Project funded by the Horizon 2020 Framework Programme of the European Union,

Grant agreement Nº: ***951947.***

Start date: **01/09/2020.**

Duration: **48 months**

D3.3. First release of 5GMED ICT Infrastructure

WP	WP3
WP Leader	CELLNEX
Responsible Author	Arslane HAMZA-CHERIF (VEDECOM)
Contributors	I2CAT, AXBY, CMS, CLNX, HSP, IRT, NBC, VLO, VEDE, CTTC
Dissemination Level	PU
Nature	RE

Dissemination Level:	
PU	Public
PP	Restricted to other programme participants (Including the Commission Services)
RE	Restricted to a group specified by the consortium (Including the Commission Services)
CO	Confidential, only for members of the consortium (Including the Commission Services)

Nature	
PR	Prototype
RE	Report
SP	Specification
TO	Tool
OT	Other

Synopsis	Deliverable D3.3 represents the developments of the 5GMED ICT infrastructure that have been deployed in the testbeds for the first validation and small-scale trials of the project use cases.

	In addition, this document also provides a detailed insight on the end-to-end 5GMED cross-border network architecture, which was previously introduced in D3.2, and its deployment at the small-scale testbeds of Castellolí, Paris, and railway cross-border corridor, including the implementation of the 5G network infrastructure, orchestration, and slicing components to validate them in the small-scale test sites. The results of the configuration and integration on the developments presented in this deliverable will be reported in D6.2.
List of Keywords	5G, C-V2X, satellite, architecture, small-scale test site, orchestration, multi-connectivity, network slicing.

Funded by the Horizon 2020 Framework Programme of the European Union

DOCUMENT HISTORY

Version	Status[1]	Date	Comments	Author
1.0	Draft	02/12/2022	Creation of the ToC and initial contribution	Thiwiza BELLACHE
1.1	Draft	31/01/2023	Collection of first contributions	Multiple contributors
1.2	Draft	14/04/2023	Collection of all contributions	Multiple contributors
1.3	Draft	20/04/2023	Available version for internal peer review	Arslane HAMZ-CHERIF
1.4	Draft	03/05/2023	Draft revision following internal peer review	Multiple contributors
1.5	Draft	08/08/2023	Collection of new & complementary contributions	Multiple contributors
1.6	Draft	28/08/2023	Available version for internal peer review	Arslane HAMZ-CHERIF & José López Luque & Francisco Vázquez-Gallego
1.7	Issued	03/10/2023	Final version. Document ready for submission	Multiple contributors

Authors in alphabetical order		
Name	Organization	Email
Alberto Gutiérrez Hernández	CELLNEX	alberto.gutierrez@cellnextelecom.com
Andrés Cárdenas Córdova	I2CAT	andres.cardenas@i2cat.net
Angelos Antonopoulos	NBC	aantonopoulos@nearbycomputing.com
Arslane HAMZA-CHERIF	VEDECOM	arslane.hamzacherif@vedecom.fr
Estela Carmona Cejudo	I2CAT	estela.carmona@i2cat.net
Francisco Vázquez-Gallego	I2CAT	francisco.vazquez@i2cat.net
Jad Nasreddine	I2CAT	Jad.nasreddine@i2cat.net
José López Luque	CELLNEX	jose.lopez.luque@cellnextelecom.com
Juan Agusti Moreno	COMSA	juan.agustimoreno@comsa.com
Judit Bastida Raja	CELLNEX	judit.bastida@cellnextelecom.com
Kévin Nguyen	VALEO	kevin.nguyen@valeo.com
Kurdman Abdulrahman Rasol	I2CAT	kurdman.rasol@i2cat.net
Luca Petrucci	AXBYD	petrucci@axbryd.com

[1] Status (a status is associated to each step of the document life cycle)
Draft. This version is under development by one or several partner(s)
Under review. This version has been sent for review
Issued. This version of the document has been submitted to EC

Authors in alphabetical order		
Name	Organization	Email
Luis Quintero Garcia	CELLNEX	luis.miguel.quintero@cellnextelecom.com
Maria A. Serrano	NBC	maria.serrano@nearbycomputing.com
Michalis Dalgitsis	NBC	mdalgitsis@nearbycomputing.com
Monika Valdez	NBC	mvaldez@nearbycomputing.com
Nuria Trujillo	HISPASAT	ntrujillo@hispasat.es
Philippe SEGURET	VALEO	philippe.seguret@valeo.com
Philippe VEYSSIERE	IRT	philippe.veyssiere@irt-saintexupery.com
Raul Muñoz	CTTC	raul.munoz@cttc.es
Ricard Vilalta	CTTC	ricard.vilalta@cttc.es
Thiwiza BELLACHE	VEDECOM	thiwiza.bellache@vedecom.fr

TABLE OF CONTENTS

LIST OF ACRONYMS

3GPP	3rd Generation Partnership Project
5G	5th Generation of Cellular Networks
5G NR	5G New Radio
5GC	5G Core Network
5QI	5G QoS Identifiers
AC	Alternating Current
ACS-GW	Adaptive Communication System Gateway
AIM	Artificial Intelligence Module
AMF	Access & Management Function
AP	Access Point
API	Application Programming Interface
AUSF	Authentication Server Function
AZ	Availability Zones
BBF	BroadBand Forum
BS	Base Station
CAM	Cooperative Awareness Message
CCAM	Cooperative Connected & Automated Mobility
CCTV	Closed-Circuit Television
CPM	Collective Perception Message
CRUD	Create, Read, Update, Delete
CSMF	Communication Service Management Function
C-V2X	Cellular-V2X
DAS	Distributed Antenna System
DC	Direct Current
DENM	Decentralized Environmental Notification Message
DL	Downlink
EC	European Commission
eCPRI	Evolved Common Public Radio Interface
EIRP	Effective Isotropic Radiated Power
eNB	Evolved Node B
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
EWBI	East/Westbound Interface
FO	Fiber Optic
FRMCS	Future Railway Mobile Communication System
GBR	Guaranteed flow Bit Rate
Geonet	Geo-networking
gNodeB	Next Generation Node B
GSMA	GSM Association
HRR	Home-routed Roaming
IaaS	Infrastructure as a Service
ICCID	Integrated Circuit Card Identifier
IM	Input Model
LBO	Local Breakout

LTE	Long Term Evolution
MCC	Mobile Country Code
MCM	Manoeuvre Coordination Message
MCS	Modulation & Coding Scheme
MEC	Multi-access Edge Computing
MNC	Mobile Network Code
MNO	Mobile Network Operators
MOCN	Multi Operator Core Network
N14	N14 interface between 2 AMFs
NAT	Network Address Translation
NBI	NorthBound Interface
NRF	Network Repository Function
NSMF	Network Slice Management Function
NSSAI	Network Slice Selection Assistance Information
NSSMF	Network Slice Subnet Management Function
NWDAF	Network Data Analytics Function
OBU	On-Board Unit
OCI	Open Container Initiative
OEM	Original Equipment Manufacturer
ONF	Open Networking Foundation
OP	Operator Platform
PDU	Protocol Data Unit
P-GW	Packet Data Network Gateway
PLMN	Public Land Mobile Network
QoS	Quality of Service
RAN	Radio Access Network
REST API	Representational State Transfer API
RSU	Roadside Unit
RX	Reception
S-GW	Serving Gateway
SMF	Service Management Function
S-NSSAI	Single NSSAI
SSTS	Small-Scale Test Site
TA	Tracking Area
TCU	Telematic Control Unit
TDD	Time Division Duplex
TMC	Traffic Monitoring Center
TX	Transmission
UC	Use Case
UDM	Unified Data Management
UE	User Equipment
UL	Uplink
UPF	User Plane Function
V2X	Vehicle-To-Everything
V2X-GW	V2X Gateway
VLAN	Virtual Local Area Network

LIST OF TABLES

LIST OF FIGURES

Funded by the Horizon 2020 Framework Programme of the European Union

EXECUTIVE SUMMARY

The present document, entitled "First release of 5GMED ICT Infrastructure", is the third deliverable of Work Package 3 and represents one of the main outputs of Task 3.3, Task 3.4, Task 3.5, and Task 3.6. The objectives of this deliverable are twofold. Firstly, it presents the detailed design of the 5GMED cross-border network architecture, complementing the initial design already described in D3.2 "5GMED ICT Infrastructure architecture" [1], by providing additional information regarding a revised architecture, which relies on key concepts such as the multi-layered cross-border network architecture, the neutral host approach, network slicing through the different tiers of a 5G network (radio, transport and core network) and lastly service management and orchestration for Multi-access Edge Computing (MEC). Secondly, it describes in a concise way how the 5GMED cross-border network architecture has been translated into a real deployment at each of the small-scale test sites for the automotive use cases (UCs) and the small-scale test site at the cross-border corridor for the railway use case.

In addition to those objectives, this document summarizes the main challenges and lessons learned through the difficult task of deploying 5G equipment and technologies from different vendors and integrating additional non-5G radio technologies. All of this, to implement a 5G cross-border network architecture able to guarantee service continuity and user experience, by reducing service interruption time and speeding the handover procedure, especially in cross-border scenarios where roaming occurs. Furthermore, it should be noted that such kind of architecture is crucial for the future adoption of Cooperative Connected and Automated Mobility (CCAM) in European cross-border corridors.

Finally, this document is in line with the project's timeline, which aims to proceed to an initial validation of the architecture based on the small-scale test sites, before moving to its final validation through the complete deployment on the cross-border corridor between France and Spain for large-scale trials. Considering this, the current document is a prerequisite for the initial tests and small-scale trials carried out by the Work Package 6, but it does not report the whole network infrastructure deployments that will be made in the cross-border corridor for the large-scale trials. In fact, this will be reported in the incoming deliverable D3.4 entitled "Final release of the 5GMED ICT Infrastructure".

Funded by the Horizon 2020 Framework Programme of the European Union

1. Introduction

1.1 Deliverable purpose

This document aims at describing and reporting the progress made on the implementation of the 5GMED cross-border network architecture at each of the test sites that will be used for the small-scale trials in both automotive and railway scenarios. To this end, first it describes in detail the 5GMED cross-border network architecture, and then it describes how this architecture is implemented at each test site.

It should be noted that the complete deployment of the 5GMED cross-border network architecture in the cross-border corridor for the large-scale trials is out of the scope of this document. In fact, this will be covered by the D3.4 document. This means that, the implementation of the 5GMED cross-border network architecture will go through two phases, a first phase in which it will be implemented at the small-scale test sites, and which is the aim of the current deliverable, and a second phase focusing on the large-scale trials, and which is the scope of the future D3.4.

Finally, it should be noted that the four 5GMED use cases (three automotive use cases and one railway use case) will be demonstrated at different test sites, with the Castellolí test site being the main one for the tests and trials of the automotive use cases. Table 1 illustrates where each use case will be validated and evaluated.

5GMED UC	UC type	Castellolí test site	Railway Cross-border test site	Paris-Satory test site
UC1	Automotive	Yes	-	Yes
UC2	Automotive	Yes	-	-
UC3	Railway	-	Yes	-
UC4	Automotive	Yes	-	-

Table 1: Mapping of 5GMED use cases with test sites for validation and performance evaluation in small-scale trials

1.2 Deliverable structure

This document is organized as follows. A description of the 5GMED cross-border network architecture is presented in Section 2, subsequently, an overview of the network architecture implementation at the Castellolí test site is presented in Section 3, followed by Section 4, that is devoted to the same topic but for the cross-border test site for the small-scale trials of the railway scenario, and then Section 5 for the Paris-Satory test site. Section 6 highlights the main challenges faced and lessons learned during the 5GMED network architecture deployment. Finally, Section 7 concludes the document.

Furthermore, in addition to these sections that are part of the main document, three Annexes are appended to the end of the document to further help the reader understand some important concepts. Specifically, Annex A: GSMA Operator platform is dedicated to GSMA Operator platform, Annex B: Exposure Gateway explains the concept Exposure Gateway, and Annex C: CAMARA API is dedicated to CAMARA API.

2. 5GMED Cross-Border Network Architecture

The 5GMED cross-border network architecture is depicted in Figure 1. It is composed of six layers that span across both sides of the Mediterranean cross-border corridor between Spain and France [1]. From bottom to top, the layers of the architecture are:

- Network Infrastructure layer.
- Multi-access edge computing (MEC) layer.
- Orchestration layer.
- Slice Management layer.
- Cloud layer.
- A Data Analytics layer that spans over the previous layers.

The 5GMED cross-border network architecture has been designed as an enabler to deploy multiple use cases simultaneously in cross-border scenarios with challenging orography via the integration of several cross-border/MNO interfaces, orchestration, 5G network slicing, Multi-access Edge Computing, and multi-connectivity elements. Furthermore, it should be noted that the cross-border interaction between the two MNOs (France and Spain) occurs at three different layers: network infrastructure layer, MEC layer, and orchestration layer.

The interaction between the network infrastructure layers is made through specific cross-border interfaces for 5G roaming and the implementation of a Neutral Host Infrastructure concept. An example of implementation of the Neutral Host Infrastructure concept in 5GMED is that the French 5G network infrastructure is designed for Multi Operator Core Network (MOCN) Radio Access Network (RAN) sharing, which is a cost-effective solution for MNOs. The MOCN scheme allows sharing the baseband, the radios of the gNodeBs, and even the frequency, which is very interesting in terms of deployment and usage of resources, resulting in a very sustainable architecture implementation. A Neutral Host approach ensures that a third party manages the gNodeB resources equally in terms of configuration, hardware, and frequency usage. Contrarily, the classical MOCN approach, where one MNO owns the site and another MNO is merely a guest, usually leads to performance disadvantages for the latter. The neutral host concept and MOCN scheme considered in the Network Infrastructure layer of 5GMED is further detailed in Section 2.1.2. 5GMED implements a realistic scenario in which two different MNOs use their own 5G network infrastructure, and a Neutral Host operator acts among them, managing the parametrization in the 5G RAN and the 5G Core to optimize the roaming process.

Table 4 summarises the parts of the 5GMED cross-border network architecture that are implemented in each test site and details some features of the implementations. Table 4 also indicates those parts in the network architecture layers that are presented at theoretical level. In the slice management layer, a theoretical design of slice federation is presented in Section 2.4.2.1 to facilitate cross-border network slicing continuity across different MNOs. Network slicing is implemented statically with slices directly configured on the 5G RAN, transport, and Core networks. For this reason, the RAN and Transport Network controllers inside the orchestration layer are proposed at conceptual level in Section 2.3. In the MEC layer, a theoretical design of MEC federation is proposed in Section 2.2.2 to facilitate cross-border communication between MEC application instances.

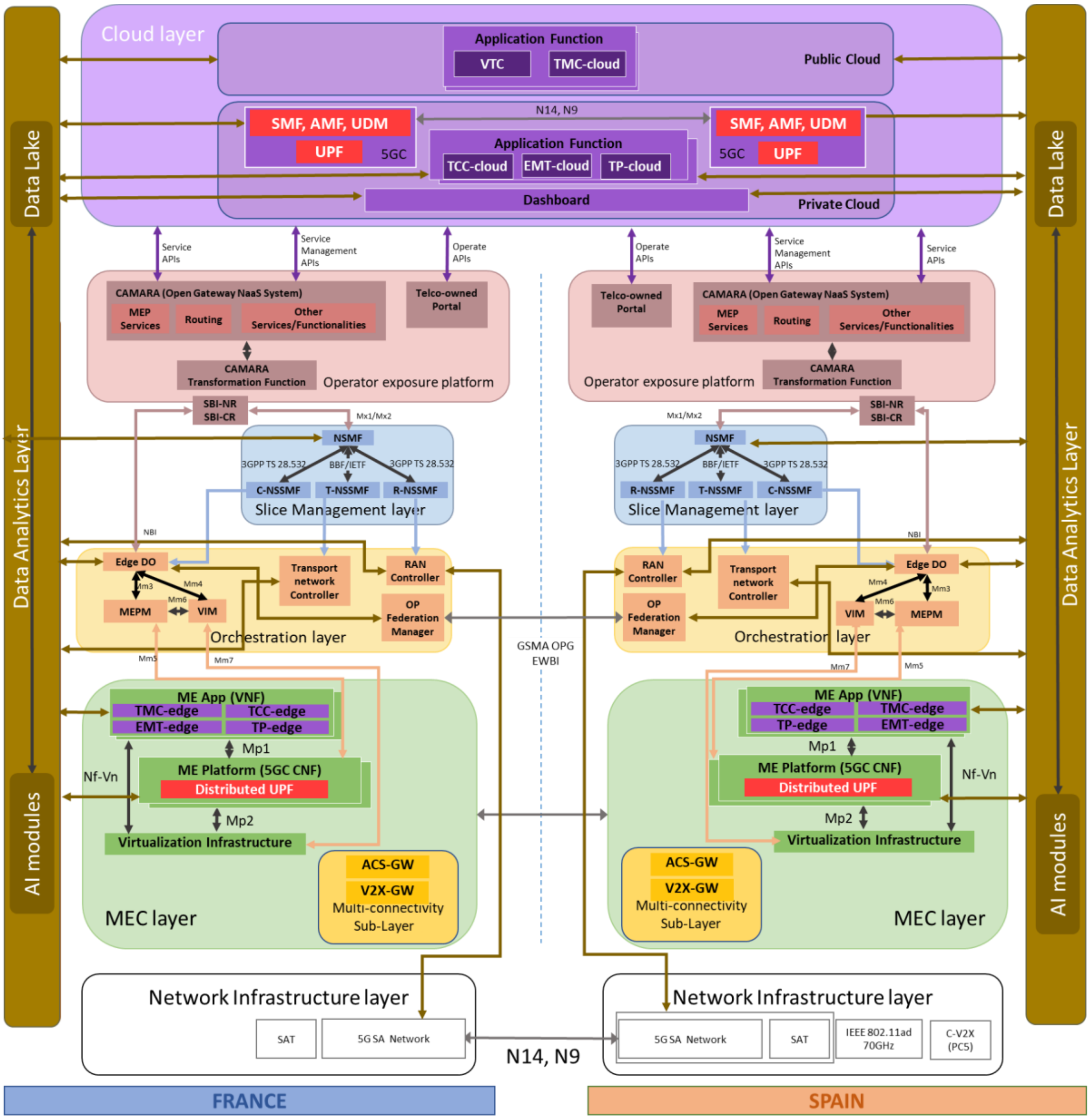


Figure 1: 5GMED Cross-border Network Architecture

The rest of this section describes each layer of the 5GMED cross-border network architecture in detail. The following Sections 3, 4, and 5 describe how the layers presented in this section translate into a concrete implementation in the small-scale test sites.

Test Site	Castellolí small-scale test site (automotive)	Paris-Satory small-scale test site (automotive)	Cross-border corridor small-scale test site (railways)	Cross-border corridor large-scale test site
Use Cases	UC1, UC2, UC4	UC1	UC3	UC1, UC2, UC3, UC4
Network Infrastructure layer				
5G Cores (SA/NSA)	1x 5G SA (Spain) 1x 5G SA (France)	1x 5G NSA	1x 5G SA (Spain) 1x 5G SA (France)	1x 5G SA (Spain) 1x 5G SA (France)
5G Roaming	HRR (N14, ePLMN)	---	HRR (N14, ePLMN)	HRR, LBO (N14, ePLMN)
5G Radio Access Network	2x 5G small cells 1x 5G macro site (2 cells)	1 gNodeB	5 gNodeBs (Spain) 2 gNodeBs (France) 1 gNodeB (DAS, in Le Perthus Tunnel)	6 gNodeBs (Spain) 6 gNodeBs (France) 1 gNodeB (DAS, in Le Perthus Tunnel)
C-V2X (PC5)	1x RSU	---	---	1x RSU (Spain, highway)
IEEE 802.11ad 70 GHz access points	---	---	15 units (Spain, rail track)	15 units (Spain, rail track)
Satellite access			Yes	Yes (only for UC3)
MEC layer				
MEC servers	1 (Spain) 1 (France)	---	1 (Spain) 1 (France)	1 (Spain) 1 (France)
MEC Federation	*Theoretical design for cross-border communication between MEC application instances*			
ACS-GW	---	---	1 (Spain) 1 (France)	1 (Spain) 1 (France)
V2X Gateway	1 (Spain) 1 (France)	---	---	1 (Spain) 1 (France)
Orchestration layer				
Domain orchestrators	2x NearbyOne 1 (Spain) 1 (France)	---	---	2x NearbyOne 1 (Spain) 1 (France)
Orchestrators Federation	GSMA OPG EWBI	---	---	GSMA OPG EWBI
RAN Controller	*Theoretical design: RAN and Transport Network controllers are not implemented because network slicing will be static*			
Transport Network Controller				
Slice Management layer				
Core Network Slicing	*Theoretical design: network slicing will be static with slices directly configured on the 5G RAN, transport, and Core networks*			
Radio Network Slicing				
Transport Network Slicing				
Slice Federation	*Theoretical design for cross-border network slicing continuity across different MNOs*			
Cloud layer				
Public cloud	AWS	AWS	---	AWS
Private cloud	Cellnex cloud server in Castellolí	---	Cellnex cloud server in Castellolí	Cellnex cloud server in Castellolí

Table 2: Summary of 5GMED cross-border network architecture layers implemented in test sites.

2.1 Network Infrastructure Layer

The network infrastructure layer of the 5GMED cross-border network architecture, depicted in Figure 2, is composed of the following parts in both sides of the border:

1) **Radio access network**: Available radio nodes in the radio access network include 5G gNodeBs, 70 GHz IEEE 802.11ad access points, C-V2X Roadside Units (RSUs), and very-small aperture terminals (VSATs) for satellite communications.

2) **Transport network**: It enables the communication between the radio access nodes and the core network, and it includes microwave point-to-point connectivity, fibre optic links and a satellite backhaul.

3) **Core network**: Two different 5G Cores are deployed, one in France and one in Spain. 5GMED will validate enhanced roaming mechanisms to reduce the signaling latency experienced by terminals and ensure cross-border service continuity.

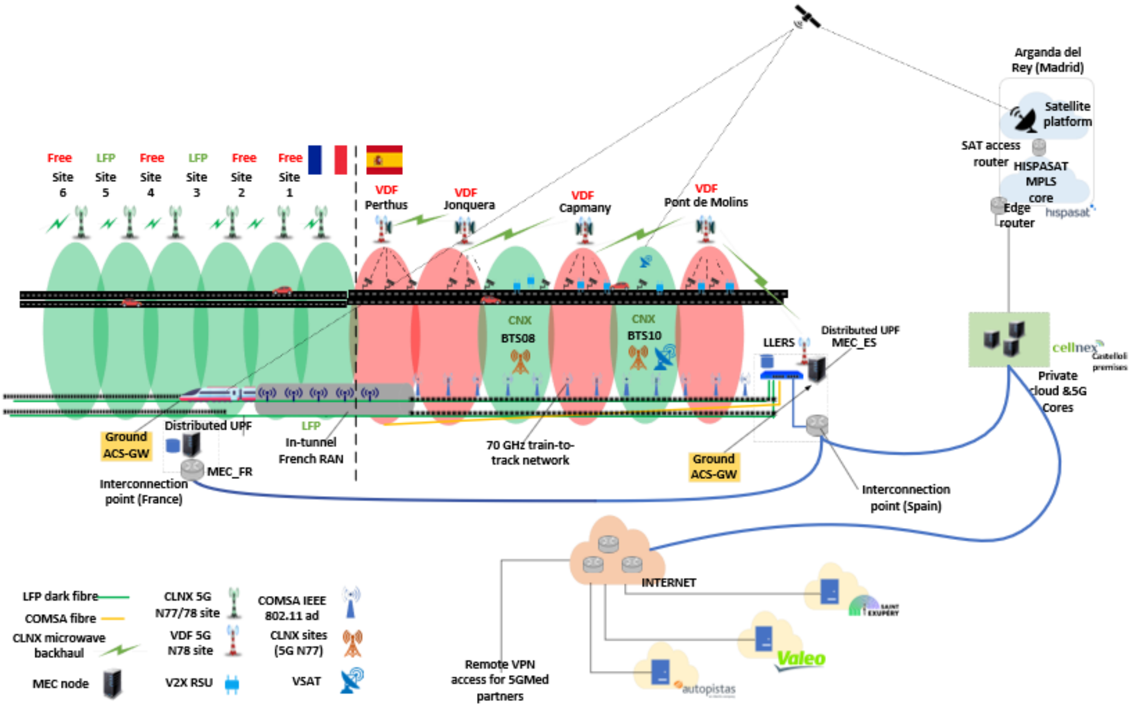


Figure 2: 5GMED Network Infrastructure Layers along the cross-border corridor in Spain (right) and France (left)

Figure 2 illustrates the targeted network infrastructure layer to be deployed along the cross-border corridor, as well as the location of the different RAN elements described below. The figure also shows the connection between MEC servers and 5G Cores, located in Castellolí, as well as the interconnection with Hispasat premises for satellite connectivity.

- In the French side of the corridor (left side of Figure 2, we can see the sites that are fully deployed and owned by Free Mobile and the sites that are deployed by Cellnex together with Free Mobile and located in LFP premises (LFP sites).

- The Spanish side of the corridor (right side of Figure 2) presents several radio access networks: 15 sites for 70 GHz IEEE 802.11ad access points, several C-V2X RSUs located in the Highway, four gNodeBs deployed by VDF and two gNodeBs deployed by CLNX; in which one of them has allocated the VSAT for satellite-backhauling.

- In the cross border between the two countries in the railways scenario, a Distributed Antenna System (DAS) is deployed inside le Perthus Tunnel.

The remainder of this section is organized as follows. Section 2.1.1 describes the internal architecture of the 5G SA networks in the Spanish and French sides of the cross-border corridor. Section 2.1.2 describes in detail the neutral host infrastructure concept considered in 5GMED.

2.1.1 5G SA Networks

Figure 3 shows the internal architecture of the 5G SA networks targeted for the corridor deployment. The block diagram includes the Network Functions (NFs) in the 5G Core of each country (Spain and France), the interfaces between NFs, the interfaces between the 5G Cores and 5G RAN, and the cross-border interfaces.

The main functionalities of the NFs are described as follows.

- **AMF (Access and Mobility Management Function)** is a control plane function in 5G Core. The main functions and responsibilities of AMF are:
  1. Registration Management: allows a UE to register and de-register with the 5G system.
  2. Reachability Management: ensures that a UE is always reachable.
  3. Connection Management: establishes and releases the control plane signaling connections between the UE and AMF.
  4. Mobility Management: is used to maintain knowledge of the UE's location within the network.

- **SMF (Session Management Function)** is part of the control plane function within 5G Core. SMF is responsible for selecting an appropriate UPF and requests information from UDM, described below. The main responsibilities of SMF are:
  1. PDU Session Management. It includes setup, modification, and release of PDU sessions.
  2. IP Address Allocation. It is applicable to PDU Sessions which transfer Ipv4 or Ipv6 packets.
  3. GTP-U Tunnel Management refers to the management of user plane GTP-U tunnel between the Base Station and UPF.
  4. Downlink Notification Management refers to the initiation of paging procedure.

- **UDM (Unified Data Management)** resides on the control plane and manages data for access authorization, user registration, and data network profiles.

- **AUSF (Authentication Server Function)** performs the authentication function of identifying UE and storing authentication keys.

- **UPF (User Plane Function)** interconnects the Data Network (DN) in the 5G architecture. It is also responsible for packet routing and forwarding, packet inspections, Quality of Service

(QoS) handling, and an anchor point for intra & inter RAT mobility. There are two mains locations for UPF: Core and MEC (Edge).

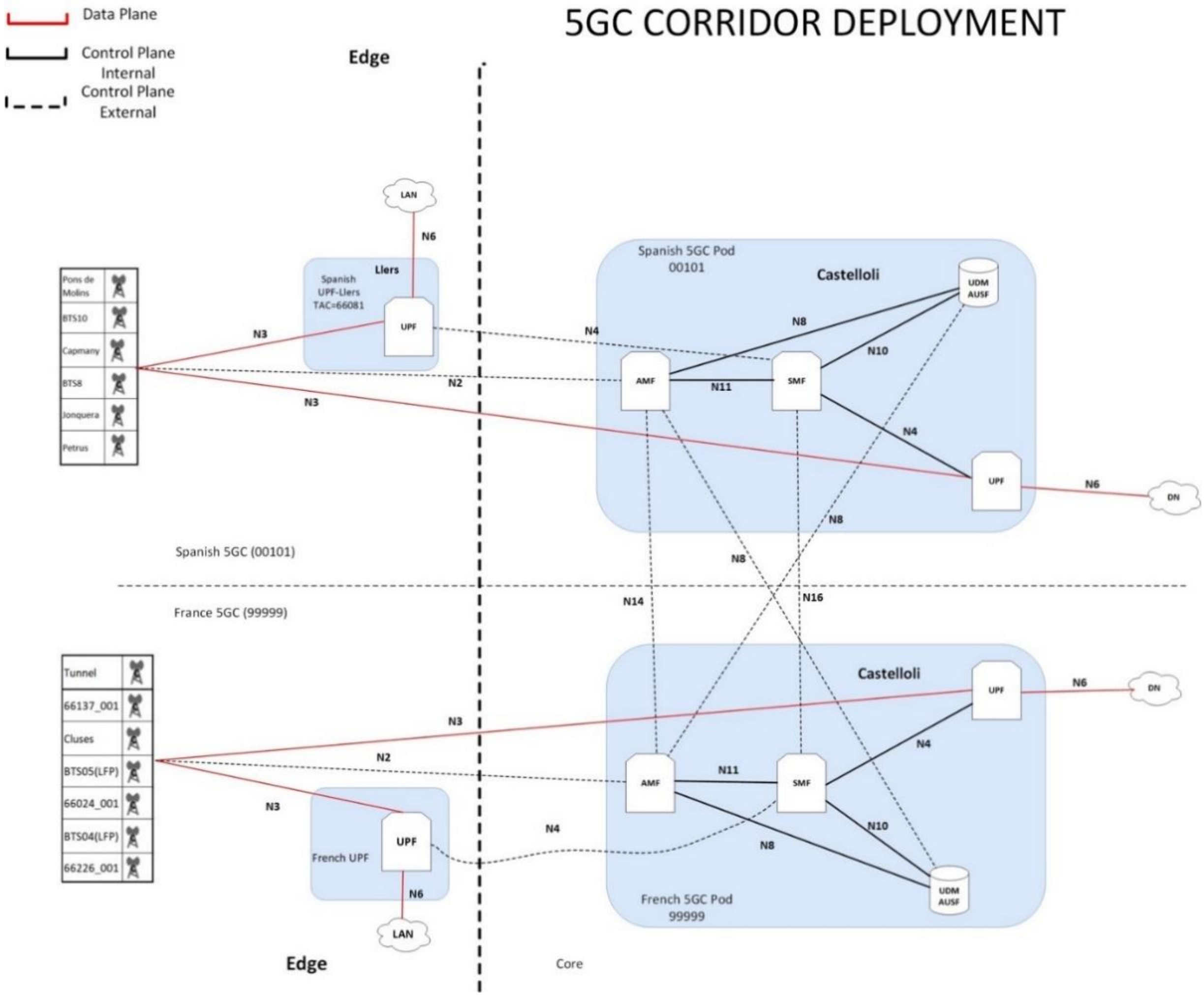


Figure 3: Internal architecture of the 5G SA networks in the cross-border corridor of 5GMED

5GMED requirements with regards to the 5G Core network are listed hereafter in decreasing order of priority.

1. **Home-routed roaming (HRR) with support of visited PLMN**. In the HRR scenario, the Visiting Network data traffic is routed to Data Network via the Home network.
2. **LBO roaming**. In LBO roaming, the data traffic stays within the VPLMN and, therefore, does not involve the SMF and UPF of the HPLMN. LBO is expected to show a reduced latency in the user data plane with respect to HRR.
3. **N14 optimization.** The N14 Reference point is between the two AMFs. In idle mode mobility, the N14 interface allows the AMF in the visited-PLMN (VPLMN) to fetch the UE context from the source AMF, thus reducing the registration/authentication time. This interface is a must in the case of a handover between different PLMNs, so that the source (controlling) network gets information from the UE about potential target cell for handover in the VPLMN.

4. **Equivalent PLMN.** The Equivalent PLMN (ePLMN) list allows a network to provide the UE with a list of PLMN identities to which roaming may take place.
5. In the LBO roaming, keep the application always connected.
6. In LBO, possibility to publish the new IP address of the UE to third party modules.
7. Availability of Network Repository Function (NRF) and its interface to integrate Network Data Analytics Function (NWDAF). NRF makes available the NWDAF, which collects data from 5G Core network functions, performs network analytics, and provides insights with closed loop automation to authorized data consumers.

With HRR in default mode, the roaming process is carried out with new registration of the UE and typically performs an interruption time up to 2 min when a user equipment moves from one country to another. In 5GMED, two main roaming optimization techniques (detailed in D3.1 [2]) are considered to minimize the interruption time:

- **UE roaming with AMF relocation and RAN assistance (idle mode mobility):** Expected interruption time around 1 second.
- **UE roaming with AMF relocation and Handover:** Expected interruption time under a hundred milliseconds.

2.1.2 Neutral Host Infrastructure

The implementation of the network infrastructure layer in the cross-border corridor is carried out under the neutral host infrastructure concept introduced at the beginning of Section 2. Figure 4 illustrates the 5GMED Neutral Host approach to be deployed in the cross-border scenario. The idea is to implement a MOCN scheme where a neutral host operator manages the configuration of the gNodeBs and the 5G Cores that need to interact in the cross-border situation.

To implement the roaming optimization techniques mentioned at the end of Section 2.1.1, the neutral host strategy of 5GMED is paramount. This strategy is twofold:

1. **Re-use of radio network infrastructure via MOCN (RAN Sharing):** MOCN functionality allows a network operator (or neutral host) to share its radio access network with other operators, thus reducing the infrastructure CAPEX and OPEX needed to deploy coverage for more than one operator in a certain area. Each MNO operates its own core network. In particular, 5GMED will show this type of network sharing on the French side of the corridor, where 5G coverage is provided through an agreement with the French operator Free Mobile. Free Mobile sites will be both connected to Free commercial core and at the same time to 5GMED core.
2. **First radio node in each side of the border deployed by a Neutral Host:** to **c**onfigure additional radio parameters (neighbour cells information). This is important to reduce the interruption time when roaming. If both nodes belong to the same neutral host operator, the alignment and configuration of these parameters is highly simplified vs the classical approach of two MNOs.

