1 of LTE. The transmission mode is organized either in Frequency Division Duplexing (FDD) or Time Division Duplexing (TDD). In the uplink (from UE to eNodeB) direction, Single-Carrier Frequency Division Multiple Access (SC-FDMA) is used, whereas in the downlink (from eNodeB to UE) Orthogonal Frequency Division Multiple Access (OFDMA) is used instead. Bandwidths used for a single carrier in an LTE system range from 1.4MHz to 20 MHz, as defined by 3GPP specifications. PRBs are composed of 12 sub-carriers spaced 15 kHz apart, giving a total bandwidth of 180 kHz per PRB. The number of PRBs available,

therefore, depends on the bandwidth of the LTE system with 100 PRBs being available in a 20MHz bandwidth (allow for guard bands). The modulation schemes used are QPSK, 16-QAM and 64-QAM. Multi-Input Multi-Output (MIMO) techniques may also be employed to improve robustness or data rates between the UE and the eNodeB. Further details may be found in [6].

In addition to the air interface described above, the other key interfaces of the eNodeB are:

- *S1*: This is the logical interface to connect an eNodeB to the EPC, often implemented over fibre or gigabit Ethernet (GbE). It is sub-divided into the U-plane interface to the SGW, referred to as S1-U, and the interface to the MME, referred to as S1-MME. An eNodeB can be connected to the elements of one operator's EPC using an S1 and connection to multiple operators is possible. In S1-Flex, the same eNodeB can be connected too multiple MME/SGW of the same operator. Finally, the S1 interface can also be sued for the purpose of handover when UEs traverse adjacent cells.
- *X2*: This is the logical interface used to connect between eNodeBs, and is also often implemented over fibre or gigabit Ethernet. It is used to exchange signaling between base stations and for the purpose of X2 handover. It is further used for load management and to support various Self-Organising Network (SON) techniques.

2. SESAME Architecture Recap

This section provides a recap of the SESAME CESC Prototype design contained in deliverable D3.1. It provides a summary of the elements of the SESAME architecture against which the PoC implementation can be compared.

Note that a significant portion of the text in this section has been reproduced from previous deliverables and is provided here for convenience.

2.1. Overview

The overall SESAME architecture is described in deliverable D2.2 [1], and presented in Figure 2-1 below.

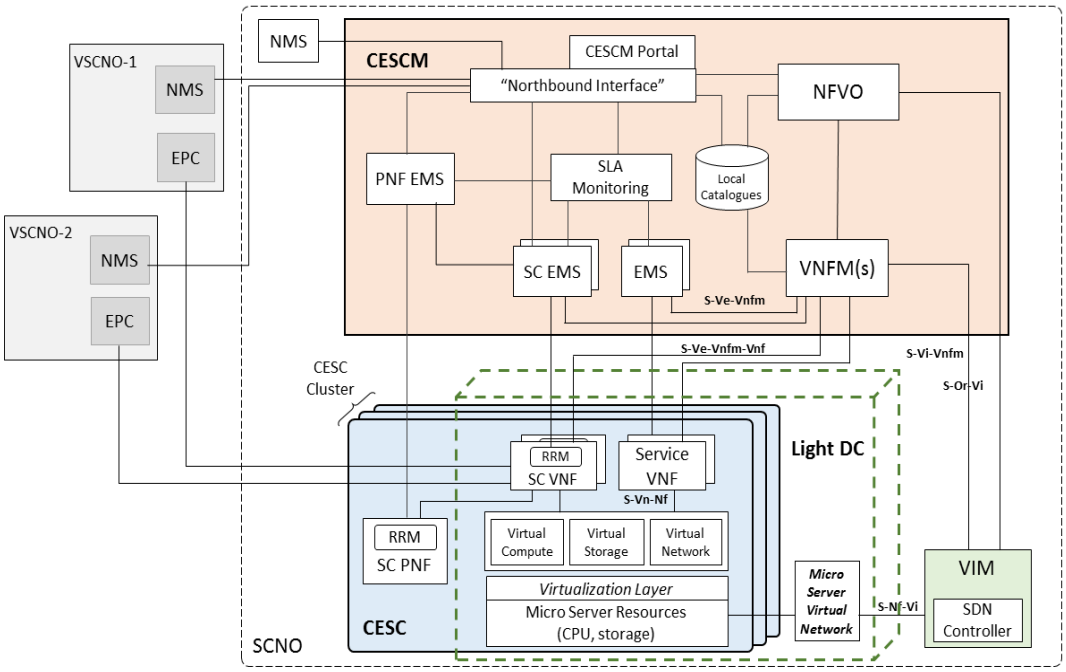

Figure 2-1: Overall SESAME Architecture

The CESC is composed of two co-located and network-connected physical devices:

1. A Small Cell Physical Network Function (SC PNF), which implements the radio interface and main protocol aspects of the LTE (H)EnB.
2. A micro-server platform, which forms a node in the distributed Light Data Centre (Light DC).

All the CESCs in a CESC cluster communicate over a local network and the collection of micro-servers within the cluster forms the distributed Light DC of that cluster.

The Light DC provides a virtualisation environment for running a collection of VNFs which, together with the SC PNFs, provide the complete functionality of the CESC Cluster. This is illustrated in Figure 2-1.

The fact that SC functions are divided between the physical cell and the micro-server is the way SESAME implements the functional split discussed in Section 2.3 of the Deliverable D2.3 [2], while resources in the Light DC are of different type and include virtual compute, virtual storage and

virtual network. Moreover, each micro-server shall have deployed a virtualization layer (or hypervisor) to create the virtual infrastructure. The virtualised infrastructure is glued together with the physical one, to create an environment which provides services to different types of users. In specific, UEs not necessarily are aware of the above virtualization but they consume the services offered by service providers accessing the SESAME infrastructure. Therefore, users might be aware that they are connected to the network of SESAME, or might just enjoy the radio access in seamless fashion.

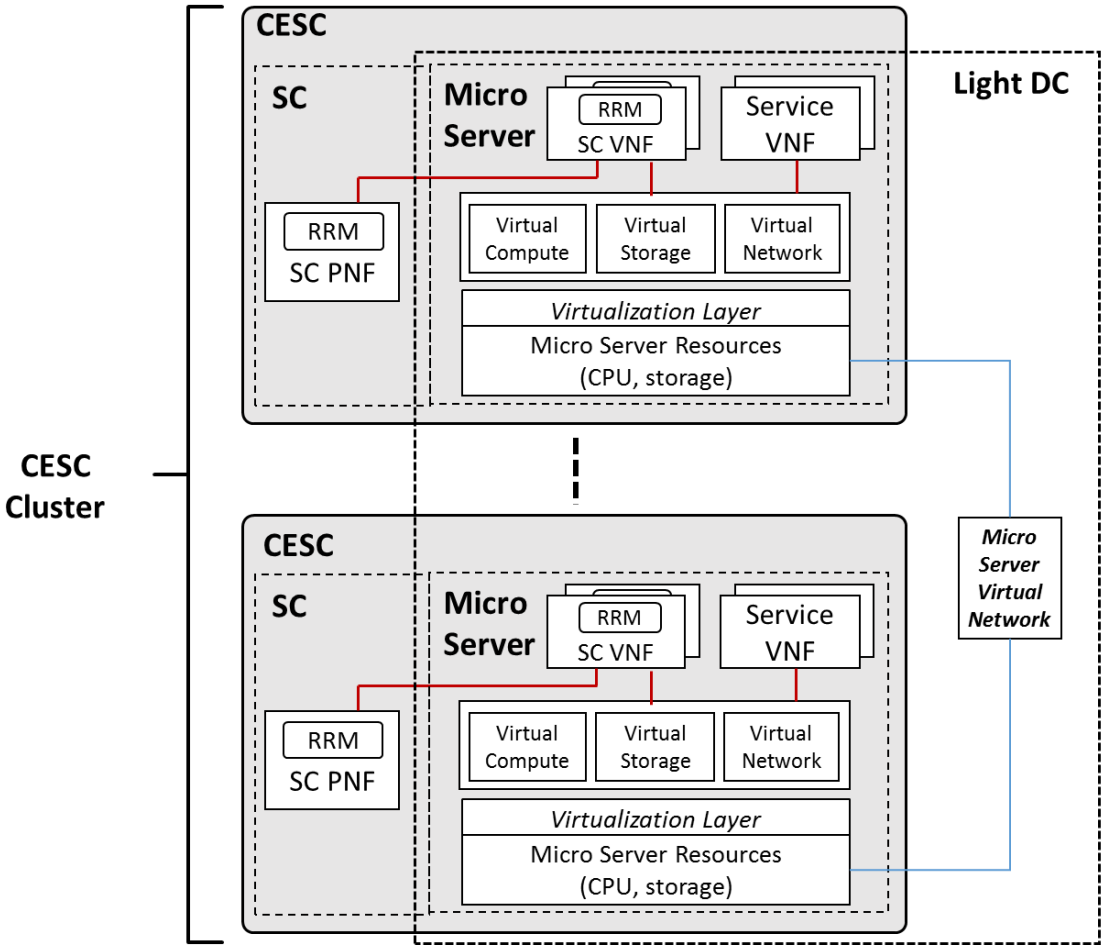

Figure 2-2: Cluster Architecture

2.2. CESC and Light DC

The CESC is the fundamental building block of the SESAME architecture providing the virtualization platform for hosting SC-VNF, Service VNFs and an implementation of PNF corresponding to the chosen functional split.

The close proximity of small cells provides an opportunity to aggregate resources into CESC clusters (Light DC) that can support a diverse set of MEC use cases. The Light DC is envisioned to provide the necessary virtualization resources to realize the objectives of SESAME.

To support the required network functions of a small cell and edge services in a virtualized environment, the light DC leverages the hardware and software resources of the CESC clusters. The light DC provides the necessary computing, networking and storage resources on top of a virtualization layer. The light DC is essentially a platform for realizing the benefits of SDN/NFV at the network edge. The network functions within light DC are implemented as "VNFs" which may be hosted on top of virtual machines are hosted on top of a hypervisor layer (e.g. KVM-*based* solutions) or as "Containers".

The SESAME architecture facilitates deployment of multiple CESCs owned by a Small Cell Network Operator (SCNO) that can be leased to multiple other operators, i.e. the Virtual Small Cell Network Operators (VSCNOs), willing to provide coverage at a given venue. These CESCs will consist of small cell physical network functions (PNFs) and small cell virtual network functions (VNFs).

The status of the Light DC prototype is described in detail in deliverable D4.4 [7] and is not covered in this document.

2.3. Small Cell PNF (SC PNF)

The Proof of Concept (PoC) PNF uses the standard S1 interface between SC PNF and SC VNF. The PNF implements the normal functions of a standard single-carrier eNodeB or HeNB, managing the allocation and scheduling of radio resources towards UEs and maintaining signalling and user plane connections towards the Core Network (CN). In the PoC implementation, the SC PNF operates exactly as if it were directly connected to an EPC or collection of EPCs.

Thus, the SC PNF offers a standard Uu LTE interface towards the UEs; and an S1 traffic interface (signalling and User-Plane) towards the rest of the CESC. The PNF is primarily managed via a standards-based TR-69[1] interface in line with normal 3GPP practice. The Data Model (parameter set or attributes) is based on the standard TR-196[2] data model, with some vendor extensions. HTTP-*based* file transfer is used for supplementary management operations such as download of software or upload of Performance Management report files.

