5GAA Automotive Association

Cross-Working Group Work Items; Automated Valet Parking Technology Assessment and Use Case Implementation Description; System Architecture, Cellular Network and PC5 Direct Communication Solutions

5GAA Automotive Association
Technical Report

CONTACT INFORMATION:
Lead Coordinator – Thomas Linget
Email: liaison@5gaa.org

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

VERSION:	
DATE OF PUBLICATION:	
DOCUMENT TYPE:	Technical Report
EXTERNAL PUBLICATION:	
DATE OF APPROVAL BY 5GAA BOARD:	

Contents

Foreword 5

Introduction 6

1 Scope 6

2 References 7

3 Definitions, symbols and abbreviations 8
3.1 Definitions 8
3.2 Symbols 8
3.3 Abbreviations 8

4 System architecture 10

5 Working assumptions and requirements for AVP use case implementation 13

6 Protocols 16

7 AVP use case implementation flows 17
7.1 Overview of AVP use case procedure 17
7.2 High-level communication sequences 17
7.2.1 AVP services discovery, reservation, and payment 17
7.2.2 Vehicle parking process 20
7.2.3 Vehicle re-park to a different location 21
7.2.4 Vehicle retrieval 22
7.3 Detailed communication sequences for AVP Type-2 24
7.3.1 A. Check-in sequence 24
7.3.2 B. Handover sequence 26
7.3.3 C. Mission assignment sequence 27
7.3.4 D. Destination and route (automated vehicle operation Type-2) 28
7.3.4.1 Uu-based implementation 28
7.3.4.2 PC5-based implementation 30
7.3.5 E. Destination reached (optional) 33
7.3.6 F. Mission accomplished 33
7.3.7 G. Sleep sequence 34
7.3.8 H. Wake-up sequence 35
7.3.9 I. Hand-back sequence 36
7.3.10 J. Check-out sequence 37

8 Implementation considerations for cellular network solutions 38
8.1 Considerations for cellular public networks 38
8.1.1 Network coverage in parking facilities 38
8.1.2 Network switching to the preferred MNO network in a parking facility 39
8.1.3 QoS provisioning in the cellular network 40
8.1.3.1 Network exposure realisations 40
8.1.3.2 3GPP QoS assurance mechanisms 40
8.1.3.3 Network slicing 42
8.1.4 Global availability and roaming 42
8.1.4.1 Authentication and roaming 42
8.1.4.2 Regional breakout 43
8.1.5 Additional network features support AVP 43
8.1.5.1 Discontinuous reception (DRX) framework 43
8.2 Considerations for the cellular non-public network 44
8.2.1 Public network integrated non-public network 44
8.2.2 Stand-alone non-public network 44
8.2.2.1 SNPN core network aspect 45

8.2.2.2 SNPN RAN aspects ... 45
8.2.2.3 SNPN UE (device) aspects ... 46
8.2.2.4 UE network selection in SNPN access mode ... 46
8.2.2.5 SNPN authentication methods ... 46
8.2.2.5.1 Embedded subscriber identification module (eSIM) profile switching ... 46
8.2.2.5.2 Extensible authentication protocol – transport layer security (EAP-TLS) ... 47
8.2.2.6 SNPN access to PLMN services ... 48
8.3 Protocol stacks ... 49
8.3.1 Vehicle AS and AVP Operator System interaction ... 49
8.3.2 Vehicle motion control interface ... 49
8.4 Communication sequence for IP and security session ... 51

9 Implementation considerations for PC5 direct communication-based vehicle motion control ... 52
9.1 Implementation architecture options for PC5 direct communication-based AVP vehicle motion control ... 53
9.1.1 Split RSU/RVO architecture ... 53
9.1.2 Co-located RVO-RSU architecture ('smart RSU') ... 55
9.1.3 Guidelines on RSU deployment ... 56
9.2 Selection of PC5 Direct Communication -based vehicle motion control ... 57
9.2.1 PC5 direct communication-based vehicle motion control use cases ... 57
9.2.2 Requirements for availability of PC5 direct communication vehicle motion control ... 57
9.3 Security mechanism for PC5 direct communication ... 58
9.4 Assumptions on cellular coverage ... 59
9.5 Vehicle motion control interface – PC5 direct communication-based vehicle motion control ... 59

10 Conclusion ... 63
10.1 Conformance of cellular public network solution ... 63
10.2 Conformance of SNPN network solution ... 64
10.3 Conformance of PC5 direct communication-based vehicle motion control solution ... 66

Annex A: Considerations on messages and protocols among ecosystem stakeholders for AVP service ... 67

Annex B: Change history ... 75

Foreword

This Technical Report has been produced by 5GAA.
The contents of the present document are subject to continuing work within the Working Groups (WG) and may change following formal WG approval. Should the WG modify the contents of the present document, it will be re-released by the WG with an identifying change of the consistent numbering that all WG meeting documents and files should follow (according to 5GAA Rules of Procedure):

x-nnzzzz

(1) This numbering system has six logical elements:
- (a) x: a single letter corresponding to the working group:
  where x =
  T (Use cases and Technical Requirements)
  A (System Architecture and Solution Development)
  P (Evaluation, Testbed and Pilots)
  S (Standards and Spectrum)
  B (Business Models and Go-To-Market Strategies)
- (b) nn: two digits to indicate the year. i.e. ,17,18 19, etc
- (c) zzz: unique number of the document

(2) No provision is made for the use of revision numbers. Documents which are a revision of a previous version should indicate the document number of that previous version

(3) The file name of documents shall be the document number. For example, document S-160357 will be contained in file S-160357.doc

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) using solutions based on cellular public networks, Standalone Non-Public Networks (SNPN) and short-range PC5 Direct Communication technologies.

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, Standalone Non-Public Network (SNPN) and short-range communication technologies. 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, SNPN-based solutions and PC5 Direct Communication 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 nonspecific.
- 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://t.ly/3Wps6
[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://t.ly/e5HJe
[9]	GSMA RSP (Remote SIM Provisioning) Technical Specification, Version 2.4, Oct 2021, https://www.gsma.com/esim/wp-content/uploads/2021/10/SGP.22-2.4.pdf
[10]	3GPP TS 23.501, 5G; System Architecture for the 5G System, v15.13.0,23 March 2022

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

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:

AVP network: communication network used in a parking facility to support AVP services, e.g. for data communication between the subject vehicle and the AVPOS and between the subject vehicle and its Vehicle 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
AVPOS	AVP Operator System
AVPS	AVP System
AVP FM AS	AVP Facilities Management Application Server
BTP	Basic Transport Protocol
E2E	End-to-End
EPA	European Parking Association
FW	Firewall
GBR	Guaranteed Bit Rate

GNW	GeoNetWorking
HV	Host Vehicle
IF	Interchange Function
ITS	Intelligent Transport System
KPI	Key Performance Indicators
MEC	Mobile Edge Computing
MNO	Mobile Network Operator
NID	Network Identifier
NW	Network
VB	Vehicle Backend
OEM	Original Equipment Manufacturer
Vehicle AS	Vehicle Application Server
Vehicle App	Vehicle Application
PDB	Packet Delay Budget
PDU	Packet Data Unit
PER	Priority Error Rate
PNI-NPN	Public Network Integrated- Non-Public Network
QCI	QoS Class Identifier
QoD	QoS on Demand
QoS	Quality of Services
RSU	Roadside Unit
RV	Remote Vehicle
RVO	Remote Vehicle Operation
SLR	Service Level Requirements
SNPN	Standalone Non-Public Network
ToD	Tele-operated Driving
User App	User Application
User AS	User Application Server
V2X	Vehicle-to-Everything
VMC	Vehicle Motion Control
WAVE	Wireless Access in Vehicular Environments
WSMP	WAVE Short Message Protocol

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.

