H2020 5GASP Project
Grant No. 101016448

D2.1 Architecture, Model Entities Specification and Design

Abstract

This document presents the infrastructure architecture and the model entities (roles) used in 5G Application & Services experimentation and certification Platform (5GASP) project. Taking the input from the vertical requirements and the experimentation facilities, it will define the detailed architecture, the internal and external components and their interfaces, the user interaction portal, the 5GASP experimentation Application Programming Interface (API) service, the experiment service orchestrator, the multi-domain approach and the physical architecture.

Document properties

Document number	D2.1
Document title	Architecture, Model Entities Specification and Design
Document responsible	Elena-Madalina Oproiu
Document editor	Elena-Madalina Oproiu
Editorial team	ORANGE Romania (ORO)
Target dissemination level	PU
Status of the document	Final Version
Version	1

Document history

Revision	Date	Issued by	Description
0.1	26.06.2021	ORO	Initial draft
0.2	30.06.2021	ITAV, VMware, UoP, Lamda Networks	Internal review
0.3	02.07.2021	ORO	Submission version

Disclaimer

This document has been produced in the context of the 5GASP Project. The research leading to these results has received funding from the European Community's H2020 Programme under grant agreement number 101016448.

Executive summary

5GASP aims at shortening the idea-to-market process through the creation of a European testbed for Small and Mid-size Enterprises (SMEs) that is fully automated and self-service, in order to foster rapid development and testing of new and innovative Network Applications (NetApps) built using the 5G Network Functions Virtualization (NFV) based reference architecture. Building on top of existing physical infrastructures, 5GASP intends to focus on innovations related to the operation of experiments and tests across several domains, providing software support tools for Continuous Integration and Continuous Deployment (CI/CD) of VNFs in a secure and trusted environment for European SMEs capitalizing in the 5G market.

The Architecture, Model Entities Specification and Design provided by the document will identify the current state-of-the-art of Cloud, NFV, Management and Orchestration (MANO), CI/CD in terms of open, most mature projects and technologies, to choose the ones to be integrated as basis for 5GASP open platform. It will evaluate existing efforts in EU funded projects, Standards and Open Source solutions (many of them made available by 5GASP partners) to define the integration and development work inside 5GASP.

This task will set up the reference architecture and Development and Operations (DevOps) like processes for the 5GASP experimentation infrastructure.

The requirements will be provided from the 5GASP NetApps, the use cases and the interoperability goals that 5GASP wants to achieve. The objectives are:

- To define the requirements for a unified 5G/NFV experimentation infrastructure for enabling 5G NetApps for interoperability with well-defined industry standard interfaces, integration with orchestration platforms, analytics, virtual infrastructure managers, and cloud native and SDN platforms;
- To define a process for automated transformation of vertical applications to interoperable 5G/NFV artefacts;
- To define the architecture of 5GASP open repository and knowledge base;
- To define the various components of the 5GASP infrastructure in such a manner that are open, interoperable, extensible and standard;
- To design the 5GASP experimentation infrastructure to support:
    - standardized 5G/NFV interfaces;
    - multidomain scenarios;
    - seamless integration of 5G/NFV technologies;
    - automated transformations of 5G/NFV models.

List of authors

Company	Name	Contribution
ORO	Elena-Madalina Oproiu Oana Badita Ioan Constantin Andreea Bonea Marius Iordache	Abstract, Executive Summary, Objectives of the Document, Related Projects, Document Structure, 5GASP NetApps vertical-specific requirements and Infrastructures - Introduction, 5GASP Experimentation Facilities Infrastructures Architectures and Capabilities (Testbeds)- Introduction, Bucharest Site, 5GASP Model Entities (Roles), 5GASP Global Infrastructure Architecture, 5GASP Internal and external components and their interfaces, 5GASP Facility, Conclusions, References, Acronyms, Content, List of Figures, List of Tables
BLB	Roman Odarchenko	Related projects, Open Source projects, Acronyms, NetApp 6: Remote Human Driving NetApp - Teleoperation for assisting vehicles in complex situations, NetApp 5: Vehicle-to-Cloud (V2C) Real-Time Communication NetApp, References
BLB	Yevgeniya Sulema	User community interaction portal, Conclusions, References
UNIVBRIS	Abubakar Siddique Muqaddas Xenofon Vasilakos	NetApp 7: Efficient MEC Handover App; Bristol Site (testbed facilities); Physical architecture: Design aspects of Disaggregated Radio Access Network (RAN), Multi-access Edge Computing (MEC) and provisional plan for MEC/Disaggregated RAN integration; Contributions to user community interaction portal
DriveU	Eli Shapira	NetApp 6: Remote Human Driving NetApp - Teleoperation for assisting vehicles in complex situations, NetApp 5: Vehicle-to-Cloud (V2C) Real-Time Communication NetApp
OdinS	Jorge Gallego-Madrid Ana Hermosilla Antonio Skarmeta	NetApp 1: Virtual On-Board Unit provisioning NetApp (vOBU), NetApp 4: Multi-domain Migration NetApp, Murcia Site, NetApp deployment workflows
ITAv	Diogo Gomes Rafael Direito Rui Aguiar José Quevedo Daniel Corujo	Introduction of section “5GASP methodology and experimentation framework”, DevOps (CI/CD) context, 5GASP CI/CD Service, E2 - Interface for CI/CD communication, E4 - Interface for Cross Domain Network Orchestration, E5 - Interface for facility and testing services management, E6 -

		Interface for facility interaction with CI/CD, E7 - Inter-facillity Interface connectivity
YoGoKo	Thierry Ernst Yakub M. AbuAlhoul	Description of Cooperative ITS (C-ITS) technologies and standards (ISO, CEN, ETSI) Description of Automotive consortium (5GAA, C2C-CC), Description of NetApps “Virtual RSU” and “ITS station”
UoPatras	Christos Tranoris Kostis Trantzas	Standards to consider (GSMA, TM Forum, 3GPP, ETSI NFV), NetApp 11: Fire detection and ground assistance using drones (FIDEGAD), Patras Site, Experimental model, Net Apps deployment and orchestration, 5GASP Model Entities (Roles), 5GASP Internal and external components and their interfaces, 5GASP NetApp Onboarding and Deployment Services (NODS), 5GASP NetApp Marketplace, E1 – Interface for communication to the NFVO (SOL005, etc), E3 - Interface for NetApp Marketplace interactions
ININ	Janez Sterle Luka Korsic Jaka Cijan Dusan Mulac	NetApp9: 5G Isolated Operation for Public Safety (5G IOPS NetApp) Description of ININ/PPDR ONE facility
VMware	Vesselin Arnaudov Gancho Manev	Approach and Methodology, Model Entities (where applicable), Global Infrastructure Architecture with 5GASP Internal/External components preface, Experiment service orchestrator and experimentation API service preface.
Neobility	Andrei Radulescu Ioana Soare	NetApp 10: Vehicle Route Optimizer NetApp
Lamda Networks	Kavvalou Angeliki Leonidas Lymberopoulos	Sub section 2.8: NetApp 8 - PrivacyAnalyzer NetApp
EANTC	Ben Shaw	NetApp testing workflows

Contents

D2.1 ARCHITECTURE, MODEL ENTITIES SPECIFICATION AND DESIGN 1

ABSTRACT 1

DOCUMENT PROPERTIES 2

DOCUMENT HISTORY 2

DISCLAIMER 2

EXECUTIVE SUMMARY 3

LIST OF AUTHORS 4

CONTENTS 6

LIST OF FIGURES 8

LIST OF TABLES 10

ACRONYMS 12

DEFINITIONS 17

1. INTRODUCTION 18

1.1 OBJECTIVES OF THIS DOCUMENT 18
1.2 STATE-OF-THE-ART 19
1.2.1 Related projects 19
1.2.2 Open source projects 24
1.2.3 Standards to consider 26
1.3 APPROACH AND METHODOLOGY 38
1.4 DOCUMENT STRUCTURE 39

2 5GASP NETAPPS VERTICAL-SPECIFIC REQUIREMENTS AND INFRASTRUCTURES 40

2.1 NETAPP 1: VIRTUAL ON-BOARD UNIT PROVISIONING NETAPP (VOBU) 41
2.2 NETAPP 2: VIRTUAL ROADSIDE UNIT PROVISIONING NETAPP (VRSU) 43
2.3 NETAPP 3: ITS STATION NETAPP 47
2.4 NETAPP 4: MULTI-DOMAIN MIGRATION NETAPP 49
2.5 NETAPP 5: VEHICLE-TO-CLOUD REAL-TIME COMMUNICATION (V2C R2C) NETAPP 51
2.6 NETAPP 6: REMOTE HUMAN DRIVING NETAPP - TELEOPERATION FOR ASSISTING VEHICLES IN COMPLEX SITUATIONS 54
2.7 NETAPP 7: EFFICIENT MEC HANDOVER NETAPP 57
2.8 NETAPP 8: PRIVACYANALYZER NETAPP 62
2.9 NETAPP 9: 5G ISOLATED OPERATION FOR PUBLIC SAFETY NETAPP (5G IOPS NETAPP) 67
2.10 NETAPP 10: VEHICLE ROUTE OPTIMIZER NETAPP 71
2.11 NETAPP 11: FIRE DETECTION AND GROUND ASSISTANCE USING DRONES (FIDEGAD) 73
2.12 OVERALL 5GASP NETAPPS VERTICAL-SPECIFIC REQUIREMENTS 75

3 5GASP EXPERIMENTATION FACILITIES INFRASTRUCTURES ARCHITECTURES AND CAPABILITIES (TESTBEDS) 76

3.1 AVEIRO SITE 76
3.2 PATRAS SITE 78
3.3 BRISTOL SITE 80
3.4 LJUBLJANA SITE 81
3.5 MURCIA SITE 85
3.6 BUCHAREST SITE 87

4 5GASP METHODOLOGY AND EXPERIMENTATION FRAMEWORK 92

4.1 EXPERIMENTAL MODEL 92
4.2 NET APPS DEPLOYMENT AND ORCHESTRATION 94

4.3 DevOps (CI/CD) context 95
4.4 5GASP Model Entities (Roles) 96
4.4.1 5GASP NetApp Developer 97
4.4.2 5GASP NF Developer 98
4.4.3 NetApp Tester 98
4.4.4 NF Tester 99
4.4.5 Service Designer 99
4.4.6 Service Experiment Designer 100
4.4.7 Service Experimenter 100
4.4.8 Service Provider 101
4.4.9 Platform Administrator 101
4.4.10 Facility Administrator 102
4.4.11 Marketplace roles 102

5 5GASP INFRASTRUCTURE ARCHITECTURE 103

5.1 5GASP Global Infrastructure Architecture 103
5.2 5GASP Internal and external components and their interfaces 104
5.2.1 5GASP NetApp Onboarding and Deployment Services (NODS) 105
5.2.2 5GASP Facility 105
5.2.3 5GASP CI/CD Service 106
5.2.4 5GASP NetApp Marketplace 108
5.2.5 External Interfaces 108
5.3 User community interaction portal 110
5.4 5GASP experimentation API service 112
5.5 The experiment service orchestrator 112
5.6 Multi-domain 113
5.7 Physical architecture: Disaggregated RAN, MEC 115
5.8 NetApp workflows 117
5.8.1 NetApp deployment workflows 117
5.8.2 NetApp testing workflows 119

6 CONCLUSIONS 121

REFERENCES 122

List of Figures

Figure 1 GSMA-NEST focus[31] 27
Figure 2 S-NESTS associated with 3GPP SST values[31] 28
Figure 3 5G Architecture, non-roaming reference architecture[38] 29
Figure 4 3GPP network slice information model 30
Figure 5 Relation between GST and 3GPP Service Profile 31
Figure 6 NFV Releases 32
Figure 7 NFV-MANO architectural framework[50] 33
Figure 8 Relation between information models[51] 34
Figure 9 Mapping relationship between 3GPP and NFV-MANO architectural framework[52] 35
Figure 10 ITS station symbol and origins[55] 36
Figure 11 Detailed ITS station architecture 37
Figure 12 NetApp generic architectural template 41
Figure 13 Virtual On-Board Unit (vOBU) provisioning NetApp Infrastructure 42
Figure 14 Virtual RoadSide Unit provisioning NetApp Infrastructure 45
Figure 15 ITS NetApp infrastructure 47
Figure 16 Multi-domain Migration NetApp 49
Figure 17 Vehicle-to-Cloud Real-Time Communication (V2C R2C) NetApp 51
Figure 18 Remote Human Driving NetApp - Teleoperation for assisting vehicles in complex situations 54
Figure 19 Efficient MEC Handover scenario 57
Figure 20 Chain of stream processors 63
Figure 21 Non-real-time datastream analysis by PrivacyAnalyzer within 5GASP 63
Figure 22 Near real-time datastream analysis by PrivacyAnalyzer within 5GASP 64
Figure 23 5G IOPS NetApp high level architecture 67
Figure 24 Standalone deployment of 5G IOPS NetApp 68
Figure 25 Distributed deployment of 5G IOPS NetApp 68
Figure 26 Vehicle Route Optimizer NetApp high level Infrastructure 71
Figure 27 FIDEGAD NetApp high level Infrastructure 73
Figure 28 ITAV Infrastructure 76
Figure 29 ITAV Industry-grade 5G Locations 77
Figure 30 ITAV Industry-grade 5G Architecture 78
Figure 31 ITAV Industry-grade Available 5G Core Functions 78
Figure 32 Patras 5G Architecture 79
Figure 33 Location of the network entities in Bristol City Centre 80
Figure 34 Test Network Functions in hosting partner technologies 80
Figure 35 PPDR ONE architecture 82
Figure 36 PDR ONE portable 5G node (left) with RRH and antenna (right) 82
Figure 37 Industrial 5G Gateway with SierraWireless development board and 5G modem 83
Figure 38 qMON Modular System Architecture 84
Figure 39 iMON System components 84
Figure 40 Murcia Site architecture 86
Figure 41 ORO Bucharest 5G facility 87
Figure 42 5G communication service scheme 88

Figure 43 The 5G ICT-17/19 platform 89
Figure 44 5G PMR Rel. 16 architecture on virtualized infrastructure 90
Figure 45 NSSAI concept overview 90
Figure 46 5G Slicing framework 91
Figure 47 ORO facility planning 91
Figure 48 5GASP experimental model 94
Figure 49 Service Order fulfillment and delivery 95
Figure 50 5GASP approach on DevOps experimentation and certification readiness Lifecyle[1] 103
Figure 51 5GASP high level architecture 104
Figure 52 5GASP facility simplified architecture 106
Figure 53 CI/CD pipeline 107
Figure 54 Communication with facility sites options 109
Figure 55 NetAppCommunity Portal sitemap 111
Figure 56 NetAppStore Portal sitemap 112
Figure 57 Multi-domain: secure overlay network 113
Figure 58 Data Flow between NetOr and respective Domains 114
Figure 59 Disaggregated RAN where a RAN controller is responsible for reserving resources and deploying QoS flows from the UE to the CU 115
Figure 60 ETSI MEC reference architecture 116
Figure 61 5GASP facility configuration 117
Figure 62 5GASP NetApp Deployment Workflow 118
Figure 63 5GASP Automation Testing workflow 119

List of Tables

Table 1 Related infrastructure projects 19
Table 2 Related Automotive projects 22
Table 3 Related PPDR projects 23
Table 4 Related open source projects 24
Table 5 vOBU NetApp KPIs 42
Table 6 vOBU NETAPP's NEST 43
Table 7 vRSU NetApp KPIs 46
Table 8 vRSU NetApp NEST 46
Table 9 ITS NetApp KPIs 48
Table 10 ITS station NetApp NEST 48
Table 11 Multi-domain Migration NetApp KPIs 50
Table 12 Multi-domain NETAPP's NEST 50
Table 13 V2C R2C NetApp KPIs 52
Table 14 V2C R2C NetApp KPIs 52
Table 15 Cloud (NSD) 52
Table 16 Vehicle (NSD) 53
Table 17 V2C R2C NEST 53
Table 18 Remote Human Driving NetApp – Teleoperation KPIs 55
Table 19 Remote Human Driving NetApp NSD 55
Table 20 Cloud (NSD) 55
Table 21 Control center (NSD) 56
Table 22 Remote Human Driving NetApp NEST 56
Table 23 Efficient MEC Handover NetApp NSD 60
Table 24 Efficient MEC Handover NEST 61
Table 25 3GPP 5QI values: 81, 82 and 83 61
Table 26 PrivacyAnalyzer NetApp KPIs 64
Table 27 PrivacyAnalyzer NetApp NEST 65
Table 28 PrivacyAnalyzer's NSDs 65
Table 29 Batch-mode privacy analysis service NSD 65
Table 30 Near real time privacy analysis service (NSD) 66
Table 31 5G IOPS NetApp KPIs 68
Table 32 5G IOPS NETAPP's NEST 69
Table 33 5G IOPS Mobile Core NSD 70
Table 34 5G IOPS Cloud BBU NSD 70
Table 35 Vehicle Route Optimizer NetApp KPIs 71
Table 36 Vehicle Route Optimizer NetApp's NEST 72
Table 37 Vehicle Route Optimizer NetApp NSD 72
Table 38 Vehicle Route Optimizer NetApp Core NSD 72
Table 39 FIDEGAD NetApp KPIs 74
Table 40 FIDEGAD NEST 74
Table 41 FIDEGAD NSDs 74
Table 42 Image recognition Service (NSD) 74
Table 43 Control Center Service (NSD) 75
Table 44 5GASP roles 96

Table 45 5GASP roles distribution 97
Table 46 5GASP NetApp Developer role distribution 97
Table 47 5GASP NetApp Developer role distribution 98
Table 48 5GASP NetAppTester role distribution 98
Table 49 NF Tester role distribution 99
Table 50 5GASP Service Designer role distribution 99
Table 51 5GASP Service Experiment Designer role distribution 100
Table 52 5GASP Service Experimenter role distribution 100
Table 53 5GASP Service Provider role distribution 101
Table 54 5GASP Platform Administrator role distribution 101
Table 55 5GASP Facility Administrator role distribution 102
Table 56 CI/CD steps 107

Acronyms

3GPP	3rd Generation Partnership Project
5G IOPS	5G Isolated Operation for Public Safety
5G PPP	5G Infrastructure Public Private Partnership
5GAA	5G Automotive Association
5GASP	5G Application & Services experimentation and certification Platform
5GC	5G Core
5QI	5G QoS Identifier
ADAS	Advanced Driver Assistance Systems
AF	Assured Forwarding
AI	Artificial Intelligence
AMazING	Advanced Mobile wIreless Network playGround
AMF	Access and Mobility Management Function
AOEP	Automotive Open Experimental Platform
API	Application Programming Interface
APN	Access Point Name
AUSF	Session Management Function
BBU	Baseband Unit
BSS	Business Support Systems
BW	bandwidth
C2C-CC	Car2Car Communication Consortium
CaaS	Container as a Service
CAM	Cooperative Awareness Messages
CAPIF	Common API Framework
CCAM	Cooperative, Connected and Automated Mobility
CEN	European Committee for Standardization
CI/CD	Continuous Integration and Continuous Deployment
CISM	Container Infrastructure Service Management
C-ITS	Cooperative Intelligent Transport Systems
CNF	Cloud-native Network Function
COP	Common Operational Picture
COTS	off-the-shelf
CP	Control Plane
CPE	Customer-Premises Equipment
CPM	Collective Perception Message
CPRI	Common Public Radio Interface
CPU	Central Processing Unit
CRUD	Create, Read, Update, and Delete
CS	Customer Service
CSI	Communication Service Instance
CSMF	Communications Service Management Function
CU	Centralized Unit

CWDM	Coarse Wavelength Division Multiplexing
DEMN	Decentralized Environmental
DevOps	Development and Operations
DN	Data Network
DNS	Domain Name System
DPDK	Data Plane Development Kit
DRT	Demand Responsive Transportation
DU	Distributed Unit
E2E	End-to-End
EDGE	Enhanced Data GSM Environment
ELK stack	Elasticsearch, Logstash and Kibana
eMBB	Enhanced Mobile Broadband
eNB	evolved Node B
ENDC	E-UTRAN New Radio – Dual Connectivity
EPC	Evolved Packet Core
EPS	Evolved Packet System
ETSI	European Telecommunications Standards Institute
EVE	Evolution and Ecosystem
FEC	Forward-Error-Correction
FIDEGAD	Fire detection and ground assistance using drones
GDPR	General Data Protection Regulation
gNB	gNodeB
GPS	Global Positioning System
GPU	Graphics Processing Unit
GSMA	Global System for Mobile Communications Association
GST	General Slice Template
GUIs	Graphical User Interfaces
H2020	Horizon 2020
HO	Handover
HSS	Home Subscriber Server
IaaS	Infrastructure as a Service
ICT	Information and Communication Technologies
IOC	Information Object Class
IoT	Internet of Things
IP	Internet Protocol
IPsec	Internet Protocol Security
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
ITS-S	ITS Station
KNFs	Kubernetes-based Network Functions
KPI	Key Performance Indicator
L2	Layer 2
L3	Layer 3

LDM	Local Dynamic Map
LIDAR	Light Detection and Ranging
LoRa	Long range, low power wireless platform
LTE	Long-Term Evolution
LTR	Local Test Repository
M	Month
MAC	Medium Access Control
MAE	Mobile Automation Engine
MANO	Management and Orchestration
MAP	Map Data
MC	Mission Critical
MCData	Mission Critical Data
MCPTT	Mission Critical Push To-Talk
MEC	Multi-Access Edge Computing
MEPM	MEC platform manager
MIGRATE	Mobile Device Virtualization through State Transfer
MIMO	multiple input, multiple output
ML	Machine Learning
mMTC	massive Machine-Type Communication
MNO	Mobile Network Operator
MPLS	Multiprotocol Label Switching
MShed	MShed Museum
MSq	Millennium Square
NaaS	Network as a Service
NBI	North Bound Interface
NER	Named Entity Recognition
NEST	Network Slice Template
NetApps	Network Applications
NetOr	Cross Domain Network Orchestrator
NFs	Network Functions
NFV	Network Functions Virtualization
NFV ISG	NFV Industry Specification Group
NFVI	NFV Infrastructure
NFVO	NFV Orchestrator
NG-RAN	New Generation - Radio Access Network
NICs	Network Interface Cards
NMS	Network Management System
NODS	NetApp Onboarding and Deployment Services
NR	New Radio
NRF	Network Repository Function
nRT-RIC	near Real Time RAN Intelligent Controller
NS	Network Service
NSA	Non Standalone Architecture
NSD	Network Service Descriptor
NSMF	Network Slice Management Function

NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slicing Selection Function
NSSI	Network Slice Subnet Instance
NSSMF	Network Slice Subnet Management Function
NWDAF	Network Data Analytics Function
OAM	Operations, Administration and Maintenance
OBU	On-Board Unit
ODA	Open Digital Architecture
ONAP	Open Network Automation Platform
ONE	Outdoor and iNdoor 5G Experiments
O-RAN	Open RAN
OSI	Open Systems Interconnection
OSM	OpenSourceMANO
OSS	Operations Support Systems
PaaS	Platform as a Service
PCI	Physical Cell ID
PDCP	Packet Data Convergence Protocol
PHY	physical
PII	Personal Identifiable Information
PKI	Public Key Infrastructure
PMR	Private Mobile Radio
P-NESTs	Private NESTs
PNF	Physical Network Function
PoP	Point of Presence
PPDR	Public Protection and Disaster Relief
qMON	Quality Monitoring System
QoE	Quality of Experience
QoS	Quality of Services
RADAR	Radio Detection and Ranging
RAN	Radio Access Network
RESTful	Representational State Transfer
R-ITS-S	Roadside ITS Stations
RLC	Radio Link Control
RRC	Radio Resource Control
RRH	Remote Radio Head
RSRP	Reference Signal Received Power
RSUs	Road Side Units
RT	Real-Time
RU	Radio Unit
SA	Standalone Architecture
SaaS	Software as a Service
SAM	Service Announcement
SDN	Software-Defined Networking
SDOs	Standard Development Organizations
SLA	Service Level Agreement
SLS	Service Level Specification

SM	Slice Manager
SMEs	Small and Mid-size Enterprises
S-NESTs	Standardized NESTs
SOM	Service Order Management
SPAT	Signal Phase and Time
SSH	Secure Shell Protocol
SST	Slice/Service Type
SW	software
T&L	Transport & Logistics
TB	Terabyte
TEE	Test Execution Engine
TM Forum	Tele Management Forum
TN	Transport Network
TOSCA	Topology and Orchestration Specification for Cloud Applications
TRL	Technology Readiness Levels
TSGs	Technical Specification Groups
TTH	Time to wireless HO
UAV	Unmanned Aerial Vehicle
UDM	Unified Data Manager
UE	User Equipment
UI	User Interface
UML	Unified Modelling Language
UPF	5G User Plane Function
UPF	User Plane Function
URLLC	Ultra Reliable Low Latency Communications
V2C R2C	Vehicle-to-Cloud Real-Time Communication
V2C/C2V	Vehicle-to-Cloud / Cloud-to-Vehicle
V2X	Vehicle-to-everything
VAL	Vertical Application Layer
vApps	vertical and cross-vertical NetApps
VDUs	Virtualized Distributed Units
VIM	Virtualized Infrastructure Manager
VM	Virtual Machine
VMS	Variable Message Signboards
VNFM	VNF Manager
VNFs	Virtual Network Functions
vOBU	Virtual On-Board Unit
VPN	Virtual Private Network
VRP	Vehicle Route Problem
vRSUs	virtual RSUs
WB	wideband
WP	Work Package
WTC	“We The Curious”
XaaS	X as a Service
YANG	Yet Another Next Generation

Definitions

This document contains specific terms to identify elements and functions that are considered to be mandatory, strongly recommended or optional. These terms have been adopted for use similar to that in IETF RFC2119 and have the following definitions:

- **MUST** This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- **MUST NOT** This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
- **SHOULD** This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT** This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- **MAY** This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides).

1. Introduction

1.1 Objectives of this document

The main objective of this document is to define and design the architecture and its related model entities (roles) of the 5GASP project.

First of all, the document describes for each of the eleven NetApps involved in the project, the vertical-specific requirements (NetApps' Key Performance Indicators (KPIs), overall integration needs and the requisite demonstration environment), as well as the high-level architecture of each NetApp. The document also presents the infrastructure and capabilities of each of the six experimentation facilities involved in the project: Aveiro, Bristol, Patras, Murcia, Ljubljana and Bucharest. These infrastructures have already been validated within the scope of several Horizon 2020 (H2020) 5G projects described further on in *1.2.1 Section*. The combination of those experimentation facilities within the scope of this project shall lead to the 5GASP integrated, open, cooperative and fully networked platform[1].

Taking the input from the NetApps's requirements the architectures and capabilities of the experimentation facilities, this document defines the detailed architecture, the internal and external components and their interfaces, the APIs to NetApp the developers/experimenters as well as the user management interface and its requirements. The architecture's components include the user interaction portal, the 5GASP experimentation API service, the experiment service orchestrator, along with all the components that will support this architecture (monitoring, logging, issue management) and the multi domain capabilities and tools. It also defines the NetApp workflows, specifically, the NetApp deployment workflows and the NetApp testing workflows.

Furthermore, this deliverable also specifies the 5GASP model entities (roles) e.g. Service Experimenter, Platform Administrator, NetApp developer, Network Function Developer, etc., and how they should be implemented in the architecture.

In order to provide a unified abstraction for all 5GASP facilities, the necessary experiment modelling and transformations (experimental model) are defined so that experiments are able to onboard and test their NetApps on any 5GASP facility, regardless of the internal details of the facility.

NetApps' deployment and orchestration are detailed based on the input of the 5GASP facility providers, referring to the interaction with the facility, considering the middleware, domain orchestrators and experimentation environments used at each location.

Finally, the document defines the initial version of high-level requirements and interactions for the CI/CD service (their final version shall be discussed in deliverable D2.3 that shall be implemented within Work Package (WP) 5) to support the DevOps experimentation and the community engagement aspects of the project (e.g. the open repository of NetApps, the 5GASP NetApp's knowledge base, etc.).

1.2 State-of-the-art

1.2.1 Related projects

The list of the related projects is essentially long, therefore the main goal of this subsection is to focus on the most closely related to 5GASP Infrastructure, Automotive and Public Protection and Disaster Relief (PPDR) projects, from which some ideas, solutions, architectures, technologies and used standards could be leveraged by the 5GASP project.

- **Infrastructure projects**

This category predominantly considers 5G Infrastructure Public Private Partnership (5G PPP) projects (*Table 1*), which aim to secure Europe's leadership in the particular 5G areas where Europe is strong or where there is potential for creating new markets such as smart cities, e-health, intelligent transport, education or entertainment & media[2].

Table 1 Related infrastructure projects

5GinFIRE[3]
The main goal of 5GINFIRE project was to build and operate an Open and Extensible 5G Network Functions Virtualization (NFV) - based Reference (Open5G-NFV) ecosystem of Experimental Facilities that not only integrates existing facilities with new vertical-specific ones, but which also lays down the foundations for instantiating fully softwarised architectures of vertical industries and experimenting with them. 5GASP aims to exploit the 5GinFIRE portal that enables experimenters of verticals through a number of open source toolsets. The latter are used in order to specify their services as Virtual Network Functions (VNFs) and deploy them in the various 5G facilities. The portal also provides access to a repository of VNFs which vertical service developers can leverage and integrate to own their services. Moreover, the interconnectivity architecture of 5GINFIRE will be exploited in 5GASP.
5G-VINNI[4]
The goal of 5G-VINNI was to develop an End-to-End (E2E) 5G facility that can be used to first demonstrate the practical implementation of an infrastructure to support key 5G KPIs and then to allow vertical industries to test and validate specific applications that depend on these KPIs. However, 5G-VINNI used principles that allowed for highly dynamic and flexible network architectures, service deployment and testing, that created new technical and commercial service deployment models. The 5G-VINNI University of Patras facility shall be leveraged by 5GASP in order to conduct the necesarry field trials related to the PPDR use cases of the 5GASP project.
5G-TOURS[5]
5G-TOURS is an ongoing 5G PPP project. The goal of 5G-TOURS is to get the European 5G Vision of "5G empowering vertical industries" closer to commercial deployment with highly innovative use cases which involve cross-industry partnerships. The ultimate goal of 5G-TOURS is to bring 5G deployments to real usage scenarios.

The knowledge acquired from 5G-TOURS especially with respect to the development of applications enabled by 5G technology os deemed valuable in respect to the demonstration of 5GASP's use cases. Specifically, 5G-TOURS shall be used as a guideline for the system architecture design, the setup and execution of the 5GASP testbeds.

MATILDA[6]

The aim of MATILDA is to design and implement a novel holistic 5G E2E services operational framework tackling the overall lifecycle of design, development and orchestration of 5G-ready applications and 5G network services over a programmable infrastructure. The project's core results were:

- intelligent and unified orchestration mechanisms applied for the automated placement of the 5G-ready applications;
- the creation and maintenance of the required network slices;
- a trial around the PPDR vertical.

The 5GASP project will benefit from these results through capabilities incorporated in the PPDR for Outdoor and iNdoor 5G Experiments (ONE) facility and through the development and implementation of the Quality Monitoring System (qMON) network and services monitoring VNFs.

5G!Drones[7]

5G!Drones aim is to trial several Unmanned Aerial Vehicle (UAV) use-cases covering Enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency Communications (URLLC) and massive Machine-Type Communication (mMTC) 5G services and to validate 5G KPIs for supporting such challenging use-cases. 5G!Drones is built on top of the 5G facilities provided by the Information and Communication Technologies (ICT) -17 projects. The project is building a software layer to automate the run of trials. This layer exposes a high level API to request the execution of a trial according to the scenario defined by the vertical, while enforcing the trial's scenario using the API exposed by the 5G facility, as well as the 5G!Drones enablers API deployed at the facility.

5GASP considers the concept of abstracting all the low-level details to run the trials for a vertical and the validation of 5G KPIs to support several use-cases via trials using a 5G infrastructure.

5GENESIS[8]

5GENESIS is a H2020 project that focuses on the validation of 5G KPIs for multiple 5G use cases by creating an E2E 5G facility. For the MANO of services across testbeds, 5GENESIS employs a MANO layer with a Slice Manager (SM) and a Network Management System (NMS).

The unification of heterogeneous physical and virtual network elements under a common coordination and the openness of a framework exposed to experimenters from the vertical industries which enables E2E slicing and experiments' automation shall be considered in 5GASP.

5GEVE[9]
5G EVE is the European 5G validation platform for extensive trials. It is one of three 5G PPP infrastructure projects which started on 1st of July 2018. The goal is to implement and test advanced 5G infrastructures in Europe. The 5G-EVE concept is based on further developing and interconnecting existing european sites in Greece, Spain, France and Italy in order to form a unique 5G E2E facility. This project offers the facility to vertical industries for execution and validation of pilots. Access is provided through a unified functional and operational API. 5G EVE achievements in the field of E2E experimentation and validation with full sets of 5G capabilities shall be analyzed and the best practices of 5G EVE shall be considered.
5G-HEART[10]
5G-HEART (validation trials) is ongoing 5G PPP project, which is focused on vertical use cases of healthcare, transport and aquaculture. In the transport area, 5G-HEART will validate autonomous/assisted/remote driving and vehicle data services. The infrastructure shared by the verticals, will host important innovations: slicing as a service and resource orchestration in access/core and cloud/edge segments with live user environments. Trials are running on sites of 5G-Vinni (Oslo), 5Genesis (Surrey) and 5G-EVE (Athens). Trials design and experimental results analysis and validation principles, especially for transport use cases, can be considered and used in the 5GASP.
5GMediaHUB[11]
5GMediaHUB aims to help Europe to achieve the goal of becoming a world leader in 5G, by accelerating the testing and validation of innovative 5G-empowered media applications and NetApps from 3rd party experimenters and NetApps developers, through an open, integrated and fully featured Experimentation Facility. 5GMediaHUB will build and operate an elastic, secure and trusted multi-tenant service execution and NetApps development environment based on an open cloud-based architecture and APIs, by developing and integrating a testing and validation system with two existing well-established 5G testbeds for enabling the fast prototyping, testing and validation of novel 5G services and NetApps. 5GASP and 5GMediaHUB may exchange the data regarding best practices in development of the NetApps, their testing, validation, certification etc. to achieve the goals of both projects in the most effective way.

- **Automotive projects**

There are several automotive projects in this section (*Table 2*).

Table 2 Related Automotive projects

5G-IANA[12]
5G-IANA started on June 1st, 2021. 5G-IANA aims at providing an open 5G experimentation platform, on top of which third party experimenters (i.e., SMEs) in the Automotive-related 5G-PPP vertical will have the opportunity to develop, deploy and test their services. An Automotive Open Experimental Platform (AOEP) will be specified, as the whole set of hardware and software resources that provides the compute and communication/ transport infrastructure as well as the management and orchestration components, coupled with an enhanced NetApp Toolkit tailored to the Automotive sector. 5G-IANA will expose to experimenters secured and standardized APIs for facilitating all the different steps towards the production stage of a new service. 5G-IANA will target different virtualization technologies integrating different MANO frameworks for enabling the deployment of the E2E network services across different domains (vehicles, road infrastructure, Multi-Access Edge Computing (MEC) nodes and cloud resources). 5G-IANA NetApp toolkit will be linked with a new Automotive VNFs Repository including an extended list of ready to use open accessible Automotive-related VNFs and NetApp templates, that will form a repository for SMEs to use and develop new applications. Finally, 5G-IANA will develop a distributed Artificial Intelligence (AI)/ Machine Learning (ML) framework, that will provide functionalities for simplified management and orchestration of collections of AI/ML service components and will allow ML based applications to penetrate the Automotive world, due to its inherent privacy preserving nature. 5G-IANA will be demonstrated through 7 Automotive-related use cases in 2 5G SA testbeds. Moving beyond technological challenges, and exploiting input from the demonstration activities, 5G-IANA will perform a multi-stakeholder cost-benefit analysis that will identify and validate market conditions for innovative, yet sustainable business models supporting a long-term roadmap towards the pan-European deployment of 5G as key advanced Automotive services enabler.
5G-MOBIX[13]
This on-going H2020 project aims at executing Cooperative, Connected and Automated Mobility (CCAM) trials along x-border and urban corridors using 5G core technological innovations to qualify the 5G infrastructure and evaluate its benefits in the CCAM context as well as defining deployment scenarios and identifying and responding to standardisation and spectrum gaps. Those trials will allow running evaluation and impact assessments and defining also business impacts and cost/benefit analysis. As a result of these evaluations and also international consultations with the public and industry stakeholders, 5G-MOBIX will propose views for new business opportunities for the 5G enabled CCAM and recommendations and options for the deployment. ITAv takes part in 5G-MOBIX.

SECREDAS[14]
SECREDAS (Security for Cross-Domain Reliable Dependable Automated Systems) is a project (2018-2022) developing secure technologies (hardware, software) to collect and transmit data, mostly for the automotive industry, but also for railways and healthcare verticals. Early on, the consortium decided to develop the technologies related to the automotive sector in compliance with Cooperative Intelligent Transport Systems (C-ITS) standards. While not a strong focus of SECREDAS, 5G is also considered as the novel technology to connect vehicles to the cloud. YoGoKo is participating to SECREDAS and is leading WP5 "connectivity". 5GASP will thus benefit from the expertise developed by YoGoKo and from technologies developed to secure access to vehicle data in conformance with C-ITS standards.

- **PPDR projects**

There are several projects related to PPDR, that have been considered (*Table 3*).

Table 3 Related PPDR projects

5G-EPICENTRE[15]
5G-EPICENTRE just started in January 2021 and will deliver an open end-to-end experimentation 5G platform focusing on software solutions that serve the needs of PPDR. The envisioned platform will enable SMEs and developers to acquire knowledge with regard to the latest 5G applications and approaches for first responders and crisis management, as well as to build up and experiment with their solutions. The engaged SMEs and organizations that will participate into the realization of the use cases constitute active players in the public security and disaster management, thus acting as key enablers for the assessment of 5G-EPICENTRE with regard to the real needs that should be addressed. Best ideas and practices can be reused in 5GASP for the PPDR use cases.
PPDR-TC[16]
The PPDR-Transformation Centre (PPDR-TC) project concentrated to provide a harmonized frequency allocation in order to enhance cross-border coordination, increase the potential for interoperability and international cooperation and improve spectrum management and planning for PPDR operations. The main outcome has been the recommendations for a PPDR roadmap in a form of a white paper for next generation PPDR systems. This was addressed to network operators and system integrators. 5GASP considers the recommendations of PPDR-TC for 3G/Long-Term Evolution (LTE) and places them in the context of 5G. Moreover, the NetApps derived from ININ's and LamdaNetwork's PPDR use cases shall provide validated proof of compliance with the PPDR-TC's recommendations and they shall also unleash the interoperability dimension of the value proposition of 5GASP, towards catering for PPDR solutions which: • are not bound to the hardware requirements of telecom operators; • enable cross-border PPDR operations to work seamlessly among collaborating albeit country specific telecom operator substrates.

1.2.2 Open source projects

The main aim of this subsection is to analyze completely different open source projects from different areas, that somehow can be connected with achievements of 5GASP objectives in terms of development of open source platforms, software, etc. Extracts of this analysis is presented in the *Table 4*.

Table 4 Related open source projects

SONATA[17]
SONATA was an open source project that developed a NFV framework that provided a programming model and development toolchain for virtualized services, fully integrated with a DevOps enabled service platform and orchestration system. Thus, Sonata influenced in the NFV ecosystem upon being the first NFV integrated approach that included service composition, testing and orchestration. The H2020 project has fulfilled the three core objectives proposed at the beginning of the project. In this way, it has contributed to reduce the time to market for networked services. SONATA outcomes were published in a public GitHub repository[18] under Apache v2.0 license, freely available for download and ready to be installed with full rights for adoption, modification and distribution.
NGPAAS[19]
An ideal 5G Platform as a Service (PaaS) was not only to facilitate building, shipping and running classical VNF with "telco-grade" quality, it combined all sort of third-party applications with those VNF for creating new more versatile and powerful cloud objects, breaking silos between connectivity and computing. Several outcomes of the project can be found on the official website of the project as an open source solutions.
5G-PICTURE[20]
5G-PICTURE developed and demonstrated a converged fronthaul and backhaul infrastructure integrating advanced wireless and novel optical network solutions. There are some project outcomes published as an Open Source[21]: • Pishahang: Joint Orchestration of Network Function Chains and Distributed Cloud Applications[22]; • MEF – Slicing Working Group: Contributed use cases and terminology definitions (ZEETTA); • TelecomInfraProject (TiP) – E2E Slicing Group: Contributed use-case review (ZEETTA).
5G-TRANSFORMER[23]
The 5GPPP Phase 2 5G-TRANSFORMER projects finished. One of its main outcomes is a full MANO stack featuring multiple advanced functionalities, such as vertical and network slice management and NFV network service composition and

federation. Overall, this allows deploying vertical-tailored slices deployed in multiple administrative domains, each having multiple datacenters interconnected by means of a heterogeneity of transport technologies (incl. mmwave, packet, optical). And more importantly, the system allows an E2E control of resources to comply with Service Level Agreement (SLA) requirements no matter where the service components are deployed (at the datacenter or administrative domain levels).
Furthermore, different domains may run different core MANO platforms (e.g., OpenSourceMANO (OSM), Cloudify), since the 5GT service orchestrator is capable of integrating any such platform through wrappers. In this way, the 5GT advanced functionality can be retained and make it work over new releases of such projects by just adapting the wrapper, hence guaranteeing its survivability.
The code also features Graphical User Interfaces (GUIs) at all layers of the stack for ease of management and visualization of databases and deployed services (incl. network service structure or network service placement). APIs towards placement algorithms have also been developed for easily testing new algorithms without the need for delving deep into the code. Monitoring jobs can also be created by interacting with Prometheus and by reacting based on alerts.

