Grant Agreement Number: 768953

Project acronym: ICT4CART

Project full title: ICT Infrastructure for Connected and Automated Road Transport

D3.2

Flexible Network Specification and Architecture

Due delivery date: 31 August 2019

Actual delivery date: 30 August 2019

Organisation name of lead participant for this deliverable: NOKIA

Dissemination level		
PU	Public	X
PP	Restricted to other programme participants (including the GSA)	
RE	Restricted to a group specified by the consortium (including the GSA)	
CO	Confidential, only for members of the consortium (including the GSA)	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 768953

Document Control Sheet

Deliverable number:	D3.2
Deliverable responsible:	NOKIA
Work Package:	WP3 – ICT Architecture for Connected and Automated Traffic
Editor:	Wimmer Markus<markus.wimmer@nokia.com>

Author(s) – in alphabetical order		
Name	**Organisation**	**E-mail**
Haetty Birger	NOKIA	birger.haetty@nokia.com
Schulz Steffen	NOKIA	steffen.schulz@nokia.com
Wimmer Markus	NOKIA	markus.wimmer@nokia.com

Document Revision History			
Version	**Date**	**Modifications Introduced**	
		Modification Reason	**Modified by**
V0.1	07/31/2019	Initial version	Markus Wimmer Birger Haetty Steffen Schulz
V1.0	28/08/2019	Final version with reviewer's comments consolidated	Markus Wimmer Birger Haetty Steffen Schulz

Abstract

This document is the initial version of the hybrid communication architecture (task T3.2 of ICT4CART). It defines the scope of the ICT4CART communication environment. It provides capabilities of each communication systems and components thereof.

The ICT4CART hybrid communication architecture covers methods of bearer service management, edge computing, and network slicing solutions to enable data exchange, including low latency data transmission by placing IT and cloud services close to a UE's point of attachment.

Legal Disclaimer

Abbreviations and Acronyms

Acronym	Definition
3GPP	3rd Generation Partnership Project
5G	5th Generation (Mobile Communication Network)
AF	Application Function
APN	Access Point Name
BS	Base Station
CAM	Cooperative Awareness Message
CN	Core Network
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CUPS	Control and User Plane Separation
DCN	Dedicated Core Network
DCSP	Data Centre Service Provider
DECOR	Dedicated Core Network
DENM	Decentralized Environmental Notification Message
E2E	End-to-End
EC	European Commission
ECM	EPS Connection Management
eDECOR	Enhanced DECOR
eNB	Enhanced NodeB
EPC	Evolved Packet Core
EPS	Enhanced Packet Service
E-RAB	Enhanced Radio Access Bearer
ETSI	European Telecommunications Standards Institute
E-UTRAN	evolved UMTS Terrestrial Radio Access
GW	Gateway
HPLMN	Home PLMN
HSS	Home Subscriber Service
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPsec	Internet Protocol Security (a protocol suite)
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Standards Organisation
IT	Information Technology
ITSC	ITS Communications
ITS	Intelligent Transport System
ITS-S	ITS-Station
GA	Grant Agreement
gNB	Next Generation NodeB
GW	Gateway
GTP-u	GPRS Tunnelling Protocol – user plane
KPI	Key Performance Indicator
LTE	Long Term Evolution
MAC	Medium Access Control
MAP	MapData Messages

MCC	Mobile Country Code
MEC	Multi-access Edge Computing, (originally called Mobile Edge Computing)
MME	Mobility Management Entity
MNC	Mobile Network Code
MNO	Mobile Network Operator
MOCN	Multi-Operator Core Network
MORAN	Multi-Operator Radio Access Network
NR	New Radio
NSA	Non-Standalone
NSaaS	Network Slice as a Service
OBU	On Board Unit
OSI	Open Systems Interconnection
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PGW	Packet Gateway
PHY	Physical (Layer)
PLMN	Public Land Mobile Network
PO	Project officer
QoS	Quality of Service
RAB	Radio Access Bearer
RAN	Radio Access Network
RSU	Roadside Unit
RTS/CTS	Request To Send/Clear To Send
SA	Standalone
SI	Subscriber Identity
SIM	Subscriber Identity Module
SIPTO	Selected IP Traffic Offload
SGW	Serving Gateway
SPAT	Signal Phase And Timing
SPATEM	Signal Phase And Timing Extended Message
STA	Station (in IEEE 802.11)
TCP	Transmission Control Protocol
TDF	Traffic Determination Function
TS	Technical Specification
TTI	Transmission Time Interval
UE	User Equipment
UPF	User Plane Function
URLLC	Ultra-Reliable Low Latency Communication
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Infrastructure
VPLMN	Visited PLMN
WP	Work Package

Table of Contents

List of Figures

List of Tables

Executive Summary

Hybrid connectivity allows an ITS Station to use more than one radio access technologies, both cellular and ad-hoc radio access technologies, to provide or use vehicular services. Multiple radio access technologies can be applied in an OBU, which then decides which access technology to use. A service deployed e.g., in an RSU can also use multiple radio access technologies. In this case, it can provide its service to OBUs in vehicles which either have cellular (LTE/5G) or ad-hoc (ITS-G5) radio access technology implemented.

Cellular radio networks are designed as multi-purpose networks. Hereby LTE is the dominant technology in Europe at the time being and for the next years. To provide real-time critical services close to a UE's point of attachment is a challenge in most existing operator's infrastructures. This document outlines possible strategies how this can be achieved. This involves the use of edge computing and network slicing strategies developed for cellular radio networks like LTE.

These strategies differ to what extend vehicular services can

- be isolated from the traffic of other users,
- be dynamically provided with the quality of service appropriate for the service;
- be provided with IT and cloud computing at the edge of the radio access network;

Hybrid connectivity provides the required level of redundancy, reliability and availability for higher levels of automated driving.

In order to allow a more flexible deployment of cellular radio networks, different network strategies and architectures are proposed and discussed.

1 Introduction

1.1 Aim of the Project

Today, significant and rapid advances in both telecom and IT industries can be accredited to fast-growing disruptive technologies. Amongst these, the ETSI ITS G5 and the 3GPP LTE technologies are quite mature. Moreover, the 3GPP 5G technology is evolving rapidly. Cellular networks such as LTE and 5G allow existing and novel vehicle features with low cost and rapid deployment since they can utilize existing cellular network infrastructure. In the light also of the above, several ICT challenges related to connectivity, data management, cyber-security and ICT infrastructure architectures still play a significant role and need to be addressed to enable road vehicle automation. Thus, it is of utmost importance for the vehicle automation to work on the direction of advancing the digital and ICT infrastructure, taking also into consideration the limitations in both resources and investments, in the physical transport infrastructure.

ICT4CART aims to address the gaps to deployment bringing together key players from automotive, telecom and IT industries, to shape the ICT landscape for Connected and Automated Road Transport and to boost the EU competitiveness and innovation in this area.

The main goal of ICT4CART is to design, implement and test in real-life conditions a versatile ICT infrastructure that will enable the transition towards higher levels of automation (up to Level 4) addressing existing gaps and working with specific key ICT elements, namely hybrid connectivity, data management, cyber-security, data privacy and accurate localization. ICT4CART builds on high-value use cases (urban and highway), which will be demonstrated and validated in real-life conditions at the test sites in Austria, Germany and Italy. Significant effort will be put also on cross-border interoperability, setting up a separate test site at the Italian-Austrian border.

1.2 Purpose of the document

This document is the first version of the hybrid ITS communication specification (task T3.2 of ICT4CART). It outlines the ICT4CART hybrid communication, and how to achieve performance and resilience especially for higher levels of automation. It shows the co-existence of cellular and ad-hoc networks as a way to achieve the required levels of redundancy, reliability, and availability. The document describes a high-level LTE/5G architecture as well as more detailed architectures focused on network slicing and multi-access edge computing.