The SC PNF supports a basic MOCN (Multi-Operator Core Network) capability:

- It broadcasts multiple PLMN-IDs so that UEs of multiple operators can request access to their PLMN of choice (normally their Home PLMN except in the case of roaming).
- It associates each connected UE with one of the PLMN-IDs.
- It maintains and broadcasts a neighbour list associated with multiple PLMN-IDs.
- It will only direct UEs to hand over to a neighbour of the same PLMN-ID.

The SC PNF does not offer any explicit differentiation of service between the PLMN-IDs.

Each PLMN-ID can be marked as “cellReservedForOperatorUse” by management action so that a particular Tenant (VSCNO) can inhibit its users from accessing the cell.

[1] TR-069 (Technical Report 069) is a technical specification that defines an application layer protocol for remote management of end-user devices. It was published by the Broadband Forum and entitled CPE WAN Management Protocol (CWMP). For more details see, *inter-alia*: https://en.wikipedia.org/wiki/TR-069

[2] TR-196 (Technical Report 196) is a Broadband Forum technical specification. Its official title is "Femto Access Point Service Data Model." The purpose of this Technical Report is to specify the Data Model for the Femto Access Point (FAP) for remote management purposes using the TR-069 CWMP. For more details see, *inter-alia*: https://en.wikipedia.org/wiki/TR-196

2.4. Small Cell VNFs (SC VNFs)

Associated with each SC PNF, there is a SC VNF for each Tenant (i.e. VSCNO); and a single SC-Common VNF to provide a coordinating role, as illustrated in Figure 2-3 below.

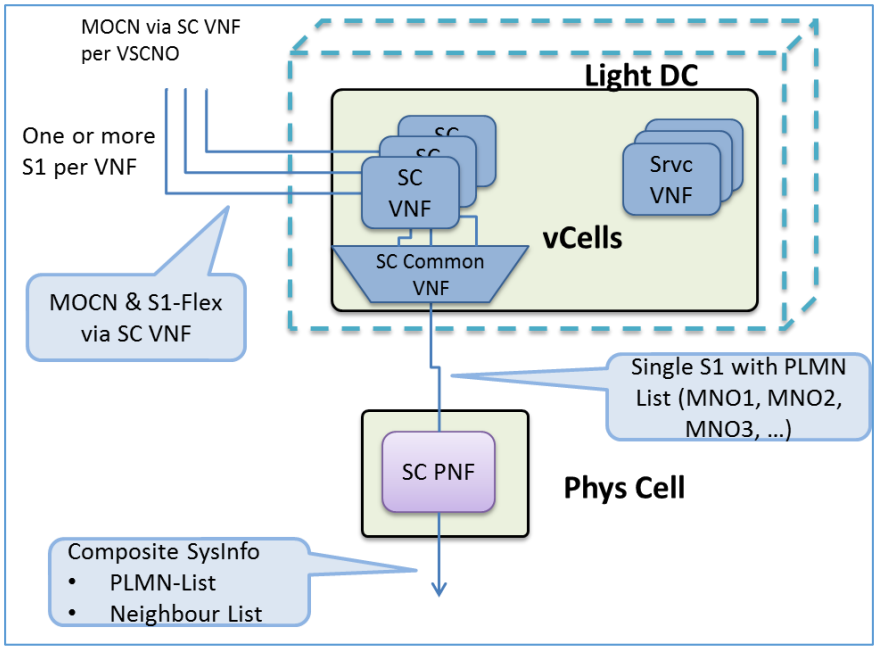

Figure 2-3: SC VNFs – Basic MOCN Aspects

Each SC VNF and SC-Common VNF lies on the S1 interface between the SC PNF and the EPC of a particular tenant. From the SC PNF's perspective, the SC-Common VNF looks like an EPC; and from the Operator's EPC perspective, the SC VNF appears as a standard single-operator Small Cell (eNodeB or HeNB).

Each SC VNF may support multiple S1 connections towards the EPC (using S1-Flex). The SC VNF provides a full implementation of the Non-Access Stratum (NAS) Node Selection Function (NNSF) and is responsible for selecting an MME to serve each UE.

Note: if a HeNB-GW is implemented for a tenant in the CESC, then S1-Flex is not used at the SC-VNF, but may be used at the HeNB-GW.

Signalling

All S1 signalling passes through the SC VNF. This allows the SC VNF to observe and interject in the signalling sequences. The most likely points of interjection are

- UE Admission.
- RAB Admission.
- Handover.

In addition, simply monitoring the call sequences allows the SC VNF to interpret the usage of the User Plane (RABs) to inform user- and service-specific behaviour of the associated User Plane.

Resource coordination between tenants

To assist in decisions regarding Admission Control and Handover, the SC-Common VNF (see below) provides the SC VNFs with a shared view of allocated resources

User Plane

All S1 user plane traffic between the UE and the EPC passes through the SC VNF. The S1 traffic is encapsulated in the standard GTP-U protocol, with each RAB associated with a GTP Tunnel Endpoint ID (TEID). In each direction of transfer (upstream, downstream), the SC VNF intercepts the RABs and relays the user data within them to User Plane Service Chains.

The General Packet Radio Service (GPRS) Tunnelling Protocol (GTP) was designed for tunnelling and encapsulation of data units between various core network entities [8]. GTP is made up of the following protocols:

- GTP-C: Control signalling between GTP peers.
- GTP-U: Transporting user data.
- GTP: Charging data.

GTP packet data units (GTP-PDUs) are classified as either G-PDUs or signalling messages [8]. The G-PDU constitutes a GTP tunnel header and a user data packet (T-PDU) for example an IP datagram. The T-PDU is the payload that is tunnelled in the GTP tunnel. Signalling messages are GTP-PDUs, except G-PDUs, sent between GTP peers as path or tunnel management messages. The GTP tunnel header consists of three individual headers, namely; an IP header, a UDP header and a GTP header.

The SESAME CESC architecture uses GTP tunnelling, first between the Small Physical Network Function (SC PNF) and the Small Cell Virtual network functions (SC VNFs) located at the micro-server and second between SC VNFs and the core network of one of a multiple of Virtual Small Cell Network Operators (VSCNOs). Consequently, all the traffic arriving at or departing from the micro-server is GTP encapsulated. However, the function specific service VNFs process IP datagrams.

The GTP part of the SC-VNF decapsulates the GTP PDUs and forwards the IP datagrams to the service VNFs. The service VNFs perform functions such as, deep packet inspection, transcoding, caching and context aware routing etc., and forward the IP datagram back to the GTP part of the SC-VNF. The GTP part of the SC-VNF then performs GTP encapsulation and forwards the GTP PDUs to the relevant serving gateway (SGW).

Figure 2-4 presents the uplink user plane service chain.

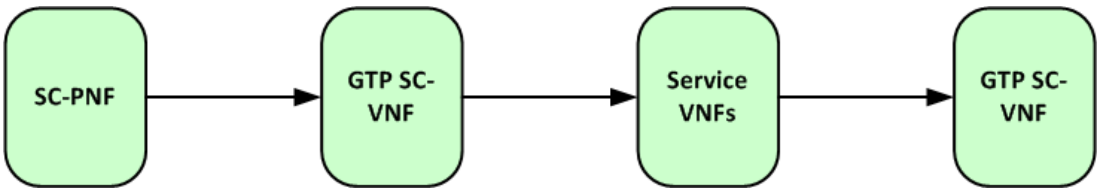

Figure 2-4: Service Chaining

Management

From a management perspective, the Operator sees the SC VNF as a cell, but with limited flexibility. For example the Operator is not able to change parameters that are implemented in the SC PNF and common to all Operators (e.g. transmit power).

2.5. SC-Common VNF

The SC-Common VNF is a "helper" function to support coordination of the SC VNFs.

Signalling

In the upstream direction (from the PNF towards the VNFs), the SC-Common de-multiplexes the S1 messages, directing them to the correct SC VNF based on PLMN-ID. In the downstream direction, the SC-Common simply merges all S1 messages into a common Stream Control Transmission Protocol (SCTP) connection.

RRM

The SC-Common monitors the RAB assignments, modifications and releases for all tenants, for all causes (including handover) and maintains a resource view that is available to all SC-VNFs.

User Plane

The SC-Common VNF is not involved in user plane traffic, which is exchanged directly between the SC-VNF and PNF and between the SC-VNF and EPC.

2.6. Service Chaining

A service chain is an ordered list of one or more functions that operate on the user plane data of a VSCNO. Each service in a service chain performs a specific task such as video transcoding or web caching and is provided by a VNF running in the CESC. Service chains are attached to the SC-VNFs such that each VSCNO sharing the CESC may implement different service chains. They may be global to the SC-VNF and therefore apply to all of the VSCNO's user data or may be specific to certain classes of E-RAB, as distinguished by the QCI value.

In the PoC demonstrator the following design aspects from deliverable D3.1 hold true:

- Both ends of the service chain are anchored in the SC-VNF; on receipt of a GTP-U packet, the SC-VNF pushes the packet into the service chain and receives it back again once it has been processed by the entire chain. The SC-VNF then forwards the processed packet to its final destination.
- There are separate service chain endpoints for uplink and downlink user plane traffic.

Figure 2-5, below, illustrates the possible user plane traffic flow for a VSCNO service chain:

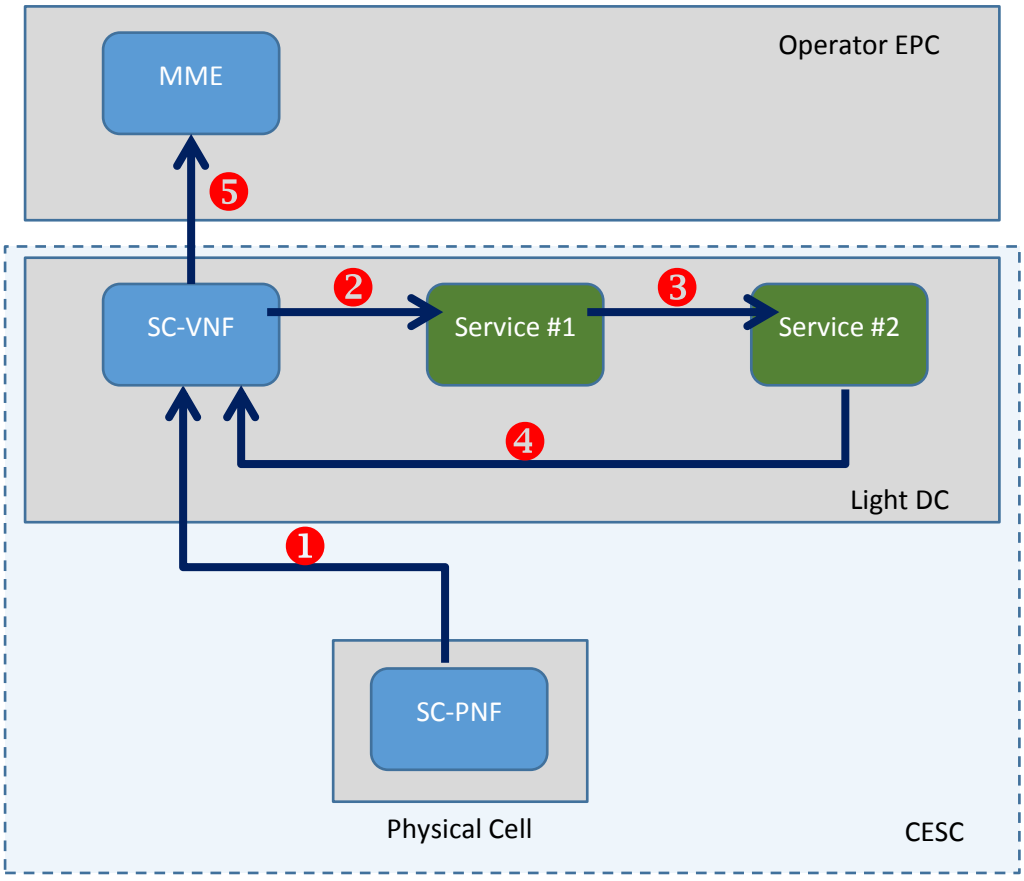

Figure 2-5: Example Service Chain Traffic Flow

2.7. PNF EMS

The PNF EMS is responsible for managing the PNF. It provides, via either the CESCM Portal or Northbound Interface, the SCNO with a consolidated view of all of the SC PNFs. This view is decomposed into separate views for:

- Configuration Management (CM);
- Fault Management (FM);
- Performance Management (PM).