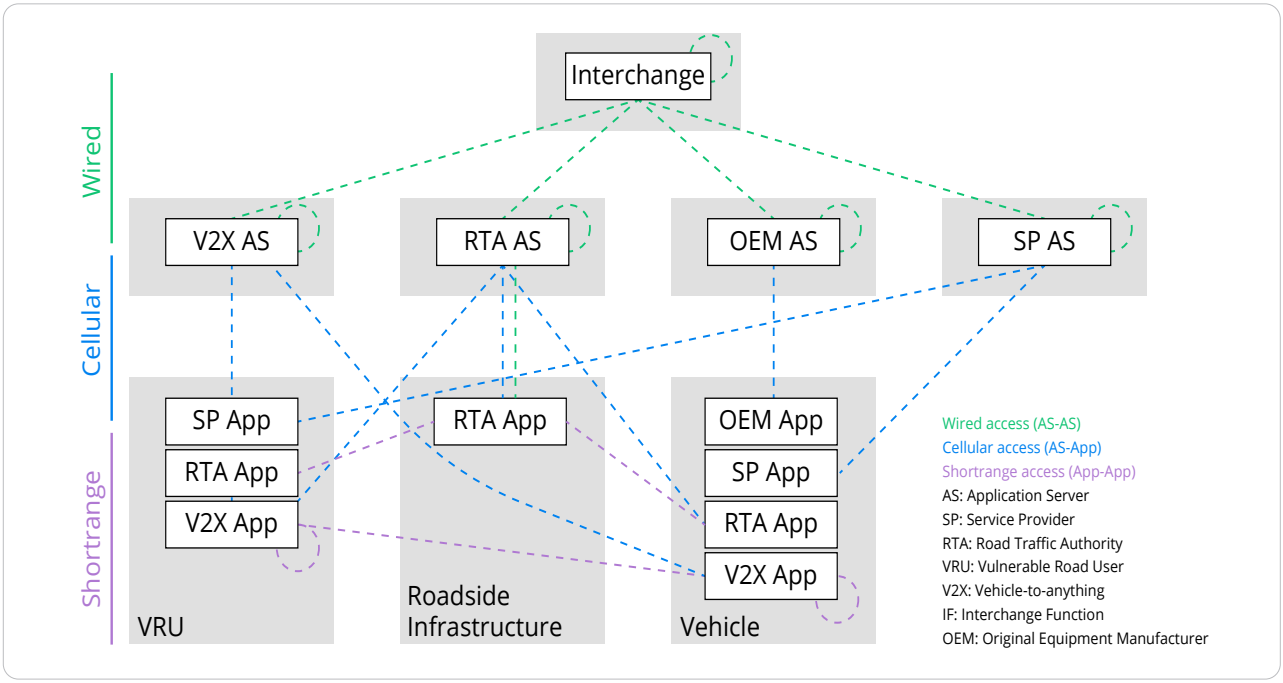
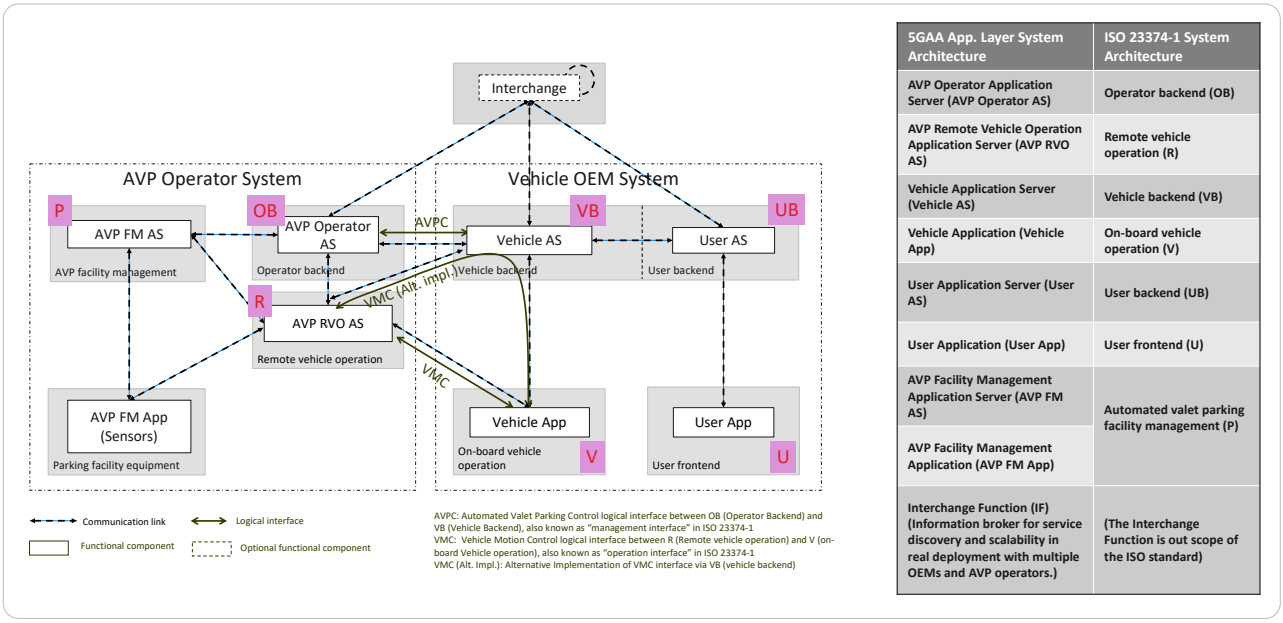


Figure 1: 5GAA V2X application layer reference architecture [2]

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 Operator Application Server (AVP Operator AS)	Operator backend (OB)
AVP Remote Vehicle Operation Application Server (AVP RVO AS)	Remote vehicle operation (R)
Vehicle Application Server (Vehicle AS)	Vehicle backend (VB)
Vehicle Application (Vehicle App)	On-board vehicle operation (V)
User Application Server (User 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 operators.)	(The Interchange Function is out scope of the ISO standard)

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

Note: Figure 2 is access-layer agnostic, i.e. the communication links can be implemented, for example, using the cellular networks or PC5 Direct Communication.

Functional components in the system include:

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

- The AVP Operator AS interacts with the Vehicle AS and User AS via backend communications to provide AVP services to the user. Tasks of AVP Operator AS include at least:
  - Managing parking facility availability.
  - Checking compatibility between vehicle and parking facility.
  - Dispatching vehicle into driverless operation.
  - Via Vehicle 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 Vehicle AS.
- The AVP Operator AS communicates with the AVP FM AS and AVP RVO AS within the AVPOS.

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 and/or AVP FM App. The AVP RVO AS in turn calculates the vehicle manoeuvre trajectory and provides instructions to the Vehicle App in the vehicle using the VMC logical interface. The AVP RVO AS communicates with the AVP Operator AS for service AVP service management.

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

- The Vehicle 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 Vehicle App. It communicates with the AVP Operator AS and User AS via backend connectivity.
- Vehicle AS is responsible of remote engagement/disengagement of AVP service of Vehicle App in the vehicle.

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

- The Vehicle App integrates services offered by the Vehicle 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 Vehicle AS. In this sense, the Vehicle App also takes the role of remote application for the AVP RVO AS.

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

- The User 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 AS also communicates with the Vehicle AS to receive AVP service-related information from the AVP Operator 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 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 Operator System, including parking facility gates and sensors installed at or in the local infrastructure, etc. It communicates with the AVP Operator AS and the AVP RVO AS and executes the AVP service commands from the AVP Operator 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 Operator System infrastructure, e.g. the parking facility gate and infrastructure sensors. It provides infrastructure sensor data to AVP FM AS and/or AVP RVO AS and executes commands from AVP FM AS.

Interchange Function (IF)

- Given the potentially large number of different AVP operators in real deployment scenarios, Interchange Functions are needed to automate the discovery of AVP operators and scale up communications between AVP Operator ASs and Vehicle 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 Operator AS (OB) and Vehicle AS (VB) for management and control signalling communications among AVP services (e.g. authentication and authorisation information, network information, service and server discovery, AVP service requests and reservations, etc. This logical interface is also known as "management interface" in ISO 23374-1 [1].

  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 Vehicle App (V) for communicating VMC information (e.g. driving commands and instructions from the AVP RVO AS and vehicle status information from the Vehicle App). This logical interface can be implemented without going through the Vehicle AS (VB) or Vehicle AS (VB), as shown in Figure 2. This logical interface is also known as "operation interface" in ISO 23374-1 [1].
  - The VMC interface can be implemented without going through the Vehicle Backend, but for security reasons the VMC interface needs to be set up under the supervision of the Vehicle 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 Vehicle 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 Vehicle Backend systems.

The communication domain between application servers and within the AVP Operator System is typically done via secured interconnections between trusted actors over 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. through end-to-end (E2E) encryption or hop-by-hop communication links among trusted entities.
2. Trust shall be established between the Vehicle AS and AVP Operator 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 Vehicle AS and AVP Operator 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 Vehicle AS, if the VMC is implemented via the Vehicle AS, or with the Vehicle App, and if the VMC is implemented directly between the Vehicle 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 Vehicle AS and AVP Operator 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 Vehicle AS.
7. The user shall be able to get the vehicle back, in the event of an AVP Operator 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 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 Operator System, the sensors in the infrastructure shall be already connected within the AVP Operator System, fulfilling the required network characteristics.
- Connectivity between Cellular Network Operators 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.

The following additional assumptions apply when cellular SNPN is used for the implementation of AVP:

- Spectrum for SNPN is available according to regional rules.
- Network coverage at the drop-off and pick-up area – vehicle needs to have access to the public network of its network provider and SNPN network in the drop-off and pick-up zone.
- The parked vehicle shall maintain 'reachability' with the Vehicle Backend via IP because a valid IP route is the only way of reaching the vehicle to trigger wake-up.
- If the AVP NPN is operating with a SIM Profile:
  - Vehicles need to support eSIM.
  - Vehicles need to support the installation of multiple eSIM profiles (minimum two; one for OEM MNO and one for current AVP SNPN).
- Support for download, installation and use of certificate-based authorisation in case AVP SNPN is operating with this technology option.
- It is assumed that roaming solutions will not be used between public networks and SNPN.
- Trusted relationship between Vehicle Backend and AVP SNPN core network for the Vehicle Backend to be informed about an IP address change from the AVP SNPN core. This assumption should be validated as part of Section 7.2.1, Figure 4, Step III.5.

The following additional assumptions apply when PC5 Direct Communication is used for the VMC interface:

- Cellular network coverage (public or SNPN) should be available throughout the parking facility
- ITS spectrum is available and appropriate channels are allocated
- ITS RSU coverage is available throughout the area where the vehicles are remotely operated

Note: Solutions based entirely on direct communication are currently out of scope of these work items.

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 Operator: provides the AVP service 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 AVPOS HV Automotive OEM: approves AVP operation of HV by AVP Operator
	Information classification	VMC information including both operational and functional safety information, transmitted between AVP RVO AS and Vehicle App Parking management control information transmitted between Vehicle App, Vehicle AS and AVP Operator 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 In addition, LTE-V2X or NR-V2X PC5 interfaces may be used for VMC procedure (Communication between Vehicle AS and AVP Operator AS are done using wired communication)
	Network and transport layer technologies	For Uu: IP with TCP/UDP with secure connections, i.e. TLS/DTLS For PC5: (Non-IP) GNW, BTP, WSMP
	Message standards	AVP application protocols need to be developed and standardised
	Framework	Uu: IP protocol stacks PC5: ETSI TC ITS protocol stacks (EU), WAVE based protocol stacks (US)
Application requirements	Use case triggers	User device or Vehicle 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 Alternatively: LTE-V2X/NR-V2X PC5 coverage in AVP operation area with minimal cellular QoS and cellular coverage in vehicle drop-off and wake-up 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 the 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.

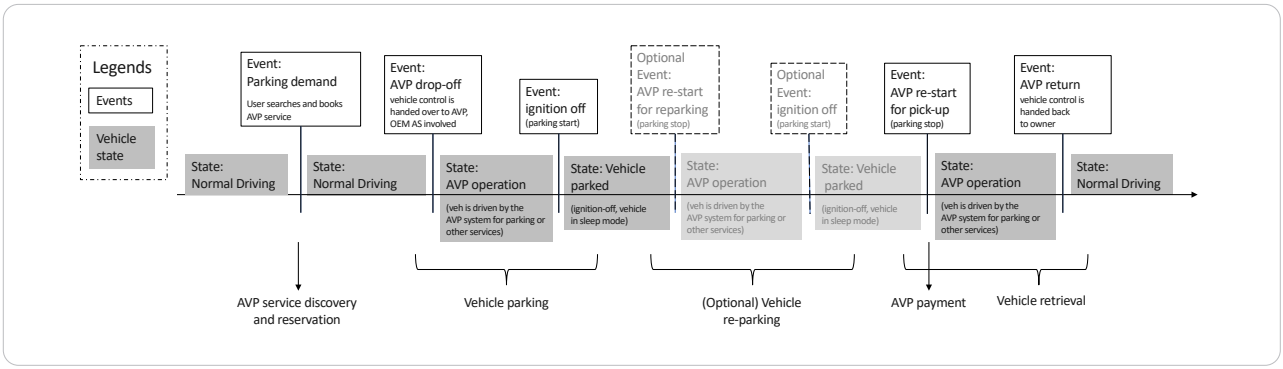


Figure 3: Events and vehicle states in AVP service cycle

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 operator publishes the availability of AVP parking and free slots, known as an AVP service announcement, and the Vehicle 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 Vehicle AS does not subscribe to AVP announcements, it can still use the Interchange Function to 'discover' available AVP operators, when a user requests such a service via the Vehicle AS. In this case, the Interchange Function serves as a discovery server (e.g. digital map server) maintaining the AVP operator list. As a result of the AVP service discovery process, the

Vehicle AS delivers information about the availability of AVP operators 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 operator'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 Vehicle App and the AVP Operator AS via the Vehicle 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'.

