5GAA webinar

Global MEC technology to support automotive services

April 4th, 2023

Moderator: Maxime Flament (5GAA CTO)
Presenters: Dario Sabella (Intel), Jyoti Sharma (Verizon), Jonathan Borrill (Anritsu), Antonio Consoli (Huawei)

Agenda

- Introduction
- MEC4AUTO approach: architecture, technical challenges
- Overview of MEC Federation Trials
- MEC interoperability Scenarios
- Edge Predictive Analytics in Multi-Operator scenarios
- MEC security: threats and mitigation strategies
- Q&A

Title: **Global MEC technology to support automotive services**

Abstract: *The 5GAA approach to MEC (Multi-access Edge Computing) technology for automotive services follows car industry needs to consider multi-operator, multiple car maker, and multi-vendor scenarios. In order to support for Global MEC deployments, 5GAA started working on this area by targeting live trials to easily demonstrate MEC applications and use cases in those scenarios of interest (MEC4AUTO architecture). This webinar will provide a comprehensive overview of the many activities in this field, including architectural enhancements inspired by the live trial implementation with 5G networks, interoperability aspects, business market analysis, but also the usage of edge predictive analytics, network slicing and also cybersecurity aspects for the targeted scenarios.*

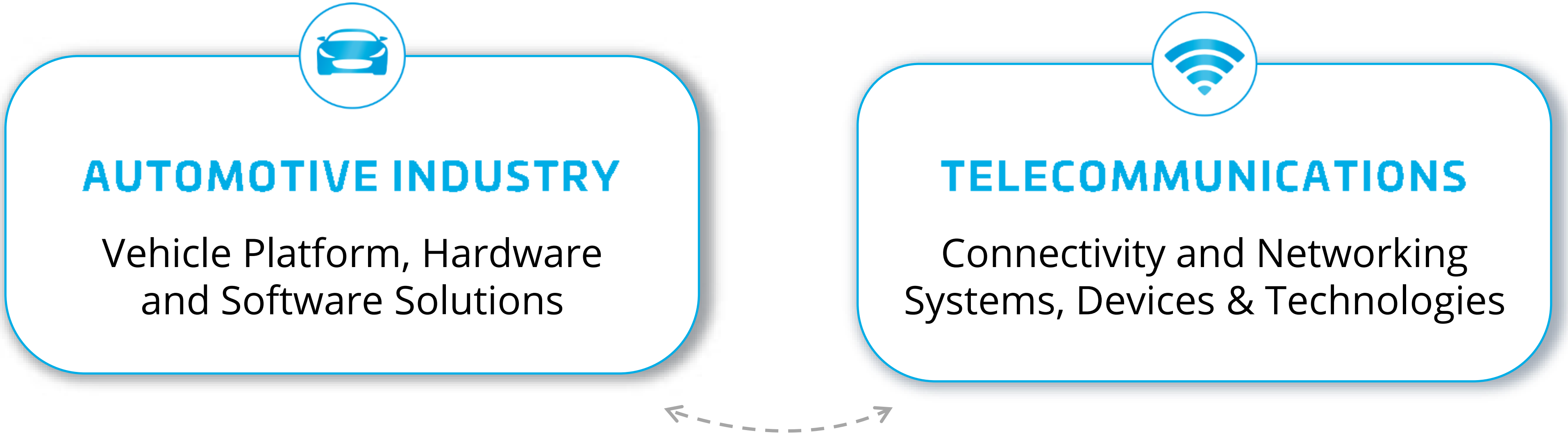
5GAA
Automotive Association

5G Automotive Association, pioneering digital transformation in the automotive industry

Learn more at WWW.5GAA.ORG

Connected mobility for people, vehicles and transport infrastructure

5GAA bridges the automotive and telecommunication industries in order to address society's connected mobility needs bringing inclusive access to smarter, safer and environmentally sustainable services and solutions, integrated into intelligent road transportation and traffic management.



AUTOMOTIVE INDUSTRY

Vehicle Platform, Hardware and Software Solutions

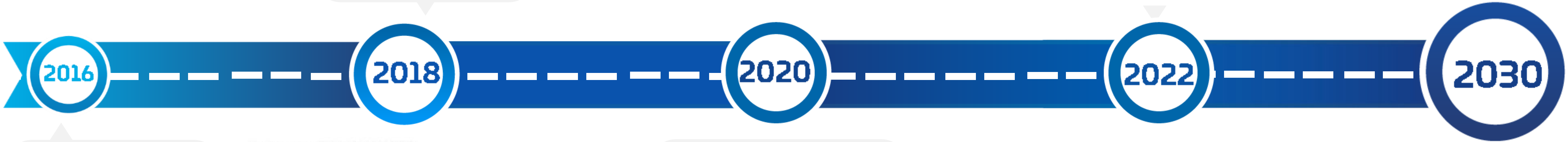
TELECOMMUNICATIONS

Connectivity and Networking Systems, Devices & Technologies

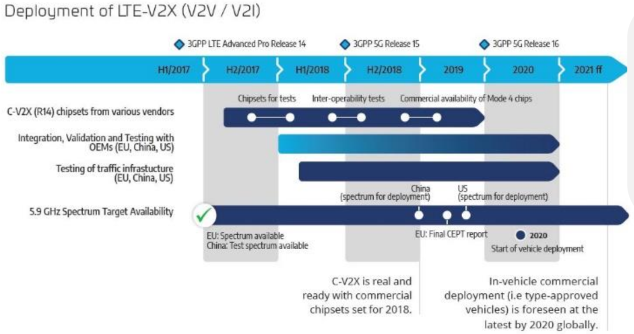
5GAA deployment objective

LTE-V2X 2020 Roadmap

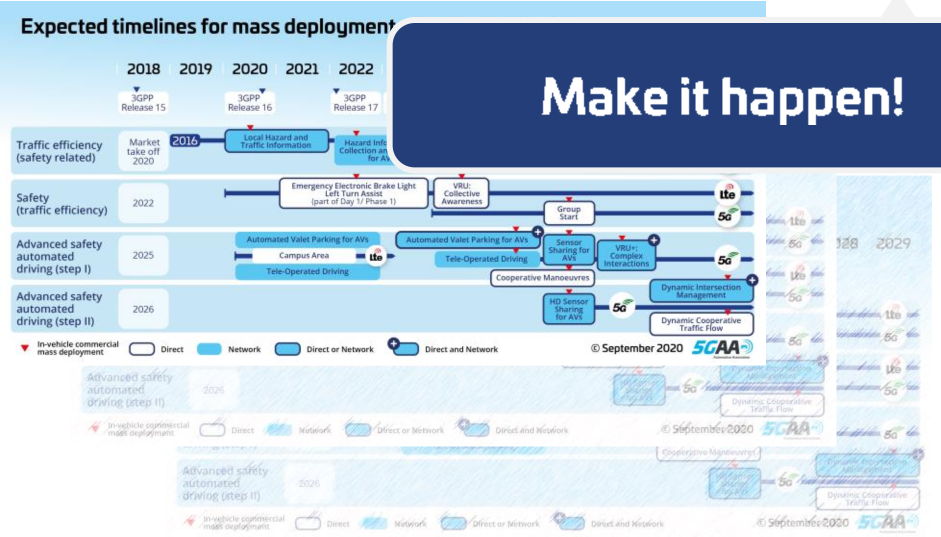
- Make an impact onto the ecosystem
- Work and contribute to the evolution of the roadmaps and their implementation
- Remove roadblocks on the way to deployment



5GAA Foundation



2030 Roadmap including 5G-V2X



Make it happen!

Live Survey

Poll#1
(Questions Q1 and Q2)

MEC4AUTO approach

architecture, technical challenges

Automated and Connected cars – key drivers

- Connected Car Vision
  - Cloud V2X services
  - Over the air updates
  - Infotainment / media delivery
  - Intelligent route and path planning
  - Tracking / fleet management
  - Transportation as a service
- Inter-Car Communication
  - Cars talk to another cars, pedestrians, road-side units
  - Road safety
  - Telematics information exchange
  - Environment perception
  - Cooperative & automated driving

MEC is a key technology for many of these drivers

Transportation-as-a-service
AI
Over-the-air updates
SAFETY AND SECURITY
Vehicle-to-everything (V2X) (V2V, V2I, V2N)
Environment modeling
Voice controls
Responsive HMI
Path planning
HD video and entertainment
Perception

5GAA

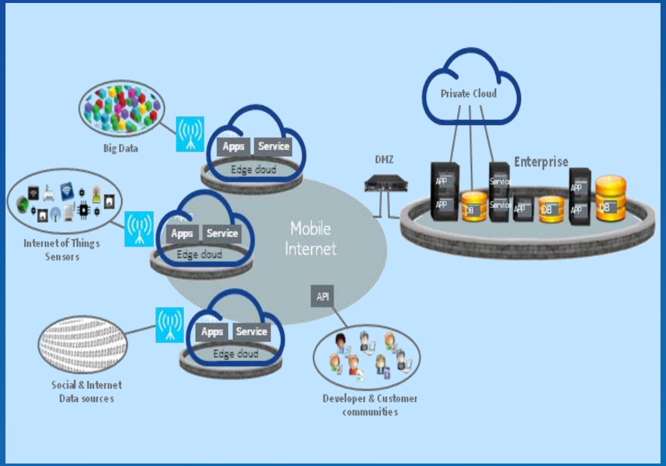
Toward fully connected vehicles: Edge computing for advanced automotive communications

White Paper

Suggested reading: 5GAA White Paper on Edge Computing
http://5gaa.org/wp-content/uploads/2017/12/5GAA_T-170219-whitepaper-EdgeComputing_5GAA.pdf

What is MEC ?

- Multi-Access Edge Computing (MEC)
is a key technology offering cloud computing capabilities and an IT service environment at the edge of the network.


Big Data
Apps
Service
Edge cloud
Internet of Things Sensors
Mobile Internet
Social & Internet Data sources
Private Cloud
DMZ
Enterprise
APP
Service
DB
API
Developer & Customer communities

Cloud-computing at the network edge.

- Proximity
- Ultra-low latency
- High bandwidth
- Real-time access to access network and context information
- Location awareness

ETSI MEC is pioneering open standards for Edge Computing

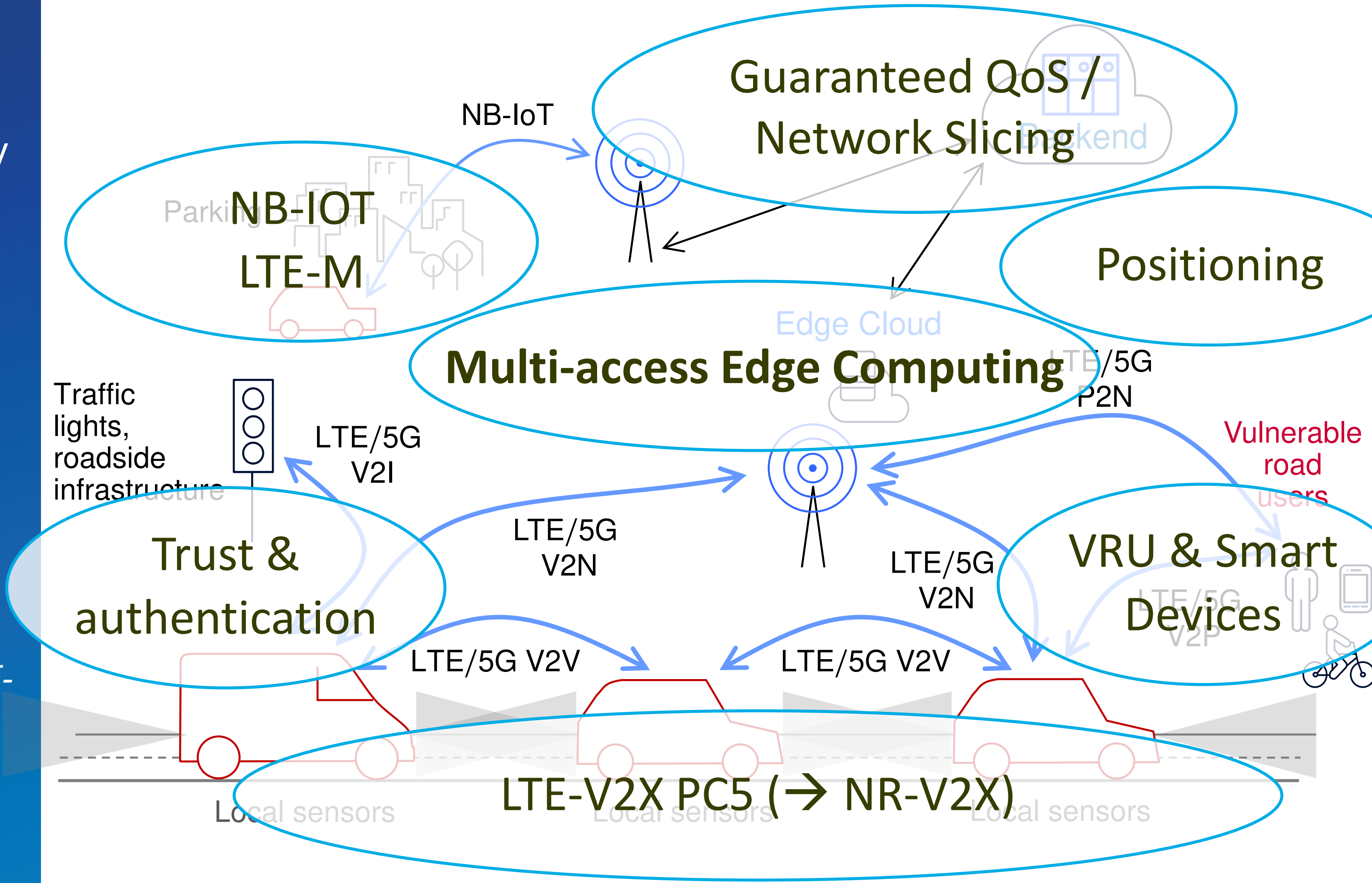
[figure: Continental AG]

C-V2X is a unified technology platform which integrates:

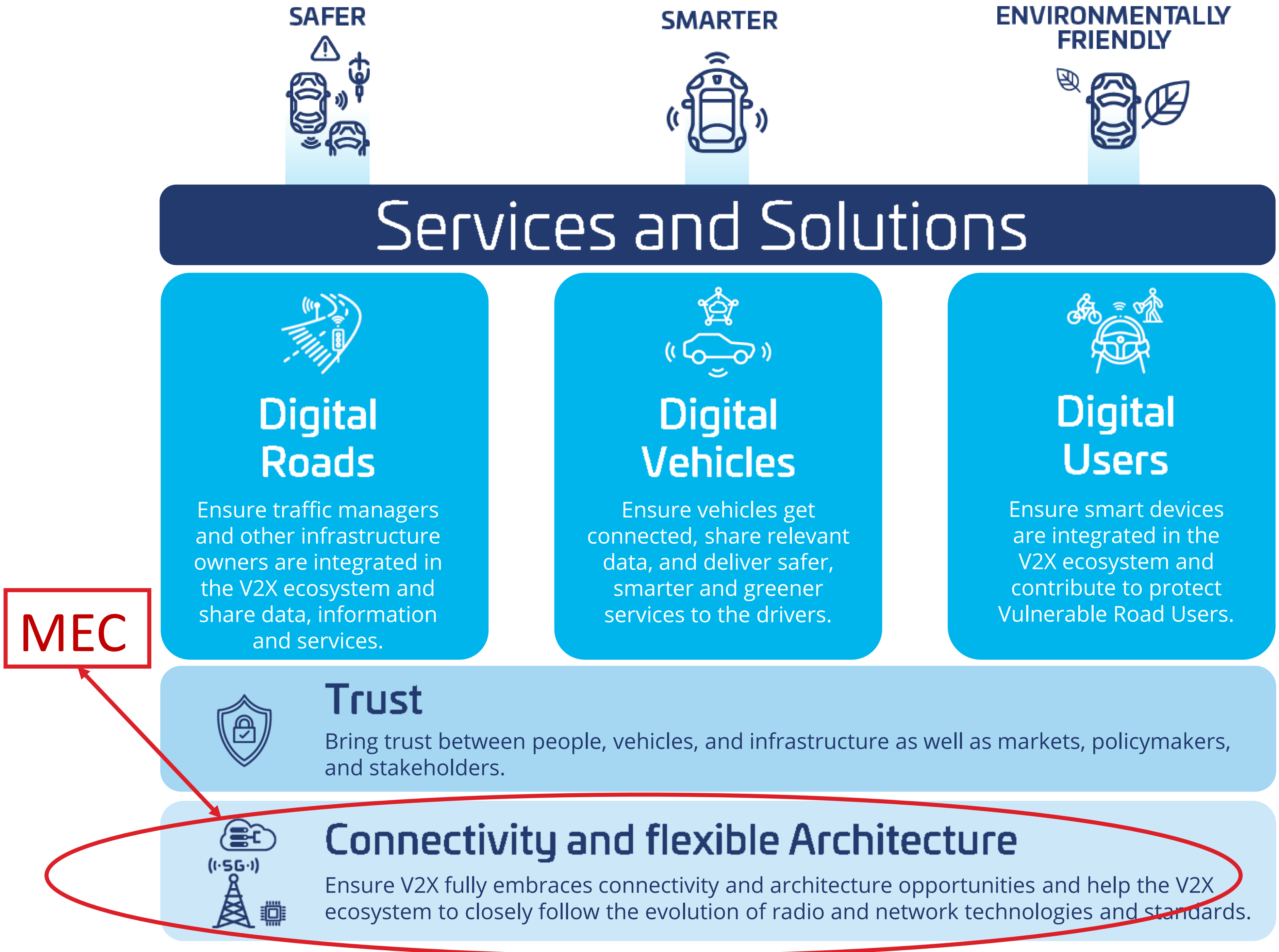
- C-V2X* direct communications mode (or “C-V2X PC5”)
- C-V2X* mobile network communications (or “C-V2X Uu”)

**(C-V2X can be substituted by LTE-V2X, 5G-V2X as appropriate)*

Automotive Connectivity Landscape



5GAA strategic objectives and priority areas



SAFER

SMARTER

ENVIRONMENTALLY FRIENDLY

Services and Solutions

Digital Roads

Ensure traffic managers and other infrastructure owners are integrated in the V2X ecosystem and share data, information and services.

