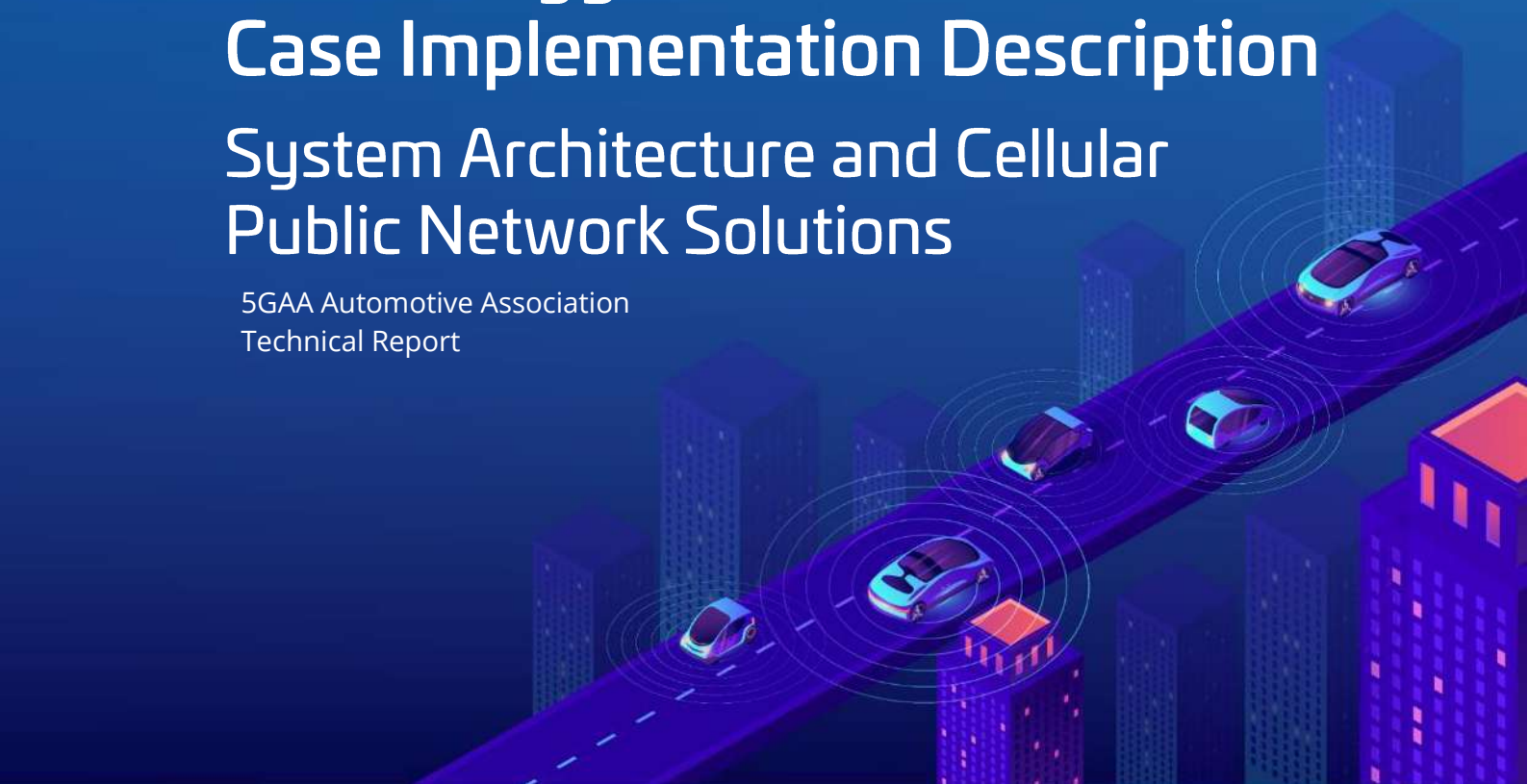
5GAA Automotive Association

Automated Valet Parking Technology Assessment and Use Case Implementation Description

System Architecture and Cellular Public Network Solutions

5GAA Automotive Association
Technical Report



CONTACT INFORMATION:

Executive Manager – Thomas Linget
Email: liaison@5gaa.org

MAILING ADDRESS:

5GAA c/o MCI Munich
Neumarkter Str. 21
81673 München, Germany
www.5gaa.org

.

VERSION:	Version 1.0
DATE OF PUBLICATION:	9 June, 2022
DOCUMENT TYPE:	Technical Report
EXTERNAL PUBLICATION:	Yes
DATE OF APPROVAL BY 5GAA BOARD:	9 May, 2022

Contents

Introduction

This 5GAA Technical Report presents the results of the 5GAA Work Items Use Case Implementation Description Phase II (UCID II) and Automated Valet Parking (AVP) with the focus on solutions using cellular public networks. Solutions using cellular non-public networks or short-range direct communication technologies are also in the scope of these Work Items, but the results will be published separately at a later stage.

1. Scope

The present document describes the system architecture and use-case implementation details of Automated Valet Parking Type-2 [3] with the focus on wireless communication solutions using cellular public networks. In addition to high-level and detailed communication sequences of the AVP Type-2 use case, the implementation considerations for cellular public network-based solutions are also elaborated considering AVP service deployment requirements.

2. References

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] ISO/FDIS 23374-1 Intelligent transport systems – Automated valet parking systems (AVPS) – Part 1: System framework, requirements for automated driving, and communication interface, May. 2022.[1]

[2] 5GAA A-200094, Technical Report, V2X Application Layer Reference Architecture, June 2020.

[3] 5GAA T-210023, Draft Use Case Description Automated Valet Parking, Bosch and BMW, March 2021

[4] 5GAA Technical Report, Safety Treatment in Connected and Automated Driving Functions, March 2021

[5] Ericsson Whitepaper, Ericsson Dynamic Network Slice Selection, 2022. https://www.ericsson.com/48fd7e/assets/local/networks-slicing/docs/ericsson-dynamic-network-slice-selection-2022.pdf

[6] GSMA, eSIM Whitepaper – The What and How of Remote SIM Provisioning, March 2018. https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf

[7] C-V2X Use Cases and Service Level Requirements Volume II, v2.1, February 2021, 5GAA_T-200116, (https://5gaa.org/news/c-v2x-use-cases-and-service-level-requirements-volume-ii/)

[8] https://www.telekom.com/en/media/media-information/archive/automated-valet-parking-with-5g-648970

3. Definitions, symbols and abbreviations

3.1. Definitions

For the purposes of the present document, the following definitions given in ISO 22374-1:2021 and the following apply:

[1] Standard ISO 23374-1 is expected to be planned in Dec. 2022.

AVP network: communication network used in a parking facility to support AVP services, e.g. for data communication between the subject vehicle and the AVPS and between the subject vehicle and its OEM Application Server (vehicle backend).

3.2. Symbols

For the purposes of the present document, the following symbols apply:

OB	Operator backend
P	Automated valet parking facility management
R	Remote vehicle operation
U	User frontend
UB	User backend
V	On-board vehicle operation
VB	Vehicle backend

3.3. Abbreviations

For the purposes of the present document, the following abbreviations apply:

5QI	5G QoS Identifier
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
APP	Application
AS	Application Server
AVP	Automated Valet Parking
AVPC	AVP Control
AVPS	AVP System
AVP FM AS	AVP Facilities Management Application Server
AVP SP App	AVP Service Provider App
AVP SP AS	AVP Service Provider Application Server
E2E	End-to-End
GBR	Guaranteed Bit Rate
HV	Host Vehicle
IF	Interchange Function
KPI	Key Performance Indicators
MEC	Mobile Edge Computing
MNO	Mobile Network Operator
OB	OEM Backend
OEM	Original Equipment Manufacturer
OEM AS	OEM Application Server
OEM App	OEM Application
PDB	Packet Delay Budget
PDU	Packet Data Unit
PER	Priority Error Rate
QCI	QoS Class Identifier
QoD	QoS on Demand
QoS	Quality of Services
RV	Remote Vehicle
RVO	Remote Vehicle Operation
SLR	Service Level Requirements
ToD	Tele-operated Driving
User App	User Application
User SP AS	User Service Provider Application Server
V2X	Vehicle-to-Everything
VMC	Vehicle Motion Control

4. System architecture

System architecture described in this section is based on the V2X application layer reference architecture agreed in 5GAA [2], as shown in Figure 1.

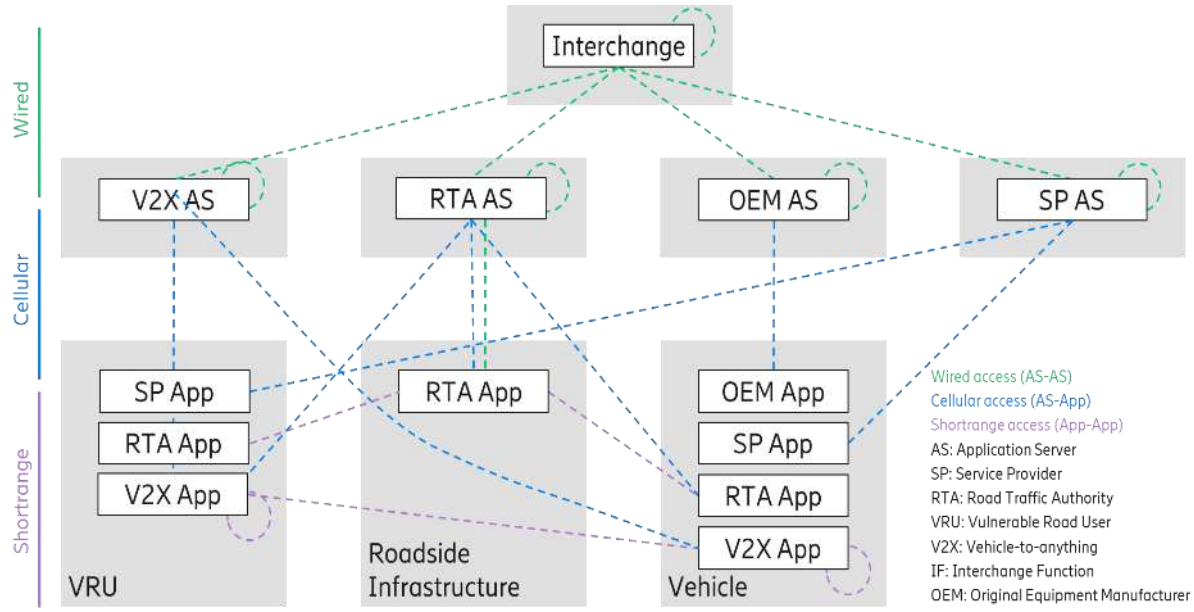
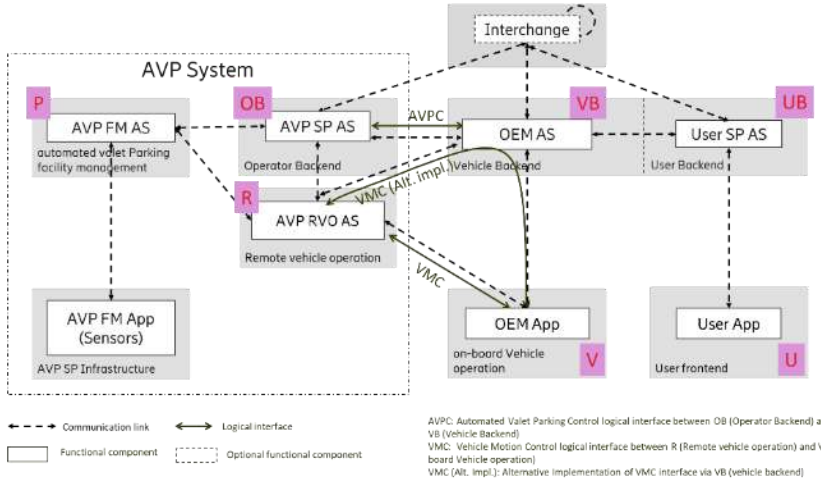


Figure 1: 5GAA V2X application layer reference architecture [2]

The next figure shows the application layer system architecture for the implementation of AVP Type-2 use case.