For the AVP SNPN network, download and installation of AVP SNPN eSIM profile or certifications need to be completed before the vehicle parking process is initiated. Please refer to Section 8.2.2.5 for details on eSIM and certification download, installation, and activation.

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.

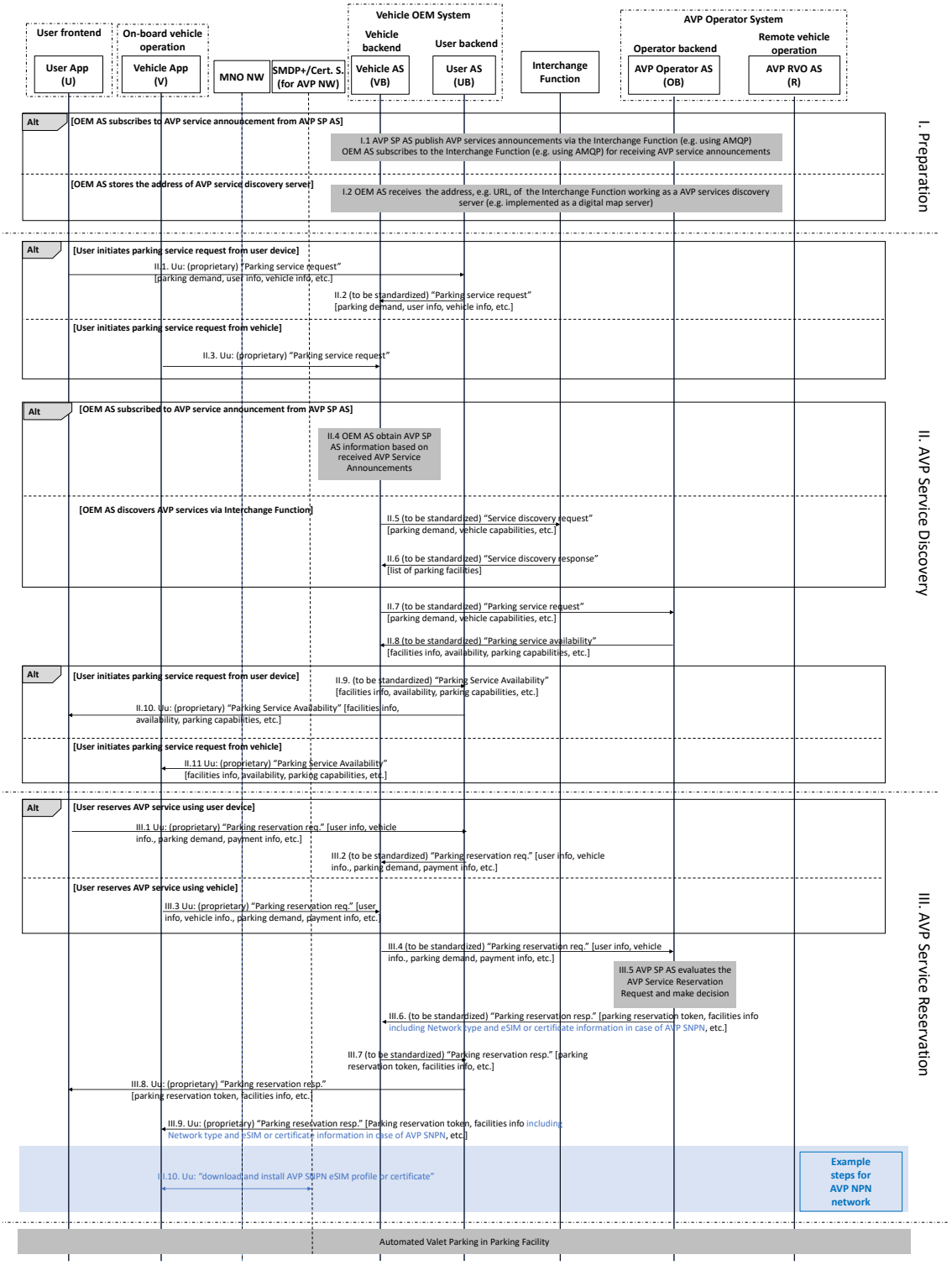


Figure 4: Example communication sequence for AVP service discovery and reservation

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 Vehicle 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 Vehicle Backend is connected to the vehicle, validates AVP requests and collects driving data directly from the vehicle. In the AVP process, the Vehicle Backend may also work as a gateway passing on requests and commands (e.g. for the VMC interface, between the vehicle and the AVP Operator System). In another implementation option of the VMC interface, the Vehicle Motion Control and feedback information may not need to pass through the Vehicle Backend if a secure channel can be directly established between the vehicle and the AVP Operator System, under the supervision of Vehicle Backend. The Vehicle 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 or SNPN in this case, are needed.

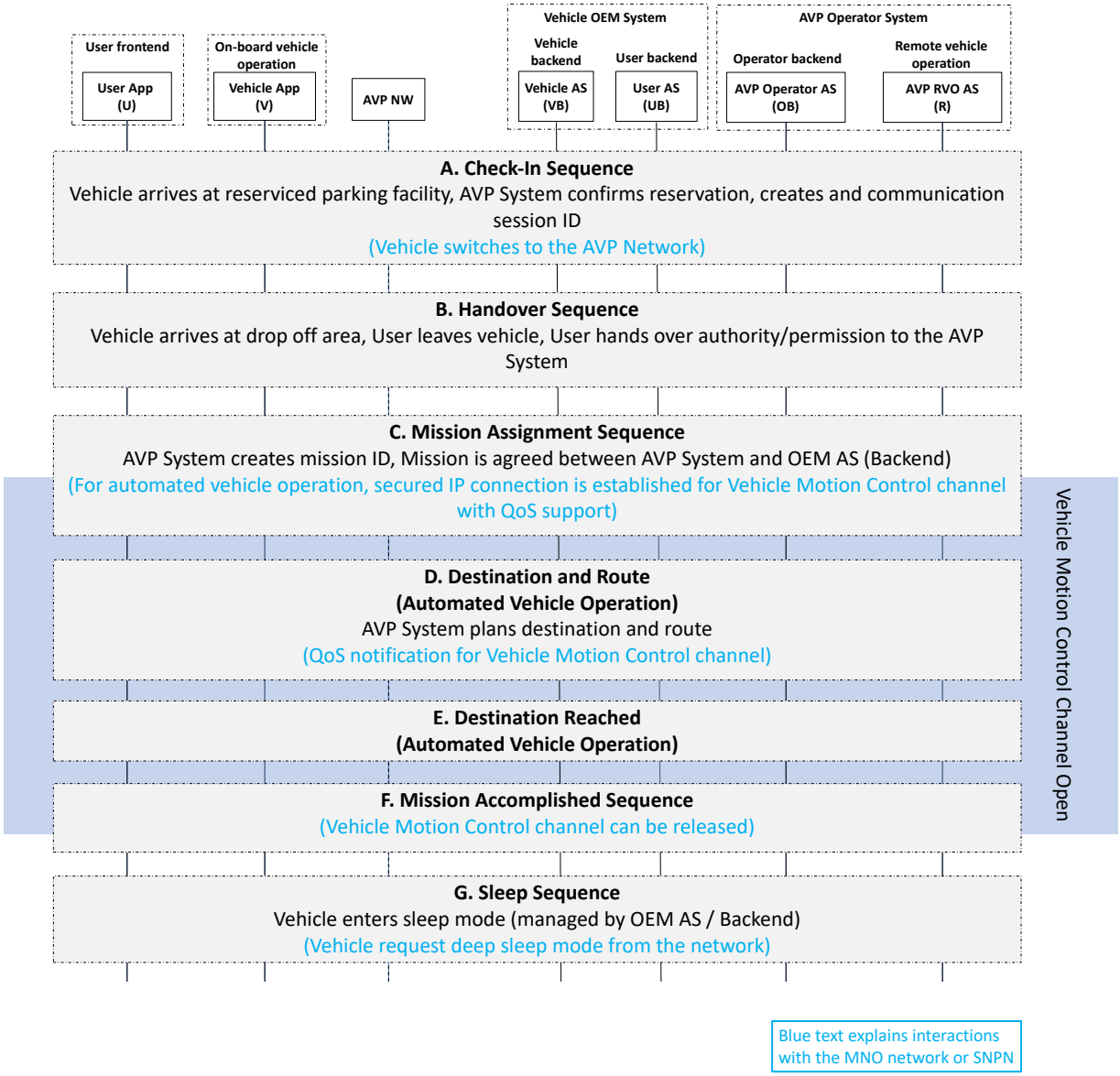


Figure 5: High-level communication sequences for AVP Type-2 parking process

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 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 or SNPN in this case, are needed.