Each view (CM, FM and PM) is organised as a hierarchy of managed objects.

The southbound interface between the PNF EMS and the SC PNF is provided by TR-069 using the TR-196 data model as this is an industry standard for the management of small cells.

The northbound interface between the PNF EMS and the CESCM Northbound Interface uses the applicable sub-set of the integration reference points offered by the Northbound Interface itself and described in Section 2.9 below.

2.8. Small Cell EMS (SC EMS)

The SC EMS is responsible for managing the SC VNFs. It provides, via either the CESCM Portal or Northbound Interface, each VSCNO with a consolidated view of the portion of the network that they are able to manage. This view includes a set of managed objects that represent:

- The SC VNFs that the VSCNO owns.
- One or more MMEs that to which VNFs may connect.
- If present, one or more S1 Gateways to which VNFs may connect as an alternative to MMEs. Note that it is possible that some VSCNOs may have a strong preference to make use of an S1 Gateway whereas others may not.
- The neighbour cells that the VNF may initiate handovers to. These fall into three broad categories:
    - Other SESAME CESCs.
    - MOCN enabled macro cells supporting multiple PLMNs.
    - Non-MOCN macro cells supporting a single PLMN.

2.9. Northbound Interface

SESAME provides a northbound interface between the CESCM and each tenant operator's NMS. It is also used internally by the CESCM, to provide the underlying capabilities of the CESCM Portal. This interface is divided into Fault, Configuration and Performance management functions. Security management is provided by a combination of the Configuration and Fault management functions. Accounting management is not provided by SESAME as this is normally performed in an operator's core network.

The northbound interface is provided by the following standards compliant 3GPP Integration Reference Points (IRPs). In all cases, SESAME makes use of the SOAP[3] Solution Set.

Due to the shared nature of this interface, security (i.e. the prevention of eavesdropping) is essential and therefore all data exchange is encrypted. Such encryption is possible through the use of HTTPS (i.e. HTTP over TLS) in the communication channels.

[3] SOAP (originally Simple Object Access Protocol) is a protocol specification for exchanging structured information in the implementation of web services in computer networks. Its purpose is to induce extensibility, neutrality and independence. It uses XML Information Set for its message format, and relies on application layer protocols, most often Hypertext Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission. For more details see, *for example*: *https://en.wikipedia.org/wiki/SOAP*

2.10. CESCM Portal

The CESCM Portal is a control panel web GUI that serves as the entry point for the users, both SCNO and VSCNO, to the CESCM and constitutes the main graphical frontend to access the SESAME platform. The CESCM Portal in general provides visual monitoring information of the running services and agreed SLAs and available network services/VNFs in the catalogues as well as infrastructure and service parameters configuration.

The CESCM Portal supports two logins with different associated permissions and enabled options:

- Administrator login for SCNO to configure CESCM elements such as NFVO, VNFM and introduce/delete VNFs to/from the local catalogues.
- User login for VSCNO to retrieve monitoring information of the running services and their compliance with the agreed SLA, as well as request for creation, instantiation and deletion of services.

The CESCM Portal is the entity responsible for granting the access to the CESCM. Hence, some additional CESCM Portal functionalities that are related to security and privacy of SESAME actors are: Authentication, Authorisation, and SLA Conformance.

2.11. SLA Monitoring

SLA Monitoring is a real-time monitoring element that allows the enforcement of the agreed SLAs between the business role players (e.g.: SCNO and VSCNO). Taking monitoring information from EMS, the SLA Monitoring is able to evaluate the level of conformance between the current service status and the KPIs defined in an SLA.

In case an SLA violation occurs, the SLA Monitoring module triggers reconfiguration alerts based on decision policies for the EMS and NFVO components in order to adjust the service parameters to the SLA levels. Upon receiving such alerts, these components initiate, *if possible*, the reconfiguration, migration, and scaling- in and out of the existing services to comply with the service agreements while dynamically maximizing the utilization of the resources.

SLA definitions are entities that will be stored in the PNF EMS as a managed element and that will be later notified to the SLA Monitoring module for their evaluation.

Additionally, the SLA Monitoring is able to provide information about the current SLA status for each tenant and service. This information can be obtained either through the CESCM Portal or the Northbound Interface components, taking into consideration possible access restrictions based on user authentication and security policies.

3. PoC Status Summary

This section compares the functionality implemented in the PoC demonstrator against that defined in Deliverable D3.1. It identifies any shortfalls -or problems- encountered and indicates where additional work may be required. As such, it provided a view on the overall success of the SESAME PoC and its ability to meet the associated objectives of the SESAME project.

3.1. Architecture Components

The majority of the modules in the architecture have been delivered and are communicating as planned:

- The SC-PNF connects to the SC-C-VNF of its host CESC.
- The SC-C-VNF provides both a multiplexing function, separating out the S1 control plane messages relating to each VSCNO, and a cell-wide admission control function. It has a separate northbound S1 connection to each configured SC-VNF and routes only the traffic applicable to the served VSCNO to each SC-VNF instance.
- Each SC-VNF provides the network slice for a particular VSCNO. It maintains a dedicated EPC connection and polices the VSNOs network slice by capping both the number of UEs and bandwidth that the VSCNO may consume on a given physical cell.
- The PNF delivers detailed performance management reports that the EMS post-processes into separate, per-VSCNO, reports.
- The EMS provides each VSCNO with a view of their virtual network that is isolated from that of other VSCNOs. Each VSCNO may provision virtual cells in a manner analogous to the provisioning of a physical cell and can manage these virtual cells:
    - The VSCNO can provision, decommission, administratively lock and unlock their virtual cells.
    - They may receive tailored performance management reports for each of their virtual cells.
    - By agreement with the SCNO, each VSCNO may apply SLAs across specific sub-sets of their virtual cells, each specifying a custom set of KPIs and associated thresholds. The EMS monitors these SLAs periodically and raises an alarm if any of the configured thresholds are not met.

Thus, it can be seen that the PoC successfully delivers clean network separation from both the operational and management perspectives.

3.2. Light DC

Currently, the SC-VNF and SC-C-VNF functions are implemented in a PC based environment that approximates the Light DC. This environment consists of:

- A PC running full CentOS 6.8[4] as the host OS[5],
- A Hypervisor provided by Oracle Virtual Box 5.1.14[6] or later,
- Multiple virtual machine instances running Ubuntu 14.04[7] for the VNFs and CentOS 6.8 Minimal for the EMS. These instance support:
  - Exactly one instance of the PNF EMS / SC EMS,
  - Exactly one instance of the SC-Common VNF.
  - From one to six instances of the SC VNF.

The above environment validates the proposed Light DC architecture and connectivity, demonstrating the separation of each VSCNO's network slice.

If possible, the SC-Common VNF and SC VNF will be ported to the Light DC as part of WP7.

At the very least, the processing resources required by these functions will be assessed in order to validate the feasibility of running them on the Light DC.

[4] See: *https://wiki.centos.org/Manuals/ReleaseNotes/CentOS6.8*
[5] The desktop environment is needed to run the VirtualBox Hypervisor.
[6] See: *https://www.virtualbox.org/wiki/Downloads*
[7] For further details see: *http://releases.ubuntu.com/14.04/*

3.3. Small Cell PNF (SC PNF)

In the PoC, the Small Cell PNF is provided by the ip.access E40 LTE Access Point [9]. No modifications have been necessary to the configuration management aspects of the SC PNF and it has performed as intended. The performance management reports produced by the SC PNF have been extended to provide per-PLMN versions of a number of counters. These are then post-processed by the EMS into separate per-VSCNO reports.

As the E40 LTE AP uses the standard TR-196 [10] data model, it is envisaged that the Access Points of other small cell vendors supporting the same data model and MOCN functionality could be substituted with only minor integration being required.

An area where the functionality delivered by the PoC could be improved would be by enhancements to the SC PNF is the Performance Management reports upon which SLA monitoring is based.

3.3.1. PM Granularity Period

A Performance Management report's granularity period defines the time frame over which measurements are captured, aggregated and reported. Currently, the PNF provided by the ip.access E40 implements a fixed length granularity period of one hour. In order to provide timely Self-X functionality, the ability to capture performance measurements over a shorter period such as 5, 10 or 15 minutes would be an advantage. It would be most useful if it were also possible to configure different measurements with different granularity periods so that each measurement was recorded and calculated over a time-frame appropriate for the measurement concerned.

3.3.2. Per-PLMN (VSCNO) Reports

The standard LTE performance measurements described in 3GPP 32.425 [11] are biased toward the RF performance of the (H)eNB as a whole and do not currently consider the possibility of capturing measurements on a per-PLMN (or per-VSCNO) basis. In the PoC, the SESAME PNF, provided by the ip.access E40, supports a total of 13 per-PLMN (thus per VSCNO) measurements split between GTP-U usage and RRC Connection establishment. Additional per-PLMN counters that might be provided include:

- E-RAB set-up and release counts and times. A comparison of such values across different PLMNs would be useful in identifying problems in a particular VSCNO's EPC.
- Handout attempts, successes and failures. Separate counters would help identify problems with specific neighbour cells or in specific EPCs.
- Average and maximum UEs per-PLMN plus aggregate in-session activity time per PLMN.
- Detailed user plane statistics such as packet delay and packet drop rate.

3.4. Small Cell VNFs (SC VNFs)

Within the PoC, the SC VNF operates as intended and provides all of the planned functionality:

- Each SC VNF serves a single PLMN and can connect to a separate EPC via a dedicated S1 connection.
- Each SC VNF polices its "network slice" in terms of both the number of UEs that it admins and the total uplink and downlink bandwidth that it consumes.
- Each SC VNF may be configured with a separate service chain for processing user plane traffic. The integration with the service chain demonstrators will be tested as part of WP7.

An area where additional SC VNF functionality might be considered is that of performance management.

Although the SC VNF is responsible for policing VSCNO specific admission control (both in terms of maximum UEs and maximum allowed uplink and downlink bandwidth), in the PoC, the reporting of actual usage is provided by the SC PNF. Architecturally, it might be better for SC VNF to measure, report and police these aspects.

3.5. SC-Common VNF

Within the PoC, the SC VNF operates as intended and provides all of the required functionality:

- It de-multiplexes S1-AP signalling from the SC PNF and routes it towards the appropriate SC VNF.
- It multiplexes S1-AP signalling from each SC VNF towards the SC PNF.
- It performs cell-wide admission control.

With the architectural split adopted by SESAME, no enhancements are envisaged for the SC Common VNF.

3.6. Service Chaining

3.6.1. Overview

The PoC provides service chaining functionality; user plane traffic arriving at the SC VNF may, optionally[8], be routed by the service chain for processing.

On receipt of traffic returned by the service chain, the SC VNF forwards it to its uplink (UL) or downlink (DL) destination.

There are separate uplink and downlink service chains and the architecture is such that each SC VNF may have a different service chain allowing each VSCNO to make a different value proposition to their users.