5GROWTH[24]

5GROWTH is a 5G PPP Phase 3 project started in June 2019, which deals with the technical and business validation of 5G technologies from the verticals' points of view, following a field-trial-based approach on vertical sites (Technology Readiness Levels (TRL) 6-7).
Its vision is to empower verticals industries, such as industry 4.0, transportation, and energy with an AI-driven automated and sharable 5G E2E solution that will allow these industries to simultaneously achieve their respective key performance targets.
Towards this vision, 5Growth will automate the process for supporting diverse industry verticals through:

- A **vertical portal** in charge of interfacing verticals with the 5G E2E platforms, receiving their service requests and building the respective network slices on top;
- **Closed-loop automation** and **SLA** control for vertical services lifecycle management;
- **AI/ML-driven E2E network solutions** to jointly optimize access, transport, core and cloud, edge and fog resources, across multiple technologies and domains.

5GROWTH project bases on the evolution of the 5G-TRANSFORMER platform and the interrelation with 5G-EVE and 5G-VINNI platforms.
As a result of the ongoing activities, all the code of the 5GROWTH stack is also published as open source[25] and is available in the project Github repository[26].

FIWARE[27]

FIWARE is a curated framework of open source platform components to accelerate the development of smart solutions. The FIWARE Community is an independent Open Community whose members are commited to materialize the FIWARE mission, that is: *"to build an open sustainable ecosystem around public, royalty-free and implementation-driven software platform standards that will ease the development of new Smart Applications in multiple sectors"*. The FIWARE Community is not only formed by

contributors to the technology (the FIWARE platform) but also those who contribute in building the FIWARE ecosystem and making it sustainable over time. As such, individuals and organizations committing relevant resources in FIWARE Lab activities or activities of the FIWARE Accelerator, FIWARE Mundus or FIWARE iHubs programmes are also considered members of the FIWARE community.
OpenSlice[28]
Openslice is a prototype open source, operations support system. It supports VNF/ Network Service Descriptor (NSD) onboarding to OSM and NSD deployment management. It also supports TMFORUM OpenAPIs regarding Service Catalog Management, Ordering, Resource, etc. 5GASP will use the achievements of this open source project for E2E slice and service management, management and orchestration across facilities, user portal and facility management.
TestProject[29]
TestProject is a free E2E test automation platform for web, mobile and API testing that's supported by the #1 test automation community.

1.2.3 Standards to consider

Whilst 5GASP is a research project, its approach is to leverage previous work done in industry Standard Development Organizations (SDO's) and possibly extend it further.
In terms of 5G standardisation, and specifically network slicing, 3GPP should be seen as the main reference, having introduced a general architecture framework for management and orchestration and defined the main management functions. Other SDOs to be considered is European Telecommunications Standards Institute (ETSI) (anything regarding virtualisation of network functions), TM Forum (related to inter-domain interfaces) and GSMA (in relation to the introduction of a uniform communication model among service providers and vertical costumer).

1.2.3.1 GSMA

The Global System for Mobile Communications Association (GSMA) is a trade body representing the interests of mobile operator worldwide. GSMA's work mainly focuses on network slicing and in particular on vertical industry requirements into network slice characteristics. The attempt to introduce an unanimously accepted communication model among operators, providers and vertical costumers have resulted in publication of two GSMA white papers[30, 31].
From the analysis conducted in the white paper[30], several service requirements on network slicing were extracted considering different expressions between industry sectors, including augmented/virtual reality, automotive, logistics, healthcare, finance, manufacturing (industry 4.0), smart cities and public safety. The aim of this overview was to analyze the specifications and requirements from the industry use cases in the direction of providing a universal template that would describe the needs of each specific vertical use case. Although requirements for each use case were addressed, quantified where possible and categorized

into performance, functional and operational requirements, there was no agreement on how verticals would express these requirements in this study.
In this context, GSMA pointed at the direction of a generic network slice template to:

- introduce certain guidelines for verticals on how to address their service requirements towards providers and operators;
- facilitate the signing of the SLA between the operator and the business customer as a guarantee that the network capabilities derived from customer's requirements are always provided. On this notion, GSMA elaborated a new paper[31] introducing two novel concepts:
  - General Slice Template (GST): a template used to describe a network slice/service. It contains all the potential attributes to define a network slice regardless the industry vertical use case.
  - Network Slice Template (NEST): a GST filled with values which serves the purpose of describing the features of vendor specific products fulfilling a particular vertical use case. Furthermore, a NEST can reference the contractual agreements between slice customer and operators, while facilitating the definition of network slices across multi-operator roaming agreements.

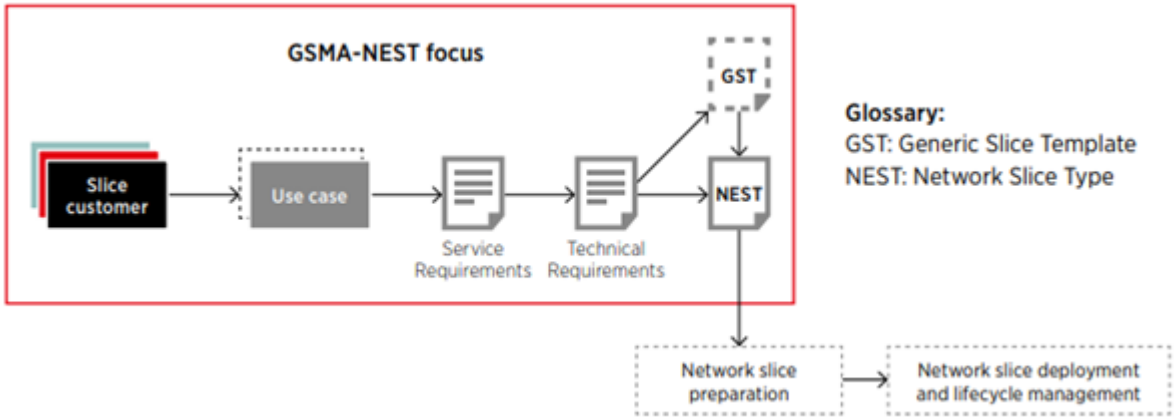


Figure 1 GSMA-NEST focus[31]

The process of creating a NEST based on customer's use case in depicted in *Figure 1*. As seen, the service requirements derived from a specific vertical industry use case are translated into technical requirements. This leads to NEST formation with industry accepted characteristics, with specific values or value ranges that have been commonly agreed and can be used by operators if they consider it appropriate. Once NEST is created, and therefore the network requirements are defined, the 3rd Generation Partnership Project (3GPP) network slice preparation phase can be initiated as described later in this document (see *1.2.3.3 Section*).
As already stated, the aim of GSMA-NEST is to define a set of NESTs with industry accepted slice characteristics shareable between all network operators. The introduction of Standardized NESTs (S-NESTs) enables the replication of network slice behaviour across network boundaries. GSMA-defined NESTs provide a mapping to the standardized 3GPP Slice/Service Type (SST) values, introducing the "*minimum requirements*" to address each Network Slice Type, as seen in *Figure 2*. On the contrary, operator-specific Private NESTs (P-NESTs) are also foreseen. The specification of P-NESTs is assigned to each respective network operator and is based on negotiations between the operator and its customers.

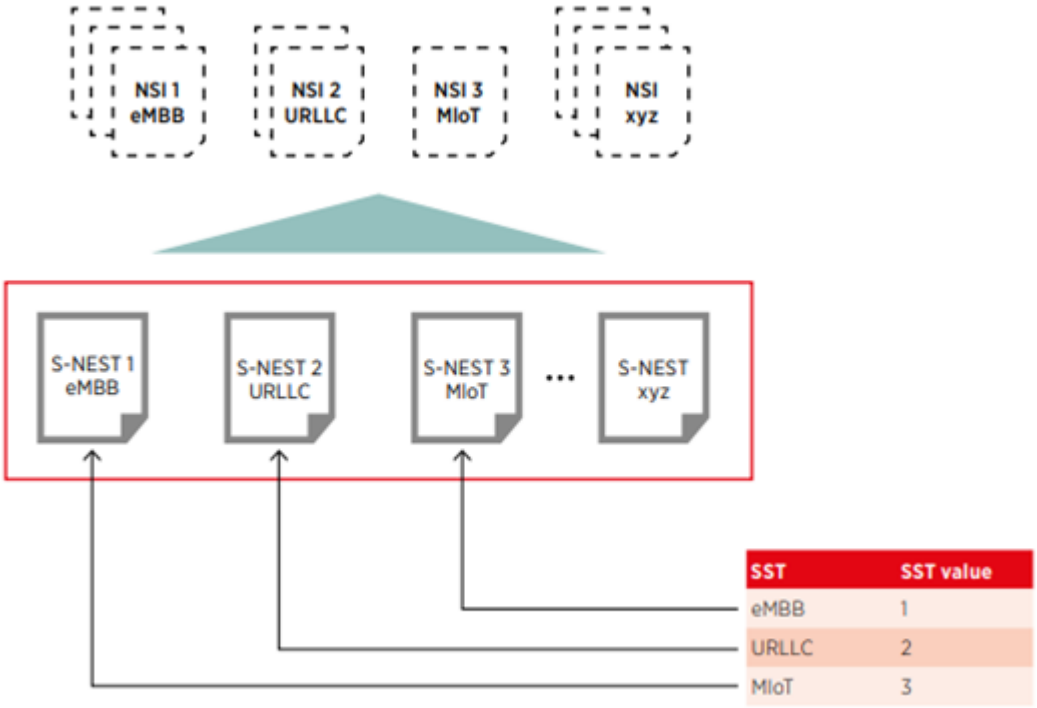


Figure 2 S-NESTS associated with 3GPP SST values[31]

1.2.3.2 Tele Management Forum

Tele Management Forum (TM Forum) is a global industry confederation actively working on evolving current Operations/ Business Support Systems (OSS/BSS), seeking solutions that facilitate their consumption by verticals and their integration into existing standards-driven architectural frameworks. In these terms, one of the TM Forum's contributions is the introduction of the Open Digital Architecture (ODA)[32], which provides scenarios for Business and Infrastructure Functions and their respective implementation through technology neutral "*flavours*". These implementations are offered in the form of Open APIs, allowing vertical customers to interact and consume offered X as a Service (XaaS), where X refers to the resource under consideration (e.g. network slice, network service, etc.).
Considering the vendor agnostic nature of the forementioned Open APIs, accompanied with their bottom-up composition across layers and broad adoption from telecommunications industry make TM Forum's Open APIs a perfect candidate for integrating components among multi-vendor environments.
TM Forum uses ODA as reference architecture to elaborate on network slicing implications. From a customer-facing viewpoint, that also affect this project, the following references are relevant:

- GB999 – ODA Production Implementation Guidelines[33]: presents slice management architectures and use cases as derived from various catalysts. Additionally, it references the set of Open APIs that could be used for slice management, including APIs for service catalogue management[34], service ordering[35], service inventory management[36].
- TMF909A – Network as a Service (NaaS) Component Suite Profile[37]: covers the operations required to be exposed in order to provide the functionality required across interworking Operational Domains.

1.2.3.3 3GPP

3GPP is the umbrella term which unites seven national or regional telecommunications SDOs as primary members (known as "*Organisational Partners*") and a variety of other organisations (referred to as "*market representation partners*"). The scope and content of the standardisation work is defined by Organisational Partners, acting as the primary decision-making body.

3GPP standardisation work consists mainly of Technical Specifications and Technical Reports documents undergoing revisions over several releases. Documents are released by specification groups. There are three top level Technical Specification Groups (TSGs) and several Working Groups (WGs) under the umbrella of each TSG.

The most relevant working groups for 5GASP are WG2 – System Architecture, WG5 – Telecom Management and WG6 – Mission-critical applications of Services & Systems Aspects TSG. Release 17 is currently being worked on with targeted freeze date in June 2022. Due to the peculiar ongoing circumstances the original timeline was revised.

1.2.3.3.1 TSG SA2 – System Architecture & Services

The specification of 3GPP Release 16 5G system architecture is included in 3GPP TS 23.501[38], 3GPP TS 23.502[39], 3GPP TS 23.503[40]. Release 16 provides the specification of the "*5G stage 2 system*", including the features and capabilities for the deployment of commercial 5G networks, further extended from Release 15.

Notable differentiation from the more traditional 4G reference model was the introduction of a Service-Based reference model, harnessing the flexibility derived from the architecture modularisation of Network Functions (NFs) with looser implementation restrictions. *Figure 3* illustrates the reference model in service-based representation for a non-roaming use case.

The interaction between NFs is based on a service-based representation, where authorised NFs are accessing their services within the Control Plane (CP) and a reference point representation, where the interaction between services is described by reference points across any NF's pair.

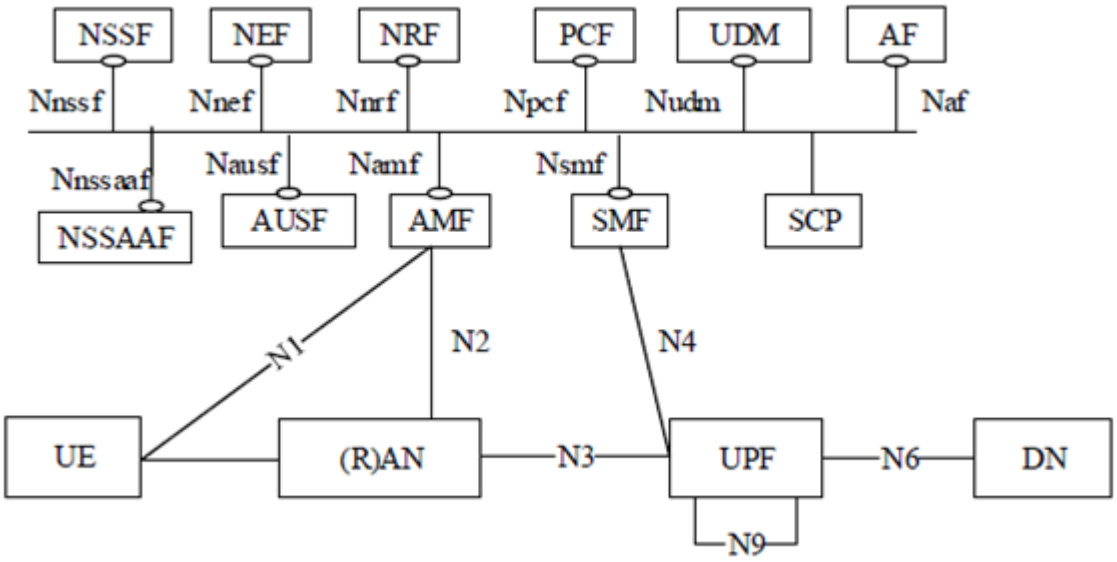


Figure 3 5G Architecture, non-roaming reference architecture[38]

1.2.3.3.2 TSG SA5 – Management, Orchestration and Charging

Working group 3GPP SA5, which mainly focuses on Management, Orchestration and Charging, specifies requirements and procedures for the provisioning of network slices to facilitate the emerging needs of 5G network services. The core set of specifications, 3GPP TS 28.530[41], 3GPP TS 28.531[42], 3GPP TS 28.532[43] and 3GPP TS 28.533[44] studies the stage 1 and stage 2 of the network slicing specification. TS 28.530 introduces network slicing concepts and use cases followed by TS 28.531, which includes technical use cases and operations. TS 28.532 proposes a set of generic management services from slice provisioning to performance and fault management, while TS 28.533 describes the concepts behind the implementation of these management services under a possible architectural framework.
Current approach (Release 16) is structured upon a service-based architecture defined in3GPP TS 28.533[44], which executes the provisioning and lifecycle management of network slices through well-defined build blocks[45] introduced as:

- Communications Service Management Function (CSMF): Responsible for translating the Customer Service (CS) related requirements to network slice related requirements and the management of the Communication Service Instance (CSI).
- Network Slice Management Function (NSMF): Assigned with the management and orchestration of the Network Slice Instance (NSI) and derives network slice subnet related requirements from network slice related requirements.
- Network Slice Subnet Management Function (NSSMF): Charged with the management and orchestration of the Network Slice Subnet Instance (NSSI).

The aforementioned entities are part on the slice provisioning hierarchy levels. There are three main hierarchies: the NSI level, the NSSI level and the NF level. The latter can be either Virtual or Physical (i.e., VNF/PNF). The NSSI level is recursive and could be composed of multiple constituent NSSIs. The information models implementing these entities are examined in 3GPP TS 28.541[46]. The slice provision hierarchy levels along with their respective information models is depicted in *Figure 4* as a Unified Modelling Language (UML) diagram.

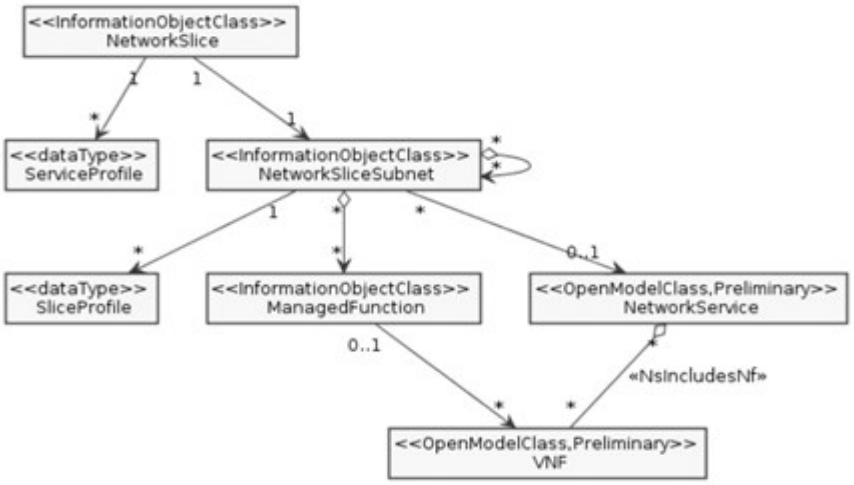


Figure 4 3GPP network slice information model

3GPP SA5 and GSMA have collaborated in the complex work of designing a model-based network slice specification. This collaboration has been based on keeping Network Slice Information Object Class (IOC) definition aligned with the GSMA's GST specification. This alignment responds to the need for a consistent mapping of customer-facing service

requirements (GSMA domain) to resource-facing service requirements (3GPP domain). It is built upon the idea that GST attributes representing network slice Service Level Specification (SLS) need to be translated into the 3GPP ServiceProfile. The ServiceProfile is a construct defined within the Network Slice IOC that allows for the service properties of a network slice (e.g. maximum/guaranteed downlink throughput, network isolation, packet delay budget, etc.) to be defined.

As shown in *Figure 5*, the GST is translated and used as input to ServiceProfile. Then, the ServiceProfile can be translated to corresponding requirements for dedicated domains, i.e., SliceProfiles. For example, 5G Core (5GC) SliceProfile is used to carry 5GC domain requirements, New Generation - Radio Access Network (NG-RAN) SliceProfile is used to carry NG-RAN domain requirements, and Transport Network (TN) requirements are translated and provide to TN domain.

Some initial attempt in the mapping of customer-facing service to resource-facing service requirements is conducted in 3GPP TS 28.541[46] and is expected to be further studied in Release 17 document.

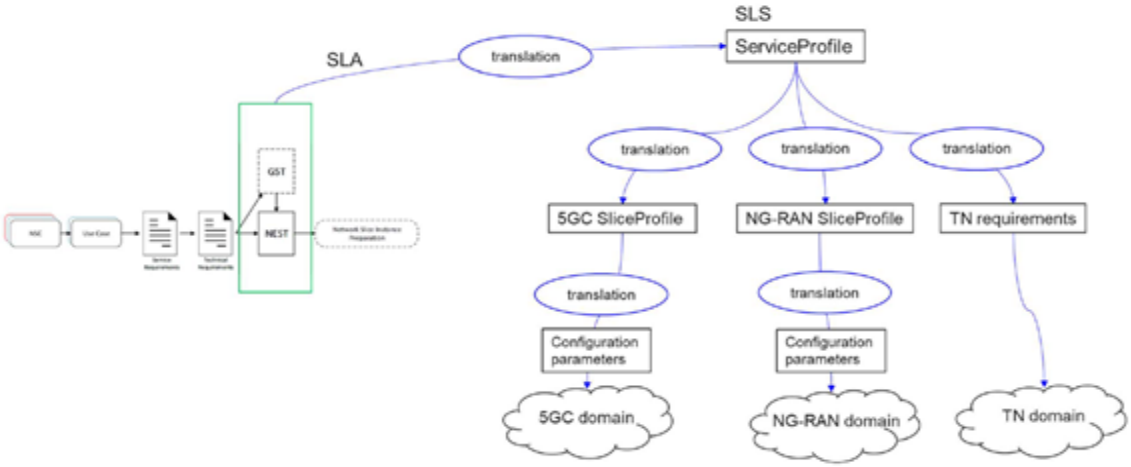


Figure 5 Relation between GST and 3GPP Service Profile[47]

1.2.3.3.3 TSG SA6 – Mission-critical applications

Working group SA6 is the application enablement and critical communication applications group for vertical markets. Its main objective is to provide application layer architecture specifications for critical communication applications (e.g. Mission Critical services for public safety, railways) along with enablers for vertical applications (e.g. automotive, drones, smart factories). Furthermore, SA6 is also responsible for providing functional architecture, procedures, information flows and deployment models to support the proposed requirements. An example of working group's proposal is the Common API Framework (CAPIF) for 3GPP Northbound APIs[48], which is a work towards the introductions of common aspects applicable to any northbound service APIs, thus tackling the duplication and inconsistency of approach between different API specifications. The common API framework applies to both Evolved Packet System (EPS) and 5G System (5GS), and is independent of the underlying 3GPP access. The 5GASP project, which relies exclusively on 5GS, shall leverage SA2's system architectural document, i.e. 3GPP TS 23.501[38], that reference the support of CAPIF by the 5GS.

1.2.3.4 ETSI NFV

NFV technology was initially introduced in 2012 by the ETSI and the NFV Industry Specification Group (NFV ISG) in particular, enabling the transition of network functions from proprietary, vendor-specific hardware to software hosted on commercial platforms[49].
Since its definition, ETSI NFV reference architectural framework has been repeatedly enhanced with new features, divided in several releases. ETSI NFV ISG's work is organised into two-year phases, with each introducing a new release. Release 1, 2 and 3 are currently completed and closed for any further contributions, while NFV Release 4 is on progress. The main focus on the Release 4 is the simplification of network deployment and operations. Deployments towards container-based approaches and introduction of service-based architectural concepts can be highlighted as principal novelties. Also, further 5G support along with the involvement of generic Operations, Administration and Maintenance (OAM) functions leads to a complete ecosystem enabling next generation network implementations, which could be leveraged in the scope of this project as well. A brief recap on the NFV Releases is depicted in *Figure 6*.

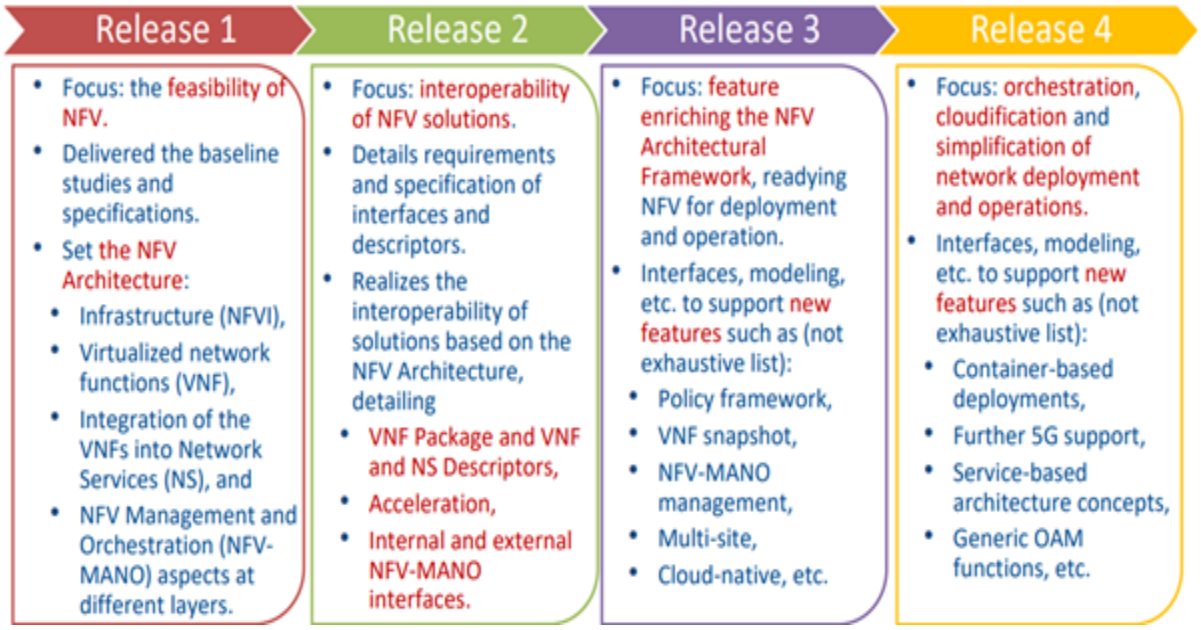


Figure 6 NFV Releases

The architectural foundations, which aim to allow consistent deployment and operation of network services in any virtualisation environment, are established in the reference architectural framework and more specifically the NFV MANO stack, originally specified in ETSI GS NFV-MAN 001[50] from ETSI NFV ISG.

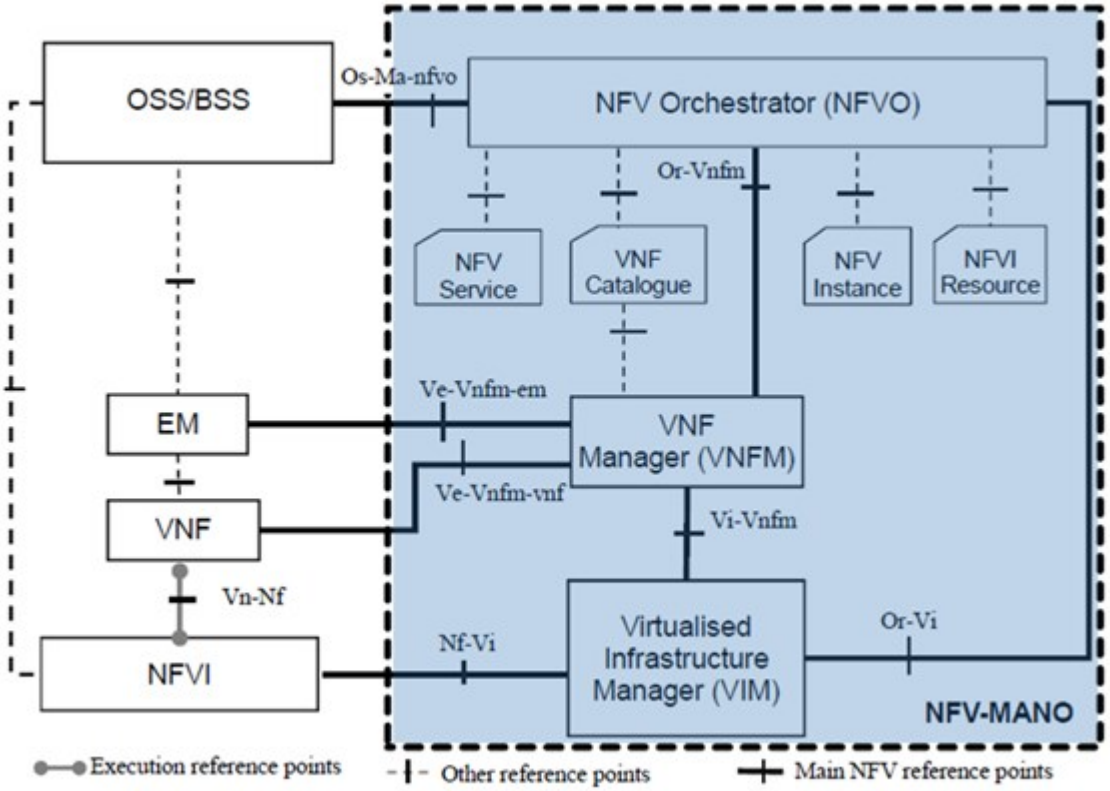


Figure 7 NFV-MANO architectural framework[50]

The NFV-MANO architectural framework depicted in *Figure 7* is comprised of three hierarchical entities:

- The Virtualized Infrastructure Manager (VIM) which controls the interaction of VNFs with physical resources under its supervision (e.g., resource allocation, deallocation, inventory);
- The VNF Manager (VNFM) which is responsible for managing the VNF lifecycle (e.g., instantiation, configuration, termination);
- The NFV Orchestrator (NFVO) which is responsible for the lifecycle management of network services deployed on NFV Infrastructure (NFVI). Also, it undertakes the orchestration of resources across multiple VIMs.

As the functional blocks taking part in NFV MANO can be reused and extended to facilitate the management and orchestration of components that can comprise a network slice, it is widely accepted in the research community that network slicing could be supported combining this architecture with slicing principles from other SDOs. To that extend, the Evolution and Ecosystem (EVE) working group was introduced with the purpose of studying how network slicing can benefit from capabilities provided by NFV MANO. This purpose is twofold: the analysis of network slicing use cases as defined by SDOs, and the attempt to map these use cases onto NFV MANO architecture. The resulting ideas of this work are included in ETSI NFV-EVE 012[51]. Although, visions on network slicing from many resources are summarised in this technical report, 3GPP is considered as the principal reference body for the definition of the network slicing concept. The main scope of ETSI NFV-EVE 012 is to

identify how NFV and 3GPP worlds could coexist in the management and orchestration of network slices.
For this purpose, an initial attempt to align terminology from NFV Network Service (NS) and 3GPP (network slice, network slice subnet, network function) under the same principal was made. As depicted in *Figure 8*, ETSI states that a network slice could accommodate a network service, thus facilitating the network requirements of a communication service. Based on this concept, ETSI NFV-EVE 012 established the correspondence between the conceptual models of both SDOs through the claim that a network service can be regarded as the resource-facing view of a network slice subnet[51].

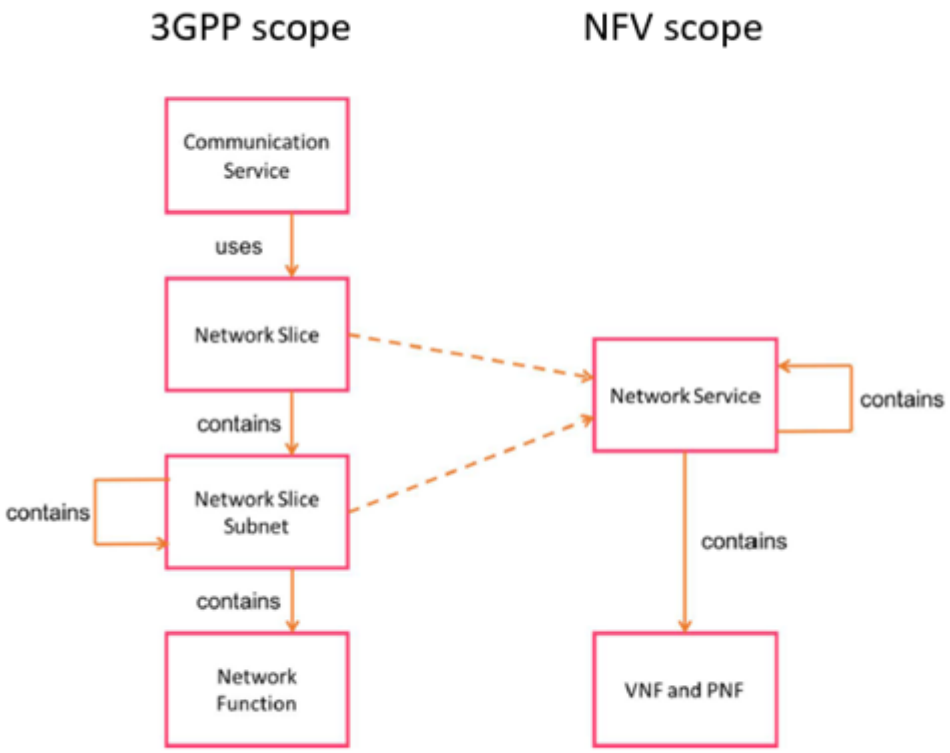


Figure 8 Relation between information models[51]

Another issue addressed in ETSI NFV-EVE 012 is the definition of a unified framework where both 3GPP management system (see *1.2.3.3.2 Section*) and NFV MANO can coexist. This also involves the definition of the potential reference points for their interaction. The initial architecture mapping approach of ETSI NFV-EVE 012 is reviewed and extended and illustrated in *Figure 9*[52].

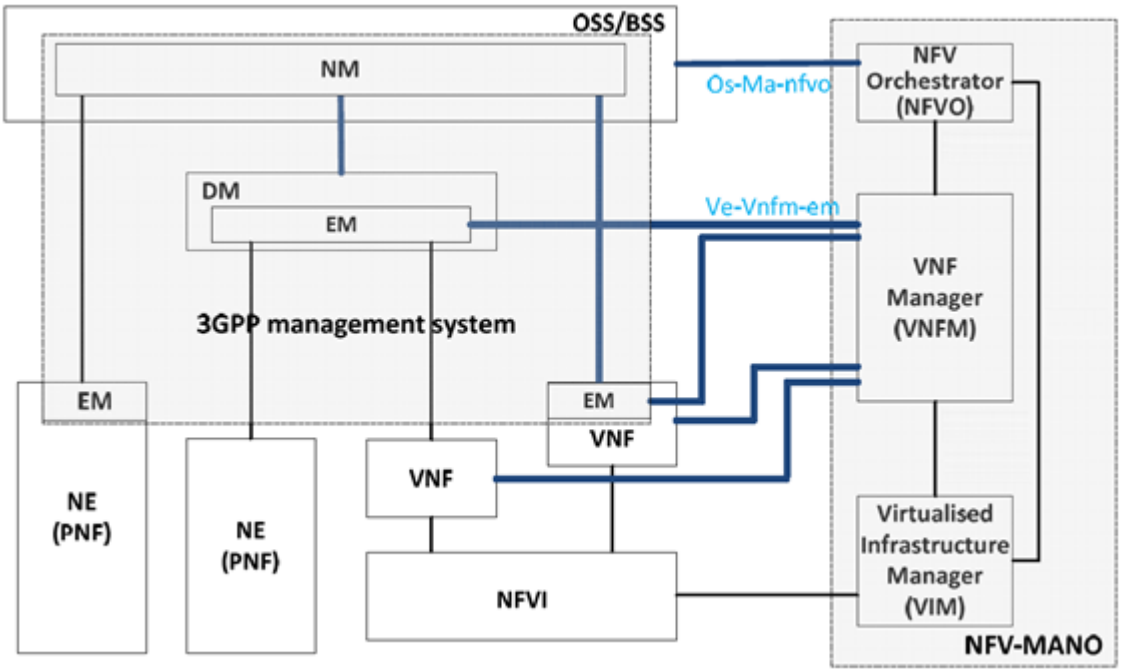


Figure 9 Mapping relationship between 3GPP and NFV-MANO architectural framework[52]

The intended interaction could take place by potentially utilising the aforementioned reference points, which are addressed as:

- Os-Ma-nfvo[53] which is used for NS lifecycle management, NS performance management, NS fault management, NSD management and VNF Package management produced by NFVO;
- Ve-Vnfm-em[54] reference point used for VNF lifecycle management, the information delivery of VNF and virtual resources failure or performance measurement information and virtualization configuration.

1.2.3.5 Automotive

Vehicle manufacturers are more and more faced with the need to provide connectivity on board of the vehicles they are producing. Connectivity is commonly known to be used for navigation and other similar use cases, but is it also required for telemetry during all the lifecycle of the vehicle. Disruptive automobile makers such as Tesla are even using connectivity to perform remote software update (e.g. reconfiguration of the battery to boost the performance in the event of public emergency as it was performed the day before a tropical storm in Florida). Connectivity is also needed to improve Advanced Driver Assistance Systems (ADAS) by communicating speed and position between vehicles in order to avoid collisions. Last but not least, electricity charging requires the exchange of data between the vehicle and the charging systems, for booking, billing, and charging International Organization for Standardization (ISO) 15118.

Many of the topics pertaining to the vehicle are being standardized, particularly at ISO in the technical committee 22 "*road vehicles*".

With the advent of 5G, vehicle manufacturers are preparing to develop a business around data collected by vehicles (for repair, lifecycle management, road safety, and other more value-added services). They have thus developed the concept of "*extended vehicle*" where

all data of the vehicle is gathered in the cloud of the vehicle manufacturer and made available to subscribed and authorized parties.
Vehicle manufacturers and their equipment providers are gathered in several association. 5GAA (5G Automotive Association) and the Car2Car Communication Consortium (C2C-CC) are particularly relevant to the work conducted by 5GASP. 5GAA is lobbying for the deployment of 5G for vehicle connectivity whereas C2C-CC is developing specification of services and technologies where information is exchanged between vehicles and the roadside infrastructure (V2X, see next section).

1.2.3.6 Cooperative Intelligent Transport Systems (C-ITS)

C-ITS shares data between vehicles, other road users, the roadside infrastructure, the urban infrastructure and services platforms in the cloud, in order to improve road safety, traffic efficiency and other value-added services. Some services may be time-critical, others, not.
C-ITS services rely on standardized data formats and messages, communication technologies and security features (Public Key Infrastructure (PKI), certificates, hardware security module, etc.) specified at ISO (technical committee 204 on "ITS", CEN (technical committee 278 on "ITS", and ETSI technical committee "ITS". All communications pertaining to C-ITS services are based on the so-called ***ITS station*** *(ITS-S) data and communication reference* ***architecture*** (ISO 21217 - edition 2020 & ETSI EN 302 665 - edition 2010)[55]. *10* presents the diagram used to represent ITS station symbol and origins.

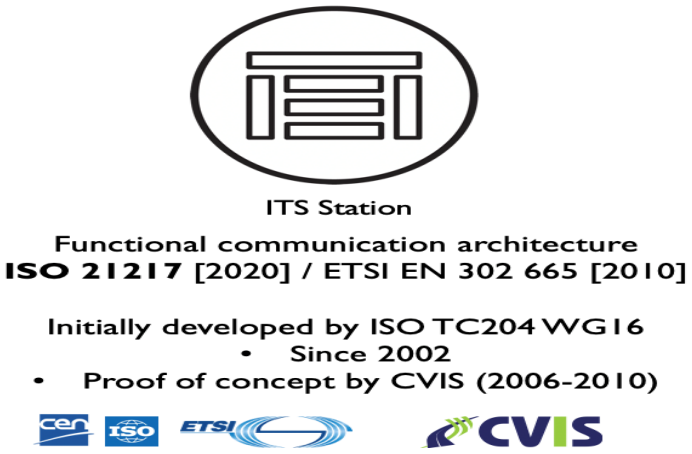


Figure 10 ITS station symbol and origins[55]

References: C-ITS Brochure[56] , C-ITS Platform[57] and C-Roads[58] provide a good source of information for getting started on the motivations behind C-ITS, C-ITS use cases, technologies and standards.
Figure 11 shows a generic detailed diagram of the functionalities of the ITS station that can be implemented in a vehicle (vehicle ITS station), in a roadside equipment (roadside ITS station), in the cloud (central ITS station) or in a nomadic device (personal ITS station).