1.3 Target Audience

This document is a public deliverable of the ICT4CART project. It is primarily targeted to the project partners involved in the design and development of the ICT4CART architecture. The document may also be of interest to any reader who wishes to be informed about the ICT4CART architecture.

2 Communication Architecture

One of the objectives of the ICT4CART project is to specify and to design the technological cornerstones expected from infrastructure which provides hybrid connectivity and communication for higher levels of automated driving. Hybrid connectivity integrates multiple access technologies such as LTE/G5 and ITS-G5. If more than one radio access technology is available, service providers and applications for vehicles can choose the radio access technology or technologies best suitable for service provisioning.
Due to the vehicles' mobility, the availability of wireless access technologies changes with location, and the hybrid communication infrastructure enhances the probability that at least one access technology is available via which service continuation is possible. The service provision may have to be adjusted to the technical abilities of the available wireless access technology, characterized by parameters such as packet loss rate, transmission latency, and data transmission range. The integration of multiple wireless access technologies for vehicular services such as automated driving increases the service availability, service reliability, and service robustness.

ETSI EN 302 665 V1.1.1 [1] specifies the ITS Communications Architecture. An ITS Station is organized in four principal layers:

- "Access" representing ITSC's OSI layers 1 and 2,
- "Networking & Transport" representing ITSC's OSI layers 3 and 4,
- "Facilities" representing ITSC's OSI layers 5, 6 and 7.
- "Applications" presenting the ITS-S applications making use of the ITS-S services to connect to one or more other ITS-S applications.

In "Facilities" and "Applications", the ITS messages are generated and processed, such as CAM/DENM [2][3] or SPAT/MAP [4]. The "Network & Transport" Layer provides end-to-end connectivity between "Facilities" in different ITS Stations e.g. by using TCP/IP (= classical OSI L4/L3 transport) or Geo-Networking [5][6].

Access technologies such as LTE and Wi-Fi operate in the "Access" Layer of the ITS Communications Architecture. The access technologies provide as a service transport of higher layer data between ITS Stations.

2.1 Cellular Radio Networks

Any access network technology controls the connectivity between its edge nodes. In LTE/5G networks, the edge nodes are the user equipment (UE) and the so-called packet data network gateway (PDN GW or PGW). The PGW provides the connection to packet data networks (PDNs). Base stations called eNB in LTE and gNB in 5G connect the UEs via the radio interface with the remaining cellular network infrastructure.

A cellular operator can only control the transport Quality of Service (QoS) within its network, i.e. between the UE and the PGW. The end-to-end QoS depends on the service agreements between all network operators providing connectivity between the ITS-S hosts.

If the user equipment is directly integrated in a car's OBU, and if the ITS-S host is run on a server or server cloud, which is directly connected to the PGW or is even run on the same hardware, then the cellular network provides an end-to-end transport QoS for the ITS service. This is especially of interest for time-critical applications as required for higher levels automated driving.

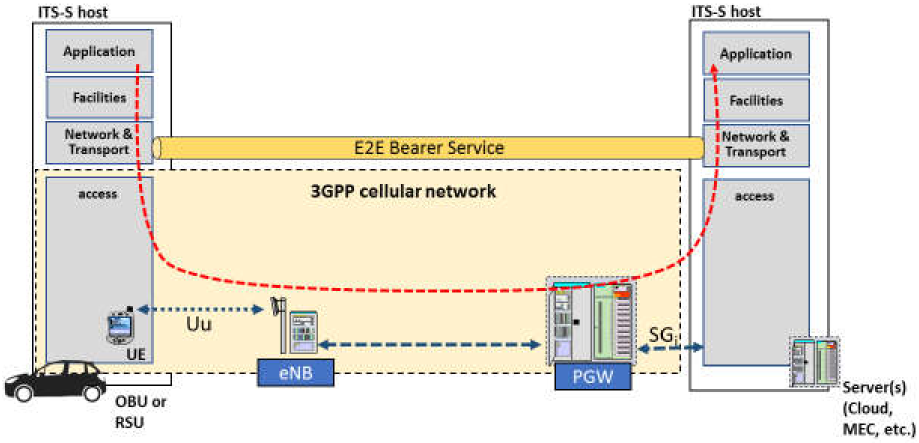

Figure 1: Cellular Communication

2.2 Ad-hoc Radio Networks

The IEEE 802.11 standard family is typically used for ad-hoc communication. ITS-G5 uses IEEE 802.11p [8]. The access nodes are called stations (STA). If the STA is directly integrated in the "Access" Layer of a car's OBU or an RSU, then direct communication is possible between those ITS Stations. The wireless devices share the radio medium in any given radio frequency region. This can lead to collisions if more than one device tries to communicate simultaneously. Mechanisms are in place to reduce the probability that those collisions happen, including CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) and RTS/CTS (Request To Send/Clear To Send).
In ITS-G5, low latency between two ITS-S hosts are inherently built into the access technology, as the ITS-S hosts directly exchange data without an intermediate network. However, in case of heavy radio frequency usage, i.e. when a huge number of wireless devices interacts within a small geographical region, access to the wireless medium can be delayed. The risk of simultaneous transmission of neighbouring wireless devices translates directly in the reliability of the wireless transmission.

The GeoNetworking protocol [5][6] may provide self-organized communication between ITS vehicle stations by e.g. prioritizing of packets depending of their importance for security and data congestion control, if used by ITS Stations.

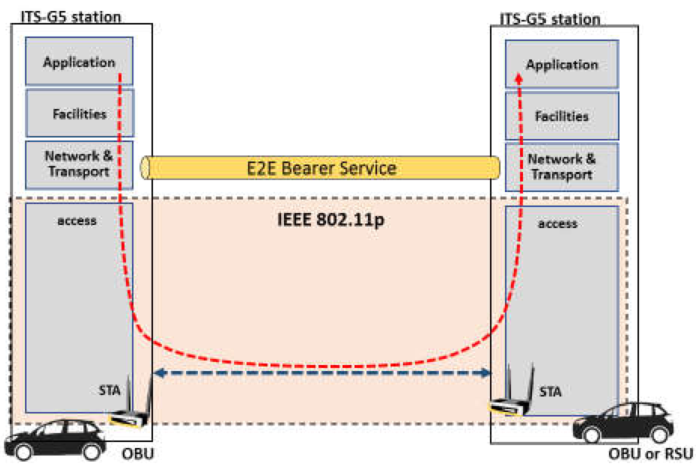

Figure 2: ad-hoc communication

2.3 Hybrid Communication

An ITS Station supports hybrid radio access, if more than one access technology is integrated in its "Access" layer. An ITS Station can then choose the radio access technology or radio access technologies used to send ITS messages and data. For instance, if LTE and ITS-G5 are integrated in traffic light system, it can send SPATEMs directly to vehicles using ITS-G5. It can also send the SPATEMs to an (central) ITS-S, which then distributes these messages to vehicles in the proximity of the traffic light systems, whose OBUs support cellular communication. This example is outlined in Figure 3 and Figure 4.