5GAA App. Layer System Architecture	ISO 23374-1 System Architecture
AVP Service Provider Application Server (AVP SP AS)	Operator Backend (OB)
AVP Remote Vehicle Operation Application Server (AVP RVO AS)	Remote vehicle operation (R)
OEM Application Server (OEM AS)	Vehicle Backend (VB)
OEM Application (OEM App)	on-board Vehicle operation (V)
User Service Provider Application Server (User SP AS)	User Backend (UB)
User Application (User App)	User frontend (U)
AVP Facility Management Application Server (AVP FM AS)	automated valet Parking facility management (P)
AVP Facility Management Application (AVP FM App)	
Interchange Function (IF) (Information broker for service discovery and scalability in real deployment with multiple OEMs and AVP SPs.)	(The Interchange Function is out scope of the ISO standard)

Figure 2: Application-level system architecture for AVP Type-2

Functional components in the system include:

AVP Service Provider Application Server (AVP SP AS), also known as Operator Backend (OB) in [1]

- The AVP SP AS interacts with the OEM AS and User SP AS via backend communications to provide AVP services to the user. Tasks of AVP SP AS include at least:
    - Managing parking facility availability;
    - Checking compatibility between vehicle and parking facility;
    - Dispatching vehicle into driverless operation;
    - Via OEM AS, handing over authority (rights and ability to perform tasks on the vehicle) with user;
    - Forwarding information between AVP RVP AS (remote vehicle operation) and OEM AS.
- The AVP SP AS communicates with the AVP FM AS and AVP RVO AS within the AVPS.

AVP Remote Vehicle Operation Application Server (AVP RVO AS), also known as Remote vehicle operation (R) in [1]

- The AVP RVO AS for Remote Vehicle Operation receives information (e.g. infrastructure sensor data) from the AVP FM AS. The AVP RVO AS in turn calculates the vehicle manoeuvre trajectory and provides instructions to the OEM App in the vehicle using the VMC logical interface. The AVP RVO AS communicates with the AVP SP AS for service AVP service management.

Original Equipment Manufacturer Application Server (OEM AS), also known as Vehicle Backend (VB) in [1]

- The OEM AS at the OEM vehicle backend offers services to the vehicles manufactured by the OEM and to its drivers and passengers by communicating with the OEM App. It communicates with the AVP SP AS and User SP AS via backend connectivity.
- OEM AS is responsible of remote engagement / disengagement of AVP service of OEM App in the vehicle.

Original Equipment Manufacturer Application (OEM App), also known as on-board Vehicle operation (V) in [1]

- The OEM App integrates services offered by the OEM AS into vehicles. For the AVP service, it performs the on-board vehicle operation following manoeuvre instructions received via the VMC logical interface, either directly from the AVP RVO AS or via the OEM AS. In this sense, the OEM App also takes the role of remote application for the AVP RVO AS.

User Service Provider Application Server (User SP AS), also known as User Backend (UB) in [1]

- The User SP AS at the User Backend, which can be hosted by the OEM User Backend, offers services for end users by communicating with the User App, e.g. installed on the user's smart phone or at the fleet management level. The User SP AS also communicates with the OEM AS to receive AVP service-related information from the AVP SP AS, and it sends AVP service requests from the end user.

User Application (User App), also known as User Frontend (U) in [1]

- The User App provides the services offered by User SP AS to the end user, e.g. via the smart phone App or the fleet management system.

AVP Facility Management Application Server (AVP FM AS), also recognised as part of automated valet Parking facility management (P) in [1]

- The AVP FM AS manages the local AVP system, including parking facility gates and sensors installed at or in the local infrastructure, etc. It communicates with the AVP SP AS and the AVP RVO AS executes the AVP service commands from the AVP SP AS and AVP RVO AS. It also provides infrastructure sensor data to the AVP RVO AS, to support remote vehicle operation.

AVP Facility Management Application (AVP FM App), also recognised as part of automated valet Parking facility management (P) in [1]

- The AVP FM App integrates the services and functions provided via the AVP FM AS into the AVP system infrastructure, e.g. the parking facility gate and infrastructure sensors. It provides infrastructure sensor data to AVP FM AS and executes commands from AVP FM AS.

Interchange Function (IF)

- Given the potentially large number of different AVP Service Providers (AVP SP) in real deployment scenarios, Interchange Functions are needed to automate the discovery of AVP SPs and scale up communications between AVP SP ASs and OEM ASs, to avoid full mesh connectivity. The IF is out scope of the ISO standard [1].

Figure 2 above also shows the logical interfaces, for which the implementation details are described in Section 5.

- **AVPC**: Automated Valet Parking Control logical interface between the OB AVP SP AS (OB) and OEM AS (VB) for management and control signaling communications among AVP services (e.g. authentication and authorisation information, network information, service and server discovery, AVP service requests and reservations, etc.

  Note: this logical interface may also be implemented via the Interchange Function to improve the scalability of the system.

- **VMC**: Vehicle Motion Control logical interface between the AVP RVO AS (R) and OEM App (V) for communicating vehicle motion control information (e.g. driving commands and instructions from the AVP RVO AS and vehicle status information from the OEM App). This logical interface can be implemented without going through the OEM AS (VB) or OEM AS (VB), as shown in Figure 2.

  - The VMC interface can be implemented without going through the OEM Backend, but for security reasons the VMC interface needs to be set up under the supervision of the OEM Backend.

  - As an alternative implementation option for automotive OEMs wanting the communication to and from vehicles to go via their backend systems – in order to utilise existing firewall, filters etc. – the VMC interface can be implemented via the OEM Backend. This option could potentially make it easier to modify interaction with parking providers and to provide/introduce new features for end customers, as the bulk of the complexity is handled in OEM Backend systems.

The communication domain between application servers and within the AVP system is typically done via secured interconnections between trusted actors via the internet. This communication domain is also commonly known as ‘backend communication’.

The communications between Application Servers (AS) and their respective Apps (clients) typically use cellular networks spanning different generations.

5. Working assumptions and requirements for AVP use case implementation

Regardless of the wireless communication technology used, the requirements for AVP use case implementation include the following:

1. For security and privacy reasons, all communication links and logical interfaces in the AVP implementation architecture (Figure 2) shall be secured appropriately, e.g. secured through end-to-end (E2E) encryption or hop-by-hop communication links among trusted entities.
2. Trust shall be established between the OEM AS and AVP SP AS.
   A. The parking facility shall be ‘approved’ to provide the AVP service.
   B. Vehicles shall be ‘approved’ to use the AVP service.
   C. Trust for network access means:
      i. The vehicle and the (preferred) AVP network shall be mutually authenticated.
   D. Trust for applications means:
      i. The OEM AS and AVP SP AS shall be mutually authenticated before any AVP session.
      ii. For any AVP mission, the AVP RVO AS needs to be mutually authenticated with the connected OEM AS, if the VMC is implemented via the OEM AS, or with the OEM App, and if the VMC is implemented directly between the OEM App and AVP RVO AS.

3. When vehicles are in the parking facility, it shall be ensured that the OEMs have access and control at any time to their connected vehicles in a secure way.
4. A short vehicle connectivity interruption (at second level) shall be allowed during the drop-off (hand-over) and pick-up (hand-back) processes (e.g. due to possible network reselection within the AVP network). Note: the communication between OEM AS and AVP SP AS shall be possible and maintained.
5. Vehicles shall be able to enter power-saving mode when left in the parking facility.
6. Vehicles shall have the ability to be remotely activated (woken up) and reached by the authenticated entities, i.e. the corresponding OEM AS.
7. The user shall be able to get the vehicle back, in the event of an AVP system failure.
    A. In the worst case scenario (e.g. total power failure of the parking facility), the vehicle can be moved manually.
8. The vehicle shall flash its hazard lights during the establishment of the mission i.e. the 'vehicle hand-over task' supporting a vehicle identification procedure.
9. Vehicles to be parked shall be capable of executing the received manoeuvre instructions from the AVP RVO AS, e.g. driving direction, speed, acceleration, distance, as described in [1] for AVP service Type 2.

When a cellular public network is used for implementing an AVP use case, the following assumptions apply:

- Wireless connectivity shall be treated as an 'open-channel' for functional safety.
    - Note: when wireless communication is concerned, functional safety requirements are fulfilled using the open channel approach together with safety monitoring on both communication sides. With this approach the wireless communication network does not need to be developed according to ASIL or other similar safety schemes. [4]
- The AVP application layer protocol shall work with standard IT protocols and security methods (TLS, IP, etc.).
- When developing the communication solution between the vehicle and AVP system, the sensors in the infrastructure shall be already connected within the AVP, fulfilling the required network characteristics.
- Connectivity between Mobile Network Operators (MNOs) and AVP RVO AS shall utilise Quality of Service (QoS) mechanisms to guarantee Key Performance Indicators (KPIs) according to the defined and applicable Service Level Requirement (SLR) values. This can be realised through, for example, network design to ensure QoS, Mobile Edge Computing (MEC) deployments, etc.

6. Protocols

The below table summarises the main properties and requirements for the AVP use case realisation:

Category	Item	Description
	Use case name	Automated Valet Parking (AVP)
	Relation to other use cases	Tele-operated Driving (ToD) [7]
	Actors and roles	Automated Valet Parking Service (AVPS) Provider: provides the AVPS by means of Remote Vehicle (RV) motion guidance, after obtaining approval from the OEM Host Vehicle (HV): HV is able to park by receiving motion guidance from AVPS HV Automotive OEM: approves AVP operation of HV by AVPS Provider
	Information classification	Vehicle motion control information including both operational and functional safety information, transmitted between AVP RVO AS and OEM APP Parking management control information transmitted between OEM APP, OEM AS and AVP SP AS, such as service discovery, reservation, payment, and AVP network information, are needed to enable AVP services
Standards and technology	Access layer technology/ies	Cellular Uu interface in 4G and beyond systems for communicating with vehicles (Communication between OEM AS and AVP SP AS are done using wired communication)
	Network and transport layer technologies	IP with TCP/UDP with secure connections, i.e. TLS/DTLS
	Message standards	AVP application protocols need to be developed and standardised
	Framework	Standardised IP protocol stacks
Application requirements	Use case triggers	User device or OEM Backend starts AVP operation
	Required information in the vehicles	N/a
Network layer requirements	Required coverage	Cellular coverage in vehicle drop-off area and AVP operation area
	Required availability	N/a

7. AVP use case implementation flows

7.1. Overview of AVP use case procedure

In this chapter, the use case is mapped to the communication architecture and illustrated with sequence diagrams including main parameters conveyed. Figure 3 shows the events and vehicle states in the AVP service cycle, starting from the user who wants to park through to when the vehicle is handed back to the owner and resumes normal driving operations after the AVP service. The following subsections describe the high-level, detailed sequences/diagrams of communication in different AVP service stages, namely AVP service discovery and reservation, vehicle parking process, vehicle re-parking process, and vehicle retrieval process.

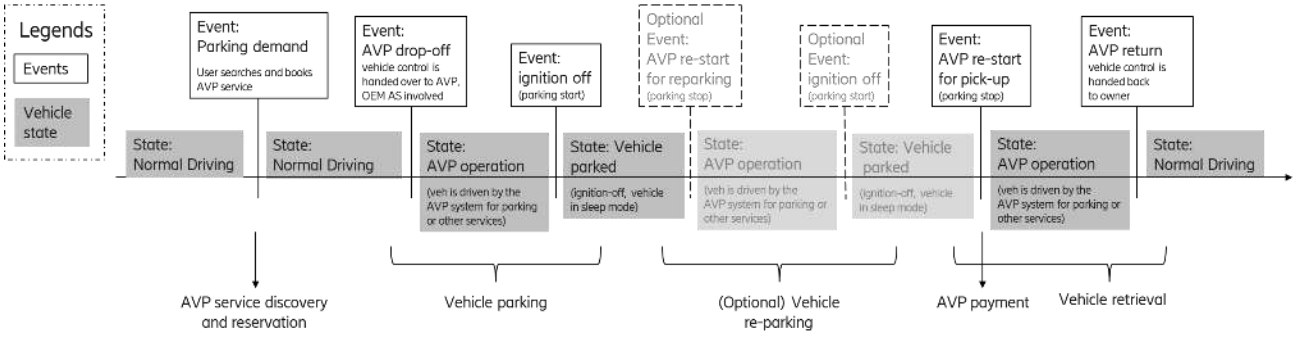


Figure 3: Events and vehicle states in AVP service cycle

7.2. High-level communication sequences

7.2.1 AVP services discovery, reservation, and payment

It is assumed that for a scalable, automated solution, methods are needed to announce the presence of available AVP parking/slots. This can be done in a number of ways, such as by using Advanced Message Queuing Protocol (AMQP) solutions where the AVP SP publishes the availability of AVP parking and free slots, known as an AVP service announcement, and the OEM AS subscribes to this type of information. The AVP service announcement needs to be standardised or agreed among industry players. In this case, the Interchange Function can serve as a message broker, e.g. using AMQP, for AVP service announcements. Alternatively, if the OEM AS does not subscribe to AVP announcements, it can still use the Interchange Function to 'discover' available AVP service providers, when a user requests such a service via the OEM AS. In this case, the Interchange Function serves as a discovery server (e.g. digital map server) maintaining the AVP AS list. As a result of the AVP service discovery process, the OEM AS delivers information about the availability of AVP service providers matching the users' parking demands and the capabilities of their vehicles.