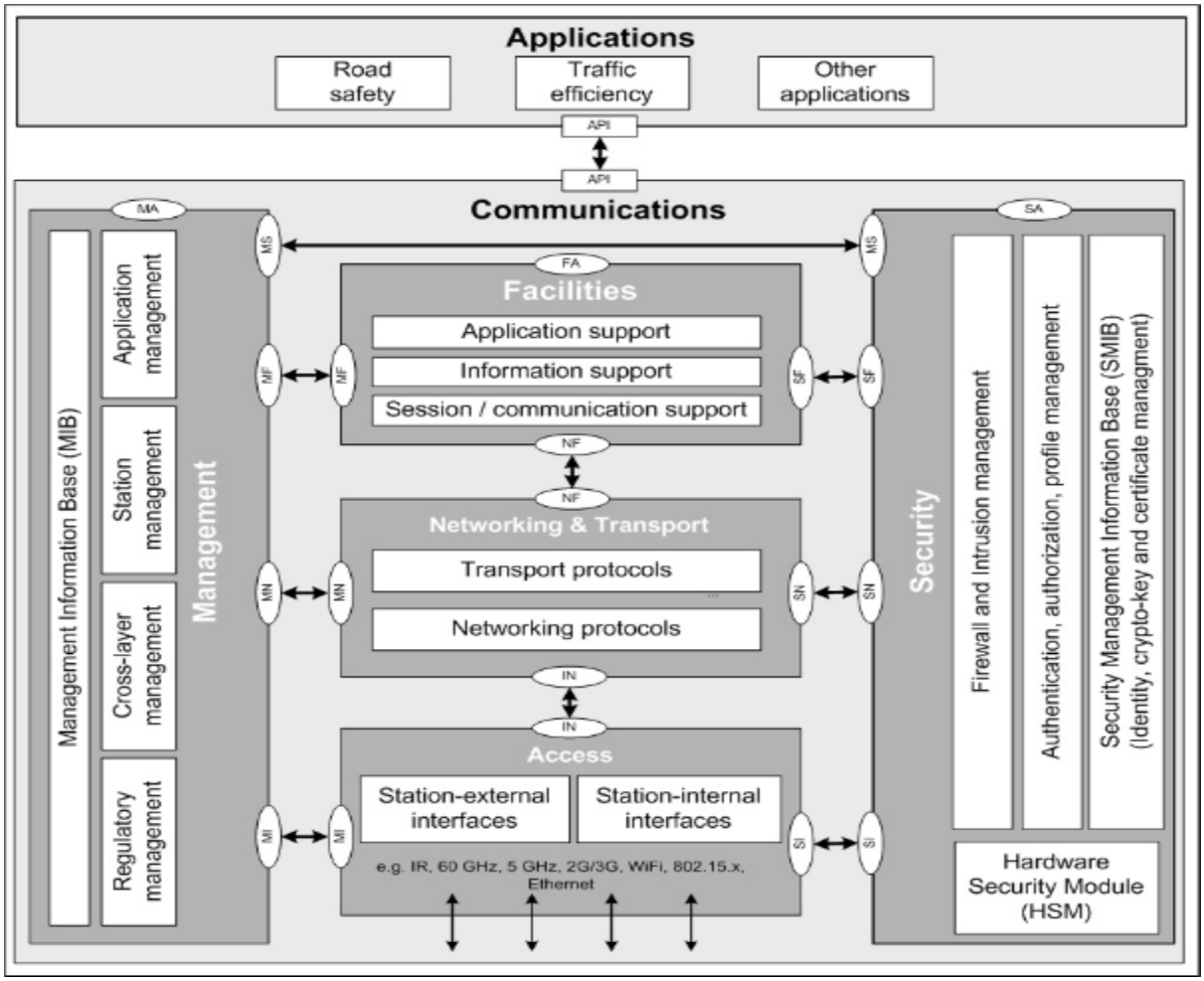


Figure 11 Detailed ITS station architecture

This layered architecture (Open Systems Interconnection (OSI) type) comprises the ITS station access technologies layer, the ITS station networking & transport layer, the ITS station facilities layer, the ITS station application entity, the ITS station management entity and the ITS station security entity. Each layer comprises a diversity of functionalities that can be chosen from according to the environment of exploitation.

Some of the functionalities are compulsory, but most are optional and may only be required for a specific deployment environment (type of service to be provided or type of hardware: vehicle, roadside equipment, nomadic device or control center).

The use of 5G communications is contemplated for communications between ITS stations:

- long-range communication between the roadside ITS station and the central ITS station;
- long-range communication between the vehicle ITS station and the central ITS station;
- short-range communication between the roadside vehicle ITS station and a roadside ITS station or between any two vehicle ITS stations.

Whether 5G or another access technology is used, ITS station must comply with the ITS station architecture and related C-ITS standards. The C-ITS services provided by ITS stations must be the same from a user's point of view. However, the characteristics and the performance of

5G technologies can allow to move some of the functionalities of the ITS station either in the edge of the network or in the cloud.

- Instead of providing some of the functionalities of the ITS station directly in physical elements (vehicle, roadside equipment), in particular data provided by sensors (e.g. magnetic loop in case roadside, or radar in the case of vehicle) or geo-localized data about the surrounding environment registered in a Local Dynamic Map (LDM), such data could be provided directly in the cloud. This leads towards the development of a generic ITS station NetApp in the cloud that provides C-ITS services alike if the data was directly available in the vehicle or roadside equipment (see *2.3 Section: NetApp 3*).
- 5G may also be used for networking between adjacent roadside ITS stations spread over a portion of road to deliver the same level of road traffic and traffic efficiency services to vehicles along the road. This leads towards the development of virtual Road Side Units (vRSU) covering a large road portion on average rather than physical RSUs covering only a tiny portion of road portion (see *2.2 Section: NetApp 2*).

1.3 Approach and Methodology

The development methodology of the 5GASP project has been defined with practicality and productivity in mind: start fast, co-produce with all relevant partners and validate with frequent feedback loops and mature and scale early.

To start fast, 5GASP is ramping up with a method of weaving together requirements and architecture driven by WP2 and utilising parallel ramp-up of WP3 and consequently WP4 and WP5 to double-click into the details of consortium-wide topics that will be assimilated in the initial architecture draft (this document). The method starts with a statement of how each partner understands and intends to leverage the project entities and relationships (NetApps, Consumers and Infrastructure Sites) and is followed by a rapid succession of harmonising discussions that lead to a consortium-wide shared understanding of requirements, architecture and design for the interfaces required by the system. These discussions are then followed by iterative refinement with specific topics in WP3, WP4 and WP5 and establish a well aligned detailed specifications for all partners in WP2.

The architecture of the 5GASP platform is driven by design goals defined by key representative industrial partners from the relevant infrastructure provider or NetApp sectors. These partners, already strongly engaged in running individual 5G-related projects, offer necessary data sources and diversification of models and entities to ensure all necessary entities, patterns and interfaces are initially considered, thus validating the overall process and ensuring success in development in WP3. The high-level goals for the 5GASP platform each contain both functional and non-functional aspects, ranging from needs and capabilities for placement and networking, compatibility with hardware and software requirements for relative NetApps, existing development and operational concepts. Especially the handling of developer usability aspects in terms of upload packages, as well as potentially sensitive and privacy-related data in a multi-party context spanning multiple trust boundaries has been discussed in terms of authentication, isolation and control of data handling.

Starting with Month (M)6, the technical work in WP3 will follow best practices that are well established in industry and be based on initial requirements established as part of the WP2 draft. As central guidance will be this project-wide joint roadmap draft (D2.1) of with three distinct phases: a continuous integration/continuous delivery system plans along with the

5GASP base platform (at M12), an integrated prototype (at M19) and a refined iteration with NetApps implementation and testing in WP4 and 5 through M24. Each partner will maintain his own detailed backlog of work items that are traced to the joint roadmap. At each release, the achievements will be tested and made available for integration and validation to other partners. The frequent cycles offer continuous awareness and learning to maximize joint productivity, minimize quality problems and giving each partner the ability to retain its own freedom and culture. The individual partners' detailed requirements from infrastructure and NetApp capabilities will not be set at the beginning of the project once for all and frozen. Instead, they will be refined throughout the entire duration of the project. In 5GASP, requirement engineering shall not be intended as a single phase in the development chain, but rather a dynamic and iterative process of tailoring and refinement, aiming to transform individual requirements into a Platform that is flexible and adaptable and result in an updated Reference Architecture in M24. This way, the development of the Platform (and its associated service layer) will gradually include more and more functionality over time, with updated documentation that reflects the current state-of-the-art.

1.4 Document Structure

This document is composed of six chapters, the first chapter, Introduction, presenting the objectives of this document, state-of-the-art (detailing related projects, open source projects and standards to consider) and approach and methodology.
Chapter 2 presents the 5GASP definition of NetApps, as well as vertical-specific requirements and Infrastructures for each of the eleven NetApps involved in the project (NetApp 1: Virtual On-Board Unit provisioning NetApp (vOBU), NetApp 2: Virtual RoadSide Unit provisioning NetApp (vRSU), NetApp 3: ITS station NetApp, NetApp 4: Multi-domain Migration NetApp, NetApp 5: Vehicle-to-Cloud (V2C) Real-Time Communication NetApp, NetApp 6: Remote Human Driving NetApp - Teleoperation for assisting vehicles in complex situations, NetApp 7: Efficient MEC handover NetApp, NetApp 8: PrivacyAnalyzer NetApp, NetApp 9: 5G Isolated Operation for Public Safety NetApp (5G IOPS NetApp), NetApp 10: Vehicle Route Optimizer NetApp, NetApp 11: Fire detection and ground assistance using drones (FIDEGAD)) and the overall 5GASP NetApps vertical-specific requirements.
In chapter 3, the architecture and the capabilities of each of the six experimentation facilities involved in the 5GASP project are described: Aveiro, Bristol, Patras, Murcia, Ljubljana and Bucharest.
The experimental model, the Net Apps deployment and orchestration, the DevOps (CI/CD) context and 5GASP Model Entities (Roles) are presented in chapter 4.
Chapter 5 describes the main part of this deliverable: the 5GASP Infrastructure Architecture, by detailing the 5GASP Global Infrastructure Architecture, 5GASP Internal and external components and their interfaces, the 5GASP experimentation API service, the experiment service orchestrator, multi-domain, physical architecture and NetApp workflows: NetApp deployment workflows and NetApp testing workflows.
Finally, chapter 6 provides conclusions and directions for future work.

2 5GASP NetApps vertical-specific requirements and Infrastructures

This chapter will describe for each of the eleven NetApps involved in the project (NetApp 1: Virtual On-Board Unit provisioning NetApp (vOBU), NetApp 2: Virtual RoadSide Unit provisioning NetApp (vRSU), NetApp 3: ITS station NetApp, NetApp 4: Multi-domain Migration NetApp, NetApp 5: Vehicle-to-Cloud (V2C) Real-Time Communication NetApp, NetApp 6: Remote Human Driving NetApp - Teleoperation for assisting vehicles in complex situations, NetApp 7: Efficient MEC handover NetApp, NetApp 8: PrivacyAnalyzer NetApp, NetApp 9: 5G Isolated Operation for Public Safety NetApp (5G IOPS NetApp), NetApp 10: Vehicle Route Optimizer NetApp and NetApp 11: Fire detection and ground assistance using drones (FIDEGAD)) the following vertical-specific requirements:

- Description of demonstration environment;
- NetApp high level infrastructure;
- NetApp KPIs;
- Overall integration needs.

Although there does not yet exist a standard definition of what a NetApp is, in 5GASP we identified some key characteristics that shall aid to the definition of a NetApp in the context of the 5G System. Specifically, in 5GASP we consider that:

A NetApp, in the context of the 5G System, is defined as set of services that provide certain functionalities to the verticals and their associated use cases.

The following are some identified characteristics of a NetApp, following the terminology introduced in Section 'Definitions' in the beginning of this document. Specifically, a NetAapp:

- Should deliver services to 5G Verticals;
- May consist of both software and hardware parts;
- Must embrace the Service Based Architecture paradigm;
- Should follow the NFV model;
- May expose APIs to be consumed by other service consumers. The exposed APIs should be delivered in an Open API model and may follow the 3GPP recommended APIs for applications (i.e. 3GPP CAPIF, Service Enabler Architecture Layer for Verticals – SEAL);
- A NetApp may be part of one or more vertical application services;
- One or more services of the NetApp may be attached to one or more 5G User Plane Function (UPF) data paths;
- May be part of one or more 5G slices. The slices may be shared or not;
- Part of a NetApp may reside at the User Equipment (UE) side. The part of the UE side may interact with a NetApp service that resides within the domain network. The UE part may follow the definition of the Vertical Application Layer (VAL) client of 3GPP;
- May be part of the 5G Core. In such case, then it must follow the 3GPP standards;
- May interact with the 5G System by consuming 5G system's APIs, if the 5G system allows. When interacting with the 5G System, it must support relevant 3GPP standards. Such interactions may include location services, Quality of Services (QoS) management, Assured Forwarding (AF) traffic;
- May support service continuity by minimizing service interruption when transferring application context;
- Software parts should be deployed either in a virtualized or containerized manner;

- May have resource and network requirements in terms of hardware, memory, Graphics Processing Unit (GPU), Central Processing Unit (CPU), availability, etc.;
- May have placement requirements (e.g. edge, region, core, etc.). Additionally, a network latency KPI must be specified by the NetApp when requesting a slice by the 5G system;
- May consume monitoring and telemetry data from the 5G System. Such data from the 5G System should be consumed by functions like the Network Data Analytics Function (NWDAF);
- May interact with the VIM/Container Infrastructure Service Management (CISM) of the domain, if this is not restricted;
- May interact with the Service or NFV Orchestrator of the domain if this is not restricted;
- Should follow relevant 3GPP security definitions and recommendations.

To gather 5GASP NetApp requirements we provided the following templates to the NetApp developers, SMEs, of the consortium:

1. A generic architectural template to be followed by the NetApps in order to be able to understand their requirements in terms of data paths, interactions with the 5G system, the placement of their components in the 5G system, etc. The developers need to describe their services according to the architectural template depicted in *Figure 12*.
2. NetApp developers were advised to identify their 5G requirements by expressing them in the form of the GST of GSMA, thus producing a NEST.
3. NetApp developers were requested to provide their integration and dependency needs in terms of resources (VNFs, NSDs, Virtualized Distributed Units (VDUs)).

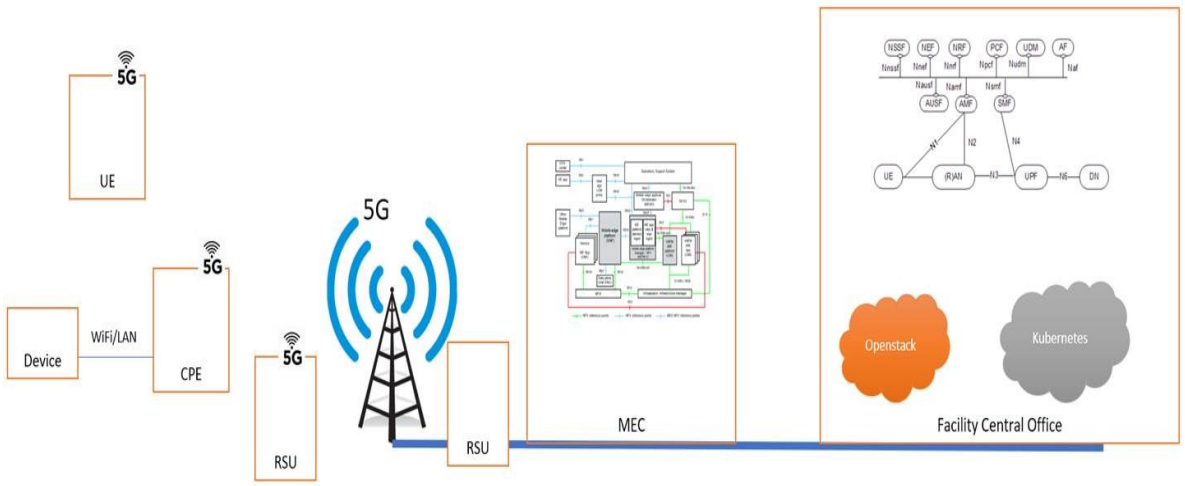


Figure 12 NetApp generic architectural template

2.1 NetApp 1: Virtual On-Board Unit provisioning NetApp (vOBU)

- **Description of demonstration environment**

One of the most important advances of 5G communications is the virtualization of computing and network functions. These advances have enabled the possibility to easily implement the MEC capabilities that aim to offload tasks performed by mobile devices and ensure low latencies responses due to the proximity of the computing facilities to the point of attachment. In order to integrate all the required virtual resources for each OBU, the novel

idea of instantiating virtual substitutes for these OBUs (vOBUs) has been proven beneficial in terms of device access delay, reliability against wireless disconnections or data cache, as the Hybrid Communications to Foster 5G Vehicular Services (SURROGATES) proposal[59] has showed in the context of the 5GinFIRE project. OdinS introduces this solution that provides the necessary vOBUs that are instantiated at the edge of the access network with the purpose of offloading computationally-intensive tasks to the network, following the MEC approach.

- **NetApp high level infrastructure**

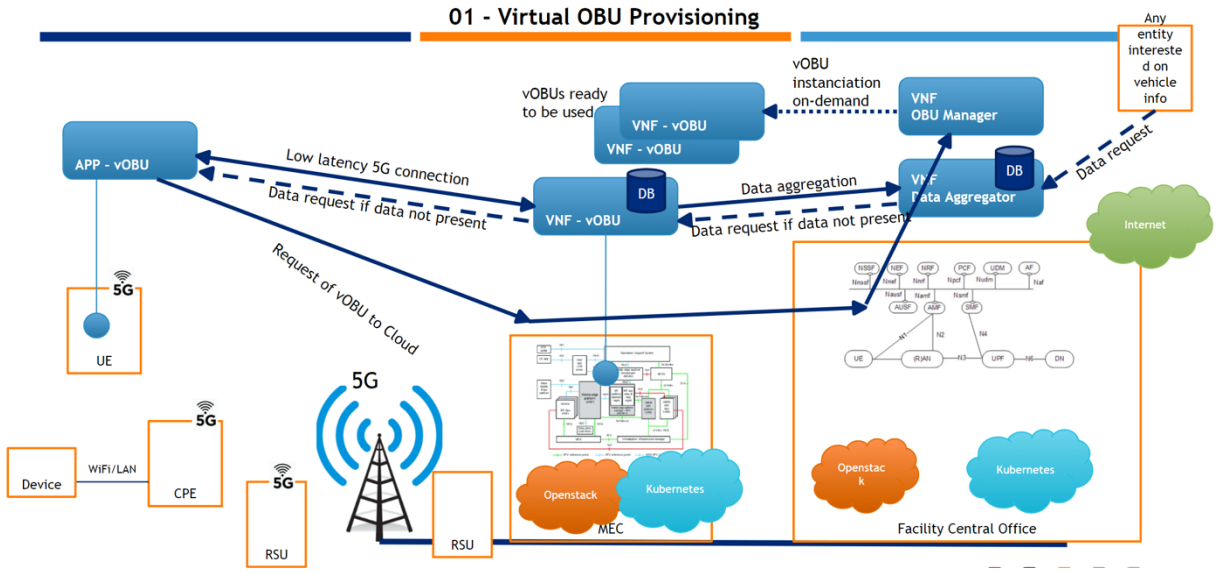


Figure 13 Virtual On-Board Unit (vOBU) provisioning NetApp Infrastructure

As depicted in *Figure 13*, the vOBU NetApp can be used to gather logging information about the status of the vehicle and to delegate the analytic processes to the virtual surrogate, that could also act as a proxy for external requests of vehicle status, avoiding them reaching to the real OBU that should be focused in higher priority tasks.

- **NetApp KPIs**

Table 5 vOBU NetApp KPIs

Generic KPI name	Metric Indicator (How)	KPI value	KPI unit
Initial time	Time needed to deploy for first time the entity (vOBU)	<5	Minutes
Transaction speed	Each message sent from an OBU needs to be redirected to the vOBU	500	Miliseconds
Packet Loss Ratio	Ratio of packets loss between the OBU and vOBU. Packets loss above packets sent	1	%
Service response time	Delay ratio while including vOBU instantiation	<30	%
Service downtime	Ratio of time the vOBU is not up and running	<10	%

Table 6 vOBU NETAPP's NEST

vOBU NETAPP's NEST	
Area of service	SP, PT, UK, RO (AUTO-V use case)
Area of service: Region specification	Murcia, Aveiro, Bristol, Bucharest
Downlink maximum throughput per UE	-
Uplink maximum throughput per UE	-
Isolation level	Virtual resources isolation
V2X communication mode	YES, New Radio (NR)
Slice quality of service parameters: 3GPP QoS Identifier (5QI)	9
Maximum Packet Loss Rate	1%
Supported device velocity	3: Vehicular: 10 km/h to 120 km/h

- **Overall integration needs**

Packaging Info (Virtual Machine (VM), container, type, etc.): NSD, 3 VM Roles (VNFD): Manager, Aggregator and the vOBUs themselves plus the onboard software (python- based).
Existing Healthcheck or Lifecycle (deployment status) Hooks or APIs: No.
Dependencies of the 5G System (requires slicing, core functionality, etc.): Requires dynamic VM deployment and MANO connectivity to recover deployment status information.
How is it operated (and does it require manual interventions): Configuration of Mobile device requires human intervention. Right now, configuration with Ansible scripts, adaptation to fully automated deployment planned. Protocol used: IPv6 (CoAP).
Dependencies (does it expose or consume services from/to other NetApps): No.

2.2 NetApp 2: Virtual RoadSide Unit provisioning NetApp (vRSU)

- **Description of demonstration environment**

Vehicular communications are taking place directly between vehicles and the roadside infrastructure for the purpose of improving road safety and traffic efficiency. This is known in Europe as C-ITS. C-ITS services rely on standards developed by ISO, European Committee for Standardization (CEN) and ETSI and make use of several key technologies, including broadcast messages transmitted between vehicles and the roadside using localized communications Vehicle-to-everything (V2X). Such services are currently being deployed using LTE for long-range centralized communications and ITS-G5 for short range localized communications, an 802.11 WI-FI variant in the 4.9 GHz frequency band.
An RSU is a type of equipment deployed on the side of the road infrastructure to detect hazardous situations or other traffic variables (black ice, humidity, obstacles, etc.) and inform passing by vehicles about such hazard and other information (traffic light time and phase, work zones, speed limits, etc.). The RSU could be attached to road traffic Variable Message

Signboards (VMS), traffic lights, electronic toll-gates, etc. or could be deployed as standalone equipment. They may be connected to control traffic center via any means (cellular, optic fiber, Long range, low power wireless platform (LoRA), etc.).
RSUs have recently been deployed across Europe to provide C-ITS service for road safety, traffic efficiency and others value added services. RSUs are then designed with communication capabilities to transmit information directly between road users and the road side, using V2X localized communications. Such localized communications between the RSU and the vehicles don't require support of any telecommunication network infrastructure.
Such services are developed in compliance with the set of C-ITS standards and particularly the ITS-S data and communication reference architecture[55,60] . The C-ITS services are provided by means of standardized messages usually sent in broadcast mode (from the RSU: Signal Phase and Time (SPaT)/ Map Data (MAP) for traffic light phases, Collective Perception Message (CPM) for intersection safety, Service Announcement (SAM) for service announcements; from the vehicle: Cooperative Awareness Messages (CAM) for anti-collision and Decentralized Environmental Notification Messages (DEMN) to announcing road traffic hazards).
RSU delivering services in compliance with C-ITS standards are also call Roadside ITS Stations (R-ITS-S). Currently deployed, R-ITS-S are usually using the ITS-G5 radio technology, a variant of WI-FI 801.11ac developed specifically for vehicular communications. Other technologies are being considered such as Bluetooth and more importantly relevant to 5GASP Long Term Evolution (LTE)-V2X (PC5 mode) and 5G NR -V2X.
In the context of 5GASP we are only going to deal with RSUs designed as R-ITS-S, irrespective of the underlying access technology used for direct communication between road users (vehicles or other) and the roadside.
In the current deployment model, RSUs are deployed alongside the road network with more or less long distances between two units (they do not need to provide seamless network coverage). In addition to perform communication operations, they also do the processing of data locally (sensor data fusion, security check, etc.). Doing this processing directly at the side of the road is not necessarily a good practice from a deployment cost and performance view point, especially when multi-sensor data fusion is to be considered.
It is not possible to deploy RSU everywhere. It would be too expensive, particularly on roads with low frequency of vehicles or in large unpopulated areas, especially if cellular coverage is available. However, it is still necessary to deploy C-ITS services with the same level of performance everywhere. In such situations, virtual roadside ITS stations would allow the collection and transmission of data alike physical ITS stations along the road.
Connecting road infrastructure using a C-ITS virtualized backend can be an efficient solution at both cost and functionality levels. Compared to deploying Physical compliant Roadside Units, the deployment costs are expected to reduce from 10 to 100x for the public sectors and at the same time improve service penetration by leveraging 5G connectivity.
One of the important innovations in 5G communications is the ability to handle multiple radio technologies and particularly to handle short range localized communications involving vehicles and the roadside infrastructure. Such feature has originally been put forward in LTE as LTE-V2X (PC5), as a solution operating in the same 4.9 GHz frequency band as ITS-G5 to gradually replace the technology currently in place (ITS-G5 in Europe). It is now emerging in 5G as V2X NR side link. The virtualization of computing and network functions is yet another major step forward as indicated in *2.1 Section*. As pointed out in the previous section, these advances have enabled the possibility to easily implement the MEC capabilities that aim to

offload tasks performed by mobile devices and ensure low latencies responses due to the proximity of the computing facilities to the point of attachment.
The purpose of this NetApp is to take the opportunity of these new features and to allow a smooth transition from one access technology to the other. Moreover, the flexibility of C-ITS services deployment when using RSU digital twin can be overcoming many of the interoperability challenges for border-crossing scenarios and accelerates C-V2X deployments with a hybrid architecture. This is the reason we are proposing to develop virtual RSUs (vRSUs).

- **NetApp high level infrastructure**

Figure 14 shows the high-level infrastructure of the virtual RoadSide Unit.

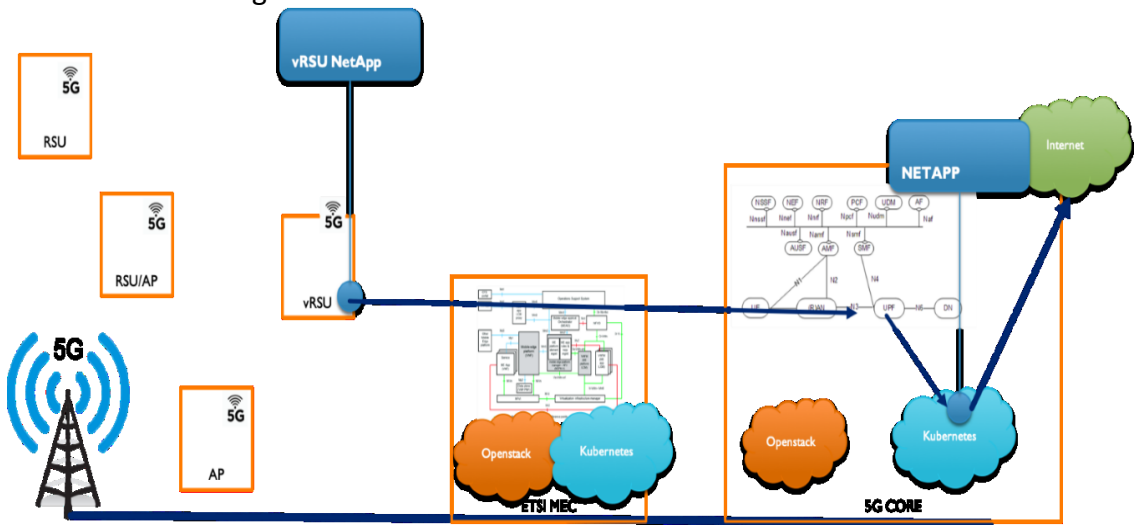


Figure 14 Virtual RoadSide Unit provisioning NetApp Infrastructure

The vRSUs performs the heavy data fusion and security operations a bit further up in the network (but still not in the cloud) in a vRSU behaving exactly like a set of physical RSUs along the roadside and serving a large area. There could be two deployment modes of vRSUs:

- deploying much simpler Layer2 (L2) / Layer3 (L3) communication relays connected to sensors and other specialized equipment alongside the road instead of physical RSUwhen these are needed locally. These relays would be connected to the vRSUs using 5G connection (or optic fiber or any other access technology) and they would communicate with vehicles using a diversity of access technologies (including ITS-G5, LTE-V2X and of course advanced forms of local 5G communications). This would ensure interoperability with systems already deployed and also would help to accommodate easily various forthcoming deployment strategies.
- in areas not equipped with communication relays, vehicles would connect directly to the vRSUs using 5G.

- **NetApp KPIs**

Table 7 vRSU NetApp KPIs

Generic KPI name	Metric Indicator (How)	KPI value	KPI unit
Latency (at relays, if applicable)	Maximum end-to-end transmission time between relays and vRSUs	30	Milliseconds
Latency (at road users)	Maximum end-to-end transmission time for time-critical road-safety messages transmitted between road users and vRSUs (directly, or through relays)	30	Milliseconds
Service downtime for time-critical road safety services	Ratio of time the vRSU is not responding	0.000001	%
Service downtime for other services	Ratio of time the vRSU is not responding	1	%

Table 8 vRSU NetApp NEST

vRSU NetApp NEST	
Area of service	SP, PT, UK, RO (AUTO-V use case)
Area of service: Region specification	Murcia, Aveiro, Bristol, Bucharest
Downlink maximum throughput per UE	-
Uplink maximum throughput per UE	-
Isolation level	Virtual resources isolation
V2X communication mode	NR-V2X
Slice quality of service parameters: 3GPP QoS Identifier (5QI)	84 (for time-critical road safety services)
Maximum Packet Loss Rate	1%
Supported device velocity	250 km/h

- **Overall integration needs**

Packaging Info (VM, container, type, etc.): Several RSUs will be virtualized on the same equipment, distributed database.
Existing Healthcheck or Lifecycle (deployment status) Hooks or APIs: No.
Dependencies of the 5G System (requires slicing, core functionality, etc.): It requires at least the availability of LTE-V2X in the edge network, until 5G NR-V2X is fully specified and available

in radio equipment. For operational deployment, it will require 5G slices with low latency and service availability guarantees, catering for mission critical safety services.
How is it operated (and does it require manual interventions): vRSUs are deployed in the edge of the network and cover a large geographic area (e.g. a portion of a road in a rural environment). On one side, they interact with mobile equipment (embedded in vehicles or possibly nomadic devices) whilst on the other side interact with traffic control centers or other types of control centers, such as fleet management, parking management, or any type of service platform. The exchange of data between UE and the vRSU must comply with C-ITS standards (data formats, communication protocols, security, etc.) either using an API to be developed and proposed by YoGoKo or using an API developed by the users themselves. Once the infrastructure is in place, any type of service (able to exploit data transmitted between vehicles and the roadside) could be developed either to demonstrate the benefit of virtual RSU for existing C-ITS services or to demonstrate how new C-ITS services can be developed.
Dependencies (does it expose or consume services from/to other NetApps): Yes, e.g. with the Privacy Analyzer NetApp for analysis of messages exchanged in the relevant Automotive use-cases.

2.3 NetApp 3: ITS station NetApp

- **Description of demonstration environment**

Instead of providing some of the functionalities of the ITS station directly in physical elements (vehicle, roadside equipment), in particular data provided by sensors (e.g. magnetic loop in case roadside, or radar in the case of vehicle) or geo-localized data about the surrounding environment registered in a LDM, such data could be provided directly in the cloud. This leads towards the development of a generic ITS station NetApp in the cloud that provides C-ITS services alike if the data was directly available in the vehicle or roadside equipment.
This NetApp developed by YoGoKo will contain the minimum ITS station facilities layer services independently of the communication protocols so that it would allow users to develop new applications and services for the Automotive and PPDR verticals and ensure that the developments are compatible with C-ITS standards.

- **NetApp high level infrastructure**

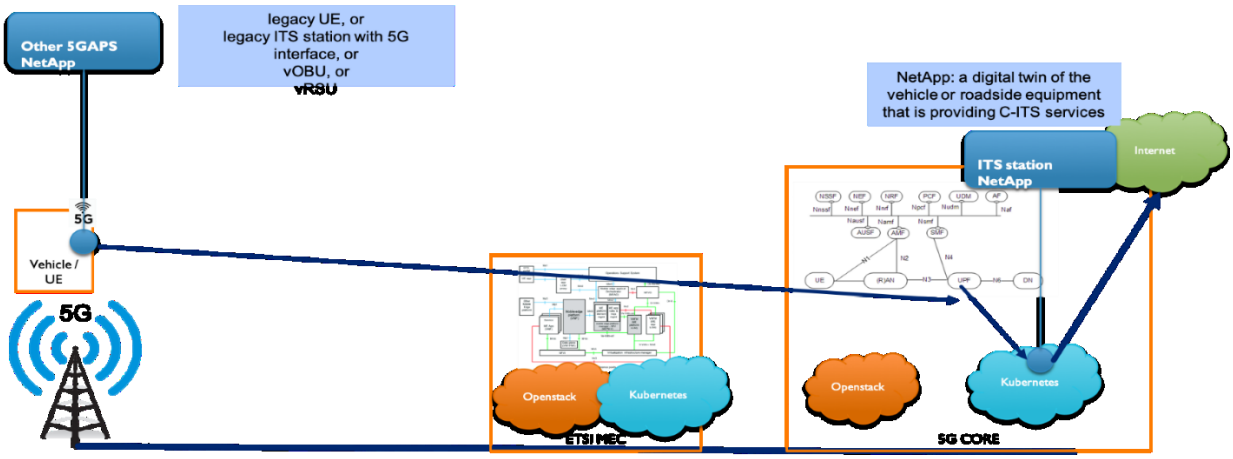


Figure 15 ITS NetApp infrastructure

Table 9 ITS NetApp KPIs

Generic KPI name	Metric Indicator (How)	KPI value	KPI unit
NetApp deployment time at the edge	The app is sending information over a communication channel and receiving the control packets from the cloud (requires the cloud entity to be up and running)	<5	minutes
NetApp deployment time in the cloud	The app is waiting for connection – reporting its status over rest API. Able to connect to remote vehicle.	<5	minutes
Frames loss	Amount of video frames received out of required	<1 / 100.000	frames
Frame latency	Maximal latency of the frames received by the cloud entity	<30	ms
Frame decoding latency	Maximal latency for decoding frames once received by the cloud entity	<15	ms
Service availability	Time percentage the NetApp is online for time-critical road safety services	>99,99999	%

Table 10 ITS station NetApp NEST

ITS station NetApp NEST	
Area of service	SP, PT, UK, RO (AUTO-V use case)
Area of service: Region specification	Murcia, Aveiro, Bristol, Bucharest
Downlink maximum throughput per UE	100,000 kbps
Uplink maximum throughput per UE	1,000 kbps
Isolation level	Virtual resources isolation
Slice quality of service parameters: 3GPP QoS Identifier (5QI)	84 (for time-critical road safety services), 9 (other services)
Maximum Packet Loss Rate	1%
Supported device velocity	250 km/h

- **Overall integration needs**

Packaging Info (VM, container, type, etc.): Several ITS stations may be virtualized on the same equipment, each serving vehicles physically present in a given area or for the purpose of distinguishing time critical road safety services from other services.
Existing Healthcheck or Lifecycle (deployment status) Hooks or APIs: No.
Dependencies of the 5G System (requires slicing, core functionality, etc.): It requires 5G slices with low latency and service availability guarantees, catering for mission-critical safety services.

How is it operated (and does it require manual interventions): ITS stations are deployed in the cloud and cover vehicles physically present in a given geographic area (e.g. a portion of a road in a rural environment). ITS stations interact with mobile equipment (embedded in vehicles or possibly nomadic devices). The exchange of data between UE and the ITS station must comply with C-ITS standards (data formats, communication protocols, security, etc.) either using an API to be developed and proposed by YoGoKo or using an API developed by the users themselves.
Dependencies (does it expose or consume services from/to other NetApps): Yes, Efficient MEC handover NetApp, vOBU NetApp, vRSU NetApp and Multi-domain Migration NetApp.

2.4 NetApp 4: Multi-domain Migration NetApp

- **Description of demonstration environment**

Solutions that provide virtual counterparts in the MEC are very handy in vehicular scenarios. The main problem that arises is the high mobility of vehicles and how to maintain the connectivity of their OBUs with their correspondent virtual surrogates when switching between different network domains. This is the case of cross-border areas where vehicles change between operators and domains. The Mobile Device Virtualization through State Transfer (MIGRATE) proposal[61] solved this issue betting on the dynamic instantiation of new virtual counterparts on demand in the new domain using the same configuration parameters of the former virtual surrogate, transferring state to the new instantiation and finally updating data paths using Software-Defined Networking (SDN) functions.

- **NetApp high level infrastructure**

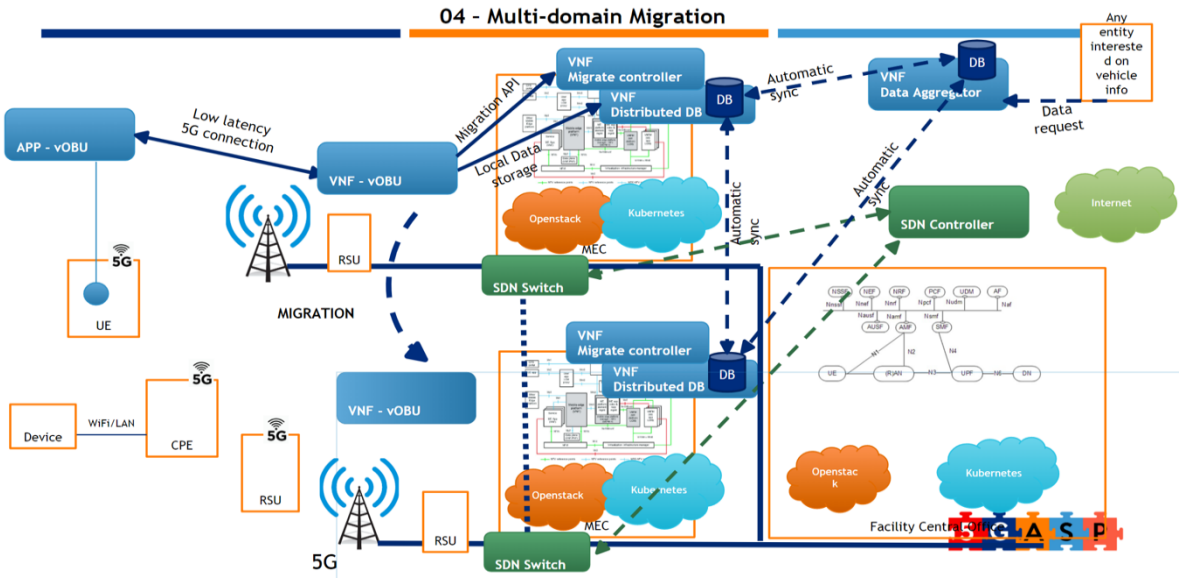


Figure 16 Multi-domain Migration NetApp

OdinS presents a supporting solution that provides interdomain mobility capabilities to the vOBUs introduced before, and in a more generic view, to any NetApp that requires it. This NetApp (*Figure 16*) enables the vOBUs to be migrated to the closest MEC to the real vehicle, reaching the low latency requirements that characterize vehicular applications. This migration procedure ensures that the OBU will maintain connectivity with its virtual counterpart in the former domain while the new virtual instantiation is getting ready with the same

configuration and state. Once it is ready, the data paths are updated to start using the new one without any packet loss.

- **NetApp KPIs**

Table 11 Multi-domain Migration NetApp KPIs

Multi-domain Migration NetApp KPIs			
Generic KPI name	**Metric Indicator (How)**	**KPI value**	**KPI unit**
Migration time	Time needed since the last message sent on the original network is processed and the first message on the visited network is processed	<5	minutes
Transaction speed	Each message sent from a OBU needs to be redirected to the vOBU	500	miliseconds

Table 12 Multi-domain NETAPP's NEST

Multi-domain NETAPP's NEST	
Area of service	SP, PT, UK, RO (AUTO-V use case)
Area of service: Region specification	Murcia, Aveiro, Bristol, Bucharest
Downlink maximum throughput per UE	100 Mbps
Uplink maximum throughput per UE	100 Mbps
Isolation level	3: Tenant/service isolation
V2X communication mode	YES-NR
Slice quality of service parameters: 3GPP 5QI	9
Maximum Packet Loss Rate	1%
Supported Device Velocity	3: Vehicular: 10 km/h to 120 km/h

- **Overall integration needs**

Packaging Info (VM, container, type, etc.): Network Service. Multiple VMs including vOBUs and distributed database.
Existing Healthcheck or Lifecycle (deployment status) Hooks or APIs: No.
Dependencies of the 5G System (requires slicing, core functionality, etc.): Requires OpenFlow as part of the datapath for transparent migration.
How is it operated (and does it require manual interventions): Requires previous mapping between OpenFlow ports and VIM deployment. Protocol used: IPv6 (CoAP).
Dependencies (does it expose or consume services from/to other NetApps): vOBU - NetApp 1.

2.5 NetApp 5: Vehicle-to-Cloud Real-Time Communication (V2C R2C) NetApp

- **Description of demonstration environment**

Autonomous vehicles are usually equipped with multiple 4K cameras and sensors such as Light Detection and Ranging (LIDAR) and Radio Detection and Ranging (RADAR) sensors. The latter generate a huge amount of data to be transferred. Moreover, as autonomous vehicle technologies continue to evolve, the data generated grows exponentially. To enable the vehicle to be highly operational, there are remote/cloud services such as teleoperation, remote driving and vehicle remote assistance that use the generated data to both estimate the status of the vehicle and to build an image of its surrounding. Such services usually send back to the vehicle specific control commands and instructions to be executed instantaneously. Naturally, the success of these services depends on the involved communication latency and reliability guarantees.

- **NetApp high level infrastructure**

The V2C R2C NetApp enables the vehicle to send and receive data at real-time (*Figure 17*). The NetApp is application-aware to ensure optimized data transmission based on the content being sent (e.g. real-time video or voice have higher priority than telemetry data). Since the transmission of the HD video generated by the cameras must be realized at real-time (i.e. buffering and retransmissions cannot be used) the NetApp uses techniques such as Forward-Error-Correction (FEC), channel bonding and dynamic encoding bitrate to assure fast video delivery while maintaining maximum video quality. In addition, when multiple channels exist, the NetApp will prioritize the data delivered to the vehicle based on the performance of the channels. *Figure 17* illustrates the V2C R2C NetApp architecture.