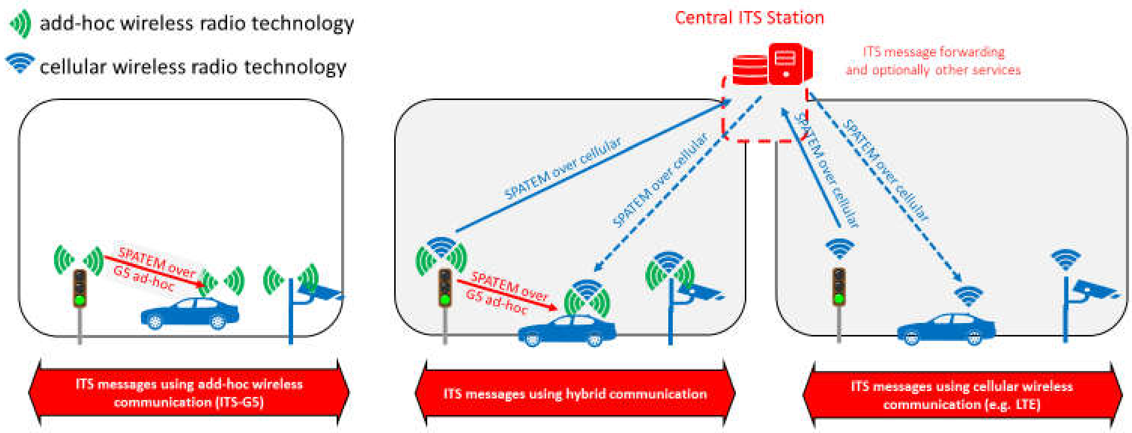

Figure 3: hybrid communication – infrastructure view

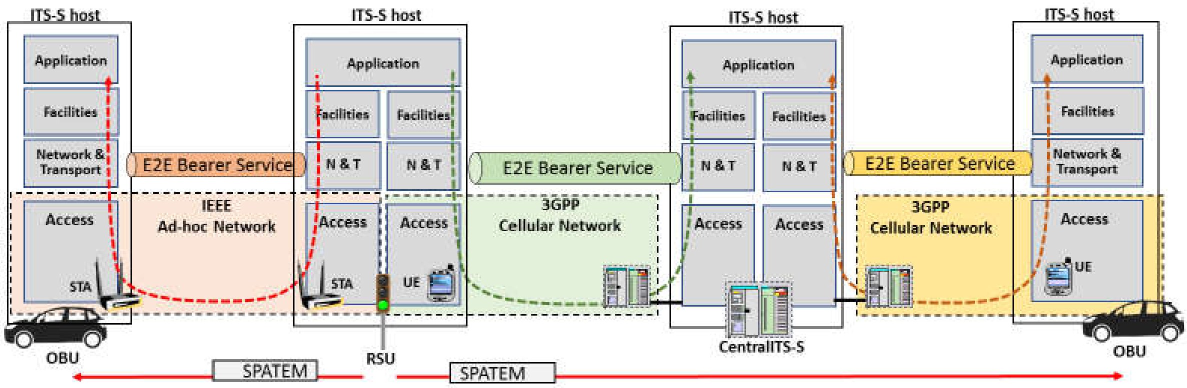

Figure 4: hybrid communication – layered view

Note that in Figure 4 the OBUs represented on the left- and right-hand side may be located within the same vehicle. In this case, an application may receive data via different radio access technologies. The application therefore must be capable to handle data duplication.

3 Cellular Communication

3.1 Cellular Radio Networks

For 5G, two packet core solutions have been specified, called **Standalone (SA)** and **Non-Standalone (NSA) mode**.

5G's Standalone (SA) mode, standardised in 3GPP Rel. 15 (in 2019), uses the 5G packet core and 5G radio access network. It enables 5G network slicing, which is a network architecture where logical networks/partitions are created with appropriate isolation, resources, and optimized topology to serve a purpose or service category or customers.[1] It enables the multiplexing of virtualized and independent logical networks on the same physical network infrastructure. Network Slice as a Service (NSaaS) can be offered by a communication service provider. This enables providers of vehicular services to create a virtual mobile network which meets the QoS requirements of their services.
For real-time data services Ultra-Reliable Low Latency Communication (URLLC) including MEC capabilities can be enabled in SA mode.

Mobile network operators intend to provide radio connectivity with the LTE radio interface and the 5G New Radio (NR) interface. Therefore, 3GPP focused on the Non-Standalone (NSA) mode during the initial 5G specification process (3GPP Rel. 15, in 2018). In the NSA mode, LTE's Evolved Packet Core (EPC) serves both LTE Radio (E-UTRAN) and 5G New Radio (NR).[2] Seven options were studied in [11], section 3.13.

3.1.1 LTE Radio and 5G New Radio

One of the seven options for NSA mode is called Option 3x. In Option 3x, signalling and control information exchange between the UE and the EPC always takes place via the LTE radio access network. 5G's NR access is expected to be rolled out first in hot-spots such as cities, while in less-densely populated areas LTE is expected to remain the dominant radio access technology for the years to come. Using the LTE radio access for signalling simplifies the network operation.
In Option 3x, two types of bearer services are distinguished for user data transmission:

- User data mapped on an LTE bearer is transmitted between the UE and the EPC via the LTE's radio access network. The 5G base station, called gNB, is not involved in the user data transmission.
- User data mapped on a 5G bearer, called New Radio (NR) bearer, is transmitted between the UE and the EPC via the gNB. The data stream between the UE and the gNB may be split: some data is directly sent between UE and gNB via the 5G radio interface; the remaining data is indirectly exchanged between UE and gNB via the LTE's eNB. The data stream split is called Dual Connectivity.

[1] Cited from [10], Introduction;
[2] https://www.3gpp.org/release-15

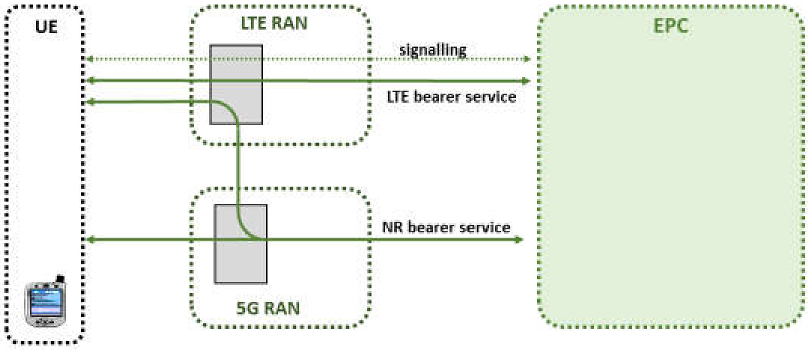

Figure 5: Non-standalone mode Option 3x

Due to the significant investment into the LTE infrastructure, it is expected that the NSA mode will be used by most incumbents in the next years. It enables the 5G NR roll-out, starting in urban hotspots, during which national coverage is provided by LTE. Any edge computing and network slicing solution introduced in in the NSA mode are available for the LTE and the 5G radio access.
For these reasons, the next sections focus on network slicing and edge computing including low latency communication with EPC based on the Non-Standalone (NSA) architecture.

3.1.2 Evolved Packet Core

There are two types of packet data flows in 3GPP cellular networks:

- The control plane carries network management information between cellular network elements. The control plane signalling is used among others for user authentication, service authorization, for establishing, modifying, and releasing resources for the user data transmission, and for user mobility handling.
- The user plane carries the packet data flows of the users.

A cellular communication network is logically divided into a Radio Access Network (RAN) and a and a Core Network (CN):

- The Radio Access Network is called Enhanced UMTS Radio Access Network (E-UTRAN) in LTE and 5G New Radio (5G NR) in 5G.
- The Core Network is called Evolved Packet Core (EPC) in LTE and 5G Core Network (5G CN or 5GC) in 5G.

The EPC deploys following network elements:

- The Serving Gateway (**SGW**) is the gateway which terminates the interface towards E-UTRAN. Its tasks include packet routing and forwarding. At transport level packet marking based on the QoS requirements is supported. Lawful interception and provision of data relevant for charging is supported.
- The Packet Data Network Gateway (**PDN GW** or **PGW**) terminates the interface SGi towards PDNs such as the Internet or corporate networks. Its tasks include per-user-based packet filtering, lawful interception, UE IP address allocation, transport level packet marking based on the QoS requirements, and provisioning of accounting information.
- The Policy and Charging Rules Function (**PCRF**) provides rules for data flow shaping at the PGW. Note that in most figures of this document the PCRF is omitted for simplicity.
- The Home Subscriber Service (**HSS**) stores a user's subscription information.