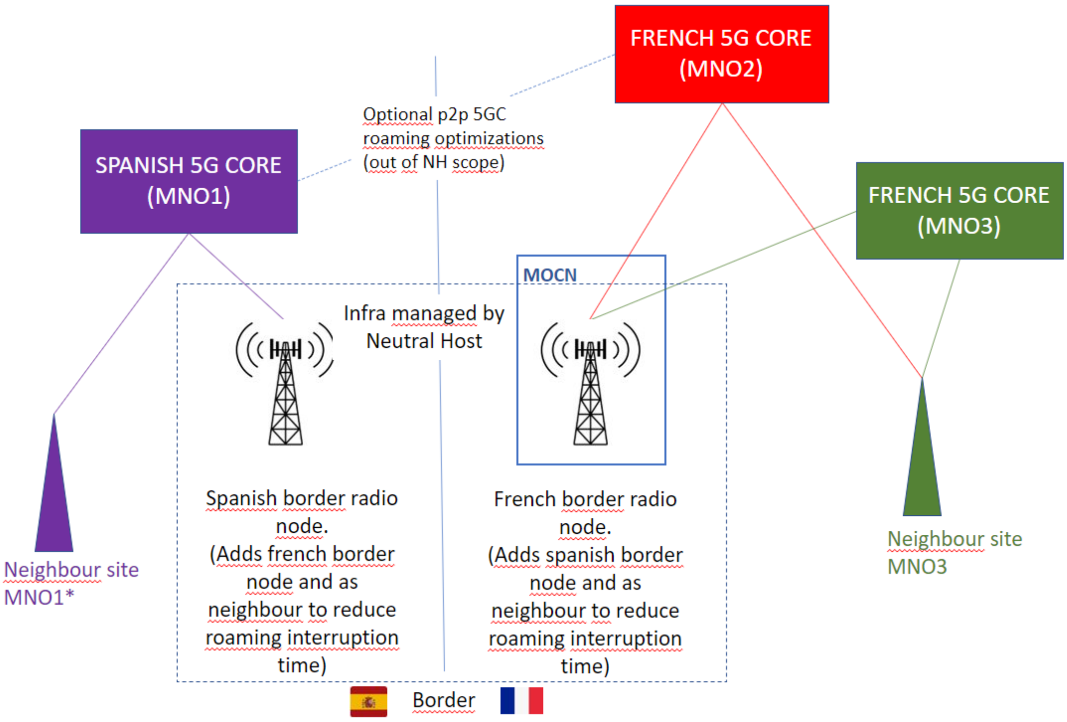

FRENCH 5G CORE (MNO2)
SPANISH 5G CORE (MNO1)
Optional p2p 5GC roaming optimizations (out of NH scope)
FRENCH 5G CORE (MNO3)
MOCN
Infra managed by Neutral Host
Spanish border radio node. (Adds french border node and as neighbour to reduce roaming interruption time)
French border radio node. (Adds spanish border node and as neighbour to reduce roaming interruption time)
Neighbour site MNO1*
Neighbour site MNO3
Border

Figure 4: Neutral Host approach for roaming optimization

2.2 MEC Layer

2.2.1 5GMED MEC Layer

The Multi-access Edge Computing (MEC) is a network architecture concept, popularized by the European Telecommunications Standards Institute (ETSI), that aims to deploy cloud computing capabilities and IT services closer to the end-client connected through a cellular network [3].

Within the 5GMED project, the MEC layer allows the deployment of certain services or network functions nearby the subscribers. The latter should be connected to the MEC server through an instance of User Plane Function (UPF) that resides in the MEC. From the cost point of view, it is not efficient to deploy a MEC in each gNodeB because in addition to the cost of the MEC servers, the MNOs must install a UPF for each MEC. Therefore, one MEC will be deployed for a group of gNodeBs based on their proximity. Figure 5 shows the distribution of the MECs over gNodeBs in 5GMED. As it can be observed in the figure, there is one MEC per MNO because the adopted approach by the project implies that each UPF is connected to one Tracking Area (TA) and that there is one tracking area per MNO. However, this can be extended to have more MECs per MNOs if more TAs are configured.

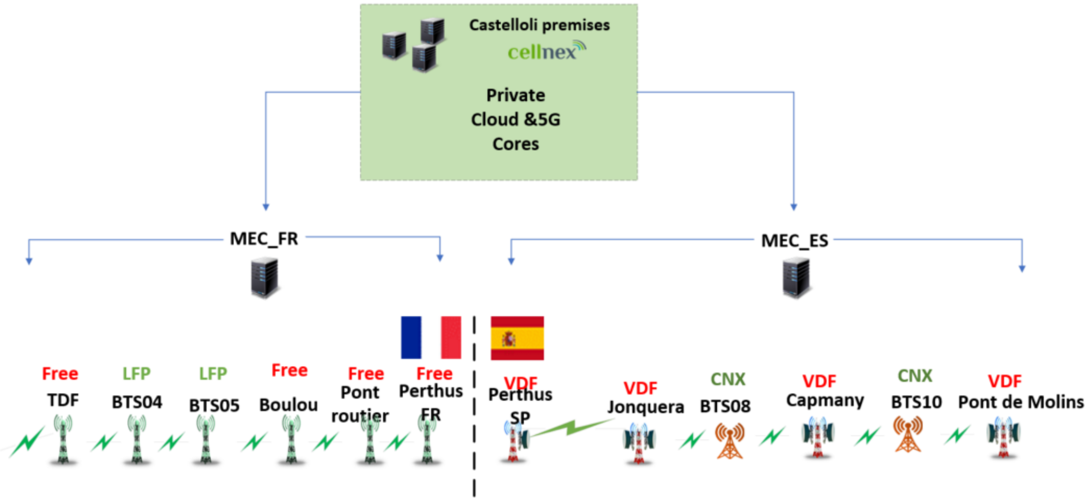


Figure 5: MEC distribution over gNodeBs

Figure 6 shows the different modules and interfaces of the MEC layer based on the ETSI MEC reference architecture in a NFV environment [2] [4]. The MEC layer includes several services or application functions required by the use cases (i.e., UC2, UC3 and UC4). This will allow the service provider to deliver reliable and real-time services to its end user applications.

In addition, the MEC layer encompasses the distributed instances of the UPF that is deployed in the Mobile Edge Platform (ME platform), the Adaptive Communication System Gateway (ACS-GW), and the V2X Gateway (V2X-GW). These gateways allow user devices to dynamically select alternative wireless access technologies to support 5G, based on network conditions and on specific QoS requirements dictated by the application. The ACS-GW is used in UC3 to manage 5G NR, 70 GHz IEEE 802.11ad and VSAT for train-to-track communications. The V2X gateway is used in UC2 to handle 5G NR and C-V2X connections for vehicular communications. The operation of the ACS-GW and V2X Gateway is described in detail in D3.2 [1].

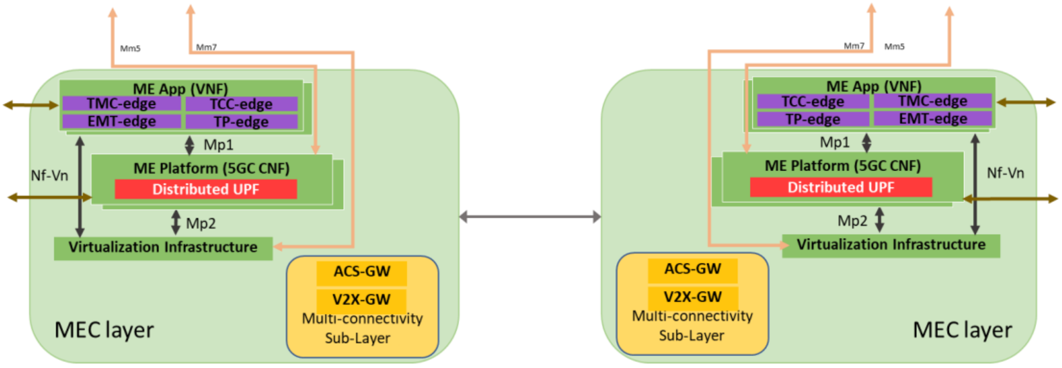


Figure 6: MEC Layer components.

2.2.2 Cross-Border Inter-MEC Data Communications based on MEC Federation

This section introduces a theoretical enhancement to the MEC layer in the 5GMED cross-border network architecture by adding MEC federation components. The objective is to provide **cross-border data communication between MEC application instances running in the MEC of the Spanish and**

French MNOs. It should be noted that federation mechanisms have been designed and implemented in 5GMED and are introduced in Section 2.3 (orchestration layer) and Section 2.4 (slice management layer). All these mechanisms intricately focus on and align with the GSMA platform's East-West bound interface presented in **"Annex A: GSMA Operator platform"**.

The proposed approach to enable cross-border data communication between MEC application instances in different MNOs relies on the use of an Exposure Gateway (presented in **"Annex B: Exposure Gateway"** that enables the exposure of MEC's or MNO's services to a consumer. The consumer, in this case, may be an application instance running in an MEC infrastructure that needs to communicate with another MEC application instance across the border. Therefore, it needs to consume an operator functionality related to the path through which it must route the application data.

The elements of the Exposure Gateway considered in 5GMED are depicted in Figure 7. The CAMARA Transformation Function connects to the lower layers through the southbound interface network resources (SBI-NR) and northbound interface network resources (SBI-NR). It provides necessary abstractions on the underlying computational and network resources to the above layers. These abstractions are leveraged in the CAMARA (Open Gateway NaaS System) block of the architecture, offering consumers the services exposed by the MNO through the Service APIs and Service Management APIs. Operate APIs are also provided to enable operation, administration, and management capabilities. The Service APIs, Service Management APIs, and Operate APIs are accessible both from the cloud layer and other service consumers, such as MEC applications running on the MEC located on the opposite side of the border, through a URL. Detailed information about the CAMARA API can be found in **"Annex C: CAMARA API"**.

CAMARA deals exclusively with customer-facing northbound APIs related to telco mobile networks. It should be noted that APIs used for east-west federation or roaming purposes are not within the scope of CAMARA. As described in Section 2.3, the Edge domain orchestrator (DO) provides both the federation manager and federation broker roles to enable interactions between MEC systems across the East-West Bound Interface, including resource sharing.

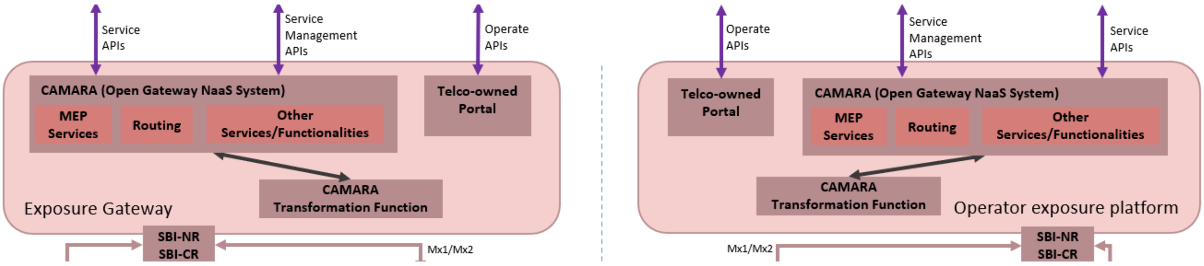


Figure 7: Exposure Gateway Platform

The operation of the MEC Federation concept to enable data communication between MEC application instances in different MNOs is described next. It is assumed that standard roaming mechanisms to establish the necessary connectivity between the UE and the UPF of the visited network are applied as necessary. Suppose MEC#1 refers to the MEC in the home network, and MEC#2 represents the MEC in the visited network. As the UE connects to MEC#2 for the first time, it is necessary to check if the application is already running in MEC#2's infrastructure; if it is not, then the federation mechanisms are applied to gather the necessary application image and descriptors; after this process, the UE can connect to the application instance running in MEC#2. Then, the transfer of application data between MEC#2 and MEC#1 must be enabled; for this purpose, the application running in MEC#2 can consume a routing CAMARA API to gather information about the route to connect to in order to reach a suitable gateway on MEC#1's side (either a V2X-GW in use case 2, or an ACS-GW in use case 3). After this, the application can successfully reach the required gateway on the other MEC, and data communication between the application instances is enabled. (Note that this workflow assumes that the CAMARA-based routing is implemented).

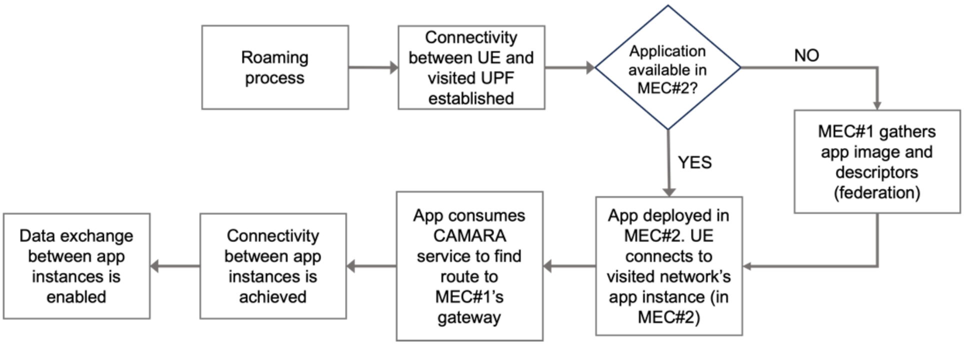

Roaming process
Connectivity between UE and visited UPF established
Application available in MEC#2?
NO
YES
MEC#1 gathers app image and descriptors (federation)
App deployed in MEC#2. UE connects to visited network's app instance (in MEC#2)
App consumes CAMARA service to find route to MEC#1's gateway
Connectivity between app instances is achieved
Data exchange between app instances is enabled

Figure 8: Application of CAMARA-based federation to enable cross-border inter-MEC exchange of application data

Furthermore, it is also assumed that the network deployment supports the secure transfer of data between gateways across each side of the border. The suggested approach to achieve this is based on the interconnection of the gateways at each side of the border through an IPX, following the approach proposed in [5] and in [6] for the enablement of end-to-end confidentiality and integrity between source and destination data. Moreover, using a CAMARA API, the application data can be routed to the destination gateway through the corresponding IPX instance.

In addition to the discussed applicability, other potential applications of the proposed CAMARA-based federation approach include edge infrastructure sharing, multi-operator federation (e.g., by enabling MNOs to extend services to each other's subscribers), etc.

2.3 Orchestration Layer

The orchestration layer includes the management and orchestration components of the 5GMED cross-border network architecture, as shown in Figure 9. These elements include:

i) The **network controllers** that interact directly with the network infrastructure, which are the Transport Network Controller that manages the transport network, and the RAN controller that manages the RAN.

ii) The **Edge-related orchestrators**, which are the edge domain orchestrator (Edge DO), the MEC platform manager (MEPM), and the virtual infrastructure manager (VIM) that manage the onboarded network and application services, as well as the underlying compute infrastructure.

iii) The **Operator Platform (OP) Federation Manager**, that manages the exposure of Edge Cloud resources and Network capabilities of operators across networks and across national boundaries.

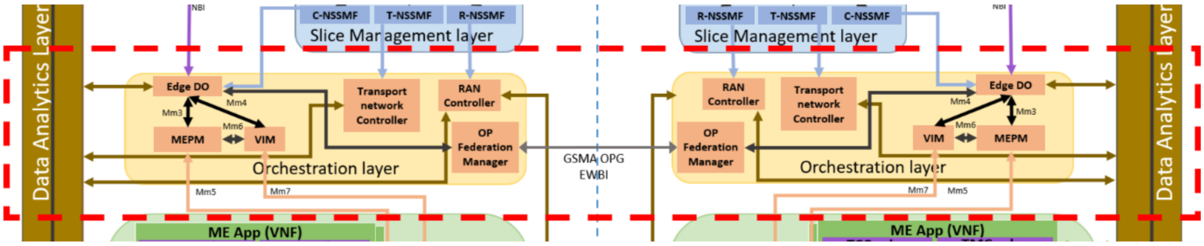


Figure 9: Orchestration Layer

The network controllers of the orchestration layer receive actions by the Slice Management layer such as to instantiate and delete network services, reconfigure the datapath and establish QoS, and re-dimension RAN slices for the core network, transport network and RAN network, respectively. Usually, these actions are performed via REST APIs. This is why from one hand the domain specific network controllers need to expose an API that allows a client (e.g. C-NSSMF, T-NSSFM, R-NSSMF) to request for the instantiation of a network slice, while on the other hand the domain specific NSSMFs in the slice management layer need to incorporate an agent framework in the form of API clients that perform action to the network controllers.

On the other hand, the Edge DO interact with the MEPM for the management of the application lifecycle, application rules and requirements, and keeping track of available MEC services (Mm3), as well as with the VIM to manage virtualised resources of the MEC host, including keeping track of available resource capacity, and to manage application images (Mm4).

In addition, the Mm5 reference point between the MEPM and the MEC layer is used to perform platform configuration, configuration of the application rules and requirements, application lifecycle support procedures, management of application relocation, etc. The Mm6 reference point between the MEPM and the VIM is used to manage virtualised resources, while the Mm7 reference point between the VIM and the virtualisation infrastructure is used to manage the virtualisation infrastructure.

Besides the specific architectural design and the orchestration components in each administrative domain, the specific peculiarities in 5GMED and the requirement for service orchestration in cross-border scenarios stress the need for cross-border/MNO communication between the different Edge DOs (per each country) in the orchestration layer. Hence, we assume the existence of two orchestrators, each assigned to a country, i.e., Spain and France, to enable cross-MNO/federation in the border.

The design of the cross-MNO/federation between domain orchestrators (one DO per MNO) follows the GSMA concept of a common "Operator Platform" (OP) [7] to make operators assets and capabilities consistently available across networks and across national boundaries. See **"Annex A: GSMA Operator platform"** for a more detailed description of the GSMA Operator Platform.

2.4 Slice Management Layer

Network slicing is a specific feature of 5G SA. It allows the division of a single physical network infrastructure into multiple isolated and flexible logical networks, known as "slices" [8]. These slices can be customized to meet the needs of different users or applications by assembling various resource partitions, including core, transport, and radio network components.

The slice management layer of the 5GMED cross-border network architecture comprises several key components shown in Figure 10. One of these components is the Network Slice Management Function (NSMF), which is responsible for the management and orchestration of NSI and derive network slice subnet requirements. Another component is the Network Slice Subnet Management Function (NSSMF), which consists of different sub-components, including the Core Network Slice Subnet Management Function (C-NSSMF), the Radio Network Slice Subnet Management Function (R-NSSMF), and the Transport Network Slice Subnet Management Function (T-NSSMF). The slice management layer interacts with the cloud layer through the Mx1/Mx2 interface to provide the configuration of the different slices.

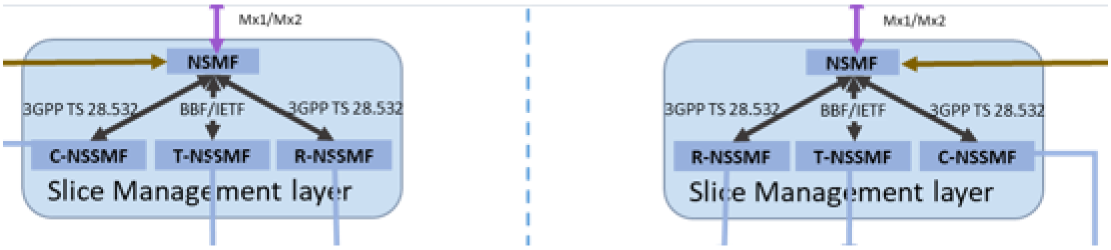


Figure 10: Slice Management Layer

The C-NSSMF is responsible for managing the core network resources. The R-NSSMF handles the radio network resources through the interface with the RAN Controller inside the orchestration layer, and the T-NSSMF manages the transport network resources through the interface with the Transport Network controller inside the orchestration layer. Together, these components enable a more efficient use of network resources, with slices being configured and allocated according to the specific requirements of each use case. Once a network slice is fully activated, it enables end-to-end connectivity among network elements. This facilitates the deployment of isolated services with performance guarantees.

Multiple standards are being defined for the interfaces between NSMF and the different NSSMF. For C-NSSMF, is being applied 3GPP TS 28.532; for R-NSSMF, 3GPP TS 28.532. For T-NSSMF it is not completely specified, as other SDO are leading its definition. BroadBand Forum (BBF) is proposing a similar approach as ONF Transport API, while IETF is leading discussions on transport slice model.

The remainder of this section is organized as follows. Section 2.4.1 provides specific details on the design and implementation of RAN slicing, transport network slicing, and core network slicing. Section 2.4.2 presents the slice federation concept that has been designed in 5GMED to provide network slicing continuity across different MNOs, allowing users to seamlessly access services and maintain a consistent network experience when moving across different MNOs. Finally, Section 2.4.3 describes the approach followed in 5GMED to ensure 5G slicing continuity when a UE moves from 5G to other radio access technologies, i.e., satellite, C-V2X, IEEE 802.11ad.

2.4.1 Network Slicing for 3GPP Technologies

In this section, specific details on network slicing are provided for multiple network segments, as detailed in previous section: RAN slicing in Section 2.4.1.1, transport network slicing in Section 2.4.1.2, and core network slicing in Section 2.4.1.3.

2.4.1.1 RAN Slicing

Understanding the impact of network slicing on the design of the 5G RAN involves identifying specific requirements. These include maximizing RAN resource utilization, making the RAN slice-aware, implementing traffic differentiation mechanisms, supporting slice isolation protection mechanisms, and enabling efficient management mechanisms.

The RAN infrastructure must have the necessary hardware and software capabilities. A slice management framework should be used to allocate resources and provide the required QoS and performance metrics. Standard interfaces and protocols must be used for interoperability between different network functions.

In 5GMED, three main requirements must be met for network slicing in the RAN. Firstly, a mechanism is needed to establish the S-NSSAI and support various types of slices. Secondly, resources must be allocated specifically for S-NSSAI. Finally, a connection must be established between S-NSSAIs and a transport endpoint.

From an integration perspective, a RAN Controller (included in the Orchestration layer below the Slice Management layer) with a northbound API controls a set of RAN infrastructures. This enables efficient management by the Slice Manager. The RAN Controller can provide information such as the controller’s name, location, and authentication schema. Each infrastructure has a defined topology that can be accessed through queries. The Slice Manager API allows the orchestrator to request a RAN partition and select interfaces and links from the topology. Using the Slice Manager’s radio service API, the orchestrator can deploy a 5G connectivity service for end-user devices and create a slice. This plan ensures the efficient deployment of 5G connectivity services by effectively utilizing RAN infrastructure resources.

In 5GMED, the dynamic configuration process of RAN slicing finally could not be implemented in the real scenario due to vendor limitations (explained later in Section 3.5), however, the Slice Manager and RAN Controller have been developed by several partners that are part of the 5GMED consortium. Instead of dynamic configuration, static RAN slicing was implemented statically by directly configuring the parameters of the slices in the gNodeB’s.

2.4.1.2 Transport Network Slicing

Transport Network Slicing uses network virtualization to offer transport for network slices that can support different applications and services with specific requirements. It is a way of partitioning network resources into isolated virtual networks, each with its own characteristics and performance objectives. Transport Network Slicing can enable network operators to manage their network resources efficiently and offer differentiated transport slices with different Service Level Agreements (SLAs) for the deployed End-to-End network slices. With Transport Network Slicing, network operators can provide tailored transport slices with specific requirements, such as high availability, low latency, or high bandwidth, to meet the diverse needs of their customers.

VLAN (Virtual Local Area Network) is a technology that allows network administrators to partition a single physical network into multiple logical networks [9]. In transport networks, VLAN can be used to create transport network slices that offer specific SLAs to different types of slice traffic (e.g., eMBB, URLCC). By assigning a VLAN tag to a specific type of traffic, network operators can ensure that each type of traffic is given the appropriate priority and bandwidth. This can help to ensure that each requested slice receives the necessary resources to function correctly while less critical traffic does not interfere with them.

Using VLAN in transport networks can be an effective way to ensure that network resources are efficiently utilized and the SLAs of different types of traffic are met. Network operators can create multiple VLANs to separate different types of traffic and assign different SLAs to each VLAN based on their requirements. This can help to optimize network performance, reduce congestion, and provide better end-to-end service.

Due to the operational nature of the 5GMED network infrastructure described in this document, dynamic VLAN configuration is not allowed in production switches chosen for the 5GMED network. Thus, 5GMED's transport slicing solution considers mapping different 5G QoS Identifiers (5QI) to specific VLANs. This has been realized with a pre-deployment of static VLAN configuration in the cross-border scenario. To demonstrate the feasibility of a dynamic solution, transport network slicing for multiple 5QI has been demonstrated in the laboratory. Furthermore, the authors in [10] have presented a secured network slicing architecture that has been validated against a vehicular scenario based on Anticipated Cooperative Collision Avoidance use case. In 5GMED, a similar scenario will be demonstrated based on the Layer 2 isolation of multiple network traffic types.

2.4.1.3 Core Network Slicing

The 5GMED use cases will use slicing based on S-NSSAI. This is suggested by the slice manager module. This means there is no need for a unique 5G Core control plane for each slice. By using S-NSSAI support, multiple slices can be enabled within a single 5G Core.

To enable the implementation of network slicing, the RAN and Core domain must be able to support such capability, as well as some functionalities, i.e., the ability to support various Quality of Services (QoS) and traffic profiles. The identification of the appropriate traffic profiles was done by using the 3GPP standards "Policy and Charging Control Architecture" under 3GPP TS 23.503 [11]. In fact, 5QI are the values specified for services that are assumed to be commonly used in 5G networks. Those values are used as references for the characterisation of QoS flow forwarding control.

Table 3 shows how the 5G QoS characteristics, such as resource type, packet delay budget and packet error rate, are associated with 5QI. Such performance characteristics, detailed below, describe the packet forwarding scheme that a specific QoS flow receives between the user and the UPF.

- The **Resource type**, which may be Guaranteed Bit Rate (GBR), Delay Critical GBR, or Non-GBR, is responsible for determining whether dedicated network resources are permanently allocated.

- The **packet delay budget** (PDB) defines an upper bound for the time a packet may be delayed between the user equipment and the N6 interface, which provides the connectivity between the User Plane Function (UPF) and any other networks such as the internet, private or public clouds.
- The **Packet Error Rate** (PER) is the parameter that defines the upper-bound rate of the Packet Data Units (PDUs) that have been processed but not successfully delivered.

As explained above, the PLMN IDs, NSSAIs, VLANs and IP addresses are some of the network parameters that are mandatory to connect the access nodes to the appropriate core instances to provide the required resources for each service.

In order to enable core slicing, the NSMF, which is responsible for the lifecycle management of the end-to-end slice, will communicate to the domain slice manager or Core NSSMF. The NSMF requires for a sub-slice in each domain and the NSSMF, which is responsible for the slice subnets within its domain, will perform the configurations to provide the network slice subnet instance, or create a subnet slice in the core network based on the slice profile.

5QI Value	Resource Type	Default Priority Level	Packet Delay Budget	Packet Error Rate	Default Maximum Data Burst Volume	Default Averaging Window	Example Services
1	GBR (guaranteed flow bit rate)	20	100 ms	10^{-2}	N/A	2000 ms	Conversational Voice
2	GBR	40	150 ms	10^{-3}	N/A	2000 ms	Conversational Video (Live Streaming)
3	GBR	30	50 ms	10^{-3}	N/A	2000 ms	Real time gaming, V2X messages
4	GBR	50	300 ms	10^{-6}	N/A	2000 ms	Non-conversational Video (Buffered Streaming)
65	GBR	7	75 ms	10^{-2}	N/A	2000 ms	Mission Critical user plane Push to Talk voice (e.g. MCPTT)
66	GBR	20	100 ms	10^{-2}	N/A	2000 ms	Non-Mission Critical user plane Push to Talk Voice
67	GBR	15	100 ms	10^{-3}	N/A	2000 ms	Mission Critical Video user plane
71	GBR	56	150 ms	10^{-6}	N/A	2000 ms	"Live" Uplink Streaming (TS 26.238[76])
72	GBR	56	300 ms	10^{-4}	N/A	2000 ms	"Live" Uplink Streaming
73	GBR	56	300 ms	10^{-8}	N/A	2000 ms	"Live" Uplink Streaming
74	GBR	56	500 ms	10^{-8}	N/A	2000 ms	"Live" Uplink Streaming
76	GBR	56	500 ms	10^{-4}	N/A	2000 ms	"Live" Uplink Streaming
5	Non-GBR	10	100 ms	10^{-6}	N/A	N/A	IMS Signalling
6	Non-GBR	60	300 ms	10^{-6}	N/A	N/A	Video (Buffered Streaming) TCP-based (e.g. www, e-mail, chat, FTP, p2p file sharing, progressive video etc.)
7	Non-GBR	70	100 ms	10^{-3}	N/A	N/A	Voice, Video (Live Streaming), Interactive Gaming
8	Non-GBR	80	300 ms	10^{-6}	N/A	N/A	Video (Buffered Streaming) TCP-based (e.g. www, e-mail, chat, FTP, p2p file sharing, progressive video etc.)
9	Non-GBR	90	-As above-	-As above-	-As above-	-As above-	-As above-
69	Non-GBR	5	60 ms	10^{-6}	N/A	N/A	Mission Critical Delay Sensitive Signalling (e.g. MC-PTT Signalling)
70	Non-GBR	55	200 ms	10^{-6}	N/A	N/A	Mission Critical Data (e.g. example services are the same as 5QI 6/8/9)
79	Non-GBR	65	50 ms	10^{-2}	N/A	N/A	V2X messages (TS 23.287[121])
80	Non-GBR	68	10 ms	10^{-6}	N/A	N/A	Low Latency eMBB applications Augmented Reality
82	Delay Critical GBR	19	10 ms	10^{-4}	255 bytes	2000 ms	Discrete Automation (TS 22.261[2])
83	Delay Critical GBR	22	10 ms	10^{-4}	1354 bytes	2000 ms	Discrete Automation; V2X messages
84	Dalay Critical GBR	24	30 ms	10^{-5}	1354 bytes	2000 ms	Intelligent transport systems (TS 22.261[2])
85	Delay Critical GBR	21	5 ms	10^{-5}	255 bytes	2000 ms	Electricity Distribution high voltage, V2X messages
86	Delay Critical GBR	18	5 ms	10^{-4}	1354 bytes	2000 ms	V2X messages (Advanced driving: Collision Avoidance, Platooning with high LoA)

Table 3: Mapping of 5QI to QoS Characteristics

2.4.2 Cross-Border Network Slicing Continuity based on Slice Federation

Network slicing continuity in different administrative domains (MNOs) is one important network-related challenge in 5GMED. This section presents a **theoretical enhancement** to **provide network slicing continuity across different MNOs**, by integrating the Slice Management layer and the Orchestration layer of the 5GMED cross-border network architecture, based on the "Operator Platform" (OP) concept [7] (see Section 2.3 and Annex A: GSMA Operator platform).

3GPP has defined a three-layer functions model providing a hierarchical approach to network slicing, enabling the translation of service requirements into network slice characteristics and their implementation across the network infrastructure. The three functions in this model are the Communication Service Management Function (CSMF), the Network Slice Management Function (NSMF), and the Network Slice Subnet Management Function (NSSMF) [12].

In cross-border scenarios, **slice federation** enables the extension of network slices across different operators' networks. The concept of slice federation allows users to seamlessly access services and maintain a consistent network experience when moving between different operators' networks. However, in the case of network slice roaming, the OP concept has not yet proposed any mechanism for federating slices. In 5GMED, we have integrated the OP with the 3GPP slice management and orchestration functions. This integration is further enhanced with the incorporation of slice federation capabilities.

In the remainder of this section, the architecture and intricacies of the proposed model are detailed, emphasizing the crucial role of the proposed Manager and its integration with the existing OP system. Particularly, Section 2.4.2.1 focuses on the encapsulation of resource requests that initiate slice federation, introducing the mechanism and on describing the building blocks of the system, while the Section 2.4.2.2 offers a step-by-step breakdown of the slice federation process, providing a practical perspective.

2.4.2.1 Slice Federation Design

The OP concept in its current release defines the role of the Federation Manager, which is responsible for implementing the east-west bound interface (EWBI) managing the federation among multiple OPs instances, with support limited to workload federation. At its core, EWBI defines a set of resources that can be used to define and deploy cloud-native applications, while no slice-related resources have been identified in [13]. To leverage the current implementation of OP-based orchestration layer and trigger these resource requests that enable slice federation, we propose the encapsulation of such requests into a Slice Federation as a Service (SFaaS) mechanism. The proposed idea is to federate a specific application called slice-request App (srApp), which carries the slice template and stipulates the slice customer request.

In network slicing, the slice template refers to a predefined set of parameters and configurations that define the characteristics and behaviour of a specific network slice. It serves as a blueprint for creating instances of network slices with consistent attributes and functionalities. The slice template includes various elements that define the slice type, quality of service parameters, network functions, resource allocation, and other specific requirements. In our approach, the slice template from the originate network is translated to a federated slice template through the introduction of a federation-specific management function for slicing as will be described below. In addition, our framework follows a cloud-native approach, in which applications need to be converted into microservices and be deployed on cloud platforms like Kubernetes. A cloud-native microservice can be seen e.g., as a Docker container, in which the Docker image lies in a public/private repository, while the container itself is referencing from Kubernetes resources, which the later are packaged into Helm Charts to simplify the management and deployment of complex applications and services.

The proposed framework for slice federation adopts a multi-stakeholder architecture, as illustrated in Figure 11, comprising four distinct entities: i) the Operator, ii) the slice customer, iii) the application provider, and iv) the end-user.