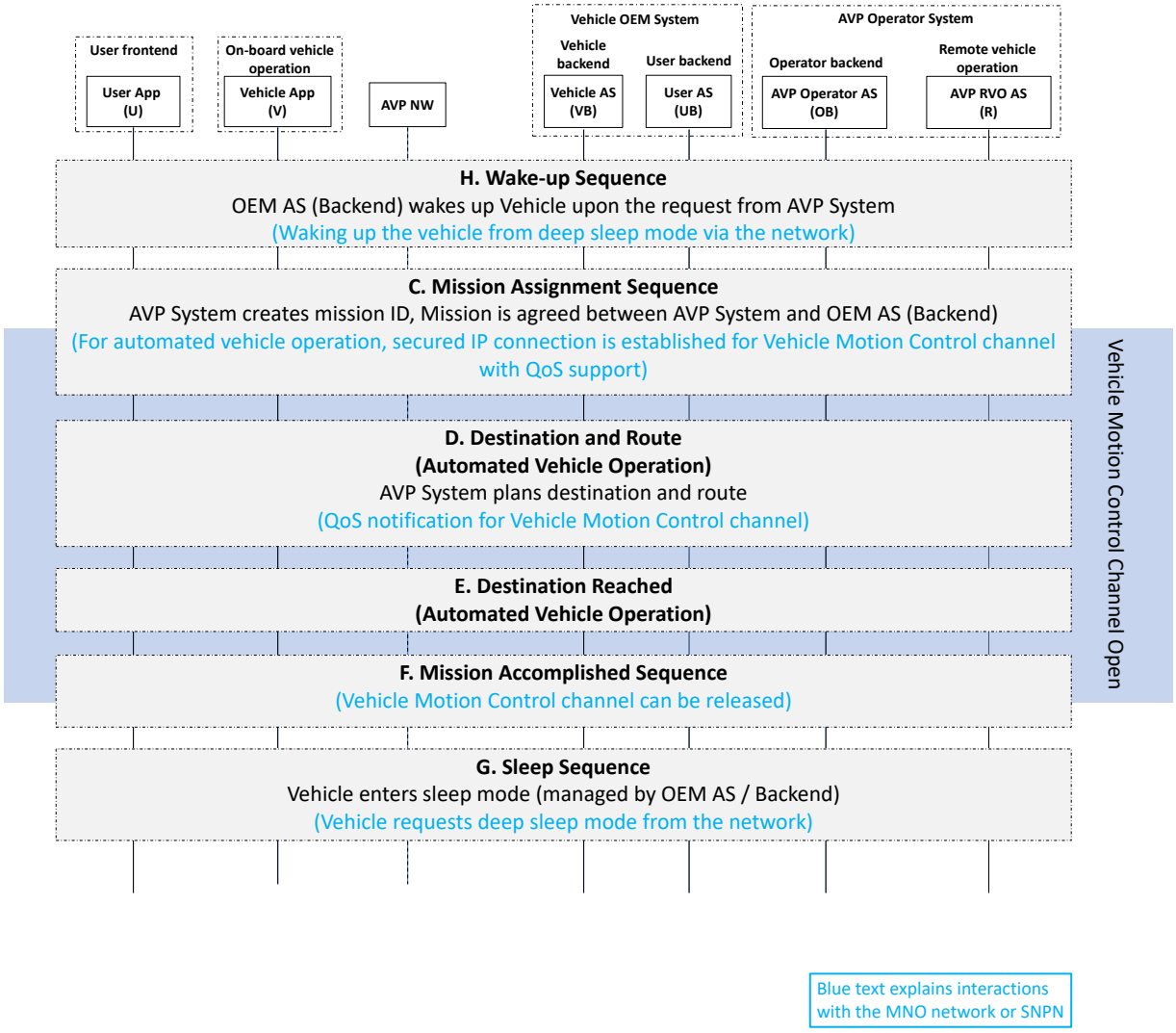


Figure 6: High-level communication sequences for AVP Type-2 re-park process

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 Vehicle 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 Vehicle 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 Vehicle

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

To summarise, the user or fleet management system decides to pick up a vehicle, wakes it up and then the AVP Operator 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 or SNPN in this case, are needed.

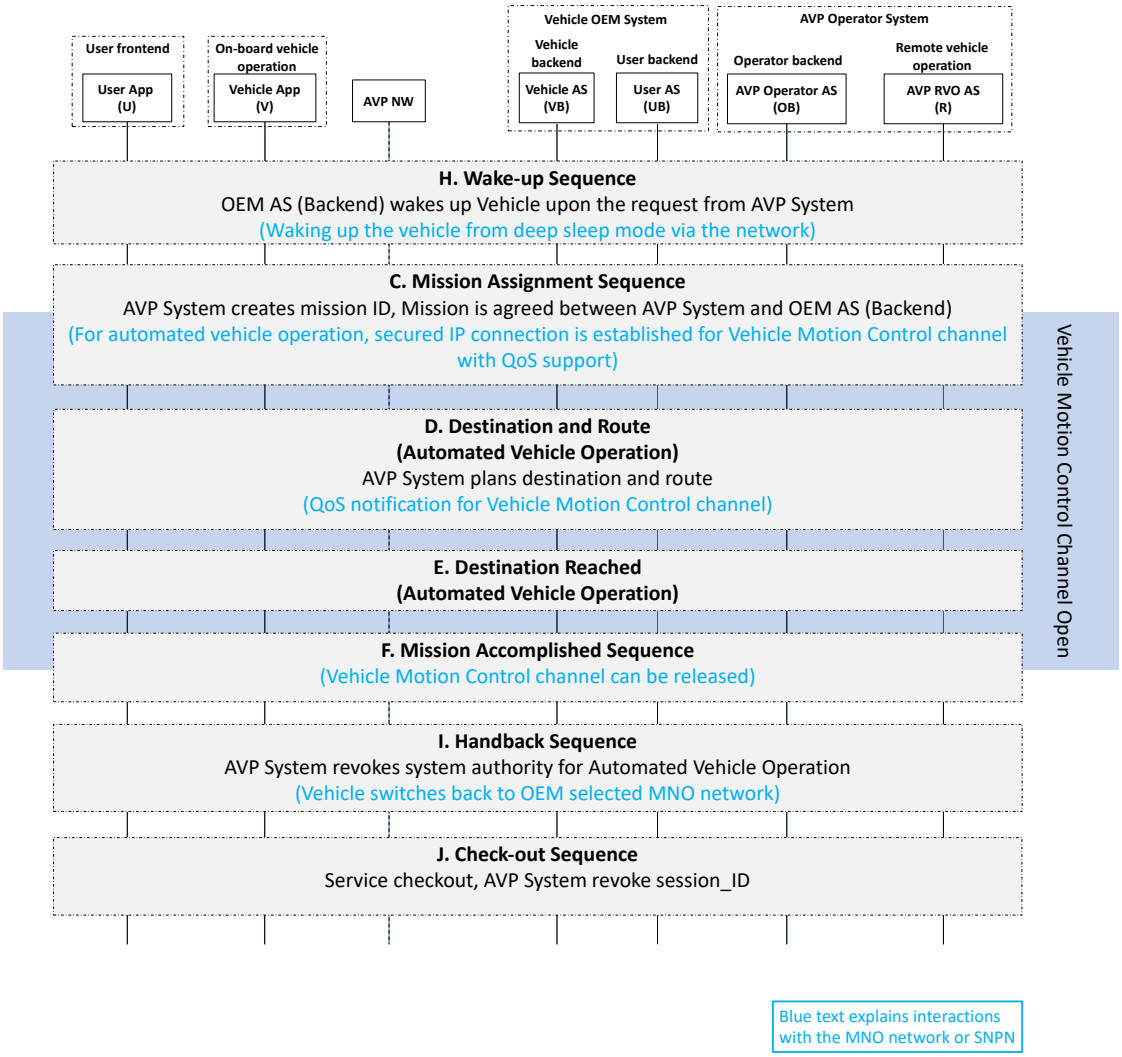


Figure 7: High-level communication sequences for AVP Type-2 retrieval process

7.3 Detailed communication sequences for AVP Type-2

7.3.1 A. Check-in sequence

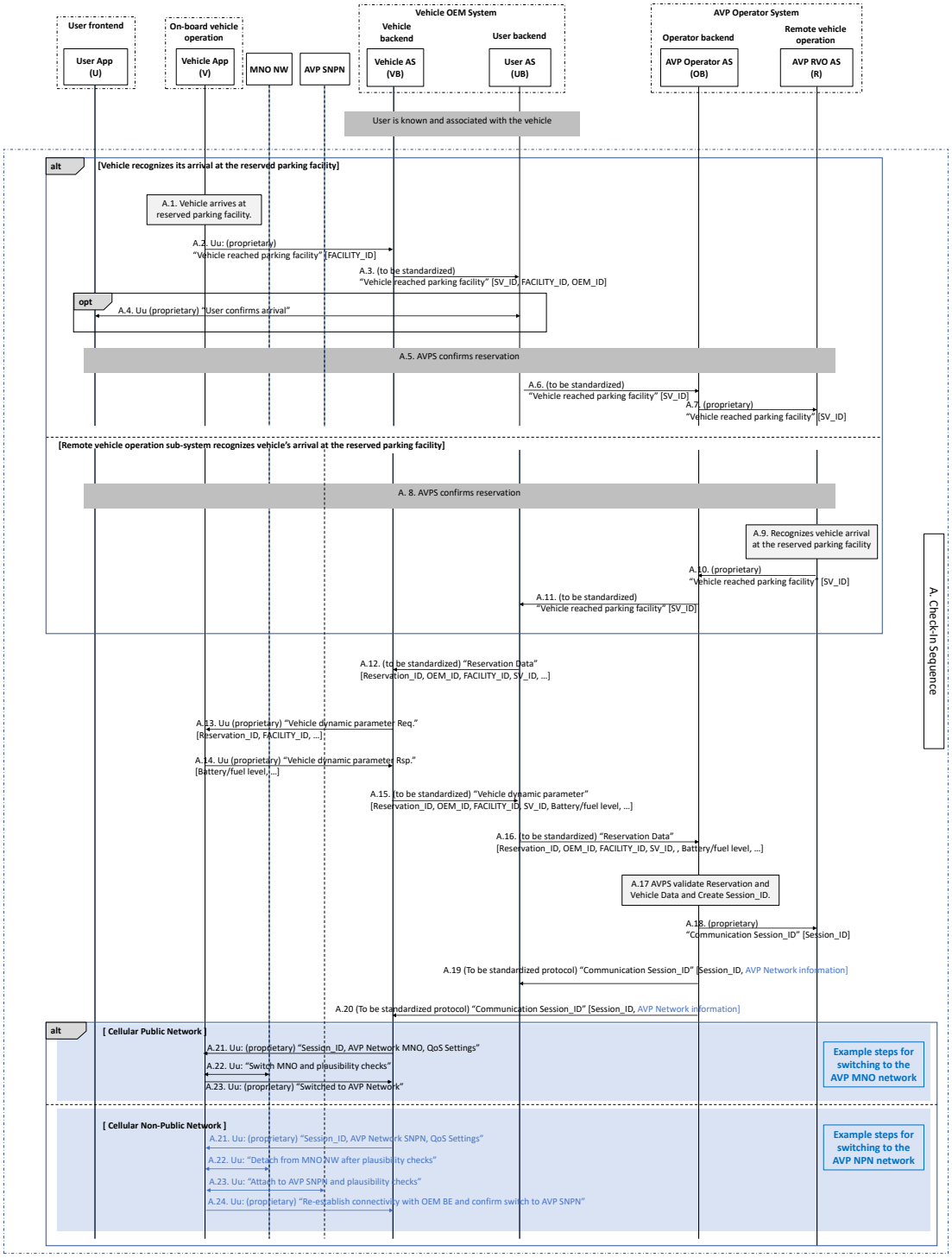


Figure 8: Communication sequence for 'check-in'

'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).
- If the AVP network is a SNPN network, 'AVP network information' includes at least the available PLMN IDs, the Network Identifier (NID) of the SNPN and ARFCN.
- If the AVP VMC network is PC5 Direct Communication , 'AVP network information' may include a new radio profile configuration (for example, RRC configuration) for AVP use.