Digital Vehicles

Ensure vehicles get connected, share relevant data, and deliver safer, smarter and greener services to the drivers.

Digital Users

Ensure smart devices are integrated in the V2X ecosystem and contribute to protect Vulnerable Road Users.

Trust

Bring trust between people, vehicles, and infrastructure as well as markets, policymakers, and stakeholders.

Connectivity and flexible Architecture

Ensure V2X fully embraces connectivity and architecture opportunities and help the V2X ecosystem to closely follow the evolution of radio and network technologies and standards.

MEC

The 5GAA path toward Global MEC deployments…

2017

5GAA white paper

“Toward fully connected vehicles: Edge computing for advanced automotive communications”

5GAA

Toward fully connected vehicles: Edge computing for advanced automotive communications

White Paper

https://5gaa.org/content/uploads/2017/12/5GAA_T-170219-whitepaper-EdgeComputing_5GAA.pdf

2018

5GAA Open Workshop on “Edge Computing and V2X”

February 8th, 2018, Munich (Germany)

On 8th February 2018, the 5G Automotive Association lead a successful Open Workshop on “Edge Computing and V2X“.
The workshop – open to both 5GAA members and non-members – aimed to provide a discussion platform for the wide range of stakeholder advocating for the evolution of cloud computing in the automotive sector.

https://5gaa.org/c-v2x-edge-computing-the-winning-technologies-for-connected-vehicles-and-autonomous-driving/

2019

MEC4AUTO work item (completed)

MEC4AUTO (2019-2020) has established the foundation of MEC activities in 5GAA

MEC4AUTO technical report “MEC for Automotive in Multi-Operator Scenarios”

MEC4AUTO technical report “MEC Use Cases and initial test specifications review”

2021

gMEC4AUTO work item (completed)

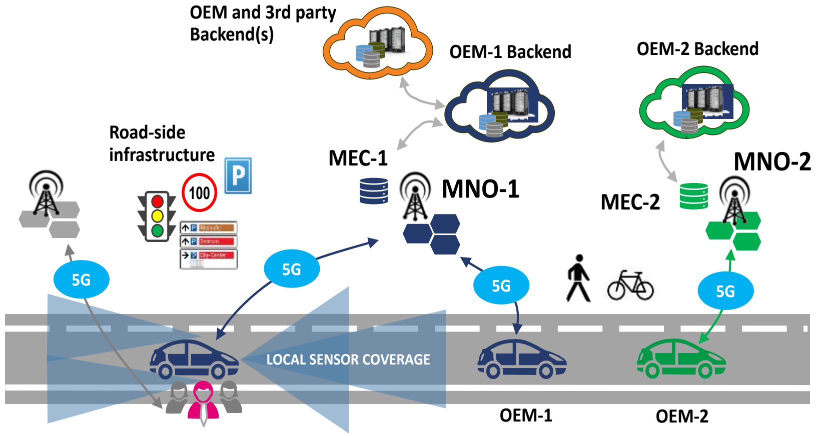
gMEC4AUTO (2021-2022) moved MEC to a trial phase, architecture blueprint, interoperability, security, ..

Focus of this webinar

High level 5GAA goal (since the time of MEC4AUTO)

- In the long-term, i.e. in a time window of two years (by 2022 at latest), 5GAA should be able to easily demonstrate the use of Multi-access Edge Computing (MEC) technology for automotive services, for example, when two distinct automotive vendors can truly test at least three use cases involving two distinct MNOs and employing network infrastructure provided by two distinct infrastructure vendors.

Heterogeneous scenario:



1. *Interop. between MNOs*
2. *Interop. between MEC vendors/suppliers*
3. *Interop between OEMs (applications)*

Key requirements from car industry:

1. How can a vehicle, which has radio access to **MNO A**, use a MEC application, which is operated by **MNO B**?
2. How do we ensure Interworking between **MNOs** whilst NOT losing the benefits of low latency?
3. How can an OEM (or a Tier-1 supplier) as the MEC application developer be sure, especially on a **global** basis, that a MEC app works in the same way whether it is operated by MNO A or by **MNO B**?
4. How do we ensure **global operational availability**?
5. How would the above two requirements be addressed in either a 1) **Neutral Host Edge Setup** or 2) **CoSP MEC Setup**?

1. *Edge resource sharing*
2. *Interworking at the Edge, 5G local breakout*
3. *MEC App portability*
4. *Global Oper. availability*
5. *Flexible MEC Deployment*

Suggested reading 5GAA MEC4AUTO technical report "MEC for Automotive in Multi-Ope Scenarios" (*)

(*) available at https://5gaa.org/wp-content/uploads/2021/03/5GAA_A-200150_MEC4AUTO_Task2_TR_MEC-for-Automotive-in-Multi-Operator-Scenarios.pdf

MEC4AUTO technical reports

- Focus on multi-MNO, multi-OEM, multi-vendor use cases for MEC

MEC4AUTO technical report TR1 "MEC Use Cases and initial test specifications review", July 2021

- MEC is a key enabler of several C-V2X applications that require ultra-low latency and high reliability.
- This report analyzed the C-V2X Use Cases, in particular those defined by 5GAA that require the processing of large amounts of data and could benefit from the use of MEC instead of uploading the data to the cloud, which could cause additional E2E delays.
- The selection of Use Cases was based on inputs from auto OEMs and their key requirements about interoperability between different operators, different vehicle OEMs and different app providers

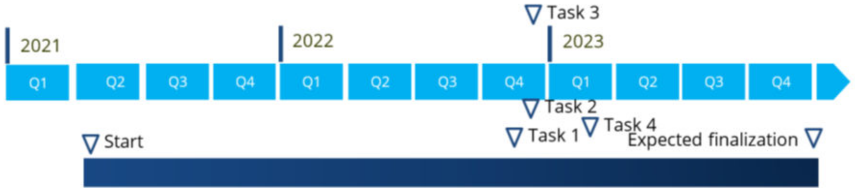
MEC4AUTO technical report TR2 "MEC for Automotive in Multi-Operator Scenarios", March 2021

- Based on the use cases selected in TR1 this report discussed the architecture and deployment aspects when Edge Computing is used for V2X use cases.
- The MEC4AUTO reference architecture was presented, by considering three main multi-MNO scenarios:

  1. Both MNO A and MNO B have a MEC platform and MEC application X.
  2. Both MNO A and MNO B have a MEC platform, but MEC application X is available only in MNO A.
  3. Only MNO A has a MEC platform and MEC application X is available only in MNO A.

Work Item Lead: Intel

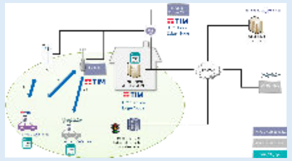
gMEC4AUTO – organization



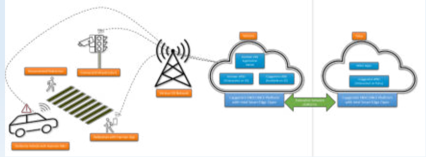
- ➢ Focus on multi-MNO, multi-OEM, multi-vendor use cases for MEC

Task 1 (Verizon)

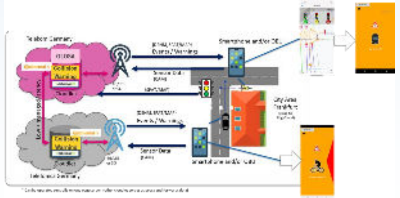
Moving toward federated MEC demos/trials (global MEC).



Demo Trial #1 on VRU (Turin, Italy)



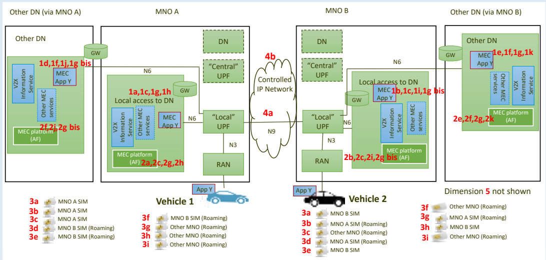
Demo Trial #2 at Virginia Smart Road (Blacksburg, Virginia)



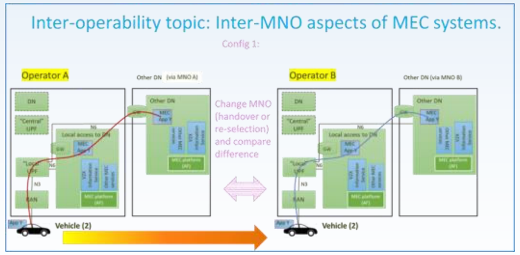
Demo Trial #3 on Collision Warnings and GLOSA (Frankfurt, Germany)

Task 2 (Anritsu)

MEC System interoperability, and test framework.



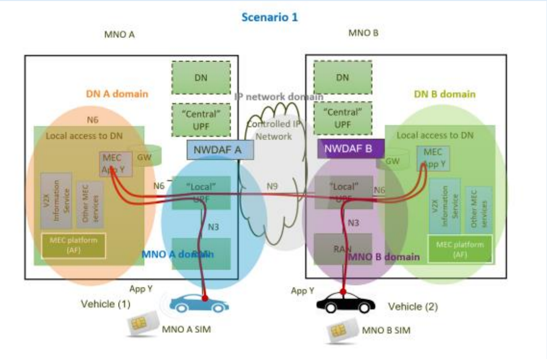
Arch. updates and interop scenarios (inspired by MEC trials)


Inter-operability topic: Inter-MNO aspects of MEC systems.
Config 1:
Operator A
Operator B
Other DN (via MNO A)
Other DN (via MNO B)
Change MNO (handover or re-selection) and compare difference
Vehicle (2)

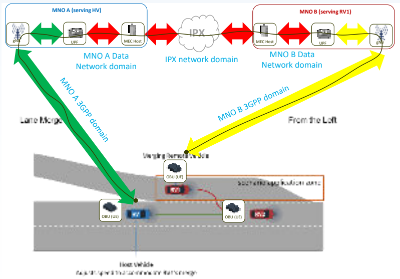
Selection of Use Cases for KPI/inter-operability assessment.

Task 3 (Huawei)

Usage of prediction, situation awareness and Network Slicing

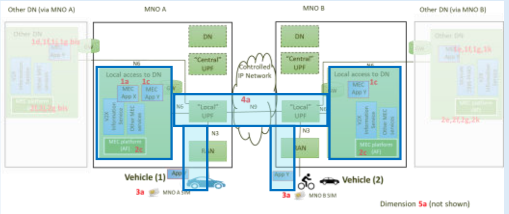


End-to-end QoS predictions across the various domains

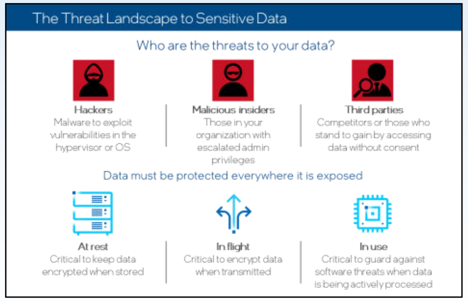


Task 4 (Telus → *Verizon*)

Cybersecurity for edge computing



Security boundaries in gMEC4AUTO architecture (example for scenario 3)



The Threat Landscape to Sensitive Data

Who are the threats to your data?

Hackers
Malware to exploit vulnerabilities in the hypervisor or OS

Malicious insiders
Those in your organization with escalated admin privileges

Third parties
Competitors or those who stand to gain by accessing data without consent

Data must be protected everywhere it is exposed

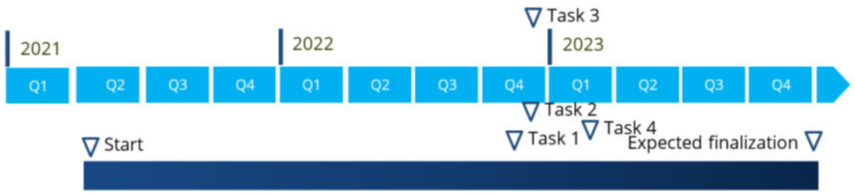
At rest
Critical to keep data encrypted when stored

In flight
Critical to encrypt data when transmitted

In use
Critical to guard against software threats when data is being actively processed

Threat landscape (security, privacy, trust)

gMEC4AUTO – main achievements



- Focus on multi-MNO, multi-OEM, multi-vendor use cases for MEC

Tasks	WG Interaction	Deliverable	Achievements
Task 1 - Moving toward federated MEC demos/trials (global MEC).	WG1, WG2	D1 (1Q22) - Public Global MEC Demo (PR), White paper.	Results from **MEC Trials** in US and EU (**5GAA PR**). Collaboration with GSMA OPG. Business SURVEY on MEC (sent to WG1, WG5, gMEC4AUTO). Joint position paper (with BRIDGE) on MEC guidelines for ROs/RTAs
Task 2 - MEC System interoperability, and test framework.	WG3	D2.2 (1Q23) - Final Report of Global MEC deployments: interoperability and system aspects.	Archit. enhancements, inspired by trials (e.g. roaming, edge resource sharing). **Interoperability and testing framework**. Re-opened MEC4AUTO TR on use cases, addition of AVP. MEC Performance Evaluation methodology, led by OEMs.
Task 3 - Usage of prediction and situation awareness and Network Slicing	WG2, PRESA	D3 (4Q22) - Report on “Predictive edge analytics and Network Slicing enabling Mobility-as-a-Service in Global MEC scenarios”	E2E analysis of predictive QoS. Collaboration with ETSI MEC and direct 5GAA impact on **standards** (V2X Information Services API, ETSI GS MEC 030). Network slicing and possible impact also in GSMA/3GPP.
Task 4 - Cybersecurity for edge computing	WG7	D4 (1Q23) - Report on “Cybersecurity for edge computing”	Analysis of **security, privacy and trust aspects** for the gMEC4AUTO architecture. Recommendations based on mapping with suitable mitigation strategies, avbailable from standards or industry-wide implementations.

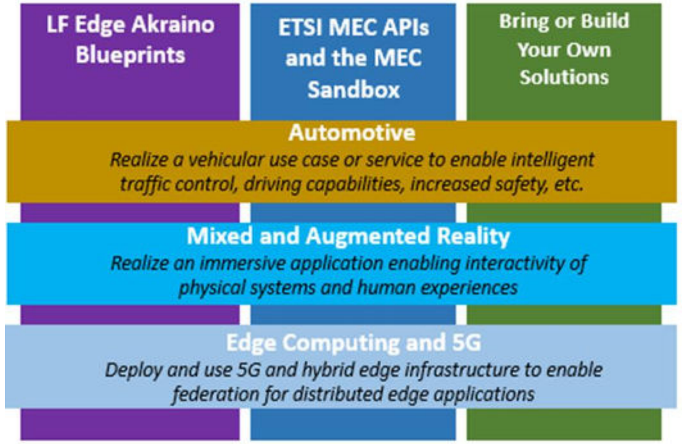
The **winner** of the **5GAA prize** (*Optare Solution*) presented their application at the 5GAA **Community Building Session** (18/10/2022), as guest speaker.

5GAA joined the organization of the **MEC Hackathon 2022**, offering to developers a prize of «*2.5k$ for the best automotive app*». Verizon (5GAA Board member) attended the Edge Computing World conference by assigning **5GAA award**: https://www.etsi.org/events/2080-2022-06-etsi-linux-foundation-edge-hackathon-2022

MEC Hackathon - 2022

- Collaboration between **ETSI (ISG MEC)**, the **LINUX Foundation (LF Edge)**, and the **5G Automotive Association (5GAA)**
- World-wide Hackathon that included 15 teams competing in 3 application verticals
- Remote Competition from July 1st to Sept 23rd ; ECW Developer Conference: Final prizegiving day (Oct 11 & 12, 2022)

Technical Challenge



LF Edge Akraino Blueprints

ETSI MEC APIs and the MEC Sandbox

Bring or Build Your Own Solutions

Automotive

Realize a vehicular use case or service to enable intelligent traffic control, driving capabilities, increased safety, etc.