- The Mobility Management Entity (**MME**) controls network access of each UE based on the user's subscription data provided by the HSS. It authenticates the UE, authorizes its network access and the QoS for its packet data flows. The MME selects the PGW(s) used to relay the UE's packet data flows to external packet data networks (PDNs). In some implementation, the MME may select also the SGW to relay to packet data flows between E-UTRAN and PGW(s). The MME manages handover and supports lawful interception. It manages the tracking area list needed for paging of UEs.

The base stations in 5G NR are called gNBs (next) generation Node Bs), and eNBs (evolved Node Bs) in E-UTRAN. As the EPC is used in the NSA mode for 5G NR and E-UTRAN, a base station in the reminder of the documents will simply be called **Node B** (**NB**).
In case of NSA mode and in case of a standalone LTE cellular network, the NodeBs are connected by means of the S1 interface to the EPC. The S1-interface to the MME carries the control plane messages and is often labelled as S1-MME. The S1-interface to the SGW user data and it typically labelled S1-U.

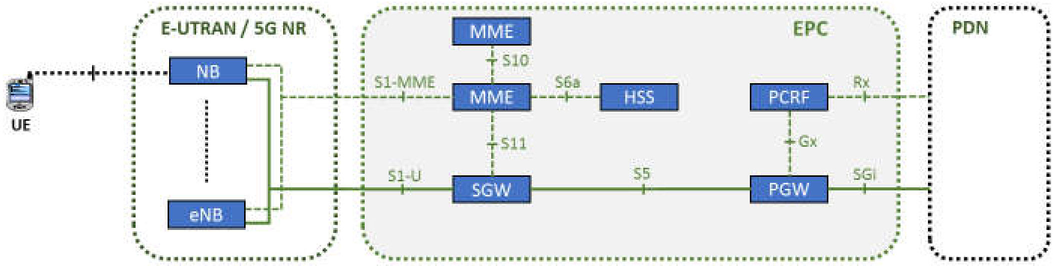

Figure 6: Non-roaming architecture for 3GPP access

In case of roaming, the UE is using the radio access network of a visited Public Land Mobile Network (VPLMN). Depending on the user's subscription profile, inter-operator agreements, the regulatory environment, etc., the UE gets connected to external networks either in its home network (HPLMN) or visited network. In real-life networks, a UE gets connected to PDNs practically always in its HPLMN because of the regulatory demands (legal interception) and because it allows the HPLMN to directly perform data flow shaping and charging information collection at its PGW.

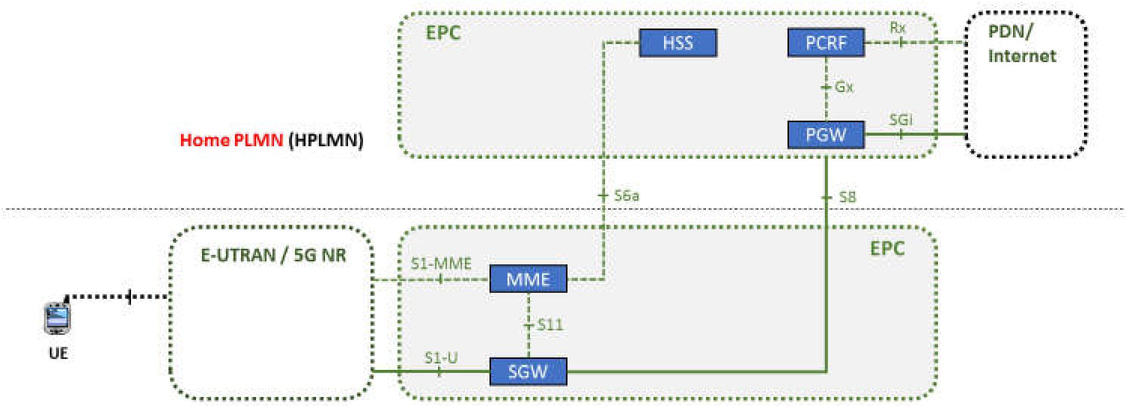

Figure 7: roaming architecture for 3GPP access: home routed traffic

When an end-to-end connection has been successfully established, then an Enhanced Packet Service (EPS) bearer defined between the UE and the PGW provides one link within the end-to-end connection. Within in mobile network, and invisible to the user, the EPS bearer is split into an Enhanced Radio Access Bearer (E-RAB) between UE and SGW, and an S5/S8 bearer service (BS) between SGW and PGW. The E-RAB is composed by a Radio Bearer between UE and eNB and an S1 Bearer between the eNB and the SGW.

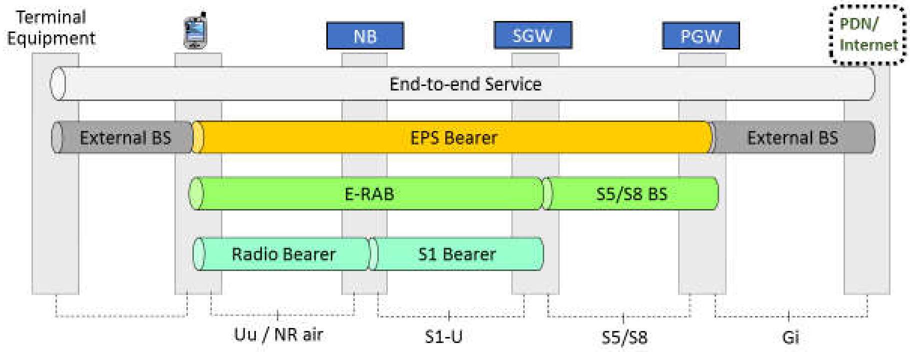

Figure 8: LTE bearer types

3.2 Edge Computing

Multi-Access Edge Computing (MEC) is a technology that provides cloud and IT services within close proximity of mobile subscribers.[3] The different MEC approaches outlined in this document are close to those discussed in [13].

3.2.1 "Bump in the Wire"

The expression "bump in the wire" encompasses all the scenarios in which the MEC platform installation is placed in locations between the base station itself and the mobile core network.[4]

The MEC data plane is placed "on the S1-interface" and is therefore in close proximity to the NodeB or an aggregation point of NodeBs. The MEC server has to process all user traffic, which is carried on S1-U and which encapsulated with an S1-U specific protocol.[5] This requires packet flow filtering to determine the user data which is forwarded to the MEC application, and the insertion of S1-U packets with user data to be sent from the MEC application to the UE. Depending on the transmission network layout, the MEC data plane may also be able to monitor the S1-MME traffic to detect when MEC application eligible users become active or inactive.In this and the following sections, the site in which MEC infrastructure is locally deployed is called **Edge Site.**

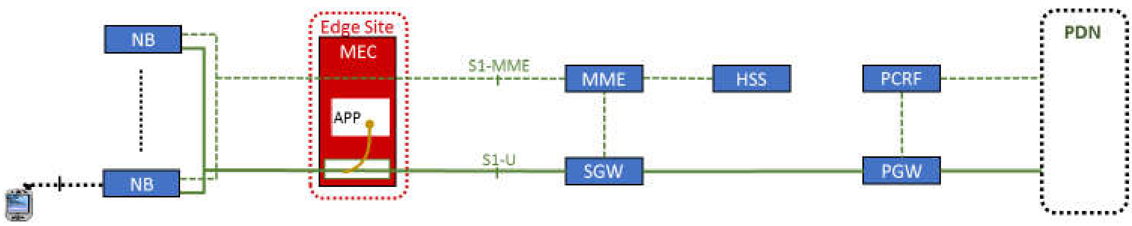

Figure 9: Bump in the wire approach

The key advantage to place the MEC server on the S1-interface is that its operation is transparent to the cellular network, and no modification of the cellular network infrastructure or its configuration is required. Localised services can be easily provided with very low latency, well suited for real-time data processing.