For cellular public networks, 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 operator 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.

For cellular non-public network/SNPN, the vehicle UE/modem first needs to detach from MNO network, then it switches to SNPN mode and executes a 'network attach' command. The SNPN network has to be known to the UE/modem and necessary credentials have to be exchanged before.

- A22 includes the step to detach from the MNO network.
- A23 includes the step when the vehicle application instructs the modem to switch to a SNPN NW and the modem attaches to SNPN according to standard 3GPP procedures. Section 8.2.2 explains the SNPN aspects and network selection.
- A24 confirms the network change to the Vehicle Backend and re-establishes the connectivity including announcement of new IP after network change.

For PC5 Direct Communication-based VMC, basic cellular QoS settings should be negotiated over the selected Uu network, after which the vehicle awaits a VMC message over the PC5 Direct Communication channel.

7.3.2 B. Handover sequence

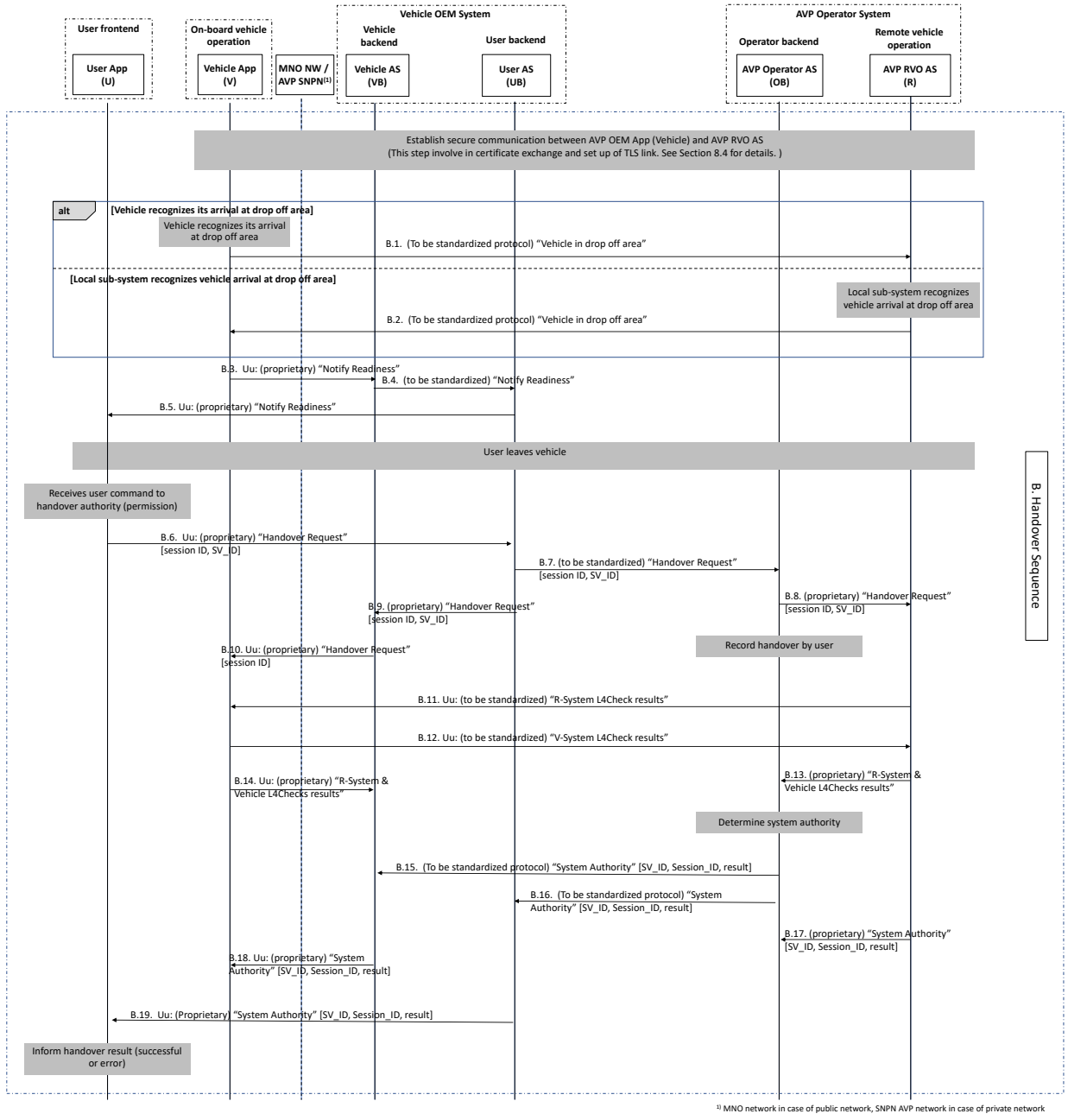


Figure 9: Communication sequence for 'handover'

Communications between AVP Vehicle App and AVP RVO AS (remote control) use secured IP-based sessions. The detailed communication sequence for establishing the secured communication session is presented in Section 8.4.

Note: The secured IP-based session is not applicable for non-IP PC5 Direct Communication , since it does not use the IP-based protocol stack nor standardised IT security methods described in Section 8.4.

7.3.3 C. Mission assignment sequence

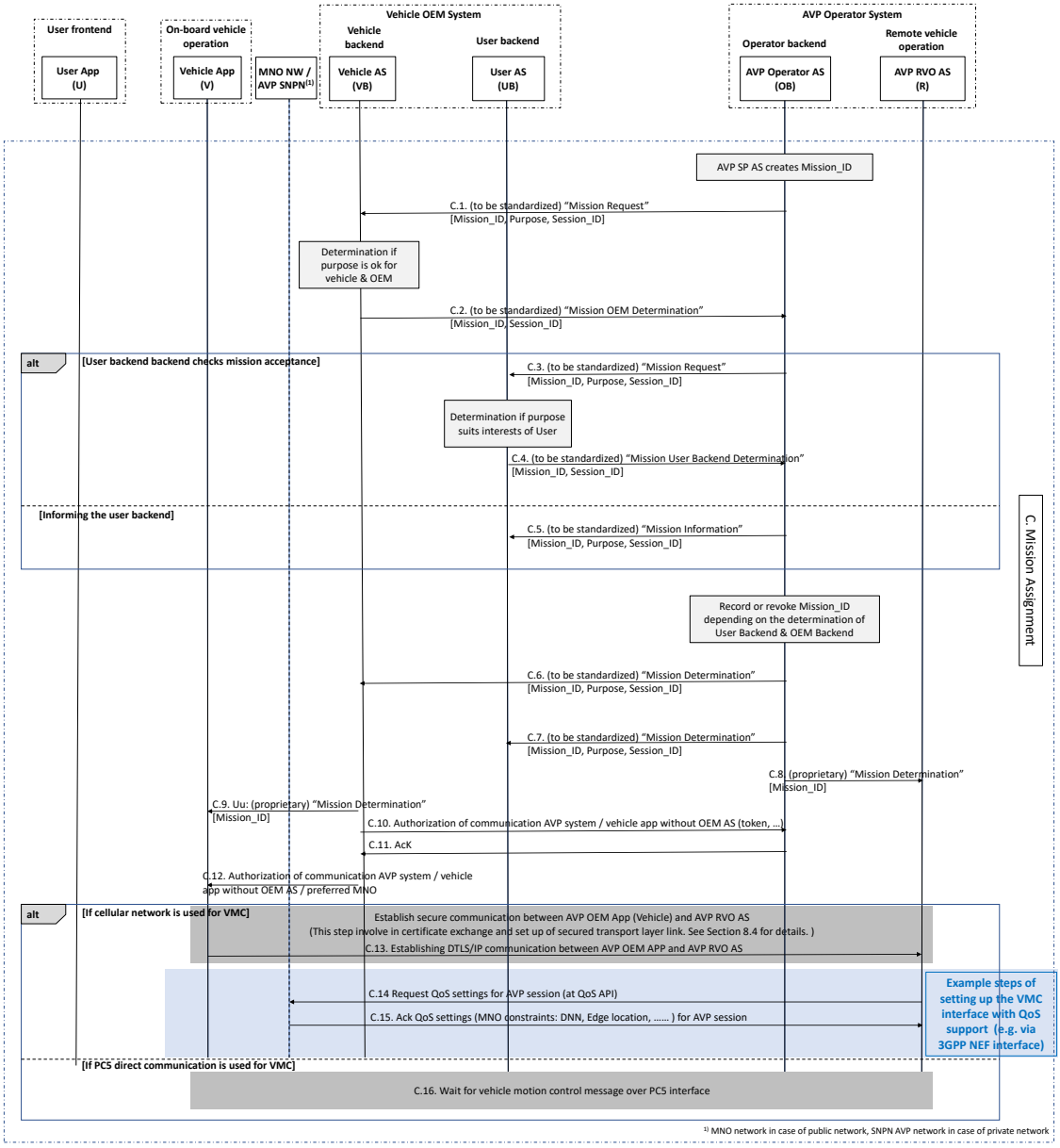


Figure 10: Communication sequence for 'mission assignment'

Step C.13, the communication between AVP Vehicle App (vehicle) and AVP RVO AS (remote control), uses secured DTLS/IP sessions. The detailed communication sequence for establishing the secured communication session is presented in Section 8.4.

Note: The secured IP-based session (C.13) is not applicable for non-IP PC5 Direct Communication , since it does not use the IP-based protocol stack nor standardised IT security methods described in Section 8.4.