Mixed and Augmented Reality

Realize an immersive application enabling interactivity of physical systems and human experiences

Edge Computing and 5G

Deploy and use 5G and hybrid edge infrastructure to enable federation for distributed edge applications

www.edgecomputingworld.com/call-for-edge-developers/

The developer call:

Realize an innovative edge application, solution, or use-case utilizing ETSI MEC Service APIs and LF Edge Akraino Blueprints

LF Edge – Akraino Blueprints:

Automotive	MEC-based Stable Topology Prediction for Vehicular Networks
Mixed & Augmented Reality	Virtual Classroom (Integrated Edge Cloud Type 4)
Edge Computing and 5G	Integrated Cloud Native NFV/App Stack Public Cloud Edge Interface (PCEI) Enterprise Applications on Lightweight 5G Telco Edge (EALTE)

Suggested ETSI MEC Services and APIs:

1) MEC011 - MEC Platform App & Service Enablement (Mp1)
2) MEC012 - Radio Network Information Service (RNIS)
3) MEC013 - Location Service
4) MEC021 - Application Mobility Service (AMS)
5) MEC028 - WLAN Access Information Service (WAIS)
6) MEC030 – V2X Information Service (VIS)

Developers were encouraged to use other APIs at their choice

Hackathon Sponsors and Supporters

Equinix offered teams access to their Metal Platform

- metal.equinix.com

Intel offered teams access and tech support for Smart Edge Open

- smart-edge-open-overview

Overview of MEC Federation Trials

gMEC4AUTO Task 1

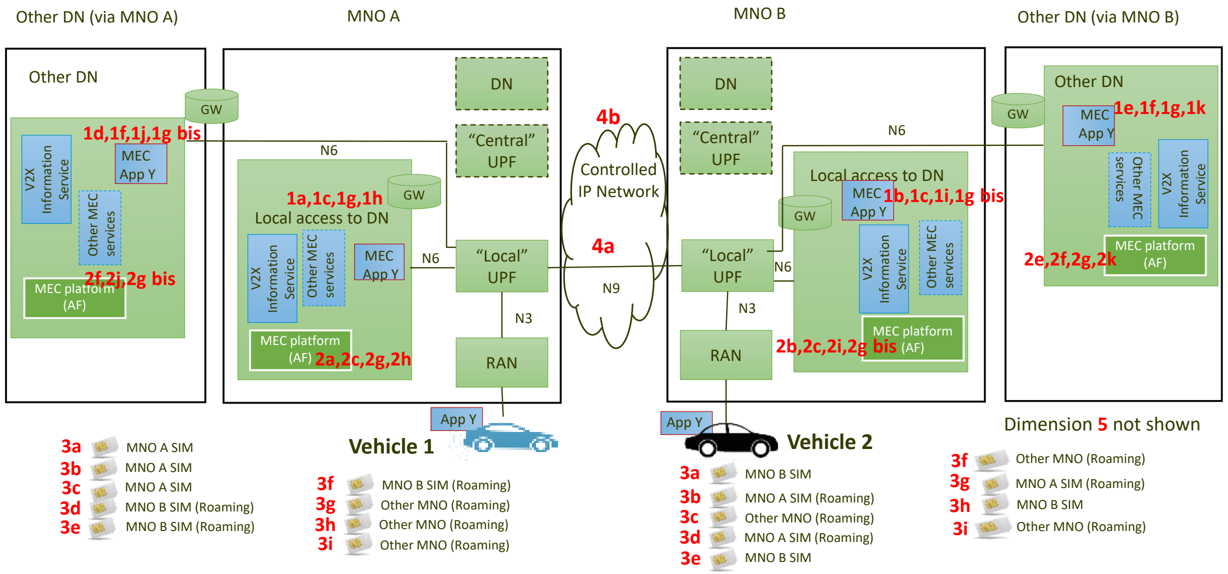
Lead Jyoti Sharma (Verizon); editor Shammi Amin

gMEC4AUTO Task 1: Moving toward federated MEC demos/ trials (global MEC).

Approach:

- ➢ Updated architecture, inspired by trials
- ➢ Scenarios categorization in 5 dimensions:

1. Presence of **MEC Application**
2. Presence of **MEC Platform to expose edge services**, like predictions
3. **Subscription** of end-user (vehicle (sub) system) according to SIM (instead of Global SIM)
4. Available **interconnection** between MNOs
5. When in **roaming** (only for cases 3b,3c,3d,3e,3f)

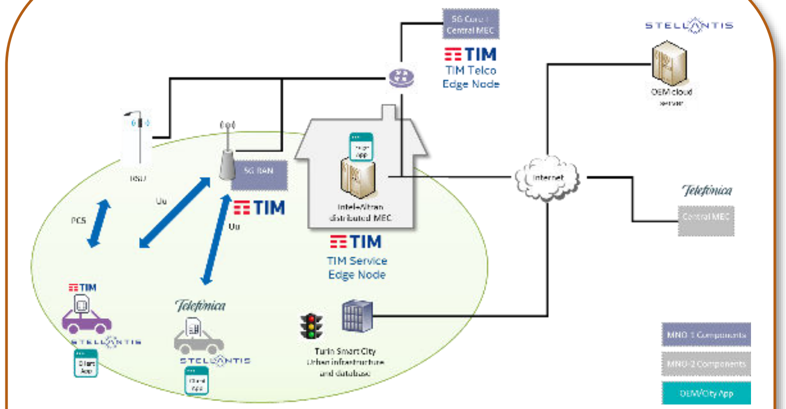


Highlights from the report:

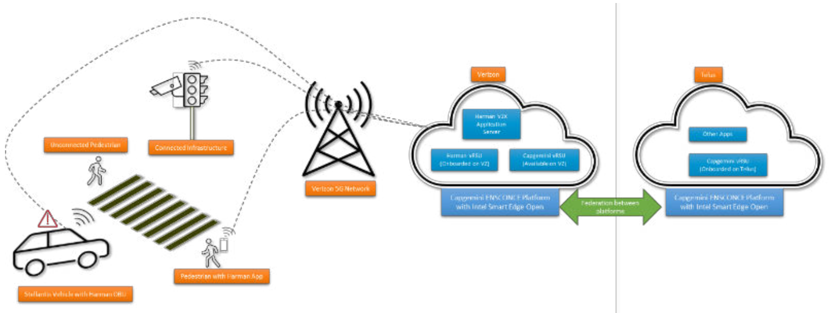
- Updated scenarios dissections for the MEC4AUTO architecture
- Description of Multi-MNO MEC Trials in different geos

gMEC4AUTO trials

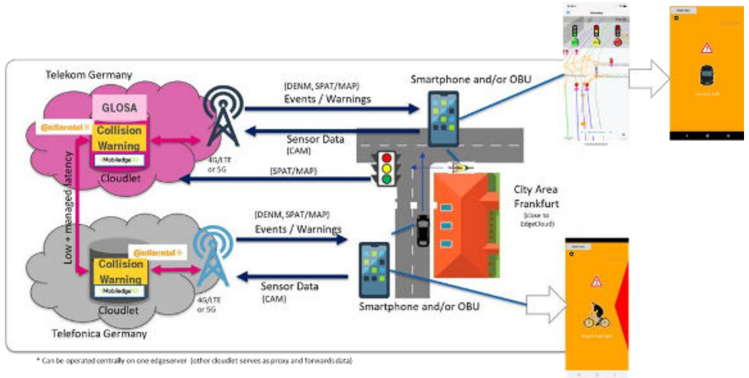
- **Task 1** - Moving toward federated MEC demos/trials (global MEC).



Trial #1 on Vulnerable Road User
(Turin, Italy)


Unconnected Pedestrian
Connected Infrastructure
Verizon 5G Network
Stellantis Vehicle with Harman OBU
Pedestrian with Harman App
Verizon
Harman V2X Application Server
Harman vRSU (Onboarded on VZ)
Capgemini vRSU (Available on VZ)
Capgemini ENSCONCE Platform with Intel Smart Edge Open
Federation between platforms
Telus
Other Apps
Capgemini vRSU (Onboarded on Telus)
Capgemini ENSCONCE Platform with Intel Smart Edge Open

Trial #2 at Virginia Smart Road
(Blacksburg, Virginia)



* Can be operated centrally on one edgeserver (other cloudlet serves as proxy and forwards data)

Trial #3 on Collision Warnings and GLOSA
(Frankfurt, Germany)

videoclip

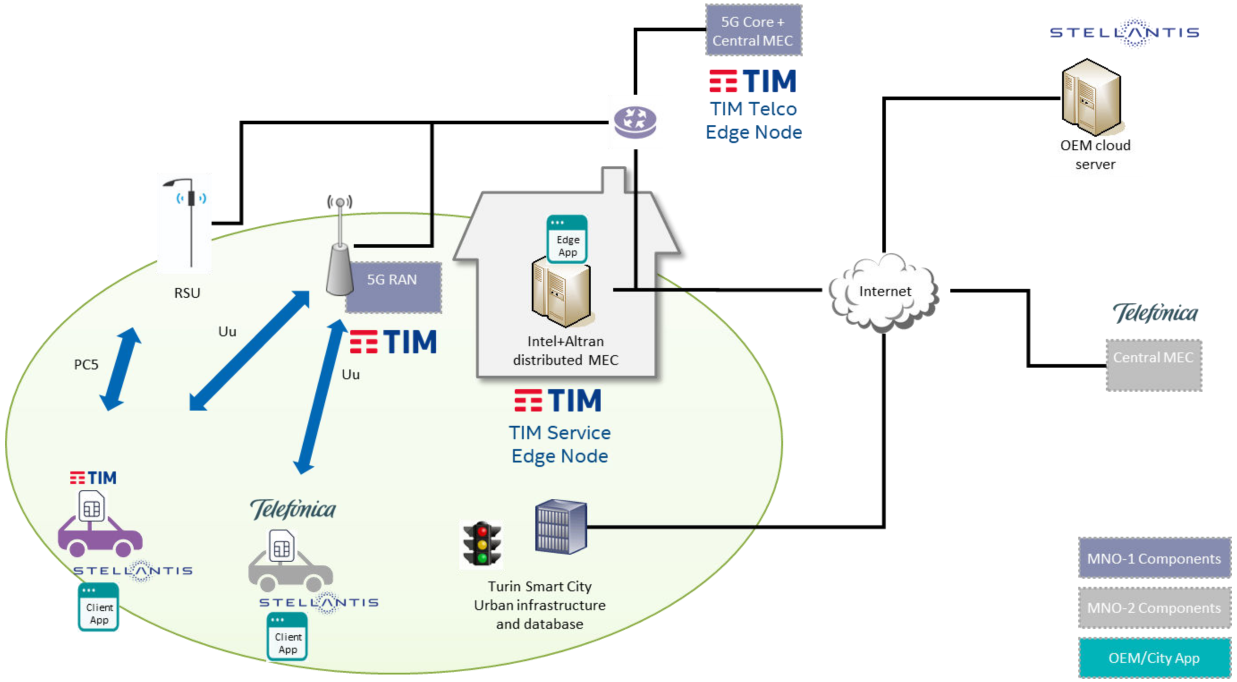
https://vimeo.com/681831127

5GAA Automotive Association

MEC Trial #1: System Architecture

- Multi-operator MEC trials, conducted in 5G live networks
- Trial with multiple operators using roaming scenario instead of Neutral Host in this first phase),
- Instantiated in 2 regions: Europe (EU) and North America (NA).
- The two regions thus instantiated two similar MEC systems in multi-MNO environment, where hosting operator (TIM in the EU example, in Fig.) was providing the radio access, to allow local connectivity with the devices and vehicles (from Stellantis) in the city (Turin, Italy)

Exemplary system architecture in the EU trial instance:

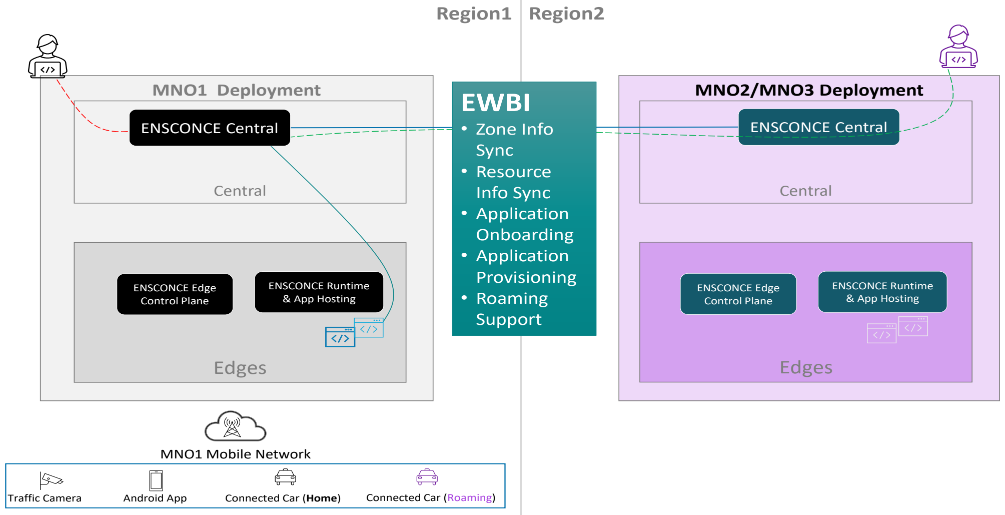


- Intel (lead of the whole trial activity) and Capgemini provided the common infrastructure
- Cisco, as provider of the hardware infrastructure hosting the MEC software platform
- Harman acted as V2X Solution Provider and MEC Application developer
- TIM, acting as host and demo coordinator through its Innovation Lab competences and facilities, provider for 5G connection, roaming features allowing local breakout and MEC infrastructure
- Telefonica and BT, acting as federated MNOs. Customers redirected by the MEC home platforms towards TIM edge platform for closest cloudlet allocation. 5G roaming set to allow local breakout.

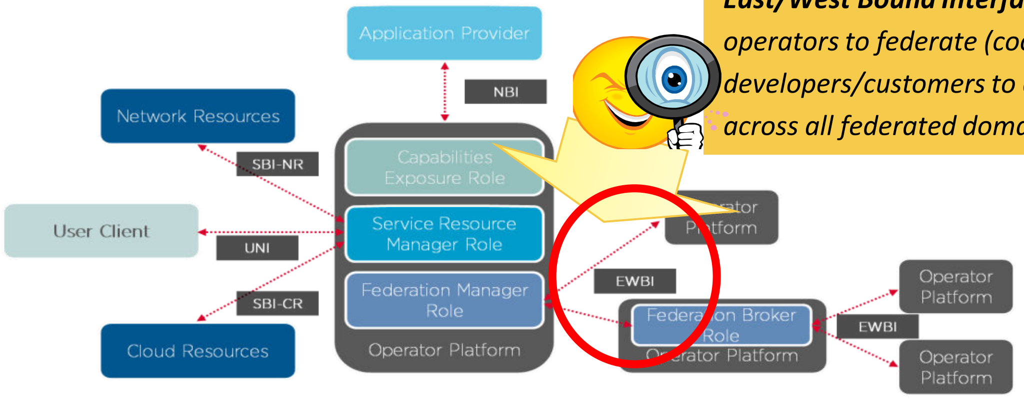
Suggested reading: Sabella et al.: «Global MEC supporting automotive services: from multi -operator live trials to standardization», IEEE CSCN 2021, https://ieeexplore.ieee.org/document/9686115

Impacts: the *path* toward standardization

The **trial** implemented a secure interconnection for the multi-MNO MEC control plane exchange through **EWBI**, according to federation requirements.

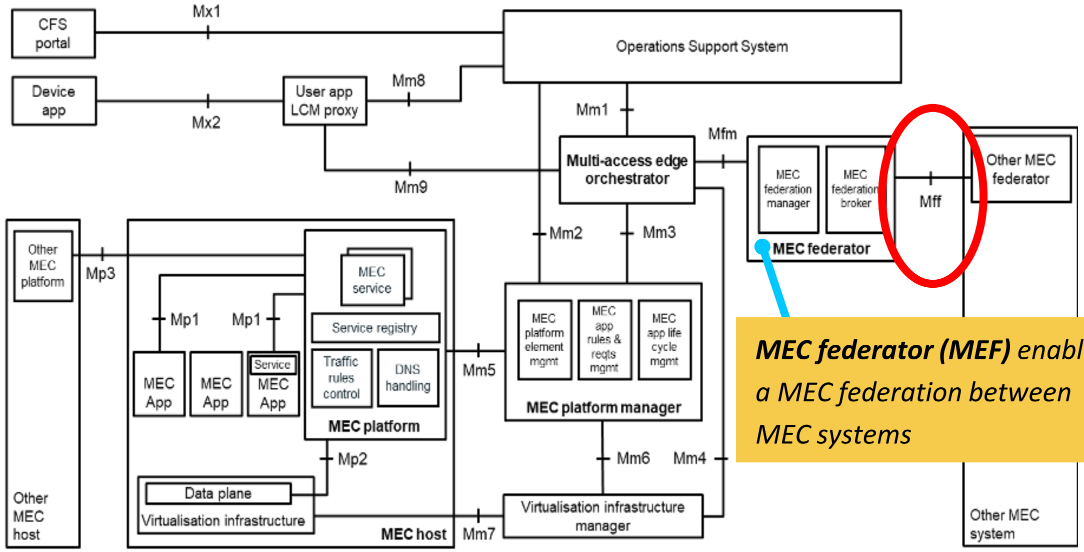


Overview of the ENSCONCE platform with EWBI interconnection between MEC systems across different regions



***East/West Bound Interface (EWBI)**, allowing operators to federate (cooperate) and developers/customers to deploy their loads across all federated domains*

Multi-operator edge "OP architecture" (GSMA OPG)