For successful deployment of AVP, methods are needed to reserve a parking spot before the vehicle arrives at the facility and to pay for the parking service. This can be done by using the AVP SP's information (e.g. URL) obtained from AVP service announcement. To make AVP service reservations, the service demand information (e.g. parking duration and slot availability) as well as the capability information (e.g. supported AVP types and interfaces) need to be exchanged between the AVP OEM App (vehicle) and the AVP SP AS via the vehicle OEM AS.

Examples of AVP service discovery and reservation processes and communication sequences are shown in Figure 4 covering part I 'Preparation', part II 'AVP Service Discovery', and part III 'AVP Service Reservation'.

Payment can, for example, be handled by registered credit cards or in the case of a fleet operator (e.g. rental car company) by prior agreements using monthly billing facilities.

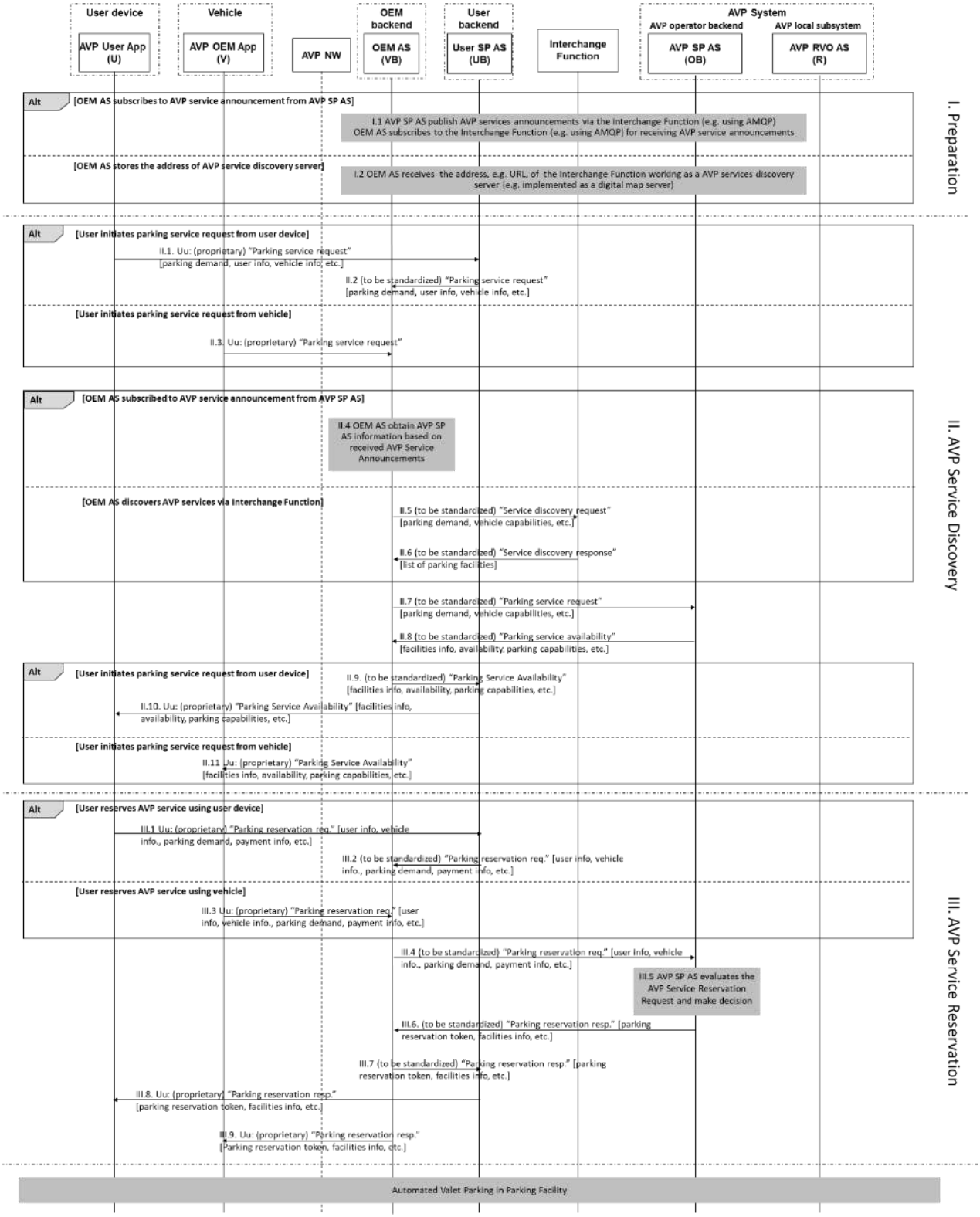


Figure 4: Example communication sequence for AVP service discovery and reservation

7.2.2 Vehicle parking process

This section describes the vehicle parking process of AVP Type-2 [1] at or within the parking facility.

This description is also applicable for AVP at or within an OEM logistics parking area. In such scenarios the OEM AS would be the OEM factory control system (fleet management system), and the 'drop-off point' is the location for vehicles ready for parking. In such scenarios, the communication would be limited to interaction between the vehicle and the OEM factory control system (fleet management system). The OEM factory control system would incorporate a series of needed/essential functions, such as MAP handling (i.e. were to park the vehicle).

As shown in Figure 2, for AVP Type-2 in a public parking facility, the OEM backend system is connected to the vehicle, validates AVP requests and collects driving data directly form the vehicle. In the AVP process, the OEM backend system may also work as a gateway passing on requests and commands (e.g. for the VMC interface, between the vehicle and the AVP system). In another implementation option of the VMC interface, the vehicle motion control and feedback information may not need to pass through the OEM backend if a secure channel can be directly established between the vehicle and the AVP system, under the supervision of OEM backend. The OEM backend system is thus connected to the AVP operator backend. [1]

Figure 5 illustrates the high-level process of vehicle parking, starting from vehicle check-in to the vehicle being parked and entering sleep mode once in the allotted space. This process is algined with the ISO 23374-1 [1] standard. The description below within the blue brackets describes specific steps, where interactions with the AVP NW, i.e. the MNO NW in this case, are needed.

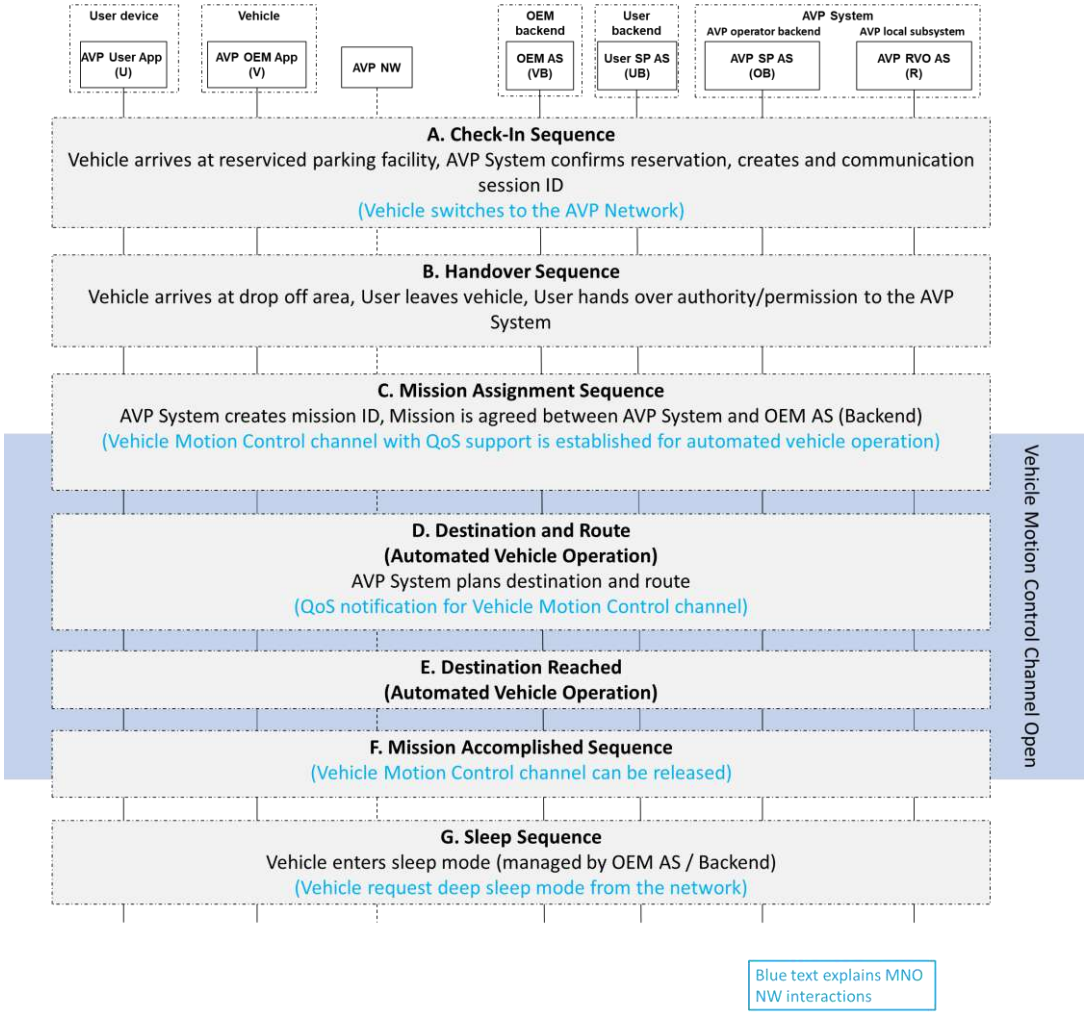


Figure 5: High-level communication sequences for AVP Type-2 parking process

7.2.3 Vehicle re-park to a different location

This section describes the vehicle re-parking process of AVP Type-2 [1] from one location to another location in the parking facility, as shown in Figure 6. Explanations in blue brackets describes specific steps, where interactions with the AVP NW, i.e. the MNO NW in this case, are needed.