The following VNFs are under development and can be used as service chain functions, integrated with the PoC as part of WP7:

- Deep Packet Inspection (vDPI) – vDPI is designed to analyse in real-time network traffic, to recognize specific applications and to categorize each traffic flow according to its service.
- Video Transcoding (vTU) - The VTU provides video and audio transcoding functions together with local storage capabilities of pre-recorded audio/video files. The services provided by the vTU can be accessed through a web-service-*based* interface, available from any browser. Through the vTU, users can originate or receive live video streams.
- vFirewall – The vFirewall control the incoming and outgoing packets to and from the inner network. It provides security barrier against potential attacks coming from the Internet that can disrupt the services running in the inner network.
- vVideo Analytics - This function is used to identify the regions in a video frame that are likely to contain a particular object of interest. For example, if an object of interest is a moving object or a green object, this function is to identify all the image regions in a video frame that contain such kind of objects.

[8] Service chaining is enabled and disabled by configuration.

3.7. Small Cell EMS (SC EMS) and PNF EMS

Within the PoC, the SC EMS and PNF EMS are provided by a single system based on the ip.access Network Orchestration System (NOS). SESAME specific EMS functionality includes:

- A Management Information Base (MIB) that includes Virtual Network Operator and Cloud Enabled Small Cells sub-trees providing tailored management views to the VSCNO and SCNO users.
- SESAME specific business logic for the provisioning of virtual cells and the configuration of their associated PNF and VNF.
- SESAME specific business logic that partitions the network into separate network slices such that a VSNO cannot view or interact with the managed objects of either the SCNO or another VSNO.

This functionality is delivered to the end-user by the NOS Client GUI, which provides Configuration Management, Fault Management and Performance Management views of the MIB. Different NOS client users have different access rights to the managed object hierarchy in order to provide network separation. For example:

- An SCNO user may view the whole network.
- A VSCNO user is only able to view the managed object relating to their network slice. They are unable to view either the objects belonging to the SCNO or those of another VSCNO.

Within the PoC, the GUI aspects of the EMS operate as intended and provide all of the required functionality. The following screenshots illustrate the functionality provided by the EMS:

Figure 3-1, **Figure 3-2** and **Figure 3-3** below illustrate the configuration management views provided to an SCNO user and two VSCNO users of different virtual networks. These illustrate the respective sub-sets of the managed object hierarchy available to each user and the isolation between the users of different VSCNOs.

Figure 3-1 illustrates the SCNO's view of a network that has two CESCs: CESC Shopping Mall and CESC Stadium. The network hosts two VSCNOs: "Not Spots" and "Pop-Up Events". As owner of the network, the SCNO user is also able to view the managed objects relating to these VSCNOs.

Figure 3-2 illustrates the management view provided to VSCNO "Not-Spots". They are only able to view the managed object and alarms relating to their own network slice and have no visibility of information relating to the SCNO or another VSCNO.
Similarly, **Figure 3-3** illustrates the view provided to VSCNO "Pop-Up Events". Again, they only have visibility of their own network slice and have no access to SCNO owned managed objects or those of another VSCNO.

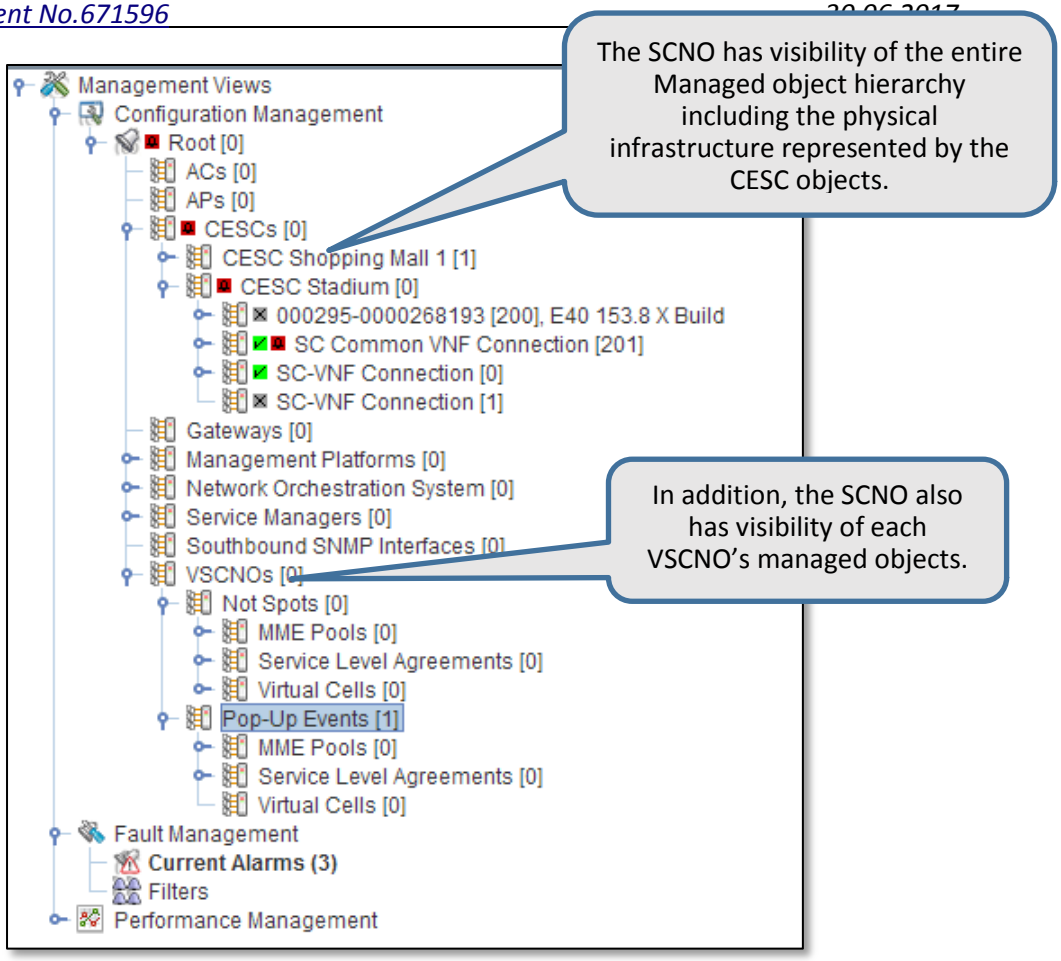

Figure 3-1: SCNO View

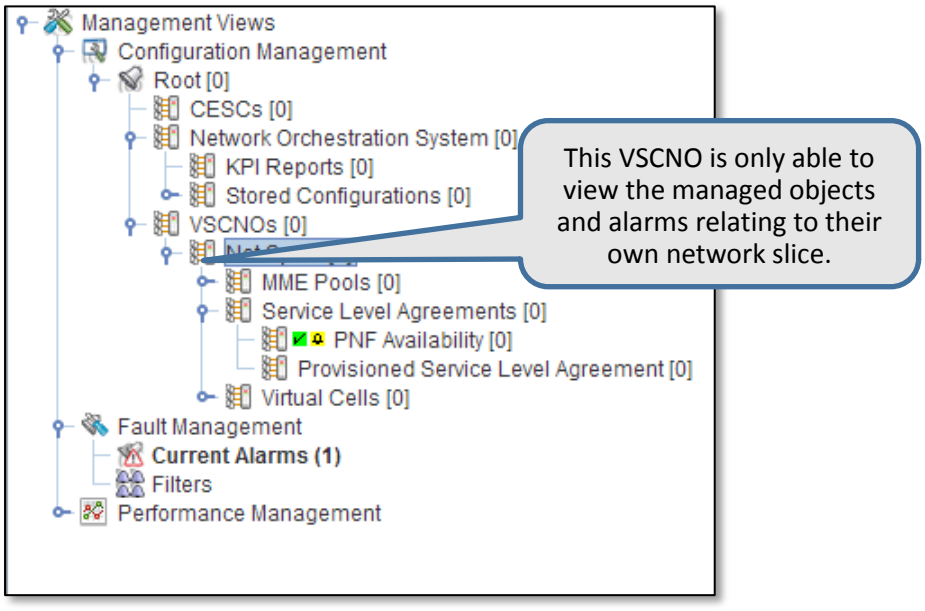

Figure 3-2: VSCNO "Not Spots" View

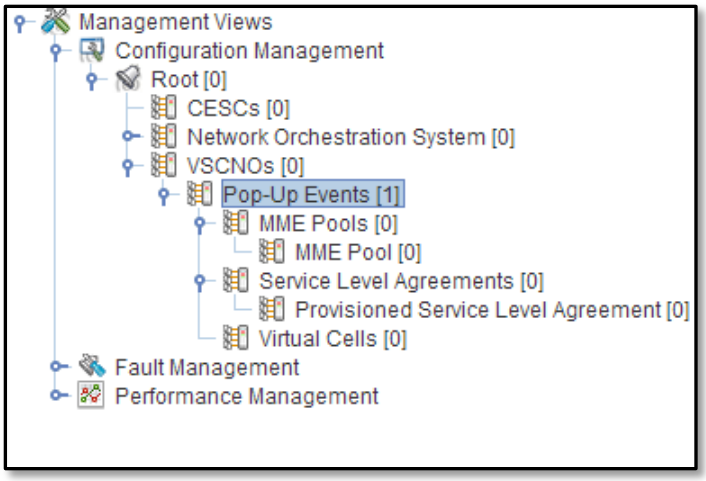

Figure 3-3: VSCNO "Pop-Up Events" View

In a commercial deployment, it would make sense to split the Small Cell EMS from the PNF EMS, as originally envisioned in D3.1. This would alleviate any security concerns that the SCNO might have with respect to granting VSCNO access to their EMS. It would also allow the Small Cell EMS to implement additional security measures such as only permitting client access via a suitably secured VPN tunnel.

Another area where further study is required is the work-flow of virtual cell provisioning. The process implemented by the current PoC assumes that CESCs are provisioned first and that a VSCNO then provisions their virtual cell on the CESC that best matches their criteria in terms of coverage and capacity. If no suitable CESC is available, the virtual cell cannot be provisioned.

An alternative approach would permit the provisioning of a virtual regardless of whether or not there is an available CESC to host it. In the case where there is not, the virtual cell would be operationally disabled and some form of work order would be generated by the system.

Once a suitable CESC became available (as a result of the SCNO acting upon the work order) the virtual cell would be assigned to the CESC and would become operationally enabled.

3.8. Northbound Interface

Effort limitations have not permitted the implementation of all of the Northbound Interface functionality as planned in deliverable D2.4. Table 1 below summarises what has and has not been implemented:

Northbound Aspect	Status in the PoC
Configuration Management	Partially implemented. The PoC implements the SOAP solution set of the CM IRP as defined in 3GPP 32.306 [12] and supports the majority of the Generic, Basic, Kernel and Notification IRPs defined in 3GPP 32.316 [13], 32.606 [14], 32.662 [15], 32.306 [12], *respectively*. See Appendix A for details. The SESAME IRP proposed in D2.4 has not been implemented but a proposed specification is provided in Appendix B. In addition, clean isolation between different VSCNO users of the Northbound CM interface is not implemented and one VSCNO can potentially view and modify the managed objects of another VSCNO.
Fault Management	Not implemented. Deliverable D2.4 specified that SESAME would support the Fault Management IRP specified in 3GPP 32.111 [16] parts 2 and 6 (SOAP solution set). This interface has not been implemented. However, as this is a standard 3GPP IRP, an implementation in SESAME would add no specific value in this area.
Performance Management	Partially implemented. A compliant subset of the XML PM file format described in 3GPP 32.435 [17] is implemented, as detailed in Appendix C. The segregation of PM reports into separate SCNO and VSCNO views, as described in D2.4, is fully implemented. The IRP operations defined in 3GPP 32.412 [18] and SOAP Solution Set described in 3GPP 32.416 [19] and specified in D2.4 [20] **have not** been implemented. Thus, file discovery using this interface is not supported. A subset of the File Transfer IRP described in 3GPP 32.341 [21] has been implemented. This provides a northbound file push using either SFTP or SCP[9] plus on-demand file pull using SCP. This allows each VSCNO to receive only those PM reports relating to their own network slice.