[3] Cited from [17].
[4] Cited from [13].
[5] The GTP-u is the transport protocol used between NB and SGW. It carries as payload the user data.

While technical easy to realise, there is a set of problems associated with this scenario:

- Legal interception interfaces in the LTE network are defined for the MME, SGW, and PGW. The MEC infrastructure therefore must provide interfaces for legal interception compliant with national law.
- The MEC data platform performs deep packet inspection of all data streams passing the S1 interface to filter the data which needs to be forwarded to the MEC application. This increases the risk of privacy violation, as the MEC server has access to all user data. For integrity and privacy protection, most mobile network operators therefore apply IPsec on the S1-interface. To still be able to inspect the S1 data flow, the MEC server must either be placed outside the IPsec gateways, where the user data flow is still unprotected, or it must become an IPsec endpoint along the S1-interface.
- Charging and network policy enforcement is controlled by the MME, SGW and PGW. These network entities have no information about the amount of data sent between the UE and the MEC application. The MEC application could overload a cell's capacity, while the MME being responsible for access and overload control is forced to limit the throughput and access for non-MEC application users.
- Cellular networks are typically hardened with firewalls against malicious attracts. A MEC servers may be connected to the Internet, e.g. for maintenance reasons or to exchange data with other MEC servers. If the MEC server's Internet access is not properly protected, it increases the risk of malicious intrusion into the mobile operator's network.

In mobile test networks, the "bump in the wire" approach provides mobile edge services rather effortless. However, in a commercial environment with strict obligations with respect to privacy, security, and data integrity, the "bump in the wire" approach shows too many vulnerabilities to be further considered as solution within ITC4CART.

3.2.2 Distributed Gateways

A cellular network is hierarchically organized, as indicated in Figure 10. A set of regional NodeBs are connected to an SGW. A set of SGWs in one region is typically linked to a local PGW, which serves as breakout point to the Internet. The number of PGWs in mobile network is normally quite small.

A MEC server can be directly connected to a PGW via the SGi-interface. This avoids additional latency in comparison to its deployment in the Internet. This solution comes with almost no deployment costs for a mobile operator, and allows a fast, cost-efficient, national-wide provision of a MEC service.

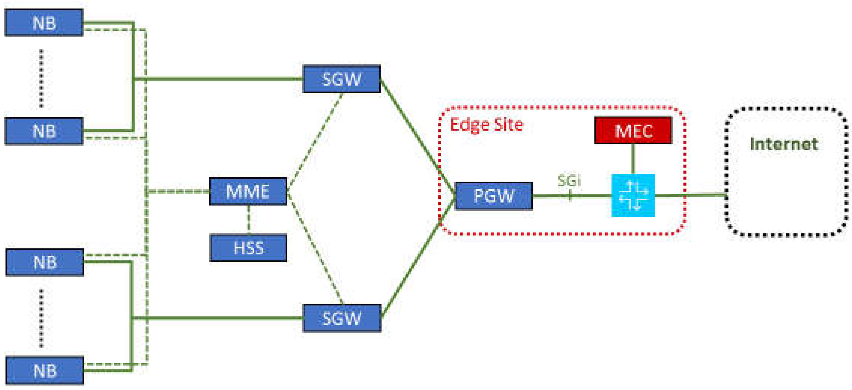

Figure 10: Example of an Edge Site at the edge of a cellular core network

The MEC service can be regionalised: A MEC service can be provided on a set of MEC servers, each of which is connected to a PGWs of the MNO. The MEC service running on a MEC server can be adapted to an area covered of NodeBs geographically close to the PGW to which the MEC server is connected to.

Regionalisation can be intensified by moving the MEC server to an SGW location. This reduces the number of hops between the UE and the MEC server and thus the latency. If a local MEC service has special requirements in terms of latency, reliability, bandwidth, etc., then infrastructure investments to meet these requirements affect only the SGW, the NodeBs geographically close to the SGW, and their transmission network.
The MEC server is still connected via the SGi-interface to the cellular core network. Therefore, also a PGW function must be deployed at the SGW site.

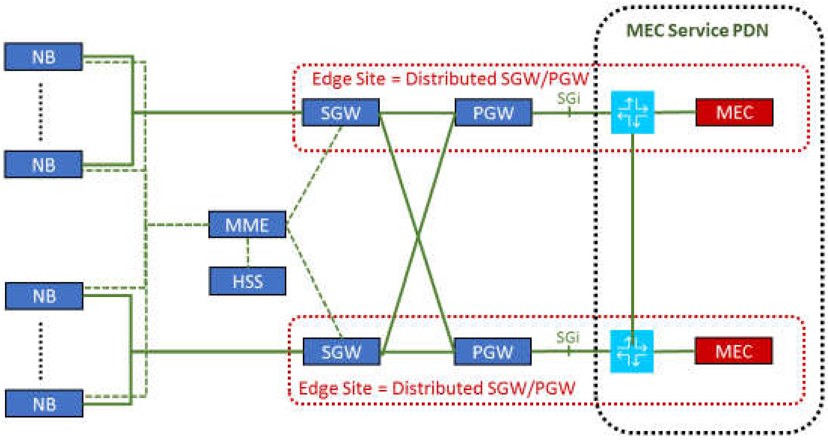

Figure 11: Example of Edge Sites at the SGW location

Figure 11 shows two MEC servers deployed at two SGW sites. Note that in a network deployment, other PGWs may exist, which for instance provide connectivity to the Internet.

The MEC servers at an Edge Site can be part of a MEC service infrastructure, and together they form a **MEC Service PDN**.

3.2.3 Distributed Evolved Packet Core

In a Distributed EPC, an Edge Site hosts all network functions of an EPC, i.e. the HSS, MME, SGW, and PGW, as well as the MEC server. The MEC server is located next to the PGW on the SGi-interface.

Each Edge Site is connected to a set of NBs and can directly provide services to a UE in the coverage area of the NodeBs, as described in section 3.2.2. All EPC functions are located in the Edge Site, all capabilities of a cellular network are available, including handover management, session management, flow control, changing, etc. An HSS located in the Edge Node avoids the need of a backhaul to a remote HSS. The local HSS also benefits a fast PDN connection establishment and thus a very fast service readiness. It also allows the Edge Site manager to more independently manage the subscriber base. Some Edge Sites may share an HSS, which is then deployed in one of the sites.

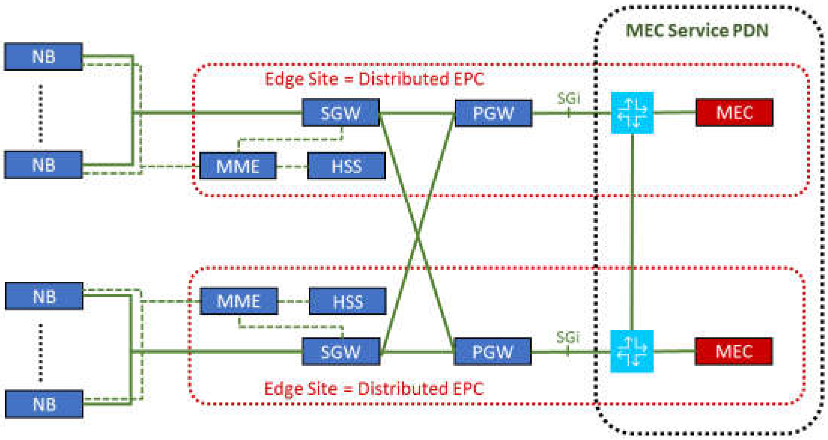

Figure 12: Example of two Distributed EPCs for one MEC Service

3.2.4 Distributed Network Function Virtualisation

In all Edge Sites, the HSS, MME, SGW, PGW, router, PCRF, and MEC services can be deployed on stand-alone hosts or cloud IT infrastructure. Some or all functions can as well be virtualized and operated on the same Network Function Virtualization (NFV) platform. This applies wherever Edge Sites are used.