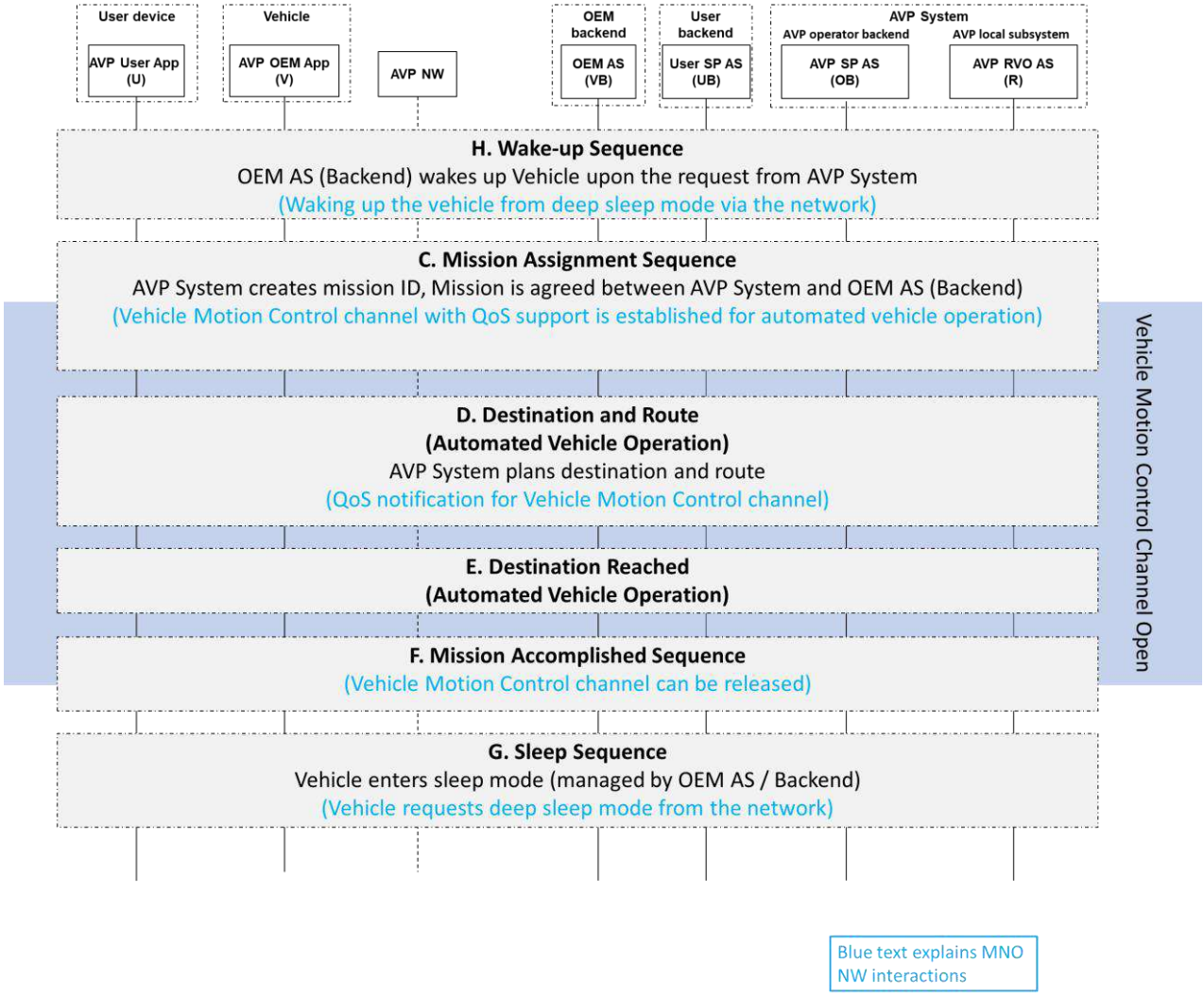


Figure 6: High-level communication sequences for AVP Type-2 re-park process

7.2.4 Vehicle retrieval

This section describes the vehicle pick-up process, AVP Type-2 [1], from the vehicle parking location to the vehicle pick-up area.

This description is also applicable to AVP at or within an OEM logistics parking area, in such scenarios the OEM AS would be the OEM factory control system (fleet management system) and the ‘pick-up’ point would be the location where vehicles waiting to be transported from the factory parking area can be found.

In such a scenario, the communication would be limited to interaction between the vehicle and the OEM factory control/fleet management system, which would incorporate functions such as MAP handling (i.e. where to park the vehicle for pick-up).

As shown in Figure 2, illustrating AVP Type-2 in public parking facility, the OEM backend system is connected to the vehicle, validates AVP requests and collects driving data directly form the vehicle. As stated previously, in the AVP process the OEM backend system can also work as a gateway passing on requests and commands. Another option outlined earlier is where the VMC interface, the vehicle motion control and feedback information don’t need to go through the

OEM backend because a direct channel has been established between the vehicle OEM App and the AVP system, and thus the OEM backend system is connected to the Automated Valet Parking System securely. [1]

To summarise, the user or fleet management system decides to pick up a vehicle, wakes it up and then the AVP system provides instructions on the how to manoeuvre the vehicle, which in turn executes the instructions until the vehicle reaches the designated pick-up location, where it is handed over to the user or loaded onto a truck/ship, etc.

Figure 7 illustrates the high-level process covering vehicle retrieval. Again, the explanations in blue brackets describe specific steps, where interactions with the AVP NW, i.e. the MNO NW in this case, are needed.

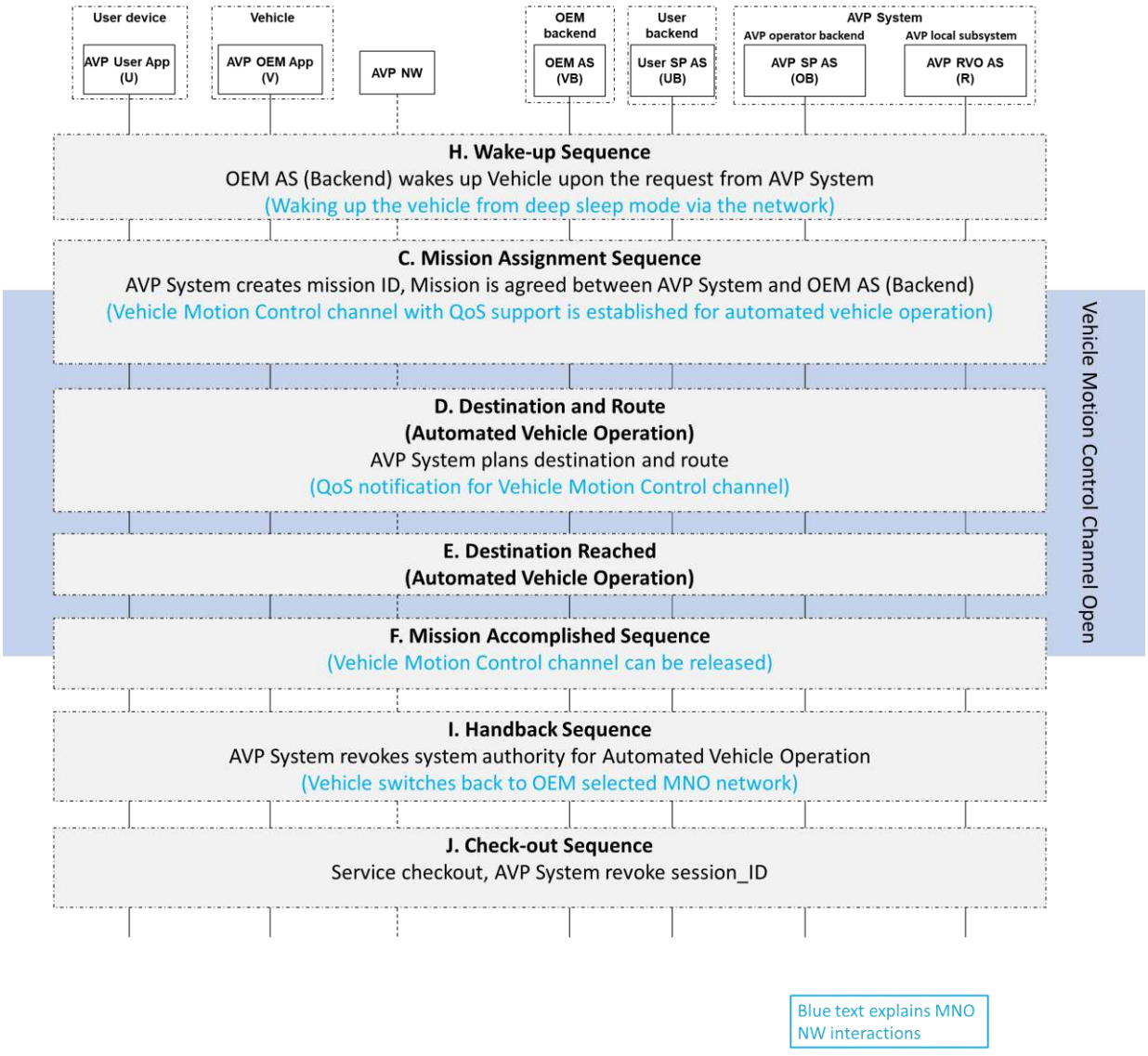


Figure 7: High-level communication sequences for AVP Type-2 retrieval process

7.3. Detailed communication sequences for AVP Type-2

7.3.1 A. Check-in sequence

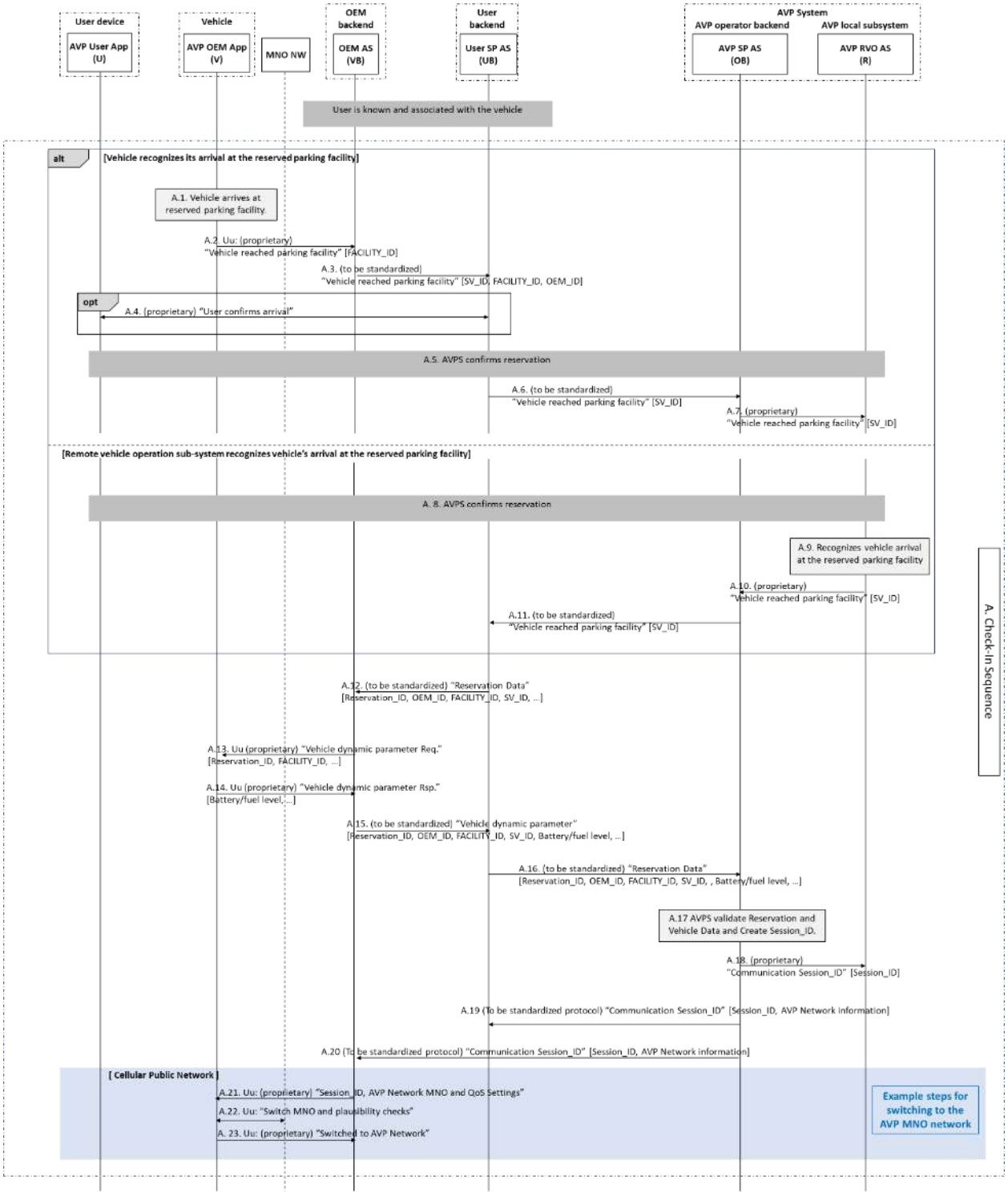


Figure 8: Communication sequence for "check-in"

'AVP network information' in steps A.19 and A.20 includes the identifier and further information about the AVP network to enable the vehicle to access the AVP network.

- If the AVP network is a public cellular network, 'AVP network information' includes at least the Public Land Mobile Network (PLMN) ID and the Absolute Radio-Frequency Channel Number (ARFCN).

A.21 to A.23 are the steps for the UE in the vehicle to switch to the AVP network.

- A.22 includes the step when the vehicle application instructs the modem to switch to a preferred NW and attaches itself according to standard 3GPP procedures.
- If the AVP network is a different AVP SP preferred MNO network than the one the UE has been connected to outside the parking facility, Section 8.1.2 explains the network switching mechanism.