Table 1: PoC Northbound Interface Implementation Status

[9] For more details see: *http://www.scp-wiki.net/*

3.9. CESCM Portal

The full CESCM Portal will be completed as part of the Deliverable D5.2. This section describes the status of the work performed to-date.

Within the PoC, the CESCM Portal is provided by two separate interfaces:

- The EMS portal that provides client access to the SC EMS and PNF EMS.
- The NFV Portal that provides access to the NFVO and VNFM functions.

The combination of these two functions allow the CESCM Portal to fully support the objectives of a Web GUI that serves as an entry point for administrator (SCNO) and normal (VSCNO) users. It provides users with access to the agreed SLAs (via managed objects) and allows them determine whether these SLAs are currently being met.

3.9.1.EMS Portal

The SC EMS and PNF EMS are provided by a single client-server solution that is based on the ip.access NOS. It uses Java WebStart [22] to provide the downloading and starting of a GUI management client from a Web page published by the NOS server. Configuration Management, Fault Management and Performance Management functions are provided to SCNOs and VSCNOs by the NOS client. The set of managed objects that may be viewed and modified are controlled by access permissions granted to individual users. In summary, the feature operates broadly as follows:

- Permissions to sub-sets of managed objects are assigned to one more user groups.
- An individual user's permissions are determined by the groups to which he belongs are the greatest permission provided by those groups. For example if a user belongs to two groups, A and B, and one group provides read-only access to a specific managed object whereas another provides read-write access, then the user has the greater of these two which is read-write access.
- By creating appropriate groups, the SCNO is able to:
  - Assign permissions to SCNO users who are able to manage all parts of the network including those aspects belonging to VSCNOs and those belonging to the SCNO and not accessible to VSCNOs.
  - Assign permissions to VSCNO users such that they are only able to view their own "network slice" and are not able to view or interact with the managed objects of other VSCNOs or the SCNO.

3.9.2.NFV Portal

The NFV Portal is currently under development and will be delivered by Task 5.2.

3.10. SLA Monitoring

Within the PoC, SLA Monitoring is provided by an SLA Monitor service running on the EMS (NOS). The SLA Monitor runs periodically to inspect managed objects of type "Monitored SLA". The configuration parameters of each Monitored SLA object define the following SLA aspects:

- The geographic scope of the SLA; i.e., the set of virtual cells over which the SLA is applied. These may be defined as all of the virtual cells of a VSCNO, a specific list of virtual cells or all the virtual cells falling within a particular geographic region.
- The temporal scope of the SLA; i.e., the time-period over which it is evaluated.
- The KPIs and associated thresholds monitored by the SLA.
- The action to take when a KPI threshold is crossed and the SLA is deemed to be in breach.

In the PoC, the following design aspects are implemented:

- The processing of received PM data from the PNF into KPI values for assessment.
- The evaluation of multiple SLAs in response to received PM data.
- Geographic scope may be set to either all of the virtual cells of a VSCNO or a defined list of virtual cells. The geographic region option is not supported.
- The following KPIs have been implemented in the PoC:

Physical Cell Availability	Based on the *Cell Unavailable Time* metric defined in 3GPP 32.425 [11], this KPI presents the time that the PNF is available as a percentage of the granularity period.
Physical Cell Call Drop Rate	This KPI calculates an aggregate call drop rate for the physical cell using the following formula based on metrics defined in 3GPP 32.425: Sum(Number of PNF initiated E-RABs released per Cause) / (Sum(Initial E-RAB Setup Success per QCI) + Sum(Additional E-RAB Setup Success per QCI))]
Virtual Cell Uplink Throughput	This KPI provides the total uplink throughput, in octets, for a virtual cell in a granularity period by summing the lengths of the uplink GTP-U packets associated with the virtual cell.
Virtual Cell Downlink Throughput	This KPI provides the total downlink throughput, in octets, for a virtual cell in a granularity period by summing the lengths of the downlink GTP-U packets associated with the virtual cell.

- The action on KPI breach may be set to one of three possible values: no action, raise an alarm of severity minor or raise an alarm of severity major.

Thus, SLA Monitoring operates broadly as intended and successfully demonstrates the key concepts:

- That a number of different SLAs can be represented by managed objects.
- That monitoring and assessment can be performed automatically, by inspection of these managed objects.
- That this monitoring can be applied on a virtual cell, a virtual cluster or a virtual network basis.
- That an automatic action can be triggered in response to an SLA breach.

For a commercially deployable system, enhancements in the following areas would be performed:

- Additional KPIs require implementation, providing VSCNOs with a better picture of the performance of their network slice.
- The geographic area option requires implementation.
- A suitable interface for triggering SON functions in response to a KPI breach is required.

4. Programmable Small Cell PoC

Besides the development activities that were described earlier in this deliverable, other PoC activities were carried out within SESAME WP3.

Particularly, SESAME studied and developed several features that leverage on RAN programmability, as well as on the SESAME architecture platform.

Specifically, advanced features were experimented for proof of concept resorting to a research prototype. The prototype is based on the software-defined radio (SDR) Ettus B210 [23], and on an eNodeB that uses the open source software Open Air Interface (OAI) [24].

Moreover, both were used to implement a programmable small cell prototype connected to the virtualised EPC of Athonet.

For the management of the RAN and to enable programmability, the small cell was interfaced to the RAN Controller 5G-EmPOWER [25], which in the SESAME architecture (see Figure 2-1) exemplifies the functionalities of the virtualised infrastructure manager (VIM) and software-*defined* network (SDN) controller.

A software agent was developed for the purpose of enabling communication between the 5G-EmPOWER and the small cell.

On the other hand, to adhere to the SESAME architecture, the CESC component (the key constituent of the data plane in SESAME) has been implemented relying on the Soekris[10] server/switch platform. Three main PoCs were developed, that is: RAN Sharing, Edge Caching and Functional Split.

The description of the three PoCs is provided in the next sections.

[10] See: *http://www.soekris.com/*

4.1. RAN Sharing

In the scope of SESAME, network services and tenant VSCNOs can be very dynamic in terms of the resource requests from the underlying infrastructure. This implies that the architecture has to be able to provide the necessary resources to accommodate such requests for existing and new virtual networks and services. Network resources are indeed required to scale with the network load increase as prescribed by a tenant SLA. The aim of this PoC is to demonstrate RAN sharing, which corresponds to slicing the radio resources available in the SESAME infrastructure into tenant-specific resource pools. Providing this capability in the SESAME architecture implies also the capability to dynamically (re)configure the radio resources (Resource Blocks in LTE) into non-overlapping chunks managed by different schedulers.

In the current implementation, there are three pillar components that have been implemented to demonstrate RAN sharing: *the RAN controller*, *a reporting and reconfiguration software agent* located at each small cell/PNF, and the *capability of the small cell to support slicing* of the available radio resources. Figure 4-1 shows the prototype implementation of the outlined programmable RAN sharing feature. The key RAN components can be readily identified and are described herein below.

5G-EmPOWER Controller: The 5G-EmPOWER controller takes the role of a VIM to manage the RAN slices. To elaborate on this, from the SESAME orchestrator perspective, 5G-EmPOWER embodies the functionalities of a VIM and SDN controller taking the responsibility of a RAN slice management and (re)configuration. For tenant networks and services, the 5G-EmPOWER controller provides REST APIs that can be used to create, modify and delete a tenant RAN slice in a small-cell/PNF (similar considerations would hold in case a functional split other than S1 virtualisation is implemented, replacing with the micro-server facility of the CESC).

Moreover, the set of REST APIs of 5G-EmPOWER is the main resource for a tenant to modify the slice configuration. The 5G-EmPOWER controller also provides the ability to control how the slice-specific resources are scheduled in a small cell.

5G-EmPOWER eNodeB Agent: The eNodeB agent is the actual workhorse that carries out the commands of the 5G-EmPOWER controller and the actual reconfiguration of the resources. The eNodeB agent provides an interface to communicate with the controller and is responsible for acting upon the RAN controller issued commands. After receiving RAN sharing command from the controller, the agent checks the feasibility of the request and, if compatible, performs the necessary updates of a tenant/slice and/or scheduling procedure.

5G-Empower-OAI: The LTE small cell/PNF used in the prototype RAN sharing test-bed is based on the OAI eNodeB software implementation. The OAI software is a complete LTE eNobeB software stack but does not provide the RAN sharing feature natively. In the current implementation, the stack has been modified at the MAC layer to add the provision of programmable RAN sharing through 5G-EmPOWER.

Realizing the complete RAN sharing concept at the MAC layer in the small cells is a two-step process. In the first step, the physical radio resources are distributed among the tenants as specified by the controller and in the second step, the individual slices are configured with a slice-specific scheduling algorithm.

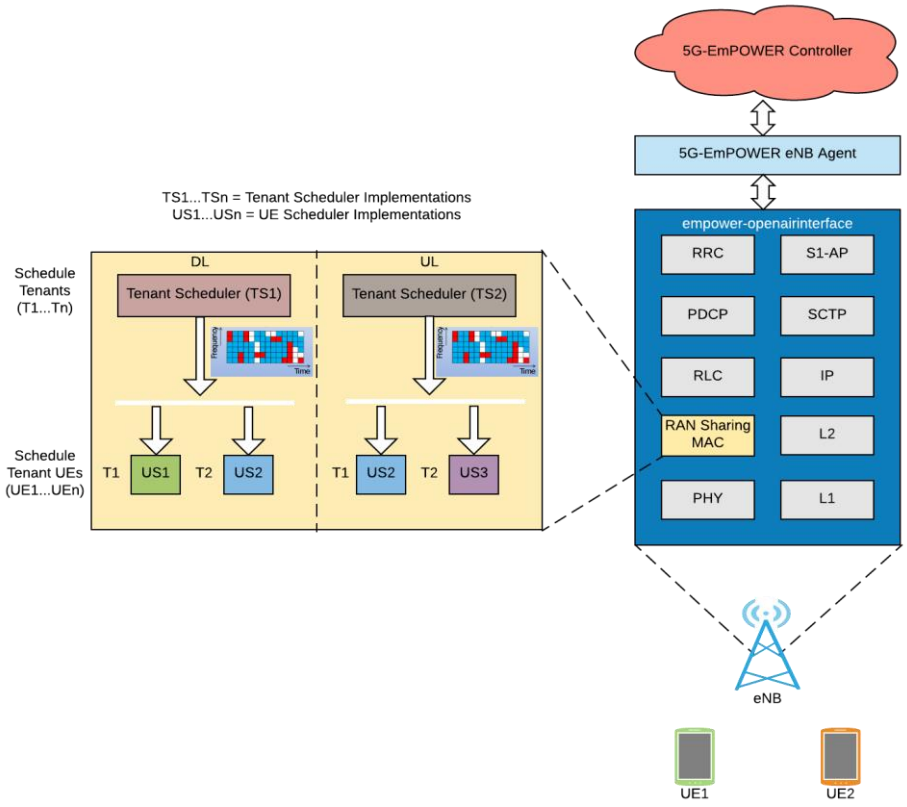

Figure 4-1: RAN sharing implementation for two different VSCNOs

In the PoC developed two tenants were demonstrated as shown in Figure 4-1; to each slice is assigned a non-overlapping amount of resource blocks.