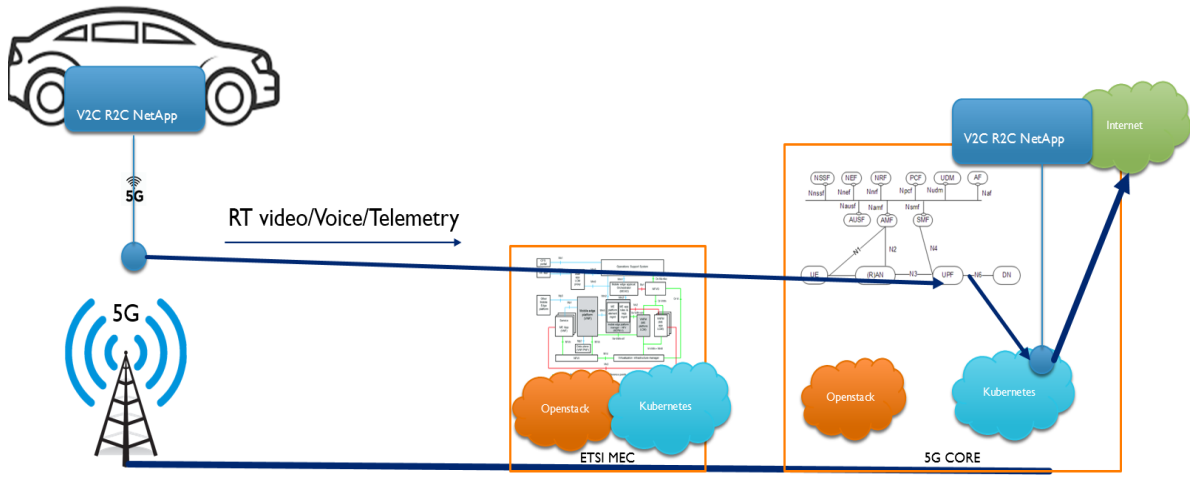


Figure 17 Vehicle-to-Cloud Real-Time Communication (V2C R2C) NetApp

- **NetApp KPIs**

Table 13 V2C R2C NetApp KPIs

Generic KPI name	Metric Indicator (How)	KPI value	KPI unit
NetApp deployment time at the edge	The app is sending information over a communication channel and receiving the control packets from the cloud (requires the cloud entity to be up and running)	<5	minutes
NetApp deployment time in the cloud	The app is waiting for connection – reporting it's status over rest API. Able to connect to remote vehicle.	<5	minutes
Frames loss	Amount of video frames received out of required	<1 / 100.000	frames
Frame latency	Maximal latency of the frames received by the cloud entity	<50	ms
Service availability	Time percentage the NetApp is online	>99	%

Table 14 V2C R2C NetApp KPIs

V2C R2C NetApp NSD	
Number of Services (NSDs)	2
Number of total VNFs	3
Dependencies of the 5G System	One slice URLLC and one slice WB (WideBand)
How is it operated	Automated deployment and provisioning
Dependencies	None from other NetApps

Table 15 Cloud (NSD)

Cloud (NSD)	
Number of total VNFs	1
Packaging Info:	CNF (Cloud-Native Network Function)
Placement (latency from-to)	Latency from UE: max 20ms
Internet access	Limited functionality without internet (maps)
Resource req (flavour cores/mem/hd)	n/a
Delivery model (Vm Image, Container (dockerhub, else?))	Docker
Ingress bandwidth (BW)	10-100 Mbits/s
Egress BW	0.1-1.0 Mbits/s

Table 16 Vehicle (NSD)

Vechicle (NSD)	
Number of total VNFs	2
Packaging Info:	CNF
Placement (latency from-to)	Latency from UE: max. 100ms
Internet access	Limited functionality without internet (maps)
Resource req (flavour cores/mem/hd)	Dedicated encoding accelerators (jetson nvidia)
Delivery model (Vm Image, Container (dockerhub, else?))	Container or VM image
Ingress BW	0.1 – 1.0 Mbps
Egress BW	10-100Mbps

Table 17 V2C R2C NEST

V2C R2C NEST	
Area of service	EU
Area of service: Region specification	EU
Downlink maximum throughput per UE	100000 kbps
Uplink maximum throughput per UE	1000 kbps
Isolation level	Virtual resources isolation
V2X communication mode	YES-NR
Slice quality of service parameters: 3GPP 5QI	9
Supported device velocity	<120 km/h

- **Overall integration needs**

Packaging Info (VM, container, type, etc.): Currently docker is used.
Existing Healthcheck or Lifecycle (deployment status) Hooks or APIs: Watchdog on a module since the application is mission critical.
Dependencies of the 5G System (requires slicing, core functionality, etc.): No clear dependency – the app is working over any communication technology with enough BW and latency low enough to operate.
How is it operated (and does it require manual interventions): NetApp is working in mode of the Vehicle client. This mode provides an efficient use of the communication interfaces to the server by analyzing the interfaces capabilities, according to it compresses and send the data at the most efficient and reliable path.
Dependencies (does it expose or consume services from/to other Netapps): Currently it is not interconnected to other NetApps, however it can be seen that a privacy-related NetApp such

as Privacy Analyzer might be interworking with this NetApp. The Vehicle Route Optimizer seems to be relevant as well but it may require some additional research to check the benefits of connection between them. In both cases the connection will be done through the standard API.
Extra requirements: the node station should be based on an Nvidia GPU.

2.6 NetApp 6: Remote Human Driving NetApp - Teleoperation for assisting vehicles in complex situations

- **Description of demonstration environment**

There is an industry consensus today that autonomous vehicles will need help in making decisions, especially in unusual, dangerous situations that can happen on the road and may require violating the traffic laws (e.g. crossing double yellow lines). For these cases, the industry has started to adopt teleoperation/remote driving solutions that enable a remote human operator to monitor and take control over the car if needed.
DriveU and BLB present a solution that enables a remote operator to take full/partial control over an autonomous vehicle in unusual/dangerous situations that can happen on the road (e.g. let an autonomous vehicle crossing double yellow lines). Ensuring safe teleoperation and human remote assistance entails reliable transmission of high-quality real-time video with minimum latency.

- **NetApp high level infrastructure**

A virtual vehicle instance is equipped with one or more 5G modems and a software (SW) module that enables the transmission of HD video to the tele-operation centre (*Figure 18*).

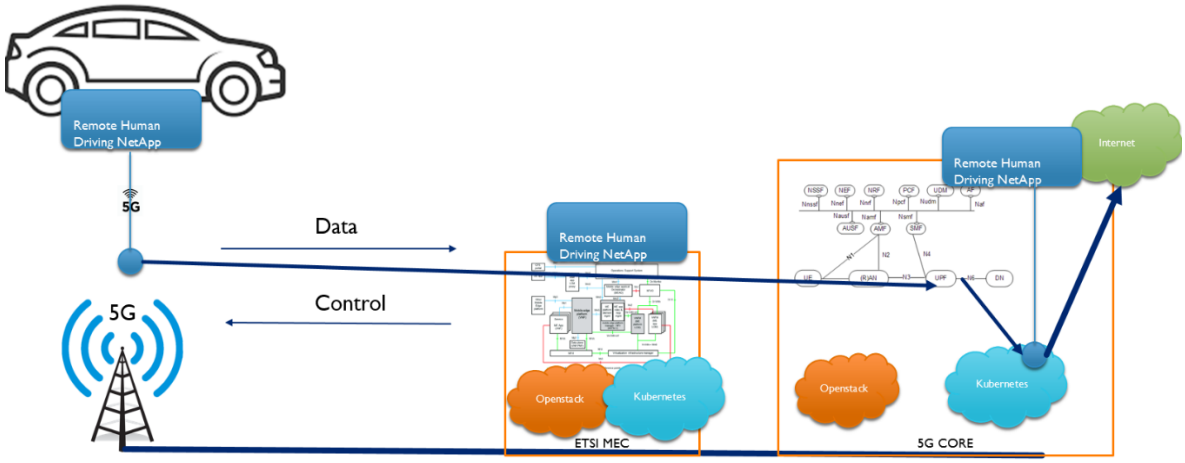


Figure 18 Remote Human Driving NetApp - Teleoperation for assisting vehicles in complex situations

- **NetApp KPIs**

Table 18 Remote Human Driving NetApp – Teleoperation KPIs

Generic KPI name	Metric Indicator (How)	KPI value	KPI unit
NetApp deployment time at the edge	The app is sending information over a communication channel and receiving the control packets from the cloud (requires the cloud entity to be up and running)	<5	minutes
NetApp deployment time in the cloud	The app is subscribed to the relay (cloud entity) and sending reports connection	<5	minutes
Contineous control messages	Amount of control messages received out of sent to the vehicle	<1 / 100.000	messages
Contorl latency	Maximal latency of the messages received by the cloud entity	<5	ms
Frame decoding latency	Latency from the receiption of the frame packets by a control node and untill it is being displayed to the controller	<15	ms
Service availability	Time percentage the NetApp is online analyzing UEs' streaming data for privacy issues	>99	%

Table 19 Remote Human Driving NetApp NSD

Remote Human Driving NetApp NSD	
Number of Services (NSDs)	2
Number of total VNFs	3
Dependencies of the 5G System	One slice URLLC and one slice WB
How is it operated	Automated deployment and provisioning
Dependencies	None from other netapps

Table 20 Cloud (NSD)

Cloud (NSD)	
Number of total VNFs	1
Packaging Info:	CNF
Placement (latency from-to)	Latency from UE: max 20ms
Internet access	Limited functionality without internet (maps)
Resource req (flavour cores/mem/hd)	n/a
Delivery model (Vm Image, Container (dockerhub, else?))	Docker
Ingress BW	10-100 Mbits/s
Egress BW	0.1-1.0 Mbits/s

Table 21 Control center (NSD)

Control center (NSD)	
Number of total VNFs	2
Packaging Info:	CNF
Placement (latency from-to)	Latency from UE: max 100ms
Internet access	Limited functionality without internet (maps)
Resource req (flavour cores/mem/hd)	Nvidia GPU
Delivery model (Vm Image, Container (dockerhub, else?))	Container or VM image
Ingress BW	10-100Mbps
Egress BW	0.1 – 1.0 Mbps

Table 22 Remote Human Driving NetApp NEST

Remote Human Driving NetApp NEST	
Area of service	GR
Area of service: Region specification	Patras
Downlink maximum throughput per UE	100000 kbps
Uplink maximum throughput per UE	1000 kbps
Isolation level	Virtual resources isolation
V2X communication mode	YES-NR
Slice quality of service parameters: 3GPP 5QI	9
Supported device velocity	120 km/h

- **Overall integration needs**

Packaging Info (VM, container, type, etc.): Currently it is packaged as docker containers.
Existing Healthcheck or Lifecycle (deployment status) Hooks or APIs: Watchdog on a module since the application is mission critical.
Dependencies of the 5G System (requires slicing, core functionality, etc.): No clear dependency – the app is working over any communication technology with enough BW and latency low enough to operate.
How is it operated (and does it require manual interventions): NetApp is working in mode of the Relay and Remote operator node. In this mode an error correction server, low latency processing service located at a customer premises, responsible to interconnect the remote operator and the operated vehicle and decompresses the data from the vehicle, send the operation commands to the vehicle.

Dependencies (does it expose or consume services from/to other netapps): Currently it is not interconnected with other NetApps, however it can be seen that a security NetApp might be connected. The Vehicle Route Optimizer seems to be relevant as well but it may require some additional research to check the benefits of connection between them. In both cases the connection will be done through the standard API.
Extra requirements: the node station should be based on an Nvidia GPU.

2.7 NetApp 7: Efficient MEC handover NetApp

- **Description of demonstration environment**

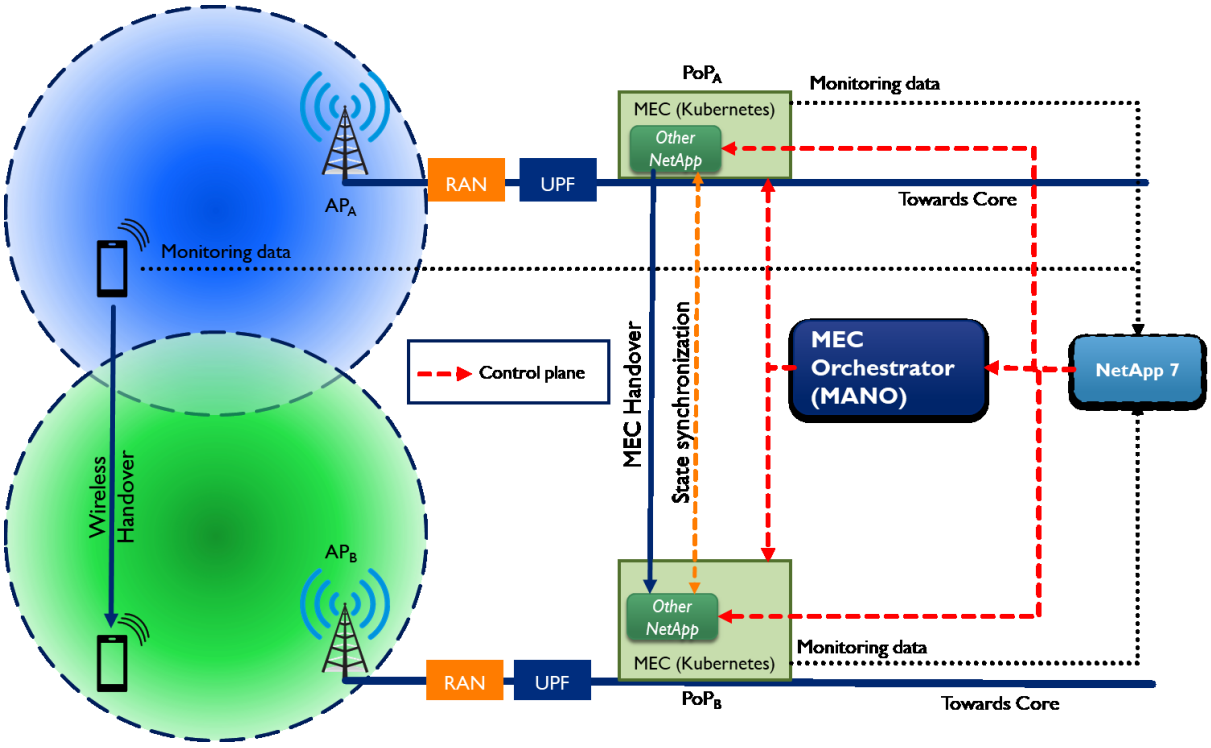


Figure 19 Efficient MEC Handover scenario

In *Figure 19* is depicted the scenario targeted by the NetApp based on the Netapp infrastructure.
With the advent of 5G networks, MEC is becoming more relevant, allowing applications to be hosted at the edge for low latency services[62]. However, mobile networks need to maintain service availability at an acceptable level i.e., the Quality of Experience (QoE) perceived by the user during mobility of its UE which may entail a wireless Handover (HO) between multiple radio cells. This is highly relevant in automotive use-cases such as the ones targeted by NetApps 1, 5, 6 and 7 where a vehicle may be moving between different radio cells, and the vehicle needs to be continually served by an edge application even after a HO event. Consider this scenario in which a UE is being served by an edge application in a MEC Point of Presence (PoP) A while being in range of a particular radio cell as shown in *Figure 19*. However, with UE mobility, wireless handover to another cell may become imminent; and as shown in *Figure*

19, the UE may be served by the edge app in MEC PoP B which is present in the new radio cell. There may be two ways to serve the UE here after HO:

- Option 1: Maintain the connection of the UE with the edge application in the MEC PoP A.
- Option 2: We refer this as MEC HO. It requires hosting the edge application in the current/local MEC host: PoP B. This could be done in further two ways:
  a) Migrate the edge application in MEC PoP A to MEC PoP B;
  b) Deploy a new instance of the edge application on MEC PoP B, and migrate the state of edge application from MEC PoP A to MEC PoP B

Option 1 may increase the latency between UE and the edge application upon handover events beyond the acceptable level, i.e. effectively causing a user-perceivable service downtime. Option 2 overcomes the latency issue by hosting the edge application in the local MEC platform (PoP B); however, it requires the application to have the up-to-date relevant application state, same as before the wireless mobility. To reduce the perceived downtime by the user during wireless mobility, the MEC mobility must be synchronous with the wireless HO. Moreover, there may be other factors which influence the MEC mobility not necessarily coupled with wireless mobility; these may include the reliability, network and compute resource availability restrictions at one MEC PoP which may necessitate moving the edge application to another MEC PoP.

Our NetApp, NetApp 7, targets to enable Option 2, by utilising ML-based techniques, based on UE radio parameters input, monitoring parameters of the compute servers such as CPU, RAM and others and network-related parameters such as latency and network capacity. Based on the former, the NetApp may predict a wireless HO, network and compute resource availability, or some other relevant QoS or reliability metric. This prediction can then be used to prepare or perform a MEC HO between the current and future serving MEC PoPs to improve or maintain the user QoE.

The Efficient MEC handover NetApp aims to support other automotive-based NetApps (namely, the "*edge apps*") in the 5GASP project. Essentially, other NetApps' administrators are expected to provide their required KPIs affecting or related to the QoE of the NetApp user. The latter KPIs will be the focus of the Efficient MEC handover NetApp to perform a MEC HO after predicting key parameters associated with the KPIs to improve or maintain QoE.

- **Overall integration needs**

Here we describe some high-level requirements along with the current status of NetApp 7.

1. **Edge application state synchronization**: As mentioned for option 2, NetApps leveraging NetAPP 7 must have a mechanism to synchronize their state among their edge application replicas. They also must have a mechanism to establish and update the state synchronization frequency among their NetApp replicas based on predictions by ML models in NetApp 7 explained subsequently.
2. **Maintaining UE-MEC PoP connectivity**: UE needs to be continually served by an edge application after wireless, or even MEC HO.

3. **Capability to request state synchronisation update**: NetApp 7 must be provided with an interface to the edge application that allows to request or trigger the update of state synchronization frequency by the edge NetApp (point 1 above).
4. **Access to MEC orchestrator**: NetApp 7 needs to have access to the MEC orchestrator to deploy new instances of edge application or scale up/down resources appropriately.
5. **Input parameters for training, testing and runtime**: Based on other NetApps KPIs, NetApp 7 tries to maintain the QoE/QoS of the service experienced by user. In the current status of NetApp 7, ML models predict the Time to wireless HO (TTH) and the Physical Cell ID (PCI), i.e. the radio cell that the UE will connect to, triggering appropriate messages to other NetApps to update state synchronization frequency. In the future, it is intended to predict an imperative MEC HO due to resource constraints in the MEC platform or some other KPI as required by other NetApps. This requires inputs from the system for ML model training and test purposes, as well as during model runtime for taking ML-based NetApp 7 decisions:
    - Fine time-granularity monitoring UE radio parameters (Reference Signal Received Power (RSRP) at the minimum and with a granularity as close as possible to a level of 10s of milliseconds), currently used by NetApp;
    - Compute resource server parameters at the MEC server (CPU, RAM, etc.);
    - Network parameters (current throughput, latency).

    Currently, this NetApp has been tested with ML models (Long Short-Term Memory architecture and clustering models) that predict handover for one user based on RSRP and Global Positioning System (GPS) values, where a custom video streaming app is tested strongly coupled with this NetApp 7[63]. The design of the API that will expose the handover prediction needs to be finalized.
6. **Location of NetApp 7**: This NetApp can be hosted in various locations in the testbed depending on the requirements of other NetApps. Currently, this NetApp has been tested with only one replica; however, for fast ML processing, it may be required to have replicas of NetApp 7 at each MEC PoP for quick decisions about MEC handover or edge application horizontal scaling.
7. **Replicas of other Edge NetApps**: NetApp 7 requires multiple replicas of other Edge NetApps to be deployed a-priori, such that NetApp 7 facilitates Edge NetApp state synchronization. Moreover, NetApp 7 needs to be supplied with the reachability information (IP address, port numbers) of other Edge NetApps.
8. **Radio Cell ID to MEC PoP mapping:** NetApp 7 requires the knowledge of the Radio cell ID currently serving a UE and its mapping to the MEC PoP. This allows the NetApp 7 to know the location of the other Edge NetApp on a MEC PoP currently serving the UE, as well as allowing to ingest monitoring data from the relevant MEC PoP to predict KPIs as needed.

- **NetApps KPIs**

Edge NetApp KPIs

Efficient MEC Handover NetApp is fundamentally different from standard edge NetApps since it provides a system service to other NetApps; thus, existing to maintain other NetApps KPIs. These KPIs may improve if edge NetApps rely on NetApp 7 to predict wireless HO, which causes to increase the state synchronization frequency among their edge replica instances or to predict a scarcity of resources in some MEC PoP causing to instantiate new edge replica instances in other MEC PoPs. An important KPI in service continuity is the perception of zero downtime, which we focus on in one paper[64] and is implemented. Nevertheless, this is related to specific use-cases such as gaming or video streaming, and can be extended to cover KPI needs by other NetApps within the automotive use-case paradigm. Other KPIs which can be considered, with specific measurements coming in at a later stage, and will need to be implemented as part of 5GASP project are:

- maximum allowed latency;
- minimum throughput from the UE to NetApp;
- maximum CPU/RAM utilization in MEC PoPs.

Efficient MEC handover NetApp (NSD)

While currently the NetApp is not packaged as a VNF/CNF and not deployed via MANO, it is intended to be packaged as such during the project. *Table 23* shows some of the intended details about this NetApp. Note that this NetApp may be packaged with other edge NetApps in a combined NSD, instead of an NSD on its own. Moreover, this NetApp even though tested with one instance, may in the future have multiple instances using different ML algorithms/techniques, hosted in different MEC PoPs depending on the other edge NetApps' use-cases. Note that the KPIs with values "n/a" is due to the fact that NetApp7 supports other NetApps KPIs (rendering them enhanced NetApps) and does not have any own KPIs.

Table 23 Efficient MEC Handover NetApp NSD

Efficient MEC Handover NetApp NSD	
Number of total VNFs	1
Packaging Info	VNF/CNF
Placement (latency from-to)	Latency from UE: max 10ms
Internet access	No
Maximum allowed latency	n/a
Minimum throughput from UE to NetApp	n/a
Max CPU/RAM utilization in MEC PoPs	n/a
Resource req (flavour cores/mem/hd)	4 Cores, 16GB Memory, 100GB storage
Delivery model (Vm Image, Container (dockerhub))	Still under consideration

Efficient MEC handover NEST

We present the NEST template filled in for this NetApp in *Table 24*. We do not fill in the mission critical support, as it is dependant on the other edge NetApps that the NetApp 7 is supporting. Note that we have an alternative to the performance monitoring support from

the Slice provider or the operator, as we may rely on receiving monitoring parameters directly from the UE or MEC servers. Moreover, this NetApp uses the monitoring parameters to predict performance, hence the performance prediction from the Slice provider/operator is also optional. The supported device velocity for now is related to a pedestrian user, which may be improved for automotive use-cases during this project.

Table 24 Efficient MEC Handover NEST

Efficient MEC Handover NEST	
Area of service	GB
Area of service: Region specification	Bristol
Isolation level	Virtual resources isolation
Downlink maximum throughput per UE	n/a
Uplink maximum throughput per UE	n/a
Performance monitoring	Throughput, latency, UE radio parameters
Performance monitoring: monitoring sample frequency	Per tens of ms
Performance prediction	Throughput, latency, and other edge NetApp KPIs
Performance prediction: frequency	Per tens of ms
Positioning support	Cell ID
Positioning support: frequency	Per tens of ms
Slice quality of service parameters: 3GPP 5QI	81, 82, 83
Supported device velocity	5 to 10 km/h

The 3GPP 5QI parameters are reproduced in *Table 25*[65] and assume all the delay critical use cases supporting edge applications such as remote control or Intelligent Transport Systems which cover many of the automotive use-cases.

Table 25 3GPP 5QI values: 81, 82 and 83

5QI value	Resource Type	Default Priority Level	Packet Delay Budget	Packet Error Rate	Default Maximum Data Burst Volume	Default Averaging Window	Example Services
81	Delay Critical GBR	11	5 ms	10^{-5}	160 B	2000 ms	Remote control
82		12	10 ms	10^{-5}	320 B	2000 ms	Intelligent transport systems
83		13	20 ms	10^{-5}	640 B	2000 ms	Intelligent transport systems

2.8 NetApp 8: PrivacyAnalyzer NetApp

- **Description of demonstration environment**

PrivacyAnalyzer is a streaming analytics Software as a Service (SaaS) for detecting privacy leaks in network communications involving Internet of Things (IoT) devices, built upon our commercial streaming analytics platform, Qiqbus. PrivacyAnalyzer offers an advanced service for testing innovative IoT applications and/or services. PrivacyAnalyser has been designed as an extension to the Qiqbus platform enhancing the latter with the unique functionality to addresses a large class of use cases where personal data must be tested for compliance with privacy requirements, before their corresponding data-driven IoT/5G/6G services can successfully penetrate the market, especially with the continuous pressure from the citizens to protect their privacy and the related legislative environments, such as General Data Protection Regulation (GDPR). The motivation behind PrivacyAnalyser is indeed the problem of confidential information disclosure, one of the most alarming privacy threats in the domain of IoT, that has not been instantiated nor implemented in real IoT/5G/6G testing environments. That is, existing methods either assume static data, which makes them unsuited for real IoT/5G/6G environments or focus on the prevention of other privacy threats. Therefore, PrivacyAnalyser has been designed and implemented as a framework to help users, such as SMEs and start-ups to assess the privacy strength of their applications (e.g. their NetApps) and/or services against confidential information disclosure. To offer such functionalities, we developed methods based on Machine Learning Pattern matching, techniques applicable to high volumes of streaming data and web-based visualisation. The initial version of some methods was initially implemented as a Proof of Concept (PoC) in the scope of the F-Interop Open Call project. After self-investement of funds by Lamda Networks, PrivacyAnalyzer was reworked in order to become a commercial SaaS, tested with various IoT devices from major manufacturers. At the technical level PrivacyAnalyzer is an online SaaS tool which enables end-users to assess the privacy strength of their applications and/or services against confidential information disclosure. PrivacyAnalyzer can identify faulty or malicious behaviour either due to software bugs that lead to excessive Personal Identifiable Information (PII) leaks, or due to privacy leaks that derive by the fact that a device has been hacked. In these scenarios, PII may be disseminated at any stage. Thus, Value Proposition of PrivacyAnalyzer is formed around its capability to alert the IoT/5G/6G integrators/service providers and end-users regarding situations where PII leaks are detected. In turn, this helps undertaking the relevant corrective actions to fix the software problems which cause the privacy leaks.

Overall, PrivacyAnalyser provides:

- automatic detection and classification of confidential data from streaming data collected from networked devices;
- evaluation of the level of privacy protection offered by encryption, de-identification, and anonymisation;
- option for users to express their preferences, regarding information that is deemed as confidential, through privacy policies;
- visualisation of the outcomes of the privacy tests using intuitive and informative User Interfaces (UIs).

- **PrivacyAnalyzer's high level infrastructure**

The system consists of a sequence of containers interconnected through a cloud native message queuing service as depicted in Figure *20*.
Each incoming message is partitioned based on selected message attributes. Messages from the same source can be processed by the same consumer while maintaining the processing order according to the order of reception. For aggregate operations on message streams i.e. for operations that apply on a messages window with arbitrary sliding interval PySpark is used.

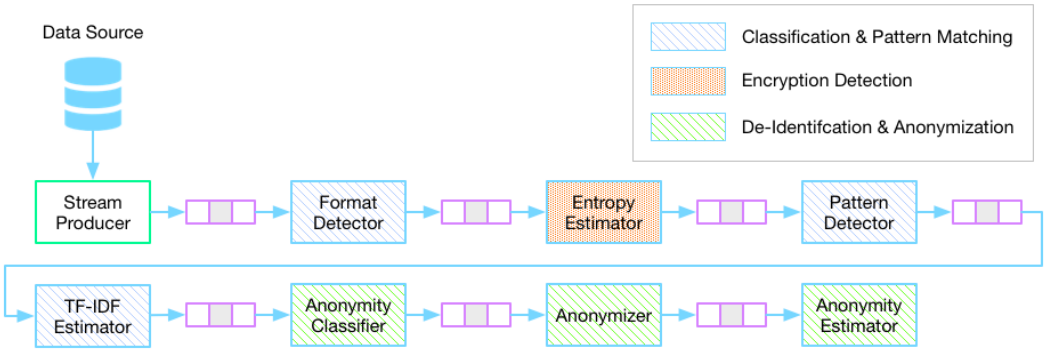


Figure 20 Chain of stream processors

Architectural position of PrivacyAnalyzer within the 5GASP environment
There are thus far considered two main ways to operate PrivacyAnalyzer within the 5GASP environment depending on the need to analyse data streams either at real time or not at real time. This shall be reflected in the following.

- **Architecture flavour I**: Non-real-time (offline or in batch mode) data stream analysis by PrivacyAnalyzer within 5GASP
  Short description: Data streams can be produced by networked devices, such a UE carried by a First Responder (PPDR) or from an RSU or a car (Automotive). In order to analyse the messages originating from such devices (each connected via a dedicated 5G slice) PrivacyAnalyzer operates in the core inside Kubernetes. The NetApp receives the streams, and analyses them for privacy vulnerabilities while a web-UI shows the analysis to the end-user.
  In this flavour, the architectural position of PrivacyAnalyzer within the environment of 5GASP is depicted in *Figure 21*.

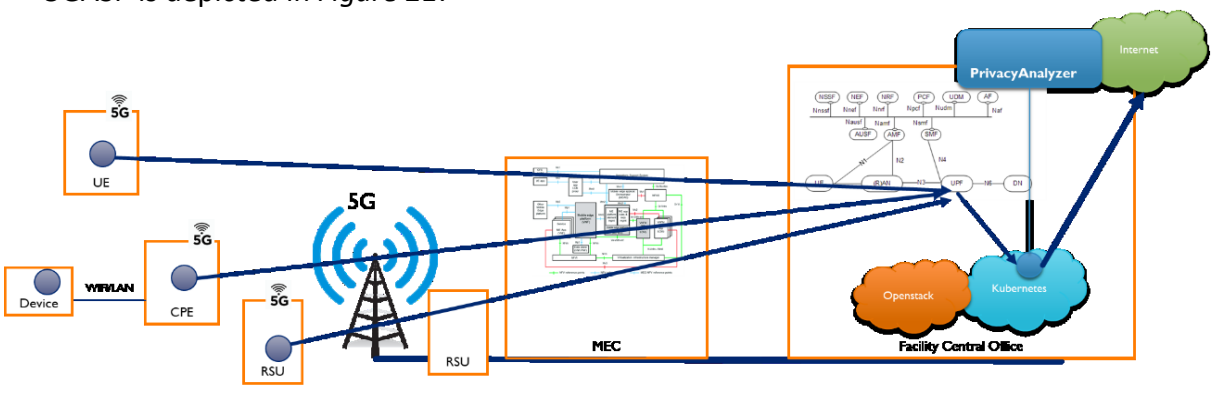


Figure 21 Non-real-time datastream analysis by PrivacyAnalyzer within 5GASP

- **Architecture flavour II**: Near real-time data stream analysis by PrivacyAnalyzer within 5GASP
  Short description: In this case, the PrivacyAnalyzer NetApp operates with the MEC environment (e.g. in the MEC environment of the UoP testbed where we initially plan to deploy and test our NetApp for the 1st year of the project). PrivacyAnalyzer's MEC instances receive the streams by networked devices producing the stream (e.g., a rugged device of a First responder or an RSU or a car) and analyse them for privacy leaks. A web-UI shows the analysis for each device. Furthermore, near real-time alerting (e.g., SMS) is also provided to the end-user.
  In this second flavour, the architectural position of PrivacyAnalyzer within the environment of 5GASP is depicted in *Figure 22*.

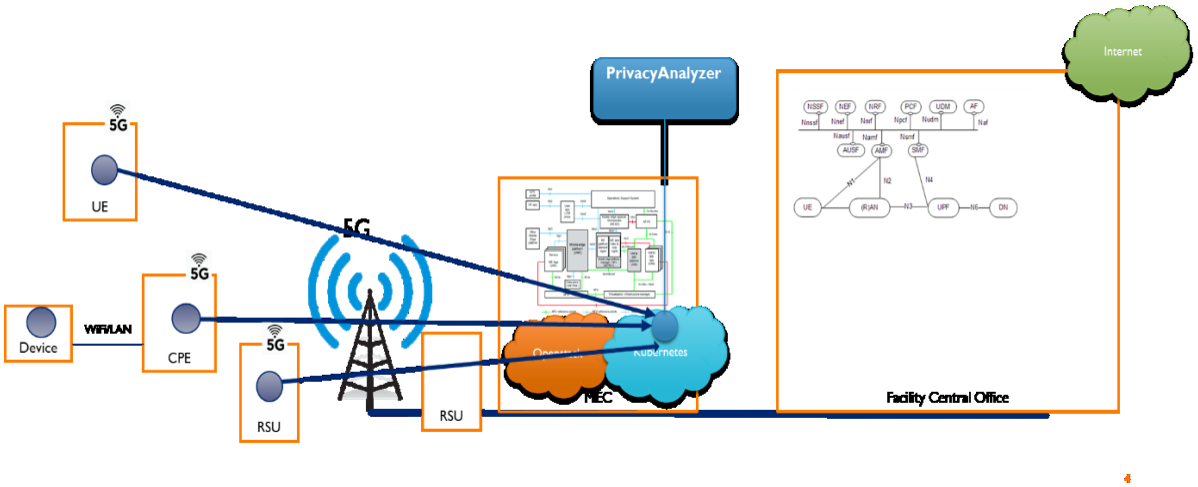


Figure 22 Near real-time datastream analysis by PrivacyAnalyzer within 5GASP

- **NetApp KPIs**

Table 26 PrivacyAnalyzer NetApp KPIs

Generic KPI name	Metric Indicator (How)	KPI value	KPI unit
NetApp deployment time at the edge	Time needed to deploy an instance of PrivacyAnalyzer on a MEC PoP	<3	minutes
Message volume	Number of messages (up to 1KB each log/XML message) analyzed per minute	>=100.000	messages
Packet Loss Ratio	Ratio of packets loss between a UE and PrivacyAnalyzer	<1	%
Service availability	Time percentage the NetApp is online analyzing UEs' streaming data for privacy issues	>99	%

Table 27 PrivacyAnalyzer NetApp NEST

PrivacyAnalyzer NETAPP NEST	
Area of service	EL (PPDR use-case)
Area of service: Region specification	Patras, Aveiro
Availability	High: >95-99.999%
Downlink maximum throughput per UE	(depends on the UE)
Uplink maximum throughput per UE	(depends on the UE)
Isolation level	Virtual resources isolation
Mission critical support	Mission-critical
Mission critical support: Mission-critical capability support	Local control
Mission critical support: Mission-critical service support	Mission Critical Push To-Talk (MCPTT); MCData; MCVideo; MC interworking
Slice quality of service parameters	5QI Value = 9 Packet Delay Budget less than $10*10^{-3}$ Jitter less than $20*10^{-3}$
Maximum Packet Loss Rate	1%
Supported device velocity	Type 1: 10 km/h – Pedestrian

Table 28 PrivacyAnalyzer's NSDs

PrivacyAnalyzer's NSDs	
Number of Services (NSDs)	2
Number of total VNFs	14
Dependencies of the 5G System	2 slices
How is it operated	Automated deployment and provisioning
Dependencies	Dependencies from PPDR UEs for the PPDR use-case None from other NetApps.

Table 29 Batch-mode privacy analysis service NSD

Batch-mode privacy analysis service NSD	
Number of total VNFs	7
Packaging Info:	CNF (Docker containers)
Placement (latency from-to)	
Internet access	Yes

Resource req (flavor cores/mem/hd)	Red Hat Enterprise >=8.3 (8 core/16GB/1TB)
Delivery model (Vm Image, Container (dockerhub, else?))	Containers
Ingress BW	Depends on the UEs involved in the PPDR use case
Egress BW	

Table 30 Near real time privacy analysis service (NSD)

Near real time -mode privacy analysis service (NSD)	
Number of total VNFs	7
Packaging Info:	CNF (Docker containers)
Placement (latency from-to)	Latency from UE: max 100ms
Internet access	YES
Resource req (flavor cores/mem/hd)	Red Hat Enterprise >=8.3 (8 core/8GB/500GB)
Delivery model (Vm Image, Container (dockerhub, else?))	Containers
Ingress BW	Depends on the UEs involved in the PPDR use case
Egress BW	

Note that in its light-weight version, the NetApp consists of the following containers: *encrypt-detector, pattern-detector, anonym-detector, anonymizer, anonym-estimator, input-connector, reporter* as discussed above in the architecture of the NetApp.
In this full version, the previous containers are deployed and orchestrated in a Kubernetes cluster. Scale-out and scale-in operations are in place in order to ensure scalability according to the number and rate of input messages, optionally according to the number of UEs producing the data streams.

- **Overall integration needs**

Existing Healthcheck or Lifecycle (deployment status) Hooks or APIs: No.
Dependencies of the 5G System (requires slicing, core functionality, etc.): 1 Slice in the basic version and per UE slices in the full operating mode, whereby each slice might have its own requirements according to the type of the UE, the messages it produces and the requirements for privacy analysis (e.g. near real-time or in batch mode as we discussed above).
How is it operated (and does it require manual interventions): Automated deployment and provisioning.
Dependencies (does it expose or consume services from/to other NetApps): The NetApp receives as input messages that are produced by UEs which could be used by other NetApps or services (e.g. the PPDR use case envisages UEs carried by First Reponders; messages from these UEs shall be received by the PrivacyAnalyzer NetApp).

2.9 NetApp 9: 5G Isolated Operation for Public Safety NetApp (5G IOPS NetApp)

- **Description of demonstration environment**

5G Isolated Operation for Public Safety NetApp (5G IOPS NetApp) aims at maintaining a level of communication between public safety users, offering them local mission critical services even when the backhaul connectivity to the core network is not fully functional or is disrupted. This operation mode is typically needed in PPDR disaster situations, when the infrastructure is damaged or destroyed, and in the out of coverage emergency cases operated in the rural areas.
5G IOPS NetApp will explore novel connectivity modes between UE, Radio Access Network (RAN) and core network elements, functions of MANO orchestration and cloud-native network function approach to assure automated deployment and self-healing capabilities of the NetApp as proposed in 3GPP Release 15 specifications for the Public Safety services. This NetApp will also be used to showcase international cross-border PPDR operation in multidomain 5G environments.

- **NetAPP high level infrastructure**

The high level architecture of 5G IOPS NetApp is depicted in the *Figure 23*.

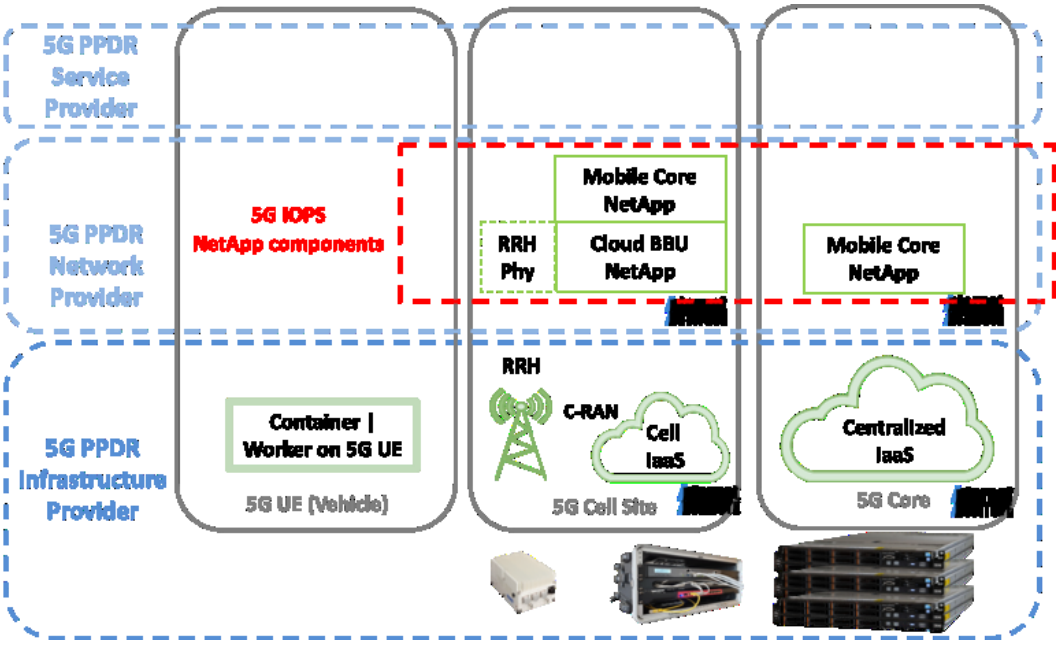


Figure 23 5G IOPS NetApp high level architecture

The NetApp can either be deployed as as standalone solution with all components placed in the edge and provide E2E 5G services directly from the edge (*Figure 24*) or as a distributed NetApp (*Figure 25*) with the components placed in different segments, i.e. 5G IOPS Mobile Core in the different network segment as the 5G IOPS Cloud BBU.
The first options covers various disaster scenarios where mission critical services are needed at the edge and core network services are not available. In this case, the 5G IOPS NetApp acts as a completely standalone 5G Network Provider with PPDR-oriented services.