7.3.2 B. Handover sequence

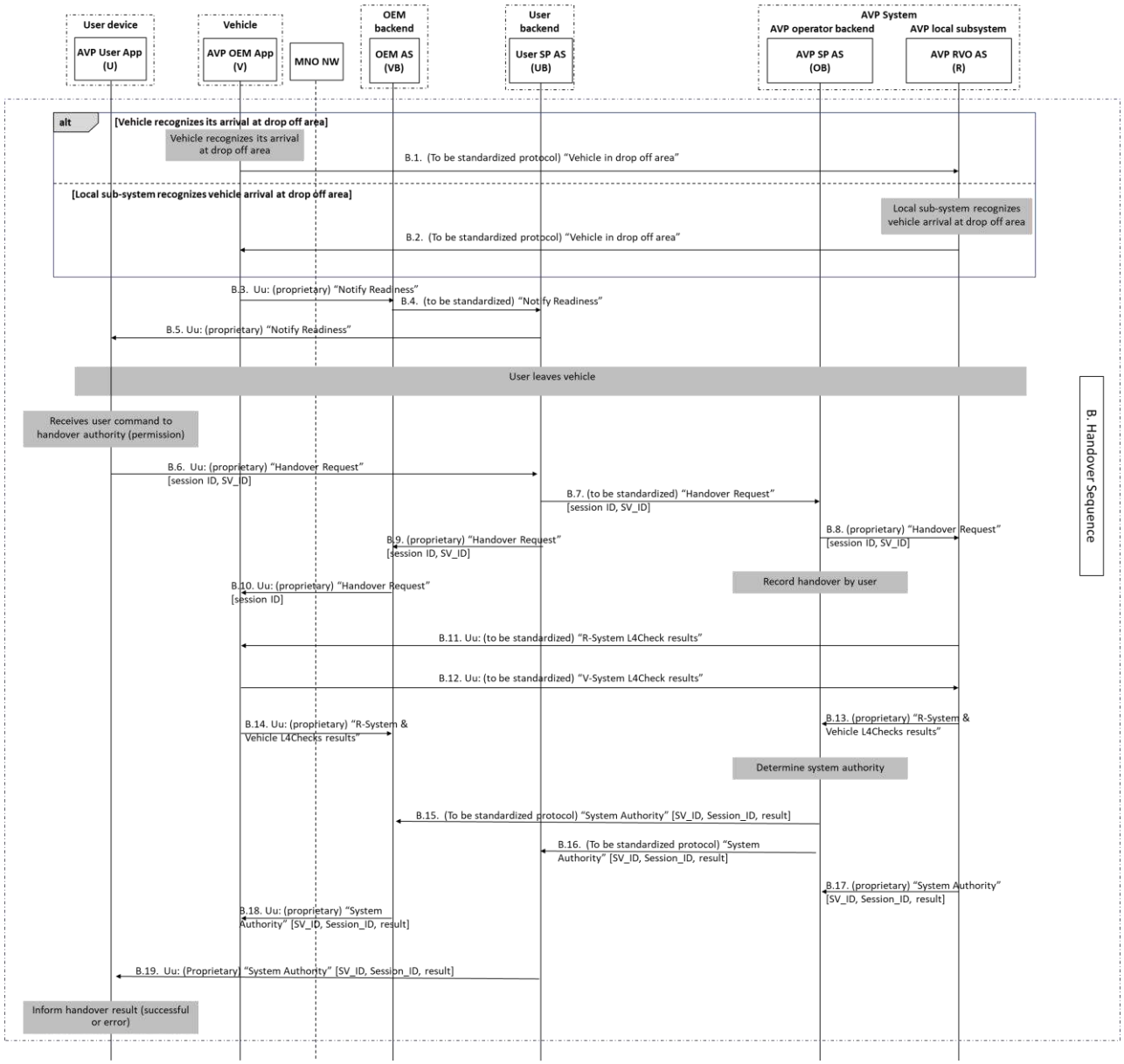


Figure 9: Communication sequence for "handover"

7.3.3 C. Mission assignment sequence

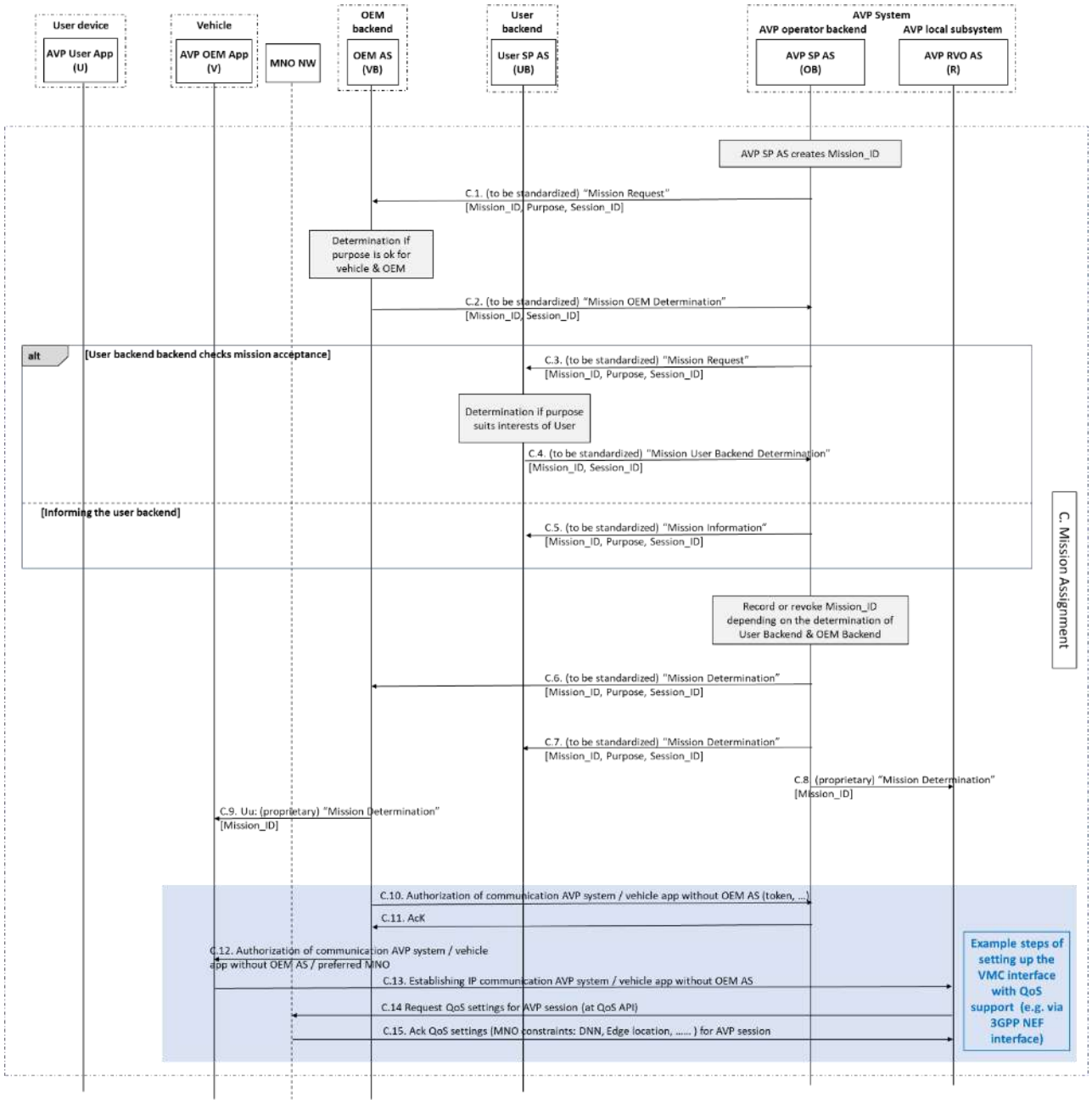


Figure 10: Communication sequence for "mission assignment"

Steps C.14 and C.15 set up the VMC interface with QoS support from the cellular network. Section 8.1.3 describes mechanisms and interfaces for negotiating and setting up QoS support in the cellular network to handle the AVP VMC interface data traffic.

7.3.4 D. Destination and route (automated vehicle operation Type-2)

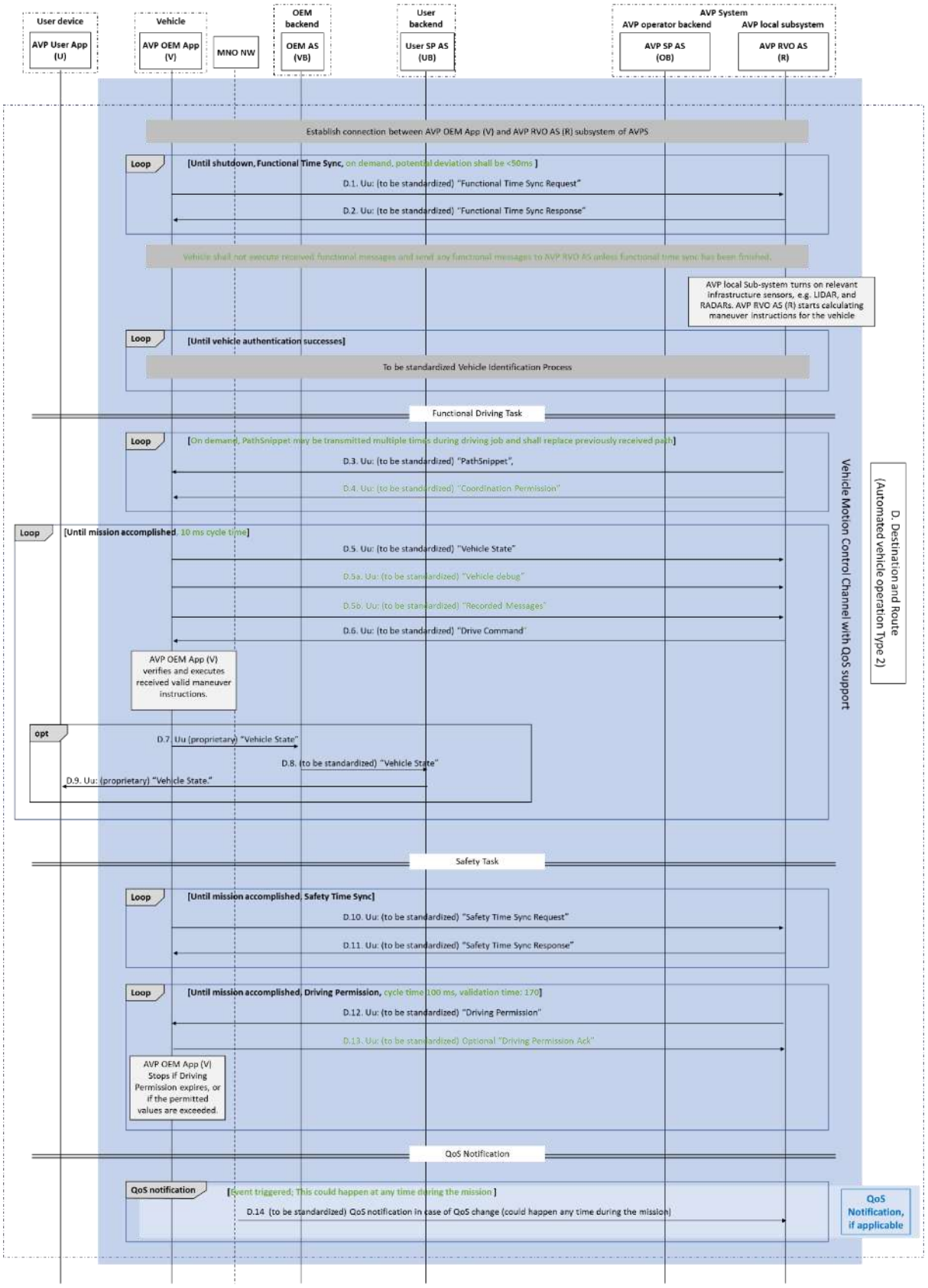


Figure 11: Communication sequence for "destination and route"

In a cellular network, the QoS notification in step D.14 utilises the network exposure interface described in Section 8.1.3. In this process, the functional driving tasks and safety tasks are separated. Each task has its own clock synchronisation and communication loops between the AVP OEM APP (vehicle) and AVP RVO AS (remote control). Step D.12 'Driving Permissions', defined in ISO 23307-1 [1], is critical for the system to fulfil functional safety requirements. If the vehicle cannot receive a valid update before the current Driving Permission expires, or the permitted operations in the valid Driving Permission are violated, it has to stop. This is to ensure safety requirements are fulfilled, even if the connectivity between the vehicle and remote control fails.