A global scheduler called tenant scheduler manages the slice resources and absolve the duty of scheduling them on a non-conflicting basis. Within each slice, a different scheduler is used to serve UEs.

The two UE schedulers used in the slices are Best CQI and Round Robin (RR), *respectively*. It is also worth pointing out that, within each slice it is possible to change the UE scheduler relying on a command from 5G-EmPOWER to the software agent and the communication flow described above.

The mapping of the tenant network slices to the actual physical resource blocks in the LTE subframes (i.e., TTIs) can be realized with two different methods to serve the users. In the first "Controller based Allocation" method, the 5G-EmPOWER controller determines the resource allocation mapping and then forwards that allocation information to the software agent, which configures the small cell/PNF resource accordingly. In the second "Dynamic" method, the actual mapping is assigned to the specific tenant scheduler, which performs the assignment at the stack level for any fixed period of time.

Currently, RAN sharing was implemented only in downlink but future activities will extend it to the uplink as well. This choice was done to develop a PoC mainly looking at the downlink traffic, which is the most relevant to demonstrate the RAN sharing concept.

4.2. Edge Caching

The SESAME Light DC platform provides the fundamental support to bring multi-access edge computing (MEC) benefits to the end-users. More specifically, the Light DC provides the edge cloud architecture that can support network and service functions to optimize quality of service (QoS) in low end-to-end (E2E) latency applications. This PoC aims to demonstrate edge caching to enable tenant VSCNOs to realize mobile edge-computing benefits and bring services closer to the users. This will alleviate the latency concerns for many 5G network applications. The edge caching has been implemented through software modules that can enable applications residing at the edge in the Light DC.

Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε. shows the high-level architecture f the edge caching framework. This architecture is based on a few fundamental software components that are presented below.

MEC-RAN Information Interface (MRI): The MEC-RAN Information Interface is a RAN-specific interface between the MEC server and the underlying physical (or virtual) network. It provides a real-time insight into the radio network information and user location awareness. The MRI enables the MEC server to communicate with other network entities such as MME, S-GW, P-GW and eNodeB, through RAN-specific control plane (S1-C, X2-C) and user plane interfaces (S1-U, X2-U). The MRI is implemented using Tshark[11] - a terminal based version of Wireshark application[12], that monitors the interfaces between eNodeB and EPC. The three types of information collected by MRI include: (i) Control Plane Information, by capturing and processing signalling messages between eNodeB and MME; (ii) Data Plane Information, by processing data plane packets between eNodeB and SGW, and; (iii) UE/eNodeB Low-level Information, relevant to Physical, MAC, RLC and PDCP layers of UE and eNodeB. These types of information are collected and stored in the MEC server to identify service requests and subsequent data traffic according to the service chain required for a particular MEC application.

MEC Application Platform Services: The MEC Application Platform services provide the fundamental middleware functionalities to support several MEC applications inside the SESAME Light DC architecture. More specifically, the MEC Application Platform services include the RNI Service (RNIS), and the Traffic Offloading Service (TOFS). The RNIS stores the radio network information in a database structure, which includes information about the users and radio cells captured by the MRI. The stored radio network information can be accessed by other services and authorized applications inside the MEC server. The TOFS takes care of routing traffic to the appropriate destinations within the MEC application service chain including support for dynamic reconfiguration. The TOFS has been implemented using an open source software switch (Lagopus[13]) and Ryu SDN Controller[14], which has been extended to support the GPRS tunnelling protocol. Additionally, a Ryu application has been developed to provide GTP/IP/UDP header encapsulation/de-capsulation service which is required to support the MEC functionality. For a particular MEC service chain that requires traffic redirection towards a service inside the Light DC architecture, the Ryu controller, based on the triggers received from RNIS, pushes flow rules in the Lagopus switch using the OpenFlow version 1.3 protocol[15].

---

[11] For further details see: *https://www.wireshark.org/docs/wsug_html_chunked/AppToolstshark.html*

[12] For more details see, *for example*: *https://en.wikipedia.org/wiki/Wireshark*

[13] See: *http://www.lagopus.org/*

[14] For more details also see: *https://osrg.github.io/ryu/*

[15] For more details see, *for example*: *https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.3.0.pdf*

MEC Applications: The MEC framework enables tenant networks to bring any MEC application at the network edge, and it can be connected to the SESAME NFV architecture. A MEC application can interact with the MEC framework and provide services to the end-users with improved quality of service since it is located close to them. A typical example demonstrated in this PoC is provided by content caches that reside in the SESAME Light DC infrastructure. Alternatively, another example can be provided by video transcoding, which is also deployed within the Light DC platform.

Hosting Infrastructure: The Hosting infrastructure refers to the hardware and software combination that provides the necessary edge infrastructure to support the MEC server and the edge-resident applications. In SESAME, this corresponds to the CESC and Light DC environment managed by the overall SESAME management framework.

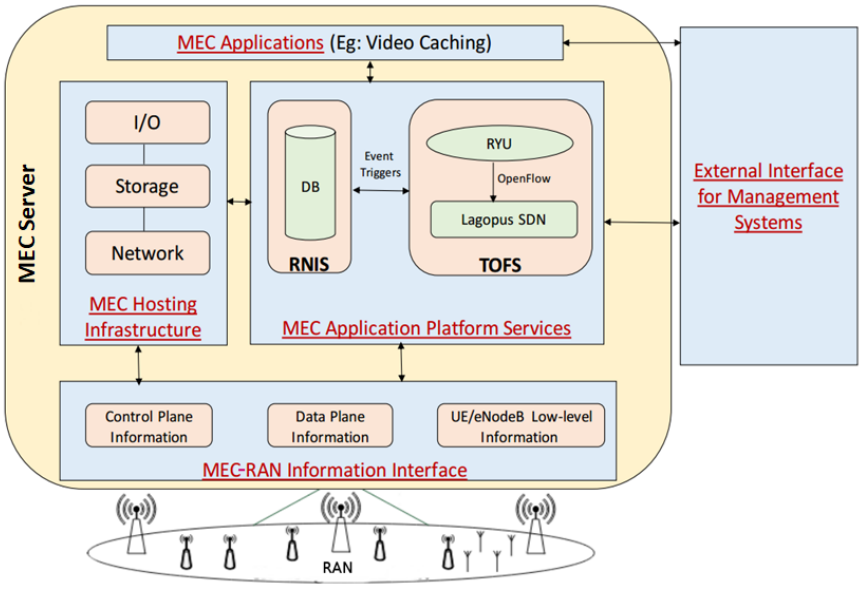

Figure 4-2: Functional blocks developed to implement edge caching in SESAME

4.3. Functional Split

In [26] and [27], it is shown that 3GPP considered various functional split decomposition options, as well as the corresponding latency and bandwidth requirements of each choice.

As discussed in previous project deliverable, the functional split consists in the possibility do the break out of the eNodeB (or PNF in SESAME) protocol stack other than S1 virtualisation.

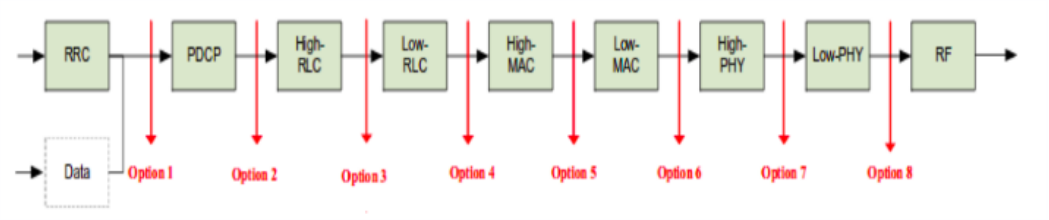

Figure 4-3: Functional split options [26]

It is worth to make a digression to better explain the functional split that was developed in this PoC. In 3GPP [26], the functional split relies on defining a Distributed Unit (DU) and a Centralized Unit (CU), which is the entity shared by different small cells to provide resource sharing benefits for both storage and processor utilization.

Comparing with the SESAME architecture, the DU corresponds to the PNF part of the CESC, while the CU to the micro-server facility in a CESC. Both terminologies will be used hereinafter interchangeably.

The selected choice for this PoC is option 4 in Figure 4-3, which implies the split at the RLC layer, with the MAC and PHY functions residing in the PNF (i.e. DU) and the PDCP, RLC and RRC functions residing on the SESAME micro-server (i.e. CU) part of the CESC.

The high-level view of this PoC is shown for convenience in Figure 4-4, which shows also the mapping between the SESAME architecture and 3GPP terminology.

The packet accelerators (located in the CU) required to support RLC segmentation and reassembly can be scaled down based on average utilization across several cells, thus achieving processor utilization benefits. Besides, storage resources (for PDUs temporary buffering) required by the RLC ARQ retransmission (in downlink) and error correction (in uplink) process can now be shared in the CU by multiple small cells, which allows determining optimization of the storage resources.

The current functional split option 4 developed for this PoC required some modifications of the OAI software at MAC and RLC layers, which are tightly coupled in downlink. In this implementation, the interface introduced between MAC and RLC is customised, but it would benefit by a standardized approach, if this will be available in the future.

Also, data requested by the MAC layer from the RRC may be cached in the DU for increased efficiency.

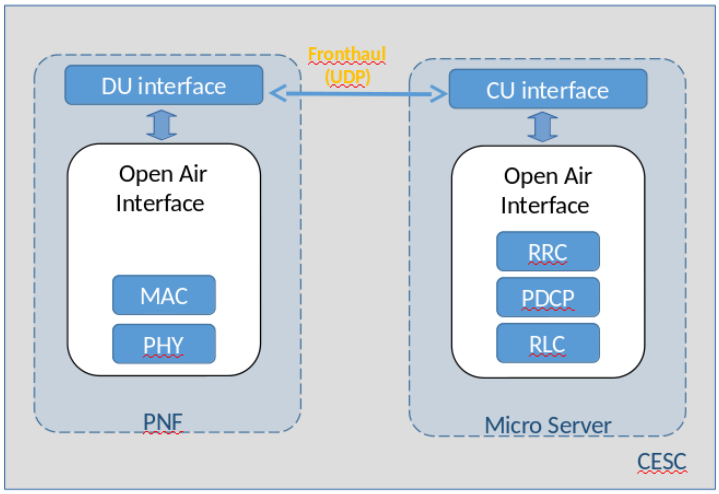

Figure 4-4: High-level view of the PoC for MAC-RLC functional split (3GPP option 4)

Referring to Figure 4-5, the functional split was implemented using two separate machines running different parts of the OAI software. In the DU, the PHY and MAC layers of the OAI protocol stack were deployed, while in the CU, all the remaining layers of the OAI protocol stack starting with RLC are present. DU and CU are connected through a communication link suitable to fulfil the strict fronthaul latency requirements (lower than 250ms, [28]). For enabling the communication between the two units, a UDP based communication protocol was developed so that frames (both MAC-RLC Status PDUs and Data PDUs) between DU and CU can be exchanged with a fronthaul latency lower than 170 microseconds.

In order to fulfil the typical one millisecond delay required by the MAC scheduler, a distributed data buffer and flow control scheme were developed for the purpose of developing the CU-DU split.

The CU interface constructs PDUs in advance and stores them in its own buffer. Then, it periodically aggregates and transmits them to the DU interface, which stores PDUs in its own buffer until requested by MAC. When the MAC layer asks for the subsequent PDU, the DU interface will provide it without the need of asking to the CU again, thus making the whole process quicker and more efficient.