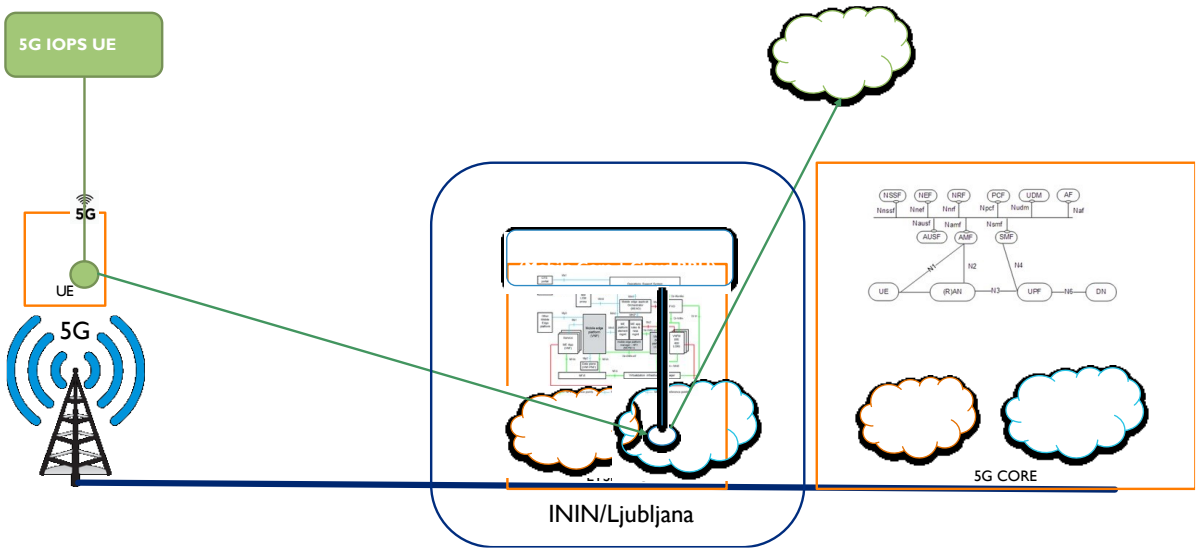


Figure 24 Standalone deployment of 5G IOPS NetApp

The distributed deployment option enables support for cross-border PPDR operation, for example placing 5G IOPS Mobile Core component at UOP site and 5G IOPS Cloud BBU at ININ site.

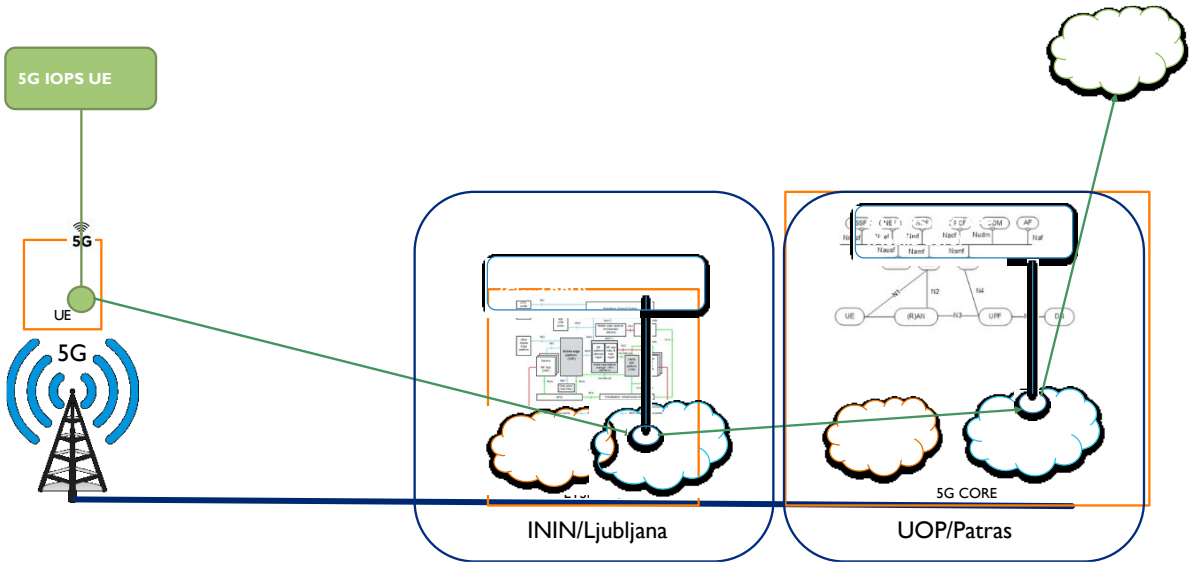


Figure 25 Distributed deployment of 5G IOPS NetApp

- **NetApps KPIs**

Table 31 5G IOPS NetApp KPIs

Generic KPI name	Metric Indicator (How)	KPI value	KPI unit
Instantiation time	Time required to provision and deploy the 5G IOPS NetApp	900	Seconds
Reconfiguration time	Time required to reconfigure the 5G IOPS NetApp (i.e. change the 5G slice)	300	Seconds
RTT	Round trip time measured with qMON monitoring application from the client	<10	Miliseconds

	device connected to 5G IOPS NetApp to the 5G Core		
DNS Reply Time	Time required to get reply from a DNS server measured with qMON monitoring application from the client device connected to 5G IOPS NetApp to the 5G Core	< 20	Miliseconds
L3 Bandwidth	Available IP download and upload bandwidth measured with qMON monitoring application from the client device connected to 5G IOPS NetApp to the 5G Core	>300 (SA mode, 2x2 MIMO, n78 TDD)	Mbps
L4 Bandwidth	Available HTTP/FTP download bandwidth and FTP upload measured with qMON monitoring application from the client device connected to 5G IOPS NetApp to the 5G Core	>250 (SA mode, 2x2 MIMO, n78 TDD)	Mbps
Web	Mean opinion score (MOS) for a selected website(s) measured with qMON monitoring application from the client device connected to 5G IOPS NetApp to the 5G Core	>4	1-5

Table 32 5G IOPS NETAPP's NEST

5G IOPS NETAPP's NEST	
Area of service	SI
Area of service: Region specification	Ljubljana
Isolation level	Virtual resources isolation
Mission critical support	1: mission-critical
Mission critical support: Mission-critical capability support	1: inter-user prioritization
Mission critical support: Mission-critical capability support	3: local control
Mission critical support: Mission-critical service support	2: MCData
Mission critical support: Mission-critical service support	3: MCVideo
Slice quality of service parameters: 3GPP 5QI	69, 70
Maximum Packet Loss Rate	10^-6
Supported device velocity	0-6km/h

NetApp NSDs

The components to be developed and form the 5G IOPS NetApp:

- 5G IOPS Mobile Core: Includes the core 5G network elements such as Access and Mobility Management Function (AMF), Session Management Function (SMF), User Plane Function (UPF) or Home Subscriber Server (HSS) in a single component while providing the configuration options to properly configure 5G elements via the OSM orchestrator
- 5G IOPS Cloud Baseband Unit (BBU): Acts as a gNodeB (gNB) on one side connected to the mobile core (e.g. 5G IOPS Mobile Core) while providing RAN via Common Public Radio Interface (CPRI)-based PCI card and Remote Radio Head (RRH) unit.

Table 33 5G IOPS Mobile Core NSD

5G IOPS Mobile Core NSD	
Number of total VNFs	1
Packaging Info	VNF/CNF
Internet access	Yes
Placement (latency from-to)	Latency from UE: max 10ms
Resource req (flavour cores/mem/hd)	4 Cores, 16GB Memory, 20GB storage
Delivery model (Vm Image, Container (dockerhub))	Container

Table 34 5G IOPS Cloud BBU NSD

5G IOPS Cloud BBU NSD	
Number of total VNFs	1
Packaging Info	VNF/CNF
Internet access	No
Placement (latency from-to)	Latency from UE: max 10ms
Resource req (flavour cores/mem/hd)	4 Cores, 16GB Memory, 20GB storage
Delivery model (Vm Image, Container (dockerhub))	Container

- **Overall integration needs**

Packaging Info: 5G IOPS components as VNF/CNF orchestrated (via MANO/Kubernetes).
Existing Healthcheck or Lifecycle (deployment status) Hooks or APIs: No.
Dependencies of the 5G System: No, for initial deployment, testing and verification. For more advanced PPDR operational scenarios to be done with evolved partners (e.g. University of Patras).
How is it operated: Fully automated deployment (MANO) and orchestration of network components to provide fully operational 5G isolated network for different PPDR scenarios.
Dependencies: Exposes 5G network capabilities to other NetApps.
Extra requirements: None.

2.10 NetApp 10: Vehicle Route Optimizer NetApp

- **Description of demonstration environment**

Using Demand Responsive Transportation (DRT) on 5G infrastructure (MEC), Neobility's NetApp can provide a near instantaneous response to the user's request. It builds a real-time distributed Vehicle Route Problem (VRP) optimizer engine, running on MEC servers closer to users and buses to increase processing speed.
We propose the orchestration to provide a service that can travel close to the corresponding vehicle switching between different virtualization and network domains seamlessly.
The 5G cloud native application uses the 5G infrastructure to calculate optimal shared routes. Using predictions, such as duration of stay and next location prediction, the shared pool of potential passengers can be increased significantly. The algorithms can predict the probability, time, and destination of the next travel, and use this data to contact potential travelers ahead of their travel-time and offer them the possibility of the route.
A key asset for the NetApp is usage of the 5G networks that will grant it increased capacity, security, elasticity and adaptability. Using a real-time distributed solution, that runs closer to the user in edge computing, will recalculate the route continuously (continuous re-optimisation) and provide a near instantaneous response to the user's request.

- **NetApp high level infrastructure**

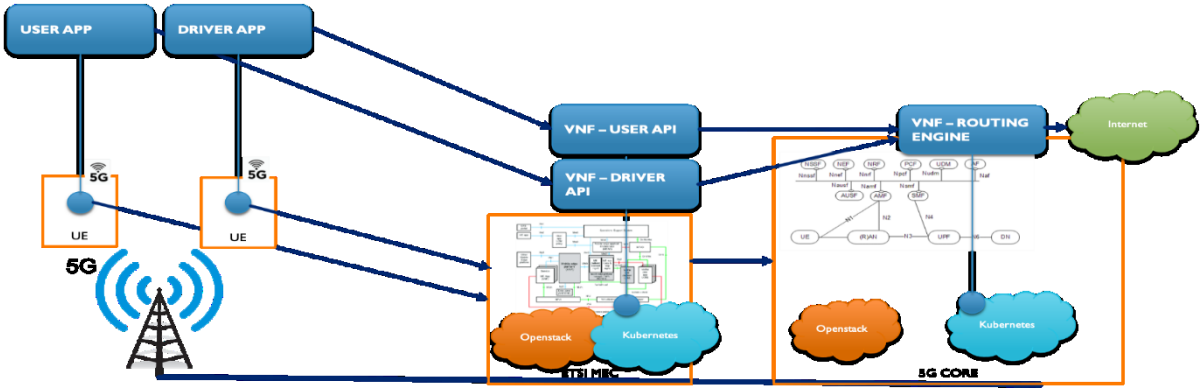


Figure 26 Vehicle Route Optimizer NetApp high level Infrastructure

- **NetApp KPIs**

Table 35 Vehicle Route Optimizer NetApp KPIs

Generic KPI name	Metric Indicator (How)	KPI value	KPI unit
Latency	Maximum end-to-end transmission time between UE & MEC	20	Miliseconds
Availability	Minimum time percentage the NetApp is online accepting requests from UEs	99	%
Initial time	Time needed to deploy for the first time	<10	Minutes

Table 36 Vehicle Route Optimizer NetApp's NEST

Vehicle Route Optimizer NetApp's NEST	
Area of service	RO
Area of service: Region specification	Bucharest
Downlink maximum throughput per UE	-
Uplink maximum throughput per UE	-
Isolation level	Virtual resources isolation
V2X communication mode	YES-NR
Slice quality of service parameters: 3GPP 5QI	70
Supported device velocity	120 km/h – Vehicular

Table 37 Vehicle Route Optimizer NetApp NSD

Vehicle Route Optimizer NetApp NSD	
Number of Services (NSDs)	1
Number of total VNFs	3
Dependencies of the 5G System	n/a
How is it operated	Automated deployment and provisioning
Dependencies	None

Table 38 Vehicle Route Optimizer NetApp Core NSD

Vehicle Route Optimizer NetApp Core NSD	
Number of total VNFs	1
Packaging Info:	CNF
Placement (latency from-to)	Latency from UE: max 20ms
Internet access	Yes
Resource requirements	n/a
Delivery model	Docker container
Ingress BW	10-100 Mbits/s
Egress BW	0.1-1.0 Mbits/s

- **Overall integration needs**

Packaging Info (VM, container, type, etc.): Multiple docker containers, communicating via HTTP and WebSocket.

Existing Healthcheck or Lifecycle (deployment status) Hooks or APIs: Every docker container will expose a healthcheck endpoint. The deployment is successful when all containers are healthy.
Dependencies of the 5G System (requires slicing, core functionality, etc.): To be determined.
How is it operated (and does it require manual interventions): The target is to be fully automated, but to be determined to what extent. Deployment to a specific PoP should be fully automated, but scaling and deploying to other PoPs might require manual intervention.
Dependencies (does it expose or consume services from/to other netapps): No.

2.11 NetApp 11: Fire detection and ground assistance using drones (FIDEGAD)

- **Description of demonstration environment**

Wildfires are one of the costliest and deadliest natural disasters across the world, especially in the Mediterranean region. The immediate impacts include damage to millions of hectares of forest resources, evacuation of thousands of people, burning of homes and devastation of infrastructure, and most importantly, threatening the lives of people.
This NetApp will give to teams a first assessment of buildings and forests on fire. The NetApp is onboarded to an air drone as a cloud native application together with services on the Edge ensuring low latency. Telemetry as well as information from infrared sensors, speakers, conventional video and thermal vision are transmitted to the 5G System and from there to the teams on the ground. The NetApp not only handles the drone live images streaming and processing, but also allows the teams on ground to adjust the altitude at which flyover takes place according to the height of the flames. Apart from the service creation time, it shall also be critical the handover between 5G stations.

- **NetApp high level infrastructure**

The NetApp is onboarded to a drone along with services running to the Edge, i.e. image recognition services, ensuring the lowest latency in case of fire detection. Besides that, information from multiple input channels is transmitted to 5G System and from there to the ground units. Ground units would be able to take over the control of the drone, apart from receiving the aforementioned information.

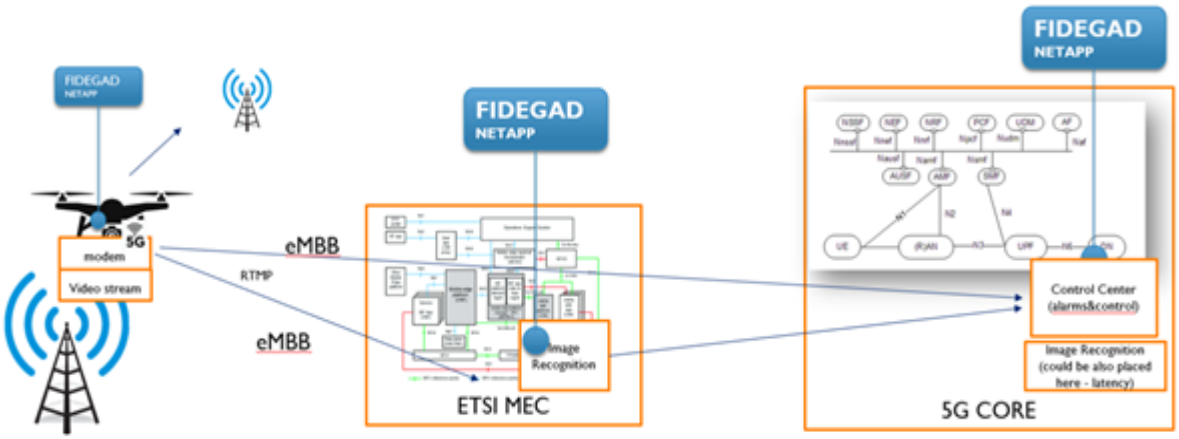


Figure 27 FIDEGAD NetApp high level Infrastructure

- **NetApp KPIs**

Table 39 FIDEGAD NetApp KPIs

Generic KPI name	Metric Indicator (How)	KPI value	KPI unit
Latency	Maximum end-to-end	50	Miliseconds

Table 40 FIDEGAD NEST

FIDEGAD NEST	
Area of service	GR
Area of service: Region specification	Patras
Downlink maximum throughput per UE	128 Kbps
Uplink maximum throughput per UE	10000 Kbps
Isolation level	Virtual resources isolation
Slice quality of service parameters: 3GPP 5QI	69
Supported device velocity	0-1 km/h
User data access	Termination in the private network

Table 41 FIDEGAD NSDs

FIDEGAD NSDs	
Number of Services (NSDs)	2
Number of total VNFs	3
Dependencies of the 5G System	1 Slice
How is it operated	Automated deployment and provisioning
Dependencies	None from other NetApps

Table 42 Image recognition Service (NSD)

Image recognition Service (NSD)	
Number of total VNFs	1
Packaging Info:	VNF/CNF (OSM)
Placement (latency from-to)	Latency from UE: max 100ms
Internet access	NO
Resource req (flavor cores/mem/hd)	
Delivery model (Vm Image, Container (dockerhub, else?))	
Ingress BW	
Egress BW	

Table 43 Control Center Service (NSD)

Control Center Service (NSD)	
Number of total VNFs	2
Packaging Info:	VNF/CNF (OSM)
Placement (latency from-to)	Latency from UE: max100ms
Internet access	Yes
Resource req (flavor cores/mem/hd)	
Delivery model (Vm Image, Container (dockerhub, else?))	
Ingress BW	
Egress BW	

- **Overall integration needs**

Packaging Info (VM, container, type, etc.): VNF/CNF (OSM). 2 NSDs: Image Recognition Service, Control Center Service.
Existing Healthcheck or Lifecycle (deployment status) Hooks or APIs: No.
Dependencies of the 5G System (requires slicing, core functionality, etc.): 1 Slice (eMBB kind).
How is it operated (and does it require manual interventions): Automated deployment and provisioning.
Dependencies (does it expose or consume services from/to other NetApps): No.

2.12 Overall 5GASP NetApps vertical-specific requirements

The NetApps represented in the project have been specifically picked to cover different use-cases in terms of deployment, dependencies to the network core, and QoS parameters, we believe there can be a reasonable extrapolation for the functionalities of novel NetApps made that concerns the proposed architecture. In particular, some of the project NetApps would need to support a containerised model that may be scheduled and executed as part of a testing or production cycle in a facility (MANO and Kubernetes) with sufficient isolation and resource reservation capability, and support a sidecar-loaded approach of acceptance tests or criteria that confirm proper operation at a facility in terms of QoS parameters (bandwidth, traffic in/egress, latency, etc.). To cater for the diversity of the requirements of the 5GASP NetApps, the 5GASP platform shall provide onboarding and testing functionalities for both VM-based and CNF-based NetApps; this shall be implemented in selected targeted facilities (e.g. Aveiro, Patras, Bristol) from the ones discussed in the next section.

3 5GASP Experimentation Facilities Infrastructures Architectures and Capabilities (Testbeds)

This chapter will discuss the architecture and the capabilities of each of the six experimentation facilities infrastructures involved in the 5GASP project, namely the Aveiro, Bristol, Patras, Murcia, Ljubljana and Bucharest facilities infrastructures. The latter have already been used and validated within the scope of several H2020 5G projects: 5GinFIRE[3], 5G VINNI[4], MATILDA[6], 5G-EVE[9], amongst others. The combination of these experimentation facilities within the scope of this project shall lead to an integrated, open, cooperative and fully networked platform.

3.1 Aveiro Site

The Aveiro Site features a platform that exploits a rich set of capabilities and characteristics that go beyond the mere aggregation of equipment. The overall infrastructure features both research graded and industry graded solutions to provide a real-life environment for developing, integrating and testing novel solutions for 5G and beyond technologies. It brings together academics, operators, vendors and vertical industries to accelerate the development of mobile communications and the creation of novel business models. The infrastructure is open to the whole research and innovation community, both academic and industrial, to foster innovation on 5G technologies and its exploitation. To this end, the infrastructure is connected to GEANT[66] and a mixture of OpenVPN and Secure Shell Protocol (SSH) tunnels can be provided.

Figure 28 ITAV Infrastructure

Research-grade infrastructure

This infrastructure accounts for over 500 physical CPU cores, 7 Terabyte (TB) of RAM, 350 TB of storage space, supported by four Gigabit switches and five 10-Gigabit switches. The platform is running OpenStack Cloud Platform (Queens release), orchestrated via OSM (release Eight). The platform comprises high performance communication infrastructures to support advanced integration and experimentation activities, ranging from high speed fiber optic links with OpenFlow-enabled switching (currently with HPE, Aruba and Pica8 switches)

to standard Internet Protocol (IP)/Multiprotocol Label Switching (MPLS) connectivity towards external networks and the Internet (Cisco 3xxx routers). These resources, hosted in a controlled-environment datacenter at the IT Aveiro premises, not only support the everyday research activities of a 60+ people research group, but also provide the underlying technological realization of key initiatives (e.g., open source evolved Node B (eNB)).
Additionally, Advanced Mobile wireless Network playground (AMazING) is an outdoor test system, intended to differentiate itself from the existing ones by increased controllability (for the experimenter) and high reproducibility of the tests, even for mobility events. It consists of a free access wireless testbed, composed of 24 fixed and controllable nodes located at the rooftop of IT-Aveiro. The testbed is extended with a high-speed mobile node (>30km/h) following a fixed single trail circuit, allowing for highly replicable mobile experiments.

Industry-grade 5G Infrastructure
The industry graded infrastructure encompasses radio cells, both outdoor and indoor, together with a 5G Standalone Architecture (SA) Core enhanced with MEC capabilities. This infrastructure is geographically distributed in four different sites, on 3 locations as depicted in *Figure 29*:

- two on-campus indoor deployments;
- one off-campus outdoor deployment;
- one off-campus indoor, edge-based deployment.

Figure 29 ITAV Industry-grade 5G Locations

Figure 30 presents the general architecture, representing the different hardware components and their interconnection. On the left side, the four different site locations are represented. Locations with more than one antenna are configured to establish automatic neighbouring relationships in order to provide seamless handovers. On the right side, the core of the network is represented, as well as the networking providing communication support for the NFVI where the 5G functions are instantiated. The NFVI is monitored by means of the eSight platform as well as the Mobile Automation Engine (MAE) solution. This last element also assumes the orchestration and life-cycle management mantle.

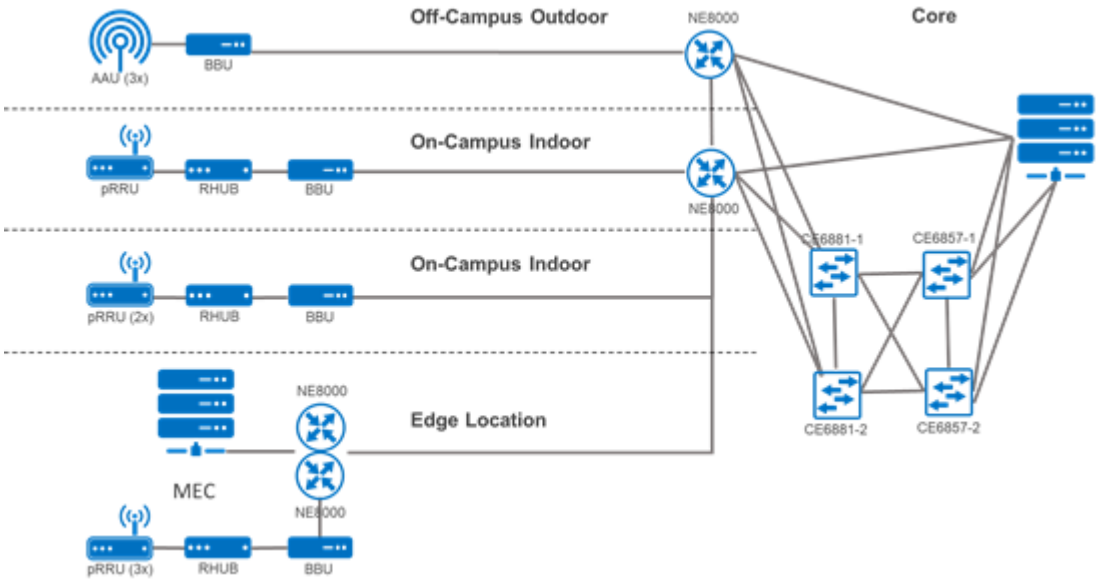


Figure 30 ITAV Industry-grade 5G Architecture

In terms of functions, the available 5G core provides the following functions: AMF, SMF, AUSF, UPF, Network Slicing Selection Function (NSSF), Network Repository Function (NRF), Unified Data Manager (UDM), as shown in *Figure 31*. These functions are complemented with an UPF instantiated in the edge site. Finally, user devices are also available: (i) 10 x Huawei Customer-Premises Equipment (CPE) Pro 2 (H122-373) and (ii) 5 x Huawei P40 Pro.

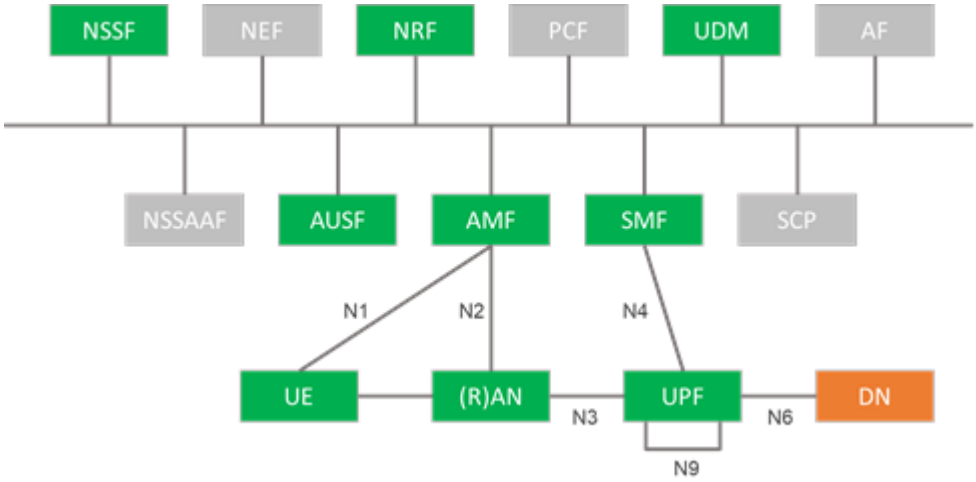


Figure 31 ITAV Industry-grade Available 5G Core Functions

3.2 Patras Site

The Patras 5G facility is an "*isolated*" non-public network for 5G and IoT applications. Isolated in terms of providing our own 5G radio and core resources, not shared with any public operator and available for any kind of experimentation, indoor and outdoor (depending on licensing). Most of the installed components are offered as Open Source but there are also dedicated components and services to support 5G and IoT scenarios. Numerous partners have deployed their technologies in the Patras 5G/Greece facility, thus creating a unique 5G playground for KPI validation and support on future verticals.

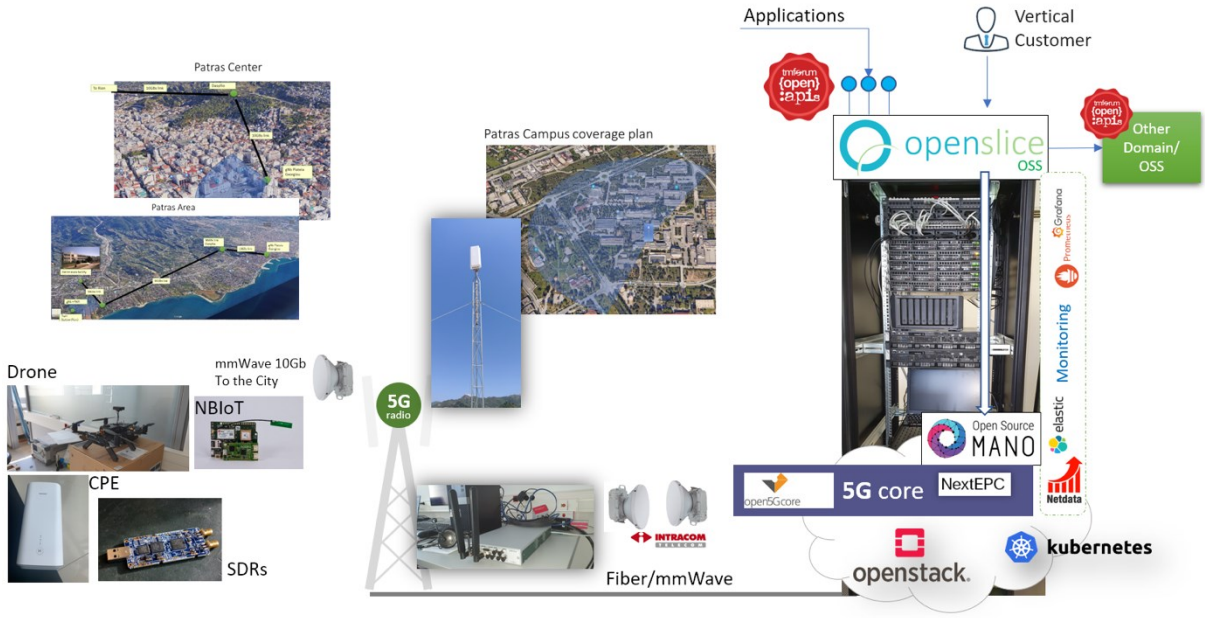


Figure 32 Patras 5G Architecture

With our Operations Support System (OSS), NFV and experimentation enabled services, like Openslice and Open Source MANO, we enable E2E automated deployment of multiple customized-slices over the whole network – access, transport and core. Patras 5G facility is equipped with a cloud platform, able to host core network components, as well as NFV and MEC deployments. The cloud platform offers a total computing power of 42 CPUs and 1.5TB of RAM and 50 TB of storage. 10GbE Network Interface Cards (NICs) Data Plane Development Kit (DPDK) enabled are also available. Patras 5G provides 5G standard-conformant components and core network infrastructure and integration of 5G core and 5G RAN with our Opensource based NFV platform. We support various flavours and installations of the 5G system, that are both Non Standalone Architecture (NSA) and SA depending on the scenarios of the customer:

- 5G Core and Evolved Packet Core (EPC) solutions that are available and can be orchestrated in the facility like (open tools): FhG Open5GCore, Open5GS, AMARISOFT Core, SRS EPC, NextEPC;
- 5G and 4G RAN: AMARISOFT 5G RAN (Classic boxes), 5G RAN open source radio (Lime, SRS)-700-800MHz, 3.5.-3.8GHz, 4G NB-IoT, LTE-M (FhG NB-IOT core) based on AMARISOFT, Various Software defined RADIO using ETTUS;
- UEs based on Limemicro's SDR and SRS software, as well as commercial UEs: Mobile phones LG and Samsung, Huawei CPE, Various SDR equipment, a Drone for testing;
- Monitoring is available through: Graphana, Prometheus, Netdata;
- OSM also configure with VNF telemetry support;
- Patras 5G has mmWave backhaul to link the access to the core network and Fixed Wireless Access to provide broadband services to the facility from various locations in the region of Patras and beyond;
- GEANT connectivity is also available.

Vertical applications can access the Patras 5G Service Catalogue through the Patras Facility site portal: https://patras5g.eu[67]. Vertical applications can self-manage and onboard their artifacts through our portal or access programmatically available services. Various artifacts can be managed through the facility portal[67] via standardized TMForum

OpenAPIs: Service Catalog, Service Order and Service Inventory, Partner Management and Users, Service Orchestration, VNFs/NSDs catalogue, NFVO endpoints via OSM North Bound Interface (NBI), Service and NFV deployment requests.
For 5GASP, the Patras5G will be enhanced with a dedicated Kubernetes cluster orchestrated by OSM and attached to our 5G core network.

3.3 Bristol Site

5GUKTest Network for 5GASP project is located within Bristol city centre as shown in *Figure 33* with the key network entities hosted at the Smart Internet Lab, "*We The Curious*" (WTC), MShed Museum, Millennium Square (MSq).

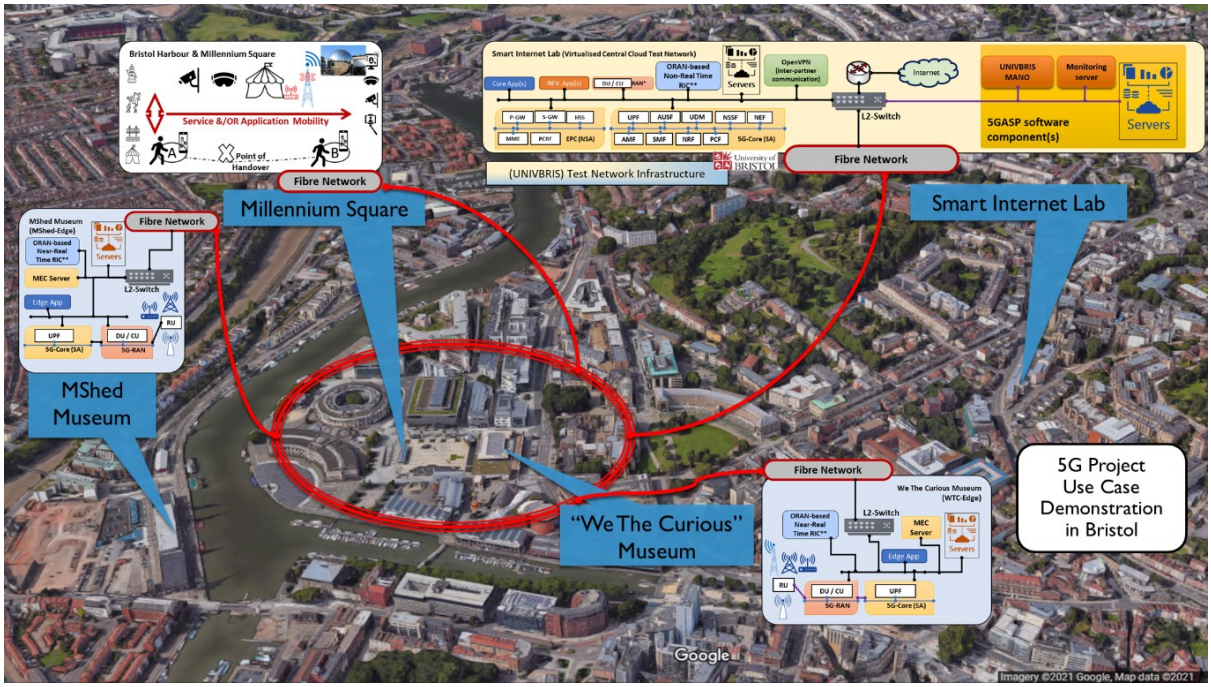


Figure 33 Location of the network entities in Bristol City Centre

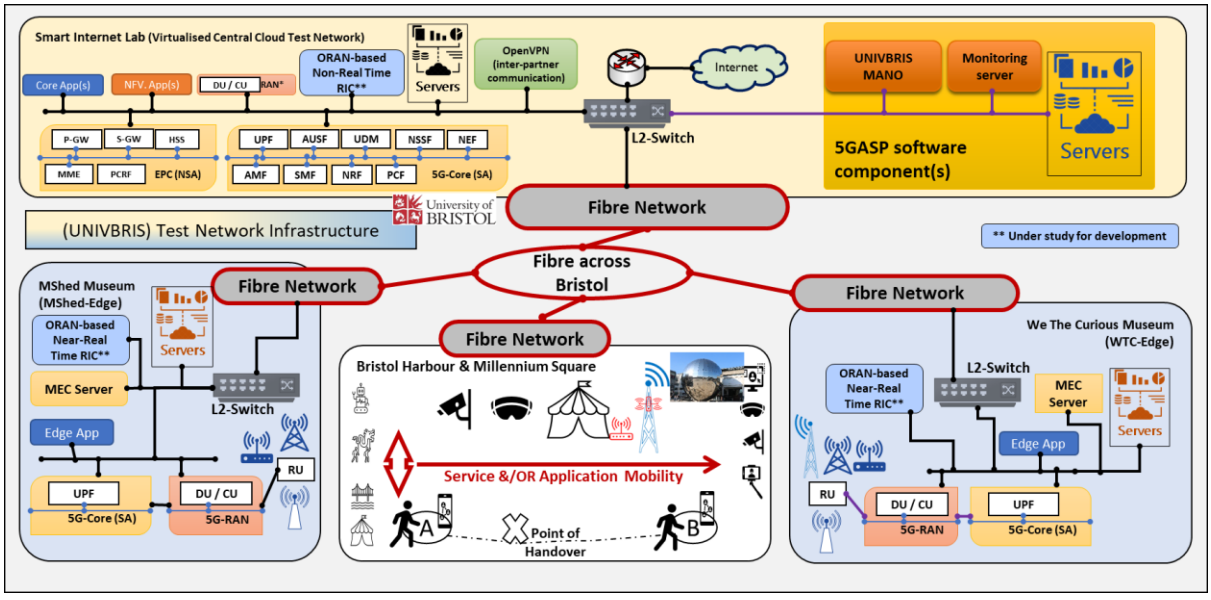


Figure 34 Test Network Functions in hosting partner technologies

A more detailed view of the network connectivity is shown in *Figure 34* depicting the connection across sites through dark fibre network. The Smart Internet lab hosts the cloud network functions for the management and operation of the 5G Cellular network as well as providing a virtualized network infrastructure for hosting 5G ASP Software components, including UNIVBRIS MANO: OSM release 9 and monitoring server.
This location also hosts the 3rd party technologies under test as part of a given research project connected to various hosting sites across Bristol. Here, we only show the WTC and MShed as way of illustrating the creation of a test network and service slices for demonstrating typical use cases and field trials that are carried out at MSq.
The hosting sites WTC, MSq and MShed at the edge of network provide IT rack and space for the compute nodes, switches as well as the access technologies to deliver E2E communication services demonstrating 5G technologies. The urban city centre outdoor 5G coverage area provides two radios cells with overlapping coverage area at the edges of the MSq offering opportunities for service mobility/wireless HO at pedestrian speed.
Summary of technologies deployed as part of the Smart Internet Lab test network include:

- 4G/5G core network;
- 4G & 5G NR;
- SDN enabled switches and service routers;
- Wi-Fi access points and management network;
- OpenStack and Kubernetes based VIMs;
- In house developed measurement and monitoring tool.

This test facility can demonstrate 5GASP use cases with these technologies:

- Edge computing with servers hosted at each site co-located with UPF;
- NFV orchestration where MANO can be hosted at the Smart Internet Lab facility;
- Open RAN (O-RAN) and xApp research and development of new functions;
- ML use cases can be realized, where the monitoring server can host Elasticsearch, Logstash, and Kibana (ELK stack). The monitoring will have access to compute infrastructure monitoring (OpenStack or Kubernetes). It can also receive UE radio parameters:
    - via the UE;
    - via the near Real Time RAN Intelligent Controller (nRT-RIC) based on O-RAN (under study for development).
- Hosting partner technologies for evaluation and field trial.

3.4 Ljubljana Site

The Public Protection and Disaster Relief facility for Outdoor and Indoor 5G Experiments (PPDR ONE) site is located at ININ's premises in Ljubljana, Slovenia. The facility comprises a radio and mobile core system (4G/5G), cloud backend infrastructure, a set of reference PPDR services and apps, a PPDR IoT kit, industrial and ruggedized end user devices as well as a test and validation toolkit. It provides indoor and outdoor experimentation sites as well as a compact portable mobile node for field-based network testing and services verification.

Figure 35 PPDR ONE architecture

The facility is based on cloud-based backend with OpenStack cloud acting as a VIM and spanning across multiple physical hosts connected via 10G-enabled internal network infrastructure. On top of OpenStack cloud the site provides Kubernetes engine to run containerized applications. Additionally, the site provides OSM NFV-based orchestrator capable of deploying and managing VNFs on OpenStack or Kubernetes-based Network Functions (KNFs) on Kubernetes engine. The storage services are based on external storage system which provides volumes to VMs, VNFs and KNFs. External access to the site can be provided with Internet Protocol Security (IPsec) or Open Virtual Private Network (VPN).
On the mobile network side, the facility provides SDR- and CPRI-based radio and mobile core system (4G and 5G) with flexible configuration options powered by NFV orchestration on top of the cloud infrastructure. The 5G network elements (core, gNB) can be established on fixed infrastructure or as a portable 5G node containing network appliance capable of running its own cloud backend. On the radio side, with SDR cards from Amarisoft, the site can provide frequency ranges from 70 MHz up to 6 GHz, channel bandwidth up to 100Mhz 5G NR and 3 x CA LTE. For macro 5G site coverage, the CPRI-based card with RRH will be used to provide n78 radio channel in 2x2 MIMO (multiple input, multiple output) mode while supporting SA and NS 5G network modes.