The Operator owns the telco infrastructure, where cloud-native applications and mobile network functions (NFs) are running, managed and orchestrated from an operator platform based on the OP concept with integrations and extensions. Specifically, the operator platform is splitted into two layers, the slice management layer and the orchestration layer. The former contains the Slice Manager, which consists of the 3GPP slice model functions like the NSMF and the domain specific NSSMF). The latter, contains the service orchestrator for the application lifecycle management in the edge-cloud sites, the Federation Manager to enable edge federation as defined by OP standards and interfaces, and the Slice Federation Manager, which is introduced in this proposal, to further extend edge federation with slice federation, leveraging the existing interfaces.

The application provider offers services for the end-users to be deployed within the telco infrastructure, while the slice customer requests a communication service in the form of a network slice to cater for its end-users' specific characteristics and requirements. The end-users represent the final consumers of both the applications and network services.

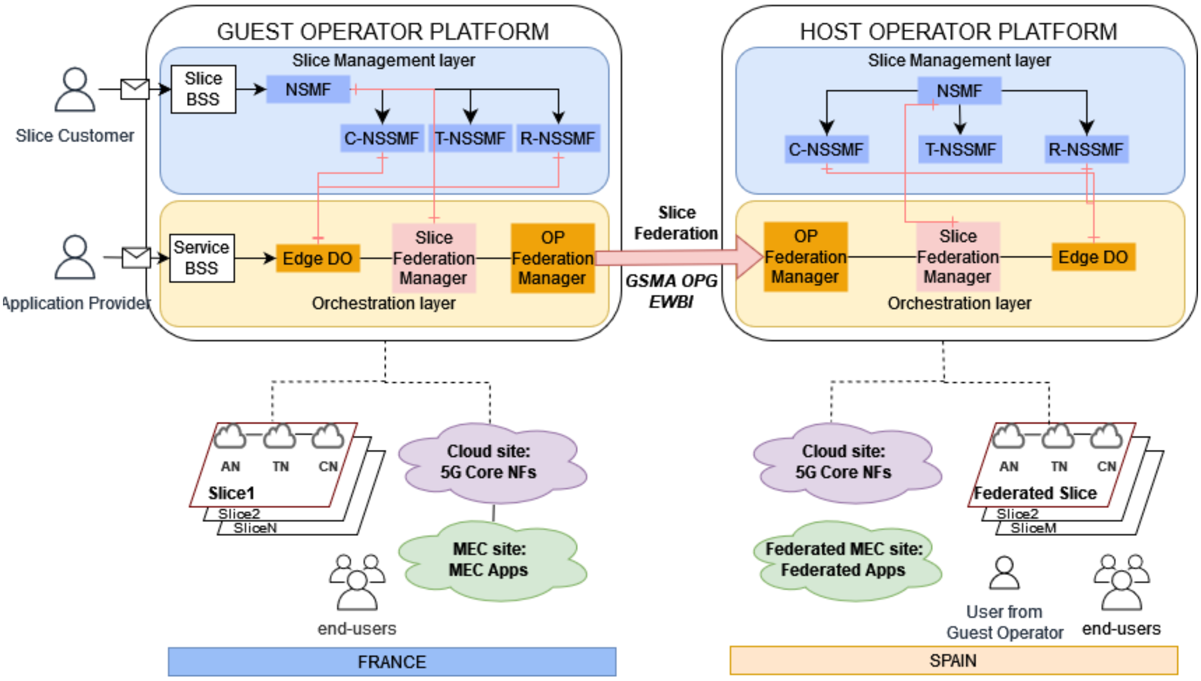


Figure 11: Proposed theoretical framework for slice federation based on the OP concept.

The telecommunication network of each operator is divided into network slices, with each slice customized to fulfil the specific requirements of the end-users across various technical domains, including the Access Network (AN), Transport Network (TN), and Core Network (CN). Slice requests are received from the slice customer, which can be either the operator or a content/service provider. Each operator, through the NSMF, provides and manages their network slices within their telco infrastructure.

From the OP concept, the Service Manager, represented here as the Edge DO, is responsible for service and resource provisioning within the telco site infrastructure. In particular, the telco infrastructure is considered a collection of multiple edge/MEC and cloud nodes across the compute continuum, capable of hosting, executing, and orchestrating cloud-native applications and NFs. It is the domain-specific slice functions in the slice layer that interface with the Edge DO, forwarding slice requests to its northbound interface (NBI). To enable further edge and slice federation, the Federation Manager facilitates the service and slice mobility among operators through federation and the EWBI endpoints. Specifically, during the federation setup, the availability zone of the Host Operator is shared with the Guest Operator, enabling the deployment of applications on the shared edge site. To facilitate slice federation, the EWBI resources must incorporate network slice domain-related information. For example, in the core network, the control plane function endpoints for the Access and Mobility Management Function (AMF), NSSF, and SMF need to be exposed.

Finally, each operator platform includes the newly introduced role of this proposal, the Slice Federation Manager. The Slice Federation Manager in Guest Operator translates the 3GPP slice requirements into federation network slice requirements. It queries the NSMF to get the slice context the user belongs to and maps it to appropriate services for federation. Such a request can be sent from an API client that resides in Slice Federation Manager and points to NSMF's API server. Therefore, it acts as a bridge among the rest of the managers running in the orchestration layer. Meanwhile, the Slice Federation Manager of the Host Operator gets the status of the slices being federated from its corresponding NSMF and creates a database and information for the federated slices. The EWBI offers the potential to include various slice-related interfaces. However, in our approach, we've chosen to incorporate these slice-related endpoints directly into the srApp federated application, streamlining the process.

2.4.2.2 Example of Slice Federation Process

This subsection describes in detail the process of slice federation, detailing its steps and intricacies. Alongside, it provides a hands-on look at the srApp, offering a real-world example of its functionality and appearance.

When all the building blocks from OP, 3GPP management slice functions, and the extensions come into play, the network slice federation process involves four phases, as described below:

- **Phase 1:** Pre-registration. It is assumed that a slice has already been created in Guest Operator for a user or group of users. The NSMF has been involved in translating customer slice requests into slice requirements. Updates of the NFs and applications involved, and the status of the slice are always reported back to NSMF from the subslice domain managers. The Slice Federation Manager constantly gets and updates its state by retrieving the slice instance and translating it into a federated slice template. It leverages the predefined API endpoints within NSMF to request the status of the user's slice. The status includes information on slice-domains, slice requirements, and specific NFs associated with the slice. The flow of the actions is depicted in Figure 12 on steps 1-3.

- **Phase 2:** Slice Federation setup. The federation establishment shall be performed to set up the federation relationship between the two operator platforms. Steps 4-9 in Figure 12 show the actions needed to establish the federation and exchange network slice related information between the operators, such as the endpoints of the Host NSMF. In this flowchart, the user's home network is the Guest Operator, and the visited network is the Host Operator.
- **Phase 3:** srApp onboarding and deployment. To onboard the srApp, files must be uploaded first (e.g., Docker images) into a public/private registry (e.g., Harbor), then the artefacts referencing the said files (e.g., helm charts with their respective Kubernetes manifests like Deployments and ConfigfMaps), and finally, onboard the application that will reference the artefacts. With the application onboarded, we can install the application to an edge site (e.g., Kubernetes cluster), depicted by step 10-11 of Figure 12, and it will start to run triggering the federated slice request.
- **Phase 4:** Federated Slice Deployment. After the deployment of the srApp, a federated slice request is sent to the Host operator NSMF (Figure 12, step 12). When the Host Operator has the customer slice template in its NSMF, the slice deployment begins through the respective domain NSMF on the infrastructure of the Host Operator. If the federated slice request is accepted, the Slice Federation Manager of each operator updates its slice federation status, and if needed more services related to the user´s slice is federated next, such as a UPF, or applications like xApps in O-RAN-based architectures.

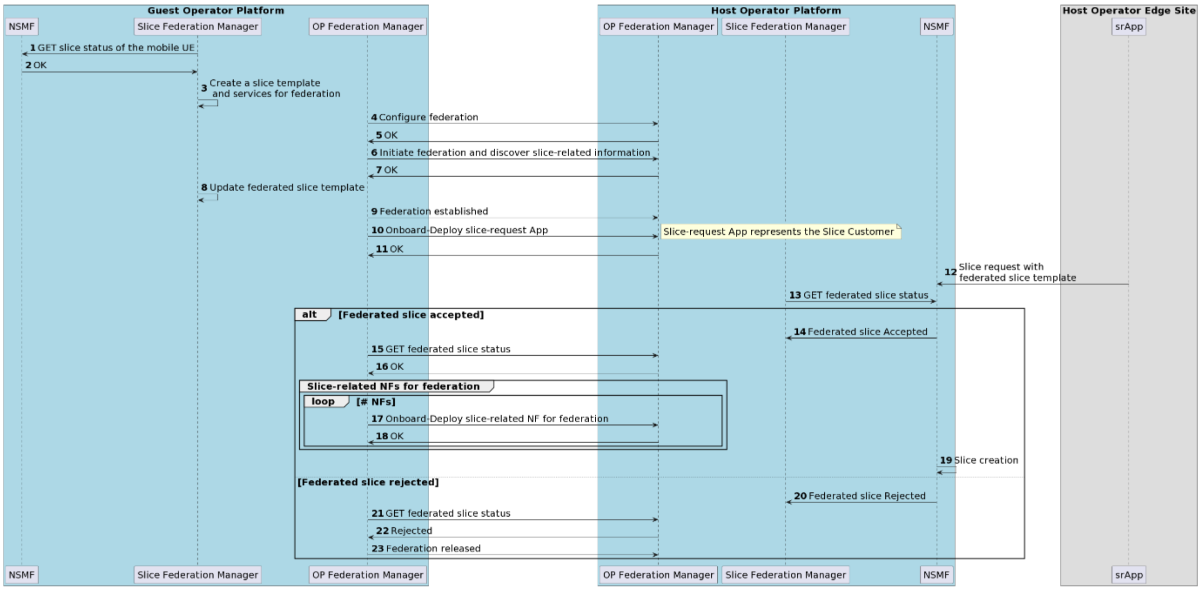

Guest Operator Platform
Host Operator Platform
Host Operator Edge Site
NSMF
Slice Federation Manager
OP Federation Manager
OP Federation Manager
Slice Federation Manager
NSMF
srApp
1 GET slice status of the mobile UE
2 OK
3 Create a slice template and services for federation
4 Configure federation
5 OK
6 Initiate federation and discover slice-related information
7 OK
8 Update federated slice template
9 Federation established
10 Onboard-Deploy slice-request App
Slice-request App represents the Slice Customer
11 OK
12 Slice request with federated slice template
13 GET federated slice status
alt [Federated slice accepted]
14 Federated slice Accepted
15 GET federated slice status
16 OK
Slice-related NFs for federation
loop [# NFs]
17 Onboard-Deploy slice-related NF for federation
18 OK
19 Slice creation
[Federated slice rejected]
20 Federated slice Rejected
21 GET federated slice status
22 Rejected
23 Federation released
NSMF
Slice Federation Manager
OP Federation Manager
OP Federation Manager
Slice Federation Manager
NSMF
srApp

Figure 12: Slice Federation flowchart between two network operators.

The above steps outline the process of network slice federation, demonstrating the role of the Slice Federation Manager and the flow of information between the various components involved. Overall, slice federation enables seamless connectivity and service continuity for users across different operators' networks, providing a consistent and unified network experience.

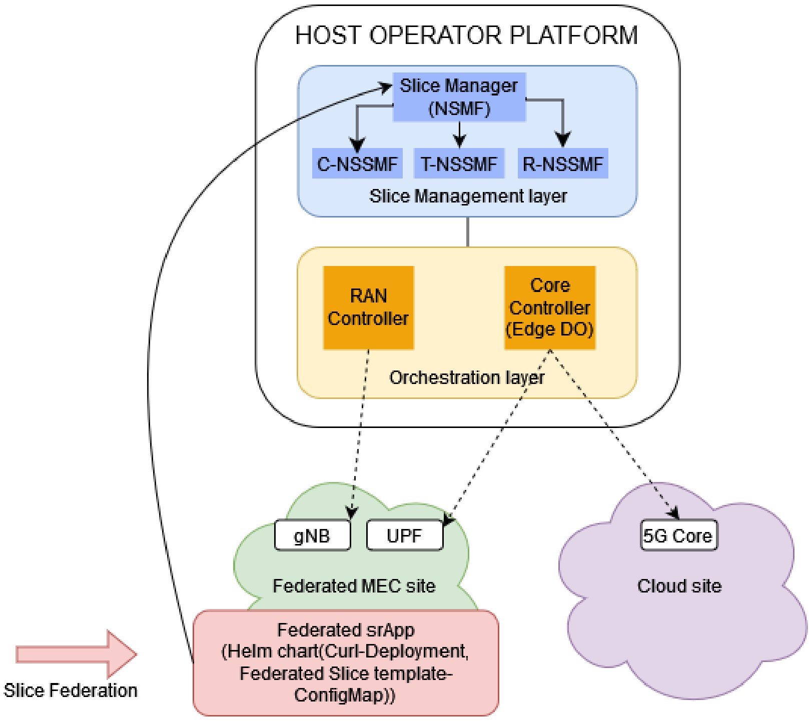
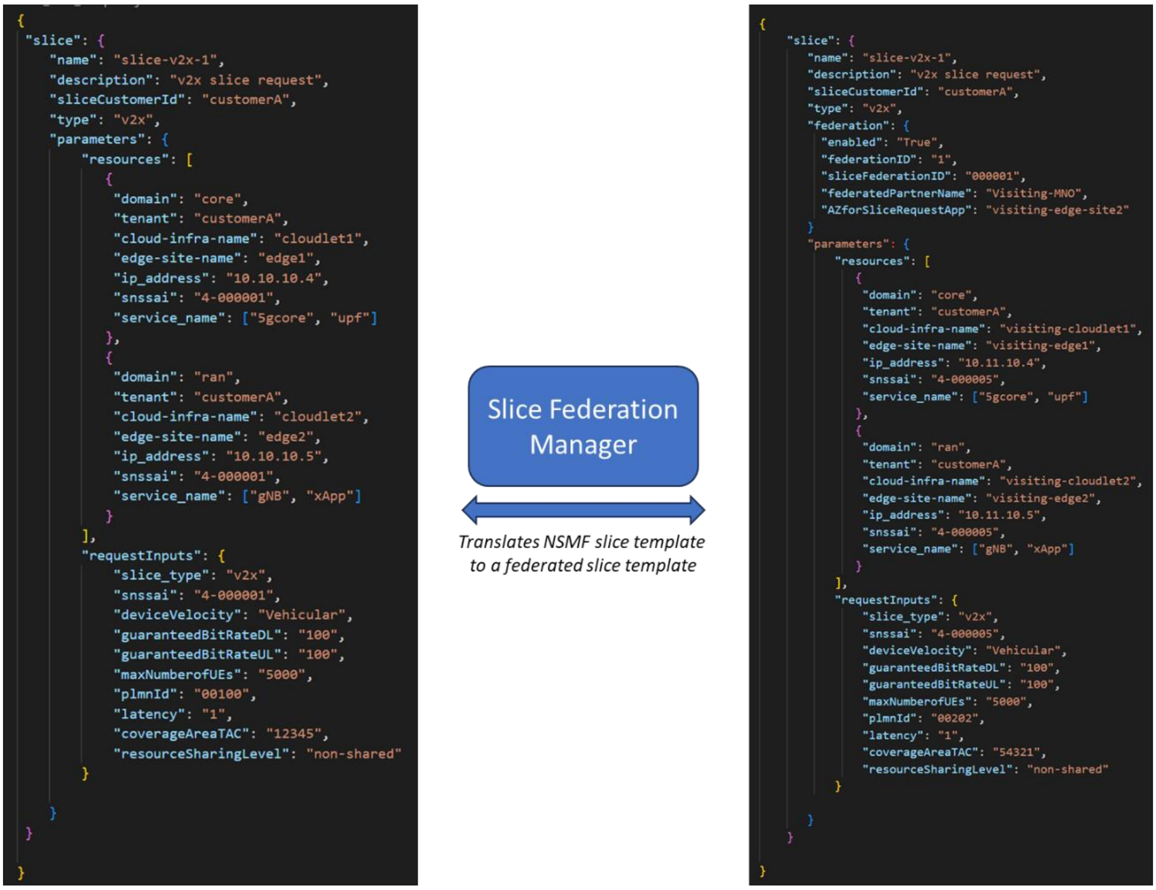


Figure 13: srApp representing the Slice Customer and triggering the federated slice request.

To delve into the intricacies of slice federation by leveraging edge federation, an application representing the slice customer is federated as a service and is deployed in the edge site of the Host Operator, and when it runs, it triggers a request to the NSMF of the Host Operator. Figure 13 illustrates an example where the federated slice template contains resources for the RAN and core network only and is initiated from the federated srApp to the NSMF of the Host Operator. An example of such a service encapsulating the federated slice request can be seen in Figure 14 as a curl Kubernetes-based microservice with the federated template as a ConfigMap Kubernetes resource, while the translation of the slice template is illustrated in Figure 15. It is shown that without federation the template has only information about the slice customer order. When a slice is federated additional information for federation is added, while many values need to be overwritten by the Host Operator telco infrastructure, like the edge sites, Kubernetes cluster IPs, as well as mobile network identifiers. Consequently, in scenarios where end-users need to switch from their home network towards the visiting network while maintaining uninterrupted service and network experience, the proposed method enables the provisioning of services or slices within the telco edge-cloud infrastructure of another operator.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: curl-deployment
spec:
  replicas: 1
  selector:
    matchLabels:
      app: curl
  template:
    metadata:
      labels:
        app: curl
    spec:
      containers:
        - name: curl
          image: curlimages/curl
          command: ["curl", "-X", "POST", "-d", "@/federated_slice_template.json", "http://slicemamager.visitingoperator.com/api/slice/create"]
          volumeMounts:
            - name: request-volume
              mountPath: "/federated_slice_template.json"
              subPath: federated_slice_template.json
      volumes:
        - name: request-volume
          configMap:
            name: request-configmap
```

Figure 14: A Kubernetes deployment manifest example to request the slice requirements to the Host Operator.



```
{
  "slice": {
     "name": "slice-v2x-1",
     "description": "v2x slice request",
     "sliceCustomerId": "customerA",
     "type": "v2x",
     "parameters": {
         "resources": [
            {
             "domain": "core",
             "tenant": "customerA",
             "cloud-infra-name": "cloudlet1",
             "edge-site-name": "edge1",
             "ip_address": "10.10.10.4",
             "snssai": "4-000001",
             "service_name": ["5gcore", "upf"]
            },
            {
             "domain": "ran",
             "tenant": "customerA",
             "cloud-infra-name": "cloudlet2",
             "edge-site-name": "edge2",
             "ip_address": "10.10.10.5",
             "snssai": "4-000001",
             "service_name": ["gNB", "xApp"]
            }
         ],
         "requestInputs": {
             "slice_type": "v2x",
             "snssai": "4-000001",
             "deviceVelocity": "Vehicular",
             "guaranteedBitRateDL": "100",
             "guaranteedBitRateUL": "100",
             "maxNumberofUEs": "5000",
             "plmnId": "00100",
             "latency": "1",
             "coverageAreaTAC": "12345",
             "resourceSharingLevel": "non-shared"
         }

     }
  }

}
```

Slice Federation Manager
Translates NSMF slice template to a federated slice template

```
{
    "slice": {
       "name": "slice-v2x-1",
       "description": "v2x slice request",
       "sliceCustomerId": "customerA",
       "type": "v2x",
       "federation": {
         "enabled": "True",
         "federationID": "1",
         "sliceFederationID": "000001",
         "federatedPartnerName": "Visiting-MNO",
         "AZforSliceRequestApp": "visiting-edge-site2"
       }
       "parameters": {
           "resources": [
              {
               "domain": "core",
               "tenant": "customerA",
               "cloud-infra-name": "visiting-cloudlet1",
               "edge-site-name": "visiting-edge1",
               "ip_address": "10.11.10.4",
               "snssai": "4-000005",
               "service_name": ["5gcore", "upf"]
              },
              {
               "domain": "ran",
               "tenant": "customerA",
               "cloud-infra-name": "visiting-cloudlet2",
               "edge-site-name": "visiting-edge2",
               "ip_address": "10.11.10.5",
               "snssai": "4-000005",
               "service_name": ["gNB", "xApp"]
              }
           ],
           "requestInputs": {
               "slice_type": "v2x",
               "snssai": "4-000005",
               "deviceVelocity": "Vehicular",
               "guaranteedBitRateDL": "100",
               "guaranteedBitRateUL": "100",
               "maxNumberofUEs": "5000",
               "plmnId": "00202",
               "latency": "1",
               "coverageAreaTAC": "54321",
               "resourceSharingLevel": "non-shared"
           }