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.

Step C.16 is only applicable for PC5 Direct Communication and the vehicle awaits reception of a VMC message over the PC5 interface.

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

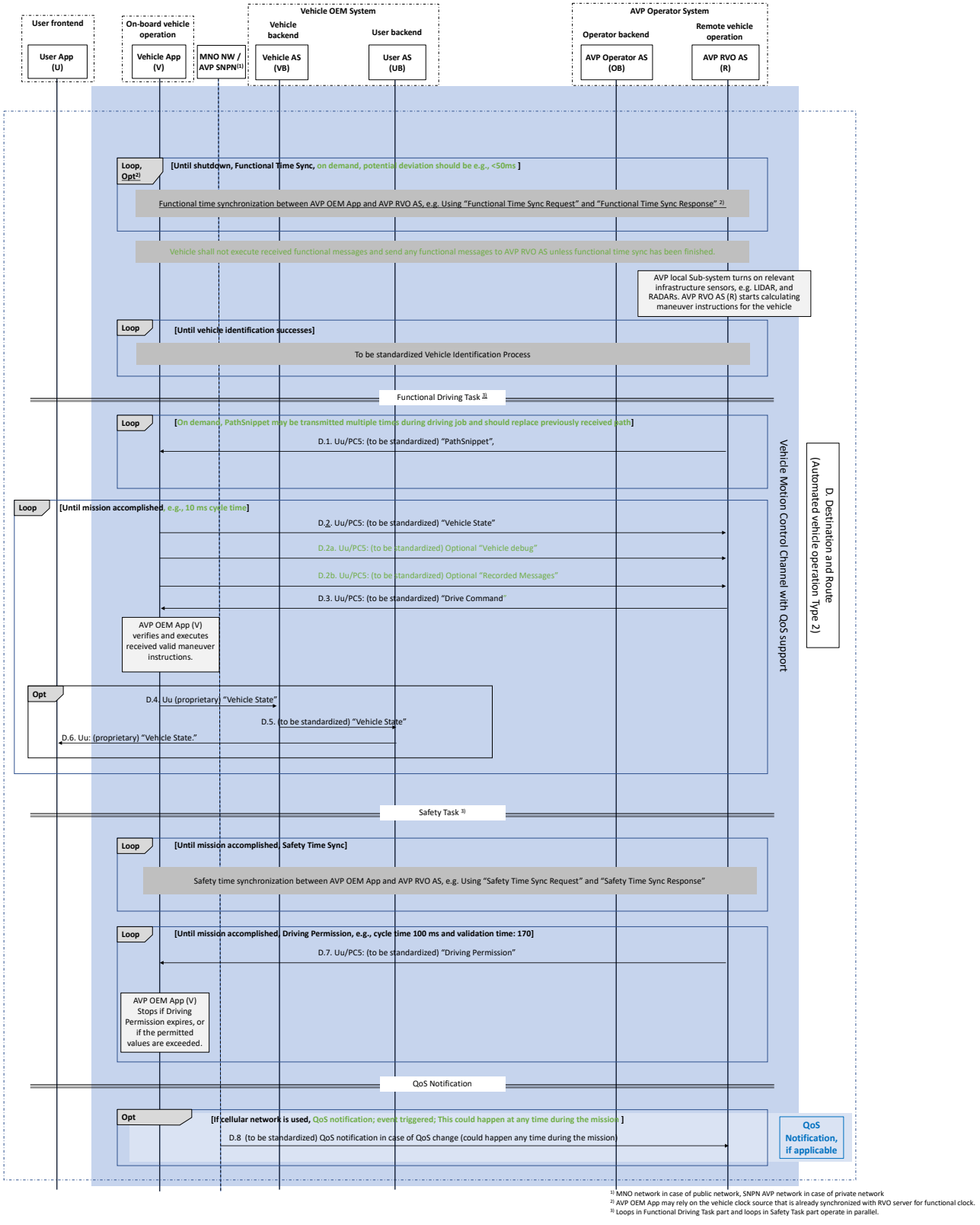
The communication sequence diagram of "destination and route" is shown in Figure 11, Figure 12a and Figure 12b for respective implementation options using the Uu interface and the PC5 interface. In this process, the functional driving tasks and safety tasks are separated. Each task has its own clock synchronisation and communication loops between the AVP Vehicle App and AVP RVO AS (remote control). Step D.7 'Driving Permissions' in Figure 11, Figure 12a and Figure 12b, 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, Figure 12a and Figure 12b are sample values and optional steps which may need some refinements according to actual implementation situation.

7.3.4.1 Uu-based implementation

For cellular networks and IP-based implementation, Figure 11 shows the communication sequence over the VMC, where the (to-be-standardised) messages for steps D.1, D.2, D.2a, D.2b, D.3, and D.7 terminate at the facilities layer of AVP RVO AS and AVP Vehicle App, respectively. Figure 22 in Section 8.3.2 shows the end-to-end protocol stacks.

Step D.8 is only applicable for cellular network-based implementations. In a cellular network, the QoS notification in step D.8 utilises the network exposure interface described in Section 8.1.3.



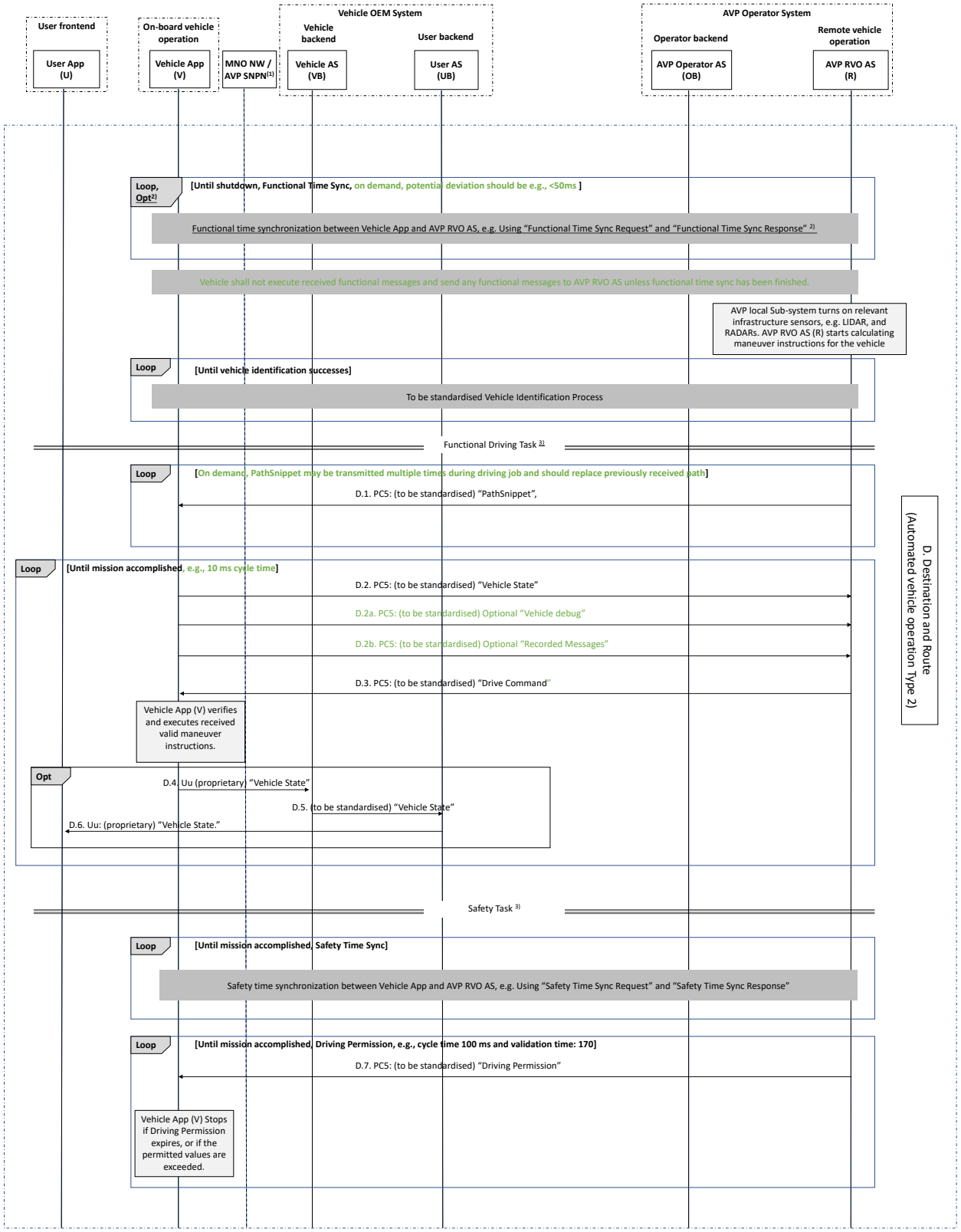
1) MNO network in case of public network, SNPN AVP network in case of private network
2) AVP OEM App may rely on the vehicle clock source that is already synchronized with RVO server for functional clock.
3) Loops in Functional Driving Task part and loops in Safety Task part operate in parallel.