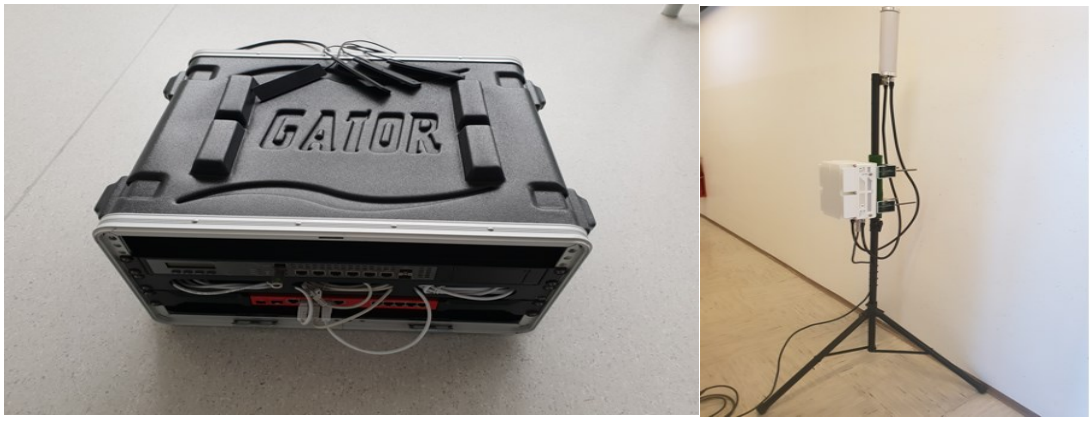


Figure 36 PDR ONE portable 5G node (left) with RRH and antenna (right)

The site also provides 5G user equipment:

- Smart Phones with SA support (OnePlus 8T);
- Smart Phones with NSA support (Samsung S20 5G, Samsung S21 5G, OnePlus 8T);
- Industrial 5G Gateways with NSA and SA support (Network appliance with industrial modems from Sierra Wireless).

Figure 37 Industrial 5G Gateway with SierraWireless development board and 5G modem

The site provides extensive network and service monitoring capabilities based on ININ's qMON E2E network monitoring and testing solution while also providing cloud and host monitoring based on Prometheus and Node exporter with visualizations in Grafana. qMON components are deployed in a distributed system architecture with modular capabilities (mobile, fixed and cloud deployment) that provides redundant local and centralized storage of network and services metrics and test results, flexible results exporting, advanced vizualizations and more.

qMON System Components:

- System Management
  - centralized cloud management of the qMON Agent probes;
  - hosted by PPDR ONE cloud backend.
- Reference Servers (VM/VNF/Docker)
  - reference test endpoints, can be deployed in various formats;
  - hosted by PPDR ONE cloud backend, additional reference servers can be established also on other sites.
- Test Agents (PNF/VNF/Docker/Android)
  - test probes, can be deployed in various formats and supports various environments (mobile, fixed and cloud);
  - supported on PPDR ONE client devices (Samsung S21, OnePlus 8T, Industrial gateway with Sierra Wireless EM9191 5G modem).
- Results Collector (VM/VNF/Docker)
  - collects the test results gathered from qMON Agent probes;
  - hosted by PPDR ONE cloud backend.

- qMON Analytics (VM/VNF/Docker)
    - Grafana- and Tableau- based dashboards for real-time and off-line test results' visualisations;
    - hosted by PPDR ONE cloud backend.

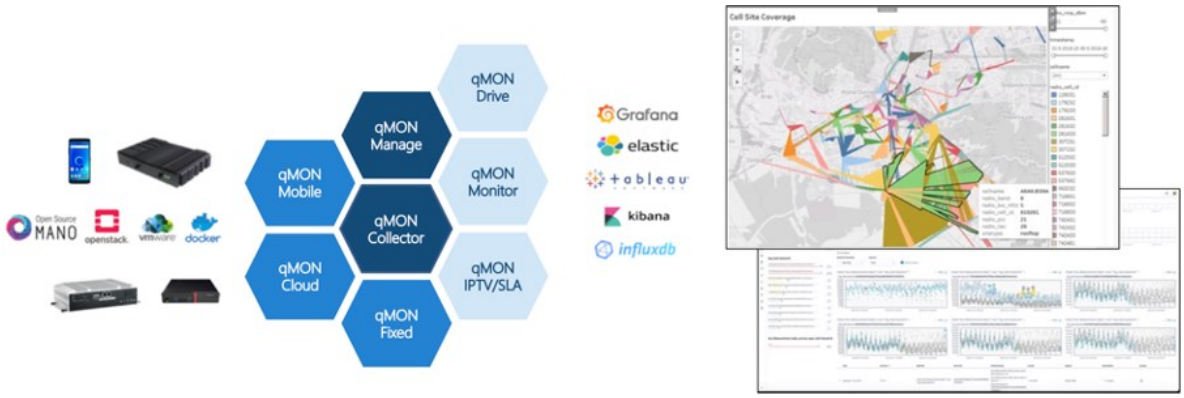


Figure 38 qMON Modular System Architecture

Regarding the PPDR services, the site will provide the iMON solution which is a real-time intervention monitoring tool designed to be used by first responders, public safety agencies and critical communication operators. It provides a Common Operational Picture (COP) in real-time and a suite of IoT-supported intervention management tools with on-site sensing and tracking capabilities based on dedicated mobile applications and sensor deployments.
iMON system components:

- iMON Dashboard
    - Tactical Dashboard exposing real-time PPDR services for a common operational picture, situational awareness and intervention management. It features a rich client HTML5/PHP web application, supporting: real-time common operational picture, RT assets tracking and backlog, data analytics and visualisations, intervention reports and logs; Backend: RT notifications, exposed APIs, automated hierarchical (group) user and device management.
    - hosted by PPDR ONE cloud backend.

- iMON Mobile App
    - Android-based Mobile application for triage and tracking from the field. Native mobile app with field sensing, time and distance-based location tracking, automated triage reporting (official procedural reporting formats, image attachments, automatically retrieved location data); automatic sync with COP; use of off-the-shelf (COTS) mobile devices with IP67[68].
    - supported on PPDR ONE client Android devices (Samsung S21, OnePlus 8T)

Figure 39 iMON System components

Facility Summary

- Cloud backend:
  - NFVO: OSM / ONAP (planned 2021);
  - NFVI: OpenStack (VNF)/Kubernetes (KNF).
- Mobile Network:
  - 4G/LTE with E-UTRAN New Radio – Dual Connectivity (ENDC) (5G NSA mode);
  - 5G NR with Core Network (5G SA mode);
  - 5G NR Cell Site (CPRI/RRH 20 W), n78, 2x2 MIMO, SA/NSA;
  - SDR based eNb/gNb (70 MHz up to 6 GHz, up to 100Mhz 5G NR bandwidth, 3 x Carrier Aggregation LTE);
  - Fixed/portable deployment.
- 5G UEs:
  - 5G Smart Phones with NSA and SA support (Samsung s20 5G, Samsung s21 5G, OnePlus 8T);
  - Industrial 5G Gateways with NSA and SA support (Network appliance with industrial modems from Sierra Wireless).

3.5 Murcia Site

Murcia site is a laboratory for experimentation located in the Computer Science Faculty in the University of Murcia. Its research purposes are focused on the area of 5G technologies with virtualization and backhaul infrastructure for the Wireless connectivity, including 5G, LoRaWAN and 802.11p self-managed infrastructure that allows experimentation in different fields.

It has a network infrastructure based on Coarse Wavelength-Division Multiplexing (CWDM) which provides a bandwidth of 10 Gbps fully available and customizable with QinQ/802.1ad allowing the isolation of different traffic. MEC functionality, including the virtualisation of edge devices. SDN is provided by two Delta AG7648-R with the latest PiCOS operating system in the core and HPE 2920 for leaf nodes switches supporting OpenFlow technology; in addition network programmability is granted by two barefoot Tofino-powered switches EdgeCore WEDGE100BF-32X-O-AC-F and Stordis BF2556X-1T-A1F. Connectivity between OpenFlow enabled switches and Programmable switches (P4) works at 6x40Gbps while programmable switches can work up to 100Gbps.

The site is equipped with a cloud platform which hosts core network components, as well as SDN, NFV and MEC deployments. Two OpenStack are deployed; rocky, a full-fledged deployment offering 160 vcpus (Intel(R) Xeon(R) Gold 6138 CPU based) and 512 GB RAM splitted into two compute nodes one on each side and Ussuri, a lightweight deployment offering 12 x86_64 vcpus (Intel(R) Xeon(R) CPU E5-2603 v3) based with 48 GB RAM and some ARM RPI 4 nodes with 4 vcpu each (Broadcom BCM2711B0 quad-core A72 based) and 8GB RAM each. Hyper-Converged Infrastruture with a 4-node cluster with 128vCores and 4TB RAM and two edge clusters providing 24vCores and 512GB RAM each is also available for extending the VIM capabilities. OSM is used as NFV orchestrator.

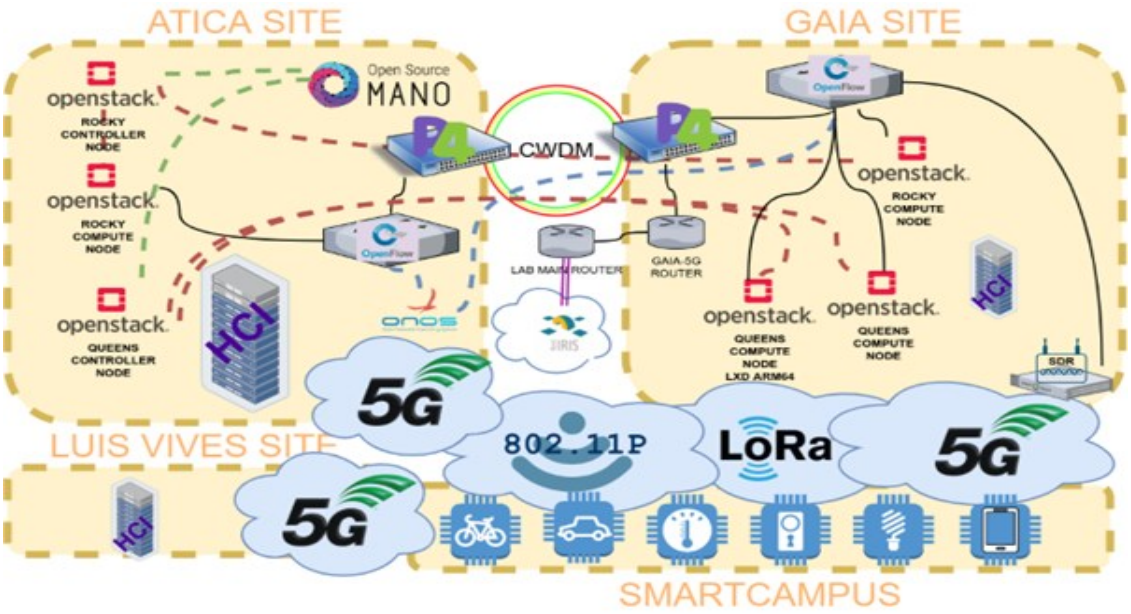


Figure 40 Murcia Site architecture

Regarding wireless connectivity, 5G and LTE provision is done by using SDR technology, in particular, 2 ETTUS B210 and one ETTUS N310 are available for experimentation. These SDR devices are accompanied with a 4 Core (I7-8700 based) with 8GB RAM the B210s and a 16 Core (AMD EPYC 7302P based) with 32GB RAM server the N310. Besides, a commercial core from Amarisoft with the associated RAN hardware and both systems are being fully integrated for having a completely functional and multi-site 5G solution. The deployment consists of two sites located in the Campus of Espinardo of the University of Murcia, and two cores are available, one turnkey solution by Amarisoft, and an experimental one which can implement multiple open source 5G cores.

Murcia Testbed also has LoRaWAN capabilities based on the 868MHz band. Currently, the infrastructure relies on a Kerlink iStation gateway, located in the Luis Vives bulding. This gateway is connected to our own deployed LoRaWAN network server (Chirpstack), the received data is also forwarded to The Things Network LoRaWAN network servers. In the future, it is planned to deploy two more gateways in the campus, in order to achieve full coverage of the Espinardo campus and also to cover Murcia area. Also, NB-IoT could be integrated into the platform provided by external providers.

Site Name: – Murcia test site (OdinS/University of Murcia)

Public/Private: Private

Software Stack:

- NFVO: OSM (Multiple Releases);
- NFVI: OpenStack (two different environments + working on a Nutanix deployment);
- Amarisoft 5G SA/NSA Core (AMF, SMF, AUSF, NSSF, NRF, UDM and UPF);
- Free5G core- 5G SA Core
- OpenAirInterface EPC with 5G NSA

Local Support Available: Yes, based on booking.

Resources granted for 5GASP: 40 cores, 125 GB RAM, 500 GB disk

Release Available: Rel15, Rel16 in progress.

CPE type and quantity:

- 5x Quectel;
- 3 x RM500Q (Qualcomm X55 based).

Telemetry / Monitoring mechanisms in place:

- GÉANT's NmaaS;
- Netdata + Grafana.

Site service level objectives (downtime reactions, etc.):

External Connectivity Available (VPN type, SSH tunnels, etc.):

- Connected to GÉANT
- Connected to GÉANT P4 Lab (GP4L)
- A Mixture of OpenVPN, wireguard and SSH Tunnels can be provided.

3.6 Bucharest Site

The facility is architecturally composed of 5G network components that will evolve during the life-cycle of the project to an E2E 5G infrastructure, able to cope with the projects NetApps needs (*Figure 41*).

The main integration and development activities will take place in Orange Bucharest 5G LAB, following several phases of implementation.

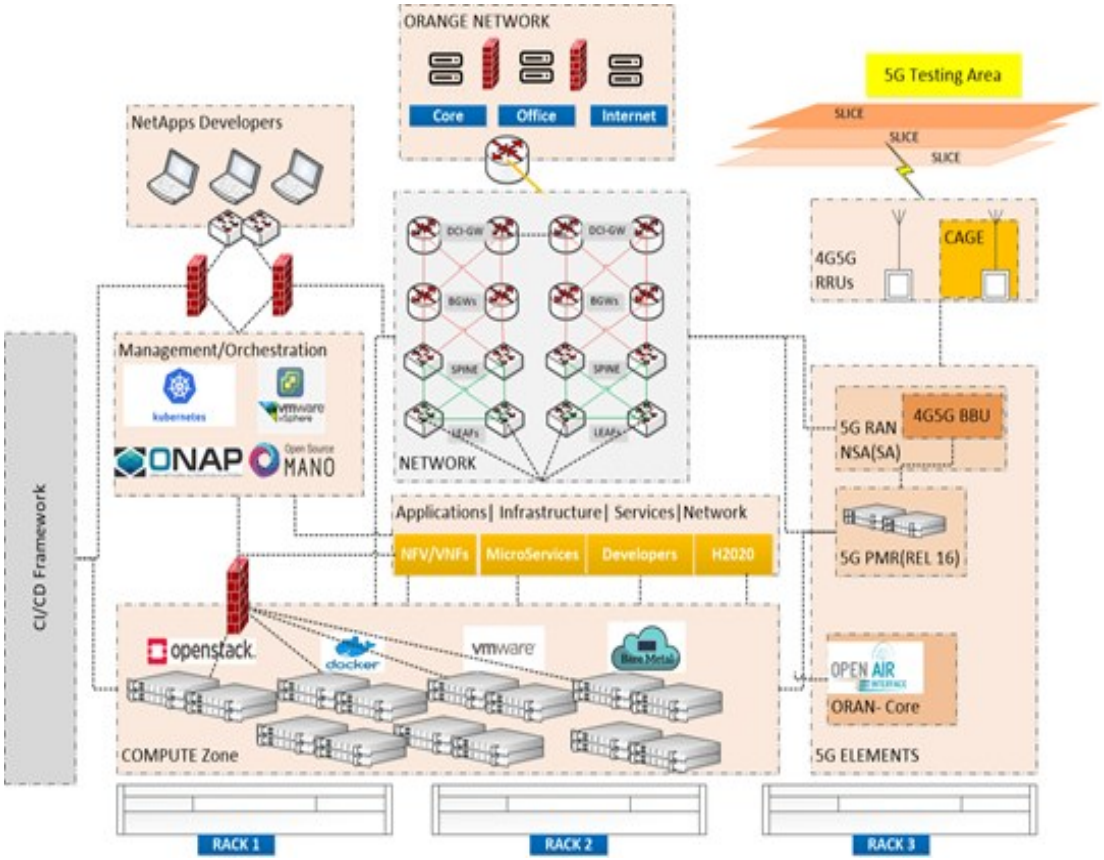


Figure 41 ORO Bucharest 5G facility

The Romanian facility deployment consists of three main implementation and validation steps:

1. **Phase 1**

5G NSA testbed, Bucharest, composed by :

- 5G NSA RAN and Core (vEPC & 5G RAN network integration), Option 3x;
- 1 RAN site (eNB/gNB) and antennas for preliminary infrastructure analysis deployed in Bucharest Lab Facility;
- Orange spectrum for testing (B3/B7/B20 and N78);
- IP/Network advanced infrastructure, IP-FABRIC architecture network for cloud services delivery, IP transport network orchestration;
- Advanced telco cloud infrastructure for VNF, CNF and bare metal apps;
- Virtualized Infrastructure as a Service (IaaS)/ Container as a Service (CaaS) supported by Openstack and Kubernetes/Docker;
- System monitoring and metrics collection;
- E2E Orchestration capabilities, OSM and ONAP;
- 5G UEs and CPEs;
- SIM cards.

The 5G NSA infrastructure is providing eMBB network service (1000Mbps downlink and 100Mbps uplink) and through specific data network Access Points Name (APN)s implementation, dedicated APNs selecting proper S/P-gateway for enhanced latency (<5ms). The communication service is statically configured, by using the SIM cards the NetApps UEs will have access to the service platform (*Figure 42*).

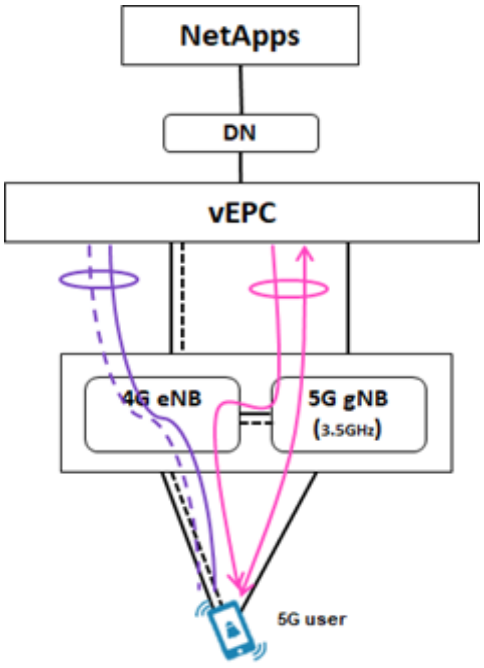


Figure 42 5G communication service scheme

5G-EVE/5G-VICTORI ICT-17/19 5G testbed based on OpenAirInterface over virtualized infrastructure (K8s) for RAN & Core, fully virtualized and automated network deployment (*Figure 43*):

- 5G NSA/SA RAN and Core 3GPP Rel 15;
- 1 site RAN antennas and vEPC/5GC network:
    - RAN SDNs
- Orange spectrum for lab testing (B1 and N78);
- Orchestration tools (ONAP) & Apps portal on-boarding;
- Virtualized Infrastructure IaaS/CaaS supported by Openstack and Kubernetes/Docker:
    - System monitoring and metrics collection
- E2E Orchestration capabilities, OSM and ONAP;
- 5G UEs and CPEs;
- SIMs.

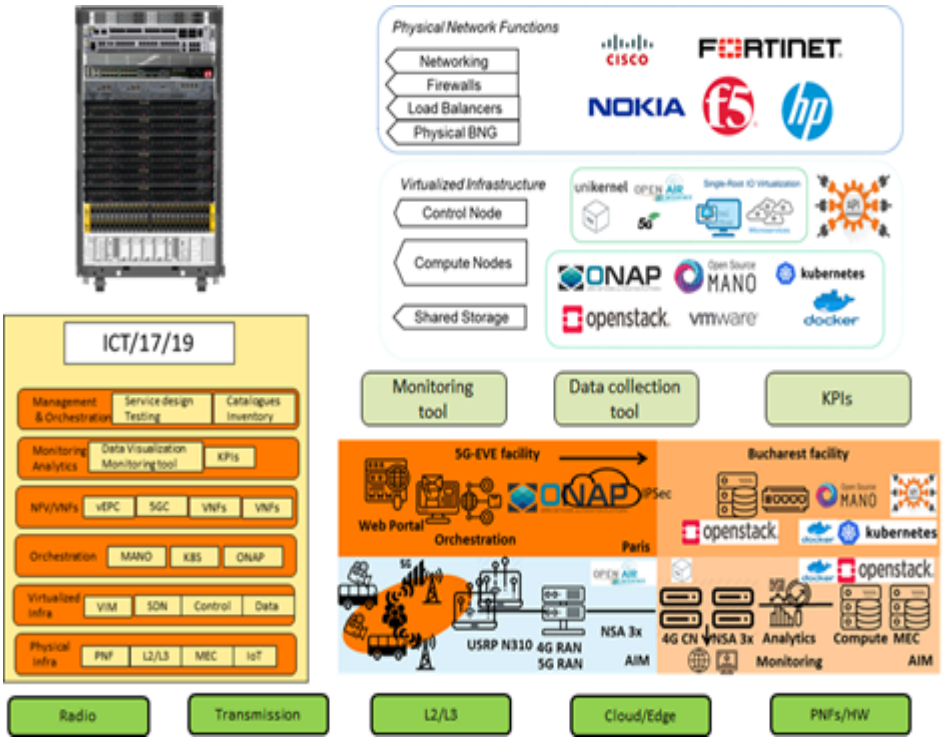


Figure 43 The 5G ICT-17/19 platform

2. **Phase 2**

5G private standalone network, Private Mobile Radio (PMR), that is integrated with the Bucharest testbed and is 3GPP Release 16, running on dedicated virtualized infrastructure, 5G SA option 2 implementation (*Figure 44*).

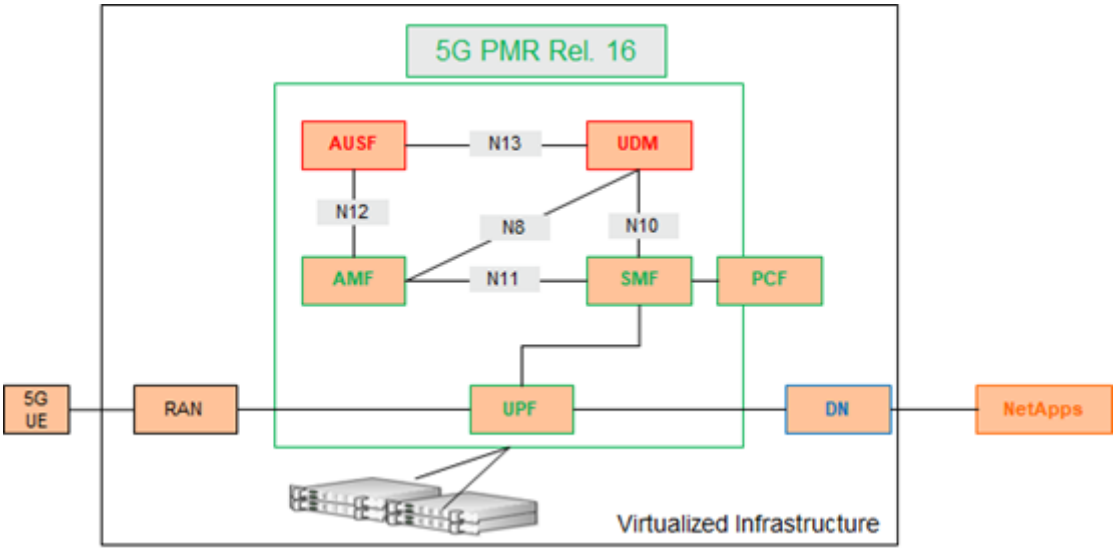


Figure 44 5G PMR Rel. 16 architecture on virtualized infrastructure

The 5G PMR provides 5G SA connectivity, service network slice implementation for the eMBB/URLLC use case's communication needs. The PMR is communicating through the Data Network (DN) with the NetApps Cloud infrastructure in Bucharest test-bed within the required KPIs in terms of bandwidth and latency.

3. **Phase 3**

5G SA, the 5G system mainly based on a virtualized network, including also some physical network components implemented by the 5G Service Based Architecture. The 5G network is composed of modularized services, flexible and adaptable, the automatic service creation running on-demand, fast network slices deployment cycles, dynamic services launched in the facility. The facility also introduces virtualization capabilities and the multi-services slicing concepts with the ability of adapting to the services as network slices for each type of usage, as in this case eMBB and URLLC. The 5G network slicing selection is based on Network Slice Selection Assistance Information (NSSAI). NSSAI concept overview is depicted in *Figure 45.*

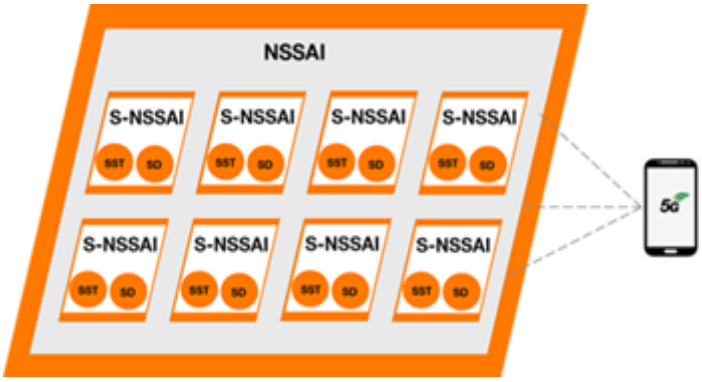


Figure 45 NSSAI concept overview

5G Slicing framework (*Figure 46*) is composed by the customized service provisioning, cost-efficient, scalable services in software-networking, assure different telco slices for eMBB and URLLC communication needs with guaranteed resource isolation. The NetApps, the vertical's, are in the loop, providing vertical services according to vertical customer specifications, through customized sliced capable networks.

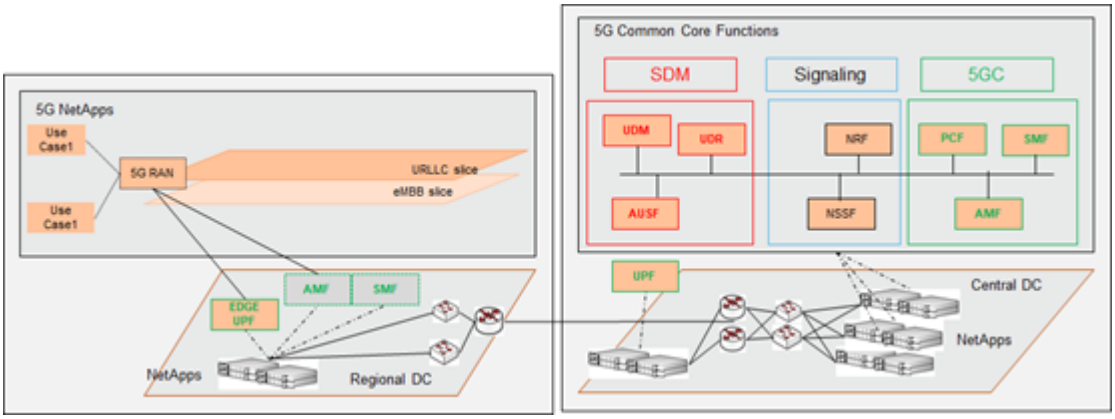


Figure 46 5G Slicing framework

For this project several network slices will be implemented, following the 5G SA Option 2 release capabilities:

- 5G SA RAN and Core, Option 2;
- Orange spectrum for testing (B3/B7/B20 and N78);
- IP/Network advanced infrastructure, IP-FABRIC architecture network for cloud services delivery, IP transport network orchestration;
- Telco cloud infrastructure for VNF, CNF and bare metal servers;
- Virtualized Infrastructure IaaS/CaaS supported by Openstack and Kubernetes/Docker;
- E2E Orchestration capabilities;
- 5G UEs and CPEs;
- SIM cards.

ORO facility planning is depincted in *Figure 47*.

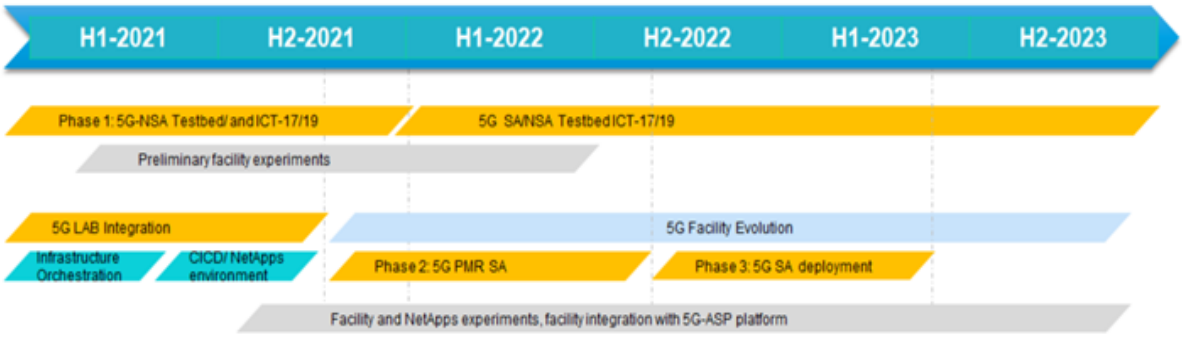


Figure 47 ORO facility planning

4 5GASP methodology and experimentation framework

5GASP follows a DevOps methodology in which development and operation teams collaborate throughout the NetApp development lifecycle. DevOps has been adopted by the IT industry in order to assure high-quality delivery of software in an Agile environment. In 5GASP we propose the adoption of this methodology, adapted to 5G NetApps development. Some of the existing DevOps tools such a CI/CD daemons require adaptions and customizations in order to incorporate NFV architecture into the CI/CD workflow. In this chapter we describe the models, the deployment and orchestration of NetApps and the testing through a CI/CD process manager.

4.1 Experimental model

The overall 5GASP facility is composed of several interworking sites, each deployed at a different geographic location and defining a single administrative domain. Every 5GASP facility site includes at least the following components:

- A NFV Orchestrator, taking care of the lifecycle management of provided network services that comprise the host network slice, the deployed NetApp and any automated tests tailored for this designated scenario.
- A Virtualized Infrastructure Manager, responsible for controlling and managing the NFV infrastructure compute, storage, and network resources within each site's infrastructure domain.
- Infrastructure resources, including access, transport and core network functions bundled together to describe the supported use cases.
- A Testcase Execute Engine, which performs and executes automated tests against the deployed NetApp on the facility.

All the components defined in a given site are from the same or different vendors and all managed by a single operator. Despite this per-site description, the whole facility shall be viewed as a single platform from the NetApp developer's perspective. This brings the need to implement adaptation layers, which unify the behavior and features offered in the different sites, abstracting underlying implantation details.

In this context, 5GASP envisions the option to provide developers with a single entry-point to the facility by means of a portal. This portal will allow any developer to onboard its NetApp, specify the accommodating site to host it and describe the tests that should be triggered once the NetApp is deployed. To provide a unified abstraction for all sites, the necessary experiment modelling and transformations need to be defined so that experiments can properly run on any 5GASP facility, regardless of the internal details. 5GASP envisages that this process can be related as a unified experimental model bundled together as a "*triplet*" triggering a service deployment order, as depicted in *Figure 48*.

The portal solution will be based on an open-source project, Openslice (see *1 Section*). Openslice offers both a user-friendly UI, multi-tenancy, support for onboarding VNFs to target facility NFVO and an Open API based on TM Forum Open APIs making it a perfect candidate for facilitating the project's needs. The main aim of the project is to define each part of the unified experimental model towards the same resource model, that provides a complete description of a given service, including information on topology and expected behavior. To

that extend, 5GASP's approach for each segment of the experimental "*triplet*", i.e. NetApps, hosting network slices and test descriptors, is to be defined under the TMF's ServiceSpecification resource model[34]. ServiceSpecification is a class that offers characteristics to describe a type of service. Functionally, it acts as a template by which services may be instantiated.

To support this approach, NetApps described as VNFDs/NSDs, depending on the defined model (Yet Another Next Generation (YANG) or Topology and Orchestration Specification for Cloud Applications (TOSCA)), that will be onboarded through the portal will be referred as ResourceFacing ServiceSpecifications expressing the resource aspects of the NetApp with its respective requirements. As enhancements of the NFV architecture towards "*cloud-native*" are currently attempted, 5GASP aims to provide effortless transformation for already containerized applications to NSDs/VNFs via Kubernetes Helm Charts, leveraging deployment schemes described in[69].

Prior to a successful onboarding, a set of elementary pre-flight tests, i.e. syntax checking, will be conducted to certify the validity of the descriptor to be onboarded. Should this step be successful, then the hosting network slice requirements shall be introduced. We can distinguish between these two options for this to be achieved:

- the developer may select the accommodating site to onboard its NetApp through a list of explicitly reported network specifications;
- 5GASP system will automatically appoint each NetApp to a target site, based on more abstract network requirements input from the developer.

Whichever the appointed case may be, network requirements will be fully aligned with GST (see *1 Section*) properties and each designated site will provide information on the range of network requirements it supports in form of NESTs. Therefore, these templates will be either available to the developer to choose from or there will be automatically allocated, depending on the NetApp fulfilling its requirements. Each one of the populated properties in NESTs will be perceived as a ServiceSpecCharacteristic resource class representing a key feature of the service specification describing the hosting network slice. Lastly, in the earlier release of the project, testing may be carried out through pre-defined automated test cases already described in each facility site. The reference to each test case can also be achieved via the adoption of ServiceSpecification model. Further holistic amplification on testing will be conducted altogether in future deliverable 5.1.

The three experimental model entities, converted to TMF's ServiceSpecification and ResourceSpecification models, can be contained and listed in service and resource catalogue(s). The design and maintenance of service and resource catalogues brings benefits both in terms of reusability and classification of the "*triplet's*" entities to distinct and explicit groups. The introduction of catalogue aims to incorporate these templates which are conceived to provide a self-contained specification of offered service instances, so that their deployment and operation can be automated as much as possible.

Once all entities are expressed to the above universal model, then bundling to a single entity can be achieved and progressed through underlying components for fulfillment. The concept of this unique entity can be facilitated through TMF's Service Order model[35]. Once a Service Order is placed, service fulfillment process is instantiated by our Service Orchestrator and runs the delivery process as per the requested specification, gets the full decomposition up to the required network level operations and executes them onto an administrative domain. The fulfillment and delivery process are further elaborated in the next section.

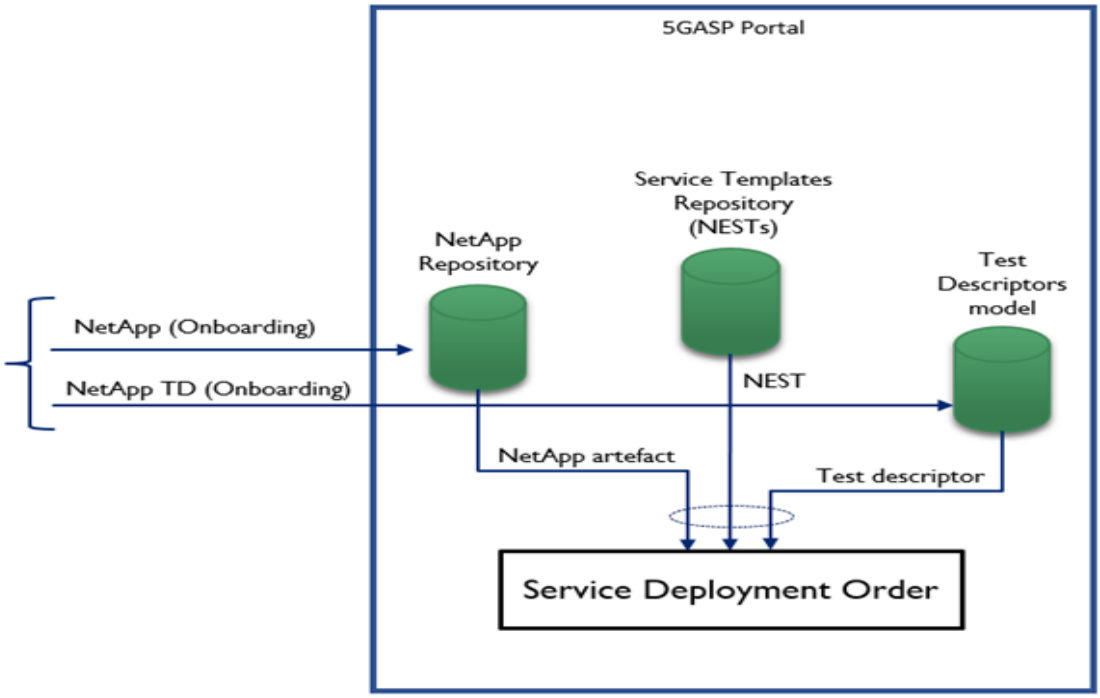


Figure 48 5GASP experimental model

4.2 Net Apps deployment and orchestration

The previous section defined the procedure of gathering the 5GASP tenant's (NetApp Developer) input into a single entity, namely Service Deployment Order. Then, as order is captured by the 5GASP system, the fulfilment process is instantiated as illustrated in *Figure 49*.

Here, order fulfilment and delivery are happening in two layers: by the Service Orchestrator and then by the NFV Orchestrator. Although the Service Orchestrator resides within the 5GASP portal, the NFVO is facility site specific, thus the two-layer distinction. Service Orchestration is aware of all underlying facility sites and their respective network capabilities and is responsible of coordinating the service deployment through certain steps depicted in *Figure 49*, simultaneously ensuring that each step is successfully progressed through. A service order may trigger orchestration process in a single facility site, or it may involve a cross-domain orchestration. In the latter case, Service Orchestrator may collaborate with a Network Orchestrator to establish a multi-site deployment. These scenarios will be further presented WP3, in deliverable 3.1.

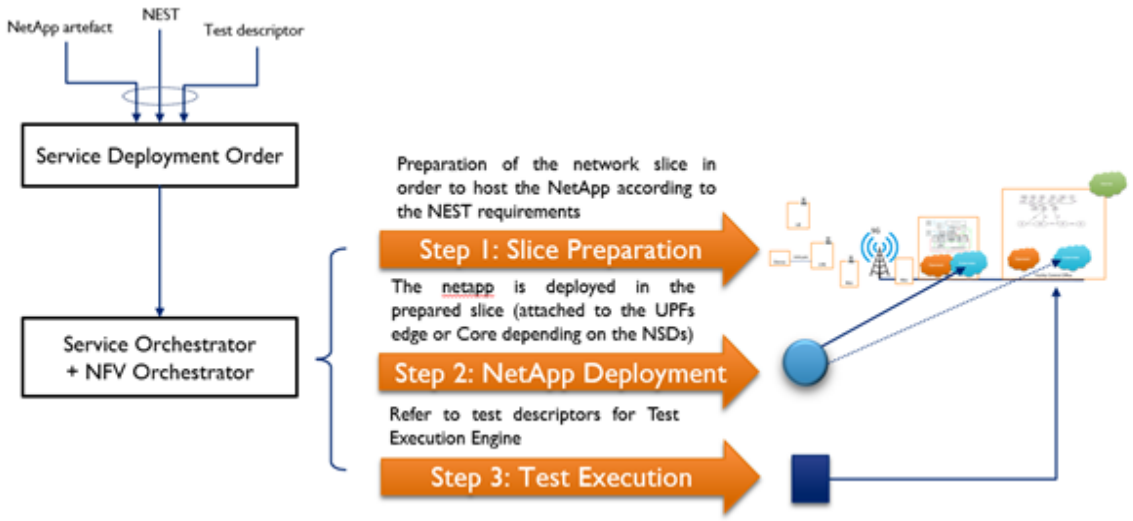


Figure 49 Service Order fulfillment and delivery

As outlined above, to begin the process, the Service Orchestrator transforms the properties of the provided NEST into network requirements which are then requested to be accommodated by the underlying facility site(s). Each facility site implements a set of these NESTs and once requested it deploys the respective service to facilitate the network requirements accordingly, e.g. 5G Core – Edge deployment, depending on latency inputs. Once the network slice is properly prepared on site's infrastructure, NetApp deployment request is expected and thus, the flow returns to Service Orchestrator for that matter. Eventually, NetApp is deployed on the previously prepared host network slice. Lastly, tests defined in the provided test descriptor are executed on the recently deployed NetApp/slice. Test-plan creation and execution will be further discussed in WP5, deliverable 5.1.

4.3 DevOps (CI/CD) context

DevOps aims to shorten the life cycle of creating a new system/software and enables continuous integration and delivery. To implement this methodology in 5GASP, automated orchestration and deployment are needed. This process was already described in the previous section. There is also the need to provide automatic testing mechanisms that can ensure the quality of the NetApps being developed. To achieve this, 5GASP uses a Test Execution Engine (TEE), that obtains tests from a Local Test Repository (LTR).

After a NetApp is fully deployed on the host network slice, the TEE will be triggered. Based on the Testing Descriptors submitted by the NetApp's developer, the TEE will obtain a set of tests from the LTR that is deployed on-premises. Then, the TEE will perform these tests and generate a report for the testing phase, which will then be forwarded to a service that will allow the developer to visualize the results of the testing phase.

To simplify the testing process and the infrastructure management, each testbed will have a TEE node and an LTR. Different testbeds might have different services enabling their TEE nodes. Regarding the LTRs, each one will store a set of tests that are specific for the testbed where they are deployed.

An architectural view of the CI/CD service, that is described in this section, will be present in *5.2.3 Section*.