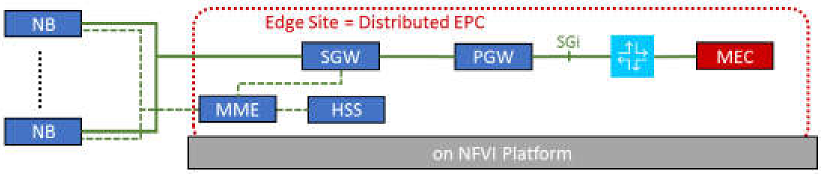

Figure 13: Example of EPC functions and MEC server on one NFV platform

Localised services with very low latency can be easily and cost-efficiently provided.

3.2.5 Distributed Edge Sites and Tromboning

The MME uses a **PGW selection function** to select the PGW during the PDN connection establishment. The PGW selection method is not specified in 3GPP standards. In 3GPP Rel. 10 (2012), the optional feature Selected IP Traffic Offload over Radio Access Network (SIPTO over RAN) was introduced. It allows the selection of a PGW that is geographically close to a UE's point of attachment. Hereby the PGW selection function uses the UE's current location information, i.e. the NB id and/or Tracking Area id.

As result of the UE mobility the NodeBs and SGWs serving the UE change, however the PGW as anchor to the PDN–remains unchanged.

During UE mobility, the MEC server changes with the UE location, therefore the MEC server and the anchor PGW are no longer co-located. This is the so-called tromboning and leads to additional latency.

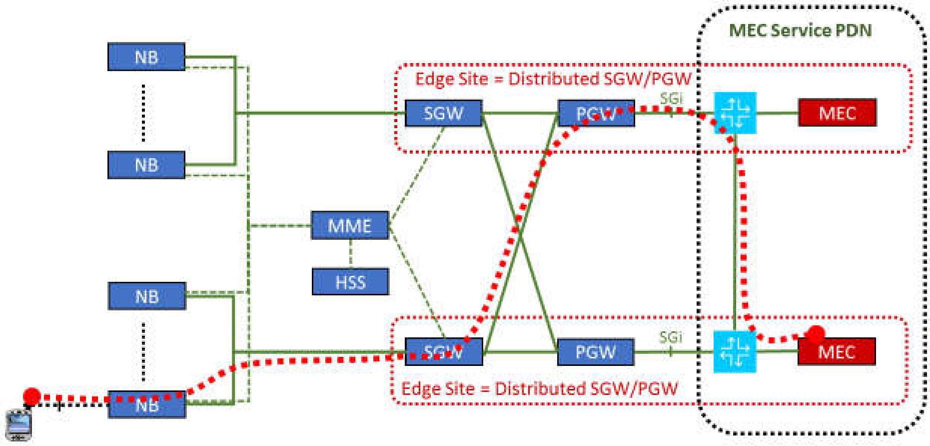

Figure 14: Example of tromboning with Distributed GWs

Either the MME or the UE has to terminate the connection to the PDN to enforces the release of the anchor PGW. The UE re-establishes once again the connection to the PDN during which the MME selects a new anchor PGW next to the geographically local MEC server, for instance by the use of SIPTO.

3.3 Network Slicing

An application client is typically installed at the mobile phone's side and an application server infrastructure in a Packet Data Network (PDN). A cellular network provides connectivity for data exchange between a UE and a PDN. The connectivity for data exchange between a UE and a PDN is characterised by a range of performance indicators, such as latency, reliability, guaranteed throughput rates, maximum throughput rates, and so on.

A PLMN network can be explicitly created with appropriate isolation, resources, and topology adapted to the application requirements. This is in general prohibitive expensive for any service provider with a specialised or small target group.

Network slicing allows independent deployment of Edge Computing, isolated from the remaining network infrastructure of a mobile network operator. The network slice for Edge Computing can be deployed both on a regional and a national scale.

Features are available which allow some degree of network slicing in LTE [14][15][16]. The features MOCN and MORAN are used for radio access network sharing and are discussed in section 3.3.1. The features DECOR and eDECOR allow the creation of basic network slices and are outlined in section 3.3.2. PDN selection based on APNs is a standard method to determine the PGW which provides connectivity to the chosen service provider, and this is discussed in section 3.3.3.

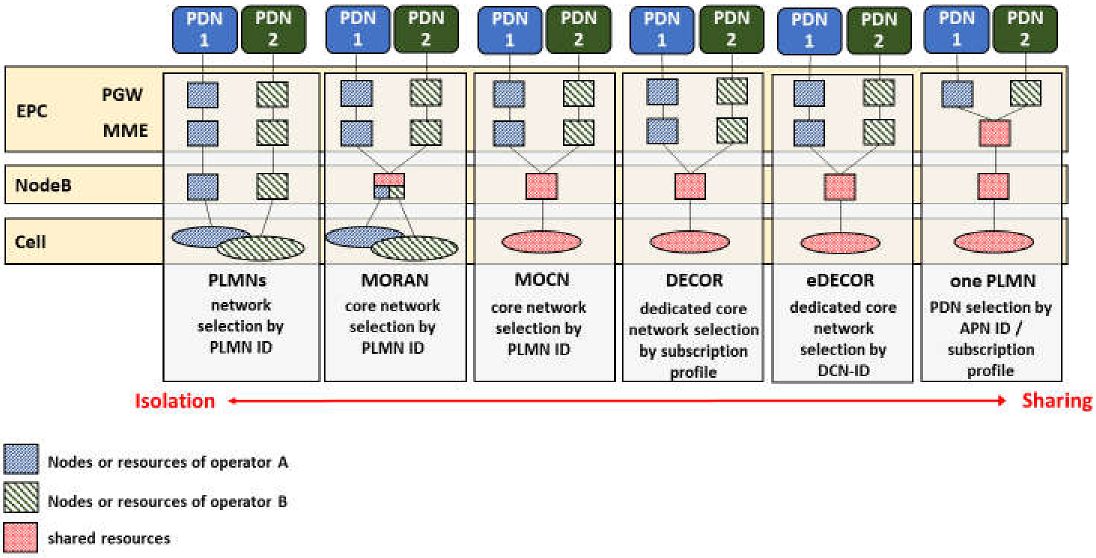

Figure 15: A selection of LTE network slicing options

An overview of selected features for network slicing in LTE is shown in Figure 15.

3.3.1 Multi-Operator Core Network

An EPC holds all cellular network functions: HSS, MME, SGW, PGW, and PCRF. The deployment of the HSS allows the EPC owner to control its subscribers directly. The MME allows the setting of the QoS for the packet data connection of the UEs. The SGW provides connectivity to selected NodeBs, and the PGW the connectivity to PDNs including the Internet.
Vehicular services can be provided on the IT and cloud infrastructure in a PDN. If a vehicular service provider operates an EPC, then it is as a mobile network operator (MNO). An MNO can deploy its EPC infrastructure with respect to quality of service, redundancy and reliability according to its needs.

Figure 16 shows each cellular network function once per EPC. In an operational network, there can be multiple network element per network function. For instance, there can be multiple, geographically distributed PGWs providing connectivity to PDNs.