Figure 11: Communication sequence for 'destination and route' – Uu-based implementation

7.3.4.2 PC5-based implementation

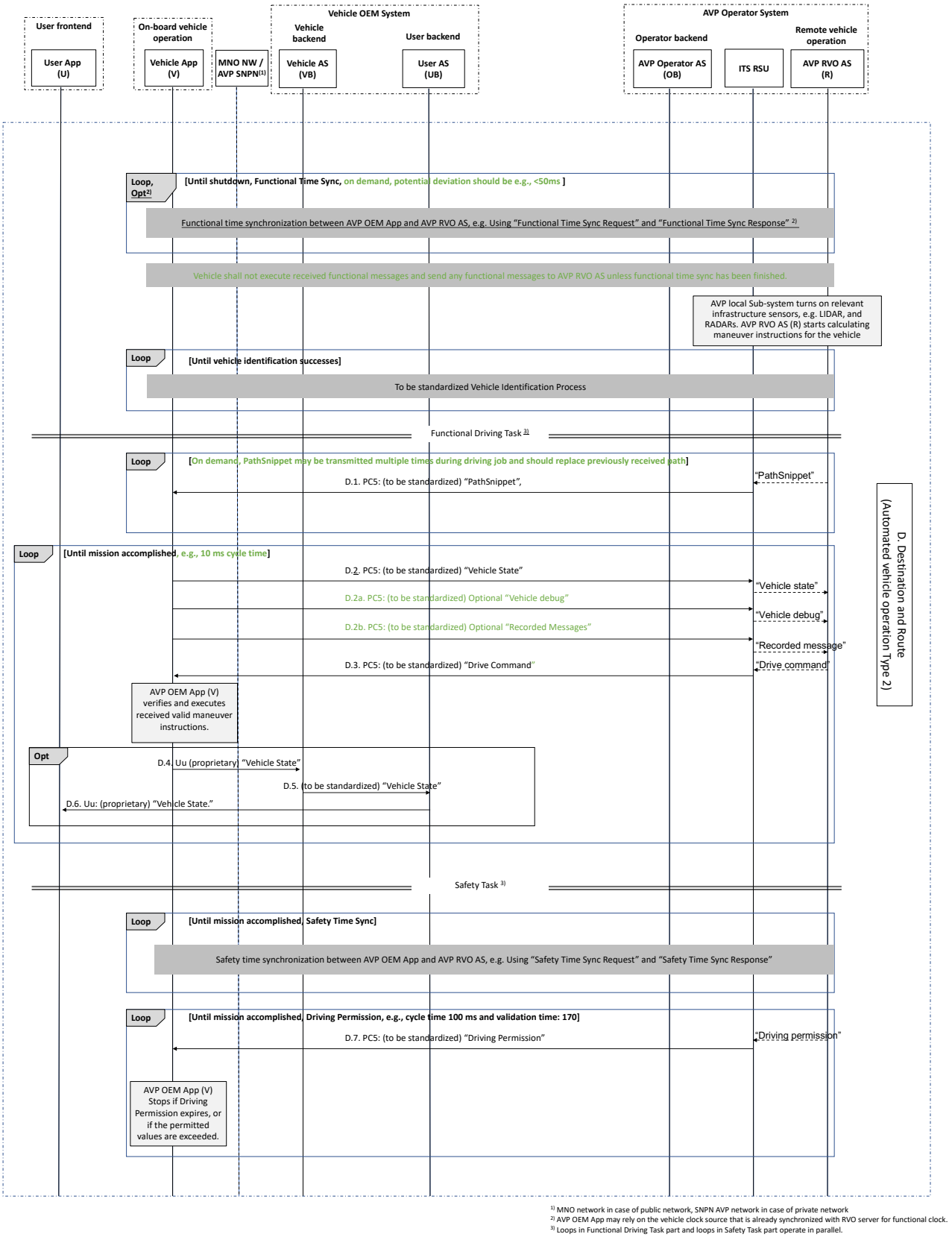
For PC5 Direct Communication-based solutions, there are several implementation options that have different locations of the facilities layer functions that terminate the (to-be-standardised) VMC messages between AVP RVO AS and AVP Vehicle App for steps D.1, D.2, D.2a, D.2b, D.3, and D.7.

- Figure 12a shows the sequence diagram for the implementation option where the facilities layer functions are located at AVP RVO AS. Figure 27 in Section 9.5 shows the corresponding end-to-end protocol stacks.
- Figure 12b shows the sequence diagram for another implementation option where the facilities layer functions are located at the RSU ITS Service, instead of AVP RVP AS. Figure 26 shows the end-to-end protocol stacks.



[1] MNO network in case of public network, SNPN AVP network in case of private network
[2] Vehicle App may rely on the vehicle clock source that is already synchronised with RVO AS for functional clock.
[3] Loops in Functional Driving Task part and loops in Safety Task part operate in parallel.

Figure 12a: Communication sequence for 'destination and route' – PC5 Direct Communication AVP RVO AS-based facilities layer



[1] MNO network in case of public network, SNPN AVP network in case of private network
[2] AVP OEM App may rely on the vehicle clock source that is already synchronized with RVO server for functional clock.
[3] Loops in Functional Driving Task part and loops in Safety Task part operate in parallel.

Figure 12b: Communication sequence for 'destination and route' – PC5 Direct Communication RSU-based facilities layer

The communication between ITS-RSU and AVP RVO AS is proprietary.

7.3.5 E. Destination reached (optional)

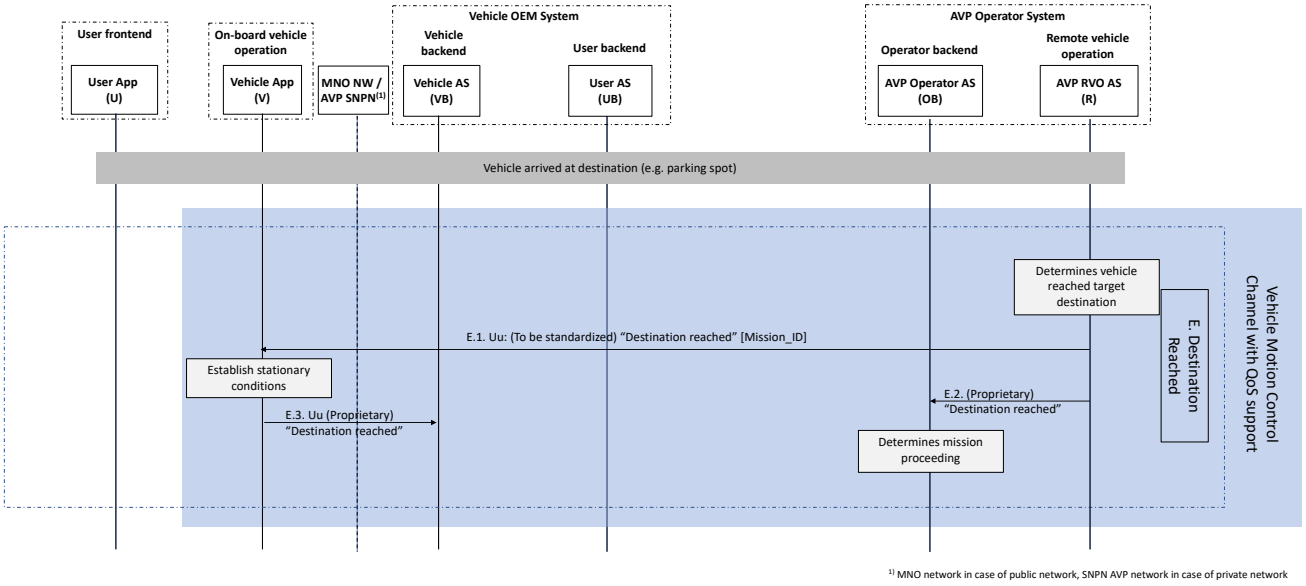


Figure 13: Communication sequence for 'destination reached'

7.3.6 F. Mission accomplished

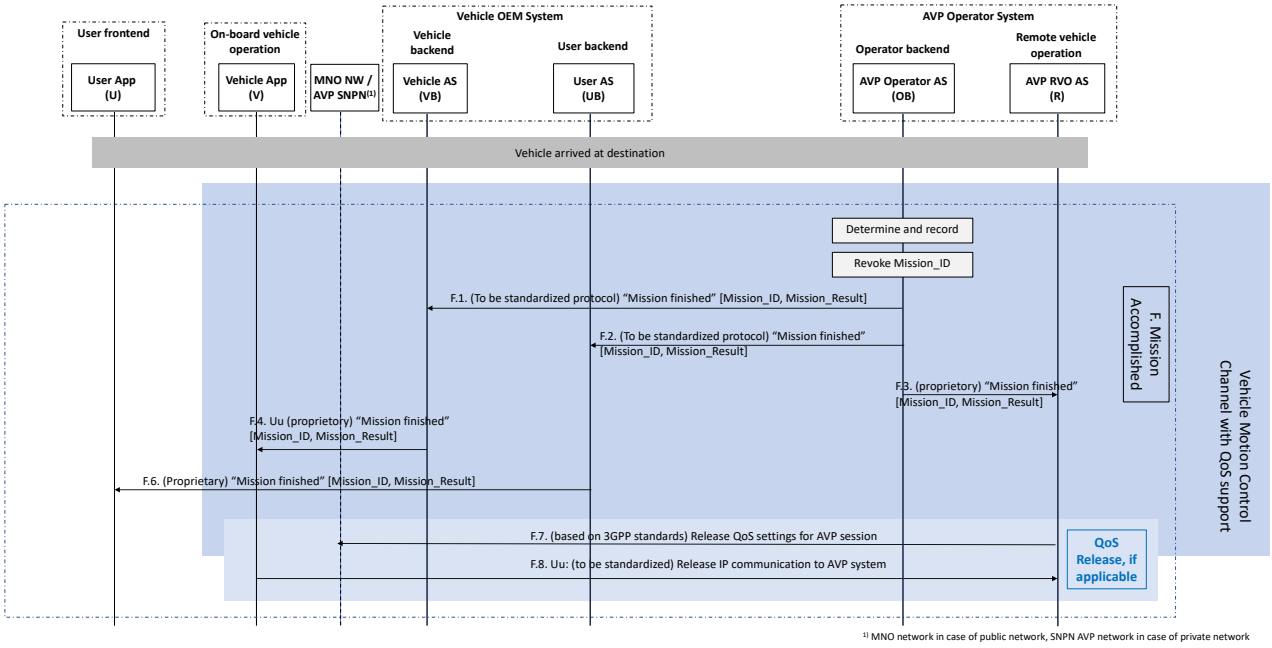


Figure 14: Communication sequence for 'mission accomplished'

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.

Note: Step F.7 and F.8 are not applicable for PC5 Direct Communication .