4.4 5GASP Model Entities (Roles)

This section defines 5GASP roles, their requirements and their interfaces with the internal architecture.
Table 44 gathers the main roles and a brief description, while *Table 45* presents the roles each 5GASP partner is playing in the project.

Table 44 5GASP roles

Role	Actions	Role expertise	Actor groups
5GASP NetApp Developer	On-boarding of NetApps packages	Services/Applications	NODS
5GASP NF Developer	On-boarding of VNF packages	Networking functions	NODS
NetApp Tester	NetApps functionalities and performances verification in target facilities	Service/Application	CI/CD services
NF Tester	Testing of VNFs functionalities and performances verification in target facilities	Networking functions	CI/CD services
Service Designer	5GASP Apps and VNFs, onboarding, service blueprints and slices	Service applications and networking	NODS
Service Experiment Designer	Design the testing procedures and target KPIs	Service applications and networking	CI/CD services
Service Experimenter	Instantiation, configuration and execution for service experiments	Service applications	CI/CD services
Service Provider	Offers the service to the verticals' end users	Service applications	NODS
Platform Administrator	Administration of 5G Services, Operation, Maintenance	System integration and service platforms	NODS
Facility Administrator	Planning/installation/configuration of 5G Test bed facility	System integration, network, 5G, Cloud, Edge	Facility
Marketplace Administrator	Managing the NetApp Store so that all validated NetApps are visible and the corresponding testing/validation information is accessible.	System integration and service platforms	Marketplace & NODS
Marketplace (end) Users	Accessing the NetApp Store and filling in the service requests in order to get the matching NetApp and network operator that successfully tested it.	Service application	Marketplace

Table 45 5GASP roles distribution

Partner name/ Role	5GASP NetApp Developer	5GASP NF Developer	NetApp Tester	NF Tester	Service Designer	Service Experiment Designer	Service Experimenter	Service Provider	Platform Administrator	Facility Administrator
P1:ITAV			x	x	x	x	x	x	x	x
P2:UoP	x	x	x	x	x	x	x	x	x	x
P3:UNIVBRIS	x	x	x	x	x	x	x	x	x	x
P4:VMWARE					x	x				
P5:ORO		x	x	x		x				x
P6:EANTC			x	x		x				
P7:OdinS	x	x	x	x	x	x	x	x	x	x
P8:ININ	x	x	x	x	x	x	x	x	x	x
P9:Lamda Networks	x	x	x	x	x	x	x	x		
P10:YoGoKo	x		x		x					
P11:BLB	x		x		x					
P12:DriveU	x		x		x					
P13:Neo	x	x	x	X	x	x	x	x		

4.4.1 5GASP NetApp Developer

This subsection briefly presents the NetApp developer role and *Table 46* aims to match each 5GASP partner to the Netpps that are involved in for development.
5GASP NetApp Developer is in charge with developing vertical and cross-vertical NetApps (vApps) uploaded on 5GASP Portal that, after testing and validation, are published on the NetApp store.

Table 46 5GASP NetApp Developer role distribution

Partner name/ NetApp number	NetApp1	NetApp2	NetApp3	NetApp4	NetApp5	NetApp6	NetApp7	NetApp8	NetApp9	NetApp10	NetApp11
P1:ITAV											
P2:UoP											X
P3:UNIVBRIS							x				
P4:VMWARE											
P5:ORO											
P6:EANTC											
P7:OdinS	x			x							
P8:ININ									x		
P9:Lamda Networks								x			
P10:YoGoKo		X	X								
P11:BLB					x	x					
P12:DriveU					x	x					
P13:Neo										x	

4.4.2 5GASP NF Developer

5GASP Network Function Developer has the role of designing and onboarding the VNFs and CNFs. It is a similar kind of profile to the NetApp developer, but applied to different technical area. While NetApp Developer focuses on service applications, the NF Developer is focused on network related functions. *Table 47* matches each partner having the NF Developer role to the corresponding NetApps.

Table 47 5GASP NetApp Developer role distribution

Partner name/ NetaApp number	NetApp1	NetApp2	NetApp3	NetApp4	NetApp5	NetApp6	NetApp7	NetApp8	NetApp9	NetApp10	NetApp11
P1:ITAV											x
P2:UoP											x
P3:UNIVBRIS							x				
P4:VMWARE											
P5:ORO	x	x		x			x	x	x	x	x
P6:EANTC											
P7:OdinS	x			x							
P8:ININ									x		
P9:Lamda Networks								x			
P10:YoGoKo		x	x								
P11:BLB					x	x					
P12:DriveU					x	x					
P13:Neo										x	

4.4.3 NetApp Tester

The NetApp Tester is the tester and validator of vApps functionalities and performances in target facilities. *Table 48* depicts the 5GASP partners involved in project through NetApp testing role point of view.

Table 48 5GASP NetAppTester role distribution

Partner name/ NetaApp number	NetApp1	NetApp2	NetApp3	NetApp4	NetApp5	NetApp6	NetApp7	NetApp8	NetApp9	NetApp10	NetApp11
P1:ITAV											x
P2:UoP											x
P3:UNIVBRIS							x				
P4:VMWARE											
P5:ORO	x	x		x			x	x	x	x	x
P6:EANTC	x	x	x	x	x	x	x	x	x	x	x
P7:OdinS	x			x							
P8:ININ									x		
P9:Lamda Networks								x			
P10:YoGoKo		X	x								
P11:BLB					x	x					
P12:DriveU					x	x					
P13:Neo										x	

4.4.4 NF Tester

The NF Tester is the tester and validator of VNFs/CNFs functionalities and performances in target facilities. *Table 49* illustrates the 5GASP partners involved in project through NF testing role point of view.

Table 49 NF Tester role distribution

Partner name/ NetaApp number	NetApp1	NetApp2	NetApp3	NetApp4	NetApp5	NetApp6	NetApp7	NetApp8	NetApp9	NetApp10	NetApp11
P1:ITAV											x
P2:UoP											x
P3:UNIVBRIS							x				
P4:VMWARE											
P5:ORO	x	x		x			x	x	x	x	x
P6:EANTC	x	x	x	x	x	x	x	x	x	x	x
P7:OdinS	x			x							
P8:ININ									x		
P9:Lamda Networks								x			
P10:YoGoKo											
P11:BLB											
P12:DriveU											
P13:Neo										x	

4.4.5 Service Designer

The Service Designer role refers to the developer of services composed by 5GASP Apps and VNFs, including onboarding, service blueprints and slices etc. This role distribution throughout the 5GASP partners and NetApps is shown is *Table 50*.

Table 50 5GASP Service Designer role distribution

Partner name/ NetaApp number	NetApp1	NetApp2	NetApp3	NetApp4	NetApp5	NetApp6	NetApp7	NetApp8	NetApp9	NetApp10	NetApp11
P1:ITAV											x
P2:UoP											x
P3:UNIVBRIS							x				
P4:VMWARE											
P5:ORO											
P6:EANTC											
P7:OdinS	x			x							
P8:ININ									x		
P9:Lamda Networks								x			
P10:YoGoKo		X	X								
P11:BLB					x	x					
P12:DriveU					x	x					
P13:Neo										x	

4.4.6 Service Experiment Designer

The Service Experiment Designer is the designer of the testing procedures and target KPIs. *Table 51* depicts how this role is distributed among the partners and project NetApps.

Table 51 5GASP Service Experiment Designer role distribution

Partner name/ NetaApp number	NetApp1	NetApp2	NetApp3	NetApp4	NetApp5	NetApp6	NetApp7	NetApp8	NetApp9	NetApp10	NetApp11
P1:ITAV											x
P2:UoP											x
P3:UNIVBRIS							x				
P4:VMWARE											
P5:ORO	x	x		x			x	x	x	x	x
P6:EANTC	x	x	x	x	x	x	x	x	x	x	x
P7:OdinS	x			x							
P8:ININ									x		
P9:Lamda Networks								x			
P10:YoGoKo											
P11:BLB											
P12:DriveU											
P13:Neo										x	

4.4.7 Service Experimenter

The Service Experimenter is in charge with instantiation, configuration and execution of service experiments for validation. *Table 52* presents the Service Experimenter role among the partners taking into consideration the NetApps that are involved in.

Table 52 5GASP Service Experimenter role distribution

Partner name/ NetaApp number	NetApp1	NetApp2	NetApp3	NetApp4	NetApp5	NetApp6	NetApp7	NetApp8	NetApp9	NetApp10	NetApp11
P1:ITAV											x
P2:UoP											x
P3:UNIVBRIS							x				
P4:VMWARE											
P5:ORO											
P6:EANTC											
P7:OdinS	x			x							
P8:ININ									x		
P9:Lamda Networks								x			
P10:YoGoKo											
P11:BLB											
P12:DriveU											
P13:Neo										x	

4.4.8 Service Provider

The Service Provider offers the service to the verticals' end users. The partners matching this role are marked in *Table 53* considering the corresponding NetApps.

Table 53 5GASP Service Provider role distribution

Partner name/ NetaApp number	NetApp1	NetApp2	NetApp3	NetApp4	NetApp5	NetApp6	NetApp7	NetApp8	NetApp9	NetApp10	NetApp11
P1:ITAV											x
P2:UoP											x
P3:UNIVBRIS							x				
P4:VMWARE											
P5:ORO											
P6:EANTC											
P7:OdinS	x			x							
P8:ININ									x		
P9:Lamda Networks								x			
P10:YoGoKo		x	x								
P11:BLB											
P12:DriveU											
P13:Neo										x	

4.4.9 Platform Administrator

The Platform Administrator role refers to the administration of 5G services, operation and maintenance. *Table 54* shows how this role is distributed among 5GASP partners and their corresponding NetApps.

Table 54 5GASP Platform Administrator role distribution

Partner name/ NetaApp number	NetApp1	NetApp2	NetApp3	NetApp4	NetApp5	NetApp6	NetApp7	NetApp8	NetApp9	Net App 10	Net App 11
P1:ITAV											x
P2:UoP											x
P3:UNIVBRIS							x				
P4:VMWARE											
P5:ORO											
P6:EANTC											
P7:OdinS	x			x							
P8:ININ								x	x		
P9:Lamda Networks											
P10:YoGoKo											
P11:BLB											
P12:DriveU											
P13:Neo											

4.4.10 Facility Administrator

The Facility Administrator is in charge with planning, installation, configuration, operation, update and maintenance of 5GASP testbeds. *Table 55* depicts the distribution of this role among 5GASP partners and NetApps.

Table 55 5GASP Facility Administrator role distribution

Partner name/ NetaApp number	NetApp1	NetApp2	NetApp3	NetApp4	NetApp5	NetApp6	NetApp7	NetApp8	NetApp9	NetApp10	NetApp11
P1:ITAV											x
P2:UoP											x
P3:UNIVBRIS							x				
P4:VMWARE											
P5:ORO	x	x		x			x	x	x	x	x
P6:EANTC											
P7:OdinS	x			x							
P8:ININ								x	x		
P9:Lamda Networks											
P10:YoGoKo											
P11:BLB											
P12:DriveU											
P13:Neo											

4.4.11 Marketplace roles

5GASP NetApp Marketplace (or NetAppStore) is a portal for businesses during the lifespan of the project and possibly even beyond that. It is a marketplace that provides a public registry of SMEs and their registered products: reusable NetApps, NFs and NSs with links to open-source repositories and useful documentation that a SME needs to know. As the marketplace will host all NetApps (after testing and validation), a separate table for each of these roles is not justified. The role description is provided in *Table 44*.

5 5GASP Infrastructure Architecture

5.1 5GASP Global Infrastructure Architecture

As outlined throughout the project, the main technical objective of 5GASP is to build and operate an easy-to-consume, interconnected reference ecosystem of experimental facilities and provide open APIs, automation and functionalities to allow creators to register, deploy and test their NetApps, network and cloud functions. The goal is to achieve secure/trusted service provisioning and easy operation taking advantage of experimental facilities featuring virtualized functions and to allow access to this multi-domain testbed in which NetApps can be deployed in minutes across several domains, following a software driven process of testing and validation towards certification. On a high-level, the architecture consists of three layers, consisting of infrastructure, services and developer-facing components. As *Figure 50* depicts, the bottom layer will be the physical infrastructure contained in each participating facility. The middle layer consisting of the 5GASP services, including the onboarding, testing and orchestration, along with the top user-facing elements such as the NetApp Community Portal and Marketplace providing user-bound interaction. For practical purposes, services within the 5GASP middle layer (providing onboarding, testing, deployment orchestration and model transformation) will be decoupled through interfaces and message-passing, so as to enable a more robust overall architecture with better non-functional properties of supportability and uptime. Each component, along with its interfaces, actors, and relevant interconnections, will be discussed in the next *5.2 Section*.

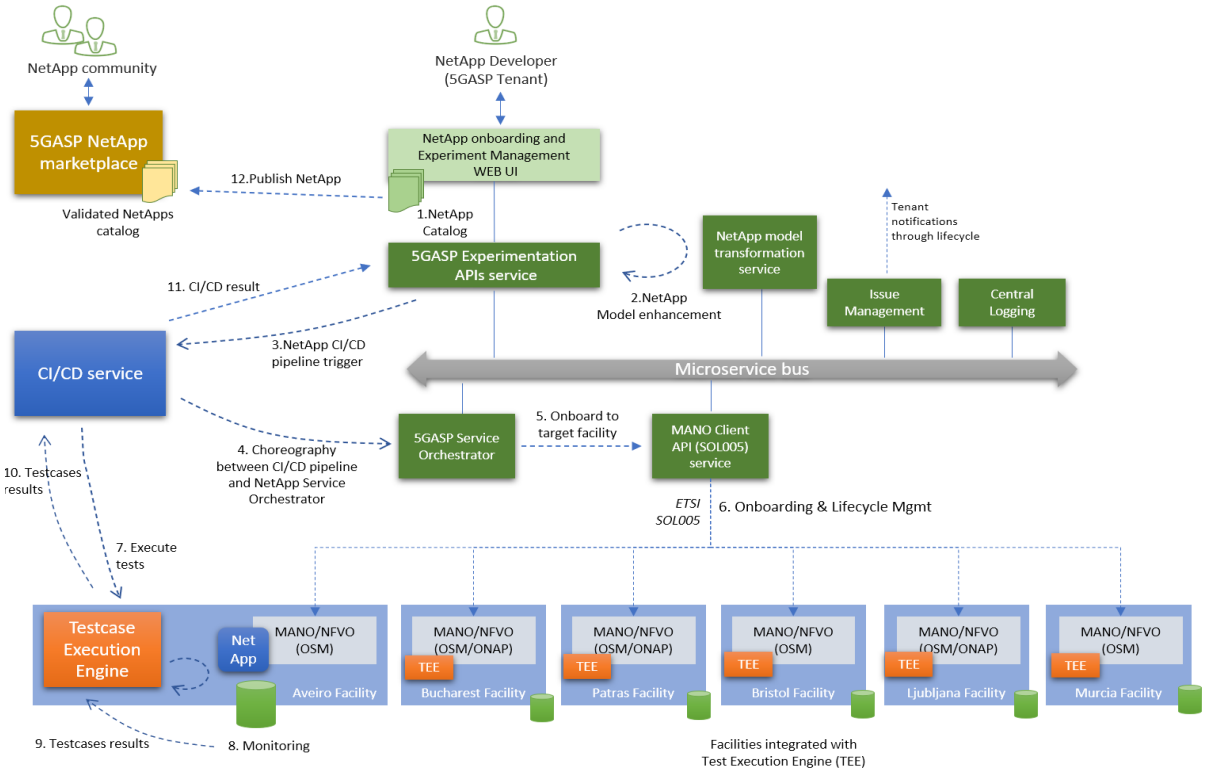
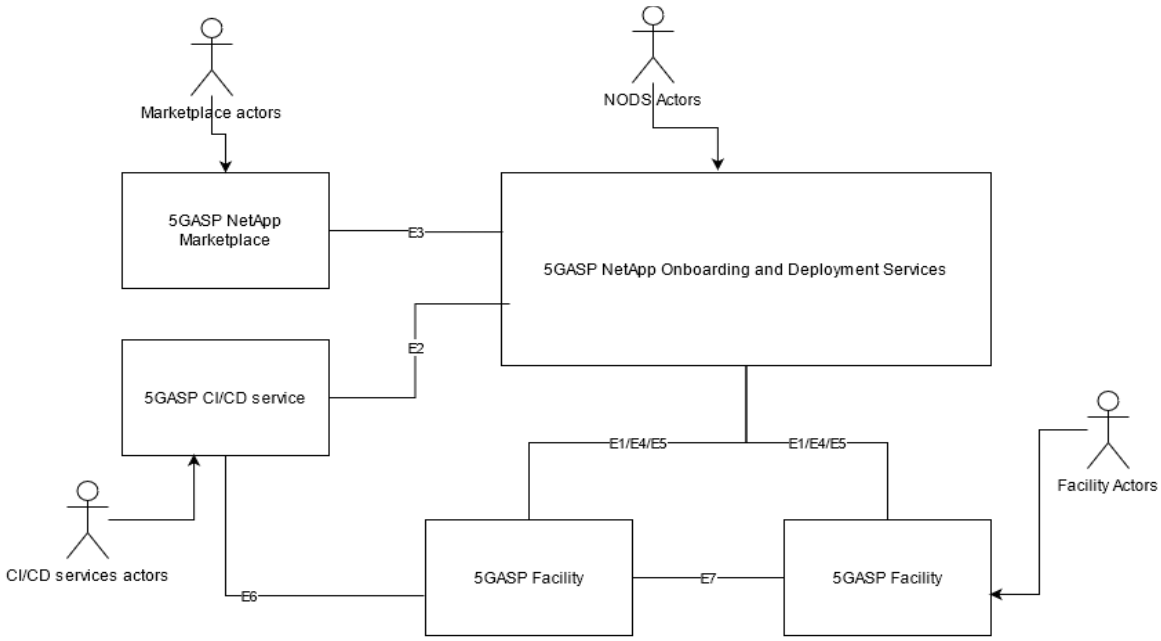


Figure 50 5GASP approach on DevOps experimentation and certification readiness Lifecyle[1]

5.2 5GASP Internal and external components and their interfaces

The 5GASP system interlocks a number of internal services, alongside their internal and public interfaces to onboard, deploy, facilitate and offer NetApps. The high-level interaction of these actors is depicted in *Figure 51*.



Heading

- E1: Interface for communication to the NFVO (SOL005 , etc)
- E2: Interface for CI/CD communication
- E3: Interface for NetApp Marketplace interactions
- E4: Interface for Cross Domain Network Orchestration
- E5: Interface for facility and testing services management
- E6: Interface for facility interaction with CI/CD
- E7 Inter-facillity Interface connectivity

Figure 51 5GASP high level architecture

The main features of the architecture, presented, in Figure 51 are:

- the 5GASP NetApp Onboarding and Deployment Services (NODS), which is a portal solution based on OpenSlice;
- a distributed CI/CD service to enable deployment and testing of the NetApps across testbeds;
- a Marketplace (or NetAppStore) to serve as a public registry for SMEs and their registered NetApps;
- the facilities to support cloud resource infrastructure management and dynamic services operation.

The sections below will go into details about these actors as well as the external interface intent for the NODS, CI/CD communication, Marketplace operations, Cross-Domain Network Orchestration and Facility testing services (including CI/CD and inter-facility communications).

5.2.1 5GASP NetApp Onboarding and Deployment Services (NODS)

Actors: **5GASP NetApp Developer, 5GASP NF Developer, Service Designer, Platform Administrator**
External Interfaces**: E1/E4/E5, E2, E3**
The 5GASP NODS is implemented by a portal solution, which is based on an open-source project called Openslice. The portal offers both a user-friendly UI, multi-tenancy, support for onboarding VNFs to target facility NFVO, interconnection with a CI/CD Service (*5.2.3 Section*) that orchestrates and executes pre-defined or developer provided test suites and an Open API based on TMFs APIs:

- Service Catalog Management API[34] which provides artefacts (e.g. models and dependencies) for the NetApp, network slice and testing specifications, along with capabilities such as packaging and exposure in service catalogues through explicit category definition.
- Service Ordering Management API[35] which permits the issuing of a service order that includes selected specifications from previously defined service catalogues and instantiation/execution parameters.
- Service Inventory Management API[36] which defines a consistent mechanism to perform operations like Create, Read, Update and Delete (CRUD) over the deployed services, providing run-time information and allowing operational configurations.
- Resource Catalog Management API[70] which allows the management of the entire lifecycle of underlying resources and the consultation of these elements during several processes, such as ordering process or allocation of implementation resources to the service specifications.
- Resource Inventory Management API[71] which defines standardized mechanisms for CRUD operation over the overall available resources or the ones facilitating the running services.

5GASP NODS, apart from an entry-point to the 5GASP system, provides a Service Order Management (SOM) and offers its own Service Orchestration and Network Orchestrator that coordinates actions with underlying NFVOs or other NFV/3GPP compliant systems. Furthermore, Service Orders across domains are also supported. Further description in the internal architecture of the 5GASP NODS, will be provided in WP3, deliverable 3.1.

5.2.2 5GASP Facility

Actors: **Facility Administrator**
External Interfaces**: E1/E4/E5, E6, E7**
This section will contain description about the 5GASP Facility. Details will be given in WP3, deliverable 3.1.
5GASP facilities, described in Chapter 3, support dynamic services instantiation and termination, cloud resources allocation, flexibility and services allocation in cloud infra. Each facility uses set of open monitoring tools as telemetry data from NFVI, Orchestrators or different 5G system components.

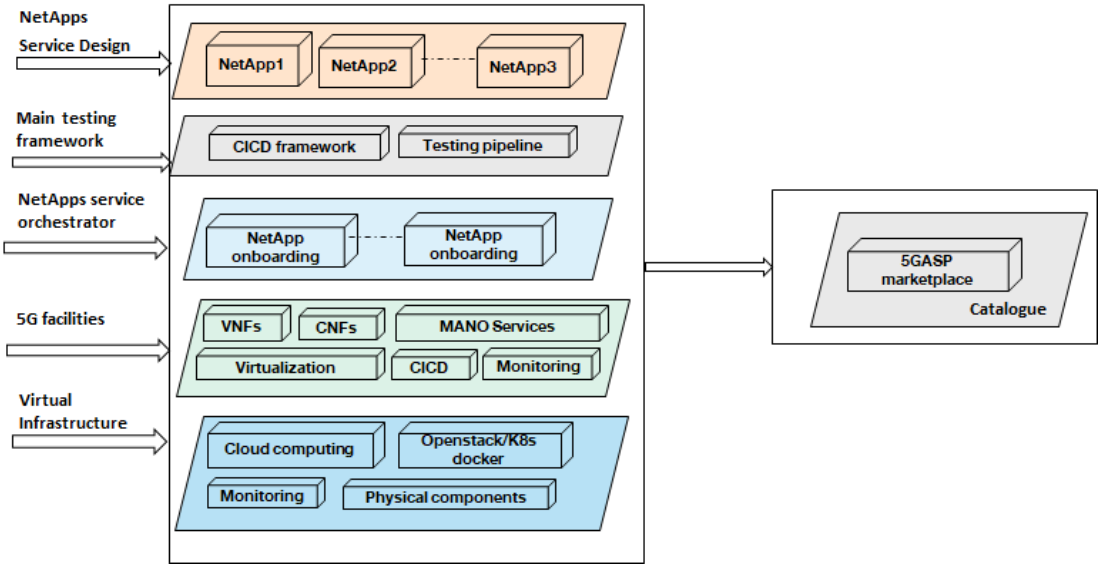


Figure 52 5GASP facility simplified architecture

In a down to top approach, as described in the simplified architecture from *Figure 52*, the 5GASP ecosystem architecture is based on a set of services and applications, VNFs or CNF running on top of the virtualized infrastructure, Apps hosted in VMs or containers, with support of different virtualization tools (e.g. Openstack, Kubernetes/Docker). 5GASP ecosystem will not only integrate existing facilities already proven in previous ICT projects, but will also lay down the foundations for instantiating fully softwarised architectures of vertical industries. Furthermore, it will provide facilities to test and validate NetApps taking into consideration vertical-specific requirements.

5.2.3 5GASP CI/CD Service

Actors: **NetApp Tester, NF Tester, Service Experiment Designer, Service Experimenter, Service Experimenter**
External Interfaces**: E2, E6**
To enable the deployment and testing of the NetApps across multiple testbeds, a distributed CI/CD service will be created. Given this requirement, we chose to have a central CI/CD Manager, that would orchestrate and manage all the CI/CD Nodes.
After the submission of the NetApps, Openslice will either enhance the NSDs to add a VNF containing the CI/CD Node Operating System image or stitch a NSD to the proper NetApp datapaths. This means that the CI/CD node will be deployed alongside the NetApp.
The deployment of the NetApps is under the scope of WP3. More information regarding the deployment and orchestration of NetApps are presented in *4.2 Section*.
Each NetApp will have, at least, one CI/CD Node to perform the needed tests. Once the CI/CD Node is up and running, it will communicate with the CI/CD Manager, registering himself and allowing the testing phase to start.
As mentioned before, when onboarding the NetApp to the 5GASP portal, the developer will have to submit a testing descriptor. This descriptor will define which tests should the CI/CD service run to validate the NetApp. These can be dynamic tests, created by the NetApp developer, or pre-configured tests.

Each testbed will have some pre-configured test, based on its hardware and the software that is deployed in the facility. These tests are stored in the facility's LTR.
During the beginning of the testing stage, the CI/CD Node will gather the needed tests from the LTR. Then, the testing phase can effectively start.
During this phase, some reports and log files will be created. These will then have to be sent to the developer, so he can check the output of the NetApp validation.
To display this information, a dashboard will be needed. A service to provide this feature will be created and the NetApp's developer will receive a web address to access it.
The CI/CD pipeline can be observed in *Figure 53*.

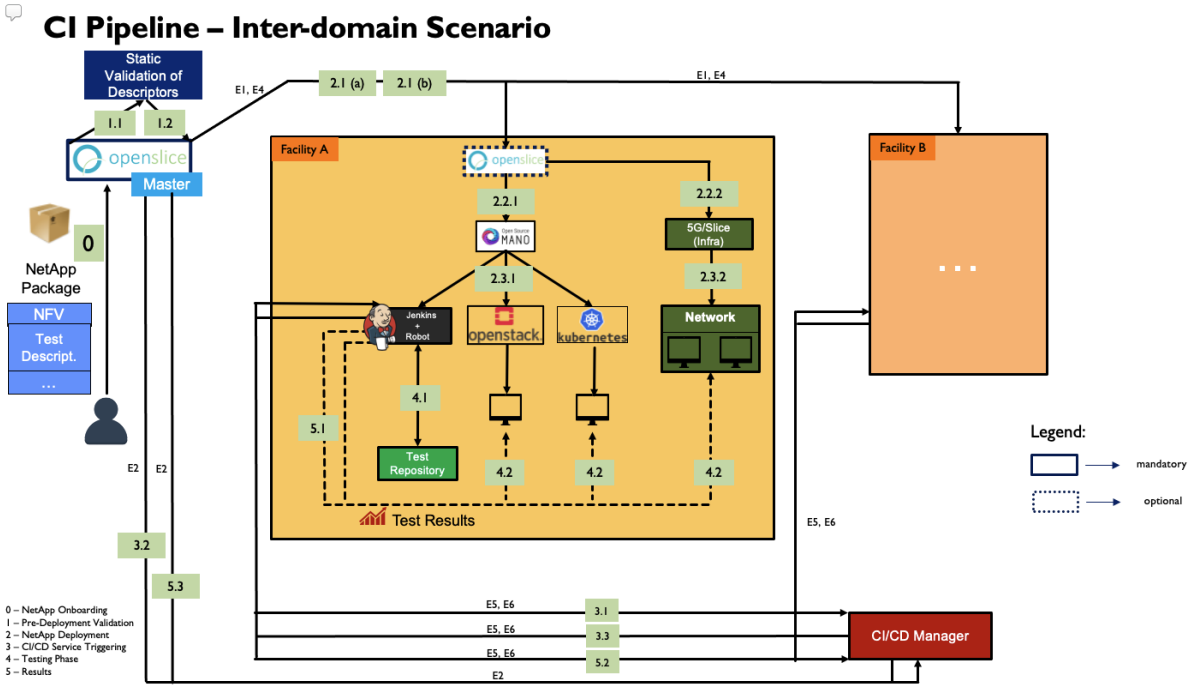


Figure 53 CI/CD pipeline

Each step presented in *Figure 53* is described in *Table 56*.

Table 56 CI/CD steps

Stage	Description
0	NetApp + Test submission to the Openslice
1.1	Static validation of the VNF descriptors
1.2	Results of the descriptors validation. If all descriptors are valid, we can move to step 2.1
2.1 (a)	The Openslice Master Node will order the Slave Node to orchestrate and deploy the VNFs
2.1 (b)	The Openslice Master Node will directly order OSM to orchestrate and deploy the VNFs
2.2.1	Select the correct NSD/VNFD/NEST to be used for the deployment and send the NSD/VNFD/NEST to OSM
2.3.1 + 2.3.2	Deployment of the VNF on the chosen facility + Deployment of a Jenkins Node

3.1	The Jenkins Node will inform the CI/CD that it is online and ready to accept jobs
3.2	The Master Openslice Node will trigger the CI/CD Service. This can only be done after step 3.1
3.3	The CI/CD Manager will send tasks to Jenkins
4.1	Jenkins will obtain some pre-configured tests (Robot)
4.2	Jenkins will test the VNFs, according to the tests that it got from the test repository and the dynamic tests that the NetApp developer uploaded to the portal
5.1 + 5.2 +5.3	The developer gets the results from the testing phase

5.2.4 5GASP NetApp Marketplace

External Interfaces: E3
5GASP NetApp Marketplace (or NetAppStore) is a portal for businesses during the lifespan of the project and possibly even beyond that. It is a marketplace that provides a public registry of SMEs and their registered products: reusable NetApps, NFs and NSs with links to open-source repositories and useful documentation that a SME needs to know. The portal also provides useful information about the certification process in form of web address to the procedure and/or documents. The NetApp Marketplace is complemented by the NetAppCommunity portal supporting developers and third-party end-users, in general.

5.2.5 External Interfaces

5GASP follows a Service Based architecture. In this section, we define the external interfaces that are provided and consumed by the various 5GASP services.

5.2.5.1 E1 - Interface for communication to the NFVO (SOL005, etc)

As already discussed, 5GASP employs a global Services Portal (see *5.2.1 Section*). Considering the different technologies deployed in each facility and the available standard interfaces, this section explores the different options provided for interconnection at the services level between the global portal and the underlying facilities.
As depicted in *Figure 54*, four options are derived:

- Option A: Single OSS exposes TMF based APIs by each Facility and inteconnected with the Global Portal;
- Option B: Facility exposes its NFVO directly to the Global Portal, ETSI NFV SOL005 is followed;
- Option C: Facility exposes other APIs (Non ETSI-NFV) (e.g. Open Network Automation Platform (ONAP));
- Option D: Facility exposes ETSI-NFV or 3GPP compliant APIs via another service (not NFVO directly).

All four options will be further presented in WP3, deliverable 3.1.

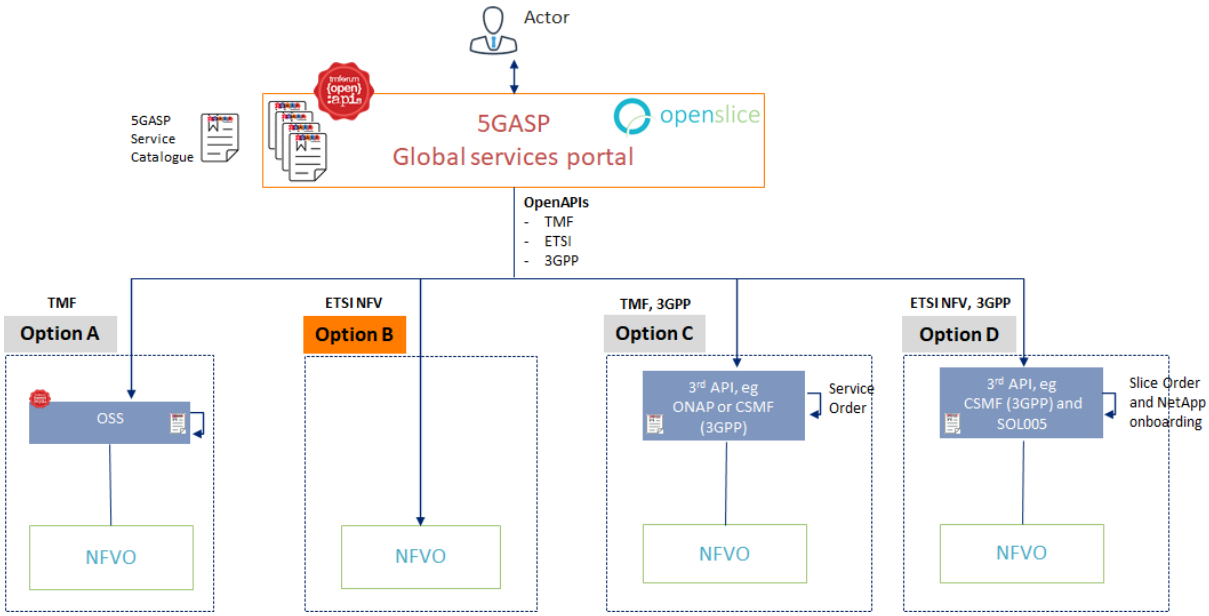


Figure 54 Communication with facility sites options

5.2.5.2 E2 - Interface for CI/CD communication

This interface will be used for communication with the 5GASP CI/CD Service. It is through this interface that the 5GASP Portal will trigger the CI/CD Service, through the master TEE. The master TEE will then forward the test jobs to the slave TEEs, that, after performing the tests, will send the results back to the master TEE. Although the previous communication is enabled by the interfaces E5 and E6, the master TEE will use again interface E2 to send the results back to the Portal.
Given that the NetApps' developers won't directly interact with the CI/CD service, the interface E2 won't be publicly available. All the communication between the master TEE and the Portal will be encapsulated inside a Wireguard, VPN tunnel.

5.2.5.3 E3 - Interface for NetApp Marketplace interactions

This interface mainly involves the publication of NetApps to the NetApp Marketplace. Following the proposed DevOps experimentation and certification readiness lifecycle and only after successful certification is acquired, the NetApp can be published to the NetApp Marketplace; therefore, it is made publicly available. In this case, as is observed widely in telecommunications industry, TMF's product resource model will be used to accomplish the required interconnection. Further discussion on this interface will be provided in WP3, deliverable 3.1.

5.2.5.4 E4 - Interface for Cross Domain Network Orchestration

The objective of this interface is to provide top-level control for cross domain network service provisioning (enforced through the E7 interface). This control-plane interface provides a hierarchical approach to cross domain communication in which the 5GASP Services play the orchestration and trusted party role in setting up cross domain communication. This interface

controls the setup of interface E7 and is interlinked with the NFVO, VIM's and Slice Manager for negotiation of cross domain overlay networks serving NS across domains. More details on this interface are provided in *5.6 Section*, Multi-domain and will be provided in WP3, deliverable 3.1.

5.2.5.5 E5 - Interface for facility and testing services management

During the first development phase, the developers will only be able to test their NetApps according to some pre-defined tests. Then, once this is made possible, we will also allow the execution of dynamic tests. To do so, the developer will have to submit its own tests to the Testbed's Local Test Repository. For this, the developer will submit the tests on the 5GASP portal, which will then forward these tests to the LTRs, via E5 interface.

5.2.5.6 E6 - Interface for facility interaction with CI/CD

This section will contain description about the E6 interface.
This interface enables the communication between the master TEE and slave TEEs. Once a test job is submitted to the master TEE, it will use interface E6 to forward these jobs to the slave TEEs, deployed at each facility. After performing the testing jobs, the slave TEEs will use, once again, this interface, to send the testing results back to master TEE.
Regarding the availability of the interface, it follows the same premise of interface E3, where all traffic occurs inside a Wireguard, VPN tunnel.

5.2.5.7 E7 - Inter-facility Interface connectivity

This interface enables the communication between any two 5GASP facilities at the data-plane level. This interface depends on control plane interface E4 and is based on IP over IP tunnels using OSS VPN Wireguard. Interface E4 will provide the endpoints and security credential necessary to connect sites peer-to-peer, providing maximum compatibility and assuring interconnection of site networks to peer-site networks for inter-facility connectivity over the internet.

5.3 User community interaction portal

The NetAppCommunity Portal will be an interactive UI application that hosts documentation, knowledge-base, common questions and answers, as well as a developer forum that allows thread-centric cooperation on topics related to creating deployment descriptors, deploying NetApps to the service, interacting with the 5GASP services, and common troubleshooting.
The structure of the NetAppCommunity Portal is shown in *Figure 55*.

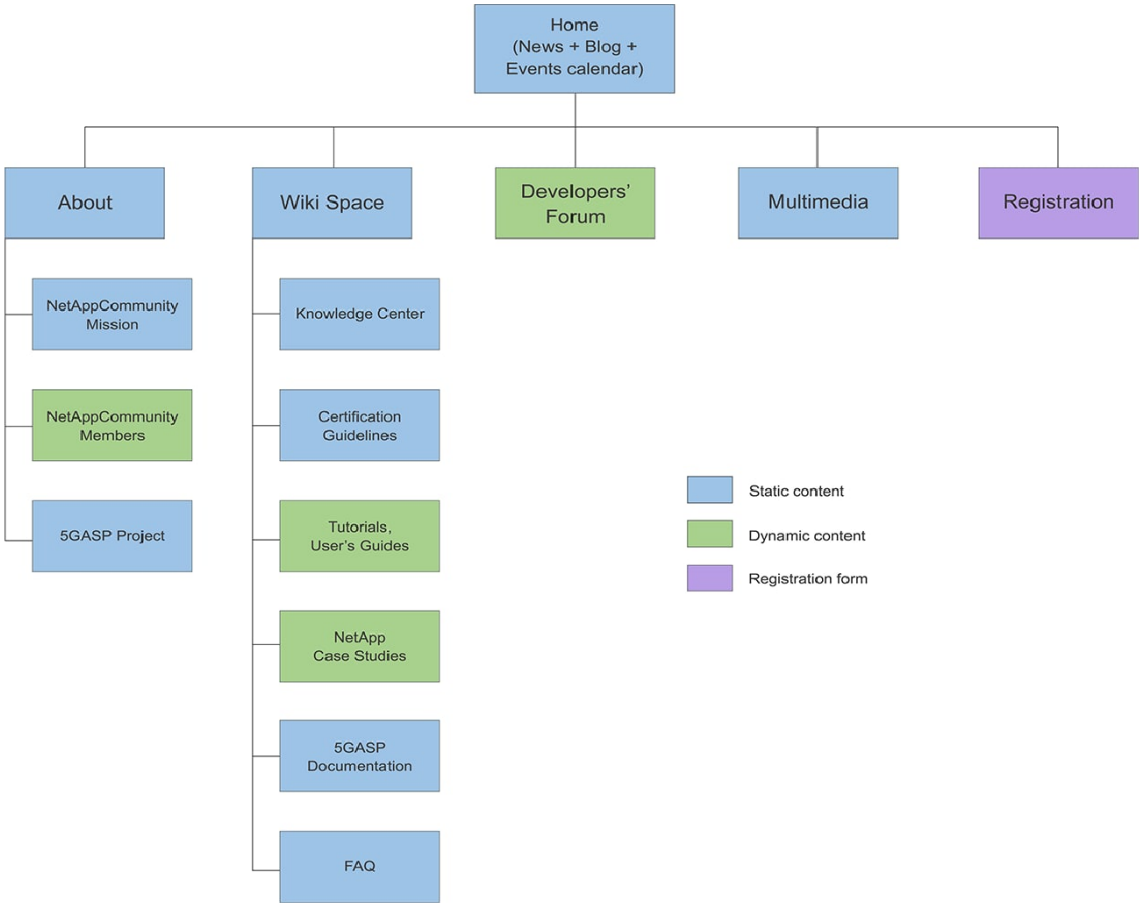


Figure 55 NetAppCommunity Portal sitemap

The "*About*" section presents the generic information on the Community and 5GASP project. The purpose of "*Wiki Space*" section is to provide users with wide range of information useful for NetApp product developers and consumers. The Development Forum is aimed at support of the Community discussions. The Public Repository of Experiments presents examples of NetApps; currently this section provides the descriptions of 5GASP NetApps which are under development and validation.

The NetAppCommunity Portal is complementary to the NetAppStore portal which is one of 5GASP innovative solutions for business. The NetAppStore portal provides operational information collected automatically during the NetApps' independent testing on the 5GASP platform. The structure of the NetAppStore Portal is shown in *Figure 56*.