From one side, less requests are needed, and from the other, the data is made available in advance. When the MAC layer performs scheduling, it transmits data fetched directly from the DU buffer of pre-built RLC PDUs.

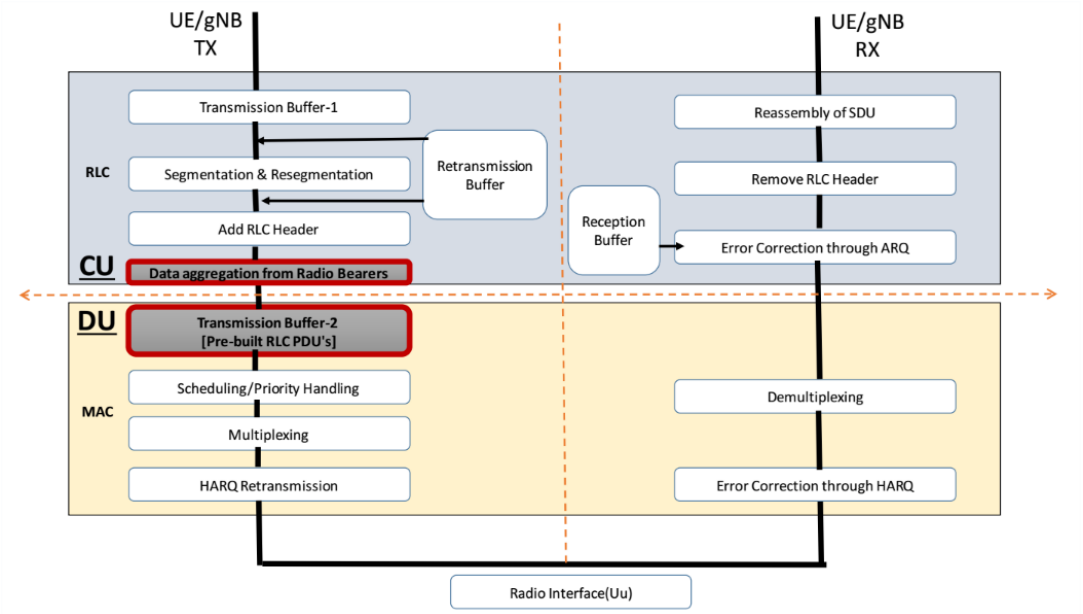

Figure 4-5: PoC implementation details of the functional split option 4

As a side consideration, the criteria that allows the selection of the most suitable functional split point may depend on different factors, including the network load and the fronthaul bandwidth availability to connect the DUs to the edge cloud infrastructure.

In some cases, there can be an advantage of enabling a more dynamic and flexible functional split, able to change the split point and layer-specific parameters depending on the varying data traffic demand and the interference conditions experienced within the RAN.

In case a dynamic split point is possible, and steered by the joint optimisation of radio resources and traffic load optimisation, different functional splits can coexist in different CESCs for a certain period of time.

In another case, virtual network requests coming from multiple VSCNOs may require different functional splits. Upon receiving the requests, the different splits can be dynamically enforced by the RAN infrastructure provider (i.e. falling with the competence of the SESAME CESCM domain).

5. Conclusions

This section summarises the overall success of the PoC demonstrator implementation, how well it meets the original design objectives and the work required to evolve towards a commercially deployable system.

5.1. Overall Status

As illustrated by the summary in Section 5.2 below, the current PoC implementation demonstrates the majority of SESAME design aspects as envisioned in the Deliverable D2.2 [1]. Specifically, it shows a split of the control plane and user plane traffic of each tenant with a clean separation between them:

- Each tenant's traffic may be terminated in a different EPC[16]. It is subject to (potentially) different caps in terms of connected UEs, uplink and downlink throughput.
- Each tenant's user plane traffic may be passed through a different service chain in order to provide the network edge services described in Section 3.6.
- With the exception of the multiplexing function provided by the SC Common VNF (see Section 2.5), each tenants control plane and user plane traffic is processed by different VNFs, hosted on different virtual machines. Thus, the scope for the traffic of one tenant to adversely affect the performance of another is constrained.

In addition to traffic separation, the PoC also demonstrates clean management separation; each tenant is only able to view and interact with their own network slice. They may provision, de-commission, lock, unlock and re-configure virtual cells in a manner analogous to a physical cell. They are also able to receive tailored performance management reports, evaluate key performance indicators and monitor Service Level Agreements that are specific to their network slice.

Those areas where effort has constrained what can be achieved with the PoC (for example the northbound interfaces) have been specified even though they have not been implemented.

In conclusion, the current status PoC implementation provides a firm foundation on which the integration tasks of Work Package 7 can be based.

[16] This is normally the case but it does not have to be. Tenants could share an EPC.

5.2. Design Aspect Summary

Design Aspect	Status in PoC
CESC and Light DC	The status of the CESC and Light DC prototype is described in detail in deliverable D4.4 [7]. Currently, The Small Cell VNF and SC-Common VNF prototypes are not hosted on the Light DC and run in a virtual machine environment based on the Ubuntu OS and Virtual Box that is intended to be representative of the Light DC. If time permits, these VNFs will be ported to the Light DC as part of work package 7.
Small Cell PNF	Conforms to the original design and operates as intended for the chosen functional split. In a commercial deployment, additional per-PLMN/per-VSCNO PM counters would be implemented to enable a full range of KPIs.
Small Cell VNF	Conforms to the original design and operates as intended. Requires porting to the Light DC platform. A commercial deployment would implement SC VNF PM reports and omit redundant SW modules inherited from the code base upon which the SC VNF is based.
SC-Common VNF	Conforms to the original design and operates as intended. Requires porting to the Light DC platform. A commercial deployment would implement SC-Common VNF PM reports and omit redundant SW modules inherited from the code base upon which the SC VNF is based.
Service Chaining	The implementation conforms to the original design but requires validating in WP7.
PNF EMS Small Cell EMS	The PNF EMS and SC EMS differ from the original design in that they are not separate entities and are both provided by the ip.access NOS. Whilst they provide the functionality required to support the PoC, a commercial deployment may be best served by splitting this functionality as originally intended. Such a split would enable a more secure system with a clean separation between SCNO and VSCNO functions.
Northbound Interface	The PoC implementation only provides a subset of the interfaces envisioned in the original design (see Section 3.8) and focuses primarily on the delivery of per-VSVNO PM reports. However, all of the northbound interfaces have been specified to the extent necessary for a commercial deployment.
SLA Monitoring	SLA Monitoring operates broadly as intended and successfully demonstrates the key concepts. Additional work is required in two key areas: • The implementation of a full set of KPIs, • The addition Self-X functionality to automatically invoke action on SLA breach.

Table 2: Design Aspect Implementation Summary

6. Appendix A – 3GPP CM IRP Conformance

This appendix defines the compliance of the EMS to the appropriate 3GPP Configuration Management IRPs.

6.1. Generic IRP (3GPP 32.316)

Operation	Support
getIRPVersion	Supported. Lists the IRPs and Versions available on the EMS.
getOperationProfile	Not supported.
getNotificationProfile	Not supported.

Table 3: Generic IRP Operation Support

6.2. Basic IRP (3GPP 32.606)

Operation	Support
getMoAttributes	Supported.
getContainment	Not supported.
createMO	Supported.
deleteMO	Supported.
setMOAttributes	Supported.

Table 4: Basic IRP Operation Support

6.3. Kernel IRP (3GPP 32.662)

Operation	Support
getNRMIRPVersion	Supported.
notifyObjectCreation	Partially Supported. The *objectClass*, *notificationId* and *systemDN* parameters are not implemented.
notifyObjectDeletion	
notifyAttributeValueChange	
notifyCMSynchronizationRecommended	Not supported.
notifyStateChange	Not supported.

Table 5: Kernel IRP Operation Support

6.4. Notification IRP (3GPP 32.306)

Operation	Support
subscribe	Partially supported. The optional *timeTick* and *ntfTransServiceNS* parameters are not implemented
unsubscribe	Supported.

Operation	Support
getSubscriptionIds	Not supported.
getSubscriptionStatus	Not supported.
changeSubscriptionFilter	Not supported.
suspendSubscription	Not supported.
resumeSubscription	Not supported.
getNotificationCategories	Not supported.
getNotificationProfile	Not supported.
getOperationProfile	Not supported.

Table 6: Notification IRP Operation Support

7. Appendix B – Proposed SESAME CM IRP

7.1. Security

The standard SOAP interface has very little security with the user ID and password of users being included as plain text in request messages. Whilst a security extension has been proposed by the Web Services Federation [29], at the time of writing it has not been widely adopted and HTTPS-*based* security has been proposed as an alternative.

In order to address this security weakness, it is proposed that the SESAME IRP uses HTTPS rather than plain HTTP. This way, each VSCNOs northbound CM requests are encrypted and not subject to eavesdropping.

In a Linux environment such as that on which the SESAME EMS is based, this can be achieved by the standard Linux Pound service. It is configured to intercept requests on TCP port 443[17] (HTTPS) with a URL containing "/3gpp/" and translate them to an internal address on port 8080 on which the EMS SOAP service is listening. IP tables firewall rules are used to prevent access on port 8080 from clients other than Pound. Thus, the SESAME CM IRP will not accept unsecured connections.

7.2. SESAME CM API

The following operations are provided by the SESAME IRP.

7.3. Change Password

This operation allows a northbound SOAP user to change their password.

7.3.1. Input Parameters

Parameter Name	Type	Qualifier	Notes
requestId	String	M	A unique identifier provided by the invoking IRPManager that enables notifications to be associated with the original request.
New Password	String	M	The new password, conforming to the EMS' currently configured password policy.

Note: this may seem both simplistic and insecure however, as the user's credentials are passed in plain text in every SOAP request, it is no more insecure that the rest of the interface. Protection is provided by encrypting the transaction using HTTPS.

7.3.2. Output Parameters

Parameter Name	Type	Qualifier	Notes
requestId	String	M	The value of requestId quoted in original request.
Status	SOAP Fault String	M	Reported in the envelope of the SOAP response.

[17] For more details see, *for example*: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

7.4. Provision Virtual Cell

This operation attempts to provision a virtual cell. The EMS attempts to provision it on the physical cell closest to the desired coordinates that has sufficient spare capacity to support the user's specified SLA.

Note that, unlike the EMS GUI client interface, a SOAP user is not able to select a host physical cell manually and must, therefore, specify a desired cell location and tolerance so that the cell can be auto-assigned.

This also means that the SSCP[18] must specify location coordinates for each physical cell if they are to allow use of the SOAP interface.

7.4.1. Input Parameters

Parameter Name	Type	Qualifier	Notes
requestId	String	M	A unique identifier provided by the invoking IRPManager that enables notifications to be associated with the original request.
ProvisionedSLA	String	M	The name of a Provisioned SLA object within the VNO's SLAs collection.
VirtualCellIdentity	Integer	O	A positive integer value, unique within the scope of the VNO's Virtual Cells collection. If not specified, the EMS uses the value of the object instance ID of the new virtual cell object.
DesiredLatitudeDegrees	Integer	M	The desired latitude of the Virtual Cell, specified in millionths of a degree.
DesiredLongitudeDegrees	Integer	M	The desired longitude of the Virtual Cell, specified in millionths of a degree.
LocationToleance	Integer	M	The location tolerance specified in metres. Only physical cells with a distance less than or equal to this tolerance are considered as candidates for hosting the virtual cell.