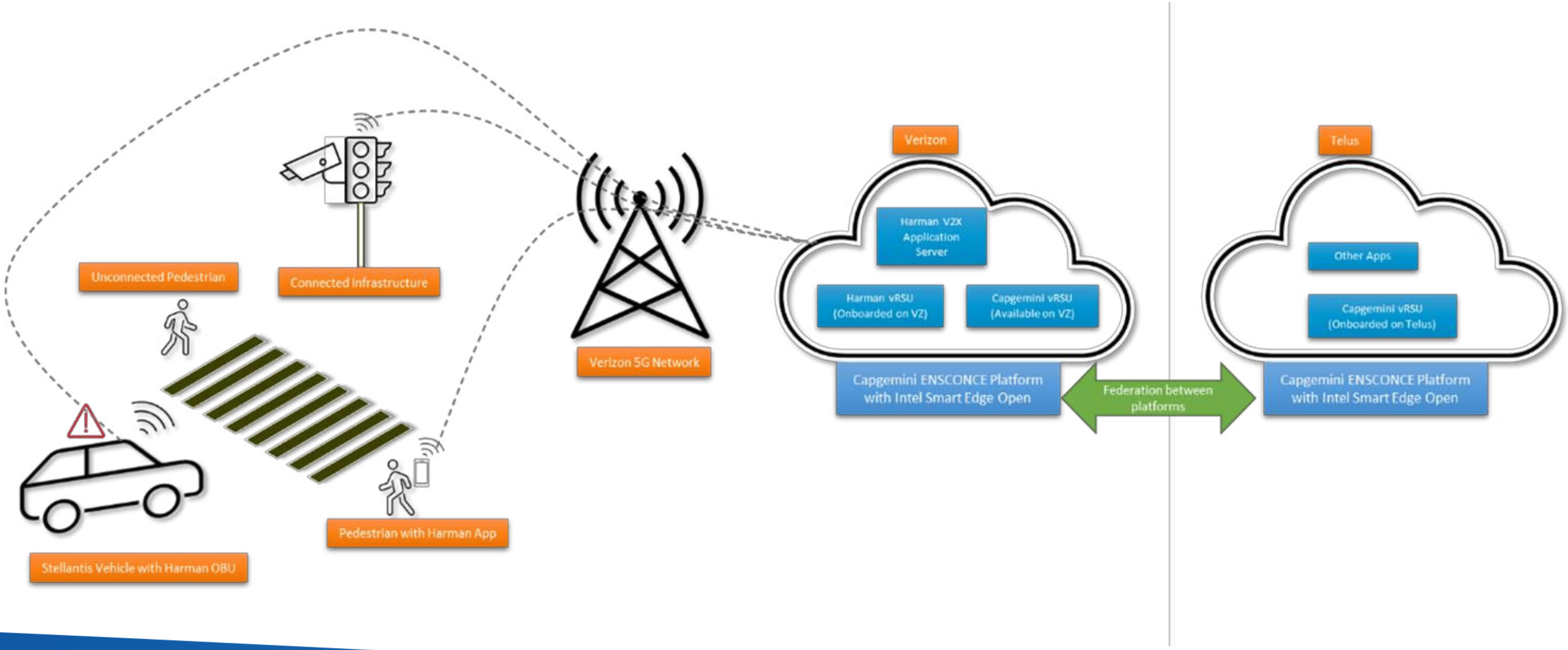
***MEC federator (MEF)** enables a MEC federation between MEC systems*

Multi-access edge system reference architecture variant for MEC federation (ongoing in ETSI MEC)

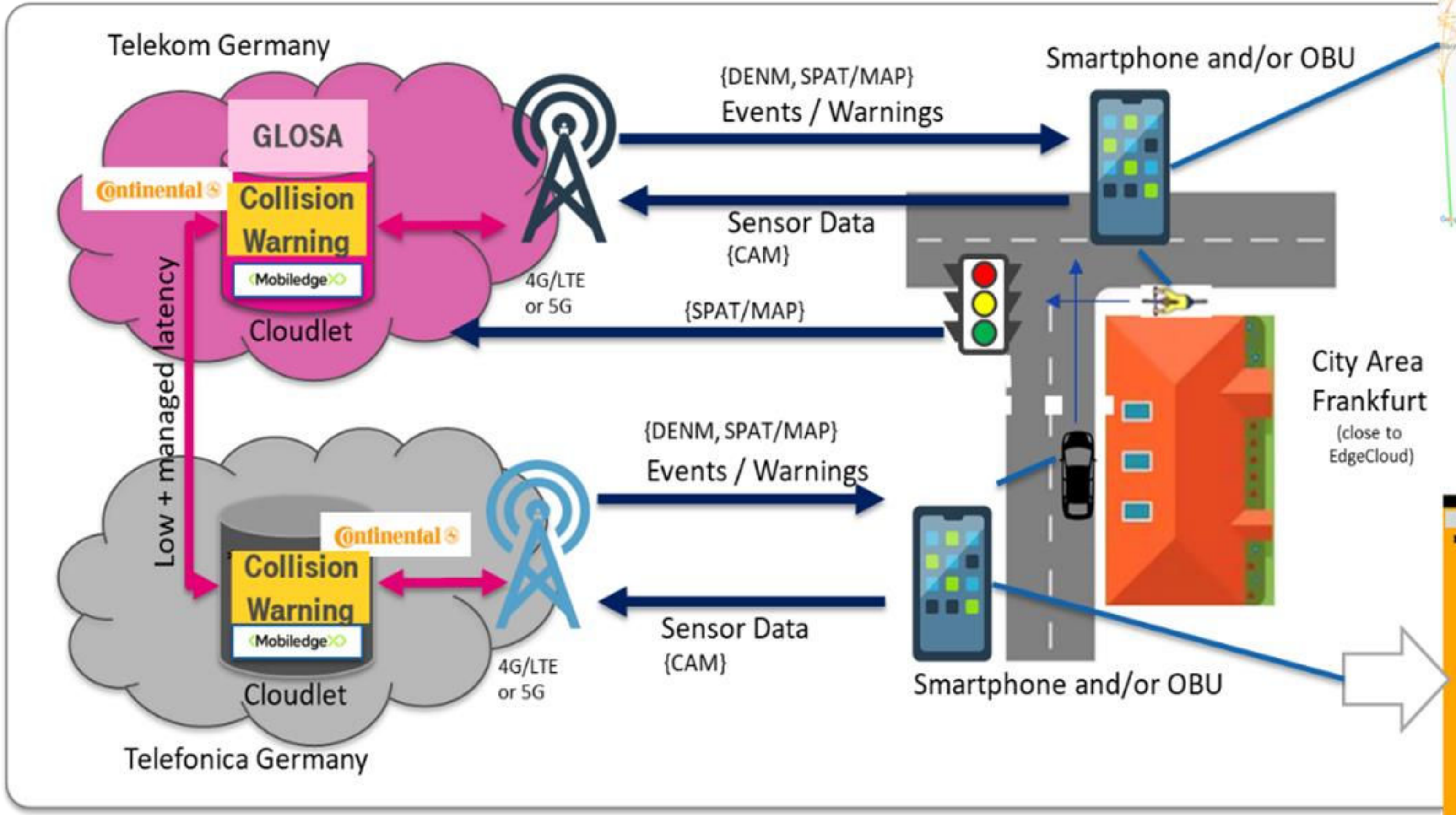
- Possible **impacts** of the present work can include:
- contributing on open-source communities (in accordance with **GSMA** OPG) with some exemplary implementations of relevant components,
- provide coherent contributions toward the relevant standard bodies (**ETSI MEC** and **3GPP**), in order to enable globally interoperable MEC deployments.

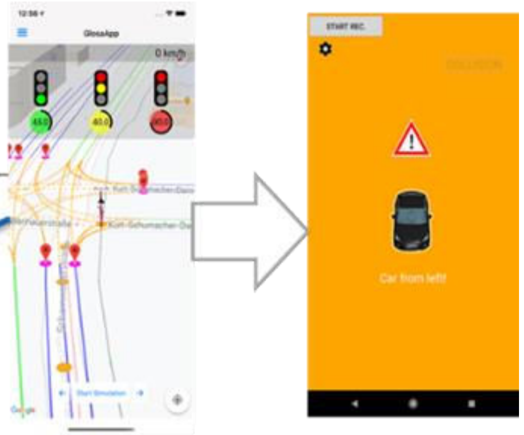
Ref. ETSI GS MEC 003 v3.1.1 (available at https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/03.01.01_60/gs_MEC003v030101p.pdf)

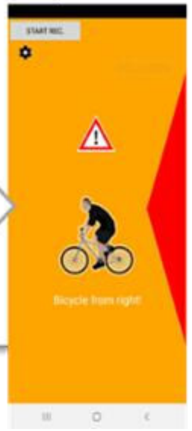
Trial #2 at Virginia Smart Road (Blacksburg, Virginia)


Unconnected Pedestrian
Connected Infrastructure
Verizon 5G Network
Stellantis Vehicle with Harman OBU
Pedestrian with Harman App
Verizon
Harman V2X Application Server
Harman vRSU (Onboarded on VZ)
Capgemini vRSU (Available on VZ)
Capgemini ENSCONCE Platform with Intel Smart Edge Open
Federation between platforms
Telus
Other Apps
Capgemini vRSU (Onboarded on Telus)
Capgemini ENSCONCE Platform with Intel Smart Edge Open

Trial #3 on Collision Warnings and GLOSA (Frankfurt, Germany)







* Can be operated centrally on one edgeserver (other cloudlet serves as proxy and forwards data)

Preliminary considerations for MEC deployments

- In general, there is a clear industry consensus on the benefits of federated MEC systems, where different business models could be further investigated in 5GAA.

- There is also some consensus on the central role of operators and service providers going forward in collaboration with the different MEC infrastructure technology providers (including data centre, neutral hosts, etc.).

5GAA Global Multi-operator MEC Trials

5GAA Press Releases

https://5gaa.org/live-trial-of-5g-connected-car-concept-to-launch-in-turin-italy/

https://5gaa.org/live-trial-of-5g-connected-car-concept-launches-in-blacksburg-virginia-va/

5GAA MEC Trial Videos

https://vimeo.com/713254675

https://vimeo.com/681831127

MEC interoperability Scenarios

gMEC4AUTO Task 2

gMEC4AUTO Task 2: MEC interoperability analysis

Approach:

- MEC considering complex scenarios where multiple applications, each with specific requirements, coexist and concurrently run into the car.
- Focus on:
  - MEC from UE perspective (service and network aspects)
  - MEC from inter-MNO (network aspects)
  - MEC from inter-OEM perspective of MEC systems.

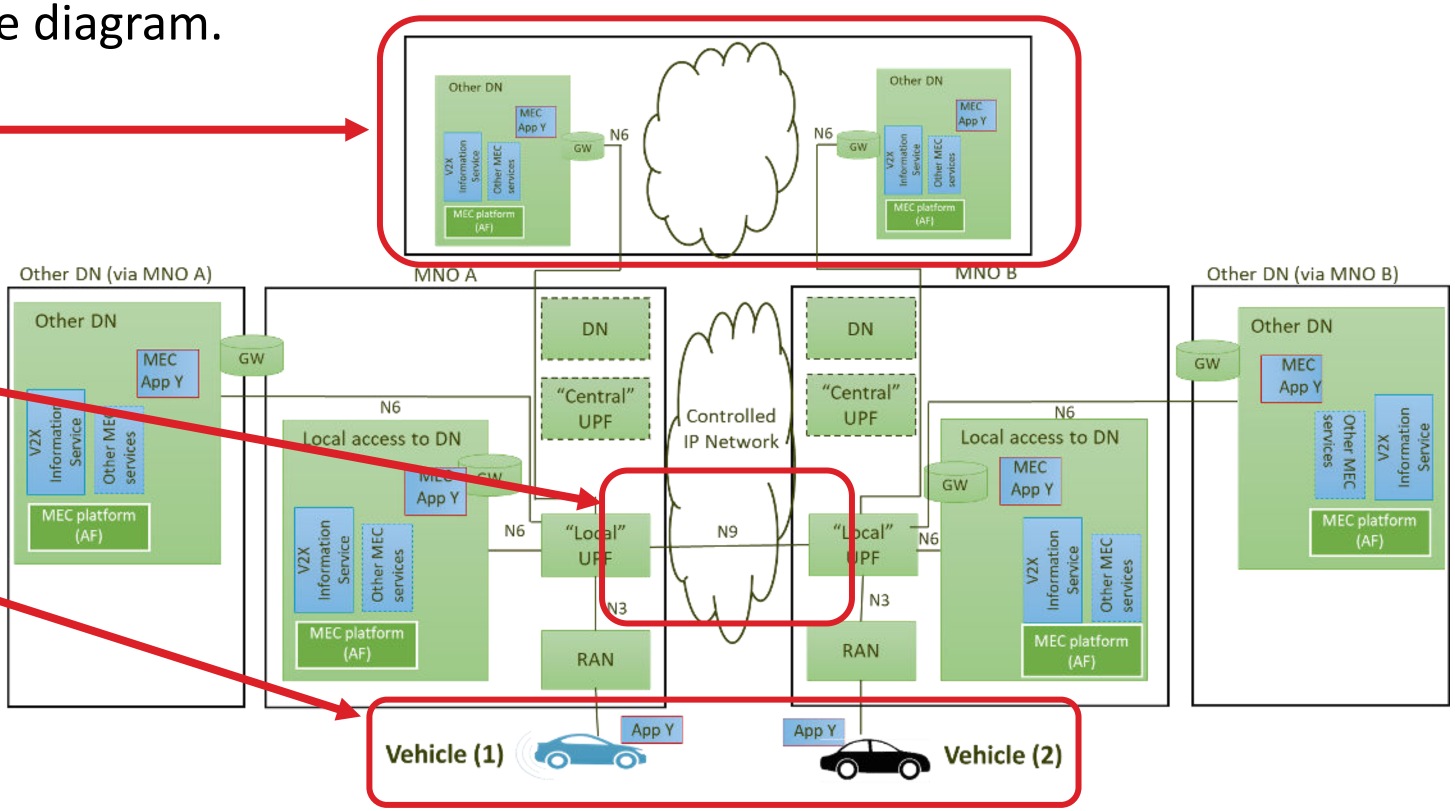
Highlights from the report:

- Selection of UCs for testing and KPI assessment (include UC with predictive QoS)
- Definition of a TOL (Test Object List) for multi-MNO/OEM scenarios.

Selection of scenarios

Step 1. Revision of reference architecture diagram.

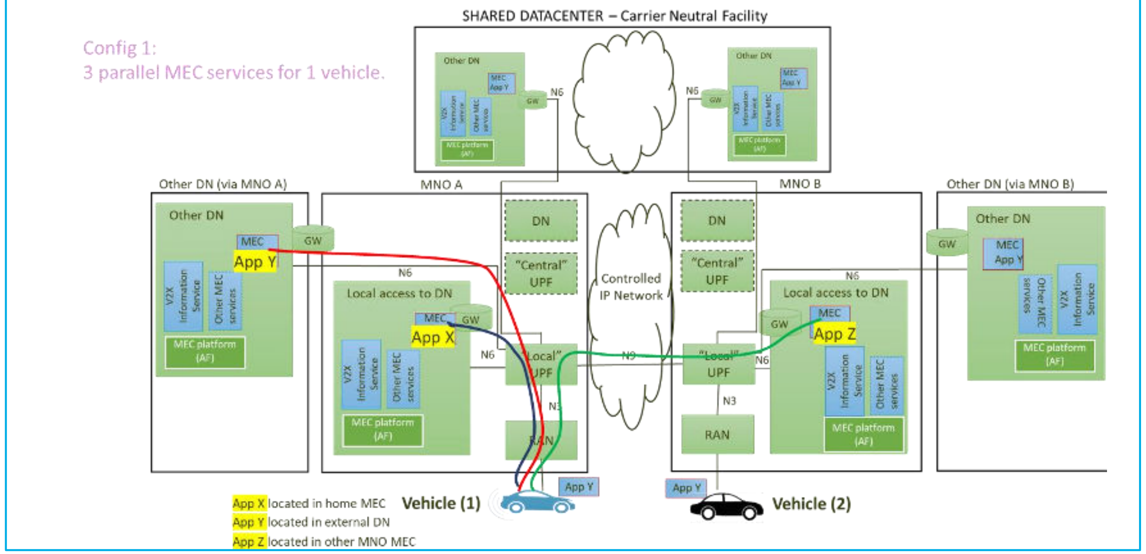
- different MEC host setups: local data network (DN inside the MNO domain), other DN (via MNO network) and setup in neutral host (NH) (thus, in shared DN).
- support for edge resource sharing use cases
- device roaming, in terms of different SIM options (MNO A, MNO B, roaming etc.)



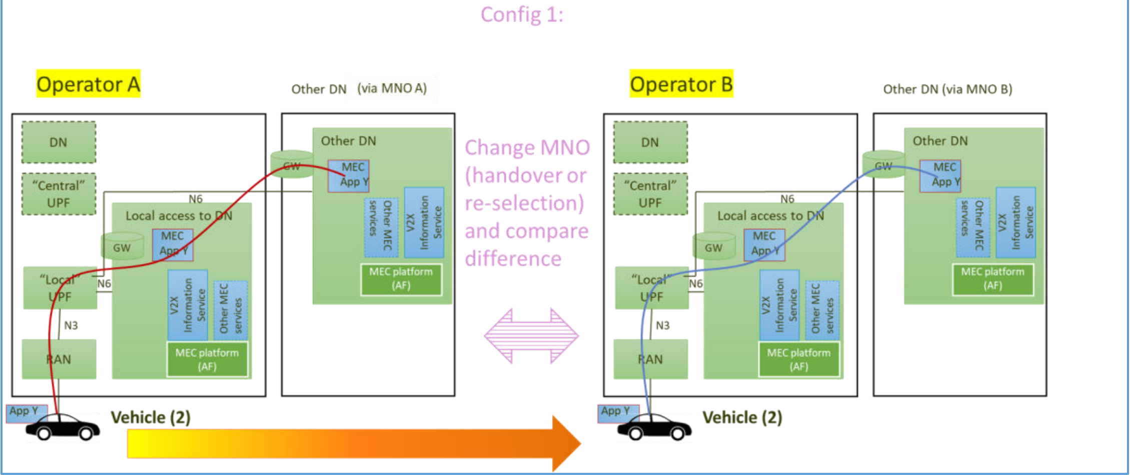
Step 2:

- Creation of many inter-operability combinations.
- Down selection to smaller group for study, based on task 1 trials configurations.