       }
    }

}
```

Figure 15: Examples of slice template from NSMF (left) and federated slice template on Slice Federation Manager (right).

2.4.3 Network Slicing for non-3GPP Technologies

As the network infrastructure layer of 5GMED is heterogeneous including several radio access technologies (i.e., satellite, C-V2X, IEEE 802.11ad) in addition to the 5G RAN, the QoS guarantees provided by the 5G network slicing should be also guaranteed when a UE moves from 5G to other radio technologies. Two approaches are considered in 5GMED to ensure 5G slicing continuity:

- For **satellite technology**, the 5GMED consortium has integrated a slice manager that guarantee the continuity of the 5G slicing as explained in D3.2 [14].
- The **C-V2X radio access network** in the 5GMED project is designed as a private network serving one slice that provides the QoS requirements of use case 2. One UE in use case 2 will have the same QoS guarantees provided by the 5G slicing mechanisms when changing to the C-V2X network and vice versa.
- The **IEEE 802.11ad radio access network** in the 5GMED project is designed as a private network serving one slice that provides the QoS requirements of use case 3. In other words, a UE in use case 3 will have the same QoS guarantees provided by the 5G slicing mechanisms when changing to IEEE 802.11ad radio access network and vice versa.

2.5 Cloud Layer

In the cloud layer (shown in Figure *16*), all back-end centralized application servers can be deployed. The layer is subdivided into private and public clouds. The public cloud hosts third-party applications such as the applications of UC1 that are hosted in Amazon Web Services (AWS). The private cloud hosts mainly the MNOs core networks, the corresponding dashboard, and third-party applications that are directly managed by the service providers such as the road operator or train infrastructure operator (e.g., the applications of UC2, UC3 and UC4). The decision to deploy the third-party applications on private or public clouds depends on the service provider policies and strategies. It should be noted that implementing the third-party applications in the private clouds will allow more flexibility in the management of these applications, especially when using an orchestrator.

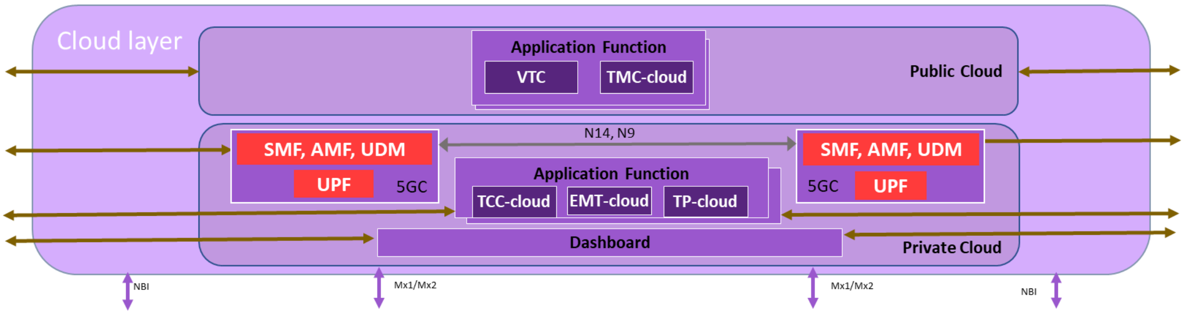


Figure 16: Cloud layer components

On the core network side, the private cloud also includes the control plane functions of the 5G networks. In addition, it includes the centralized User Plane Function (UPF) for each Mobile Network Operator (MNO).

The dashboard is used to: 1) monitor network and service Key Performance Indicators (KPIs), and 2) provide the configuration parameters for orchestrators, network slicing managers, and infrastructure. In 5GMED, we will have only several service KPIs dashboards to facilitate visualization in each use case and there will be different dashboards for each MNO.

Funded by the Horizon 2020 Framework Programme of the European Union

The cloud layer interacts with the data analytics layer to provide the latter with the needed data and to initiate the AI modules required by the applications. In addition, the data analytics layer will provide the dashboard with the different KPIs collected from the different layers. Furthermore, the cloud layer interacts with the slice management layer through the Mx1/Mx2 interface to provide the configuration of the different slices. Finally, it interacts with the orchestration layer to configure the Edge DO through the NBI interface.

2.6 Data Analytics Layer

The data analytics layer makes the Artificial Intelligence (AI) paradigm an integrated part of the 5GMED cross-border network architecture and not just a set of algorithms provided by service providers. It includes a set of AI modules designed and deployed by the network operators and that can be used by them or any service provider to optimize either network performance or service performance. In the case of 5GMED, an AI module has been developed for use case 4, the Data Analytics Module (DAM), as described in Section 3.7. In addition, the Data Analytics layer should contain a data lake where all the data required by these modules will be stored. These data include network and service KPIs, in addition to enrichment information that are collected by the different sensors deployed in the network. As AI is not a focus of 5GMED, the data lake is not developed during the project and left for future work.

The AI modules of the Data Analytics layer should be designed with open APIs that allow third-party applications to interact with them. The AI modules can use real-time data collected from the network or the application servers, or historical data saved in the data lake. Therefore, the following interfaces are proposed:

- Data analytics – Cloud interface: This bi-directional interface allows the data analytics to collect context information from the application servers, such as the speed of the vehicles, videos, and images from sensors and lidars, etc. Additional information can be also extracted from the core network, such as latency and throughput of connected vehicles/users. The collected data will allow the AI modules in this layer to exploit additional information that can help in optimizing the network/service. In addition, this interface will allow the decisions of the AI modules to be communicated to the applications. For instance, if in UC1 the AI module detects in reduction in the QoS, it can notify the tele-operation center with an alarm to reduce the speed. Finally, this interface can be used by the dashboard to access the information stored in the data lake from the different layers in order to show them.

- Data analytics – Network slicing interface: Similar to the previous interface, it provides access to the network slices-related information, which can be used later on by the AI modules together with other collected information, for instance, to dynamically adjust the configuration of the slices. The decisions of the AI module will be communicated to the NSMF through this interface too.

- Data analytics – Orchestration interface: This bi-directional interface allows the data analytics layer to collect data related to the radio technologies and transport network. In addition, it will allow a collaboration between the two layers to find the best decision and communicate it to the concerned module(s) in the network infrastructure layer and MEC layer.

- Data analytics – MEC interface: This is very similar to the first interface except for the dashboard that does not exist in this layer. It will be used for the applications and network elements that are deployed in a distributed way.

As mentioned before and to optimize the performance of the applications and network, the AI modules in this layer will have full access to network and services information stored in the data lake. However, this will not jeopardize network data privacy as no information will be exposed to external modules. On one side, service providers will have access to AI modules that can optimize their services. On the other side, the MNOs will be able to provide better services for their clients without exposing any of their sensitive information. To provide descriptive information about the AI modules to the service providers who want to use them, the data analytics layer shall contain catalogues with AI modules descriptor files.

It should be noted that this layer is a theoretical proposal by 5GMED and only one AI module will be developed, which is the DAM.

For each application, the orchestrator will create and manage the AI module instances either in the MEC or in the cloud depending on application preference and AI module functionality. At the border the orchestrator should trigger the same AI module in the visited network when needed in addition to the exchange of information.

Funded by the Horizon 2020 Framework Programme of the European Union

3. Castellolí Small-Scale Test Site

The Castellolí small-scale test site is located 55 km north-west of Barcelona and is part of the Parcmotor Circuit, illustrated in Figure 17, a test track rented by OEMs (Original Equipment Manufacturers) for stress tests of vehicles [15]. It features two private 5G SA networks operated by Cellnex, and its premises host both the test 5G networks and the datacenter where most of 5GMED services are running. Castellolí small-scale test site provides a reliable testing environment that enables partners to refine and improve the 5GMED services before deployment in real-world scenarios. The following sections describe in detail the implementation of the test site.

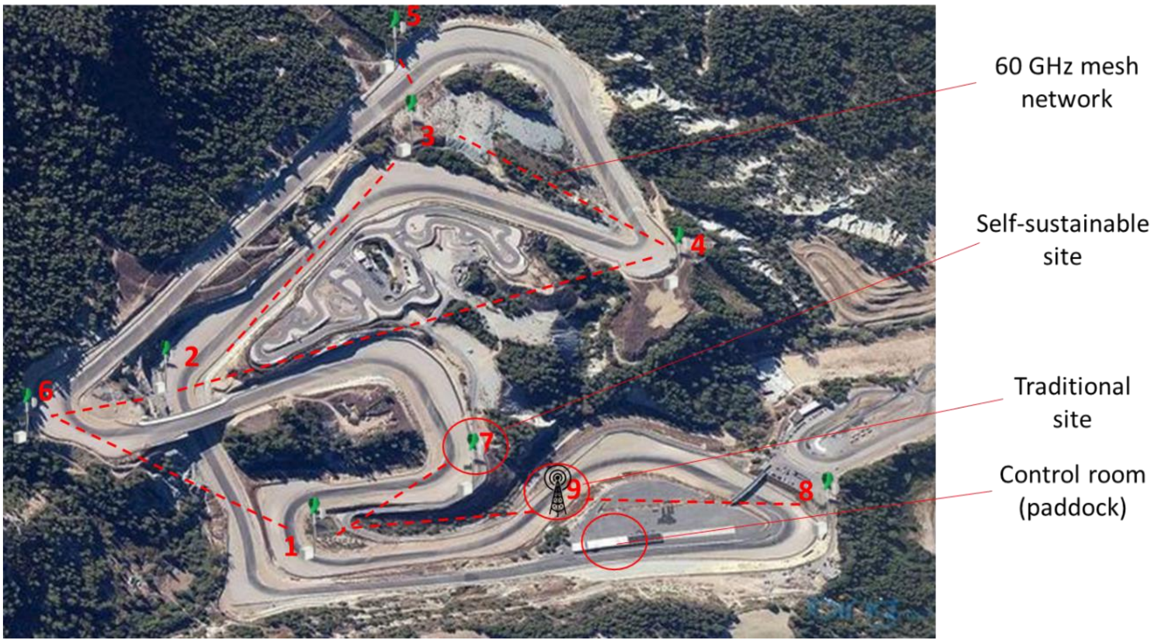


Figure 17: Overview of the small-scale test site at Castellolí Parcmotor circuit

3.1 End-to-End Architecture Implementation

The end-to-end cross-border network architecture implemented in Castellolí test site is based on the 5GMED cross-border network architecture described in Section 2 and depicted in Figure 1.

Figure 18 represents the physical implementation of the 5GMED cross-border network architecture layers in Castellolí. 5GMED has deployed and tested two 5G SA networks representing the cross-border scenario with one Spanish MNO and one French MNO with Home Routed roaming. The network infrastructure integrates a multi-vendor 5G RAN (Ericsson, Sunwave), which operates in the experimental N77 band, as well as one MEC server and one orchestrator for each MNO and local private servers.

In the rest of this section, the implementation of the network infrastructure layer, MEC layer, orchestration layer, slice management layer, cloud layer, and data analytics layer are described, respectively, in Section 3.2, Section 3.3, Section 3.4, Section 3.5, Section 3.6, and Section 3.7.

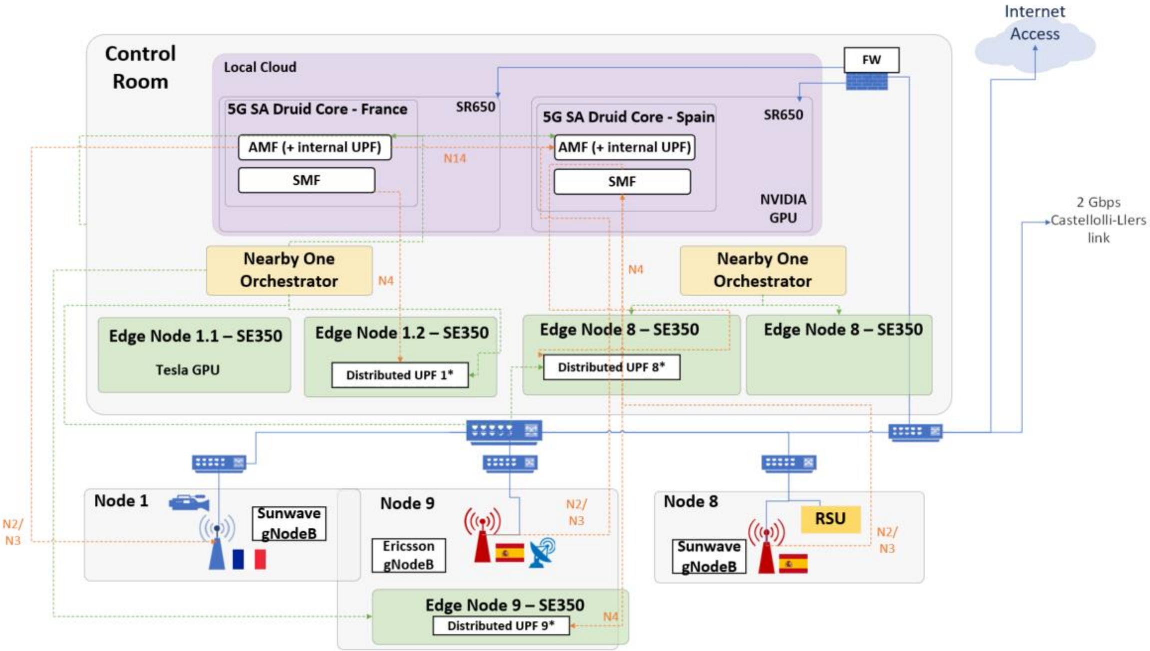


Figure 18: Physical implementation of the 5GMED cross-border network architecture in Castellolí small-scale test site

3.2 Network Infrastructure Layer

In this section, we describe the network infrastructure layer of the two 5G SA networks deployed in the Castellolí small-scale test site, including the equipment that composes the 5G Radio Access network in Section 3.2.1, the 5G Core deployment and specifications in Section 3.2.2, the transport network in Section 3.2.3, and the C-V2X Roadside units in Section 3.2.4.

3.2.1 5G Radio Access Network

The 5G Radio Access Network deployed in Castellolí consists of three gNodeBs (represented as node 1, node 8, and node 9 in Figure 18) of two distinct types:

- Two Sunwave 5G small cells (4x4 MIMO) with one sector each.
  - Node 1: One cell connected to the "French" core with PLMN-id 99999.
  - Node 8: One cell connected to the "Spanish" core with PLMN-id 00101.

Node 9: One Ericsson macro site (Massive MIMO 64x64 antennas per sector) with three sectors, connected to "Spanish" core with PLMN-id 00101.*Figure 19* depicts the location of each gNodeB in Castellolí and Table 4 provides global information related to each site. Finally,

Table *5* details the composition of each site.

Site name	Cell type	MIMO type	Equipment provider	Affected PLMN Country	Affected PLMN-id
Node 9	macro site with 3 cells	64x64 per sector	Ericsson	Spain	00101
Node 8	small cell	4x4	Sunwave	Spain	00101
Node 1	small cell	4x4	Sunwave	France	99999

Table 4: Features of the gNodeBs at the Castellolí small-scale test site

Site name	Product type	Product name	Product details	illustration
Node 9 (Ericsson gNodeB)	**Ericsson Advanced Antenna System (AAS)**	**Ericsson Air 6449 B77D**	• 64TX/64RX • Max total carrier BW is 200MHz for NR • 4 x 25 Gbps eCPRI • Weight: 37 – 47 kg (band dependent) • -48 VDC (3-wire or 2-wire) • -40 to +55̊ C • Support number of layers: DL/UL 16/8 • Up to 100 watts of power transmission. Current TX power set to 1W. • Bandwith: 100 Mhz in band n77. (3800 – 3900 MHz) • ARFCN DL: 656666 • ssbFrequency: 654048 • GSCN: 8062 • Tranmission: Optical fiber 1 Gpbs	
	Ericsson Baseband Unit	**Ericsson Baseband 6641**	• 19 inch wide, 1U high, 352mm deep • 1 x 4x25 Gbps (QSFP28) • 3 x 25/10/1Gbps ports (SFP28/SFP+/SFP) • 1 x 100Mbps/1Gbps RJ45 electrical port • Support for NR (5G high/AAS/mid/low band) or LTE • Support for Mixed Mode baseband NR (5G) + LTE • 9 x 2.5/4.9/9.8/10.1/10.3/24.3/25 Gbps Radio Interface ports • 9 eCPRI ports • Dual -48VDC power feeding • Built-in cell site router functionality • E5 interface for Elastic RAN / NR Advanced RAN coordination	

Site name	Product type	Product name	Product details	illustration
Node 1 and Node 8 (Sunwave gNodeBs)	Sunwave Antenna	JZD – 65DPG1515-3842T0	• 4 ports antenna • 15 dBi Gain • Bandwith: 3800-4200 MHz	
	Sunwave RRU	sCELL-3470RRU	• Product Name: sCELL-3470RRU • 4T4R • Max total carrier BW is 100MHz for NR • 5W (37 dBm) Output Power • Bandwith: 100 MHz in band n77. (3800 – 3900 MHz) • Weight 12Kg • 48 VDC	
	Sunwave Baseband Unit	-	• 2x RJ-45 100/1000 BASE-T Ethernet Port • 4 x 10Gbps ports SFP+ Ethernet Port • 4 x Radio Interface ports	

Table 5: Composition of gNodeBs at the Castellolí small-scale test site

Funded by the Horizon 2020 Framework Programme of the European Union

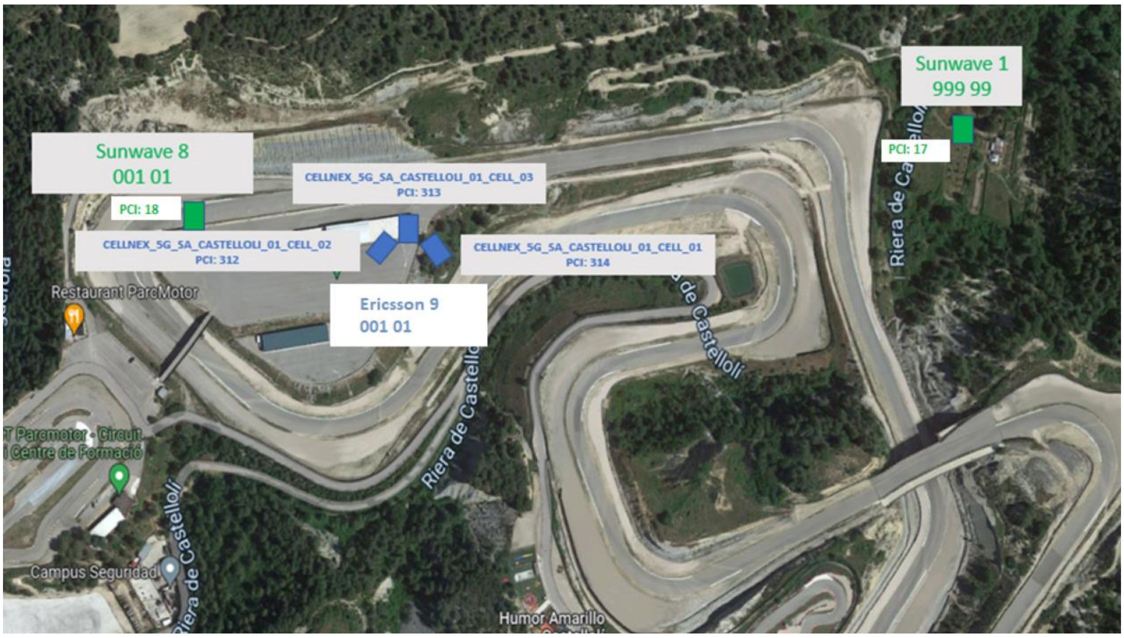


Figure 19: Location of gNodeBs and radio sectors in Castellolí test site.

3.2.2 5G Core Network

3.2.2.1 5G Core by Druid

In 5GMED, the 5G Core deployed in Castellolí has been supplied by **Druid**, an Irish company specialized in 4G/5G private network solutions. The solution is composed of two 5G Core instances, running on different servers, each one covering one country (Spain and France). The deployed solution consists of a **5G Stand-Alone (SA)** configuration with the following network functions: AMF, SMF, UDM, AUSF, and centralized and distributed UPFs. The same solution has been deployed in the two 5G cores. There are two distributed UPFs, one on the French side (node 1) and the other on the Spanish side (node 8).

The requirements of the 5G Core network are presented in Section 2.1.1. Below is described how these requirements are fulfilled by the Druid 5G Core:

1. **Home-routed roaming with support of visited PLMN**. This functionality is already available in the system currently deployed.
2. **LBO roaming**. This functionality is already available in the system currently deployed.
3. **N14 optimization.** N14 functionality is already available in idle mode and connected mode.
4. **Equivalent PLMN.** Already available.
5. **In the LBO roaming, keep the application always connected.** No date provided for availability yet.
6. **In LBO, possibility to publish the new IP address of the UE to third party modules.** Already available.
7. **Availability of Network Repository Function (NRF) and its interface to integrate Network Data Analytics Function (NWDAF).** Not included in the roadmap of Druid.

Druid provides a technology platform called **Raemis**, which consists of cellular software assets optimized for business use cases. This platform offers mobile communication solutions that are tailored to meet the needs of enterprises. The current **Raemis**’s version deployed in both 5Gcores is: **Raemis Enterprise v5.7.0.0.Tiger73.Cellnex05.**

The Raemis functionality that has been implemented in 5GMED has the following characteristics:

- Dashboard.
- 5G private network with private subscribers, private cell network, N2 handover, Idle mode cell reselection, UE attachment/implicit detach/re-attach, and data service.
- Real-time System Monitoring.
- Cells Management.
- Network Management including 5G data slicing.
- Alarm Monitoring.
- System management.
- Traffic separation.
- QoS of Service per user group.
- Access control per user or user group.

Four Packet Data Networks (PDNs) have been created, each of them being associated with an enterprise VLAN. The VLAN segregation has also been used for the slicing. These PDNs enable the separation of users, load balancing, and QoS allocation.

The Raemis software includes features to monitor UE activity and system status. The following are screenshots of the Spanish and French Raemis GUI:

- Figure 20 shows a general status of the Raemis system displaying attached users, activity, and cells status.
- Figure 21 shows the user’s IMSIs with information related to associated device. Additionally, when a user is attached, that screen shows its assigned IP.
- Figure 22 shows gNodeB configuration. For example, this gNodeB (10) has been associated with PLMN-id 99999.
- Figure 23 shows the different Cells connected to the 5GCore with their respective status, IPs and PLMN.
- Figure 24 shows the interfaces and their configuration.

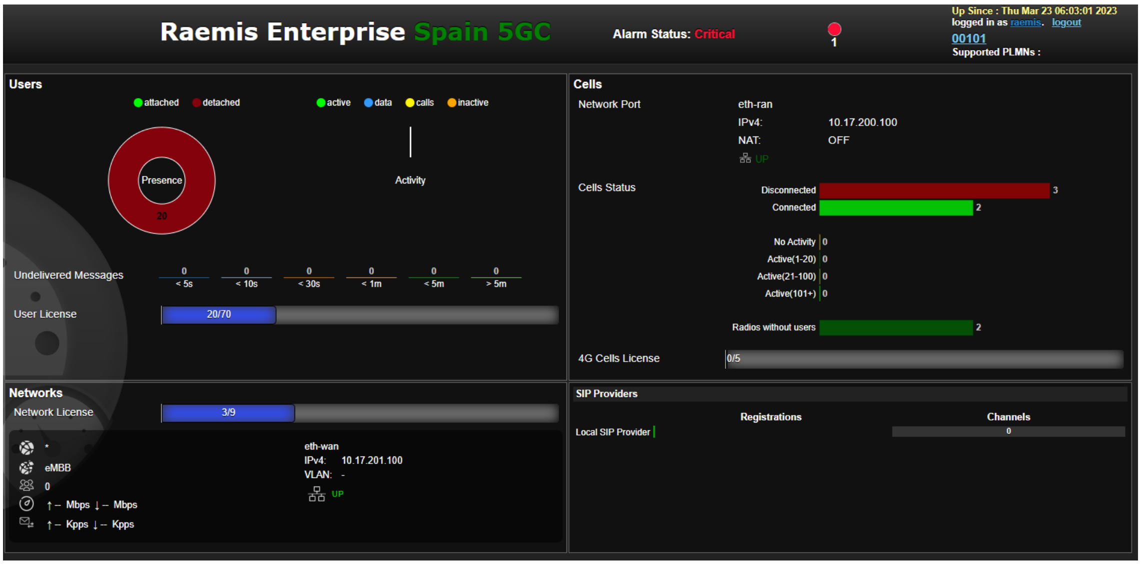
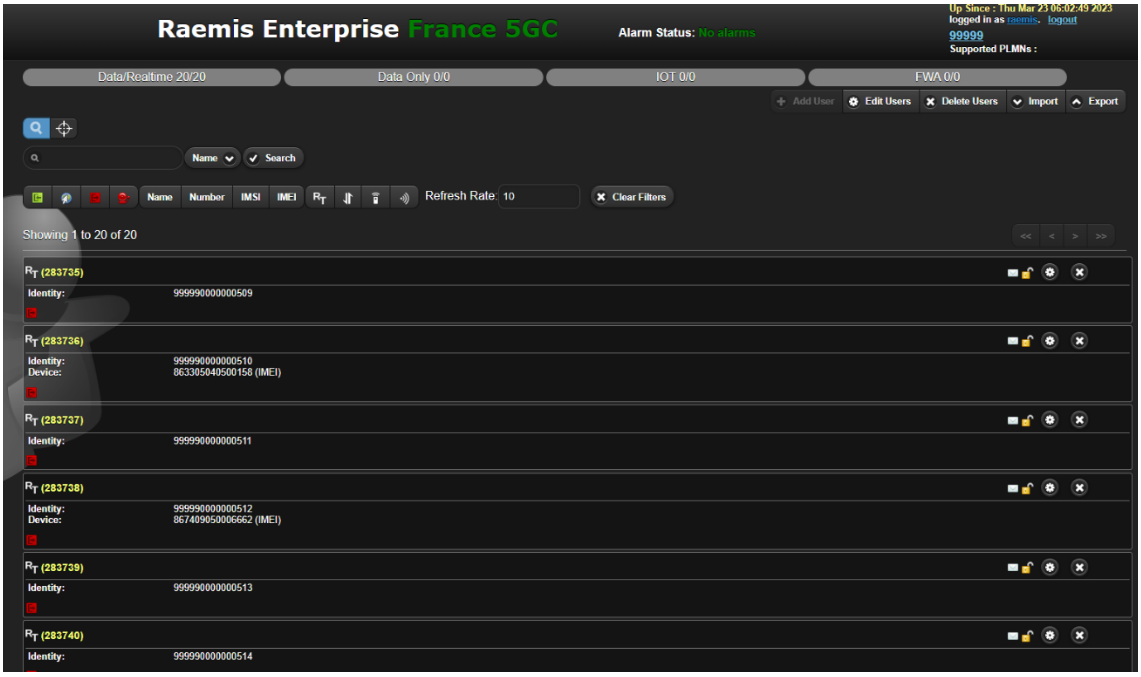


Figure 20: Dashboard example for the Spanish 5G Core



Showing 1 to 20 of 20

RT (283735)
Identity: 999990000000509

RT (283736)
Identity: 999990000000510
Device: 863305040500158 (IMEI)

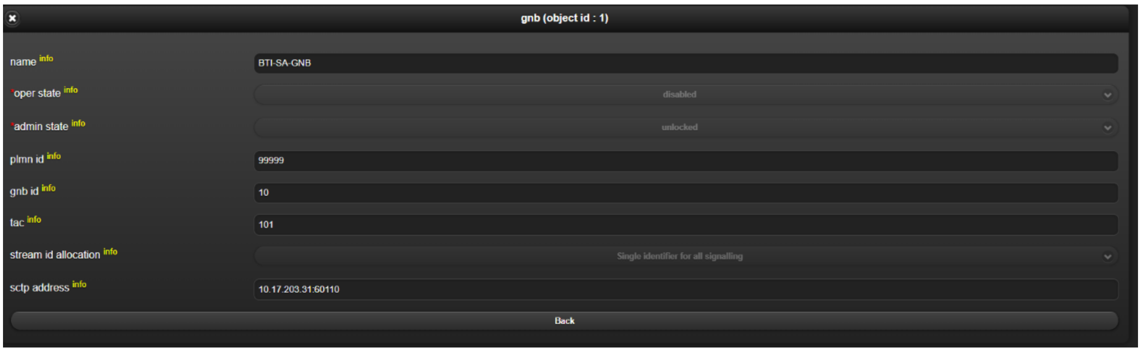
RT (283737)
Identity: 999990000000511

RT (283738)
Identity: 999990000000512
Device: 867409050006662 (IMEI)

RT (283739)
Identity: 999990000000513

RT (283740)
Identity: 999990000000514

Figure 21: User's menu example for the French 5G Core

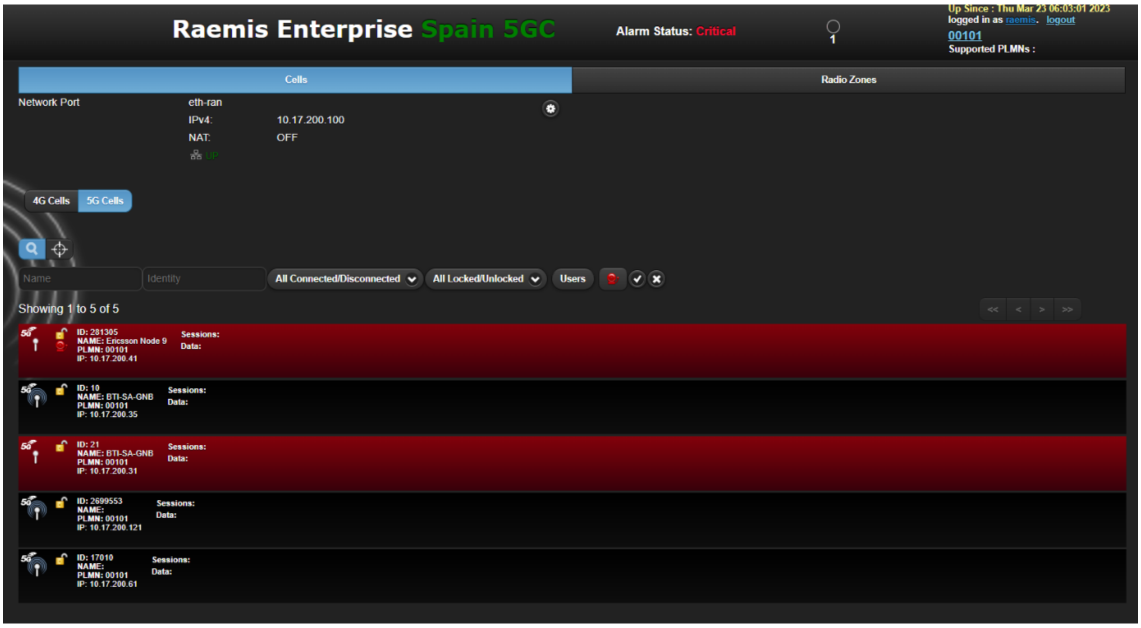


gnb (object id : 1)

name info	BTI-SA-GNB
*oper state info	disabled
*admin state info	unlocked
plmn id info	99999
gnb id info	10
tac info	101
stream id allocation info	Single identifier for all signalling
sctp address info	10.17.203.31:60110

Figure 22: gNodeB menu example for the French 5G Core

Funded by the Horizon 2020 Framework Programme of the European Union



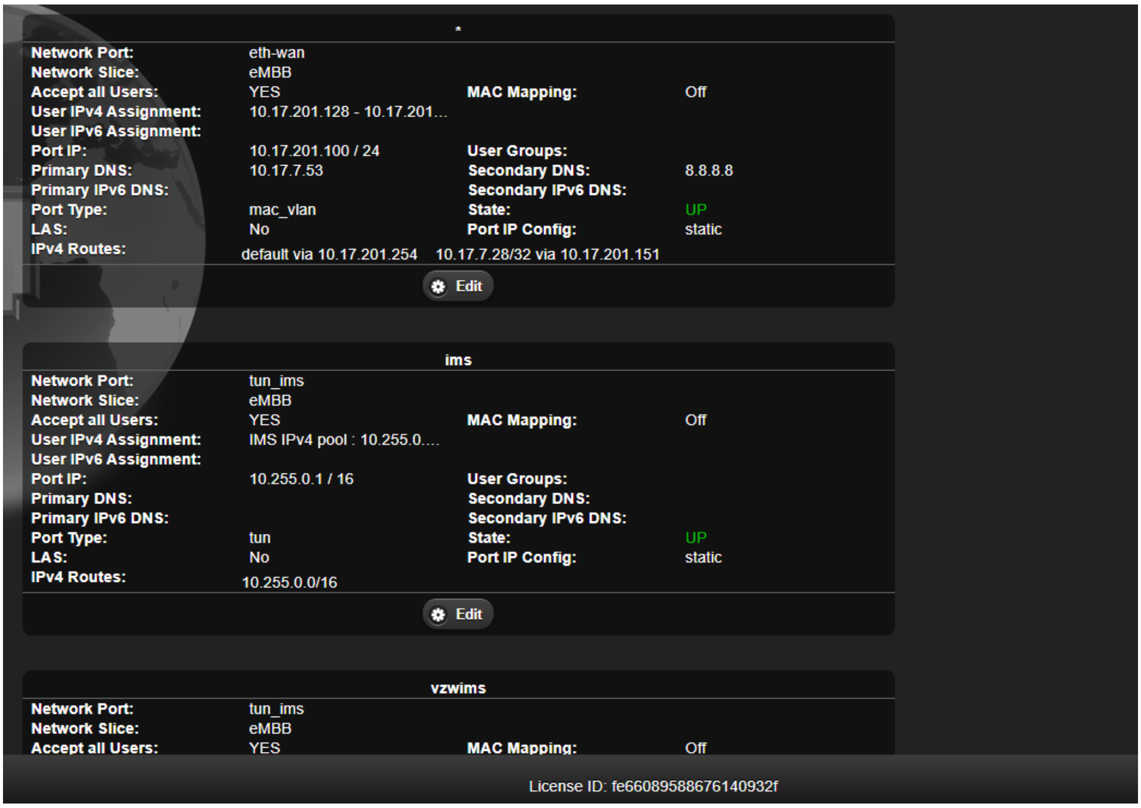
Up Since : Thu Mar 23 06:03:01 2023
logged in as raemis. logout
00101
Supported PLMNs :

Network Port	eth-ran	
	IPv4:	10.17.200.100
	NAT:	OFF
	UP	

Showing 1 to 5 of 5

ID: 281305 NAME: Ericsson Node 9 PLMN: 00101 IP: 10.17.200.41	Sessions: Data:
ID: 10 NAME: BTI-SA-GNB PLMN: 00101 IP: 10.17.200.35	Sessions: Data:
ID: 21 NAME: BTI-SA-GNB PLMN: 00101 IP: 10.17.200.31	Sessions: Data:
ID: 2699553 NAME: PLMN: 00101 IP: 10.17.200.121	Sessions: Data:
ID: 17010 NAME: PLMN: 00101 IP: 10.17.200.61	Sessions: Data:

Figure 23: Cell menu example for the Spanish 5G Core



*

Network Port:	eth-wan		
Network Slice:	eMBB		
Accept all Users:	YES	**MAC Mapping:**	Off
User IPv4 Assignment:	10.17.201.128 - 10.17.201...		
User IPv6 Assignment:			
Port IP:	10.17.201.100 / 24	**User Groups:**	
Primary DNS:	10.17.7.53	**Secondary DNS:**	8.8.8.8
Primary IPv6 DNS:		**Secondary IPv6 DNS:**	
Port Type:	mac_vlan	**State:**	UP
LAS:	No	**Port IP Config:**	static
IPv4 Routes:	default via 10.17.201.254 10.17.7.28/32 via 10.17.201.151		

ims

Network Port:	tun_ims		
Network Slice:	eMBB		
Accept all Users:	YES	**MAC Mapping:**	Off
User IPv4 Assignment:	IMS IPv4 pool : 10.255.0....		
User IPv6 Assignment:			
Port IP:	10.255.0.1 / 16	**User Groups:**	
Primary DNS:		**Secondary DNS:**	
Primary IPv6 DNS:		**Secondary IPv6 DNS:**	
Port Type:	tun	**State:**	UP
LAS:	No	**Port IP Config:**	static
IPv4 Routes:	10.255.0.0/16		

vzwims

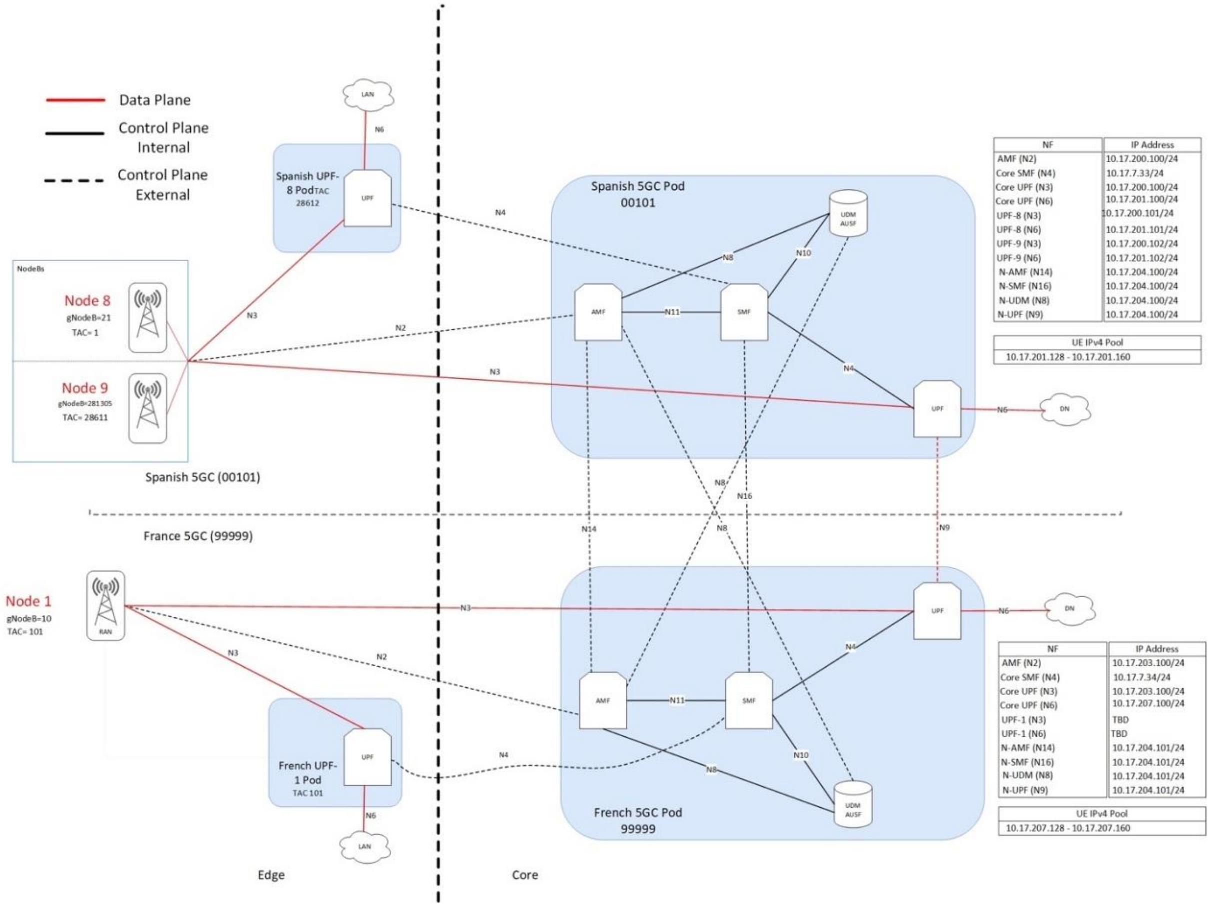
Network Port:	tun_ims		
Network Slice:	eMBB		
Accept all Users:	YES	**MAC Mapping:**	Off

License ID: fe66089588676140932f

Figure 24: Network menu example for Spanish 5G Core

Figure 25 shows the internal architecture of the 5G SA networks that have been implemented in the test site at Castellolí. The block diagram includes the NFs in the 5G Core of each country (Spain and France), the interfaces between NFs, the interfaces between the 5G Cores and 5G RAN, and the cross-border interfaces. As it can be observed in

Figure 25, this implementation matches with the design of the 5G SA networks that are targeted for the corridor deployment shown in Figure 3, but with a reduced number of gNodeBs in the 5G RAN of each country. The two 5G Cores have been deployed in two separated **Lenovo SR-650 servers** (one in each server) placed in the same rack as depicted in Figure 26.



NF	IP Address
AMF (N2)	10.17.200.100/24
Core SMF (N4)	10.17.7.33/24
Core UPF (N3)	10.17.200.100/24
Core UPF (N6)	10.17.201.100/24
UPF-8 (N3)	10.17.200.101/24
UPF-8 (N6)	10.17.201.101/24
UPF-9 (N3)	10.17.200.102/24
UPF-9 (N6)	10.17.201.102/24
N-AMF (N14)	10.17.204.100/24
N-SMF (N16)	10.17.204.100/24
N-UDM (N8)	10.17.204.100/24
N-UPF (N9)	10.17.204.100/24

UE IPv4 Pool
10.17.201.128 - 10.17.201.160

NF	IP Address
AMF (N2)	10.17.203.100/24
Core SMF (N4)	10.17.7.34/24
Core UPF (N3)	10.17.203.100/24
Core UPF (N6)	10.17.207.100/24
UPF-1 (N3)	TBD
UPF-1 (N6)	TBD
N-AMF (N14)	10.17.204.101/24
N-SMF (N16)	10.17.204.101/24
N-UDM (N8)	10.17.204.101/24
N-UPF (N9)	10.17.204.101/24

UE IPv4 Pool
10.17.207.128 - 10.17.207.160

Figure 25: Internal architecture of the 5G SA networks deployed in the small-scale test site of Castellolí

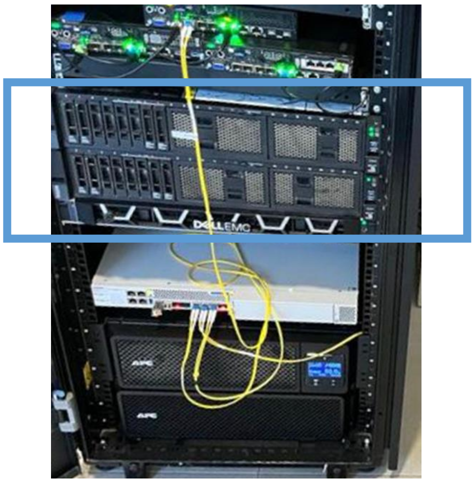


Figure 26: Castellolí Rack with SR650 Lenovo servers that host the two 5G Cores

Druid has provided 20 SIM cards for each PLMN-id, as illustrated in Table 6 and Table 7.

ICCID	MSISDN	IMSI
83705	283705	1010000045495
83706	283706	1010000045496
83707	283707	1010000045497
83708	283708	1010000045498
83709	283709	1010000045499
83710	283710	1010000045500
83711	283711	1010000045501
83712	283712	1010000045502
83713	283713	1010000045503
83714	283714	1010000045504
83715	283715	1010000045505
83716	283716	1010000045506
83717	283717	1010000045507
83718	283718	1010000045508
83719	283719	1010000045509
83720	283720	1010000045510
83721	283721	1010000045511
83722	283722	1010000045512
83723	283723	1010000045513
83724	283724	1010000045514

Table 6: Spanish SIM cards

ICCID	MSISDN	IMSI
83725	283725	999990000000499
83726	283726	999990000000500
83727	283727	999990000000501
83728	283728	999990000000502
83729	283729	999990000000503
83730	283730	999990000000504
83731	283731	999990000000505
83732	283732	999990000000506
83733	283733	999990000000507
83734	283734	999990000000508
83735	283735	999990000000509
83736	283736	999990000000510
83737	283737	999990000000511
83738	283738	999990000000512
83739	283739	999990000000513
83740	283740	999990000000514

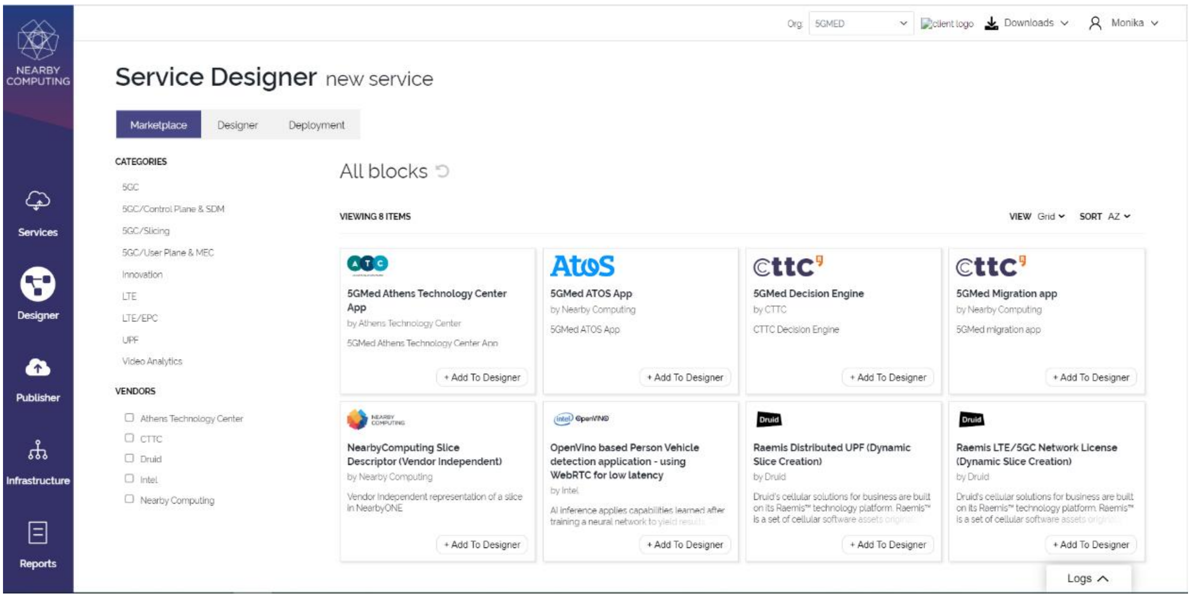
Funded by the Horizon 2020 Framework Programme of the European Union

ICCID	MSISDN	IMSI
83741	283741	999990000000515
83742	283742	999990000000516
83743	283743	999990000000517
83744	283744	999990000000518

Table 7: French SIM cards

3.2.2.2 5G Core Deployment via NearbyOne Orchestrator

The 5G Core may be deployed manually, or through the orchestrator. For 5GMED, the core is deployed as a service through the NearbyOne orchestrator described in Section 3.4 as part of the orchestrator's onboarded application in its Marketplace. The image below shows the NearbyOne Marketplace, the onboarded applications for 5GMED are displayed alongside the 5G Core and the distributed UPFs, which Druid provides.



Service Designer new service

All blocks

VIEWING 8 ITEMS

5GMed Athens Technology Center App
by Athens Technology Center
5GMed Athens Technology Center Ann

5GMed ATOS App
by Nearby Computing
5GMed ATOS App

5GMed Decision Engine
by CTTC
CTTC Decision Engine

5GMed Migration app
by Nearby Computing
5GMed migration app

NearbyComputing Slice Descriptor (Vendor Independent)
by Nearby Computing
Vendor Independent representation of a slice in NearbyONE

OpenVino based Person Vehicle detection application - using WebRTC for low latency
by Intel
AI inference applies capabilities learned after training a neural network to yield result

Raemis Distributed UPF (Dynamic Slice Creation)
by Druid
Druid's cellular solutions for business are built on its Raemis™ technology platform. Raemis™ is a set of cellular software assets origin

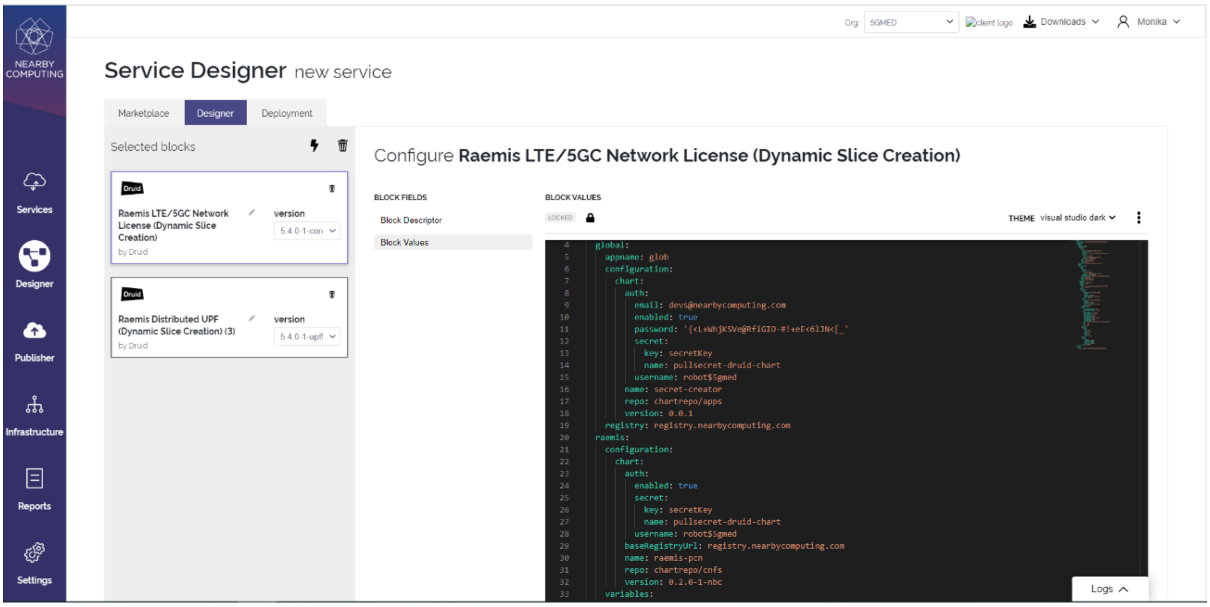
Raemis LTE/5GC Network License (Dynamic Slice Creation)
by Druid
Druid's cellular solutions for business are built on its Raemis™ technology platform. Raemis™ is a set of cellular software assets origin

Figure 27: NearbyOne Marketplace for 5GMED

The orchestrator has the ability to onboard the network functions provided by Druid that are needed to enable access to the workloads to be deployed. Druid's software components are packaged into Nearby Blocks and are onboarded on the platform. The conversion is made by encapsulating logic and code for the different application-specific functionalities and is created according to the defined policies. Nearby Blocks describe how to deploy the 5G Core, including several aspects such as:

- Rendering Druid's configurations
- 5G Core placement across the registered clusters
- Number of Instances to be deployed.

The procedure which consists in defining and packaging the different components of a block and in uploading this block into the NearbyOne platform is known as Block Onboarding.



Service Designer new service

Configure **Raemis LTE/5GC Network License (Dynamic Slice Creation)**

Raemis LTE/5GC Network License (Dynamic Slice Creation)
by Druid
version 5.4.0-1-con

Raemis Distributed UPF (Dynamic Slice Creation) (3)
by Druid
version 5.4.0-1-upf

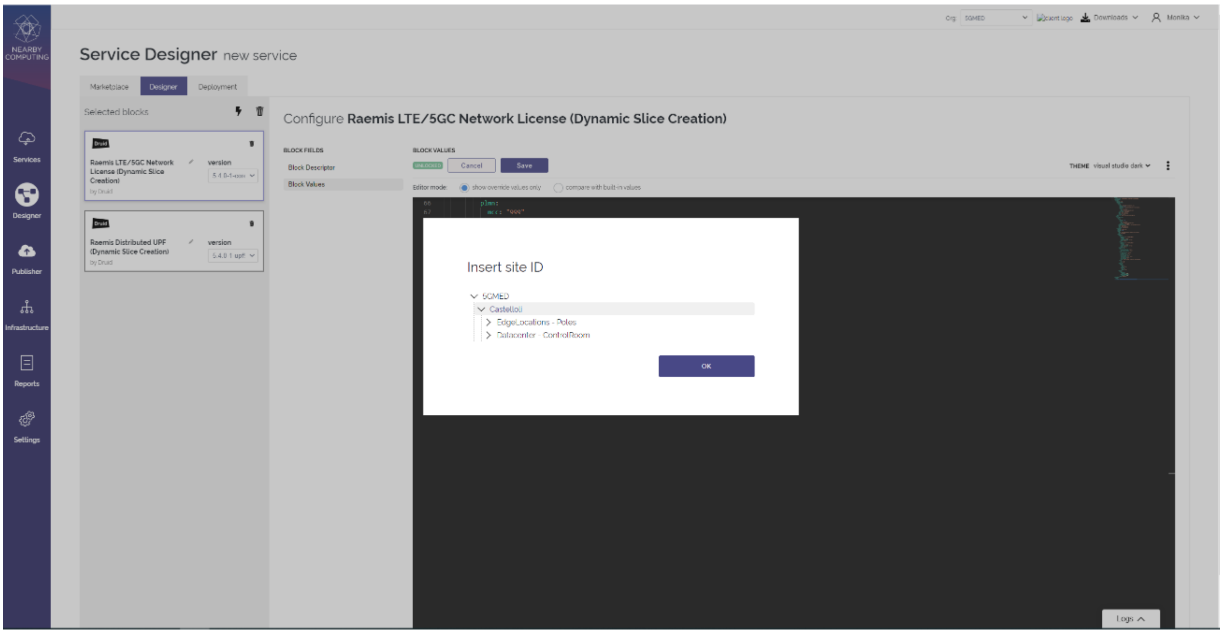
BLOCK FIELDS
Block Descriptor
Block Values

BLOCK VALUES