The values and communication steps in green text in Figure 11 are sample values and optional steps which may need some refinements according to actual implementation situation.

7.3.5 E. Destination reached

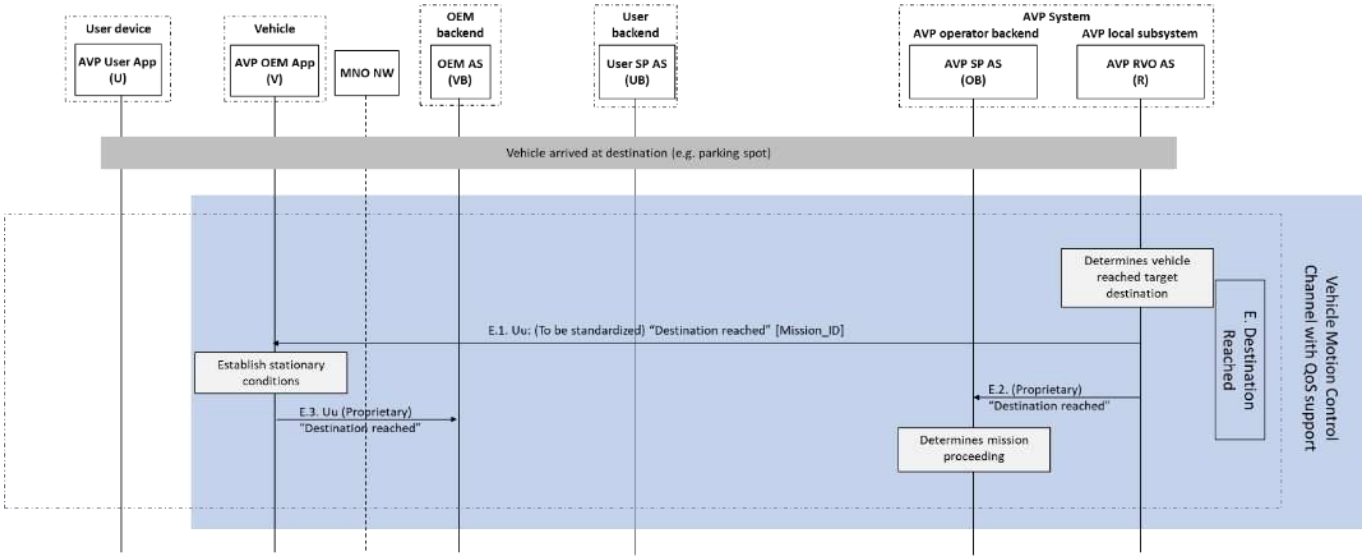


Figure 12: Communication sequence for "destination reached"

7.3.6 F. Mission accomplished

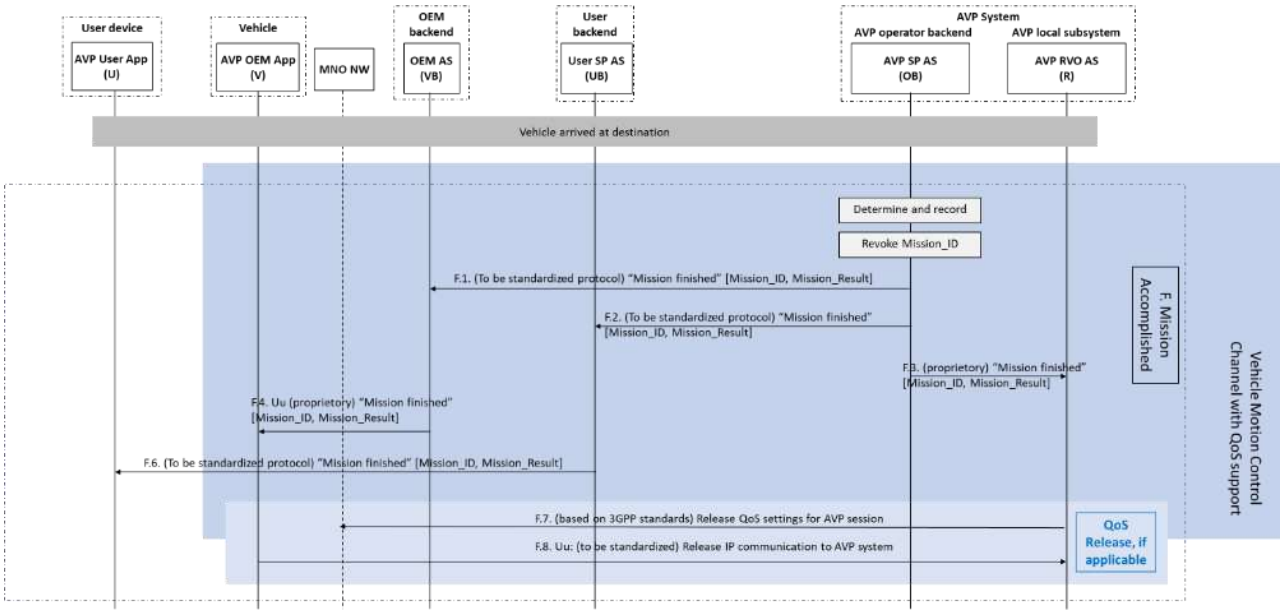


Figure 13: Communication sequence for "mission accomplished"

Step F.7 disengages the VMC interface's QoS support for data traffic in the cellular network. Section 8.1.3 explains the cellular network exposure mechanisms and interfaces used in this step.

7.3.7 G. Sleep sequence

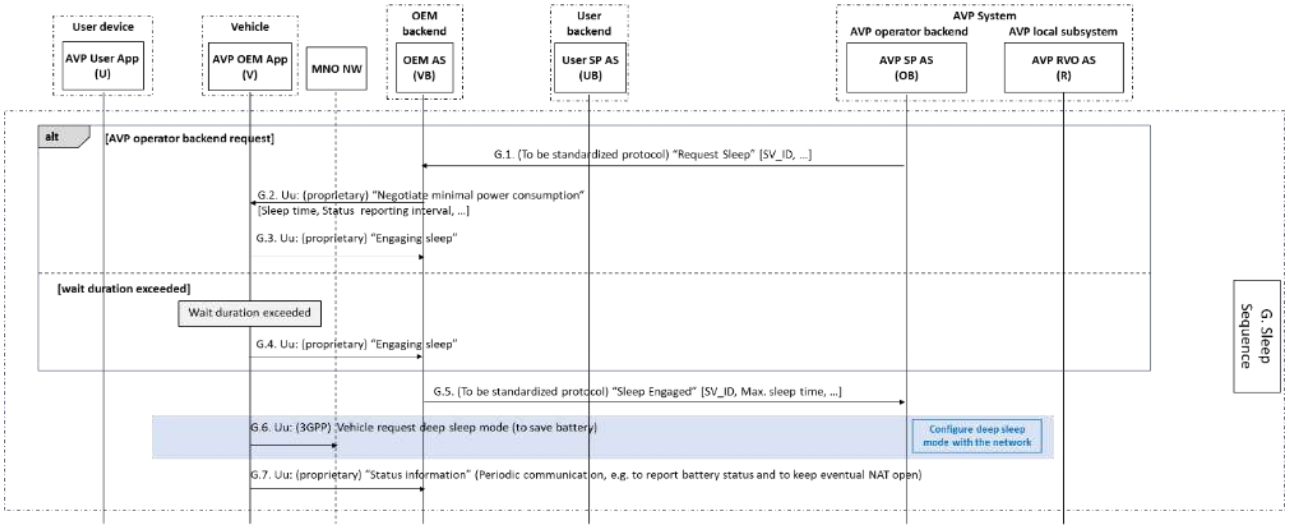


Figure 14: Communication sequence for "sleep"

In step G.6, optionally, the vehicle requests a DRX from the network, which effectively discontinues the 'reception mode' and puts it into 'sleep mode' to save battery. This is further described in Section 8.1.5.

7.3.8 H. Wake-up sequence

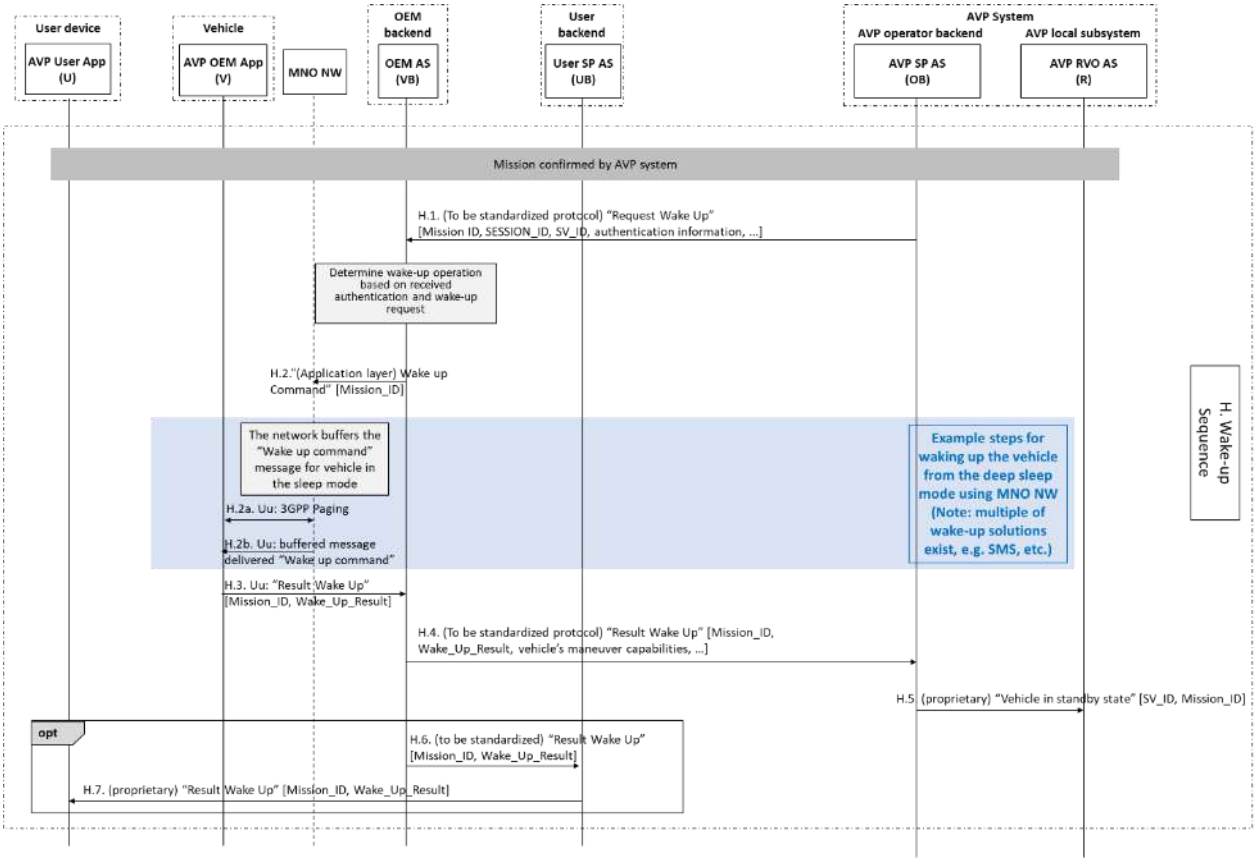


Figure 15: Communication sequence for "wake-up"

In step H.2a, the cellular network pages the UE (vehicle). H.2b shows the vehicle receiving the buffered message from the OEM backend – in this example it is a 'Wake Up command'. In H.3, the vehicle acts according to the OEM procedure and performs the desired action (i.e. the vehicle replies with a 'Wake-Up_result' message).