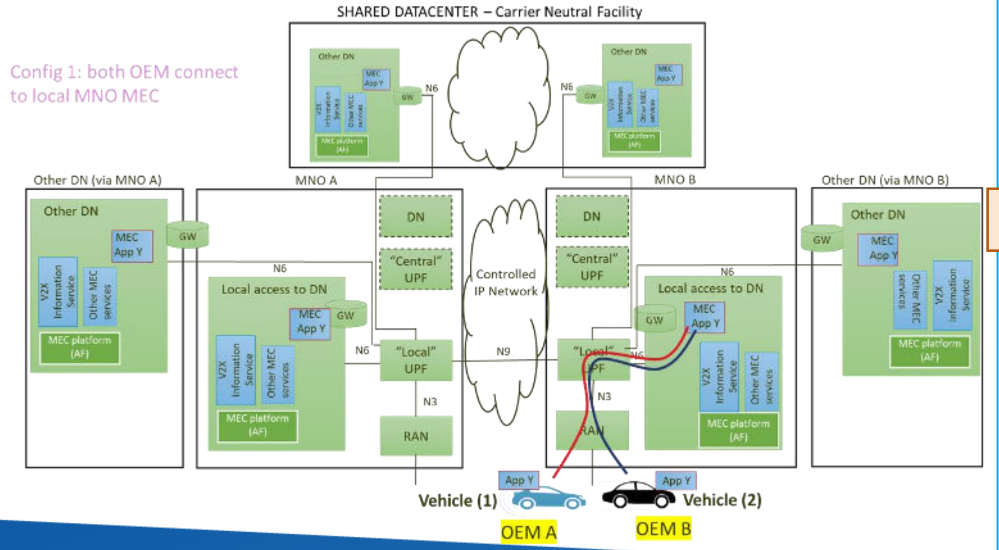
Interoperability of MEC from UE (OEM) perspective (service and network aspects)



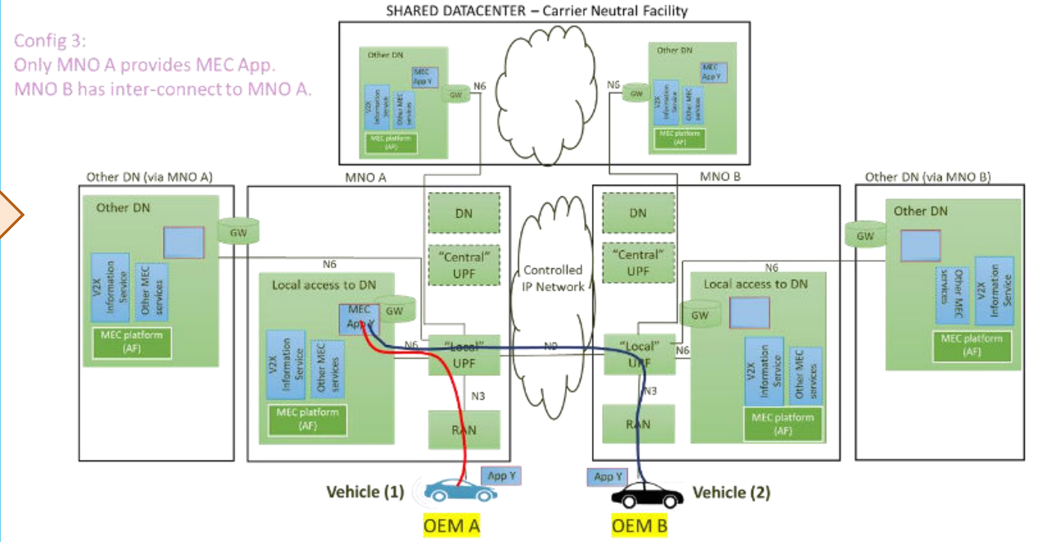
Inter-operability topic: Inter-MNO aspects of MEC systems.



Inter-operability topic: Simple Inter-OEM (V2N2V) MEC service



Inter-operability topic: Required Inter-OEM (V2N2V) MEC service



5GAA Automotive Association

Selection of Use Cases for testing and KPI assessment

Starting from the selected use cases from previous MEC4AUTO Technical Report as follows:

- See-Through
- In-Vehicle Entertainment (**IVE**)
- Intersection Movement Assist (**IMA**)
- Vulnerable Road User (**VRU**), In-Vehicle Sensor-based Approach, Infrastructure Sensor-based Approach
- Vehicle Platooning

Consider other MEC-related use cases which have emerged since the original MEC4AUTO report (requiring low latency and high reliability).

- In particular, the Automated Valet Parking (**AVP**) use case is of interest.

In addition, the following list of use cases have been selected for Predictive Quality of Service (PQoS), according to the 5GAA NESQO TR:

- RT Situation Awareness and High Definition Map (Hazardous Location Warning)
- Software Update
- Tele-Operated Driving
- High-Density Platooning
- Advanced Safety (Lane Merge)
- In-Vehicle Entertainment

From the above candidate use cases, three have been recommended for further study:

- **IVE** has a relatively simple implementation architecture, and can more easily be defined and studied. Also includes P-QoS.
- **VRU** also includes the off-load of compute resources from vehicle-to-network, and represents a more complex set of interactions.
- **AVP** (Type 2) has an advanced definition of architecture and deployment within 5GAA and industry, which enables a real-world analysis of a use case with multiple actors involved in the scenario, and also has a complex architecture.

KPI assessment

The previously published MEC4AUTO report proposed an initial set of KPIs.

- These KPIs are defining the key attributes to be ensured when using MEC to support a use case.

Interoperability study and testing should ensure that these KPIs are not impacted or affected by different interoperability scenarios.

- Whilst the actual measured value for any KPI may change with different interoperability scenarios, in each one it is required that the related service provider can still ensure and maintain a specified performance level for each KPI.

Metric/KPI	Description	Beneficiary
End-to-end latency	The latency definition in the scope of MEC4AUTO is referring to round-trip time (RTT), measured on the application level. Depending on the service type, the RTT might include heterogeneous paths (e.g. simple client-server applications, or multi-client communication through server, etc.).	End user, OEM
Bandwidth saving	A key benefit of MEC is a reduced load on the transport network. This can be measured in terms of network throughput saving (i.e. user plane traffic at IP level) with respect to the usage of remote server applications.	MNO
Security and privacy	Security compliance can be a complex assessment and hard to perform in an exhaustive manner. The same considerations apply to privacy. Rather, a qualitative assessment of a use case for this metric can be performed.	All stakeholders
Energy efficiency	MEC energy efficiency benefits can be defined at the UE side (terminals) and at the network side (linked to infrastructure bandwidth saving).	MNO and End User device
Bitrate guarantee	Besides latency, MEC can also have an impact on the capability to provide bitrate guarantees. This is not intended for quantitative evaluations but for qualitative one. Examples of such evaluations could be attributes such as “best effort/elastic”, “guarantee required – fixed bitrate”, “guarantee required – minimal bitrate”, “maximum bitrate (no benefit for application if higher one is provided)”, “event-triggered messages without fixed bitrate requirement”, etc.	End user

Definition and review of Test Object List (TOL).

- **End-to-end latency** was previously defined as RTT in previous MEC4AUTO studies. Two key points that affect the latency requirement are
  1. the traffic type (e.g. UDP packet size, packet rate).
  2. the asymmetric nature of many V2X use cases – different uplink and downlink data traffic loads – as defined in the 5GAA Use Case Description Documents.

  Definition should be refined to define uplink and downlink latency separately, with appropriate traffic types and the statistical nature of the latency distribution (e.g. 99% of downlink UDP packets to be within 20mS latency).

- **Bandwidth saving** in cellular networks is generally designed to manage a greater volume of downlink user plane data compared to uplink (for example, video streaming content distribution networks use a large volume of the data on 4G/5G).
  - The 5G air interface is generally supporting larger downlink data rates than uplink data rates, leading to greater downlink capacity in networks.
  - Some automotive UCs use higher uplink data rates compared to downlink.

  Evaluation of MEC deployment-based bandwidth saving should evaluate the impact of different interoperability scenarios on the bandwidth of the specific use case, and the relative impact on related UL and DL transport network traffic.

- **Security and privacy** is defined above as a qualitative metric for MEC KPIs. For the interoperability assessment, any possible impact on security and privacy should be identified in a qualitative manner for the different scenarios. The topic of MEC security is handled separately and in more detail in the gMEC4AUTO Task 4.

- **Energy efficiency** savings from MEC are closely related to the bandwidth savings.
  - The reduced bandwidth required in the transport network (reduction in data processing operations) leads to reduced power consumption by the network.
  - The ability to provide services more locally from a roadside unit (RSU) or small cell, rather than a macro cell, can reduce the level of radio frequency (RF) power transmission required to support the service.

- **Bitrate guarantee** is described above as a qualitative parameter in terms of KPI assessment. For the interoperability assessment, then, the possible impact on mechanisms used to deliver the bitrate should be identified for the different scenarios and use cases.

Definition of TOL related to each deployment scenario

Based upon the analysis the Test Object List can be reviewed in the context of each of the three deployment scenarios which were identified for study.

Multi services (MEC from OEM) scenario

- E2E latency: Traffic data type (UL and DL), latency (UL and DL), availability (e.g. 99.9%).
- Bandwidth saving: Multi-locations of AS may give multiple savings simultaneously.
- Security and privacy: Multiple MEC locations and servers to be considered simultaneously.
- Energy efficiency: Include offload of compute resources from vehicle to MEC/cloud.
- Bitrate guarantee: Type of guarantee (e.g. best effort, minimum rate, fixed rate), availability (e.g. 99.9%)

Inter-MNO scenario

- E2E latency: Traffic data type (UL and DL), latency (UL and DL), availability (e.g. 99.9%).
- Bandwidth saving: No extra comments.
- Security and privacy: Change of MNO access route to MEC may imply change of security and privacy domain.
- Energy efficiency: No extra comments.
- Bitrate guarantee: Type of guarantee (e.g. best effort, minimum rate, fixed rate), availability (e.g. 99.9%).

Inter-OEM scenario

- E2E latency: Traffic data type (UL and DL), latency (UL and DL), availability (e.g. 99.9%).
- Bandwidth saving: No extra comments.
- Security and privacy: Different OEMs’ implementations are connected simultaneously.
- Energy efficiency: No extra comments.
- Bitrate guarantee: Type of guarantee (e.g. best effort, minimum rate, fixed rate), availability (e.g. 99.9%).

Remarks on MEC interoperability

- In this study we defined **a new architecture framework** for MEC4AUTO, outlining the different components and players within an automotive MEC deployment scenario.
- Analysed the different combinations and scenarios and identified three leading scenarios for further interoperability analysis, based upon the actual trials and demonstrations.
  - MEC interoperability from UE (OEM) perspective
  - Inter-OEM perspective of MEC interoperability
  - Inter-MNO perspective of MEC interoperability
- From the set of **candidate use cases**, the three were recommended for further study, as follows:
  - **IVE** was selected because it has a relatively simple implementation architecture, and can more easily be defined and studied.
  - **VRU** was chosen because it also includes the aspect of off-loading compute resources from vehicle-to-network, and represents a more complex set of interactions between different entities.
  - **AVP** (Type 2) was selected as it has an advanced definition of architecture and deployment within 5GAA and industry. This enables a real-world analysis of a use case that has multiple actors involved in the scenario, and also has a complex architecture.
- The **KPIs related to performance evaluation of MEC** have then been analysed, with specific observations on their relevance to interoperability and testing of MEC deployments. These have been analysed in the context of the three identified scenarios, and how these scenarios may affect the KPIs related to:
  - E2E latency
  - Bandwidth saving
  - Security and privacy
  - Energy efficiency
  - Bitrate guarantee
- Lastly, the latest MEC test and interoperability related developments in industry have been reviewed. This looked at ETSI MEC, 3GPP, GSMA, CAMARA, GCF, and NGMN organisations. We can see progress and new initiatives in the industry, with multiple trails, Plugtests, and testing specifications being developed.

Edge Predictive Analytics in Multi-Operator scenarios

gMEC4AUTO Task 3

gMEC4AUTO Task 3:
Edge Predictive Analytics and Network Slicing in Multi-Operator scenarios

5GAA

MEC for Automotive in Multi-Operator Scenarios

Highlights from the report:

- Identified the need for analytics related to the **E2E user plane link between two V2X application instances in multi-MNO and multi-domain MEC deployments:**
  - In cooperation with ETSI MEC ISG, the WI contributed to the new version of the standard GS MEC 030 to support the new functionality
- Studied enhancements for the **V2X message interoperability service**
- Studied the use of **network slicing** for MEC multi-domain applications, suggesting further enhancements

Motivation for Predictive Edge Analytics: to enhance the contextual awareness of V2X applications

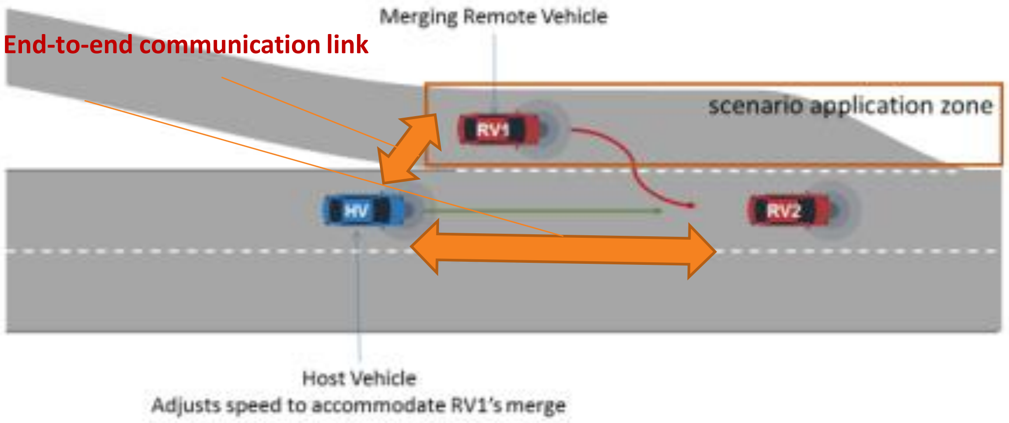
Example: Cooperative Lane Merge/Change

Predictive edge analytics are part of the **contextual awareness** of a V2X application:

- they provide early notifications about potentially undesirable effects, poor user experience, limited support of selected features or when a service could be no longer available or available again.

Cooperative Lane Merge/Change (using Uu and MEC) can benefit of **predictive edge analytics**:

- It involves **vehicles exchanging data** (e.g. their intended trajectories to coordinate their lateral (steering) and longitudinal controls (acceleration/deceleration)) **to ensure a smooth manoeuvre** [3]
- several messages need to be exchanged over a **certain period of time** amongst the involved vehicles and **SLRs should be supported during the whole lane merge/change operation**
- **predictive QoS notifications of the end to end communication link, may determine different actions in the involved vehicles** (e.g. abort maneuver or switch to a different communication mode).


End-to-end communication link
Merging Remote Vehicle
scenario application zone
RV1
HV
RV2
Host Vehicle
Adjusts speed to accommodate RV1's merge

Cooperative Lane Merge/Change (using Uu and MEC) [1]

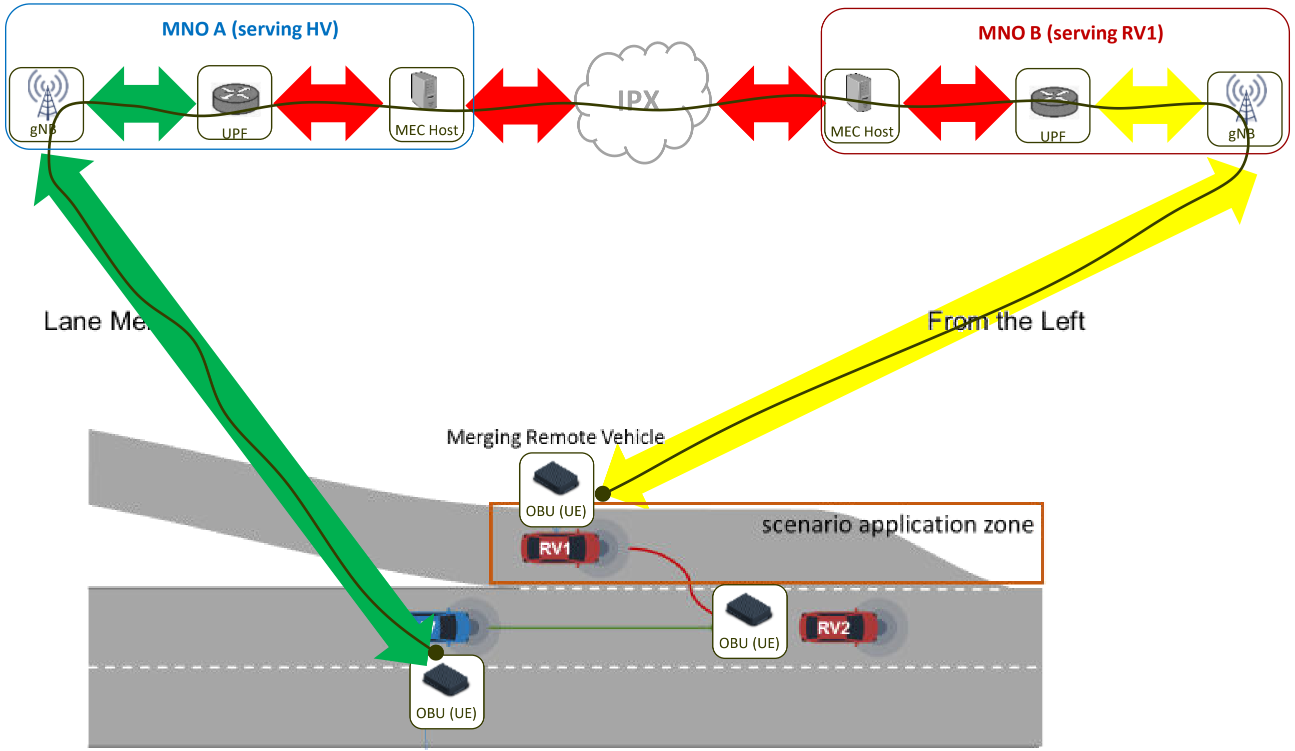
[1] 5GAA_T-190032_Use Case Description Cooperative Lane Merge_v1.1
[2] MEC4AUTO Technical Report Use Cases and initial test specifications review
[3] 3GPP TS 22.886 Study on enhancement of 3GPP Support for 5G V2X Services

Predictive Edge Analytics in multi-MNO MEC deployments

Gap analysis

- Predictive QoS (P-QoS) of an **E2E user plane link** between two V2X application instances:
  - V2N2V: between two application instances in two vehicular UEs
  - V2N2I: between an application instance in vehicular UE and an application instance in an infrastructure element.