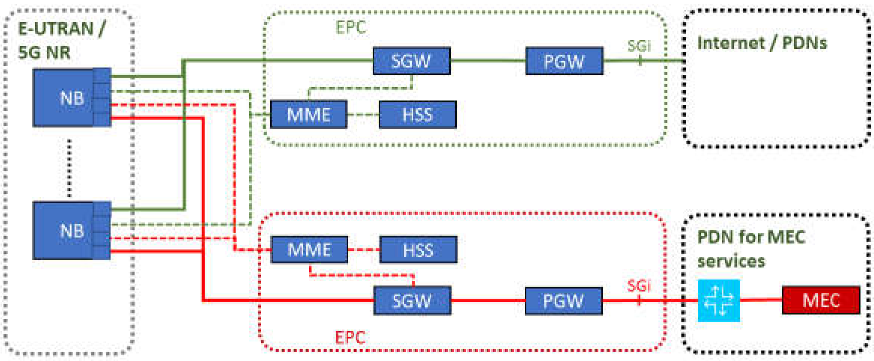

Figure 16: Example of MOCN/MORAN with two operators

An EPC operator may also operate its dedicated Radio Access Network (RAN), or it may share the Radio Access Network with other EPCs:

- In case of the LTE network sharing solutions **MOCN** (Multi-Operator Core Network) multiple EPCs are connected to a common Radio Access Network and share NodeBs, including the radio resources.

- In case of the LTE network sharing solutions **MORAN** (Multi-Operator Radio Access Network) multiple EPCs are connected to a common Radio Access Network and share NodeBs, but own dedicated radio resources.

The connection of multiple EPCs to a single NodeB via dedicated S1 interfaces is a basic feature called S1-flex, originally introduced for load balancing.

Because the radio access network is shared, a mechanism has to be provided to select an EPC. This is based on PLMN IDs for MOCN and MORAN**.** A Public Land Mobile Network (PLMN) ID identifies a mobile network operator. In each cell of a radio access network, basic information is continuously broadcasted, including the PLMN identifiers of the EPCs sharing the radio access network. The UE selects during the connection establishment an appropriate PLMN corresponding to the information stored on the Subscriber Identity Module (SIM).

One problem of EPC slices based PLMNs is that the available PLMN ID number space is very limited, and its allocation requires the permission of national regulation authorities. Therefore, this approach is only applicable for a limited number of service providers. Another problem is that a UE can only connected to one PLMN at a time.

3.3.2 Dedicated Core Network

In the 3GPP Rel. 13 (2016) feature Dedicated Core Network (DECOR), the network slice is called Dedicated Core Network (DCN). A DCN comprises of one or more MME and it may comprise of one or more SGW, PGW, and PCRF.[6] Similar to Multiple Operation Core Networks (MOCN) described in the previous section, multiple Dedicated Core Networks share a common radio access network based on S1-flex architecture.

Because the radio access network is shared, a mechanism has to be provided to select a DCN. In DECOR, a dedicated network is selected based on the users' subscription profile. The subscription profile of a user in the HSS lists PDNs, identified by their respective APNs, to which the user can be connected to. Per APN, the QoS requirements are provided, and optionally a "UE Usage Type", which identifies the network slice which has to be used. DECOR thus allows the introduction of a service-based network slice selection, designed to meet the needs of the user and its services.

The UE is unaware that DECOR is used. Therefore, a redirection between DCNs cannot be avoided as the UE may initially get attached to the wrong DCN. The HSS now plays a vital role, as it provides the MME in the DCN with the parameter "UE Usage Type", which is used by the MME to tell the NodeB to redirect the UE's Attach Request to the desired DCN.

The LTE Rel. 14 (2017) feature enhanced Dedicated Core Network (eDECOR) is an optimised version of DECOR, in which the UE provides a DCI identity to assist the NodeB in its task to directly select the desired DCN, thus reducing the call setup time. This is very similar to MOCN, where the PLMN ID is provided by the UE and used by the NodeB to determine the EPC. Unfortunately, only UEs from 3GPP Rel. 14 (2017) and later releases may support eDECOR, which represents a big challenge for eDECOR to become a widely used feature.

[6] [12], section 4.3.25.1.

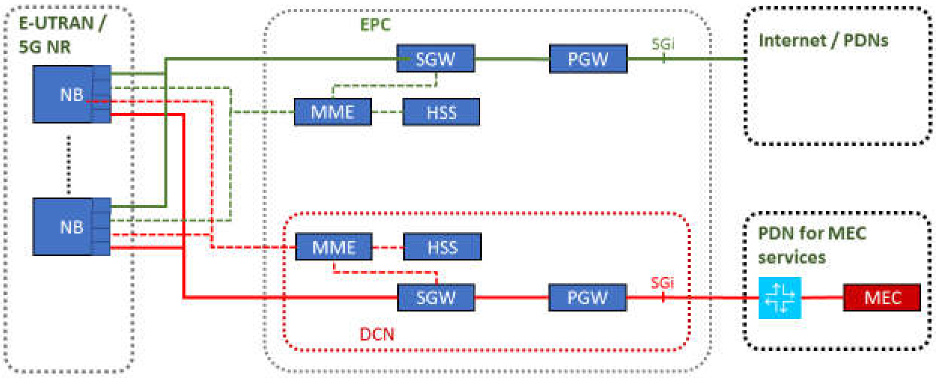

Figure 17: Example of a DCN within an EPC

The HSS function and thus the subscriber management falls into the responsibility of the MNO. There are no restrictions though to distribute the HSS on multiple platform. An MNO there can enable the operator of the slice to manage its subscriber base and runits HSS. This allows the slice operator to set to QoS parameters in the HSS according to the needs of its subscribers, as long as the QoS settings are in accordance with the agreement with the MNO.
A problem is that a UE can only be connected to one DCN at a time, like MOCN described in the previous section.

3.3.3 APN based PDN selection

Vehicular services can be provided on the IT and cloud infrastructure in a PDN. A PDN is typically identified with an Access Point Name (APN)[7]. Given the APN, a mobile network operator selects a PGW which provides a connection to the desired PDN. The PGW selection is outlined in section 3.2.2 and belongs to the standard capabilities of a mobile network. The existing MNO's infrastructure can be used. This also means that the availability, reliability and redundancy depend on the infrastructure provided by the MNO. An MNO may e.g. improve the latency be adding new SGWs and PGWs geographically closer to a UE's point of attachment and connect the PDN to the newly added PGWs.

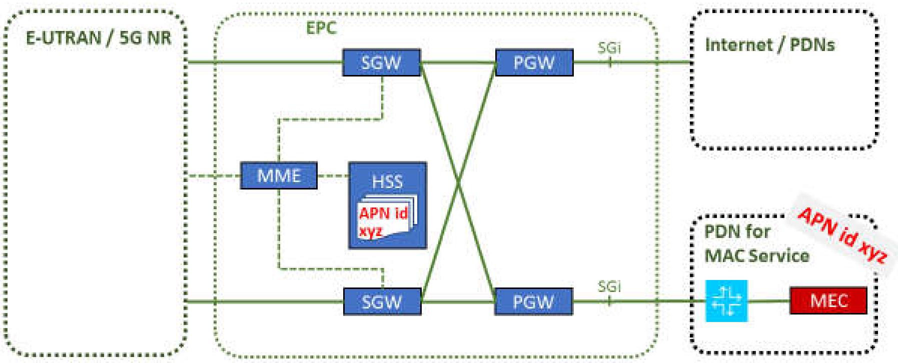

Figure 18: Example of a PDN being accessible via a (dedicated) PGW

The APN based PDN selection allows a UE to be connected to multiple APNs. Because the Core

[7] Several APNs may be e.g. used to identify different applications hosted within a PDN. An PDN may also be identified by a so-called PDN GW identifier, if the PDN is the only external network connected to PGWs identified with this identifier. A PGW IP address may be used as well, if the PDN is connected to one PGW.