```
global:
  appname: glob
  configuration:
    chart:
      auth:
        email: devs@nearbycomputing.com
        enabled: true
        password: '{<L+WhjKSVe@RfiGIO-#!+eE<6lJN<[_'
        secret:
          key: secretKey
          name: pullsecret-druid-chart
        username: robot$5gmed
      name: secret-creator
      repo: chartrepo/apps
      version: 0.0.1
  registry: registry.nearbycomputing.com
raemis:
  configuration:
    chart:
      auth:
        enabled: true
        secret:
          key: secretKey
          name: pullsecret-druid-chart
        username: robot$5gmed
      baseRegistryUrl: registry.nearbycomputing.com
      name: raemis-pcn
      repo: chartrepo/cnfs
      version: 0.2.0-1-nbc
  variables:
```

Figure 28: Chaining and Configurations Refinement through NearbyOne

The image above shows what it looks like when Druid's UPF and 5G Core blocks are selected for configuration. In this Service Designer tab, the components are chained, the configurations are displayed, and certain values and policies may be refined based on requirements.



Service Designer new service

Configure **Raemis LTE/5GC Network License (Dynamic Slice Creation)**

Raemis LTE/5GC Network License (Dynamic Slice Creation)
by Druid
version 5.4.0-1-con

Raemis Distributed UPF (Dynamic Slice Creation)
by Druid
version 5.4.0-1-upf

BLOCK FIELDS
Block Descriptor
Block Values

BLOCK VALUES

Editor mode: ● show override values only ○ compare with built-in values