- Example of potential QoS issues not covered by 3GPP Rel-18 P-QoS:
  - N6 or in the network containing the MEC host (Data Network)
  - Network segment of IP interconnect between MNOs (e.g., N9 or IPX)
  - Network of the MNO serving the remote vehicle (which can be different from the MNO serving the host vehicle)



Breakdown of the E2E user plane link (*)

●—● end-to-end user plane link between two V2N2V application instances

🟩 QoS prediction **available** (via 3GPP interface)

🟥 QoS prediction **not available** (via 3GPP interface).

🟨 QoS prediction **may be available** (via 3GPP interface) for the RV1 vehicle but **currently not available** for the HV vehicle via standard interface (**).

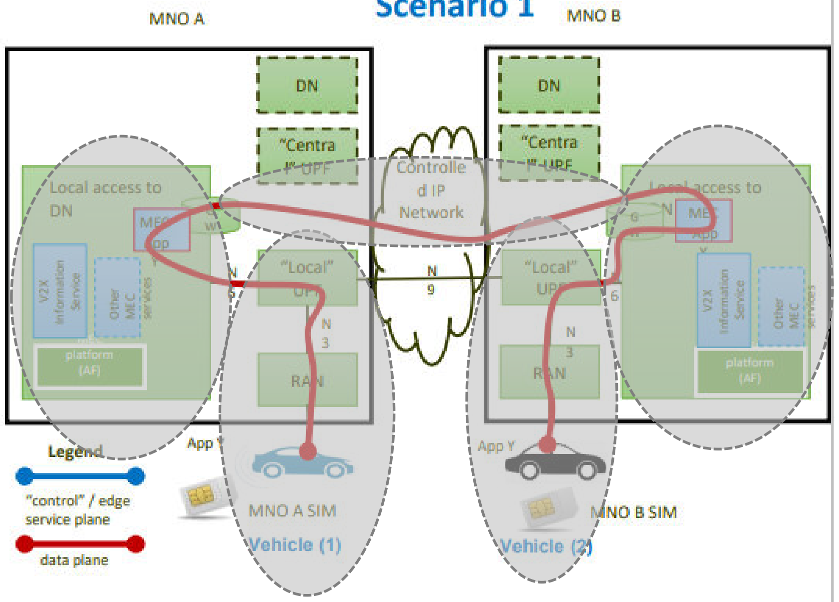
(*) 5GAA MEC4AUTO TR Scenario 1. Other deployment options may be possible, with different configurations for E2E user plane link
(**) RV1 vehicle may share the QoS prediction with HV via user plane connection, no standard currently specifies this.

MEC Scenarios and analytics domains

Typical deployments of multi-MNO MEC infrastructure (V2N2V)

⬚ Example of an analytics domain relevant to one segment of the E2E user plane link between two application instances

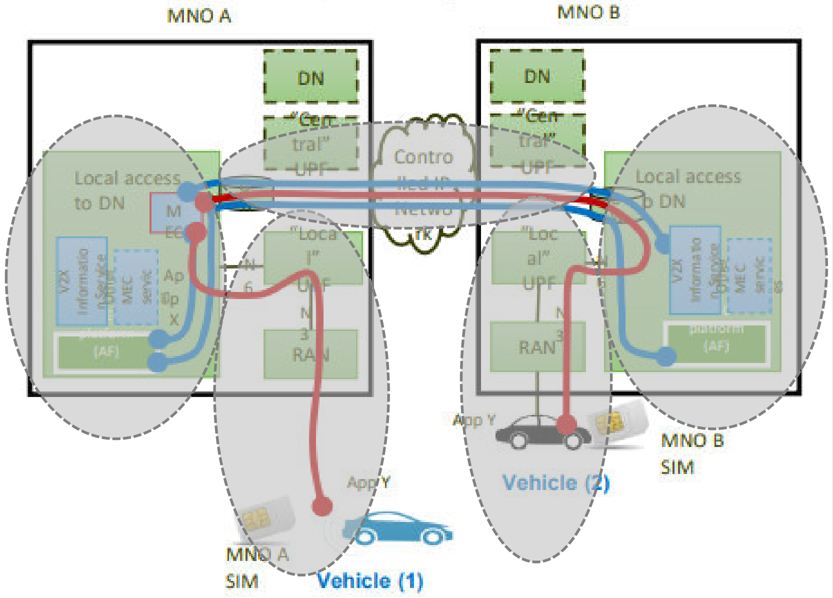
Scenario 1



- Presence of MEC application: **vehicle (1): MNO A vehicle (2): MNO B**
- Presence of MEC platform: **vehicle (1): MNO A vehicle (2): MNO B**
- Vehicle subscriptions: **vehicle (1): MNO A vehicle (2): MNO B**
- Available interconnection between MNOs: **Controlled IP network**
- Roaming: **No**

Both MNO A and MNO B have MEC platform and MEC application X

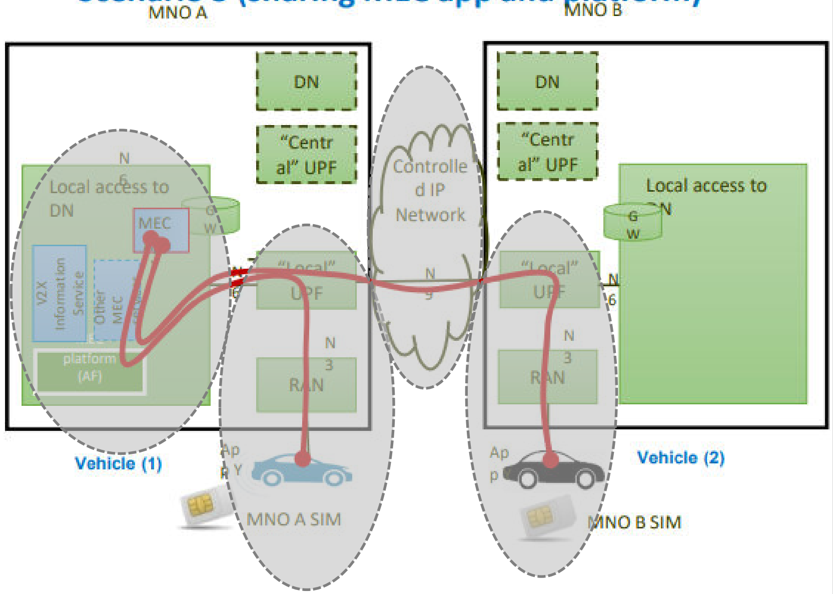
Scenario 2 (sharing MEC app)



- Presence of MEC application: **vehicle (1): MNO A vehicle (2): MNO B**
- Presence of MEC platform: **vehicle (1): MNO A vehicle (2): MNO A**
- Vehicle subscriptions: **vehicle (1): MNO A vehicle (2): MNO B**
- Available interconnection between MNOs: **Controlled IP network**
- Roaming: **No**

MEC application X is available only in MNO A

Scenario 3 (sharing MEC app and platform)

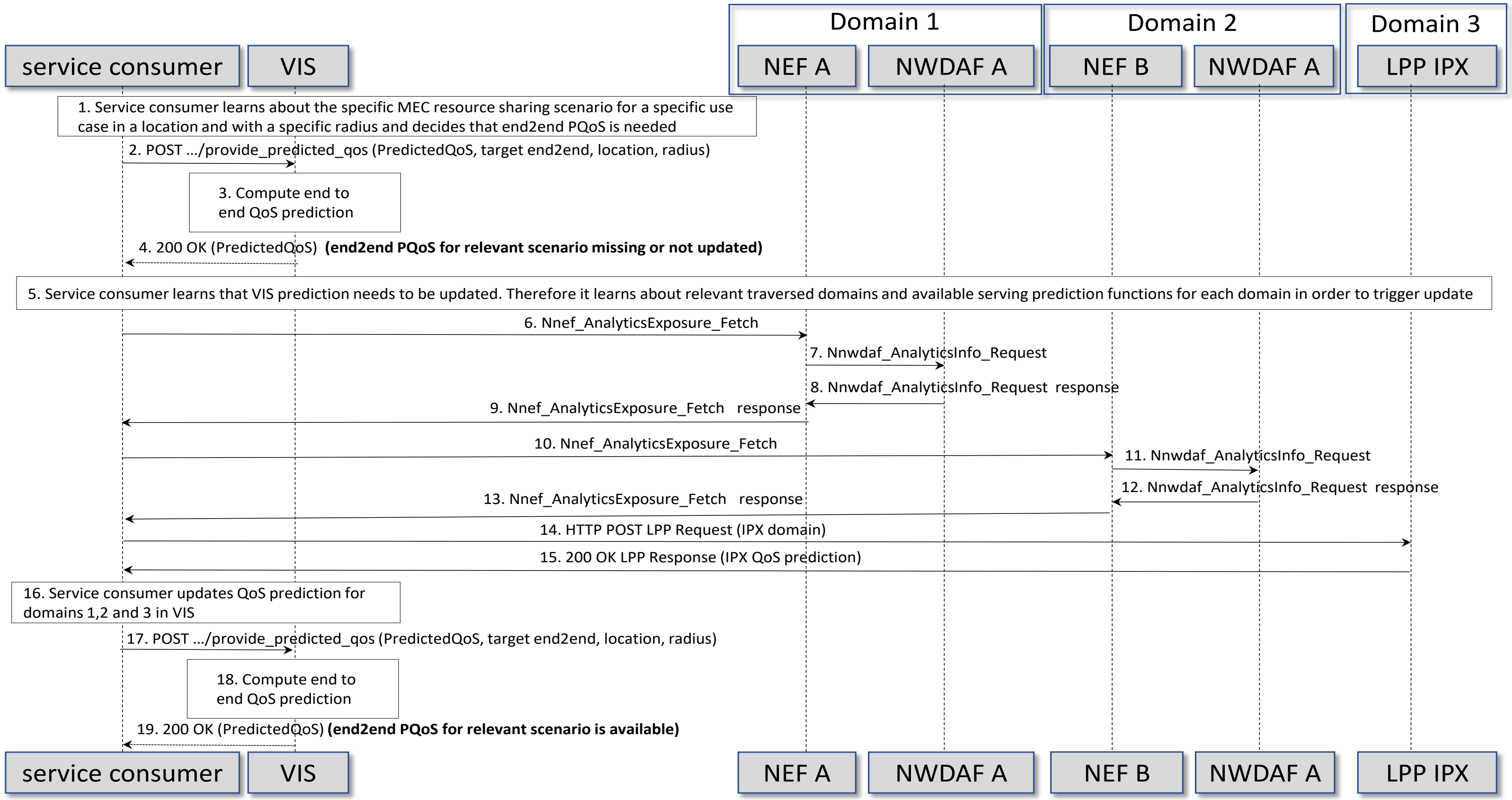


- Presence of MEC application: **vehicle (1): MNO A vehicle (2): MNO A**
- Presence of MEC platform: **vehicle (1): MNO A vehicle (2): MNO A**
- Vehicle subscriptions: **vehicle (1): MNO A vehicle (2): MNO B**
- Available interconnection between MNOs: **N9**
- Roaming: **No**

MEC platform and MEC application X is available only in MNO A

How V2X Information Services (VIS) API can support predictive edge analytics in multi-domain MEC deployments

- 5GAA gMEC4AUTO contributed to ETSI MEC GS 030 significant enhancements of the VIS in order to support predictive edge analytics in **multi-domain MEC deployments**
- VIS can now cooperate with PFs in multiple domains by receiving domain-specific analytics and **provide** to MEC applications and platforms **consolidated views on the multi-domain end-to-end user plane link**
- *Note*: **VIS complements 3GPP network prediction service** (based on NWDAF) or other domain-specific PFs



1. Service consumer learns about the specific MEC resource sharing scenario for a specific use case in a location and with a specific radius and decides that end2end PQoS is needed

2. POST .../provide_predicted_qos (PredictedQoS, target end2end, location, radius)

3. Compute end to end QoS prediction

4. 200 OK (PredictedQoS) **(end2end PQoS for relevant scenario missing or not updated)**

5. Service consumer learns that VIS prediction needs to be updated. Therefore it learns about relevant traversed domains and available serving prediction functions for each domain in order to trigger update

6. Nnef_AnalyticsExposure_Fetch

7. Nnwdaf_AnalyticsInfo_Request

8. Nnwdaf_AnalyticsInfo_Request response

9. Nnef_AnalyticsExposure_Fetch response

10. Nnef_AnalyticsExposure_Fetch

11. Nnwdaf_AnalyticsInfo_Request

12. Nnwdaf_AnalyticsInfo_Request response

13. Nnef_AnalyticsExposure_Fetch response

14. HTTP POST LPP Request (IPX domain)

15. 200 OK LPP Response (IPX QoS prediction)

16. Service consumer updates QoS prediction for domains 1,2 and 3 in VIS

17. POST .../provide_predicted_qos (PredictedQoS, target end2end, location, radius)

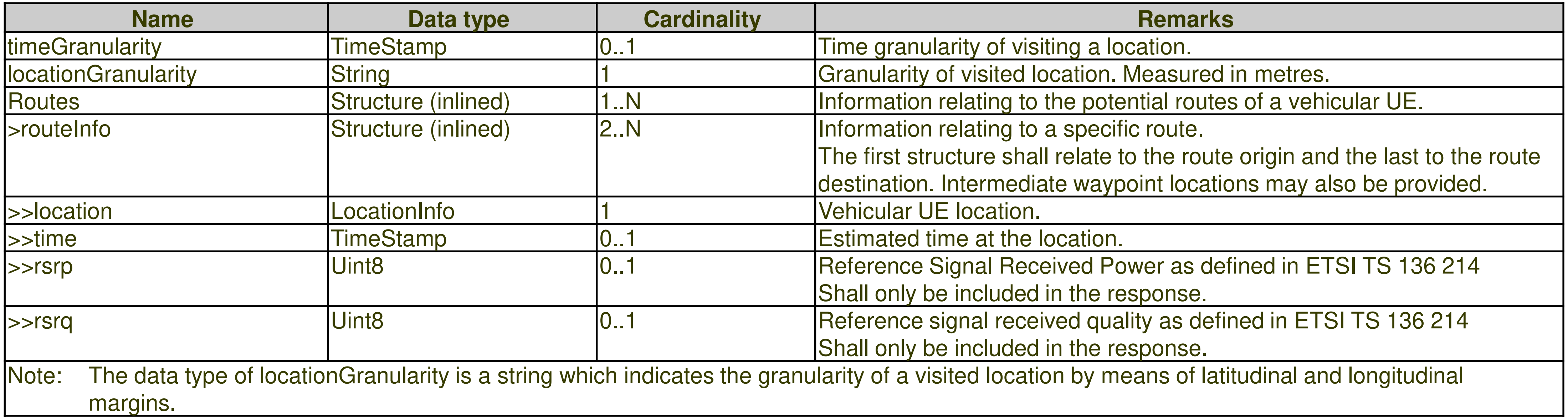
18. Compute end to end QoS prediction

19. 200 OK (PredictedQoS) **(end2end PQoS for relevant scenario is available)**

Figure - VIS cooperating with other prediction functions

Enhancements to the VIS data model for QoS prediction (1 of 2)

PredictedQoS data type before 5GAA input (source: Table 5 of ETSI GS MEC 030 v2.1.1)



Name	Data type	Cardinality	Remarks
timeGranularity	TimeStamp	0..1	Time granularity of visiting a location.
locationGranularity	String	1	Granularity of visited location. Measured in metres.
Routes	Structure (inlined)	1..N	Information relating to the potential routes of a vehicular UE.
>routeInfo	Structure (inlined)	2..N	Information relating to a specific route. The first structure shall relate to the route origin and the last to the route destination. Intermediate waypoint locations may also be provided.
>>location	LocationInfo	1	Vehicular UE location.
>>time	TimeStamp	0..1	Estimated time at the location.
>>rsrp	Uint8	0..1	Reference Signal Received Power as defined in ETSI TS 136 214 Shall only be included in the response.
>>rsrq	Uint8	0..1	Reference signal received quality as defined in ETSI TS 136 214 Shall only be included in the response.
Note: The data type of locationGranularity is a string which indicates the granularity of a visited location by means of latitudinal and longitudinal margins.			

Issues on the data model of v 2.1.1:

- Only supports single UE prediction, not E2E paths. In case of E2E paths, how to identify uniquely those paths?
- Does not support a notice period (by when is the prediction required)
- RSRP and RSRQ are not the best representation of QoS for an application. Do not take into account of differentiated traffic treatment
- Does not include confidence: how good is the prediction?