[18] For more details see: *https://www.isc2.org/sscp/default.aspx*

7.4.2. Output Parameters

Parameter Name	Type	Qualifier	Notes
requestId	String	M	The value of requestId quoted in the original request.
Status	SOAP Fault String	M	Reported in the envelope of the SOAP response.
VirtualCellIdentity	Integer	M	The virtual cell identity allocated to the cell.
distinguishedName	DN	O	If the request was successful, this defines the full distinguished name of the new virtual cell object.

7.5. Remove Virtual Cell

This operation attempts to decommission a previously provisioned virtual cell. Prior to deleting it, the EMS will attempt to lock the virtual cell object.

7.5.1. Input Parameters

Parameter Name	Type	Qualifier	Notes
requestId	String	M	A unique identifier provided by the invoking IRPManager that enables notifications to be associated with the original request.
VirtualCellIdentity	Integer	M	The virtual cell identity originally allocated to the virtual cell.

7.5.2. Output Parameters

Parameter Name	Type	Qualifier	Notes
requestId	String	M	The value of requestId quoted in original request.
Status	SOAP Fault String	M	Reported in the envelope of the SOAP response.

7.6. Modify Virtual Cell

This operation is used to lock or unlock the virtual cell or to modify its SLA.

7.6.1. Input Parameters

Parameter Name	Type	Qualifier	Notes
requestId	String	M	A unique identifier provided by the invoking IRPManager that enables notifications to be associated with the original request.
VirtualCellIdentity	Integer	M	The virtual cell identity originally allocated to the virtual cell.
administrativeState	String	O	If specified, the new value of the VC's *AdministrativeState* attribute. One of: - UNLOCKED - LOCKED
ProvisionedSLA	String	O	The name of a Provisioned SLA object within the VNO's SLAs collection.

At least one of *administrativeState* or *ProvisionedSLA* must be specified and the request fails if neither is supplied.

If the specified value of either *administrativeState* or *ProvisionedSLA* is the same as its current value then it is ignored. If both parameters are supplied and have the same value as the cell's current state then the request is deemed successful even though it has no effect.

7.6.2. Output Parameters

Parameter Name	Type	Qualifier	Notes
requestId	String	M	The value of requestId quoted in original request.
Status	SOAP Fault String	M	Reported in the envelope of the SOAP response.

7.7. Retrieve Virtual Cell

This operation retrieves the status of a virtual cell.

7.7.1. Input Parameters

Parameter Name	Type	Qualifier	Notes
requestId	String	M	A unique identifier provided by the invoking IRPManager that enables notifications to be associated with the original request.
VirtualCellIdentity	Integer	M	The virtual cell identity originally allocated to the virtual cell.

7.7.2. Output Parameters

Parameter Name	Type	Qualifier	Notes
requestId	String	M	The value of requestId quoted in original request.
Status	SOAP Fault String	M	Reported in the envelope of the SOAP response.
administrativeState	String	M	If successful, the current value of the VC's *AdministrativeState* attribute. One of: - UNLOCKED - LOCKED.
operationalState	String	M	The value of the VC's *OperationalState* attribute. One of: - ENABLED - DISABLED
availabilityStatus	String	M	The value of the VC's *AvailabilityStatus* attribute. A coma separated list that may contain any or none of "In-Test", "Failed", P"ower. Off", "Offline", "Off Duty", "Dependency", "Degraded", "Not Installed", "Log Full".

8. Appendix C – 3GPP PM IRP Conformance

This section details the conformance of the XML PM files produced by the SESAME PNF to 3GPP 32.435 [17].

XML Element or Attribute	Use of Element
/ measCollecFile / fileHeader @ fileFormatVersion	Compliant. Set to "32.435 V7.0".
/ measCollecFile / fileHeader @ vendorName	Compliant. Set to "ip.access" by the ip.access E40.
/ measCollecFile / fileHeader @ dnPrefix	Compliant. Set to the value of the *Device.Services.FAPService.{i}.DNPrefix* parameter of the PNF's TR-196 data model [10].
/ measCollecFile / fileHeader / fileSender @ localDn	Compliant. Set to "AP_TR069#0" by the ip.access E40.
/ measCollecFile / fileHeader / fileSender @ elementType	Compliant. Set to "LTE AP" by the ip.access E40.
/ measCollecFile / fileHeader / measCollec @ beginTime	Compliant.
/ measCollecFile / measData	Compliant. The ip.access E40 generates at most one instance of this element. If there is no data to report then this element is omitted.
/ measCollecFile / measData / managedElement @ localDn	Compliant. Set to "AP_TR069#0" by the ip.access E40.
/ measCollecFile / measData / managedElement @ userLabel	Compliant. Set to the equipment serial number of the access point by the ip.access E40.
/ measCollecFile / measData / managedElement @ swVersion	Compliant.
/ measCollecFile / measData / measInfo	Compliant. For the ip.access E40, there is one instance of this element for each package of measurements at each granularity period. That is, if the E40 is reporting measurements from 5 packages from 4 different granularity periods then there will be 20 instances of this element.

XML Element or Attribute	Use of Element
/ measCollecFile / measData / measInfo @ measInfoId	Compliant[19]. The ip.access E40 sets this attribute to the name of the package that defines the measurements contained in this measInfo element.
/ measCollecFile / measData / measInfo / job @ jobId	Compliant. Set to the value of the *Device.FAP.PerfMgmt.Config.{i}.X_000295_JobId* parameter of the PNF's TR-196 data model [10].
/ measCollecFile / measData / measInfo / granPeriod @ duration	Compliant. Always set to "PT3600S" by the current version of the ip.access E40.
/ measCollecFile / measData / measInfo / granPeriod @ endTime	Compliant.
/ measCollecFile / measData / measInfo / repPeriod @ duration	Compliant.
/ measCollecFile / measData / measInfo / measTypes	Compliant. This optional element in not used in favour of the 'measType' variant (see below).
/ measCollecFile / measData / measInfo / measType	Compliant. There is one instance of this element for each measurement value to be reported. A measInfo may contain zero instances of this element if all the measurements in the corresponding package have a zero value for the granularity period.
/ measCollecFile / measData / measInfo / measType @ p	Compliant. This contains a number that is used to uniquely identify a measurement within the file.
/ measCollecFile / measData / measInfo / measValue	Compliant.
/ measCollecFile / measData / measInfo / measValue @ measObjLdn	Compliant. Always set to the empty string by the ip.access E40.
/ measCollecFile / measData / measInfo / measValue / measResults	Compliant. This optional element in not used in favour of the 'r' variant (see below).
/ measCollecFile / measData / measInfo / measValue / r	Compliant. There is one instance of this for each measType defined in this measInfo element. Each instance of this element has a one-to-one correspondence with a measType element, with the attribute p being used to tie the two elements together. A measValue may contain zero instances of this element if all

[19] 3GPP 32.435 is not explicit about the contents of the measInfoId element.

XML Element or Attribute	Use of Element
	the measurements in the corresponding package have a zero value for this granularity period. The content of this element is set to the value of the measurement being reported.
/ measCollecFile / measData / measInfo / measValue / r @ p	Compliant. The value of this attribute is set to the same value as the measType attribute p, for the corresponding measType element.
/ measCollecFile / measData / measInfo / measValue / suspect	Compliant. This element is set to TRUE if the reported measurement is dubious; this element is omitted if the reported measurement is reliable. It is typically set following boot to indicate that the first granularity period contains partial results .
/ measCollecFile / fileFooter / measCollec @ endTime	Compliant.

Table 7: 32.435 Compliance

9. References

[1] "Deliverable D2.2: Overall System architecture and Interfaces – First Iteration," H2020 SESAME project, April, 2016.

[2] "Deliverable D2.3: Specification of the CESC components – First Iteration," H2020 SESAME project, April, 2016.

[3] "Deliverable D3.1: CESC Prototype design specifications and initial studies on Self-X and virtualization aspects," H2020 SESAME project, June, 2016.

[4] I. T. a. M. B. S. Sesia, "LTE The UMTS Long Term Evolution: From Theory to Practice," John Wiley & Sons, Second Edition, 2011.

[5] 3GPP, "The Evolved Packet Core," Available at: *http://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core*.

[6] 3GPP TS 36.123 Version 10.3.0, "The Evolved Packet Core, LTE: Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Layer Procedures," 3GPP, Oct. 2011.

[7] "Deliverable D4.4: Light DC prototype," H2020 SESAME project, June 2016.

[8] 3GPP TR 29.060 v13.2.0, "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface (Release 13)", 3GPP, September, 2015.

[9] "E40 nanoLTE, 4G Enterprise Access Point Data Sheet, Available at: *http://www.ipaccess.com/uploads/wysiwyg_editor/files/2017/E40-Datasheet-v1.0.pdf*" ip.access Ltd, 2017.

[10] "TR-196, Femto Access Point Service Data Model, Issue 2", Broadband Forum, 2011.

[11] 3GPP TS 32.425, " Performance measurements, Evolved Universal Terrestrial Radio Access Network, E-UTRAN, Release 11", 3GPP, Dec, 2012.

[12] 3GPP TS 32.306, "Configuration Management (CM); Notification Integration Reference Point (IRP): Solution Set (SS) definitions (Release 10)", 3GPP, Sept, 2010.

[13] 3GPP TS 32.316, "Generic Integration Reference Point (IRP) management; Solution Set (SS) definitions (Release 10)", 3GPP, June, 2010.

[14] 3GPP TS 32.606 , "Configuration Management (CM); Basic CM Integration Reference Point (IRP); Solution Set (SS) definitions (Release 10)", 3GPP, Sept, 2010.

[15] 3GPP TS 32.662, "Configuration Management (CM); Kernel CM Information Service (IS) (Release 10)", 3GPP, March, 2011.

[16] 3GPP TS 32.111-6 , "Fault Management; Part 6: Alarm Integration Reference Point (IRP): Solution Set (SS) definitions (Release 10)", 3GPP, Sept, 2011.

[17] 3GPP TS 32.435, "Performance measurement; eXtensible Markup Language (XML) file format definition (Release 10)", 3GPP, March, 2012.

[18] 3GPP TS 32.412, "Performance Management (PM) Integration Reference Point (IRP): Information Service (IS) (Release 10)", 3GPP, March, 2011.

[19] 3GPP TS 32.416, "Performance Management (PM) Integration Reference Point (IRP); Solution Set (SS) definitions (Release 10),", 3GPP, March, 2011.

[20] "Deliverable D2.4: Specification of the Infrastructure Virtualisation, Orchestration and Management – First Iteration", H2020 SESAME project, June, 2016.

[21] 3GPP TS 32.341, "Telecommunication management; File Transfer (FT) Integration Reference Point (IRP);Requirements (Release 10)", 3GPP, March, 2011.

[22] Sun Microsystems (Oracle), "Java Web Start: See *http://docs.oracle.com/javase/tutorial/deployment/webstart/*".

[23] "USRP B210, available at: *https://www.ettus.com/product/details/UB210-KIT*".

[24] "Open Air Interface, available at: *http://www.openairinterface.org/*".

[25] "5G-EmPOWER, available at: *http://empower.create-net.org/*".

[26] TR 38.801 V14.0.0, "Study on New Radio Access Technology: Radio Access Architecture and Interfaces", 3GPP, March 2017.

[27] Nomor research, "3GPP 5G Adhoc: Any Decisions on RAN Internal Functional Split?", Jan. 2017.

[28] Document 159.07.02, "Small Cell Virtualization Functional Splits and Use Cases", Smal Cell Forum .

[29] Web Services Specifications available at:, [Online]. Available: *http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.html*.

[30] TR 38.801 V14.0.0, "Study on New Radio Access Technology: Radio Access Architecture and Interfaces", 3GPP, March 2017.