```
plmn:
  mcc: "999"
```

Insert site ID

5GMED
Castellolí
EdgeLocations - Poles
Datacenter - ControlRoom

Figure 29: Deployment of 5G Core and UPFs to Castellolí

Once ready, the distributed UPF and the 5G Core are both ready to be published and deployed to the target infrastructure, which in the image above shows, the infrastructure in Castellolí.

3.2.3 Transport Network

The transport network of the small-scale test site in Castellolí is composed of several elements illustrated in Figure 30 and described below.

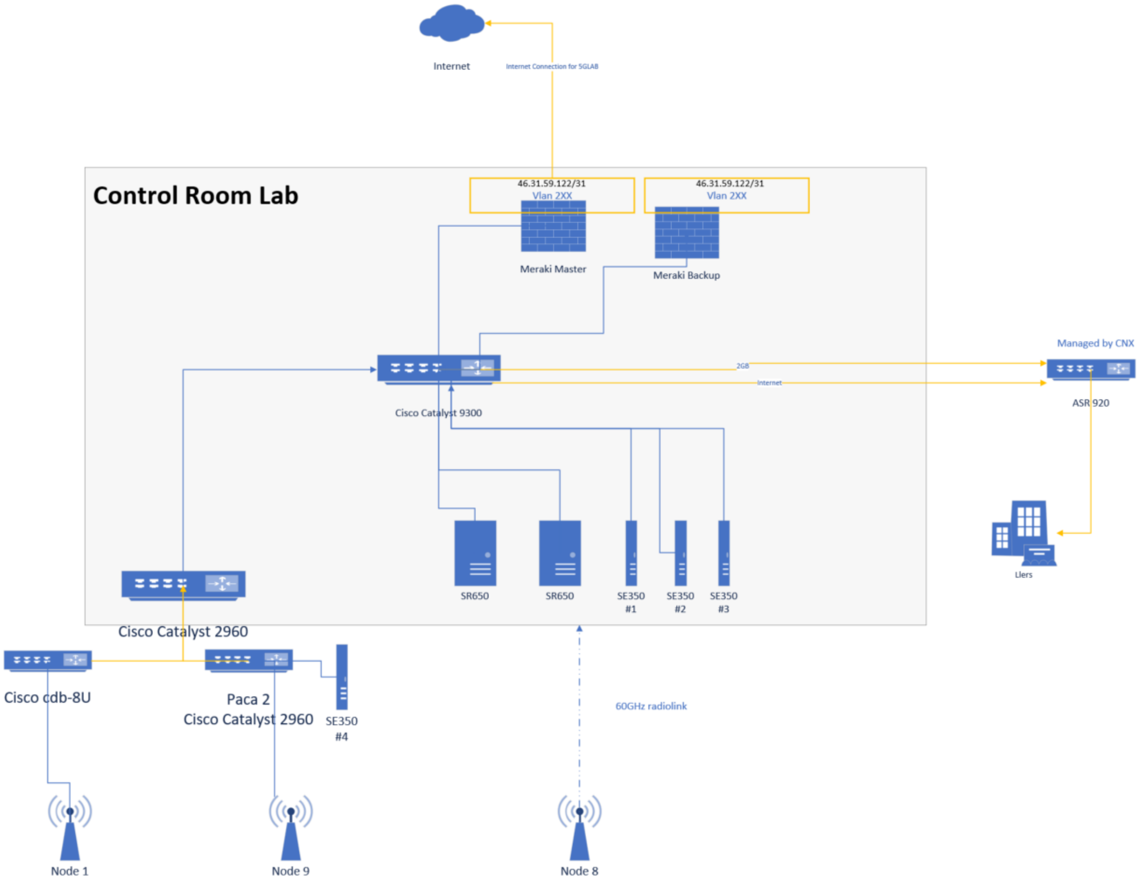


Figure 30: Transport Network of the small-scale test site of Castellolí

- **Cisco ASR920** is an aggregation service router. In its current configuration, the router provides connectivity to Internet and to the 5GMED equipment placed at the LFP Maintenance Base in Llers.
- **Cisco Meraki (x 2):** Both devices are deployed in high availability mode (the backup FW is turning on if something happens to Meraki Master). They are managed from the same control panel and located entirely in the cloud. In the current configuration, they provide firewall and routing functionalities to the rest of 5GMED network.
- **Cisco Catalyst 9300:** It is the main switching point for all the network elements of the Control Room Lab. In fact, this equipment establishes Ethernet networks that provide a bandwidth of 480 Gbps. In combination with the Cisco Meraki, it guarantees optimal Internet speeds and high-speed data transfer. In the current setup, it allows the connectivity of the virtual environment where all the computational machines that generate the functions of the different applications are installed. It allows the connectivity with the gNodeBs in Castellolí Circuit, as well as with the external nodes in the Spanish and French corridor.

- **Palo Alto Firewall:** Connected to the **Cisco Catalyst 9300,** it allows the access through the Management Network to the deployed and configurable equipment by isolating the Castellolí Circuit environment from the Cellnex production environment.

The equipment described so far is situated in the **"Control Room Lab"**. A switch has been installed to give access to the gNodeBs. This switch belongs to the Cisco Catalyst 2960 Series, which is a family of fixed-configuration, standalone switches capable of providing fast Ethernet and Gigabit Ethernet connectivity.

The gNodeBs are connected to the transport network in the following way:

- **Node 1** is a Sunwave 5G small cell connected to a Cisco CDB-8U switch, which is connected to the Control room by FO cable.
- **Node 8** is another Sunwave 5G small cell that is connected to the Control room through a radio link in the 60 GHz frequency band.
- **Node 9** is an Ericsson macro cell that connects to the CRL by fiber optics, via a Cisco Catalyst 2960.

Finally, the transport network has been segregated in different VLANs, with each VLAN dedicated to different applications and network services, as highlighted in Table 8.

VLAN ID	Service Description
200	Connectivity Radio – AMF (N2, N3 interfaces) – Spanish 5G Network
201	Connectivity UPF – Data Network (N6 interface) – Spanish 5G Network
202	Connectivity UPF – SMF (N4 interface) – Spanish 5G Network
203	Connectivity Radio – AMF (N2, N3 interfaces) – French 5G Network
204	Roaming between UPFs (N9 interface)
207	Connectivity UPF – Data Network (N6 interface) – French 5G Network
208	Connectivity UPF – SMF (N4 interface) – French 5G Network
211	Operation and Maintenance for Radio Nodes
212, 215, 218, 231-232, 250	UC3 Services
216	UC2 Services
217	UC4 Services

Table 8: 5G Transport Network VLANs for Castellolí

3.2.4 C-V2X RSU

The Castellolí circuit installation includes Cellular Vehicle-to-Everything (C-V2X) communication technology over specific spots. Telematic Communication Unit (TCU) from the vehicles will send and receive traffic directly to/from the V2X Gateway deployed on the infrastructure, via a Road-Side Unit (RSU) located along the circuit. To do so, a forwarding process – briefly described below – is used to forward traffic between PC5 (air interface) and UDP (ethernet network). While C-V2X allows direct communication between vehicles and infrastructure devices in proximity over 5.9 GHz, the V2X Gateway, on the infrastructure side, facilitates the connection of the C-V2X network to a cloud-based system that allows the data collected by the OBUs and RSUs.

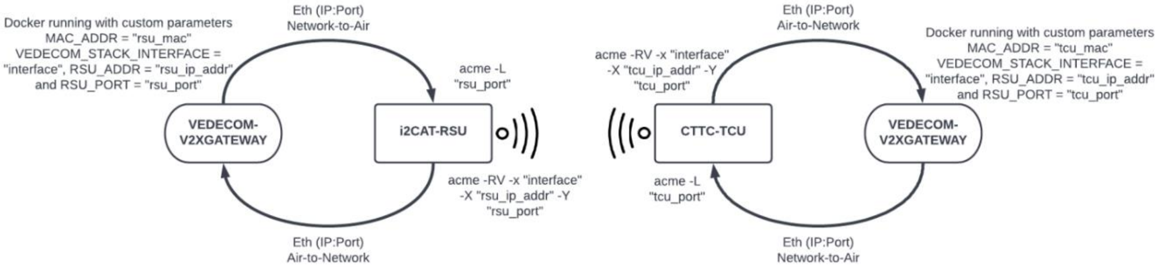


Figure 31: End-to-End traffic flow between the V2X Gateway and the TCU, going through the C-V2X RSU.

To allow traffic exchange between the V2X stack deployed on the infrastructure and the one in the vehicles, the **ACME tool** – developed by Qualcomm- is used. This tool, which offers multiple functionalities such as radio interfaces health checks, is designed to verify the functionality of C-V2X communication between devices based on the 9150 chipsets. In this sense, one of its functionalities is to act as a UDP-PC5 proxy, forwarding messages from the V2X Gateway to the RSU or OBU involved to test the reliability and effectiveness of the communication link. Unlike an 802.11p (ITS-G5) radio proxy, where headers from the Layer 2 (LLC level) are changed to the appropriate EtherType (radio or ethernet), ACME proxy encapsulates or decapsulates the traffic being transmitted or received on a UDP payload. Hence, from the V2X Gateway perspective, a RSU can be identified using the IP:Port tuple. Figure 31 presents a diagram of the current ACME based traffic flow, whereas Table 9 details the characteristics and features of the RSU deployed in the circuit.

Component	Value
Equipment	Cohda Wireless RSU MK6C
Standards	IEEE 1609 ETSI TS 103 613 3GPP R14 SAE J3161 GB/T 31024
C-V2X Bandwidth	20 MHz
Connectivity	C-V2X PC5 (Qualcomm 9150) / Ethernet
Operating System	Linux 4.9.88
Application Processor	i.MX8 QXP
Security	SXF1800 FIPS 140-2 level 3 compliant
C-V2X Receiver Sensitivity	-93.4 dBm
Environmental Operating Ranges	-40ºC to +65ºC
C-V2X Maximum Transmit Power	Class 3 with 21.5dBm
GNSS	GPS/GLONASS/Galileo/Beidou
Dimensions	W 260 x L 260 x 65 mm
Power Supply	POE 802.3at

Table 9: Characteristics of the C-V2X RSU deployed in Castellolí

Funded by the Horizon 2020 Framework Programme of the European Union

3.3 MEC Layer

The MEC layer deployed in the Castellolí small-scale test site consists of four SE350 Lenovo edge servers depicted in Figure 32. The small form factor of Lenovo SE350 allows to have edge computing capabilities co-located with a radio site along the corridor, thus making an efficient use of space and energy, while offering good computing capabilities as highlighted by its technical specifications detailed in Table 10. Two of the edge servers are part of the infrastructure managed by the NearbyOne orchestrator described in Section 3.4.

Figure 32: Lenovo SE350 Server

For the project needs, the four Lenovo SE350 servers host the following network functions and services of the automotive use cases that need edge computing (i.e., UC2 and UC4):

- **Server 1 associated to Edge Node 1:** Distributed UPF (France) + Follow-me service (UC4)
- **Server 2 associated to Edge Node 1:** TMC Edge (UC2)
- **Server 3 associated to Edge Node 8:** Distributed UPF (Spain) + Follow-me service (UC4)
- **Server 4 associated to Edge Node 8:** TMC Edge (UC2)

Size	43.2mm Height/ 209mm Width/ 376mm Depth
Weight	3.6 kg
Processor	One Intel® Xeon® processor D-2100 product family
Memory	256 GB (4 x 64GB LRDIMM)
Connectivity options	Ports: Two USB 3.1 / Two 1Gb Ethernet/ Two 10Gb SFP+
	WLAN: IEEE 802.11 a/b/g/n/ac
	LTE (3GPP R11)

Table 10: Lenovo SE350 technical specifications

The MEC server supporting UC2 services in Edge Node 1 has an Nvidia Tesla T4 GPU integrated, which is used to process the video analytics needed for UC2.

It should be noted that the V2X Gateway server to be used in UC2 is also deployed on the MEC servers in both sides of the corridor to disseminate/forward V2X messages to connected and automated vehicles along the corridor for UC1 and UC2. More information about it can be found in [16].

3.4 Orchestration Layer

This section describes the implementation of the orchestration layers deployed in the small-scale test site of Castellolí. The orchestration layer is based on the NearbyOne orchestrator. Two instances of the NearbyOne orchestrator are deployed, each one in a different country and assigned to a different MNO. The two instances of the NearbyOne orchestrator are deployed in the SR650 servers shown in Figure 18.

Each NearbyOne orchestrator takes the role of the Operator Platform in the federation scenario of the orchestration layer described in Section 2.3. To achieve federation, the NearbyOne orchestrator has been extended to implement the missing GSMA APIs features needed to achieve federation. Most of the functionalities defined in the NBI, SBI and UNI are already covered by the NearbyOne orchestrator. However, the development efforts focus on supporting the East-Westbound interface federation RESTful API [17], that covers the most relevant features to enable federation between two operators.

The integration between NearbyOne orchestrator and the EWBI federation API has been achieved by implementing the needed subset of the resources of the API required to define and deploy cloud-native applications. These resources and the operations to manage them are described in greater details hereafter:

- **FederationManagement:** Federation defines the relationship between the two OPs to stablish an agreement to allow exposure of Edge Cloud resources and Network capabilities of the Host OP to the Guest OP. A federation relationship is a directional relationship wherein a (Host) OP exposes its edge cloud resources and network capabilities to the (Guess) OP. Thus, if two OPs want to expose edge cloud resources and network capabilities with each other, then both OPs would need to initiate a directional federation creation request towards each other. The FederationManagement API operations allow to create, manage and remove directed federation relationship between OPs.
- **ApplicationOnboardingManagement**: Assuming that a federation has been previously established between Ops, this API operations register, retrieve, update and remove applications over EWBI towards a partner OP. The partner OP refers to the Host and/or the Guest Ops.
- **ApplicationDeploymentManagement:** An OP uses this API operations to control the deployment and termination of applications that have been onboarded on a partner OP, i.e., to create, update, retrieve and terminate application instances over EWBI.
- **ArtefactManagement:** *Artefacts* are packaged contents of scripts, Terraform, Ansible playbooks, or configuration required to run the application. This API operations upload, remove, retrieve and update application artefacts over EWBI towards a partner OP. To avoid managing file repository federation, NearbyOne manages only plain text configuration specifications of the application. Typically, the Artefact has references to Files.
- **FileManagemenUpload**: A *File* specifies a necessary resource to run an application in the Home OP. It can either be an actual file or a reference to one. This API operations remove, retrieve and update application binaries over EWBI towards a partner OP. To avoid managing file repository federation, NearbyOne manages only references to files. These references can

be containers in an Open Container Initiative (OCI) repository or Helm charts in a chart museum.

- **AvailabilityZoneInfoSynchronization**: An *Availability Zone* groups the infrastructure where the Applications need to be executed, such as Kubernetes clusters. This API operations manage the access to Home OP availability zones and their status updates.

The EWBI federation RESTful API exposes a set of Create, Read, Update, Delete (CRUD) operations on the API resources. Every interaction performed against the API is authorized using the OAuth Client Credentials flow.

The NearbyOne orchestrator implements both sides of the federation API, by means of a Guest agent and a Host agent. The guest agent enables NearbyOne to behave as a Guest OP that wants to deploy services in some host Availability Zones (AZs).

- The NearbyOne Host agent reacts when API calls are received. The federated Guest applications are deployed in its infrastructure as Service Chains that can be inspected from the NearbyOne Dashboard. The federated app uses a custom Helm chart that includes a Kubernetes Ingress.
- The NearbyOne Guest agent shows the AZs from the Host OP as part of its own infrastructure where applications (NearbyOne Blocks) can be deployed. NearbyOne Blocks that are enabled for federation will be able to run both locally and in federated Availability Zones equally, being able to be moved between them. When deploying in a federated Availability Zone, the Guest agent will internally perform the application onboarding and deployment flows in the background.

The sequence diagram in Figure 33, shows the complete federation flow to have an application instance running on the Host infrastructure from a Guest OP, and then, to delete it. First, the federation needs to be stablished. For this, the user of the Host OP adds the Guest OP as partner and, as a result, the client credentials (ID and secret key) are created (Steps 1-2). Then, the user of the Host OP shares *offline* (not using the OPs) these credentials and the federation URL with the user of the Guest OP (Step 3). Once the Guest operator has this data, the federation can be stablished by adding the Host partner to its OP (Steps 4-6). If the federation creation is satisfactory, the Host and the Guest OPs exchange the needed information to setup the Availability Zones (Steps 7-12).

As explained before, to deploy an application in the Host infrastructure, the first step is to onboard the application: upload files (Step 14), then the artefacts referencing the said files (Step 16), and finally onboard the application that will reference the artefacts (Step 18). After onboarding it, the application is deployed in the selected availability zone of the Host OP (Steps 20-25).

The application can be undeployed and then the artifacts, and files will be cleaned up in the Host OP (Steps 26-30).

The NearbyOne orchestrator dashboard has been extended to incorporate the Federation features. The federation establishment is shown in the following figures. Figure 34 shows the federation settings of the Host OP, i.e., the NearbyOne orchestrator in France in this example; Figure 35 shows the federation settings of the Guest OP, i.e., the NearbyOne orchestrator in Spain in this example. In both cases, the federation is enabled: France has added Spain as the Guest partner and Spain has added France as the Host partner.

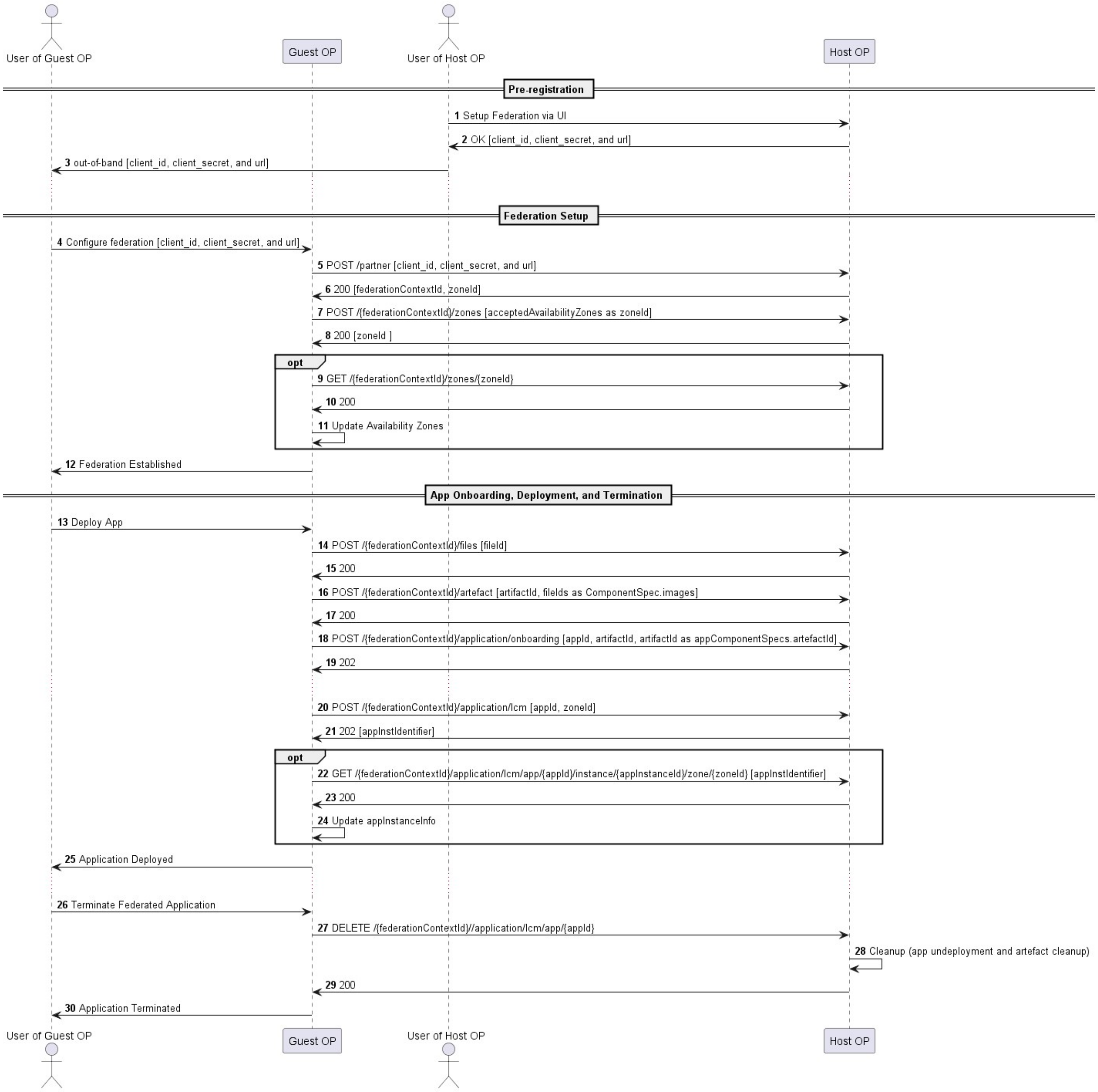
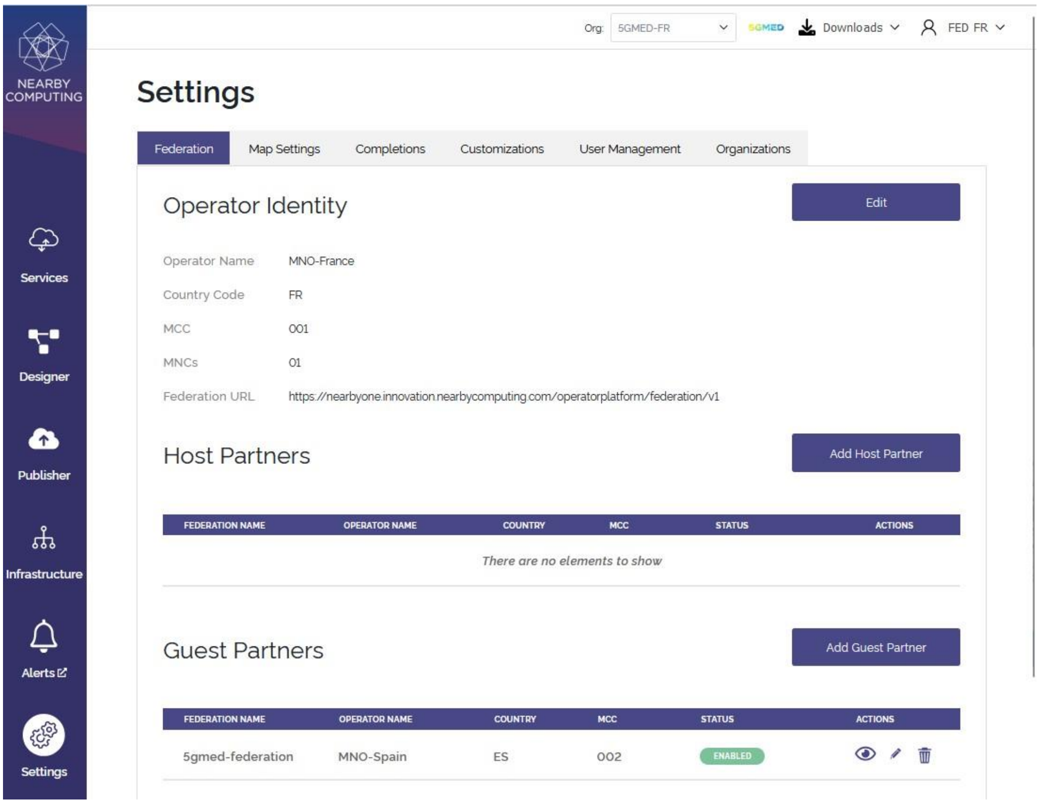

User of Guest OP
Guest OP
User of Host OP
Host OP
Pre-registration
1 Setup Federation via UI
2 OK [client_id, client_secret, and url]
3 out-of-band [client_id, client_secret, and url]
Federation Setup
4 Configure federation [client_id, client_secret, and url]
5 POST /partner [client_id, client_secret, and url]
6 200 [federationContextId, zoneId]
7 POST /{federationContextId}/zones [acceptedAvailabilityZones as zoneId]
8 200 [zoneId]
opt
9 GET /{federationContextId}/zones/{zoneId}
10 200
11 Update Availability Zones
12 Federation Established
App Onboarding, Deployment, and Termination
13 Deploy App
14 POST /{federationContextId}/files [fileId]
15 200
16 POST /{federationContextId}/artefact [artifactId, fileIds as ComponentSpec.images]
17 200
18 POST /{federationContextId}/application/onboarding [appId, artifactId, artifactId as appComponentSpecs.artefactId]
19 202
20 POST /{federationContextId}/application/lcm [appId, zoneId]
21 202 [appInstIdentifier]
opt
22 GET /{federationContextId}/application/lcm/app/{appId}/instance/{appInstanceId}/zone/{zoneId} [appInstIdentifier]
23 200
24 Update appInstanceInfo
25 Application Deployed
26 Terminate Federated Application
27 DELETE /{federationContextId}//application/lcm/app/{appId}
28 Cleanup (app undeployment and artefact cleanup)
29 200
30 Application Terminated
User of Guest OP
Guest OP
User of Host OP
Host OP

Figure 33: Sequence diagram for federation CRUD operations



Settings

Operator Identity

Operator Name: MNO-France
Country Code: FR
MCC: 001
MNCs: 01
Federation URL: https://nearbyone.innovation.nearbycomputing.com/operatorplatform/federation/v1

Host Partners

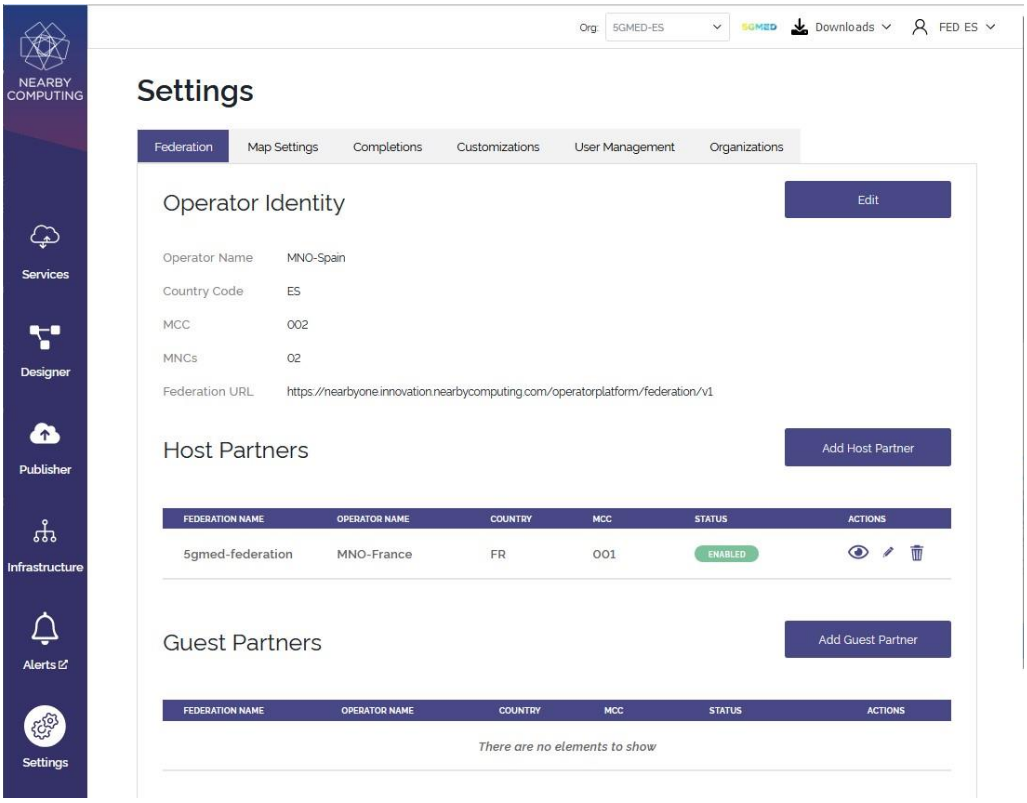
FEDERATION NAME	OPERATOR NAME	COUNTRY	MCC	STATUS	ACTIONS

There are no elements to show

Guest Partners

FEDERATION NAME	OPERATOR NAME	COUNTRY	MCC	STATUS	ACTIONS
5gmed-federation	MNO-Spain	ES	002	ENABLED	

Figure 34: Federation setup from HOST OP.



Settings

Operator Identity

Operator Name: MNO-Spain
Country Code: ES
MCC: 002
MNCs: 02
Federation URL: https://nearbyone.innovation.nearbycomputing.com/operatorplatform/federation/v1

Host Partners

FEDERATION NAME	OPERATOR NAME	COUNTRY	MCC	STATUS	ACTIONS
5gmed-federation	MNO-France	FR	001	ENABLED	

Guest Partners

FEDERATION NAME	OPERATOR NAME	COUNTRY	MCC	STATUS	ACTIONS

There are no elements to show

Figure 35: Federation setup from GUEST OP.

3.5 Slice Management Layer

In this section, we describe the implementation of the slice management layers deployed in the small-scale test site of Castellolí. The slice management layer is divided into three sublayers as described in Section 2.4.1:

- **RAN Slicing:** i2CAT has developed a RAN slice manager to be used in 5GMED. However, due to the lack of radio Operations Support Systems (OSS), RAN slicing will not be implemented for dynamic configuration, instead, static RAN slicing has been implemented by directly configuring the parameters of the slices in the gNodeB's. Implementation details are presented in Section 3.5.1.
- **Transport Slicing:** the transport network has been designed to implement different VLANs for the different services and to separate the different access networks. In this way we ensure the proper transport network performance. Details are presented in Section 3.5.2.
- **Core Slicing:** NBC has integrated Druid 5G Core as a service and, hence, the 5G Cores can be deployed through the NearbyOne orchestrator with any defined core slices. Implementation details are presented in Section 3.5.3.

The implementation of Network Slicing in 5GMED will be purely static, i.e., 5G slices are pre-defined and parameters to enable these slices are manually configured on RAN, transport, and Core. Thus, the slice managers of each of the domain as well as their integrations to the orchestrator will not be leveraged and implemented. Regardless of it is dynamic or static network slicing, the project could still make use of network slicing. Multiple slices with different configurations and use cases are used, each with its own VLAN. The proper definition of user groups, allocation of resources, and management of the network is critical to successfully implement network slicing. Table 11 shows the different requirements for each use case in terms of 5QIs, Guaranteed Bit Rate (GBR), Packet Delay Budget, Packet Error Rate (PER), and Service Security Type (SST) metrics. These parameters are critical to determine the expected quality of service for each use case. The mapping of user types and use cases defines the different types of users that will use the 5G network in 5GMED for each use case. The 5QI parameters allow operators to classify traffic based on their specific requirements. This enables differentiation of QoS treatment for each type of traffic and ensures that end users receive the appropriate level of service.

Use Case	5QI	GBR	Packet Delay Budget	PER	SST
1: Remote Driving	85	Delay Critical GBR	5 ms	10^{-5}	3 = MIoT
2: Road Infrastructure Digitalization	84	Delay Critical GBR	30 ms	10^{-5}	4 = V2X
3: FRMC	71 74	GBR GBR	150 ms 500 ms	10^{-6} 10^{-8}	1 = eMBB
4: Follow-me	71	GBR	150 ms	10^{-6}	2 = URLLC

Table 11: Use cases requirements based on User Type and 5QI metrics

3.5.1 RAN Slicing

The configuration of network slicing is highly dependent on the ability of the gNodeB to support network slicing and to meet the various QoS and traffic profile requirements. The configurable parameters, including Slice Differentiator (SD), Slice/Service Type (SST), PLMN ID, Tracking Area Code (TAC), and TAI, are used to differentiate the slices based on the specific requirements. The SD is used when there is more than one slice of the same type, while the SST defines the type of service offered. The PLMN ID is used to identify the operator and the network, while the TAC is used to determine the tracking area within the network. The TAI combines the MCC, MNC, and TAC that, uniquely identifies a particular slice. The handover may affect slicing as it involves the transfer of the data session from one base station to another. To ensure seamless handover, slices must be designed to work across multiple base stations, and configurable parameters must be set accordingly.

3.5.2 Transport Network Slicing

A dynamic transport network slicing solution would consist of the deployment of two Transport slice Managers accessible by the Orchestrators. Each Transport Slice Manager would offer as an NBI a REST API aligned with ONF Transport API [18] to provide a dedicated transport connectivity service for each end-to-end network slice. This connectivity service request would be translated into SNMP commands that are needed to configure the related VLAN profiles in transport network equipment, such as routers and switches.

As previously detailed in Section 2.4.1.2, the Transport Network Slicing solution in Castellolí test site will not be able to offer the dynamic allocation of VLAN on top of each border transport network equipment. This is because the 5GMED network infrastructure uses a production network and, thus, no dynamic configuration from software components of Cisco switches is available. Therefore, in the test site of Castellolí we have implemented static VLAN configuration that deals with the mapping of 5QI to multiple transport slices. Dynamic transport network slicing has been demonstrated in [19].

3.5.3 Core Network Slicing

For the Core Slicing, the Druid 5G Core allows traffic separation, load balancing, and QoS configuration as previously described in Section 3.2.2. In fact, multiple Data Network Names (DNNs) may be created and be associated with a specific VLAN. Through this traffic separation, logical groups are created, allowing assignments to specific DNNs that best suit the needs of each group. Moreover, this capability allows the users to create different DNNs that can provide different QoS levels.

Regarding the implementation for 5GMED, four slices covering the four different use cases will be statically created and manually configured in the 5G Cores, all having a unique DNN with differentiated QoS defined in Table 11.

3.6 Cloud Layer

This section describes the implementation of the private cloud deployed in Castellolí small-scale test site. The private cloud of Castellolí is composed of two Lenovo SR650 servers (Figure 36), hosting the two Druid 5G Cores and different VMs with the Cloud-based applications of the service providers for each use case. The SR650 computing capabilities provides a reliable, secure, and cost-effective solution for the 5GMED Cloud (Table 12).

With the help of VMWARE software virtualization, the SR650 servers can easily manage and scale resources, allowing the Cloud to quickly meet use cases demands. The VMWARE vSphere management console allows for effortless provisioning and management of the Cloud’s virtualized resources. This helps to ensure that the 5GMED Cloud can provide users with the highest levels of performance and efficiency. Additionally, 5GMED secure and reliable platform allows for the Cloud to be accessible from any point of the network, providing users with easy access to the Cloud's resources.

Furthermore, the P2 service for UC3 (Obstacle Detection) requires extra computational capabilities, so an NVIDIA GPU was integrated in one of these SR650 for this purpose, as detailed in D5.1 [20]. Finally, an acceleration card Tesla T4 was as well installed in the MEC for video analytics purposes used in UC2.

Figure 36: Lenovo SR650 server

Size	Height: 86.5 mm / Width: 482.0 mm / Depth: 763.7 mm
Weight	Up to 32.0 kg
Processor	One Intel® Xeon® processor 6137 product family
Memory	3 TB (4 x 64GB LRDIMM)
Connectivity options	Ports: Two USB 3.1 / four 1Gb Ethernet/ four 10Gb SFP+
	WLAN: IEEE 802.11 a/b/g/n/ac

Table 12: Lenovo SR650 server technical specifications

3.7 Data Analytics Layer