Enhancements to the VIS data model for QoS prediction (2 of 2)

PredictedQoS data type after 5GAA input (source: Table 6.2.6-1 of ETSI GS MEC 030 v3.1.1)

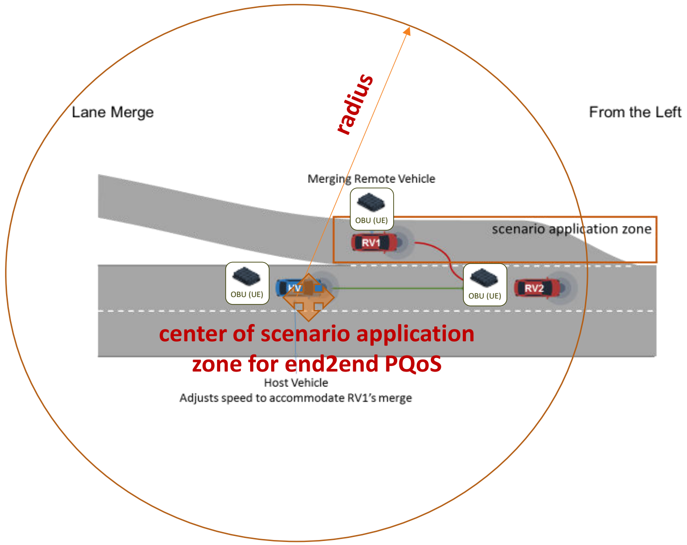
Name	Data type	Cardinality	Remarks
predictionTarget	Enum (inlined)	1	Indicates target of QoS prediction. Valid values: 1. SINGLE_UE_PREDICTION: The predicted QoS is to be intended as journey-specific for a requesting vehicular UE. 2. E2E_APPLICATION_INSTANCE_PREDICTION: The E2E user plane link between two V2X application instances, where one instance relates to a single vehicular UE and the other instance to an application instance within another network, i.e. either another vehicular UE as in the V2N2V casem or an infrastructure element as in the V2N2I case. Shall only be included in the request.
timeGranularity	TimeStamp	0..1	Time granularity of visiting a location.
locationGranularity	String	1	Granularity of visited location. Measured in metres.
noticePeriod	TimeStamp	0..1	Information on when the predicted QoS is needed at the service consumer interface. The value of the notice period depends on the application reaction that has to be triggered by the service consumer. The value of the notice period shall be equal or a multiple of the timeGranularity, if it is present. If present, it shall only be included in the request.
predictionArea	Structure (inlined)	0..1	Geographical area including the two ends of the user plane link between two V2X application instances. It shall only be present when “predictionTarget” = E2E_APPLICATION_INSTANCE_PREDICTION
>center	LocationInfo	1	Center of geographical area including the two ends of the user plane link between two V2X application instances.
>radius	String	1	Radius of geographical area including the two ends of the user plane link between two V2X application instances. Measured in meters.
routes	Structure (inlined)	1..N	Information relating to the potential routes of a vehicular UE. Shall only be present when "predictionTarget" = "SINGLE_UE_PREDICTION".
>routeInfo	Structure (inlined)	2..N	Information relating to a specific route. The first structure shall relate to the route origin and the last to the route destination. Intermediate waypoint locations may also be provided.
>>location	LocationInfo	1	Vehicular UE location.
>>time	TimeStamp	0..1	Estimated time at the location.
~~>>rsrp~~	~~Uint8~~	~~0..1~~	~~Reference Signal Received Power as defined in ETSI TS 136 214 [i.13].~~ ~~Shall only be included in the response.~~
~~>>rsrq~~	~~Uint8~~	~~0..1~~	~~Reference Signal Received Quality as defined in ETSI TS 136 214 [i.13].~~ ~~Shall only be included in the response.~~
qos	Structure (inlined)	1	Predicted QoS at the related time and vehicular UE location. Shall only be included in the response.
>stream	Structure (inlined)	1..N	Predicted QoS at the related time and vehicular UE location for the specific data stream. In case of the 3GPP network, this is mapped to a QoS flow. Stream needs to also contain the stream ID which, in case of the 3GPP network, can be mapped on to the 5QI or QCI.
>>qosKpi	Structure (inlined)	1..N	This structure contains the prediction for a specific QoS KPI related to a given data stream.
>>>kpiName	String	1	The name of the KPI (e.g. latency, UL bitrate, etc.). It can be included in the request and in the response.
>>>kpiValue	String	1	Information on the predicted value for the specific QoS KPI. It can be in different forms, such as upper bound and lower bound, CDF, actual value, etc. Shall only be included in the response.
>>>confidence	String	0..1	Confidence of the prediction, as returned by the relevant domain PF. The value and the measurement of the confidence depends on the SLA. Shall only be included in the response.
Note: The data type of locationGranularity is a string which indicates the granularity of a visited location by means of latitudinal and longitudinal margins.			

Other possible VIS enhancements (FFS):

V2X message interoperability and QoS prediction

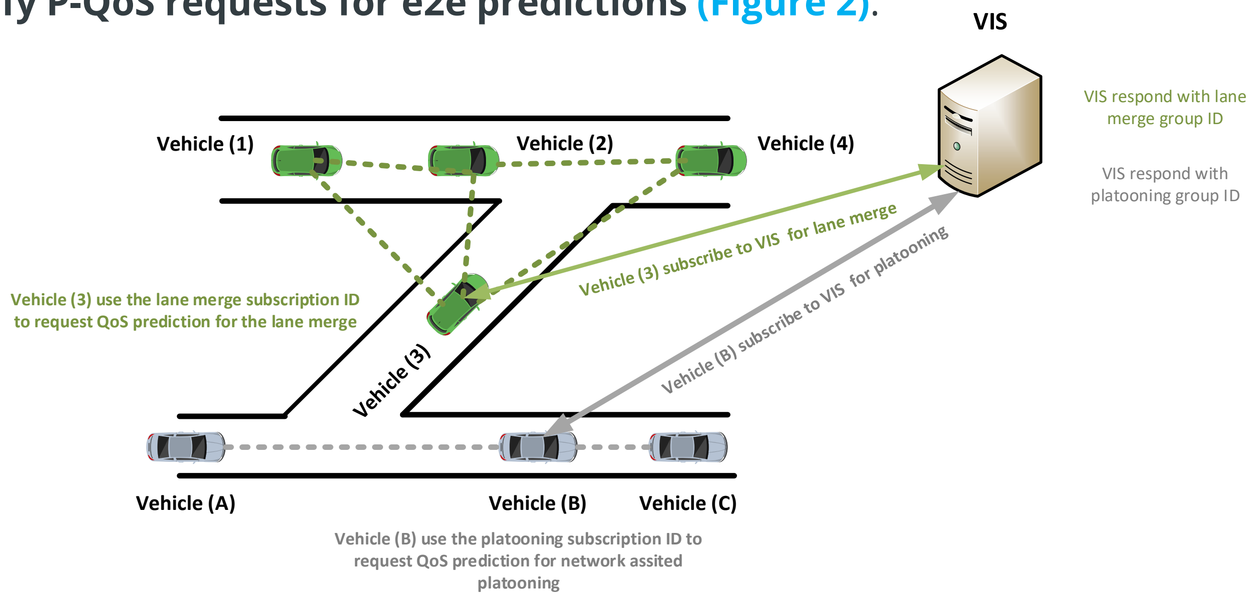
VIS API for **V2X message interoperability (*)** can be used to publish/subscribe and receive notifications from different vehicle OEMs or operators, decoupling the application from specific message brokers:

1. **Predicted message latency can be embedded in the information returned to the V2X application instance**. For example, if the latency is too high the application may decide not to wait/not to send a specific V2X message and determine related countermeasures (e.g. abort service or implement a decision according to data that is locally available instead of data cooperatively acquired form other vehicles). In this case:
   - It requires a **unique way to identify the set of end-to-end connections** (Figure 1) associated with a use case or service request.
2. V2X message interoperability Subscription ID can be used to **identify P-QoS requests for e2e predictions** (Figure 2).



Lane Merge
radius
From the Left
Merging Remote Vehicle
OBU (UE)
RV1
scenario application zone
OBU (UE)
HV
OBU (UE)
RV2
center of scenario application zone for end2end PQoS
Host Vehicle
Adjusts speed to accommodate RV1's merge

Figure 1 - Road traffic scenario of lane merge with three vehicles; the end-to-end user plane links for this scenario are HV-RV1, RV1-RV2 and HV-RV2



VIS
VIS respond with lane merge group ID
VIS respond with platooning group ID
Vehicle (1)
Vehicle (2)
Vehicle (4)
Vehicle (3) use the lane merge subscription ID to request QoS prediction for the lane merge
Vehicle (3) subscribe to VIS for lane merge
Vehicle (3)
Vehicle (B) subscribe to VIS for platooning
Vehicle (A)
Vehicle (B)
Vehicle (C)
Vehicle (B) use the platooning subscription ID to request QoS prediction for network assited platooning

Figure 2 - Example of the usage of subscription ID for the request of QoS predictions for lane merge and platooning use cases

(*) ETSI GS MEC 030 v3.1.1 Section 5.5.10

Network slicing for multi-domain MEC applications

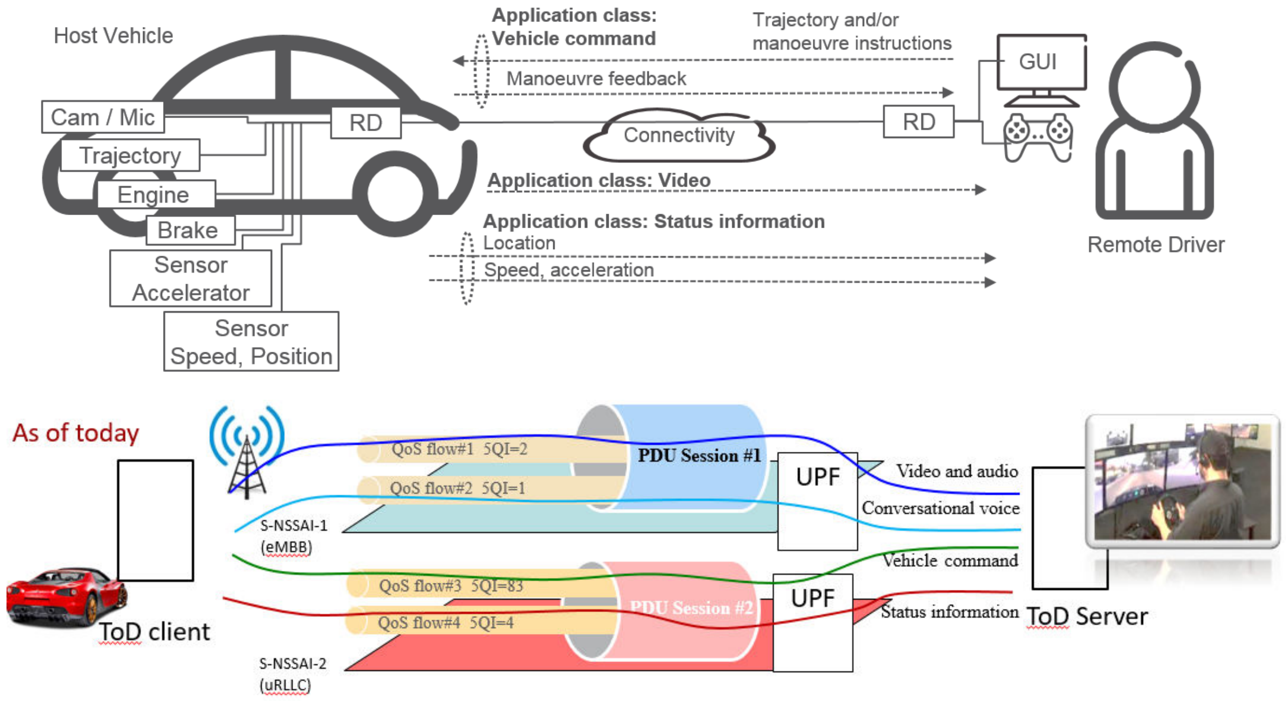
A MEC application using multiple slices

Relevant for GSMA

- Connectivity for a V2X application in the MEC environment may benefit from using **one or more S-NSSAIs** on **different SSTs**.

- Different EAS may be associated to different traffic (mapped on different slices). **New requirements for EAS discovery and URSP** may need to be studied.

- Support of different S-NSSAIs (on required SSTs) and different EASs may not always be possible **along the entire route** of a vehicle moving **over a wide geographical area, operator networks and country borders.**



Tele-operated Driving using two SSTs of eMBB and URLLC type

- Multi-domain applications may benefit from **a new prediction functionality** which **checks availability of slices and EASs along the route** and send prompts if gaps (slices or EASs) are identified.
- E.g., route planning based on the services that may be needed along the planned path.

MEC Security:
threats and mitigation strategies in multi-MNO scenarios

gMEC4AUTO Task 4

gMEC4AUTO Task 4: cybersecurity for edge computing

- Approach:
  - the 5GAA approach to MEC cybersecurity, from automotive perspective, is following the work started in MEC4AUTO
  - Here, the reference architecture is targeting MEC systems deployed in Multi-MNO, Multi-OEM and multi-vendor environments.
  - As a consequence, this document targeted a very specific and tailored scenario, thus covering a smaller part of the entire "*galaxy*" of cybersecurity.

Highlights from the report:

- The report analyzed the main **threats** from **security**, **privacy** and **trust** perspectives,
- Provided an overview of the most relevant **mitigation strategies** available in the industry, by evaluating them in terms of suitability for the 5GAA gMEC4AUTO architecture and targeted use cases.
- Finally, the report highlighted possible **gaps** and future work in that perspective.

gMEC4AUTO approach to MEC Security (1/2)

- The previously published MEC4AUTO report described at high level the elements to be secured by the system, by providing some examples of security boundaries (identified by the MEC system itself and the associated security services that the MEC hosts for connected vehicles), in some key cases of interest:
  - Security boundary in a single OEM use case
  - Security boundary in a single OEM, multi-MNO MEC use case
  - Security boundary in a multi-MNO MEC roaming use case

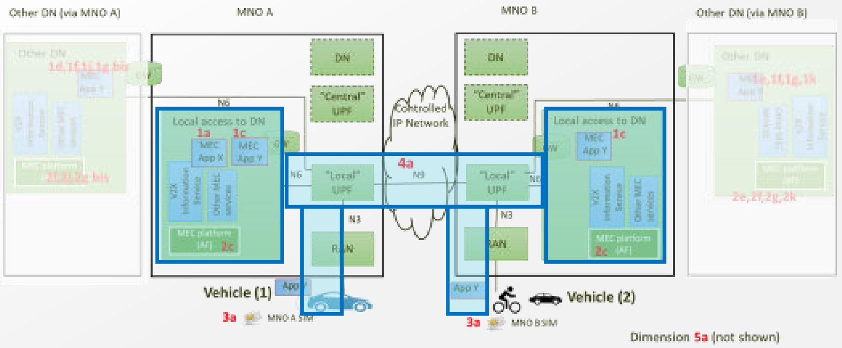
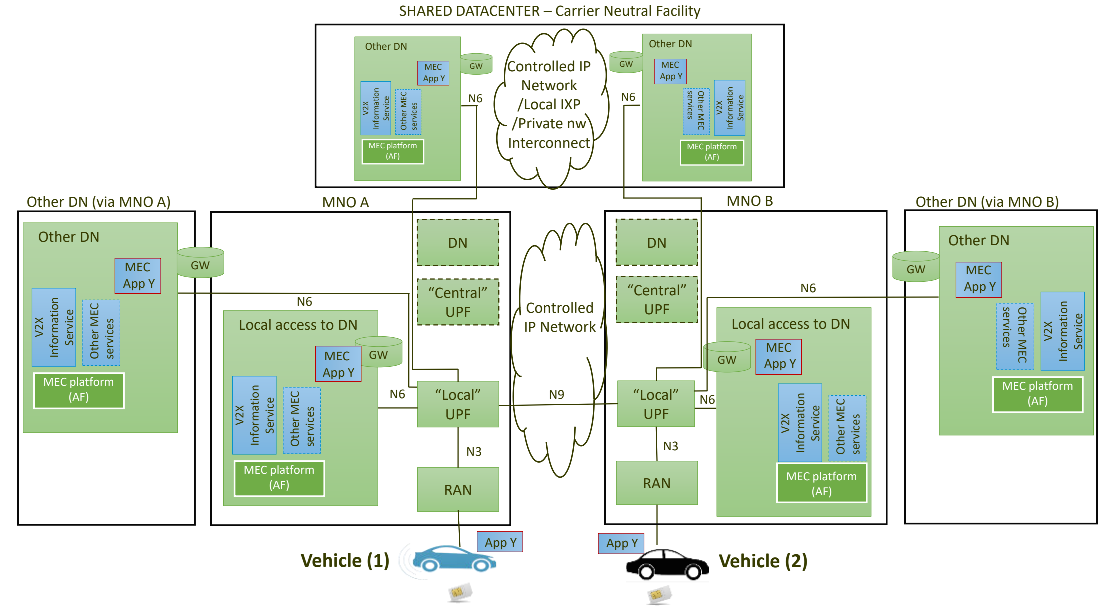


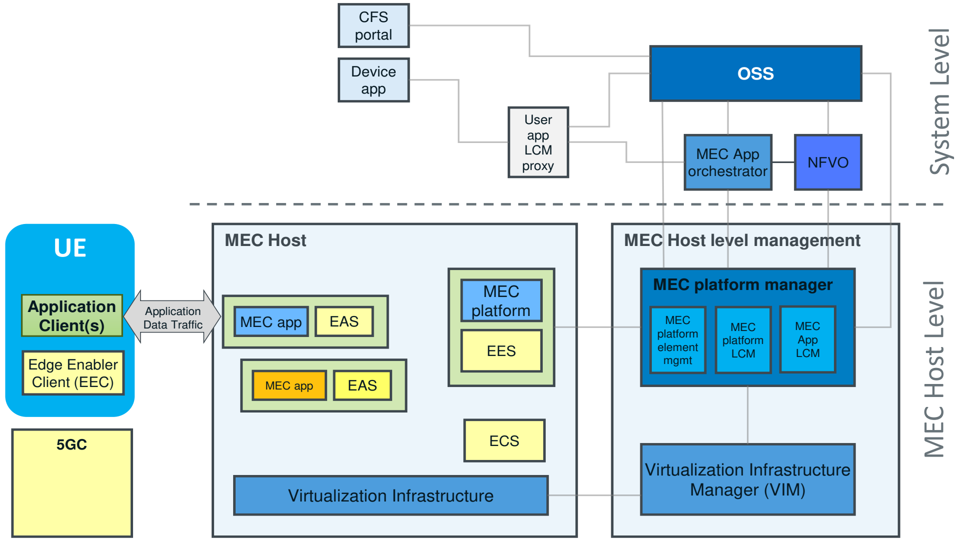
Figure - Example of security boundaries for Trial #3 (described in [30])



The updated gMEC4AUTO architecture expands the set of security boundaries, as it also introduces the possibility of *hosting MEC platforms and applications in other data networks (DN)* via the MNOs, other than the *presence of shared datacenters* (as carrier neutral facilities).

gMEC4AUTO approach to MEC Security (2/2)

- Regarding single MEC systems, threat factors can be broadly categorized based on various areas of vulnerabilities: from Platform Integrity to Virtualisation and Containerization, Physical security, APIs and Regulatory issues.
- More in detail, all MEC security threats can be at various levels (figure below): MEC App / EAS / other applications, MEC platform / EES, NVFI and infrastructure (that may include implicitly also security issues at real estate level), management & orchestration (also possibly including non-standard orchestration frameworks).