7.3.9 I. Hand-back sequence

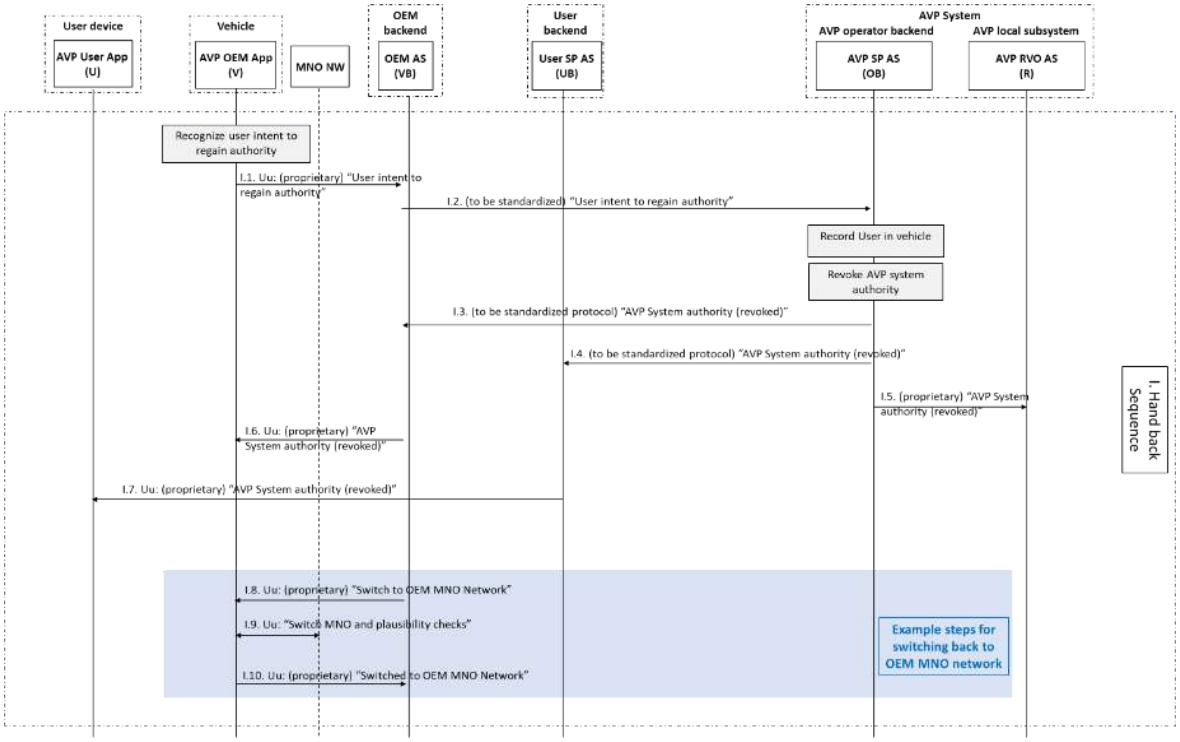


Figure 16: Communication sequence for "hand-back"

In I.8, it describes what happens when the vehicle needs to switch to a preferred MNO for the AVP session; while leaving the parking facility the OEM backend instructs the vehicle to switch back to the MNO used prior to the AVP session. In I.9, the application on the vehicle side instructs the modem to switch to the MNO to be used outside the parking facility and attaches to the preferred NW according to standard 3GPP procedures.

7.3.10 J. Check-out sequence

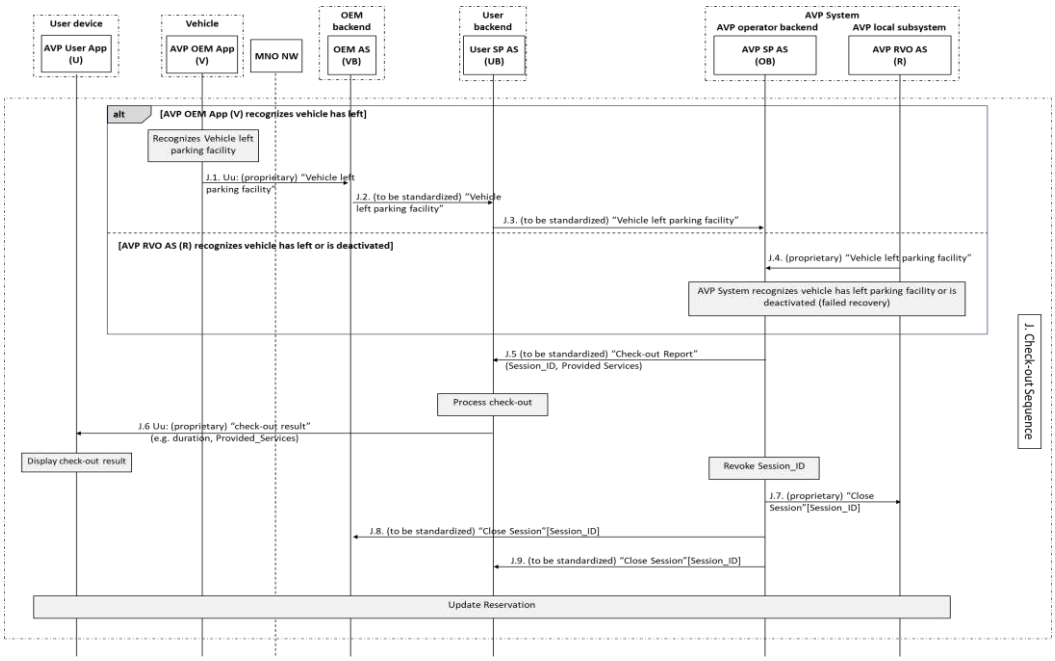


Figure 17: Communication sequence for "check-out"

8. Implementation considerations for cellular network solutions

8.1. Considerations for cellular public networks

8.1.1 Network coverage in parking facilities

In many cases, parking facility owners have an agreement in place with MNOs. If there is a need to extend or enhance the existing cellular public network in the parking facility to support AVP, it can be done by updating the existing agreement or making new agreements with these MNOs.

In order to improve the customer experience, there is an inherent investment driver for MNOs to boost network coverage in parking facilities. This has already been seen in high-value parking garages in airports, train stations, concert halls and shopping malls, with a lot of mobile network traffic. Also, MNO agreements exist on a case-by-case basis between the MNO and the facility owner, to reduce complexity and costs of coverage. There are also examples where tower companies invest in passive and active infrastructure, which is then shared by multiple MNOs. One additional investment driver is the increase of car-sharing vehicles, which can only be serviced if there is good network coverage.

To provide AVP Type-2 service to vehicles, it should be noted that technical requirements need to be fulfilled by the parking facilities, including the communication network, which are under the responsibility of the parking facility owner supported by the MNOs.

For this AVP Type-2 use case implementation description, it is assumed that major MNOs are already present because initial AVP scenarios are likely to occur mainly in urban and suburban areas or in other high mobile traffic locations, such as shopping areas, transport hubs and country clubs. It is assumed that most parking areas have coverage at least on some floors and, since the uptake of AVP-capable vehicles will happen over time, AVP can initially be restricted to those areas already covered.

When the penetration rate of AVP-capable vehicles increases, coverage for deep underground parking facilities can be gradually realised. Here, several approaches are possible including:

- MNOs provide additional radio equipment, potentially using network-sharing between MNOs;
- Tower companies, network infrastructure real estate providers, or the parking facility owners provide space or a site where MNOs can set up.

In this situation, there might be no need for more advanced 5G coverage; from a bandwidth perspective, as well as latencies, LTE might be sufficient in many cases.

An additional factor is the spectrum available for the networks. Because coverage improvement is one of the most important investment drivers, spectrum with better propagation capabilities inside buildings will reduce upfront capital needs.

8.1.2 Network switching to the preferred MNO network in a parking facility

A ‘preferred MNO’ refers to a network operator who provides an agreed level of AVP coverage and performance to a given parking facility. Information about preferred MNO(s) is provided to the OEM backend system from the parking facility system. The OEM backend then orders the application in the vehicle to switch to the indicated MNO network, i.e. in a roaming situation the vehicle switches connection from one ‘visited NW’ to another. The switching should be executed in the drop-off/pick-up zones. The information from the parking facility system to the vehicle (via the OEM backend) about the ‘preferred network’ comprises frequency bands (e.g. Absolute Radio-Frequency Channel Numbers, or ARFCNs) and NW identities (e.g. PLMN ID), so the in-vehicle application can configure the modem to attach to this network and speed up network reselection. The vehicle application can also read out information about the used network from the modem and store that in order to facilitate faster reselection when the vehicle is picked up. Such network-switching follows the roaming process between MNOs and is possible where subscriptions with permanent roaming are used (in many cases globally).. Of course, roaming contracts between MNOs need to be in place, which is mostly the case.

If no permanent roaming is in place, MNOs who have AVP-capable vehicles among their subscribers will need to be accommodated. Alternatively, national roaming would have to be applied or the coverage has to be extended to the area where the parking facility is located, thus enabling AVP services to vehicles using cellular connectivity from any MNO.

Note: this does not hinder collaboration between MNOs regarding network-sharing mentioned in Section 8.1.1.

8.1.3 QoS provisioning in the cellular network

As coverage is a prerequisite for a well-functioning mobile network, it is important to address possible congestion scenarios affecting the ability to fulfil AVP use-case requirements. Quality of Service needs to be established for the AVP application, specifically controlling the motion of the vehicle.

This section first introduces the 3GPP features for prioritising dedicated application traffic flows and offers an introduction to the Network Exposure interfaces interacting with the cellular network.

8.1.3.1 3GPP QoS assurance mechanisms

Figure 18 illustrates the different 3GPP-defined QoS assurance mechanisms:

- Network Slicing is defined in 3GPP as a logical network that provides specific capabilities and network characteristics. It is a tool to separate resources and provide a defined network characteristic, for example an Industry Vertical which facilitates use-case differentiation and secures the necessary capacity and performance to meet Service-Level Agreements even in high-demand situations (heavy network load). Note: the same QoS Class Identifier (QCI) or 5G QoS Identifier (5QI) value may have different behaviours in different Network Slices; see Section 8.1.3.2 for details.
- There is at least one PDU sessions within one Network Slice.
- For one PDU session, multiple QoS Flows can be defined. The number of simultaneously active QoS Flows is typically limited.
- One of more Applications Flows can be contained within one QoS Flow. Application Flow based on separation and prioritisation allows traffic characteristics to be differentiated by priority, Packet Error Rates (PER) and Packet Delay Budgets (PDB), and supports Guaranteed Bitrate (GBR), Delay Critical GBR, and non-GBR for such flows.

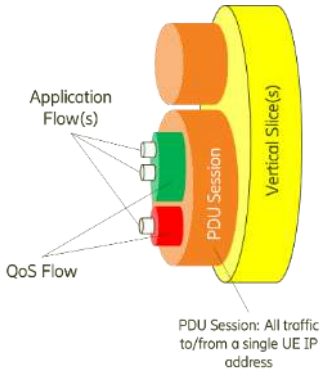


Figure 18: 3GPP QoS assurance mechanisms

With respect to Quality on Demand (QoD)/Quality of Service (QoS) APIs, these should be radio-access technology agnostic. Therefore, depending on the local deployments of the MNOs, the QoD API might be available in 4G, 5G, or both.

It is important to note that all described QoS mechanisms are working on an application level, and not device level. So, different applications might make use of different Network Slices, and some applications might use a QoD API while others may not. This also addresses the needs of automotive applications with different QoS requirements because they are operated in parallel (e.g. an AVP application is executed while at the same time status information is transmitted to the OEM backend, or a map download is performed).

8.1.3.2 Network slicing

Network Slicing is a tool for separating network resources to provide a more consistent service. Additional tools, such as the 3GPP QoS framework, may be applied for traffic flows within a given Network Slice.

User Route Selection Policy (URSP) provides a foundation to deliver dynamic Network Slice selection, enabling traffic steering and the separation of services for devices when using the slices. When devices are being provided with URSP capabilities, the UE is able to use the Network Slices according to the policies defined for the subscription.

The network offers the information about available slice types to the device via URSPs, so the URSP adds further details regarding which network slices the device's underlying applications should use when activated. [5] Therefore, the device knows in advance of a certain parking process, which slice types are available, and how to get access to the relevant slice type for the AVP application. Applicable slice(s) to use need to be discussed with the corresponding MNO.

8.1.3.3 Network exposure realisations

The 5G system also supports so-called 'Network Exposure' interfaces which allow more dynamic interaction. The 5G system 'exposes' different Network Services that can be viewed, configured or modified by authorised Application Service Providers.