This section describes the implementation of the Data Analytics layer deployed in the small-scale test site of Castellolí. It is composed of the Data Analytics Module (DAM) of UC4 deployed on a Lenovo SR650 server virtualized with VMWare. The DAM interfaces with the NearbyOne orchestrator and is used by UC4 services to optimize the migration or relocation of a MEC application following the movements of the UE, i.e., Follow-ME concept of UC4.

The main function of the DAM is to trigger the migration of the MEC application from one MEC to another when the UE moves along the corridor, and certain conditions are met. For example, when the RAN QoS starts degrading due to user mobility. The DAM has been designed to collect metrics from various sources: the 5G network, the UC4 applications, the vehicle, etc. Some examples of metrics collected from the vehicle are the position and speed of the users, which could be used to predict when a handover between edge nodes will be necessary. These metrics were used to develop the first iteration of the DAM.

The architecture of the DAM is represented in Figure 37. It is composed of three different software modules and interfaces described in D4.2: the Input Module (IM), the Artificial Intelligence Module (AIM), and the Decision Engine (DE). In a first iteration of the DAM development, the IM acquires only the speed and position of the UE at an instant t0 and the AIM analytically calculates the position at t0 + 30 s (time required by the orchestrator to move the application from one edge node to the next). The DE knows the borders of the zones covered by each edge node (geo-fences of edge zones are input to the DE) and then, depending on the predicted position, the DE will inform the orchestrator if the user will be in the next 30 s crossing the border of the current edge node zone and hence, trigger the orchestrator to move the application to the next edge node. This first simple iteration, without any AI in the AIM was developed to test in a simple way the follow-ME concept of UC4.

The subsequent iterations of the DAM developments were supposed to integrate network and application metrics as can be seen in Figure 37. However, it should be noted here that, in order for the AIM to efficiently use other metrics, such as RAN metrics or environment metrics, we would have needed huge amount of data with high diversity on a large scale of time to be able to train the AI model and predict, e.g., network congestion, traffic jams, etc. in order to be more accurate on the likelihood of a change of edge node. This type of datasets could not be obtained in the timeframe of 5GMED and is not available as open data. We could have only produced a DAM that would have needed subsequent datasets to train it properly on a given portion of the cross-border corridor along the motorway. Therefore, it was decided to drop further developments of the DAM where AI is required and stick to the first iteration development for further deployments and large-scale trials in the cross-border corridor.

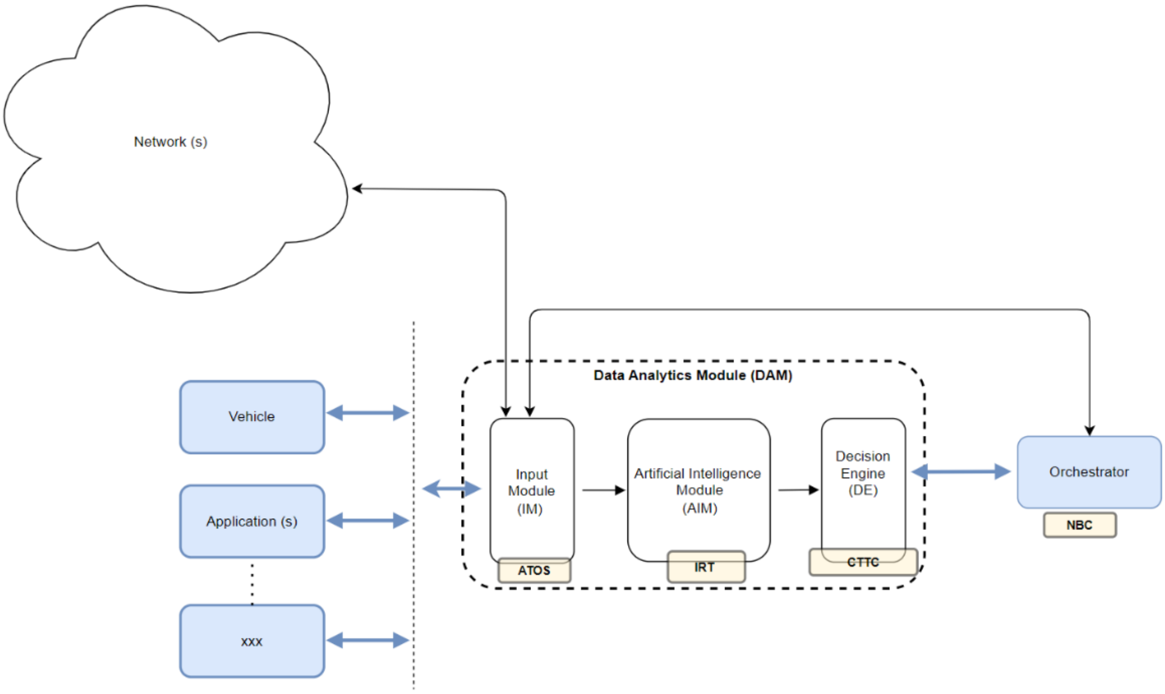


Figure 37: Architecture of the Data Analytics Module

Funded by the Horizon 2020 Framework Programme of the European Union

4. Cross-Border Test Site for Small-Scale Trials in Railways

The location of the Mediterranean cross-border corridor, situated between Figueres (Spain) – Perpignan (France), is shown in Figure 38. It has a total length of 60 km and includes the highway E-15 and the rail track of the high-speed train between Spain and France. Two types of trains are available for tests and trials in the railway scenario. A commercial SNCF TGV will be used for large-scale trials at high speed (300 Km/h) and a maintenance train from LFP is available for small-scale trials at low speed below 90 Km/h.

The cross-border test site for the small-scale trials of the railway UC3 relies on a complex setup mixing specific elements geographically located close to the railway and highway with others that are deployed at the Castellolí test site presented in Section 3. The railways part of the corridor will be covered with 5G in the Spanish and French open-air sections, 5G in the tunnel segment, and IEEE 802.11ad (70 GHz) in part of the Spanish open-air section. In the rest of this section, more detailed information is provided about the implementation of the test site.

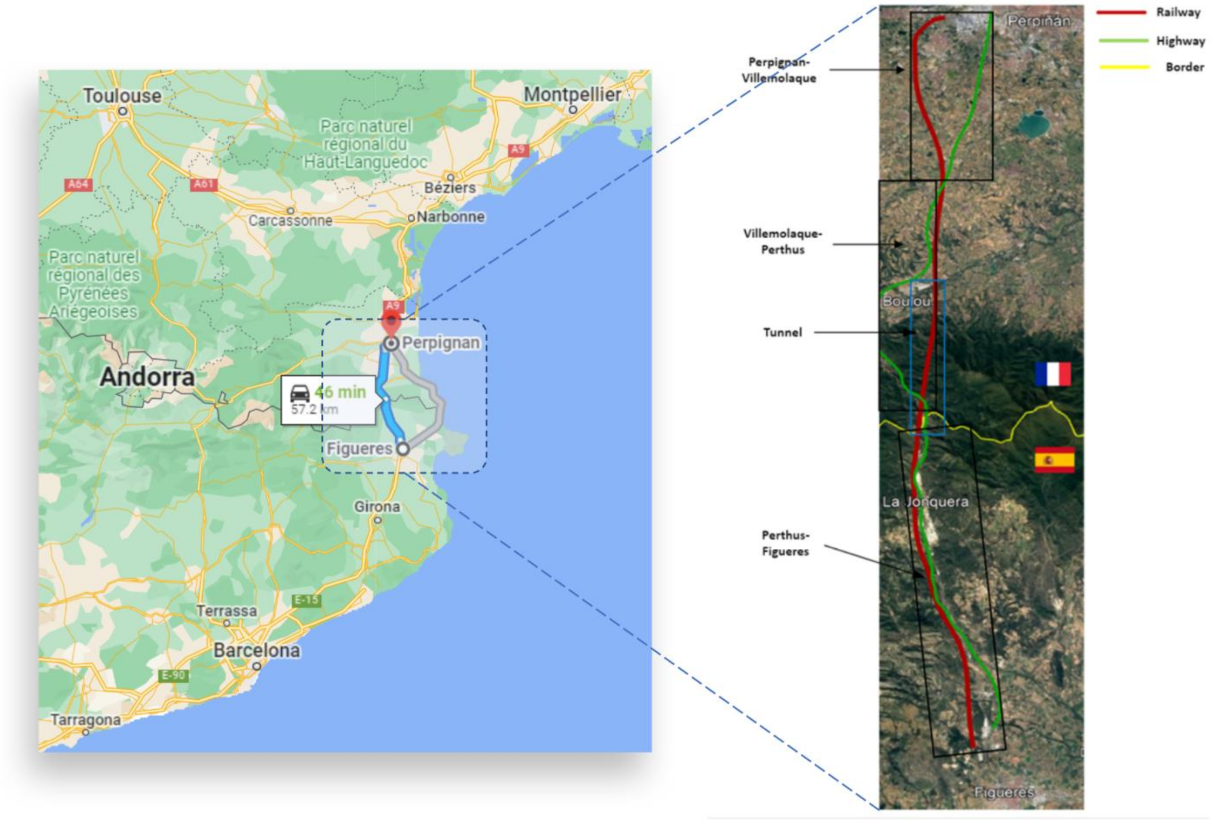


Figure 38: Location of the Mediterranean cross-border corridor showing the highway and rail track between Figueres and Perpignan

4.1 End-to-End Architecture implementation

The end-to-end network implemented in the cross-border corridor for the small-scale trials in the railway scenario is based on the 5GMED cross-border network architecture described in Section 2 and depicted in Figure 1.

In the rest of this section, the implementation of the network infrastructure layer and MEC layer are described, respectively, in Section 4.2 and Section 4.3. The implementations of the orchestration layer, slice management layer, and cloud layer are exactly the same as the ones described in Section 3.4, Section 3.5, and Section 3.6, respectively, for the small-scale test site of Castellolí (represented in Figure 18). The Data Analytics layer is not used in the railway scenario.

4.2 Network Infrastructure Layer

This section describes the network infrastructure layer implemented in the cross-border corridor for the small-scale trials in railway scenario. It consists in three different technologies: 5G, IEEE 802.11ad (70GHz), and satellite.

Two 5G SA networks have been deployed in the cross-border corridor, including the equipment that compose the 5G Radio Access network (Section 4.2.1), the 5G Core (Section 4.2.2), and the transport network (Section 4.2.3). The IEEE 802.11ad radio access network is described in Section 4.2.4. Finally, the satellite access network is described in 4.2.5.

4.2.1 5G Radio Access Network

The 5G RAN deployed in the corridor for the small-scale trials of the railway use case is comprised of 12 gNodeBs, with 6 in Spain and 6 in France. At the moment of edition of this document, a total of 7 gNodeBs have been successfully deployed and are already operational.

The deployed gNodeBs are illustrated in Figure 39 to Figure 43. Figure 39 illustrates the location of gNodeBs deployed in France, with those marked with a red tower symbol representing sites deployed by Cellnex using French operator Free Mobile spectrum (band N78), whereas BTS04 and BTS05 sites marked with green circle, are gNodeBs deployed by Cellnex in LFP infrastructure. For sites in Spain (Figure 40), there is a similar situation where red towers symbolizes gNodeBs from Vodafone (band N78) and green circles sites deployed by Cellnex in LFP towers. The sites deployed by Cellnex are a good example of how a neutral host operator can invest and contribute to increase 5G coverage in areas which have not been covered by traditional MNOs due to several reasons detailed in WP7 deliverables.

Furthermore, a DAS system has been installed inside Le Perthus tunnel, an 8 km railways tunnel connecting Spain and France. Figure 44 illustrates the distribution of the radio Access Points along the tunnel. The DAS is composed of 23 Access Points connected via fiber to a Master Unit from CommScope, which in turn is connected to one RRU and a BBU from Nokia. The spectrum used in the tunnel is granted by Free Mobile in Band N78.

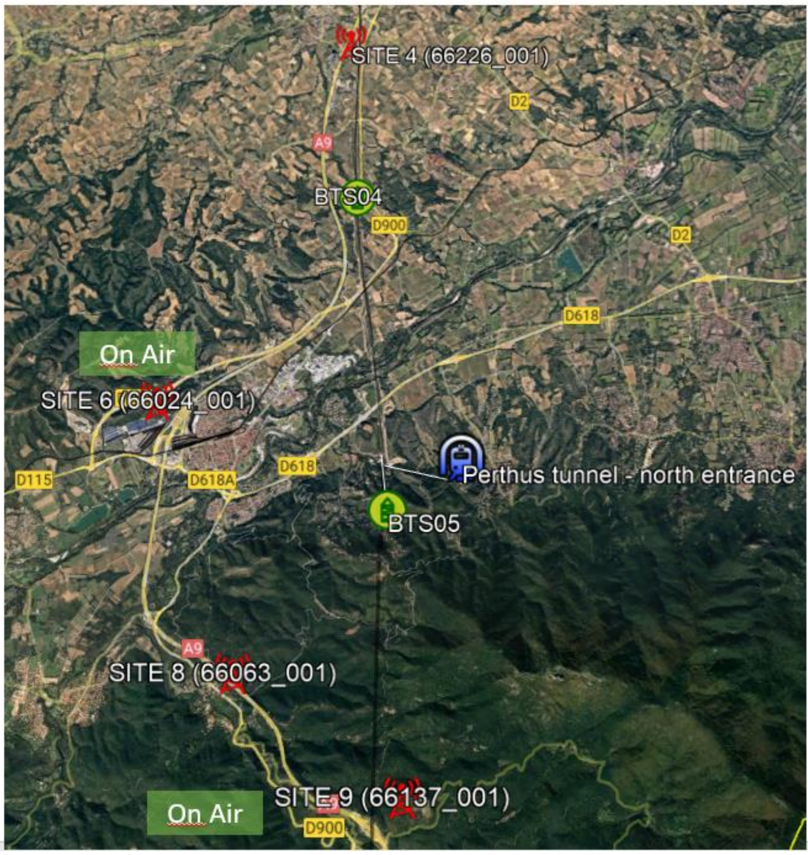


Figure 39: Location of 5G sites in France

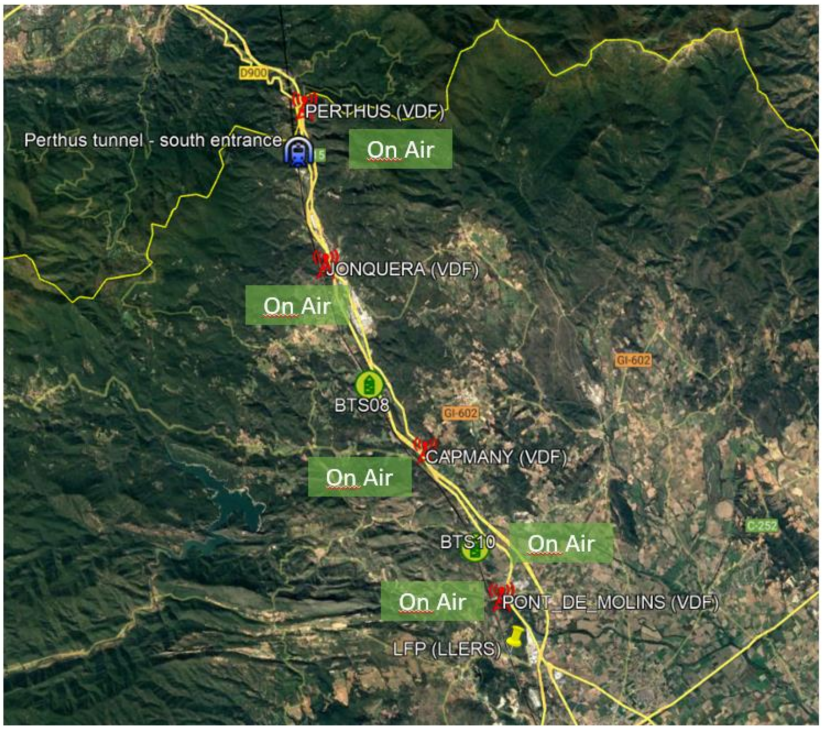


Figure 40: Location of 5G sites in Spain

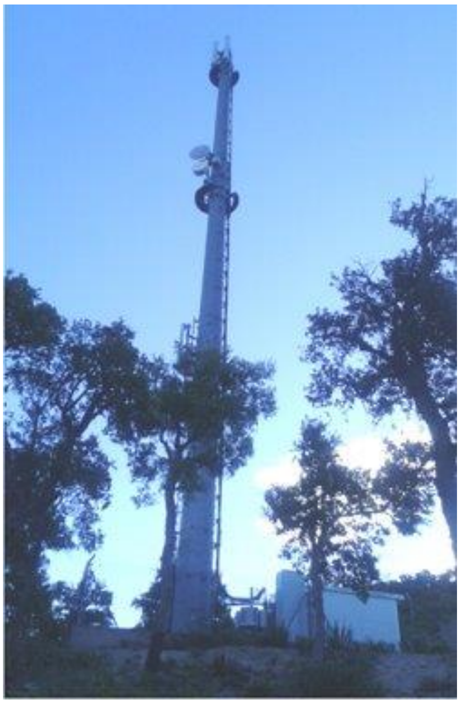


Figure 41. Le Perthus Site (Spain)

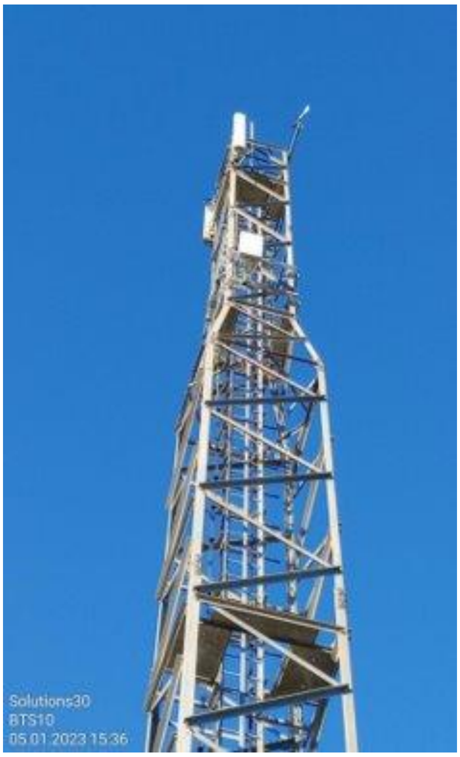


Figure 42: BTS 10 Site (Spain)

Figure 43: Views of the Railway from BTS 10 Site (Spain)

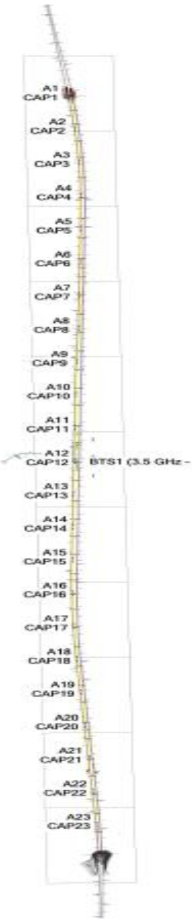


Figure 44: Distribution of 5G radio access points in Le Perthus Tunnel

Funded by the Horizon 2020 Framework Programme of the European Union

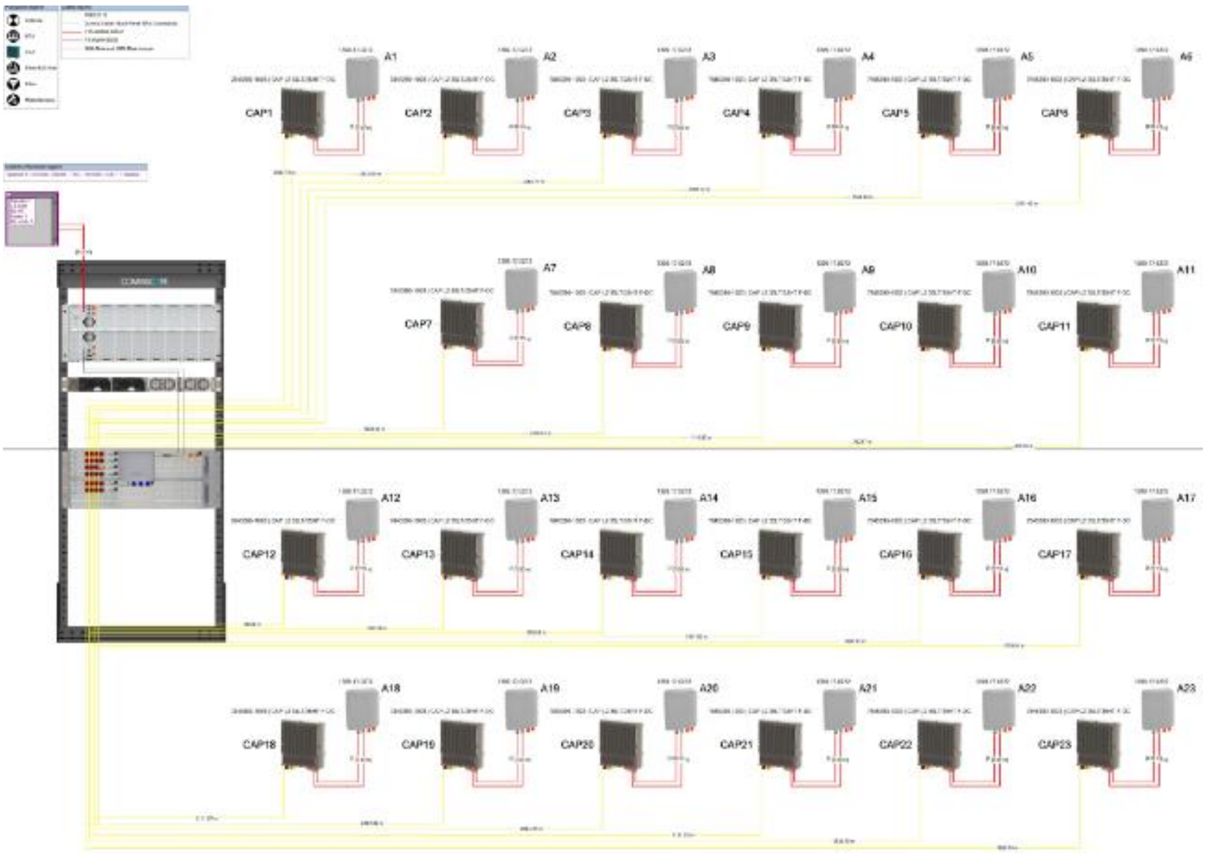


Figure 45: Detail 5G radio access Points connections to Master Unit

4.2.2 5G Core Network

The 5G Cores used for the two 5G SA networks deployed in the cross-border corridor are the same as those deployed in Castellolí (described in Section 3.2.2), one on the French side and the other on the Spanish side. The network functions used in both 5G Cores are: AMF, SMF, UDM, AUSF and centralized UPF. In Section 2.1.1, Figure 3 shows the internal architecture of both 5G SA networks in France and Spain with all the network functions and interfaces.

The only difference between the cross-border corridor test site and the small-scale test site of Castellolí is the use of distributed UPF nodes. They will be located in two different places. The Spanish UPF is placed in Llers, near the LFP offices in the Spanish MEC. The French UPF is in LFP premises situated close to the north exit of Le Perthus tunnel, in the French MEC.

4.2.3 Transport Network

The transport networks of the cross-border corridor test site consist of microwave radio links and fibre optical links. As illustrated in Figure 46 the transport network can be divided into three zones:

- Castellolí circuit.
- Spanish corridor: segment of the cross-border corridor in Spain.
- French corridor: segment of the cross-border corridor in France.

In Castellolí Circuit, an optical fiber was installed to connect Castellolí with the Cellnex interconnection center of Figueres Avinyonet, with a bandwidth capacity of 2Gbps.

Furthermore, from Figueres Avinyonet, and in order to reach the aggregation point of all backhaul traffic coming from the gNodeBs located in LFP BTS-11, two radio links in the 80GHz band with a bandwidth of 2Gbps have been installed:

- Radio link between the Site of Figueres Avinyonet and Torre Vodafone covering a distance of 2.3 Km.
- Radio link between the Site of Torre Vodafone and the BTS-11 covering almost 1 km.

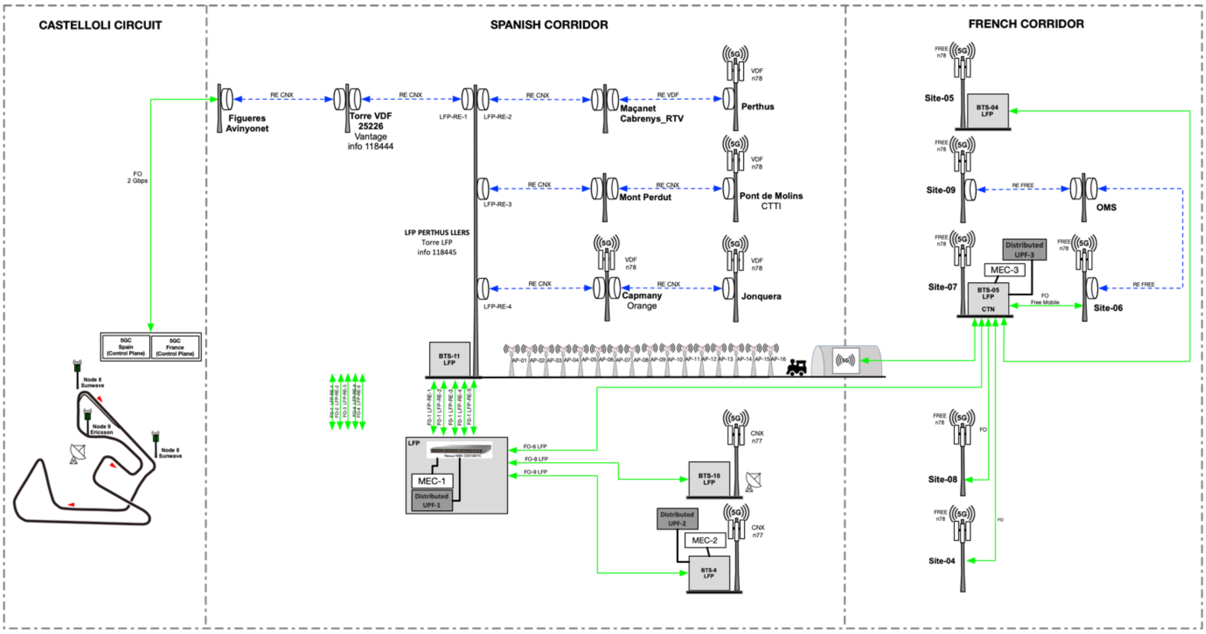


Figure 46: Diagram of the transport network deployed in the cross-border corridor (radio links in dotted blue lines, fiber links in green plain lines)

To give connectivity to the 5G node of Perthus, it has been necessary to install a radio link between the site BTS-11 LFP and Maçanet Cabrenys to cover a distance of 21 km, then it has been made use of an existing Vodafone radio link between Maçanet and Perthus.

To reach the 5G node of Pont de Molins, it has been necessary to establish two links:

- Radio link between BTS-11 LFP and Mont Perdut to cover a distance of 15 Km with a capacity of 2 Gbps.
- Radio link between Mont Perdut and Pont de Molins to cover a distance of 15 km with a dimensioned capacity of 800 Mbps.

To access Capmany's 5G nodes, a radio link has been installed with the BTS-11 LFP Site to cover 7.3Km and has a transmission capacity of 800 Mbps. From Capmany, another radio link has been installed with the site Jonquera covering the distance 7.3Km and with the same capacity as Capmany.

For the white areas not covered by Vodafone radios, Cellnex has installed a first 5G node in the n77 band on the BTS-10 LFP site, and a second one will be installed in BTS-8 LFP, once the testing phase in

Castellolí test site concluded and the equipment was not needed there anymore. BTS-10 and BTS-08 are connected via optical fiber down to BTS-11 of LFP.

The French corridor has connectivity with the Spanish Corridor via a connected optical fiber between site BTS-11 LFP on the Spanish side and site BTS-05 LFP on the French side. In the French corridor, the site BTS-05 LFP has been established as the concentration point of all connections. The following sites are connected by optical fiber to this site: Site-05, Site-06, and Site-07. Site-6 is an intermediate point to reach Site-09 which uses two Radio links:

- Radio Link between Site-06 and Site OMS
- Radio Link between Site OMS and Site-09

Site-04 has 5G radio equipment but there is still no defined optical fiber connection with the BTS-05 LFP site, and finally there is the Site-08 that is still in the design phase.

4.2.4 IEEE 802.11ad Radio Access Network

The IEEE 802.11ad radio access network is specifically tailored and optimized for train-to-ground communication. It uses the licensed exempt operation in the 57-71 GHz millimetre wave band to supply gigabit capacity.

It is based on a series of trackside radio units deployed on poles attached to the existing catenary stanchions along the track which will set up a radio connection with one or two antennae units deployed on the train, as illustrated in Figure 47.

The deployment of this infrastructure will cover approximately 17.5km from the south entrance of the Le Perthus tunnel towards the LFP Maintenance Base in Llers, close to Figueres with high data rate.

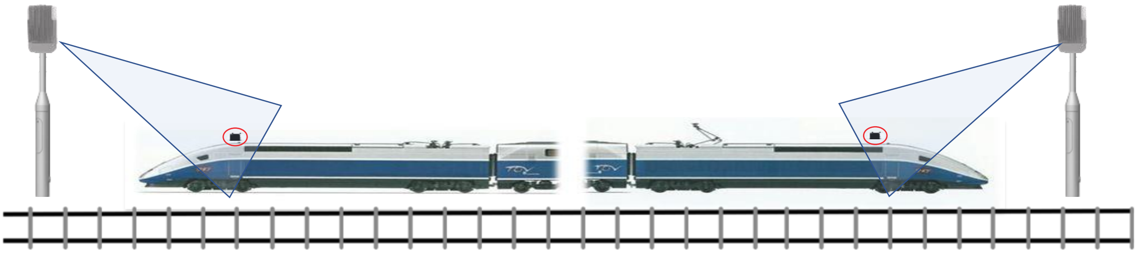


Figure 47: IEEE 802.11ad 70GHz train-to-track system

The deployment of the trackside radio units or access points considered plays a crucial role in providing continuous coverage and connectivity for the railway. The specific locations of each unit have been carefully chosen to ensure maximum coverage and efficiency. A total of 15 trackside radio units have been necessary to cover the railway section that will be tested. They are named from AP-1 (closest unit to Le Perthus tunnel) up to AP-15 (closest unit to the LFP Maintenance Base). The Figure 48 shows an orthophoto obtained with the Google Earth program with all the positions of the fifteen locations.

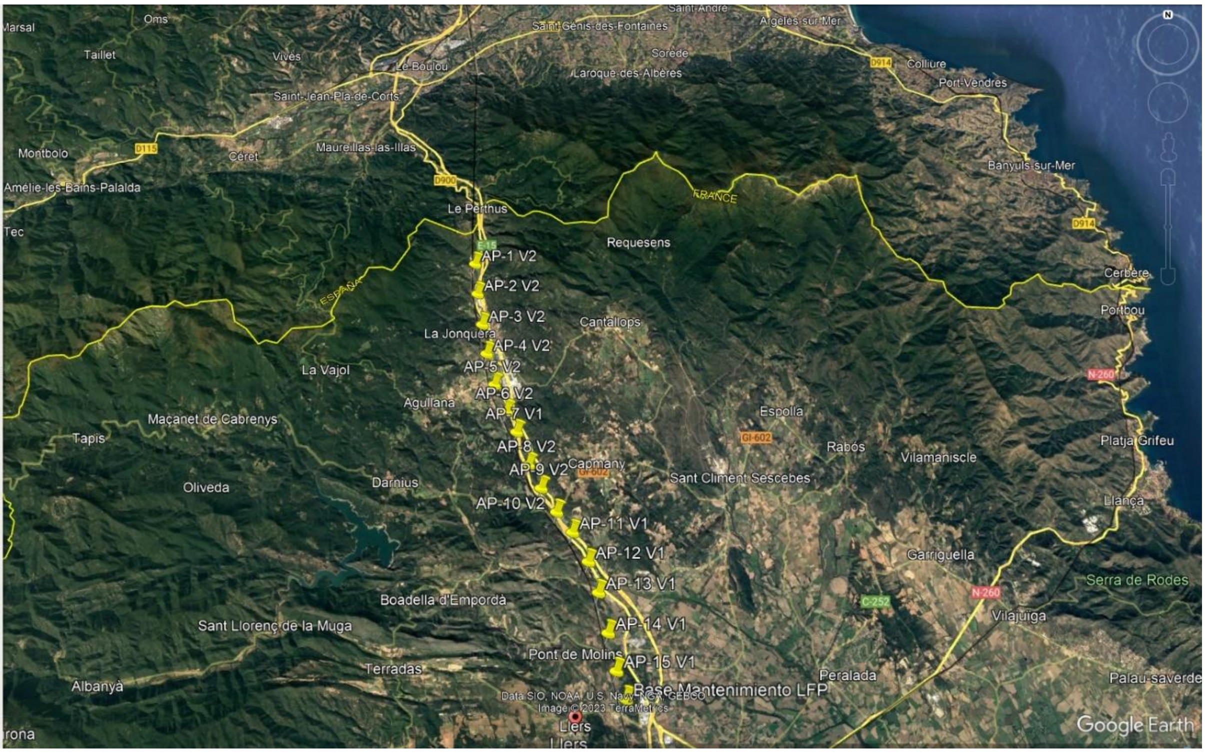


Figure 48: Orthophoto of the Trackside survey for the 70GHz network

The fifteen locations of the trackside radio units are listed in Table 13, which provides both the stanchion locations (latitude and longitude) and the railroad direction (France-to-Spain direction: line V1 and Spain-to-France-direction: line V2).

The IEEE 802.11ad radio access network is composed of the following elements:

- The trackside radio units set up the radio link with beamforming to approaching trains. This link establishment process is extremely short, around 2-3 seconds.
- A backhaul to interconnect the trackside radio units.
- A central switching point, with a L2 switch, the aggregation unit, and a firewall, all hosted in the LFP maintenance base in Llers.

The IEEE 802.11ad network components deployed in the train were described in deliverable D5.1 [20].

Trackside radio units	Line	Latitude	Longitude
1 **(From Le Perthus Tunnel)**	V2	42.439675	2.861983
2	V2	42.428652	2.863661
3	V2	42.417338	2.866406
4	V2	42.407055	2.868994
5	V2	42.396277	2.872947
6	V2	42.387093	2.878704
7	V1	42.380147	2.883388
8	V2	42.369325	2.888946
9	V2	42.361700	2.894553
10	V2	42.354028	2.901332

Funded by the Horizon 2020 Framework Programme of the European Union

Trackside radio units	Line	Latitude	Longitude
11	V1	42.347666	2.908133
12	V1	42.338559	2.914901
13	V1	42.329117	2.919163
14	V1	42.317107	2.923115
15 **(To LFP Base)**	V1	42.306069	2.926435

Table 13: Trackside locations for radio units

Trackside units

Each trackside radio unit has one front-facing antenna and one rear-facing antenna. The standard used to connect with the train unit is IEEE 802.11ad with infrastructure extensions. Radio planning of the track site has been conducted to obtain the best location for each ground units to ensure good radio coverage and maximum performance and resilience. The train and ground antennas need a direct line of sight to work properly.

Each trackside unit radio has been installed at the top of a composite pole attached to an existing catenary stanchion in the trackside. Sometimes stanchions cannot be used due to nearby signals/signage or similar reasons. In this case, the nearest suitable stanchions have been selected. Figure 49 illustrates a trackside antenna at the top of the composite pole. The use of such poles in the corridor was specially approved by the LFP safety team in June 2022, as a prerequisite to the network deployment.

The composite pole has been designed with a support base that allows it to be lowered and raised during assembly and maintenance tasks of the installed equipment. The pole has an anchoring system that allows it to be fixed once the work is done.

1. At the base of the stanchion, on the opposite side of the pole, there is a cabinet that houses an AC/DC converter (see Figure 50).
2. The average power consumption of trackside radio unit is 40 Watts.
3. Fibre ODF tray (16 ways). The mmWave radio unit has a 10G SFP+ Ethernet port equipped with a single-mode fibre transceiver.
4. The average power consumption of trackside radio unit is 40 Watts.
5. Fibre ODF tray (16 ways). The mmWave radio unit has a 10G SFP+ Ethernet port equipped with a single-mode fibre transceiver.

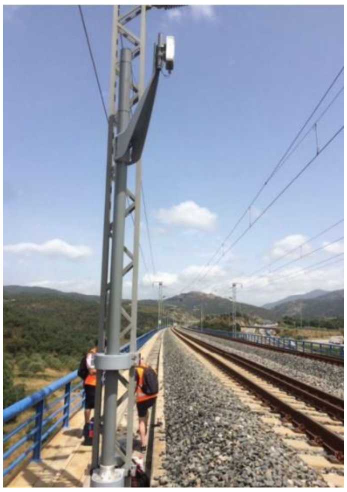


Figure 49: Trackside antenna on top the composite pole.

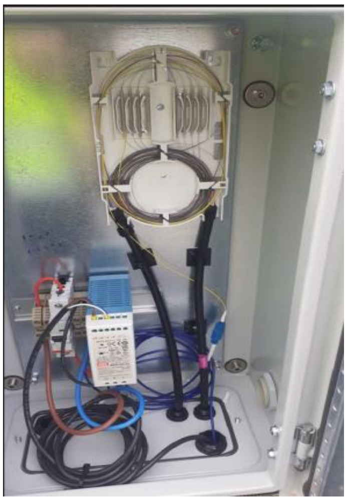


Figure 50: Internal view of the cabinet

Backhaul

The backhaul is based on a 16 multicore optical fiber which provides connectivity with a single fiber to each pole cabinet. The multicore fiber ends at the LFP Llers maintenance base, on a 24 ports Ethernet switch, as depicted in Figure 51.

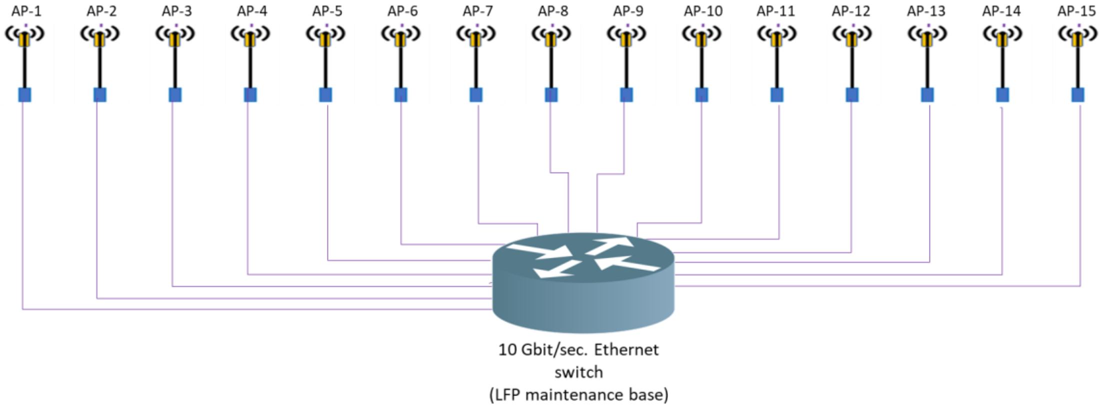


Figure 51: 802.11ad 70 GHz backhaul.

Central switching point

Co-located with the 10 Gbit/s Ethernet switch there is an 802.11 aggregation unit (depicted in Figure 52). This server is used to supply the aggregation of the two logical data streams coming from the two train units in only one aggregated flow. Finally, a firewall connects with the rest of the 5GMED ground components described in D5.1 [20] (particularly, with the ground ACS-GW unit).

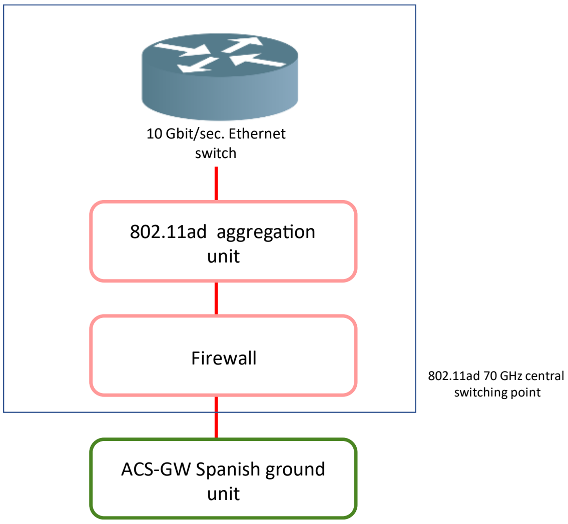

10 Gbit/sec. Ethernet switch
802.11ad aggregation unit
Firewall
802.11ad 70 GHz central switching point
ACS-GW Spanish ground unit

Figure 52: 802.11ad 70 GHz central switching point and connection to the ACS-GW

4.2.5 Satellite

Satellite connectivity is envisioned more and more as a solution to complement terrestrial coverage and ultimately provide service continuity, especially with the development of LEO (Low Earth Orbit) satellite constellations which will guarantee a much lower latency than GEO (Geosynchronous Earth Orbit) satellites.

In 5GMED, satellite connectivity is used to complement terrestrial 5G coverage for the train to ground connectivity in those remote and isolates areas of railway European corridors where there is no 5G connectivity. To this end, a Very Small Aperture Terminal (VSAT) antenna and modem have been installed on the roof of the LFP maintenance train roof to provide continuous satellite connectivity to the onboard services (represented as “direct access” in Figure 53), so that both full-coverage and multi-connection diversity are achieved jointly with the rest of radio access technologies, i.e., 5G and IEEE 802.11ad 70 GHz. The satellite connection onboard the train will be used for several services of UC3, such as service P1 on IoT and to backhaul the neutral host 5G cell inside the train depicted Figure 54.

In addition, satellite connectivity will also be used in 5GMED to provide backhaul to a fixed gNodeB (node of BTS10) to validate the scenario where a node is isolated from terrestrial networks. This scenario is represented as “fixed backhaul” in Figure 53. An VSAT fixed satellite antenna has been placed at Castellolí (Figure 55) for satellite backhauling.

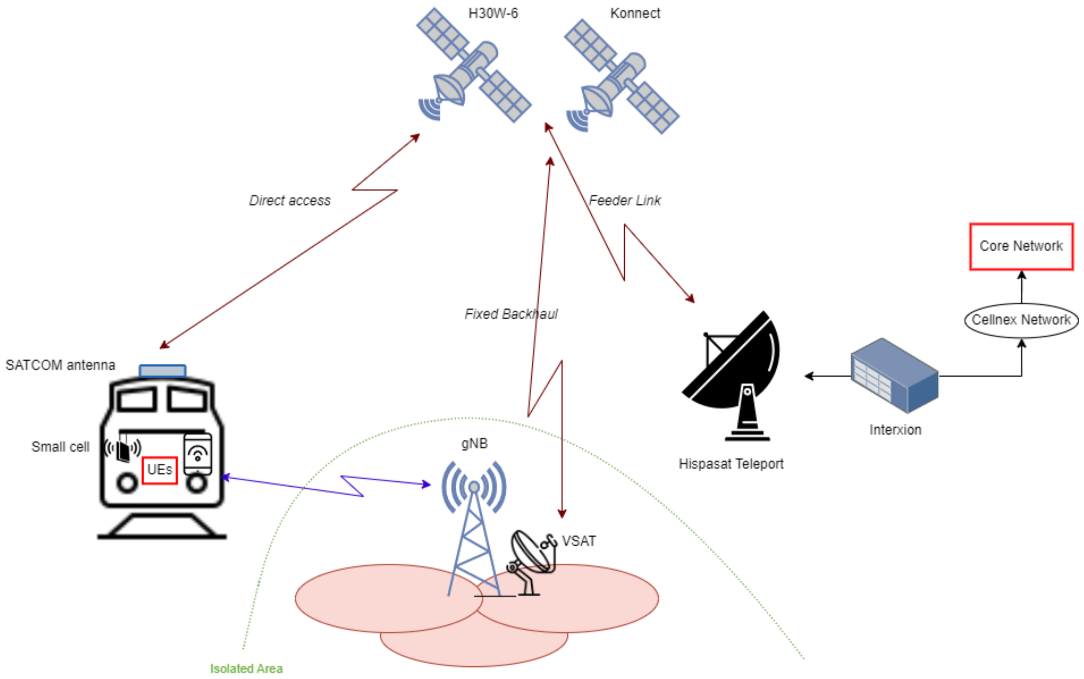
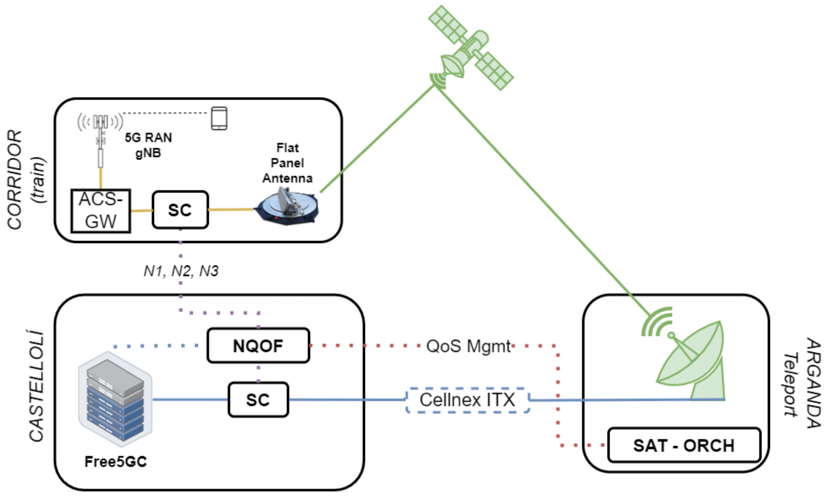


Figure 53: Use of satellite in 5GMED: direct access for train-to-ground connectivity and satellite backhauling



Legend	
Physical Link	═══
Logical interface	┄┄┄
NQOF	Network orchestrator (satellite & slicing)
SC	Slice Clasiffier

Figure 54: Satellite backhauling of the neutral host 5G cell on-board the train (service B2 of UC3)

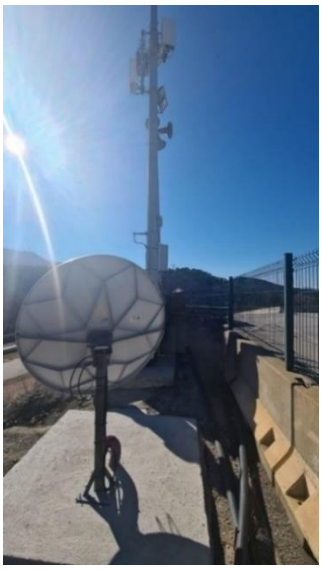


Figure 55: VSAT deployed in the circuit of Castellolí

4.3 MEC Layer

The same model of Lenovo SE350 servers deployed in Castellolí (described in Section 3.3) will be deployed in the corridor, two of them in Spain and another two in France. The MEC located in Spain will be in LFP Base at Llers (address: Carretera de Llers a Hostalets, GIP-5107, 17730 Llers, Girona). The MEC location in France will be in LFP North Base (address: Poste de Contrôle, Chemin de Balmourene, 66740 Montesquieu des Alberes).

In each location, the edge servers will serve different purposes:

- MEC1: The first edge node in each country will host the distributed UPF when the roaming configuration (LBO) will require so, as well as the Follow-me services for UC4.
- MEC 2: The second edge server in each country will serve the non-orchestrated applications for UC2 and UC3 services.

The MEC layer deployed for UC3 includes an instance of the ACS-GW and the components of the performance (FRMCS) and business services. The reason for including the ACS-GW in the MEC Layer is to support multi-connectivity between the train and the ground components and to satisfy the performance requirements of the critical services on the train. The ACS-GW for UC3 deployed in the MEC layer manages the connections for the different techlogies:5G, 70 GHz and the satellite, to provide service continuity to the FRMCS and business services.

4.4 Cloud Layer

The cloud layer deployed at Castellolí and explained in Section 3.6, is essentially a virtual layer that exists between the test site and the corridor. This cloud layer is accessible from both the test site and the corridor, allowing information to be exchanged between the two locations that in fact, compose the whole 5GMED network. The cloud layer enables a quick and secure communication, while also providing a secure environment to store and process data, allowing the users to access and share resources in an efficient manner.

Funded by the Horizon 2020 Framework Programme of the European Union

5. Paris-Satory Small-Scale Test Site

The small-scale test site in Paris-Satory is owned by VEDECOM and is located at Versailles/Satory, 20 km south-west from Paris (shown in Figure 56). It provides a test area to perform tests of connected and autonomous vehicles. It is a mix of closed and open roads, with a closed test circuit, in addition to urban and semi-rural public roads (both separated lanes and the open road are available) to support different types of vehicular use cases. In the rest of this section, more detailed information is provided about the implementation of the test site.

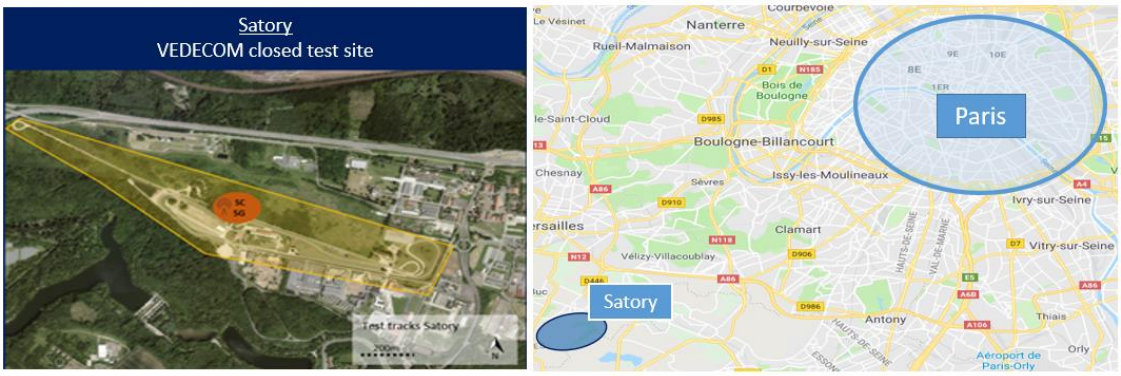


Figure 56: Paris-Satory small-scale test site

5.1 End-to-End Architecture Implementation

As shown in Figure 57, two types of 5G NSA networks are available in Paris-Satory test site: a public/commercial 5G NSA network operated by Bouygues Telecom, and a private 5G NSA network operated by TDF. The architecture of these networks is illustrated in Figure 58, and the parameters/characteristics of the private network are summarized in Table 14.

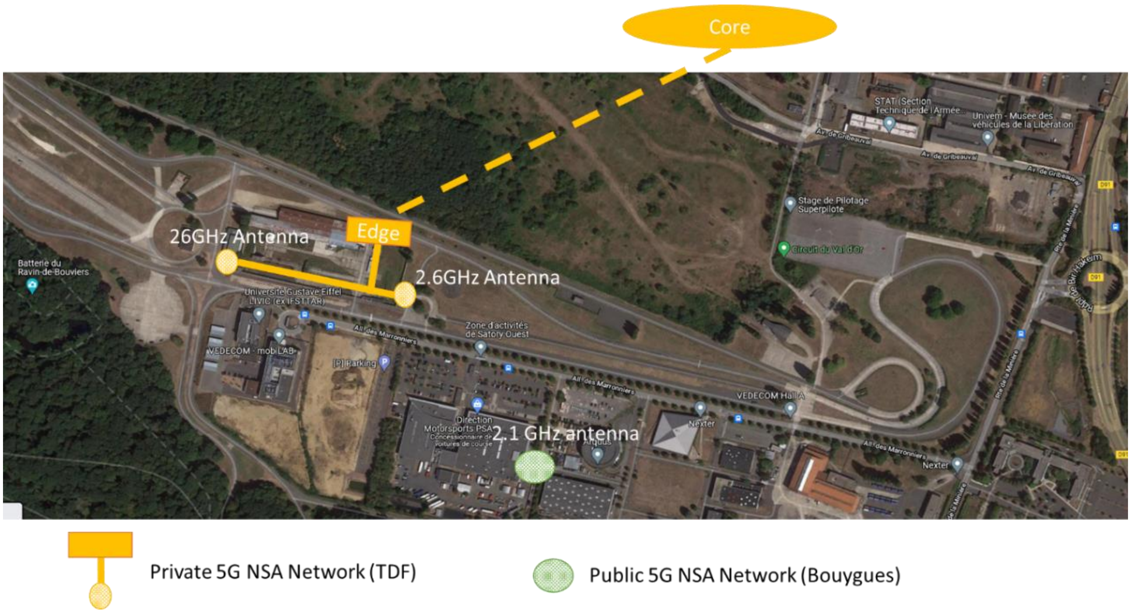


Figure 57: Illustration of 5G NSA networks at Paris-Satory test site

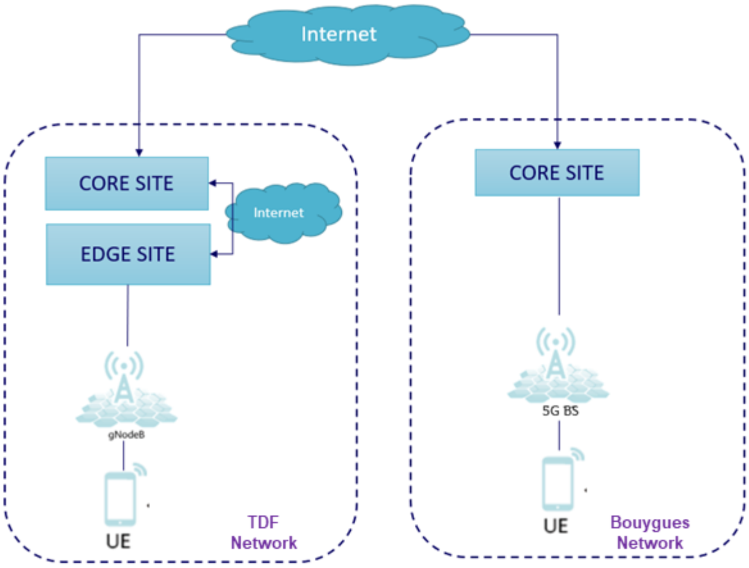


Figure 58: Internal architecture of the 5G NSA network deployment in Paris-Satory test site

Network name	Parameter	Value
TDF Private 5G NSA network (mmWave)	LTE DL Carrier Frequency (EARFCN)	37900
	NR DL Carrier Frequency (NRARFCN)	2058333 2059999
	LTE Duplex mode	TDD
	NR Duplex mode	TDD
	LTE DL Bandwidth	5 MHz
	LTE UL Bandwidth	5 MHz
	NR bandwidth	100 MHz
	Type of environment	Outdoor
	BS max EIRP	55 dBm
	UE max EIRP	55 dBm
	BS location	Latitude/ Longitude: 48.78637, 2.090895
	LTE PCIs	12
	NR PCIs	129 / 130 / 131 / 132
	MCC	1
	MNC	45
	MNC	

Table 14: TDF private 5G NSA network parameters of Paris-Satory test site

In the rest of this section, we describe the implementation of the network infrastructure layer, MEC layer, and Cloud layer of the Paris-Satory test site, respectively, in Section 5.2, Section 5.3, and Section 5.4. The rest of the layers of the 5GMED cross-border network architecture have not been implemented in Paris-Satory test site.

5.2 Network Infrastructure Layer

As explained earlier, two 5G NSA networks are deployed at Paris-Satory: a public/commercial one operated by Bouygues Telecom and a private one operated by TDF. Both networks operate isolated, and there are no cross-MNO interfaces between them to allow testing of cross-border challenges.

This section presents the network infrastructure of the TDF private 5G network, which is owned by VEDECOM and will be used for validation tests of UC1 (remote driving). The 5G Radio Access network is described in Section 5.2.1, the core is described in Section 5.2.2, and the roadside units are described in Section 5.2.3.

5.2.1 5G Radio Access Network