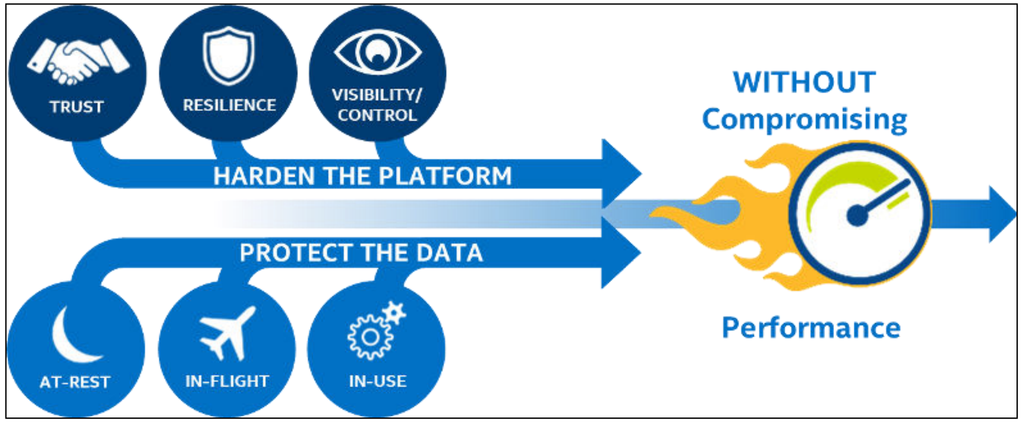
Functional elements of the MEC synergized architecture that may be subjected to security threats [36])

- Tailoring the security threats to gMEC4AUTO architecture (multi-MNO scenarios), here are the main aspects to be considered:
  - Workloads are outside the PLMN trusted domain but running on external ECSP domains.
  - Mutual trust between MEC apps and MEC platforms, meaning that 1) in principle the edge application from MNO A should be considered as though it would be running in a “hostile” environment (MNO B) and also vice-versa, 2) a platform operated by MNO B is hosting “unknown” applications which may endanger the system.
  - Security threats are also related to all the communication links (both data plane and control plane), meaning that all relevant communication channels can be untrusted, in principle.
  - Furthermore, devices can be a source of security issues; for example, the car but also the VRU, including smartphones and other connected devices.

gMEC4AUTO: security landscape

- Many potential threats have been identified (and divided into three categories: **security** threats, **privacy** threats and **trust** concerns) to secure operations in this environment.
  - Note, this list is not exhaustive, but represents major categories of threats most likely encountered.

- As a high-level recommendation, security needs to be designed into **SW and HW** developments from the start
  - Indeed, the goal of gMEC4AUTO technical report is to shed some light on those aspects).



- Security threats in gMEC4AUTO architecture
  - Malware injection attacks (e.g. SQL)
  - Man-in-the-middle attacks (MitM)
  - Denial of service (DoS) attacks
  - Advanced persistent threat (APT)
  - Ransomware
  - Other attacks

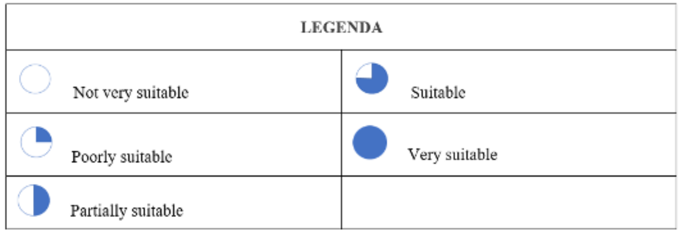
- Privacy threats in gMEC4AUTO architecture
  - Data privacy
  - Identity privacy
  - Location privacy during service migration

- Trust concerns in gMEC4AUTO architecture
  - Establishment of trust among different application servers
  - Secure and "stateful" application migration
  - Data location and lifecycle
  - Continuous authorization and authentication

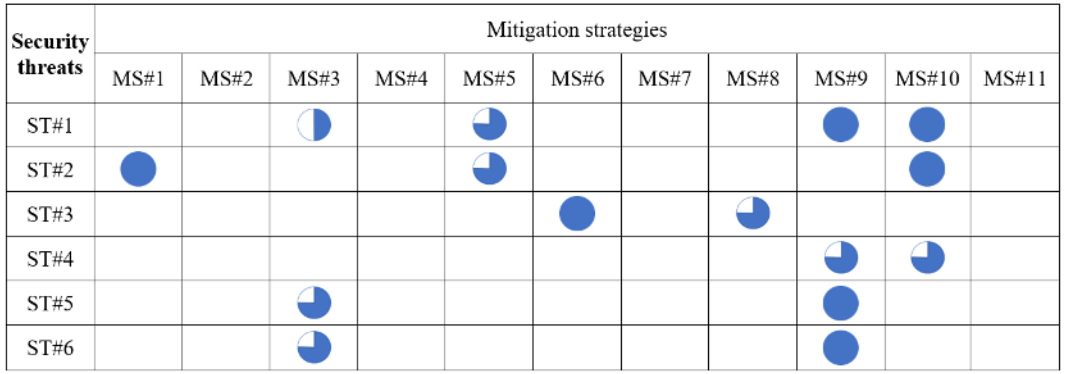
gMEC4AUTO: mitigation strategies

- Some of the most relevant mitigation strategies available in the industry:

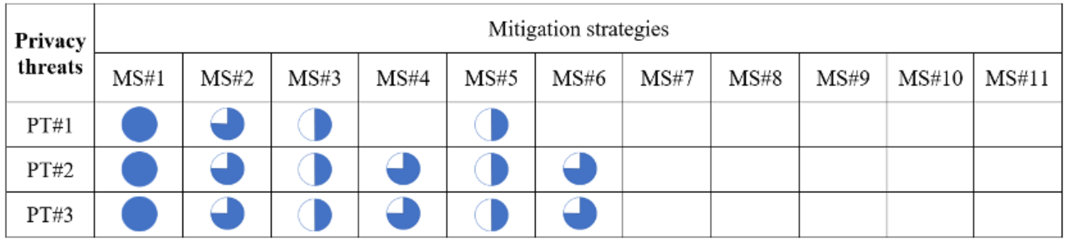
  - **MS#1** – Data plane encryption
  - **MS#2** – Security on control plane
  - **MS#3** – Security of containers
  - **MS#4** – Identity and authentication
  - **MS#5** – OAuth 2.0
  - **MS#6** – User application LCM proxy
  - **MS#7** – Security credential management
  - **MS#8** – Misbehaviour detection
  - **MS#9** – Attestation and HW root of trust (RoT)
  - **MS#10** – Chip-to-cloud assurance solutions in NFV
  - **MS#11** – Secure migration service



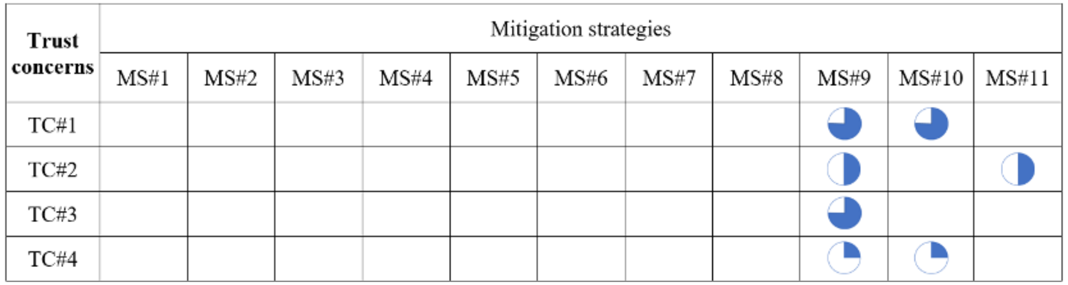
LEGENDA	
○ Not very suitable	◕ Suitable
◔ Poorly suitable	● Very suitable
◑ Partially suitable	



Security threats	Mitigation strategies										
	MS#1	MS#2	MS#3	MS#4	MS#5	MS#6	MS#7	MS#8	MS#9	MS#10	MS#11
ST#1			◑		◕				●	●	
ST#2	●				◕					●	
ST#3						●		◕			
ST#4									◕	◕	
ST#5			◕						●		
ST#6			◕						●		



Privacy threats	Mitigation strategies										
	MS#1	MS#2	MS#3	MS#4	MS#5	MS#6	MS#7	MS#8	MS#9	MS#10	MS#11
PT#1	●	◕	◑		◑						
PT#2	●	◕	◑	◕	◑	◕					
PT#3	●	◕	◑	◕	◑	◕					



Trust concerns	Mitigation strategies										
	MS#1	MS#2	MS#3	MS#4	MS#5	MS#6	MS#7	MS#8	MS#9	MS#10	MS#11
TC#1									◕	◕	
TC#2									◑		◑
TC#3									◕		
TC#4									◔	◔	

- These strategies are being evaluated in terms of suitability for the **gMEC4AUTO architecture**
  - Note: here the focus is on MEC systems deployed in multi-MNO, multi-OEM, and multi-vendor environments

Remarks on gMEC4AUTO security

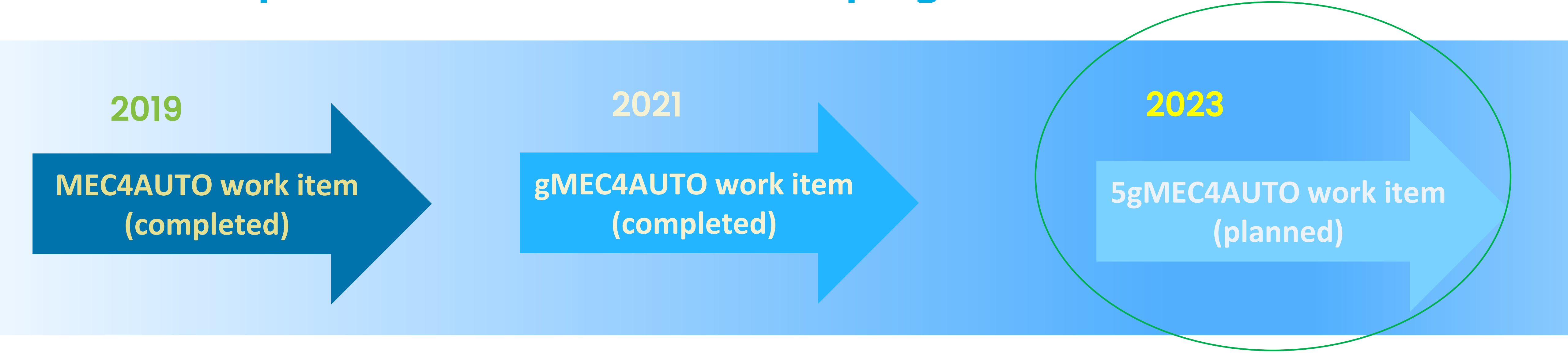
- In general, there are already many mitigation strategies available in the industry, that can be suitable for the 5GAA gMEC4AUTO architecture and targeted use cases.

- While security is better covered by existing tools, more work on privacy and trust may be needed (first in industry groups, and then in standard bodies).
- In particular:
  - further work is needed on standards to fully cover the specific needs on **identity protection**; some more work is needed to fully cover the specific needs on **location privacy**, while at the same time being capable to offer ubiquitous and global MEC services in the above-stated environments.
  - In particular, the need to offer MEC services across a federation could be in contrast with the concept of “separation of concerns” by OPG. This fundamental trade-off should be first resolved by industry associations such as GSMA (and also vertical market representatives, 5GAA) to effectively drive the standardization work on proper directions addressing industry needs.
  - Another conclusion is that trusted computing is a core enabler for measuring and validating the trustworthiness and resilience of a system. In this context, both **authentication** and **attestation** are prominent security constructions for creating assurances on platform integrity and the ability to protect data in accordance with various security levels and policies.
  - Overall, what is needed is a **trust architecture** and a dynamic trust assessment methodology enabling vehicles to continuously assess the level of trust that they can place on the MEC when consuming/using its services.

Moving ahead on Global MEC deployments…

Possible directions and future activities

The 5GAA path toward Global MEC deployments…



2019

MEC4AUTO work item (completed)

2021

gMEC4AUTO work item (completed)

2023

5gMEC4AUTO work item (planned)

MEC4AUTO (2019-2020) has established the foundation of MEC activities in 5GAA

- Architecture work, focus on Multi-MNO, Multi-OEM, Multi-vendor environments
- Analysis of MEC-relevant use cases (both from a technical and business points of view)
- Early analysis of security aspects (in collaboration with 5GAA WG7)
- MEC Trials planning

gMEC4AUTO (2021-2022) moved MEC to a trial phase

- Reporting the first Multi-MNO trials across different geos.
- Re-opening of TR on use cases (adding AVP), and working on MEC performance evaluation methodology
- Arch. enhancements inspired by trials (e.g., roaming cases, edge resource sharing); position paper on MEC to engage Road Operators (RO) and Traffic Authorities (RTA)
- 5GAA Inputs to MEC V2X API on E2E QoS predictions
- 5GAA participation to MEC Hackathon 2022 (organized by ETSI/LF Edge) – special prize on the best Automotive App
- Task dedicated on MEC security exploring the threats

5GAA companies are bringing ideas for future activities in 2023-2024

- Follow-up trials (+ demos co-located with events), permanent testbed facilities with ROs/RTAs (opportunity to engage more partners and customers). The aim is to create a blueprint for large-scale commercial deployments enabling MEC applications and creating the best business model fit.
- More work on edge application development engagement (e.g., Hackathons, collaborations with other ind. groups,..)
- Further work on additional use cases and MEC performance evaluation methodology → useful to better convince decision makers and speedup adoption
- Further work on MEC testing and interop., on biz aspects

Live Survey

Poll#2
(Questions Q3-Q6)

5GAA
Automotive Association

Q&A

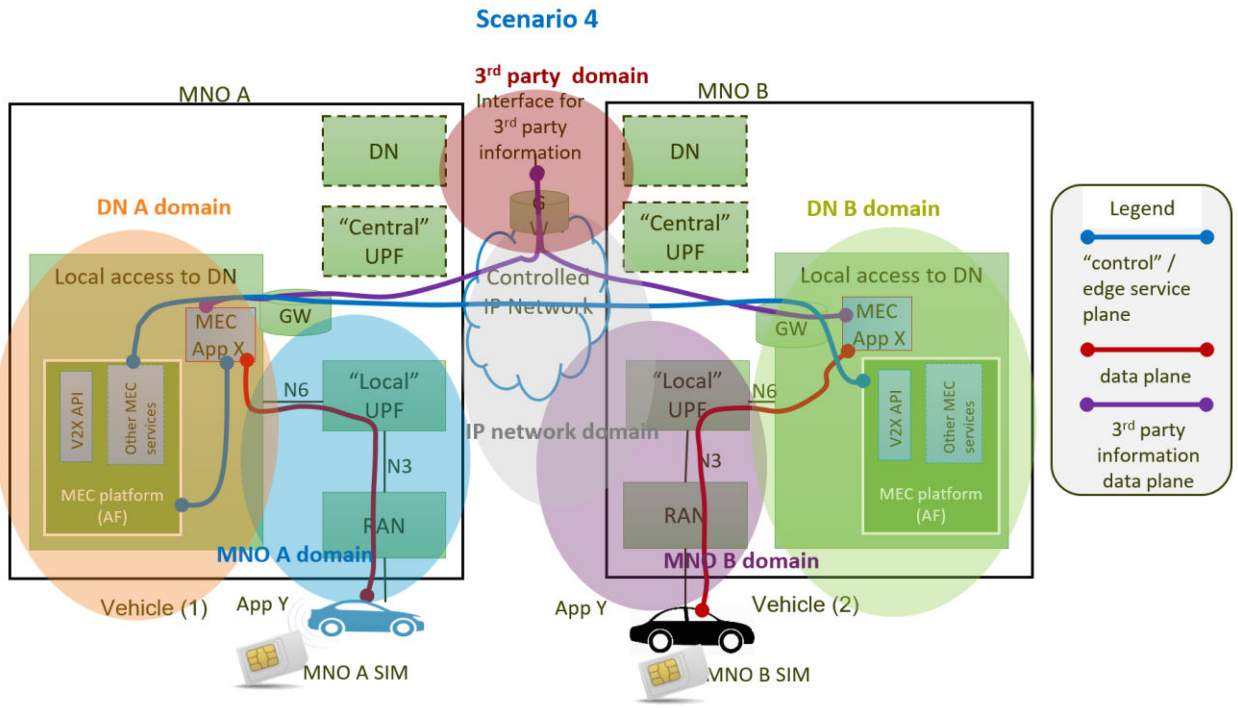
Thanks!

5GAA Automotive Association

BACKUP slides

MEC Scenarios and analytics domains

Scenario 4: MEC applications in MNO A and MNO B exchange information with a RTA or third party (V2N2I)



- Scenario 4 is equivalent to Scenario 1 + interface with third parties (e.g. road operator).
- An additional domain is added to the list for **third parties.**
- The MEC platform and application can also support the generation of analytics for this domain, either directly or in cooperation with a PF located in the third-party domain
- Analytics on user plane link with a third-party and indications of the 5 different prediction domains for the end-to-end link.