The Network Exposure interfaces follow the HTTP REST Model, which is widely used in the internet community. 3GPP has standardised a set of APIs, which thanks to the Network Exposure Function (NEF) supports QoS Flow setup. The NEF 'AFsessionWithQoS' API is formally specified in TS 29.522. However, TS 29.522 refers to TS 29.122 for the detailed specification. TS 29.122 contains the T8 reference point, which is exposed by the SCEF in the 4G system.

CAMARA provides an abstraction of the network APIs to simplify the use of 3GPP network features, e.g. for 'QoS on Demand'. By hiding telecommunications complexity behind APIs and making them available across telco networks and countries, CAMARA enables simple and seamless access. CAMARA is an open source project within the Linux Foundation to define, develop and test the APIs. It works in close collaboration with the GSMA Operator Platform Group to align API requirements and definitions. Harmonisation of APIs is achieved through fast and agile working code with developer-friendly documentation. API definitions and reference implementations are free to use (Apache2.0 licence). Currently, more than 25 'hyperscalers', aggregators, telco operators and vendors are part of CAMARA (see camaraproject.org.)

8.1.4 Global availability and roaming

8.1.4.1 Authentication and roaming

Authentication is required for different layers, namely authentication for network access and application-level authentication.

- Authentication for network access:
    - For cellular public network, Subscriber Identity Module (SIM)-based authentication is used, which works the same as authentication used by other connected vehicle applications in roaming situations. Network access credentials are stored on the SIM card and used for the authorisation (after unlocking the SIM).
    - Cellular public network solutions for AVP can work with just one SIM card. Switching network can be done via roaming, as explained in Section 8.1.2, but it is up to the car OEMs to use additional modem(s)/SIMs for improved coverage or combined capacity from multiple MNO networks.
    - Embedded SIM (eSIM) follows the same principle while increasing flexibility. As an example, vehicles can use an eSIM profile for the 5G network in a factory and switch to another eSIM profile (from the contracted MNO) for connected vehicle services on public roads. GSMA has worked on the framework and solutions for eSIM profiles. [6]
- Authentication for E2E communication at transport and/or application layers:
    - TLS/DTLS supporting mutual authentication on top of the IP connection is well supported by cellular public networks.
    - Any application layer authentication method (e.g. digital certificate or user credentials) that is agnostic to the lower layers can be used independently and in addition to cellular network authentication.
    - If digital certificates are used, the appropriate Public Key Infrastructure (PKI) needs to be in place, to ensure mutual trust between authenticated entities. This is out of scope of the present document.

In the roaming situation, Quality on Demand and Network Slicing described in Section 8.1.3 are network capabilities aligned across network operators. When Quality on Demand is used for prioritising the AVP data traffic and the vehicle is in a roaming situation, the visited MNO network needs to provide the required QoS API (as described in Section 8.1.3.3) and the provider of the global roaming subscription for the vehicle needs to take care of the appropriate roaming contracts. 5G slicing applied via UE Route Selection Policies is a 3GPP technology, and thus aligned inherently. From an operational perspective, the slice types need to be aligned so 5GAA and its partners are aiming for profiles to be used globally (see camaraproject.org.)

Local AVP (country based), which includes the use of MEC, needs the agreement between the global roaming SIM provider and the MNO of the visited network. The agreement needs to provide all commercial and technical terms and conditions, to use the visited network properly. Terms and conditions are the result of commercial negotiations among the MNOs involved.

8.1.4.2 Regional breakout

Regional breakout can be used to minimise the packet delay between the vehicle and the remote vehicle operation server in a region or country. There are standard 3GPP procedures for local breakout. It is already operating in some countries based on 4G, and with 5G it leverages the core network and local User Plane Function (UPF). The local breakout needs to be negotiated between the host MNO and the visited MNO. It should be part of future roaming agreements. The technologies are already specified in 3GPP. They need to be implemented by the MNOs. The 5GAA gMEC4Auto Work Item is working on local breakout solutions for MEC operations in visited networks (roaming).

8.1.5 Additional network features support AVP

8.1.5.1 Discontinuous reception (DRX) framework

For the cellular User Equipment (UE) to save energy, the network supports the Discontinuous Reception (DRX) feature. The DRX forces a UE to turn off its transceivers for a DRX cycle and does not need to monitor the radio channel. If the UE wants to use UE-specific DRX parameters, the UE includes its preferred values consistently during Initial Registration and Mobility Registration procedures.

8.2 Protocol stacks

A number of interfaces need to be standardised for the AVP function and Protocol Stacks for those interfaces are depicted in the following sections. The IP is used at the network layer to ensure portability between different infrastructures used. Higher layer protocols (i.e. TCP) are determined by the purpose of the interactions. HTTPS is often used within Cloud Native designs, specifically Request/Response-based communication. Many features like Security and Authorisation are already available and can be re-used.

8.2.1 OEM AS and AVP system interaction

As shown in the initial architecture (Figure 2), the AVP Control (AVPC) interface between AVP operator backend (AVP System) and OEM backend is used to initiate and control the AVP function, e.g. exchanging authentication/ authorisation information, providing the vehicle network information, service and server discovery, AVP service reservation and request, etc.

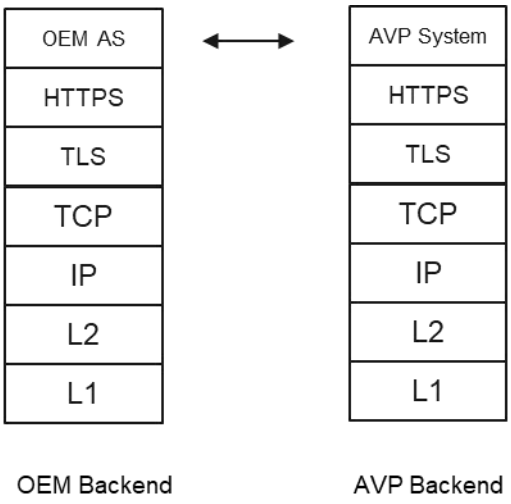


Figure 19: Protocol stacks for OEM AS and AVP system interaction

As an example, Figure 19 shows that for the AVPC interface HTTP Post messages and JSON encoding are used. Procedures of AVP Type-2 use case are described in Section 7.

8.2.2 Vehicle motion control interface

This section describes the interaction needed for vehicle motion control. As shown in the AVP System architecture (Figure 2), information about vehicle movement is communicated through the Vehicle Motion Control (VMC) logical interface between the remote vehicle operation and the vehicle. This logical interface can be implemented via the OEM backend or without traversing the OEM AS.

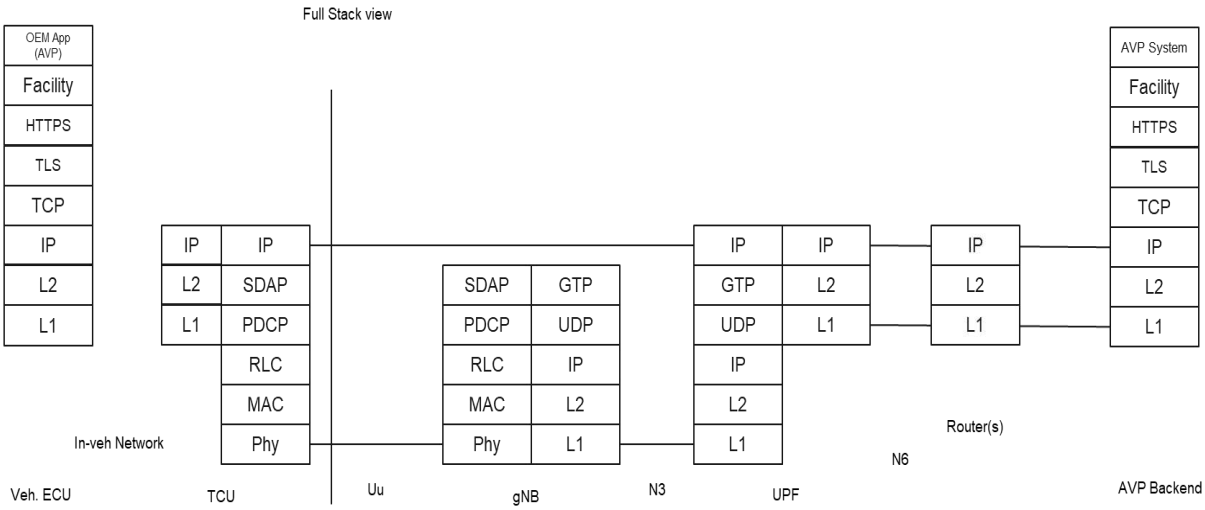


Figure 20: Protocol stacks for Vehicle Motion Control

Figure 20 shows what happens when a vehicle AVP OEM app (left) communicates with an AVP System backend server (right) over a 5G cellular system with NR radio. A 4G cellular system or any system that can transfer IP and meet the performance requirements may also be used.

If OEM AS acts as proxy/FW between vehicle and AVP System, then proprietary protocols can be used to transport the facilities layer message between OEM AS and vehicle (i.e. only the OEM AS needs to be compliant with all protocol layers).

This protocol stack assumes using HTTP for VMC because it offers many features and is very simple to use for different purposes. Other protocols than HTTP may also be used as far as all requirements outlined in Section 5 are fulfilled. HTTP Version 1.0 and Version 1.1 typically only support unidirectional Request/Response communication. Features such as WebSockets can be used to enable bi-directional communication. HTTP Version 2 and HTTP Version 3 (based on QUIC/UDP) support bi-directional communication natively.

HTTP Post messages are used to transfer the facility layer message as a payload on an IP connection between the vehicle and AVP System, i.e. only one vehicle is addressed per IP connection. The AVP System can simultaneously support multiple IP connections with different vehicles.

IP connection is initiated by the vehicle to avoid NAT problems. After establishment, the IP connection can be used bi-directionally, e.g. leveraging WebSockets or HTTP 2/HTTP 3 features.

The certificates used for TLS earlier obtained from the parking system (via the OEM backend) can, in turn, be used for authentication and protection, and to ensure that the motion control message comes from the correct source (i.e. standard TLS is used instead of having the facility layer message signed with an ETSI 1609.2 certificate and indicating what is allowed with Service Specific Permissions). The encrypted TLS session can better protect the data privacy of AVP users.

9. Conclusion

This 5GAA Technical Report describes implementation solutions using cellular public networks for an AVP Type-2 use case. Requirements and system architecture for this AVP Type-2 use case implementation are duly documented. In addition to the implementation solution with detailed communication sequences, the technical considerations of cellular public networks in the implementation and operation of AVP services are also discussed. Table 1 summarises the technical requirements of AVP Type-2 use cases, as outlined in Section 5, and how they are fulfilled by the described implementation solution using cellular public networks.

Table 1. Conformance of cellular public network solution to AVP Type-2 requirements outlined in Section 5

AVP deployment requirements	Cellular public solution	Note
Security and privacy requirements	All communication links and logical interfaces implemented using cellular network are secured through E2E encrypted TLS or DTLS connections, and interconnected actors are mutually authenticated using certificates.	
Trust between vehicle OEM and AVP Service Provider domain	For AVP network access, cellular networks provide SIM-based authentication. For transport and application layer authentication, cellular networks support any authentication solution using IP-based connections, e.g. TLS, DTLS, digital certificated or user credential-based authentication.	If digital certificates are used, the appropriate Public Key Infrastructure needs to be in place, to ensure mutual trust between authenticated entities. This is out of scope of the present document.
Access for vehicle to OEM backend	The access to the vehicle OEM backend is provided via a cellular public network.	
Short interruption to connectivity between vehicle and OEM backend at drop-off and pick-up areas	Connectivity interruption only happens when the AVP network's preferred MNO is different from the one used for connecting the vehicle on the public roads. Such interruption caused by network switching can be optimised down to a few seconds interruption, if information about the preferred MNO can be provided to the UE in advance.	See Section 8.1.2.
Vehicle power-saving mode	The cellular network supported by the Discontinuous Reception (DRX) framework promote UE energy saving.	See Section 8.1.5.
Vehicle remote wake-up	As the cellular public network is available in parking facilities, the remote wake-up feature can be implemented via a cellular Uu modem.	
Service Level Requirements of the Vehicle Motion Control	SLR values in the 5GAA Use Case Description [3] can be fulfilled by public cellular networks.	That cellular networks can fulfil SLRs has been previously demonstrated, e.g. at the AVP PoC [8]

Annex A:
Change History

Date	Meeting	TDoc	Subject/Comment
2022.05.09	5GAA F2F#22	5GAA T-220002	V1.0 First public release