Network is shared a potential service provider has no access to dedicated resources.

3.3.4 Network Slices with Multiple Operators

Mobile network operators can coordinate their slices, which enables connectivity to the same MEC service. This can be done on a regional and/or national level. An example is provided in the figure below.

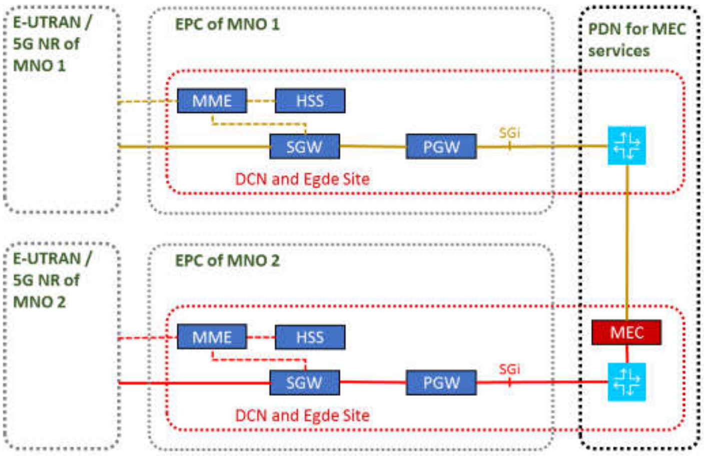

Figure 19: Example of Network Slicing (here DCN) and Edge Computing combined

4 Hybrid Connectivity Requirements

Hybrid connectivity allows an ITS Station to use more than one radio access technology to provide or use vehicular services. Multiple access technologies can be applied in an OBU, which then decides which access technology to use. A MEC service deployed e.g. in an RSU can also use multi access technologies. In this case, it can provide its service to OBUs in vehicles which either have LTE/5G or ITS-G5 in implemented.

The purpose of this chapter is to provide a summary of the requirements pertaining to the Hybrid Connectivity environment. These are a subset of the ICT4CART architecture requirements identified in the project deliverable D2.3. D2.3 covers all the system requirements related to hybrid connectivity, the IT environment (data flows, management and analytics), and cyber-security and data privacy.

The goal of the ICT4CART hybrid connectivity is to ensure a flexible, reliable data with low transmission latency according to the use case requirements. A hybrid communication system must connect vehicles, road infrastructure and other devices with service platforms, whereby each entity may support one or several access technologies.

4.1 Functional Requirements

A summary of the functional requirements pertaining to the hybrid connectivity environment, as identified in D2.3, is provided in Table 1.

- R-HY-1: ITS hybrid communication support is supported by the allowing the use of multiple access systems, including ITS-G5 and LTE/5G, see section 2.3.
- R-HY-2: ITS-G5 support is given, and its capabilities and restrictions are outlined in section 2.2.
- R-HY-3: Cellular communications support is provided; its capabilities and restrictions are outlined in section 2.1.
- R-HY-4: Concurrent access network use, i.e. the ability of a network device such as an OBU to use multiple access technologies, should be supported (see section 2.3).
- R-HY-5: QoS determination depends on the used communication systems. In LTE/5G, it depends on the (existing) network layout and the extent to which network virtualisations can be realised, as outlined in section 2.3.
- R-HY-6: Seamless Service Continuity depends on the radio technologies. In LTE/5G, seamless service continuation is inherently inbuilt by its ability to handover a UE from one cell to the next. Inter-operator handover depends on national and international roaming agreements between operators.
- R-HY-7: Network Slicing is an inbuilt feature in 5G, as described in section 3.1. For LTE, variants of network slicing exist, as described in section 3.3, whose deployment depends on MNOs' network capabilities.
- R-HY-9: Deployment strategies of MEC in section 3.2.
- R-HY-8: Geofencing is supported in LTE/5G by providing infrastructure, e.g. as IT and cloud infrastructure as part of MEC, and by providing connectivity via the SGi-interface to the infrastructure.

Table 1 – Functional Requirements Pertaining to the Hybrid Connectivity Environment.

ID	Name	Description	Scope	Priority
R-HY-1	ITS hybrid communication support	A hybrid ITS communication system shall be capable of accommodating a variety of different access systems thus providing a multi-access system environment to ITS Station users.		1
R-HY-2	ITS-G5 support	A hybrid ITS communication system shall be capable of accommodating the ad-hoc wireless solution ITS-G5.		1
R-HY-3	Cellular communications support	A hybrid ITS communication system shall be capable of accommodating cellular communication systems, such as LTE or 5G.		1
R-HY-4	Concurrent access network use	ITS-S host concurrently using different access system (e.g. ITS-G5 and LTE) shall be supported.		1
R-HY-5	QoS determination	A hybrid ITS communication system shall provide an ITS-S application/facility with transport QoS of the available and used access technologies.		1
R-HY-6	Seamless Service Continuity	The user experience shall be as far as possible unaffected by the change of an access service provider and/or a radio access technology (RAT).		1
R-HY-7	Network Slicing	A cellular network in a hybrid ITS communication system shall support network virtualization that allows multiple networks to run on top of a shared physical radio network infrastructure. It shall be possible to isolate specific services within a dedicated logical network with the appropriate QoS.		
R-HY-8	Geofencing	A hybrid ITS communication system shall be able to provide infrastructure for an ITS-S application (e.g. ITS-S router or ITS-S host) to control the area and the size of the area in which ITS data is being distributed, e.g.		1

		to local ITS stations such as vehicle ITS		
R-HY-9	MEC	A hybrid ITS communication system shall be able to provide infrastructure for the distribution of time-critical messages to ITS-S hosts within a small-scale geographical area. Cellular access networks shall support this using multi-access edge commuting (MEC).		1

5 References

[1] ETSI EN 302 665, Intelligent Transport Systems (ITS); Communications Architecture

[2] ETSI EN 302 637-2, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service

[3] ETSI EN 302 637-3, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Environmental Notification Basic Service

[4] ISO TS 19091, Intelligent Transport Systems – Cooperative ITS – Using V2I and I2V communications for applications related to signalized intersections

[5] ETSI EN 302 636-4-1, Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality

[6] ETSI EN 302 636-4-1, Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 2: Media-dependent functionalities for ITS-G5

[7] IEEE 802.11-2016 - IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

[8] IEEE 802.11p-2010 - IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments

[9] ETSI TS 103 301, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services

[10] 3GPP TS 28.530, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Management and orchestration; Concepts, use cases and requirements

[11] 3GPP TR 38.912, 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Study on New Radio (NR) access technology

[12] 3GPP TS 23.401, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access

[13] ETSI White Paper No. 24, MEC Deployments in 4G and Evolution Towards 5G, First edition – February 2018, by Fabio Giust, Gianluca Verin, Kiril Antevski, Joey Chou, Yonggang Fang, Walter Featherstone, Francisco Fontes, Danny Frydman, Alice Li, Antonio Manzalini, Debashish Purkayastha, Dario Sabella, Christof Wehner, Kuo-Wei Wen, Zheng Zhou, ISBN No. 979-10-92620-18-4

[14] 3GPP TS 23.236, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Intra-domain connection of Radio Access Network (RAN) nodes to multiple Core Network (CN) nodes, 3GPP TS 23.251, Technical Specification Group Services and System Aspects; Network Sharing; Architecture and functional description

[15] 3GPP TS 23.251, Technical Specification Group Services and System Aspects; Network Sharing; Architecture and functional description

[16] 3GPP TR 23.711, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Enhancements of Dedicated Core Networks selection mechanism

[17] Ahmed, Arif; Ahmed, Ejaz. A Survey on Mobile Edge Computing. India: 10th IEEE International Conference on Intelligent Systems and Control (ISCO'16), India.