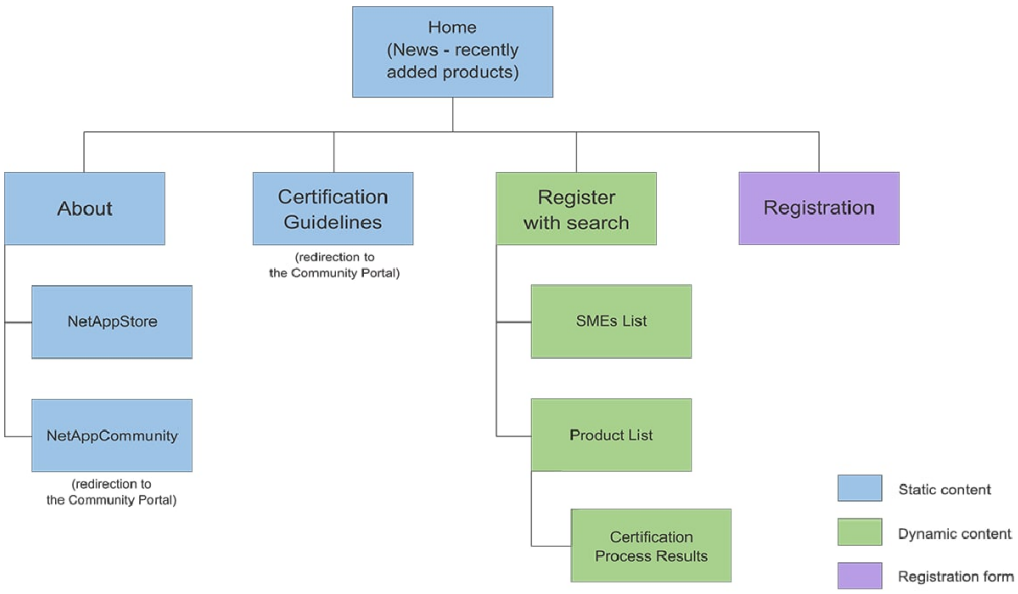


Figure 56 NetAppStore Portal sitemap

The NetAppStore will support business around NetApps, NFs and NSs. It will provide a public registry of SMEs and their reusable products: NetApps, NFs and NSs. The information on the NetAppStore portal will be provided by the 5GASP platform independently from NetApp developers and Network Operators. Such information is collected automatically from a pool of testbeds that run tests defined by various entities.
The NetAppStore and NetAppCommunity portals will be detailed further in WP6 (task 6.1).

5.4 5GASP experimentation API service

The behavior of the programmable interfaces that govern experimentation has been presented in *5.2.1 Section* and *5.2.3 Section*. The high-level flow is that developers performing experiments through the 5GASP service will first step through the NetApp NODS and its implementation of the several relevant Open API-based protocols for service catalog management and manipulation. As part of this onboarding process of the NetApp to the 5GASP portal, the developer will provide alongside a testing descriptor that defines which tests the CI/CD service would run to validate the NetApp. Results of these tests would be available from the CI/CD orchestrator that delegates to each testbed and programmatically reachable through the facility's LTR, along with reports and log files related to each run. These will be accessible from the Representational State Transfer (RESTful) interface of the orchestrator.

5.5 The experiment service orchestrator

While the actual deployment of the NetApps is under the scope of WP3, as described in *5.2.3 Section* and *5.2.5.2 Section*, 5GASP will feature a distributed CI/CD service to facilitate testing of the NetApps in the selected facilities. The services will feature a primary/secondary design, the primary residing in the 5GASP infrastructure and secondaries deployed over the facility test sites. Internally, the 5GASP services will communicate to the primary, which will schedule

and relay the test (as part of the NetApp descriptors) to be executed at the secondary nodes, close to the deployment of the NetApp in a given facility.

5.6 Multi-domain

One of 5GASP objectives is to provide a solution to instantiate an E2E Service across multiple domains without prior negotiations. That is technically possible by using an E2E Network Slice composed of NSs or Network Slices. There are three distinct options for the E2E Network Slice: its subnets are composed of NSs; its subnets are composed of other Network Slices; finally, or there is a hybrid approach, where its subnets are comprised partially by NSs and Network Slices. Each of those approaches can generate the same Network Slice architecture, where the differencing factor is the abstraction level of the entities deployed at each domain. To better understand some of the possible architectures of that E2E Network Slice, *Figure 57* presents the NS and the NSI approach.

In 5GASP we will connect the independently E2E Network Slice Subnets by creating and configuring a VPN tunnel between them, providing a secure channel where the communication between domains can successfully occur. For this project and use cases, the technology chosen to implement this VPN tunnel was Wireguard, a state-of-the-art and minimalist framework that allows the rapid instantiation and configuration of VPNs. Contrary to federation that pre-establishes communication channels between areas, a VPN tunnel is necessary for the multidomain mechanism to create a communication channel between independent domains.

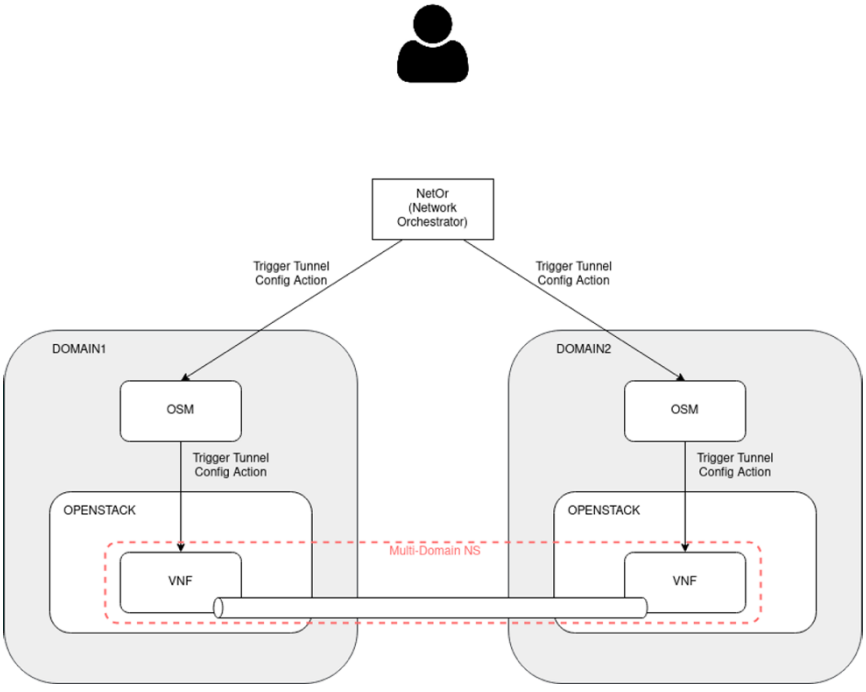


Figure 57 Multi-domain: secure overlay network

To successfully achieve this innovation, not only the network resources (NSs and NSIs) need to be aligned with this mechanism, but there must exist a third-party entity, preferentially outside all domains in question, that will allow the connection of the tunnel peers. That agent

will receive and process the dynamic tunnel endpoints information and exchange it with the remaining peers, effectively completing the tunnel configuration. We name this agent NetOr (Cross Domain Network Orchestrator), this entity can conceptually be a third party or one of the involved domain operators. NetOr, in addition to all the other features and functionalities it provides, also gathers and redistributes the tunnel information according to peers.
Figure 58 presents the expected data flow between the NetOr and the various domains.

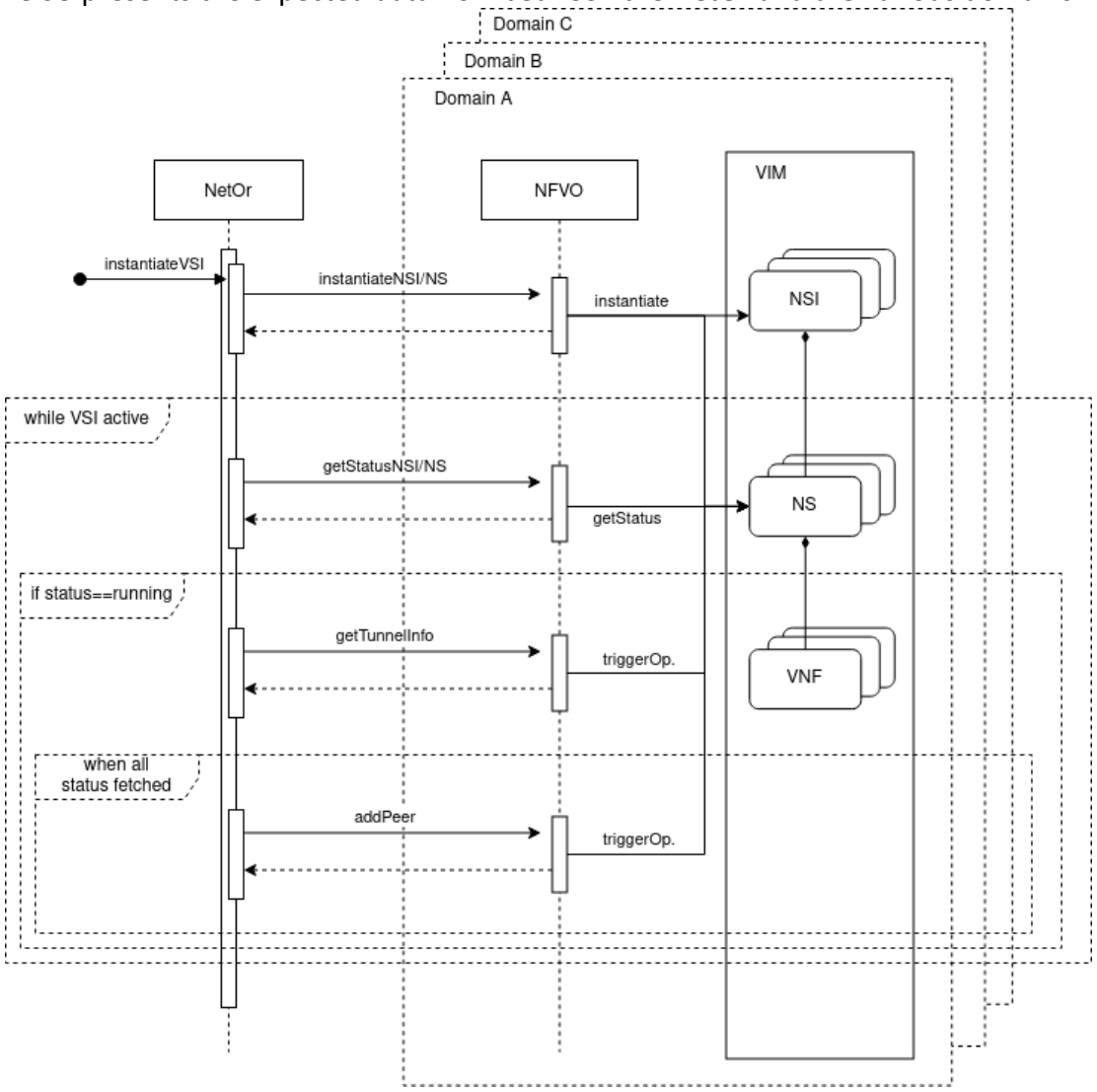


Figure 58 Data Flow between NetOr and respective Domains

As presented in *Figure 58*, the process starts by instantiating a Vertical Service based on blueprints, descriptors, and templates that support and activate the inter-domain mechanism. With that request, the system creates all necessary management entities and instantiates the network resources (NSIs or NSs) in the respective domains. After instantiating the Vertical Service, there is continuous polling over the status and information of its components. When the NetOr system verifies that a Vertical Service component is ”*running*” (meaning that it is deployed and configured), it triggers a runtime operation to fetch the tunnel information, such as the IP of the tunnel peer machine and the self-generated tunnel public key. Once all the Vertical Service components are ”*running*” and their tunnel information fetched, the NetOr proceeds to exchange that information between peers,

effectively providing the necessary data to peers and configuring the tunnel in the process. Only the NetOr knows all tunnel peers since it instantiated them independently and on different domains.

5.7 Physical architecture: Disaggregated RAN, MEC

- **Disaggregated RAN**

To facilitate testing of NetApps exploiting 5G, each 5GASP facility is equipped at a minimum with a RAN, MEC, 5G Core network, compute capabilities at all MEC and core sites and a transport network interconnecting all these. Here we mention the approach of disaggregated RAN as a first step towards OpenRAN and its benefits in 5GASP. The concept of a disaggregated RAN architecture refers to a 5G gNB split into three parts: a Centralized Unit (CU), a Distributed Unit (DU) and a Radio Unit (RU), a concept adopted by the O-RAN alliance as shown in *Figure 59*. The RU hosts parts of the physical (PHY) layer functions, including beamforming[72]. The DU hosts the Radio Link Control (RLC) layer, the Medium Access Control (MAC) layer, and parts of the PHY layer. The CU hosts Radio Resource Control (RRC), Service Data Adaptation Protocol (SDAP) and Packet Data Convergence Protocol (PDCP) functions.
Each CU is connected to multiple DUs, where each DU in turn is connected to multiple RUs[73]. This split allows resource pooling as well as centralized scheduling, where each of these components can be provided by different vendors democratizing the RAN ecosystem. Furthermore, as an evolution of Cloud RAN, the CU and DU converge to becoming virtualized, thus allowing agility and flexibility while deploying RAN solutions on COTS hardware[74].

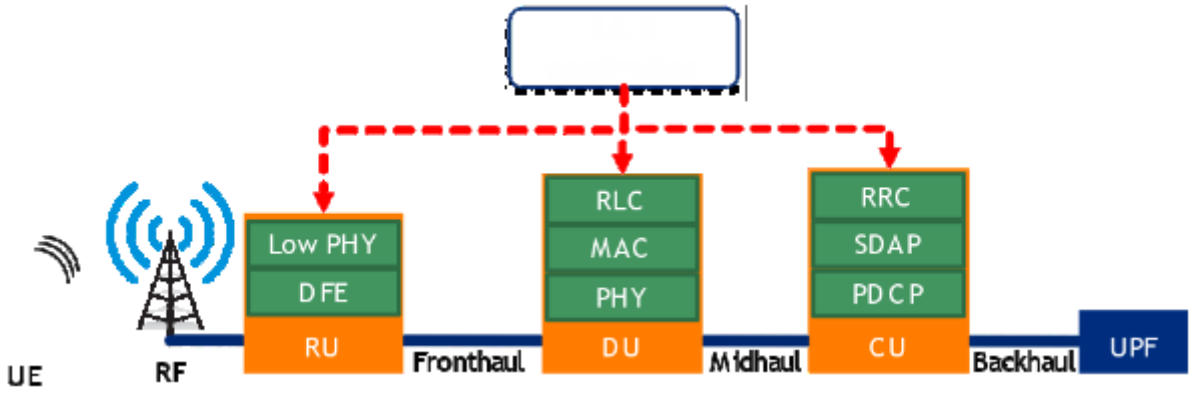


Figure 59 Disaggregated RAN where a RAN controller is responsible for reserving resources and deploying QoS flows from the UE to the CU

- **Multi-access edge computing**

The concept of MEC has been briefly introduced in *2.1* and *2.7 Sections*. To re-iterate, MEC enables NetApps with very low latency requirements to be hosted near the UEs where they are hosted in a compute environment at the edge. This allows the UEs to offload compute intensive tasks to the MEC system.
We briefly describe here the MEC architecture as proposed by ETSI in *Figure 60* including its various elements and reference points and how it can be integrated within a 5GASP facility. This architecture is based on three levels: MEC host, MEC system level and MEC host-level management[75]. The components at the MEC host are located at each edge site. They include the virtualization infrastructure to provide the compute, storage and network capabilities to

host the MEC applications, which are analogous to NetApps, as well as the MEC platform. The latter provides functionalities to enable the deployment of MEC applications as well as enabling these applications to provide or consume MEC services. These services include the influencing of traffic rules at the data plane received from the MEC apps themselves or the MEC platform manager (MEPM); maintaining Domain Name System (DNS) records from MEPM and acting as a DNS proxy/server.
The MEPM manages the lifecycle of applications, providing element management functions to the MEC platform and managing application rules and requirements. The MEC orchestrator maintains an overall view of the MEC system and is also responsible for onboarding and deploying MEC applications as well as the relocation of applications upon need.

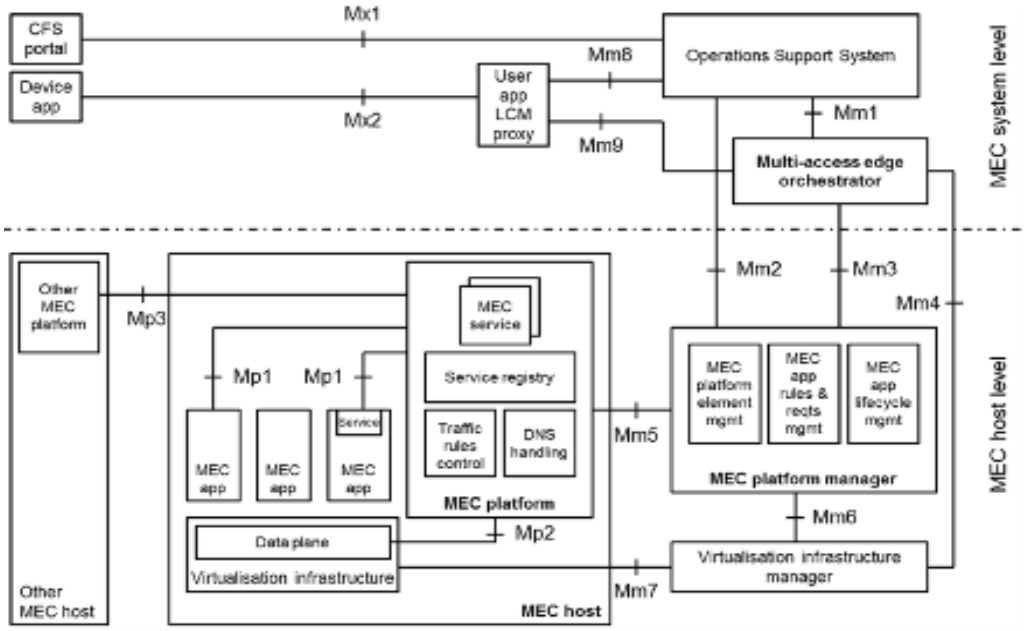


Figure 60 ETSI MEC reference architecture

The services provided by the MEC platform or other MEC applications can be used to enable innovative NetApps to be co-located at the MEC host. These services may include radio network information, location specific information of the UE(s), bandwidth management and traffic steering services. With regards to 5GASP, the MEC orchestrator can be used to deploy the NetApps and allow services to be exposed to it via the MEPM.

- **MEC and Disaggregated RAN integration/ MEC and Disaggregated RAN integration provisional plan**

The integration of MEC system with 5G is inevitable to reap the full benefit of NetApps hosted as MEC applications. This requires the MEC orchestrator to act as an Application Function to interact either with the Network Exposure Function (NEF) or other 5G NFs in the 5G core to facilitate MEC integration with 5G[76]. This includes *traffic steering*, such that the MEC platform acting as a 5G Application Function can interact with the 5G core to eventually have the traffic from the UE reach a MEC application, where the Session Management Function (SMF) in the 5GC can configure traffic rules at a particular UPF as shown in *Figure 61*. This is also enabled by the fact that the UPF, which is part of the 5G network data plane, can be deployed flexibly at the edge site. For the radio network information, the MEC platform can be integrated with

the RAN controller – and as we converge to OpenRAN, with the nRT-RIC to receive the information from the RAN elements and possibly to align its own management and control decisions with RAN controller decisions.

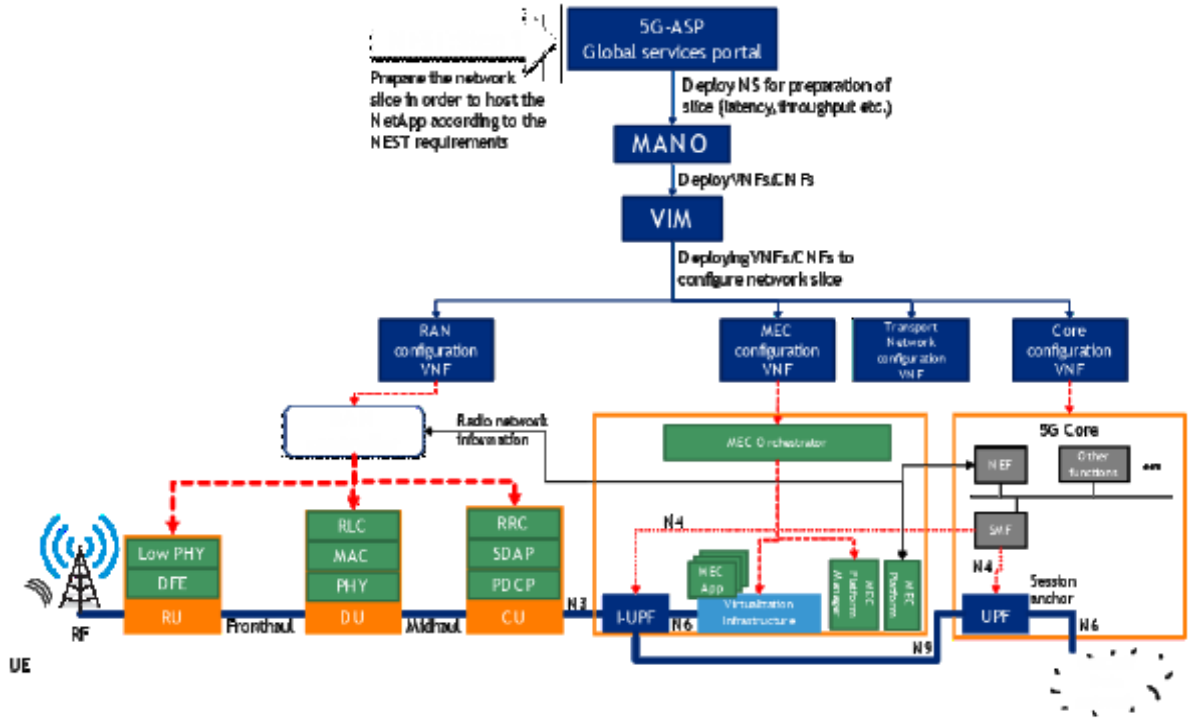


Figure 61 5GASP facility configuration

In the 5GASP context, as described in *4.2 Section*, for the network slice to be prepared, a potential way is to have each facility NFVO deploy a network service. This network service includes functionality to reserve resources and to deploy connectivity on the RAN, transport network, the 5G core as well as the MEC system before the actual NetApp is deployed, where the information about these resources can be used as network slice instantiation parameters, or the configuration of network service when the VNFs start, as shown in *Figure 61*. This architecture is loosely defined and can be adapted based on each facility's capabilities and functionality. Using this architecture, the RAN controller (which reserves radio resources on the RU, DU and CU) may receive the QoS requirements for the slice preparation, which may be translated to the deployment of QoS flows from a UE to the CU. The core network may deploy a UPF either at the core side or an intermediate Initial UPF (I-UPF) at a MEC host as dictated by slice requirements where an N9 interface exists between these UPFs. Furthermore, the MEC orchestrator can be leveraged to configure traffic routing from UPF to specific a MEC host, such that when a deployed NetApp can receive traffic from the UPF.

5.8 NetApp workflows

5.8.1 NetApp deployment workflows

5GASP will provide an automated deployment procedure that will be transparent to the developer using the service. By doing so, the knowledge about deployment insights required from the experimenter will be significantly reduced. However, the full functionality of the automated deployment of NetApps will be achieved at later stages of the project. This is

because the onboarding process is a necessary previous step of the deployment workflow, and it will be partly manual in the first version of the 5GASP portal. At the beginning, the developer uploads each descriptor of the triplet one by one. When the network slice descriptor is submitted, the 5GASP portal will offer to the user a list of target facility sites that fulfil the network requirements needed by the NetApp and the experimenter will select one of them, where the NetApp will be deployed. Further on in the timeline of the project, when the descriptors are uploaded in a package, the 5GASP ecosystem will automatically select the site which better suites the network necessities of the NetApp. The onboarding details are deeply examined in WP4, thus further details can be found in task 4.1.
In 5GASP, the NetApps deployment process is triggered by the 5GASP portal once the onboarding procedure is performed. In *Figure 62*, it can be seen that the deployment step is started in the corresponding facility after the NetApp onboard.

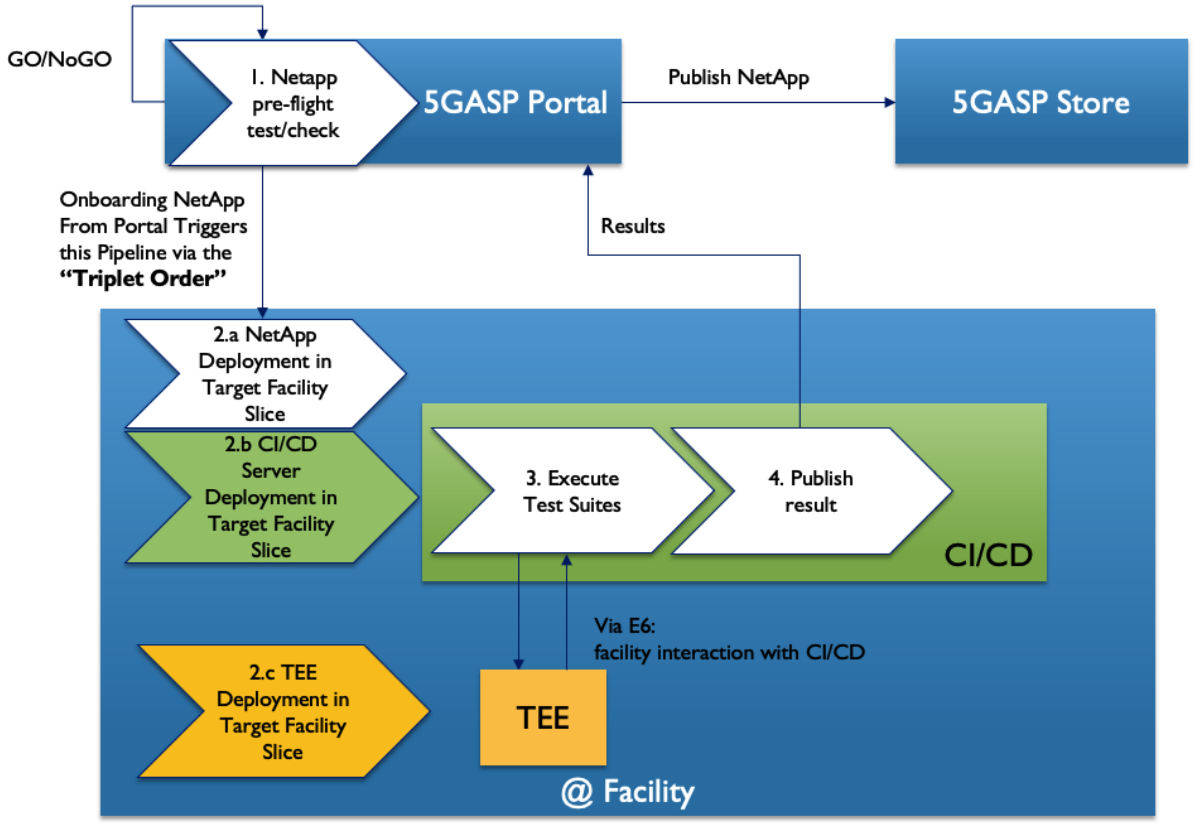


Figure 62 5GASP NetApp Deployment Workflow

As it can be seen in the *Figure 62* , the deployment of the NetApp is performed with an already executed series of pre-flight tests, that check the validity of the descriptors included in the Triplet Order. Depending on the nature of the NetApp, we can distinguish two different scenarios when talking about the deployment scenario: single-domain NetApps and multi-domain NetApps.
NetApps deployed in a single domain scenario will be the most common configuration during the development of the project. In this case, the 5GASP portal sends the required deployment information to the target facility site, which is received by the NFVO and the network slicing infrastructure manager. Once the network resources requested are reserved, the NetApp is

instantiated on top of the configured network slice. Then the CI/CD server that will be used for the testing procedure is also deployed.
In the scenario of multi-domain NetApps, the procedure is almost the same, with the difference that the 5GASP portal has to send the deployment information of the VNFs and the network to each corresponding target facility site.
Regardless the type of scenario, once the deployment has been established and confirmed by the site/s, the CI/CD service receives the deployment data and the testing phase can start.

5.8.2 NetApp testing workflows

The automation onboarding process in 5.8.1 Section is included in the full automation testing procedure to deploy NetApp and TEE in the target Facility. 5GASP Store is the main automation management for Test Plan, Auto Certification, Test Report, NetApp Publishmanet and Certificate Publishment. It will be partly manual in the first version of the 5GASP Store. The workflow is defined as shown in *Figure 63*.

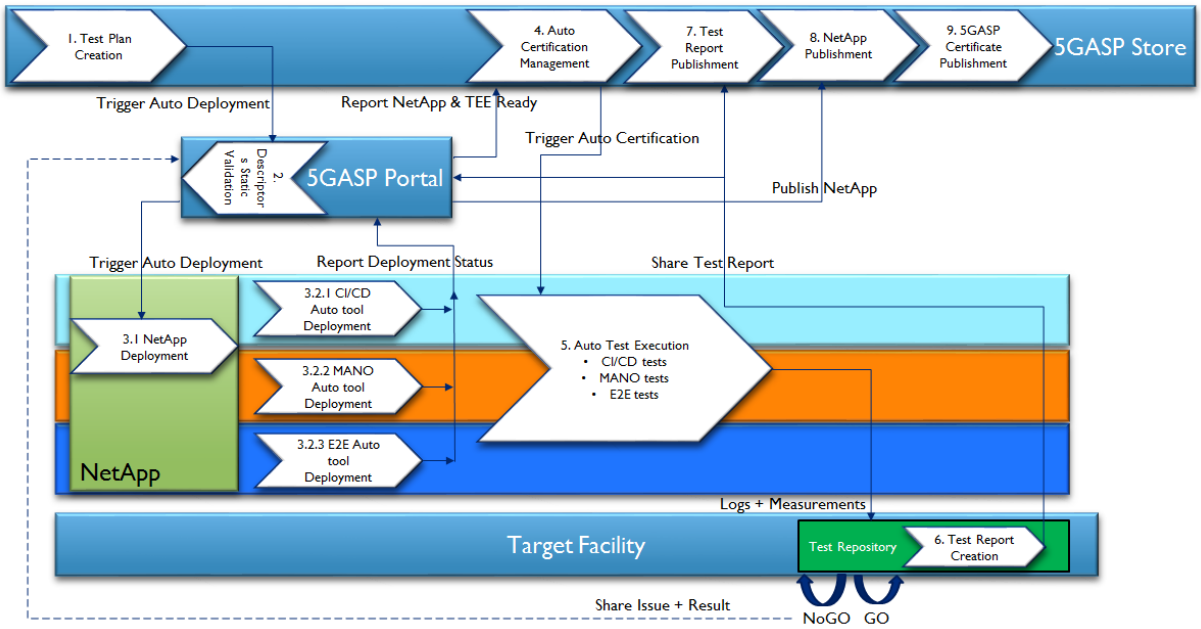


Figure 63 5GASP Automation Testing workflow

- In the beginning, the tester should create a Test Plan including the certification processes (i.e., Test Cases), the target Facility, the recommended Test Tools and the expected execution timeline. 5GASP Store will automatically upload the triplet descriptors of the NetApp and the Test Tools one by one to 5GASP Portal.
- 5GASP Portal should validate these descriptors. If the static validation is successful, 5GASP should trigger Auto Deployment to the target Facility as defined in *5.8.1 Section*.
- NetApp and TEE with the recommended Test Tools should be auto deployed in the target Facility. Currently, there are 3 pre-defined test domains, CI/CD testing for the NetApp functional and Developer dedicated tests, MANO testing for the MANO functional and NFVI performance tests, and E2E testing for the performance tests of

Network slice and application traffic. MANO should report the deployment status to 5GASP Portal. And then 5GASP Portal should report the readiness to 5GASP Store.

- 5GASP Store should start the Auto Certification process based on Test Plan and trigger the Auto Test Execution by uploading the Test Catalog (i.e., test config and scripts) to TEE in the target Facility.
- TEE should store the test catalog to Test Repository and then start the auto Test Execution for the tests of all the test domains. After each round of the tests, TEE should also store the logs and measurements to Test Repository.
- Test Repository should share the logs and results to 5GASP Portal when any test is not successful; Test Repository should create and share Test Report to both 5GASP Portal and 5GASP Store when all tests are successful.
- (Optional) NetApp Developer should do the troubleshooting and update NetApp when the logs and results are shared by Test Repository.
- 5GASP Store should publish Test Report when Test Report is shared by Test Repository.
- 5GASP Portal should trigger NetApp Publishment to 5GASP Store by uploading the certificated NetApp.
- 5GASP Store should publish the certificated NetApp.
- 5GASP Store should publish a 5GASP Certificate.

The test catalogs, logs, measurements, results and test reports have to be protected in Test Repository until the end of 5GASP project. The details of automation testing and test tools are deeply defined in WP5, thus further details can be found in deliverable 5.3.

Automation testing in a single domain scenario will be the most common configuration during the certification of 5GASP project. In this case, the 5GASP Store sends the required testing information via 5GASP Portal to the target facility site, which is received by the NFVO and the network slicing infrastructure manager. Once the network resources requested are reserved, the NetApp and TEE are instantiated on top of them.

In the scenario of multi-domain NetApp certification, the procedure is almost the same, with the difference that the 5GASP portal has to send the deployment information of the VNFs and the network to each corresponding target facility site.

6 Conclusions

The main goal of this document is to define and design a general architecture of the 5GASP project with all the main components and particular capabilities, so as to serve as a foundation and guiding principle to the rest of the project modules, WPs. Its intent is to be revised towards the end of the project (M30) as part of D2.3, and the delta of architectural plan and specific considerations needed to be taken during the implementation phase, to be captured and used as lessons-learned for NetApp development and deployment.

To achieve our goal, first of all we have deeply analyzed in *Section 1*, the most relevant related projects, open source projects and standards to consider, in order to create a clear and common approach for our future direction of this architecture deliverable and for the entire project.

The document proceeds to address important aspects and components of the project which represents the foundation for future deliverables of other WPs of the project, such as: multi-domain, DevOps context: CI/CD pipeline, internal and external interfaces, user interaction portal, the experiment service orchestrator, 5GASP experimentation API service and NetApp testing workflows.

To define all those important components, we have analyzed very carefully in *Section 2* each NetApp-specific requirements and architecture using a project template consisting of four sections: demonstration environment (description), NetApps' high-level infrastructure, NetApps' KPIs and overall integration needs.

In Section 3 we have detailed all the main architectures and the capabilities of each of the six experimentation facilities infrastructures involved in the project.

Taking the input from the NetApps' requirements and infrastructures (*Section 2*), and the architectures and capabilities of the experimentation facilities (*Section 3*), we have defined the detailed architecture, the internal and external components and their interfaces, the exposed APIs and the user management interface and requirements.

In *Section 4* we have described the experimental model, the NetApps deployment and orchestration, the DevOps (CI/CD) context and 5GASP Model Entities (Roles).

Section 5 presented the 5GASP Infrastructure Architecture, by detailing the 5GASP Global Infrastructure Architecture, 5GASP Internal and external components and their interfaces, the 5GASP experimentation API service, the experiment service orchestrator, multi-domain, physical architecture and NetApp workflows: NetApp deployment workflows and NetApp testing workflows.

As discussed in the document, most of the interfaces and process details defined in the deliverable will be implemented in other WPs and reported in subsequent deliverables. For example, in WP3 and deliverable 3.1, the defined onboarding process and the E1 to E5 and E7 external interfaces, will be implemented by the portal and its external services. In addition, the models and the APIs defined will be implemented by tasks of WP3. The development and support (including content creation and updating) of the NetAppCommunity and NetAppStore portals will be provided within WP6 (Task 6.1), and the content of the NetAppCommunity portal will be created within WP7.

References

[1] 5GASP proposal

[2] https://5g-ppp.eu/

[3] https://5ginfire.eu/

[4] https://www.5g-vinni.eu/

[5] http://5gtours.eu/

[6] https://www.matilda-5g.eu/

[7] http://5gdrones.eu/

[8] https://5genesis.eu/

[9] https://www.5g-eve.eu/

[10] http://5gheart.org/

[11] http://www.5gmediahub.eu/

[12] https://5g-ppp.eu/5g-iana/

[13] https://www.5g-mobix.com/

[14] https://secredas-project.eu/

[15] https://www.5gepicentre.eu/

[16] http://www.ppdr-tc.eu/

[17] https://sonata-nfv.eu

[18] https://github.com/sonata-nfv

[19] http://ngpaas.eu/

[20] https://www.5g-picture-project.eu

[21] https://www.5g-picture-project.eu/publication_open_source.html

[22] https://github.com/CN-UPB/Cloud-NFV-Orchestration/

[23] http://5g-transformer.eu/

[24] https://5growth.eu/

[25] https://5growth.eu/open-source/

[26] https://github.com/5growth

[27] https://www.fiware.org/

[28] https://openslice.readthedocs.io/

[29] https://testproject.io

[30] https://www.gsma.com/futurenetworks/wp-content/uploads/2020/01/2.1_Network-Slicing-Use-Case-Requirements-Booklet-1.pdf

[31] https://www.gsma.com/futurenetworks/wp-content/uploads/2020/01/3.0_Characterisation-of-Network-Slices.pdf

[32] TM Forum, “TMF IF1167 – ODA Functional Architecture”, 2020

[33] TM Forum, “GB999 – ODA Production Implementation Guidelines”

[34] TM Forum, “TMF 633 – Service Catalog Management”

[35] TM Forum, “TMF 641 – Service Ordering Management”

[36] TM Forum, “TMF 638 - Service Inventory Management”

[37] TM Forum, “TMF909A – API Suite Specification for NaaS”

[38] 3GPP TS 23.501

[39] 3GPP TS 23.502

[40] 3GPP TS 23.503

[41] 3GPP TS 28.530

[42] 3GPP TS 28.531

[43] 3GPP TS 28.532

[44] 3GPP TS 28.533

[45] 3GPP TR 28.801

[46] 3GPP TS 28.541

[47] GSMA, “NG.116 Generic Network Slice Template v4.0” https://www.gsma.com/newsroom/wp-content/uploads//NG.116-v4.0-1.pdf

[48] 3GPP TS 23.222

[49] ETSI, "Network Operator Perspectives on NFV priorities for 5G", White Paper, 2017

[50] ETSI NFV ISG, "GS NFV-MAN 001, Network Functions Virtualisation (NFV); Management and Orchestration, v1.1.1" ,2014

[51] ETSI NFV ISG, "GR NFV-EVE 012, Evolution and Ecosystem; Report on Network Slicing Support with ETSI NFV Architecture Framework, v3.1.1," 2017

[52] 3GPP, "TS 28.500 v.16.0.0, Management concept, architecture and requirements for mobile networks that include virtualized network functions", 2020

[53] ETSI NFV ISG, "ETSI GS NFV-IFA 012, Network Functions Virtualization (NFV) Release 3; Management and Orchestration; Os-Ma-nfvo reference point - Interface and Information Model Specification, v3.1.1", 2018

[54] ETSI NFV ISG, "ETSI GS NFV-IFA 008, Network Functions Virtualization (NFV) Release 3; Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification, v3.1.1", 2018

[55] ITS station communication architecture for Intelligent Transport Systems. ISO TC 204. International Standard ISO number 21217. Last edition 2020

[56] Cooperative intelligent transport systems (C-ITS) Guidelines on the usage of standards, https://www.itsstandards.eu/app/uploads/sites/14/2020/10/C-ITS-Brochure-2020-FINAL.pdf, June 2020

[57] European Commission. C-ITS platform phase II: Cooperative Intelligent Transport Systems towards Cooperative, Connected and Automated Mobility, Final Report,

https://ec.europa.eu/transport/sites/transport/files/2017-09-c-its-platform-final-report.pdf/

https://ec.europa.eu/transport/themes/its/c-its_en, September 2017

[58] C-Roads – The Platform of Harmonized C-ITS Deployment in Europe, http://www.c-roads.eu, 2019

[59] https://5ginfire.eu/surrogate/

[60] ETSI EN 302 665 - edition 2010

[61] https://5ginfire.eu/migrate/

[62] "5G Vision: 100 Billion connections, 1 ms Latency, and 10 Gbps Throughput", Huawei 2015 (http://www.huawei.com/minisite/5g/en/defining-5g.html)

[63] N. Uniyal, A. Bravalheri, S. Wu, W. Featherstone, X. Vasilakos, D. Warren, R. Nejabati and D. Simeonidou, "Intelligent Mobile Handover Prediction for Zero Downtime Edge Application Mobility," submitted to IEEE Globecom 2021

[64] X. Vasilakos et al., "Towards Zero Downtime Edge Application Mobility for Ultra-Low Latency 5G Streaming," 2020 IEEE Cloud Summit, 2020, pp. 25-32

[65] ETSI System Architecture for the 5G System (3GPP TS 23.501 version 15.3.0 Release 15), Sept 2018

[66] https://www.geant.org/

[67] https://patras5g.eu

[68] https://www.ruggear.com/company/worth-knowing/ip67-and-ip68.html

[69] ETSI NFV ISG, "GR NFV-IFA 029, Architecture; Report on the Enhancements of the NFV architecture towards "Cloud-native" and "PaaS", v3.3.1," 2019

[70] TM Forum, “TMF 634 - Resource Catalog Management”

[71] TM Forum, “TMF 638 - Resource Inventory Management”

[72] S. Sirotkin, “5G Radio Access Network Architecture,” John Wiley & Sons, 2021

[73] C. Cox, “An Introduction to 5G: The New Radio, 5G Network and Beyond,” John Wiley & Sons, 2020

[74] ETSI White Paper No. 23, "Cloud RAN and MEC: A Perfect Pairing,” February 2018

[75] ETSI GS MEC 003 V2.2.1, “Multi-access Edge Computing (MEC); Framework and Reference Architecture,” Dec 2020

[76] ETSI White Paper No. 28, "MEC in 5G networks,” June 2018