TDF private 5G NSA network uses the 2.6 GHz and 26 GHz (mmWave) bands. At the radio level, access to 5G NR is provided by a gNodeB with two sectors in the 26 GHz radio band to cover a full portion of the road on the test track as illustrated in Figure 59. Additionally, communication in 2.6 GHz radio band is operated in 4G, for backhaul communication. Thus, this deployment follows the principle of 5G NSA option 3x, which means that the user-plan is split across 4G and 5G cells whereas the control-plan remains under the scope of the 4G cell.

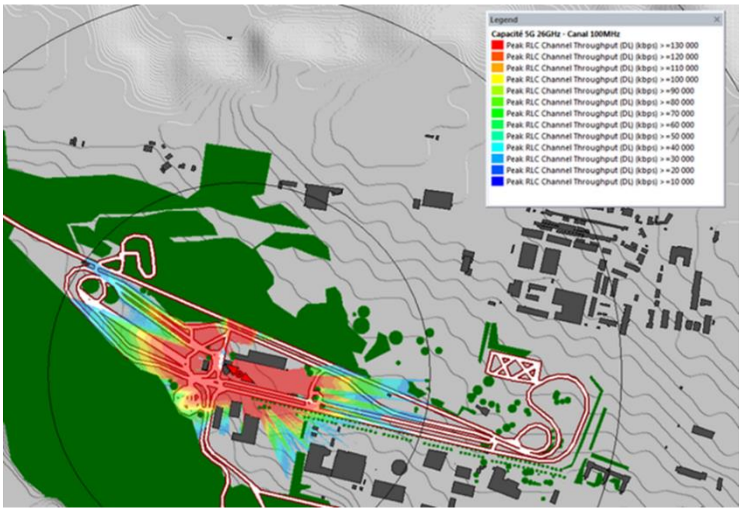

Legend
Capacité 5G 26GHz - Canal 100MHz
🟥 Peak RLC Channel Throughput (DL) (kbps) >=130 000
🟧 Peak RLC Channel Throughput (DL) (kbps) >=120 000
🟧 Peak RLC Channel Throughput (DL) (kbps) >=110 000
🟨 Peak RLC Channel Throughput (DL) (kbps) >=100 000
🟩 Peak RLC Channel Throughput (DL) (kbps) >=90 000
🟩 Peak RLC Channel Throughput (DL) (kbps) >=80 000
🟩 Peak RLC Channel Throughput (DL) (kbps) >=70 000
🟩 Peak RLC Channel Throughput (DL) (kbps) >=60 000
🟩 Peak RLC Channel Throughput (DL) (kbps) >=50 000
🟦 Peak RLC Channel Throughput (DL) (kbps) >=40 000
🟦 Peak RLC Channel Throughput (DL) (kbps) >=30 000
🟦 Peak RLC Channel Throughput (DL) (kbps) >=20 000
🟦 Peak RLC Channel Throughput (DL) (kbps) >=10 000

Figure 59: Simulation of radio coverage in 26Ghz radio band at Paris-Satory test site

5.2.2 Core Network

The core network deployed for 5G NSA option 3x is hosted at TDF and the radio equipment's are connected to it through a VPN tunnel. An edge infrastructure has been deployed following the Infrastructure as a Service (IaaS) model. This model includes two tenant - the network operator and the user - and is configured to ensure internet connectivity from the P-GW as illustrated in Figure 60.

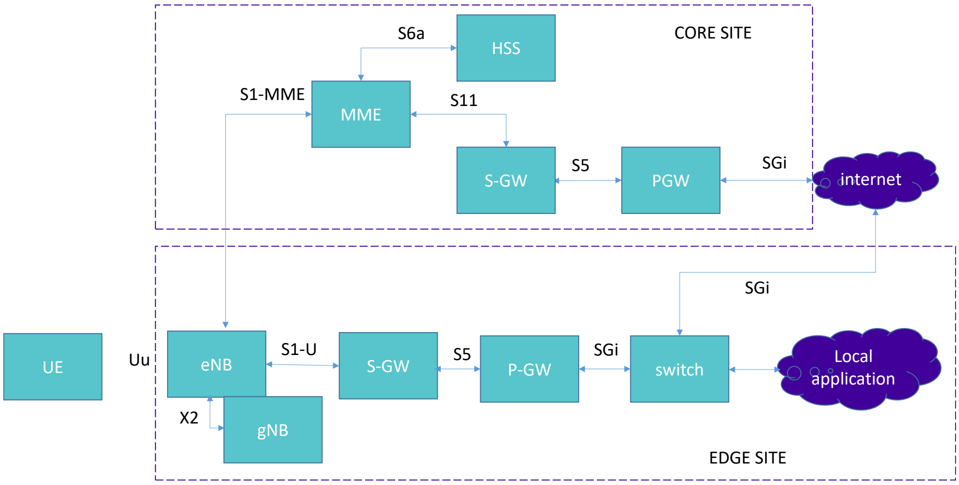


Figure 60: Architecture of the 5G NSA core network deployment Paris-Satory

5.2.3 Roadside Units

The test site also features a set of RSUs deployed on the public street with V2X capabilities, allowing the exchange of common V2X messages (CAM, DENM, etc.…) between vehicles. Currently, the supported V2X technology is based on the ETSI ITS-G5 standards with a planned support for C-V2X in the future. These RSUs are based on a custom setup with a hardware provided by UNEX, and a software developed internally by VEDECOM. The Table 15 summarizes their technical specifications.

Component	Value
CPU	NXP i.MX8 QXP
RAM	2GB
Storage	16GB+µSD
OS	Linux Debian 11
GNSS	GPS/EGNOS/GALILEO/GLONASS
Connectivity	Ethernet PoE 100Mbps full duplex
	2*ITS-G5
	Cellular modem 2G/3G/4G/5G
Power supply	48V via PoE
	Battery backup (supplied)
Integrated software	ITS Stack support
	ETSI Geonet
	CAM, DENM, SPAT, MAP, IVI, CPM, and POI
	TS 103-097 security
Weight	< 2.5kg
Dimensions	31 x 21 x 7.5 cm (Length x Width x Height) Antenna 21.5cm (Length)

Table 15: Characteristics of the RSU deployed in Paris-Satory

Funded by the Horizon 2020 Framework Programme of the European Union

5.3 MEC Layer

Figure 61 represents the MEC servers infrastructure implemented in Paris-Satory test site. Such edge site is composed of roadside infrastructure servers and an IaaS platform based on SDN technologies, i.e., OpenStack.

Thanks to its flexibility, the IaaS-based MEC platform can support different applications. As a matter of fact, it embeds a networking application and a computing & storage application. As shown in Figure 61, both the Service Gateway (S-GW) and the Packet Gateway (P-GW) of the evolved packet core (EPC) have been detached from the core site and implemented at the edge in the network host of IaaS. Such an approach enables forwarding of data exchanged with a user equipment, i.e., a connected vehicle, towards application running on the application host.

To summarize the Paris-Satory test site (Figure 62) is composed of:

- A 5G Private Network in Non-Standalone (NSA) mode
- An IaaS-based MEC platform hosting different applications.
- Five RSUs deployed along the public road that can collect data and disseminate V2X messages to road users.
- Three RSUs installed along the test track and used for laboratory and closed site testing.
- Three infrastructure servers used to monitor the different roadside sites.

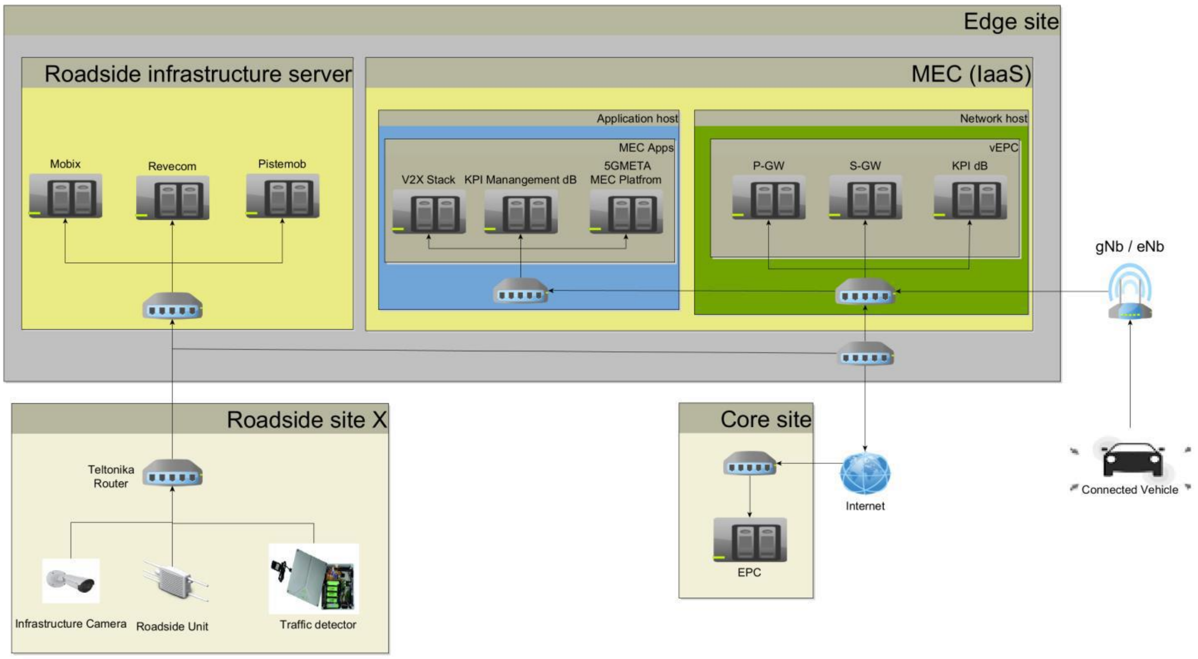


Figure 61: Illustration of the MEC instantiated as Infrastructure as a Service and relation with other components.

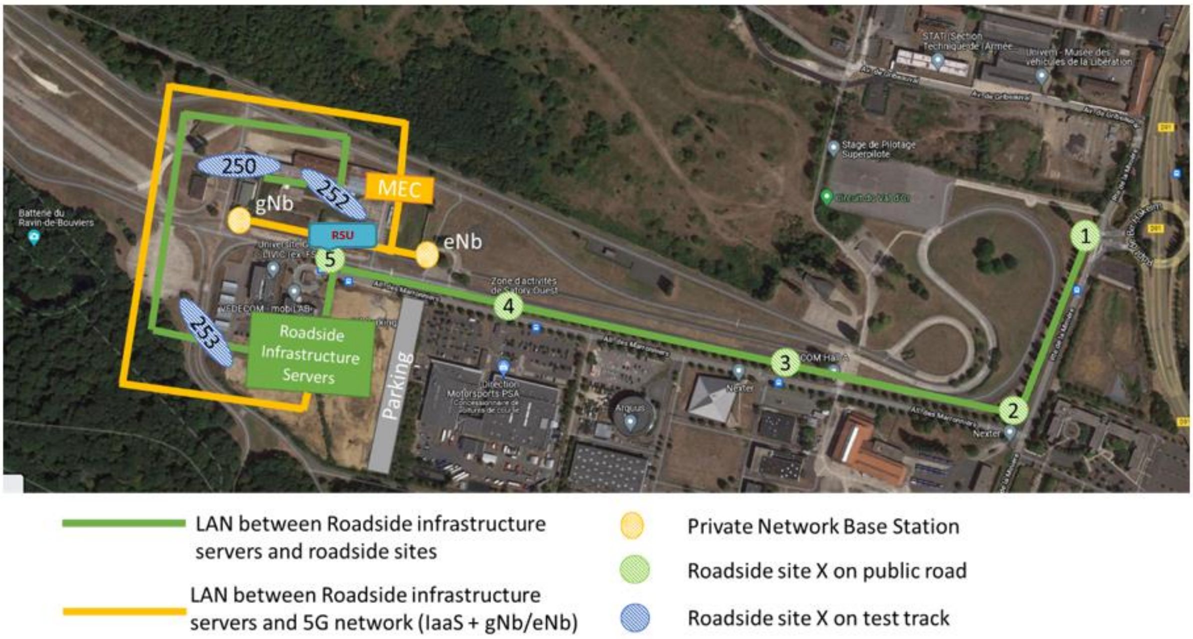

250
252
253
gNb
MEC
RSU
eNb
1
2
3
4
5
Roadside Infrastructure Servers
Parking
LAN between Roadside infrastructure servers and roadside sites
LAN between Roadside infrastructure servers and 5G network (IaaS + gNb/eNb)
Private Network Base Station
Roadside site X on public road
Roadside site X on test track

Figure 62: Description of the edge environment deployed at Versailles.

5.4 Cloud Layer

The Cloud layer used in the Paris-Satory test site for the tests and trials of UC1 is based on the Valeo Teleoperation Cloud (VTC) illustrated in Figure 63. The VTC consists of several backend servers hosted on the Amazon Web Services (AWS) platform.

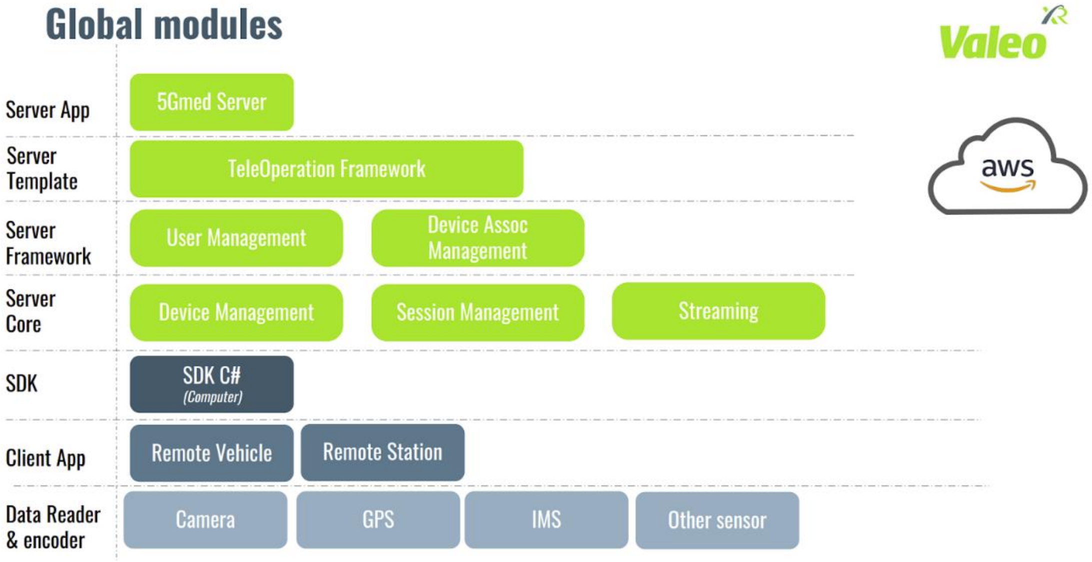


Figure 63: Valeo Teleoperation Cloud

The cloud components are hosted on a Virtual Private Cloud (VPC), within AWS. A VPC isolates computing resources from the other computing resources available in the public cloud. The VPC has a dedicated subnet and VLAN that are only accessible by the VPC customer. It prevents elements from the public cloud from accessing computing resources within the VPC. The main server App (5GMED

Server) is hosted on Amazon Elastic Compute Cloud (Amazon EC2) with two (2) CPUs, four (4) GB of memory, and a network bandwidth that can achieve up to 10 Gbps. It hosts the global cloud infrastructure.

The server Template holds the Tele-Operation Framework. It consists of sets of rules for routing and streaming services. It monitors services and makes it scalable. As computing power or network bandwidth needs to adapt, the Teleoperation Framework adapts every service to fit the needs, by increasing or decreasing the size of Memory, the type of CPU, the size of the bandwidth, the User Management service and the device Association management link all devices that use the same server and the same streaming session. Users are stored in Amazon DynamoDB (database). Every user/device provides authentication certificates to allow them to connect to the VPC and transmit data. The Device Association Management service checks the Users DynamoDB and allows or denies access to the VTC.

Services like Device Management and Session management checks the identity of every client App and creates or destroys streaming sessions for teleoperation. It also stores in dynamoDB the states of every device state (connected or not), session (Online or Offline).

The Software Development Kit (SDK) is embedded in every Client App. It reaches the API of The Valeo Cloud Platform and allows session users to connect to available streaming sessions.

The Client App enables streaming locally using data generated from sensors like Camera, GPS, Command control and other metrics. Data generated by both the Remote station and the Remote Vehicle sensors is sent through the cloud.

Funded by the Horizon 2020 Framework Programme of the European Union

6. Main Challenges and Lessons Learned

Through deployment of the cross-border 5GMED network architecture, the consortium has encountered many challenges, especially during the implementation and testing phases of the network at the different test sites. This section enumerates the most relevant challenges and lessons learnt.

It is important to remark that the project aims to implement two 5G SA networks with cross-MNO/border connectivity that ensures very low interruption time when crossing the border, and this has proven to be the one of biggest challenges.

On one hand, during the early stage of the project, several tests have been conducted to test the roaming, and intrinsically the handover between gNodeBs of different vendors. After several attempts, the consortium found out that the handover process was impossible due to incompatibility issues between Ericsson and Sunwave's radios, and the vendors declared themselves incompatible with each other. Therefore, the Castellolí small-scale test site had to be redesigned using only Sunwave gNodeBs. The project is currently testing the handover between Ericsson and Nokia's gNodeBs at the test site on the cross-border corridor, and the preliminary results have been more successful, which is also explained by the fact that these vendors are categorized as Tier1 vendors and are commonly used by network operators.

The roaming optimization mechanisms are also a big challenge that is still being addressed by the project. To do so, the Castellolí small-scale test site was selected for testing these roaming techniques, because it is a time effective solution where a lot of cross-border situations can be triggered within a very short period of time, in contrast with the cross-border corridor where it is more difficult to reproduce them and it takes more than an hour to cross the border, turn around, and cross it again in the other direction. This choice facilitated the work of the 5GMED's network team working on this topic and allowed them to learn and progress. Nevertheless, an important challenge subsisted in the fact that the commercial 5G Cores were still under development for inter PLMN-IDs handovers. Thus, the project had to align its timeline with the manufacturer's releases roadmap and subsequently do more tests with the different 5G Core releases and the roaming techniques that they were providing. For example, the N14 interface release arrived later than expected and that added extra delays, as well as the complexity of making the hand-over work: we could not understand the behaviour of roaming in movement until the vendor found the correct parametrization in the 5G Core for the handover to work.

Another important challenge was related to the UE's limitations. Most smartphones do not support "testing" (non-commercial) PLMN IDs, which negatively impacted the end-to-end network performance trials. Additionally, only a limited numbers of UE's models support slicing, while being limited to a single active slice. A similar issue has been encountered, consisting of a lack of support of slicing by equipment provided by some RAN vendors (e.g., Sunwave), thus it was not possible to test it directly on the small-scale test site of Castellolí, as it was planned in the beginning.

Moreover, the last point is that the deployment of orchestrated (dynamic) network slicing in the RAN side is still far from being realistic. The available commercial RAN equipment allows communication with an orchestrator through OSS, but having an OSS is not cost-effective for a project with a limited number of gNodeBs, and using an existent one from Vodafone or Free Mobile was finally discarded due to cybersecurity risks.

Finally on the corridor, it was known that the irregular orography may cause some challenges, but the consortium did not know that it was going to be so complex. The transport network in the corridor is very elaborated, it requires multi-hop microwave links and multiple fiber interconnections that made the transmission a difficult point in the commissioning of each node.

7. Conclusions

This deliverable is the first document reporting the implementation and deployment of the 5GMED ICT Infrastructure in the test sites of 5GMED for the execution of small-scale trials. Furthermore, the deliverable describes in detail the key concepts of the 5GMED cross-border network architecture, and hence should be considered as complementary to the deliverable D3.2. More specifically, it is important to keep in mind that this project aims to demonstrate the benefit of a such architecture in guaranteeing service continuity and better user experience, by reducing service interruption time and speeding the handover procedure, especially in cross-border scenarios where roaming occurs. To do so, the project has identified two distinct stages: a first one in which the architecture will be tested on the small-scale test site of Castellolí; and a second one during which the same architecture will be demonstrated and validated on the cross-border large scale test sites.

The present document is directly linked to this first stage since, it comes back on the different test sites dedicated to the small-scale trials of both the automotive use cases (UC1, UC2 and UC4) as well as the railway use cases (UC3). Furthermore, it details how the architecture has been translated into a concrete deployment and implementation at each test site. Finally, it gives some insights related to the main challenges faced during this activity.

Finally, and as explained earlier, this deliverable is related to the first stage of the project and therefore is a prerequisite and an input to the tests and trials activities to be carried out by the Work Package 6; and in a similar fashion the incoming deliverable D3.4 “Final release of the 5GMED ICT Infrastructure” will report the deployment and implementation of the same architecture on the cross-border corridor for the large scale trials during the second stage of the project.

8. References

[1] J. N. e. al, «5GMED Architecture for Advanced Automotive and Railway Communication Services in Cross-Border Scenarios,» *2022 IEEE Future Networks World Forum (FNWF),* 2022.

[2] 5GMED, «D3.1 Analysis of 5GMED Infrastructure Requirements and 5G Handover between Networks and Cross-Border,» [En ligne].

[3] ETSI, «MEC: Multi-access Edge Computing,» [En ligne]. Available: https://www.etsi.org/technologies/multi-access-edge-computing.

[4] ETSI, «GR MEC 017, "Mobile Edge Computing (MEC); Deployment of Mobile Edge Computing in an NFV environment" V1.1.1,» 2018.

[5] GSMA, «Official Document IR.34 - Guidelines for IPX Provider networks (Previously Inter-Service Provider IP Backbone Guidelines), Version 14.0,» August 2018.

[6] S. &. A. N. Mohan, «. (2011). A convergent framework for QoS-driven social media content delivery over mobile networks. 1 - 7. 10.1109/WIRELESSVITAE.2011.5940846.,» vol. 2011.

[7] GSMA, «5G Operator Platform,» [En ligne]. Available: https://www.gsma.com/futurenetworks/5g-operator-platform/.

[8] X. P. G. E. A. e. a. FOUKAS, «Network slicing in 5G: Survey and challenges,» *IEEE Communications Magazine,* vol. 55, n° %15, 2017.

[9] I. Standards, IEEE Standard for Local and metropolitan area networks--Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks.

[10] R. e. a. Vilalta, «Applying security service level agreements in v2x network slices,» *2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN),* 2020.

[11] 3GPPP, «TS 23.503: Policy and charging control framework for the 5G System (5GS); Stage 2».

[12] 3. T. 2. v. 1. R. 17, « Management and orchestration; Concepts, use cases and requirements,» 2023.

[13] GSMA, «East-Westbound Interface APIs,» 23 03 2023. [En ligne]. Available: https://www.gsma.com/futurenetworks/wp-content/uploads/2023/03/GSMA-Operator-Platform-Group-East-Westbound-Interface-APIs-v2.pdf.

[14] 5GMED, «D3.2: ICT Architecture and Initial Design».

[15] 5GMED, «D2.2 Initial definition of 5GMED test cases, deployment options and tools».

[16] 5GMED, «D4.2 Initial apps for automotive test cases».

Funded by the Horizon 2020 Framework Programme of the European Union

[17] GSM Association, «East-Westbound Interface API - yaml file,» [En ligne]. Available: https://www.gsma.com/futurenetworks/wp-content/uploads/2023/03/EWBI_Federation_API_v2.zip. [Accès le 21 June 2023].

[18] ONF, «TAPI v2.1.3 Reference Implementation Agreement,» 2020.

[19] e. a. L Gifre, «Slice Grouping for Transport Network Slices Using Hierarchical Multi-domain SDN Controllers,» chez *OFC*, 2023.

[20] 5GMED, «D5.1 Railways Application Requirement Analysis Report».

[21] GSMA Association, «Operator Platform Telco Edge Requirements,» 29 March 2023. [En ligne]. Available: https://www.gsma.com/futurenetworks/resources/operator-platform-telco-edge-requirements/.

[22] GSM Association, «Southbound Interface Network Resources APIs,» 29 March 2023. [En ligne]. Available: https://www.gsma.com/futurenetworks/resources/southbound-interface-network-resources-apis/.

[23] GSM Association, «User-Network Interface APIs,» 29 March 2023. [En ligne]. Available: https://www.gsma.com/futurenetworks/resources/gsma-operator-platform-group-user-network-interface-apis/.

[24] GSMA Association, «East-Westbound Interface APIs,» 2023 March 29. [En ligne]. Available: https://www.gsma.com/futurenetworks/resources/east-westbound-interface-apis/.

[25] CAMARA, «CAMARA Presentation,» June 2023. [En ligne]. Available: https://camaraproject.org/wp-content/uploads/sites/12/2023/06/CAMARA-Presentation.pdf.

[26] GSMA, «GSMA Open Gateway: Universal mobile network open APIs for developers,» [En ligne]. Available: https://www.gsma.com/futurenetworks/gsma-open-gateway/.

[27] C. L. N. a. T. F. GSMA, «White Paper: "The Ecosystem for Open Gateway NaaS API Development",» June 2023..

[28] M. 2023, «Camara Project and Open Gateway details are revealed but no answers about commercial models.,» [En ligne]. Available: https://www.analysysmason.com/research/content/articles/mwc-camara-gateway-rdmv0-rma04/.

[29] L. Foundation, «CAMARA Project,» [En ligne]. Available: https://camaraproject.org/.

[30] LFP Perthus, *https://www.lfpperthus.com/la-ligne.html.*

Funded by the Horizon 2020 Framework Programme of the European Union

9. Annex A: GSMA Operator platform

The GSMA Operator Platform group defines the concept of a common “Operator Platform” (OP) [[7] to make operators assets and capabilities consistently available across networks and across national boundaries. GSMA foresees that operators will collaborate to offer interoperability through a common platform that allows to package and expose their services and network capabilities.

The operator platform, which leverages federation, enables access to the Edge/Cloud capability of an operator, or even other operators that are part of the federation, by just connecting to a single platform. This is implemented by following the four-side approach shown in the figure below (Figure 64).

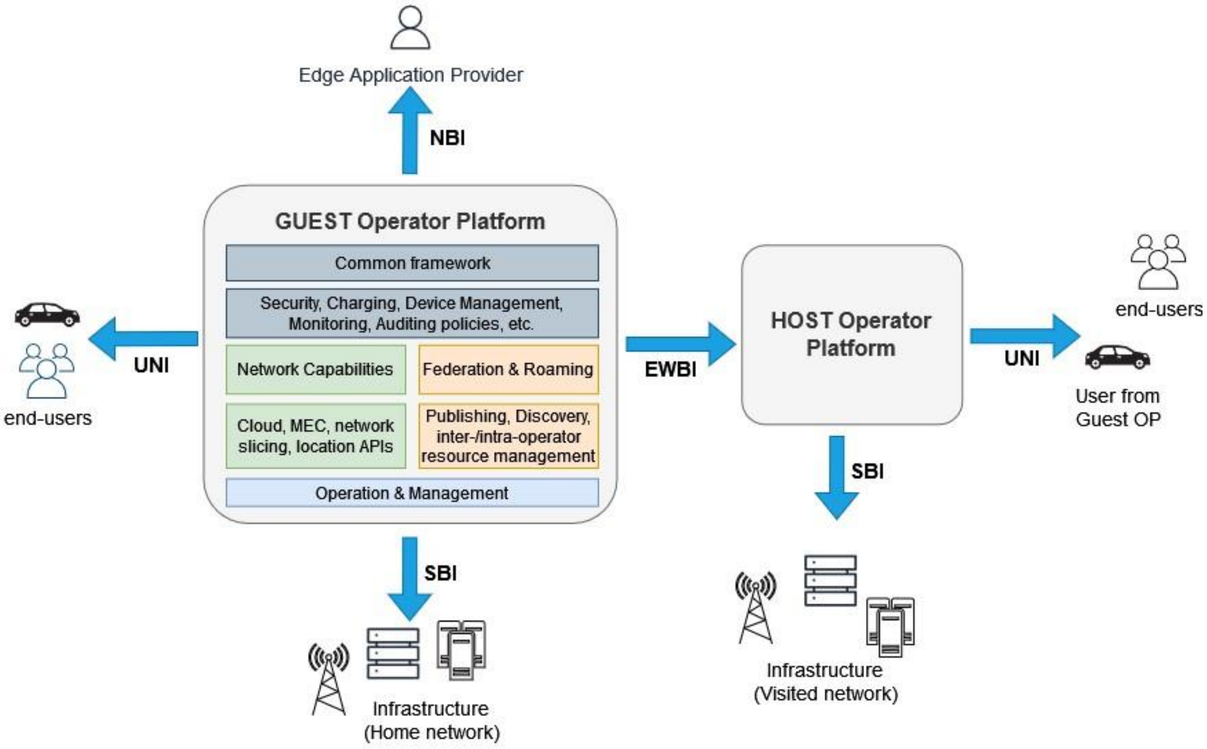

Edge Application Provider
NBI
GUEST Operator Platform
Common framework
Security, Charging, Device Management, Monitoring, Auditing policies, etc.
Network Capabilities
Federation & Roaming
Cloud, MEC, network slicing, location APIs
Publishing, Discovery, inter-/intra-operator resource management
Operation & Management
UNI
end-users
EWBI
HOST Operator Platform
UNI
end-users
User from Guest OP
SBI
Infrastructure (Home network)
SBI
Infrastructure (Visited network)

Figure 64: High-level federation building blocks and APIs.

The four interfaces of this model, as defined by the GSMA Operator Platform Group [21], are:

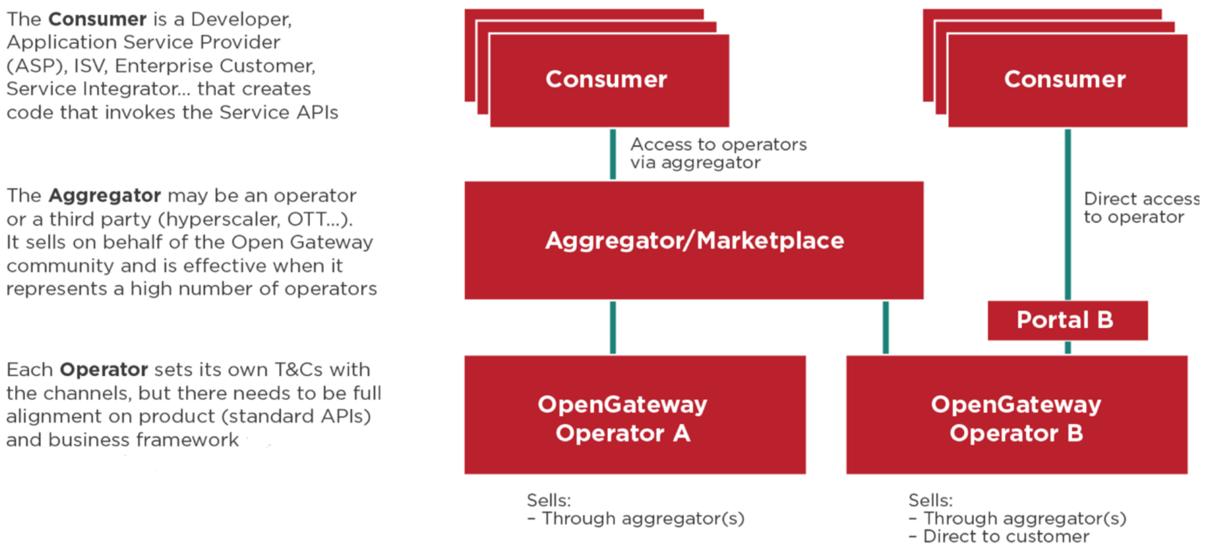
- **The Northbound Interface (NBI)** enables service management and fulfilment of enterprise and Application Providers’ use case requirements.
- **The Southbound Interface (SBI)** [22] is responsible for connecting the OP with the specific operator providing the infrastructure to deliver the network services and capabilities to the user.
- **The User-Network Interface (UNI)** [23] enables the User Client hosted in the user equipment to communicate with the OP.
- **The East/Westbound Interface (EWBI)** [24] is the interface between instances of the OP that extends an operator’s reach beyond its footprint, enabling them to exchange information about the network and service status.

In a federation scenario, the HOST OP is the owner of the infrastructure residing in the visited network, while the GUEST OP belongs to the operator that has its own infrastructure in the home network and can use the infrastructure of the visited network.

10. Annex B: Exposure Gateway

The concept of Exposure Gateway enables the exposure of MNO's services to a consumer, who can be an application service provider, developer, or other relevant stakeholders. The Exposure Gateway is described in ETSI [4], CAMARA [25], and GSMA Operator Platform [26]. Several prerequisites must be met to enable such federation: MNOs must agree to share their edge cloud resources, establish a resource-sharing policy, and enable connectivity between the operator exposure platform instances to facilitate Exposure Gateway signalling.

The Exposure Gateway presents equivalent functionalities to the OpenGateway layer of the Open Gateway Network as a Service (NaaS) system architecture [27], as represented in Figure 65. The purpose of the OpenGateway (equivalent to the Exposure Gateway) is to provide a means for the MNOs to expose their functionalities. Thus, the Exposure Gateway is a key component, necessitating the exchange of resource catalogues for efficient resource utilization.



The **Consumer** is a Developer, Application Service Provider (ASP), ISV, Enterprise Customer, Service Integrator... that creates code that invokes the Service APIs

The **Aggregator** may be an operator or a third party (hyperscaler, OTT...). It sells on behalf of the Open Gateway community and is effective when it represents a high number of operators

Each **Operator** sets its own T&Cs with the channels, but there needs to be full alignment on product (standard APIs) and business framework

Figure 65: Diverse Relationship Models for the Open Gateway in Network as a Service (NaaS)

An Exposure Gateway (based on the Open Gateway NaaS architecture) is required to expose the service APIs to consumers. These APIs are exposed directly to consumers, but an aggregator can also be added in scenarios where a single-entry point for consumers is required across all MNOs.

The functionalities provided by the Open Gateway Network as a Service (NaaS) are complementary to the concept of the CAMARA project, designed to ensure the standardization of APIs across networks, simplifying cross-network integration.

Funded by the Horizon 2020 Framework Programme of the European Union

11. Annex C: CAMARA API

CAMARA APIs are designed to prioritize scalability, global reach, and simplicity of use, resulting in improved service delivery and user experience. CAMARA provides an abstraction from network APIs to service APIs, which is necessary to facilitate application-to-network integration. This abstraction is implemented through a southbound interface network resources (SBI-NR) and a southbound interface cloud resource (SBI-CR), using a transformation function that abstracts network APIs into service APIs to facilitate application-to-network integration. It should be noted that CAMARA deals exclusively with customer-facing northbound APIs related to telco mobile networks. APIs used for east-west federation or roaming purposes are not within the scope of CAMARA.

Moreover, CAMARA collaborates with the GSMA Operator Platform Group to align API requirements, and it is also in alignment with the Open Gateway NaaS architecture. In this context, the Open Gateway initiative [27] operates within the CAMARA project, which also hosts the open-source APIs developed by Open Gateway [28]. The integration of the CAMARA and Open Gateway concepts is depicted in Figure 66.

This approach covers three types of Northbound APIs:

- Service APIs: These APIs are intended for end consumers and integrated by developers to invoke a given telco capability, such as quality on demand (QoD), device location, edge discovery and selection, and others. Such APIs are implemented by CAMARA.
- Service Management APIs: These APIs enable end consumers to perform management functions or to get data about offered Service APIs during runtime e.g., service availability and performance information. Such APIs are implemented by CAMARA.
- Additionally, Operate APIs are provided to offer programmable access to operation, administration, and management capabilities. These APIs facilitate seamless integration of the Open Gateway NaaS Platform with portals, marketplaces, and other aggregator platforms. These APIs are out of the scope of CAMARA and are covered by standards development organizations.

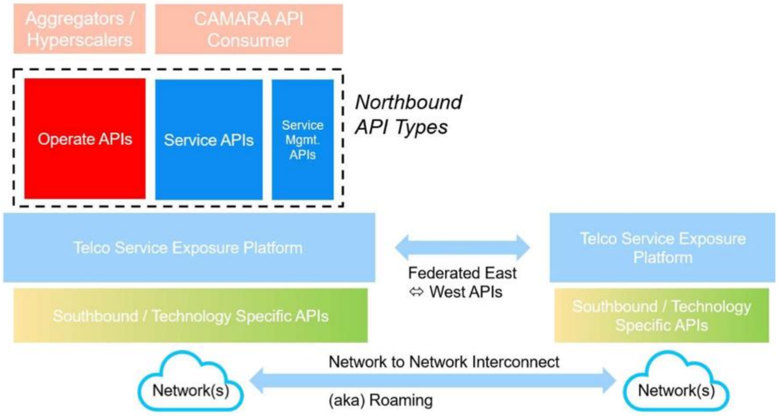

Aggregators / Hyperscalers
CAMARA API Consumer
Operate APIs
Service APIs
Service Mgmt. APIs
Northbound API Types
Telco Service Exposure Platform
Federated East ⇔ West APIs
Telco Service Exposure Platform
Southbound / Technology Specific APIs
Southbound / Technology Specific APIs
Network(s)
Network to Network Interconnect
(aka) Roaming
Network(s)

Figure 66: Northbound API types in the GSMA-CAMARA approach [7]

Some specific CAMARA APIs available to consumers are also depicted in Figure 66, including MEP services, routing, and more. It's important to note that CAMARA is an ongoing project, with continuous development of new capabilities