7.3.7 G. Sleep sequence

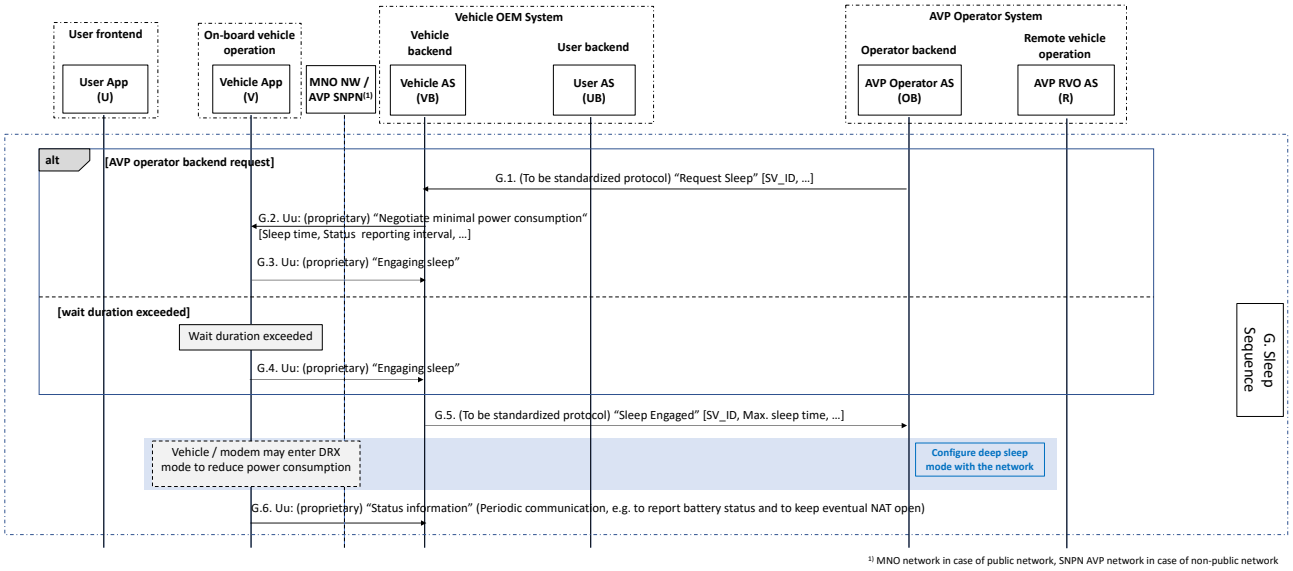


Figure 15: Communication sequence for 'sleep'

During sleep mode, optionally, the vehicle goes into DRX mode, which effectively discontinues the 'reception mode' for longer periods and also puts the modem part it into 'sleep mode' to save battery. This is further described in Section 8.1.5.

In order to know the valid IP address of the vehicle at any time the Vehicle AS (Vehicle BE) may use, for example, the RADIUS-based interface of the AVP Operator System's SNPN core for notifications in the event that the IP address changes or is re-assigned (e.g. if the lease time of the IP address has expired).

In step G.6 the vehicle may send 'keep alive' messages with optional additional status information.

7.3.8 H. Wake-up sequence

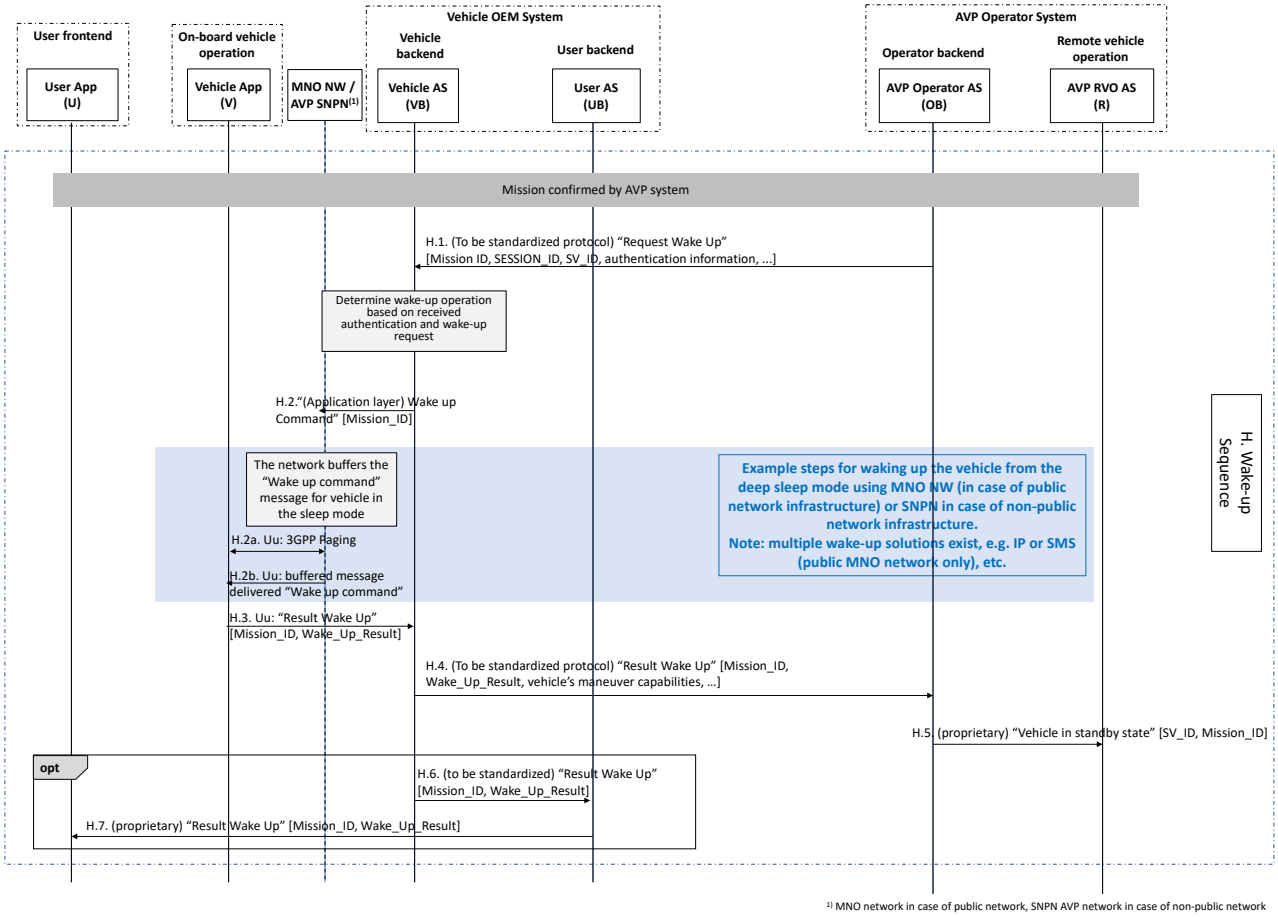


Figure 16: Communication sequence for 'wake-up'

In step H.2a, the cellular network pages the UE (vehicle). H.2b shows the vehicle receiving the buffered message from the Vehicle 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

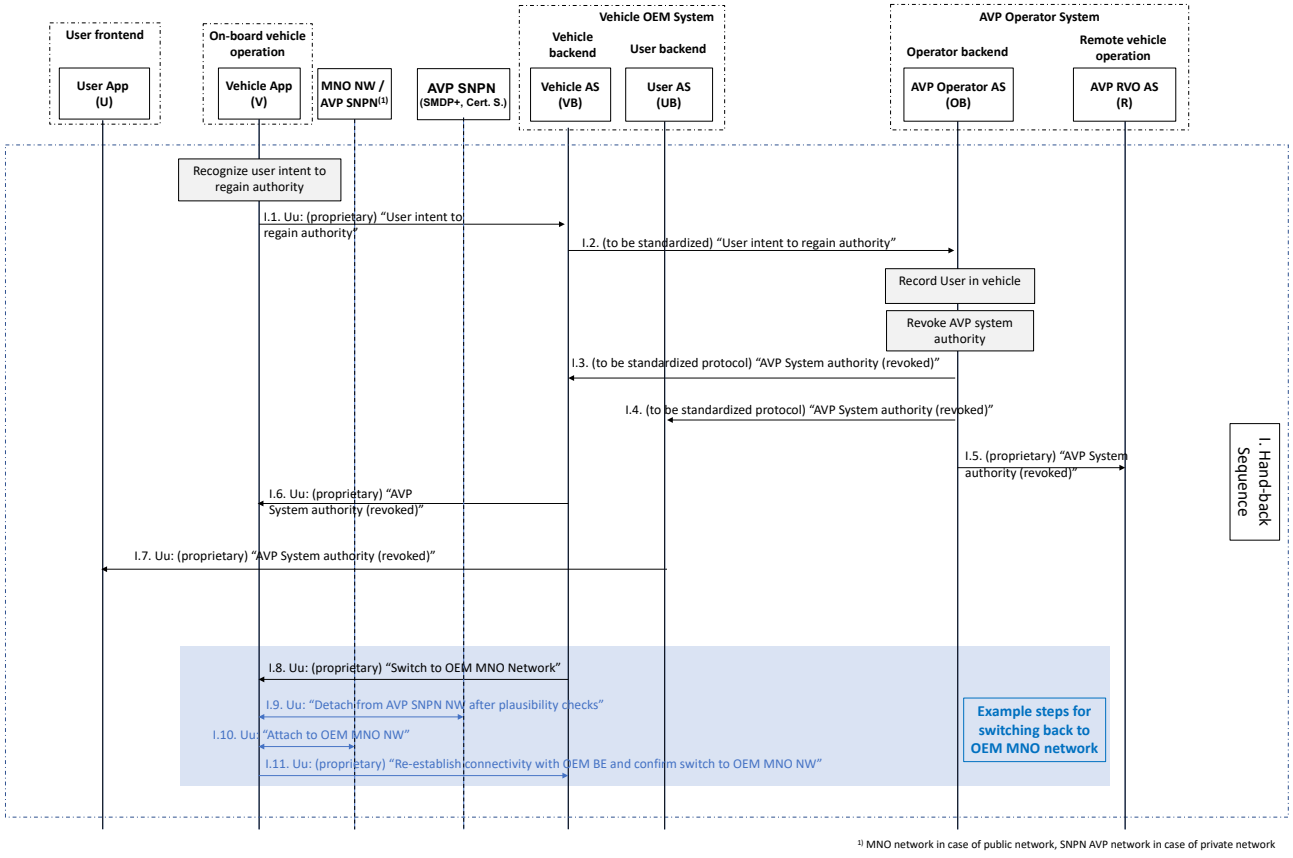


Figure 17: Communication sequence for 'hand-back'

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 Vehicle Backend instructs the vehicle to switch back to the MNO used prior to the AVP session.

In I.8 if the vehicle needed to switch to a SNPN for the AVP session, then when leaving the parking facility the Vehicle Backend instructs the vehicle to deactivate the SNPN mode and switch back to MNO used prior to the AVP session.

I.9 is specific to SNPN and in I.9 the application on the vehicle side instructs the modem to deactivate the SNPN mode and detach from the SNPN network.

In I.10, 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.

In I11, the application on the vehicle side confirms the network switch and re-establishes connectivity with the Vehicle Backend (e.g. announce new IP address) after the network has changed.

7.3.10 J. Check-out sequence

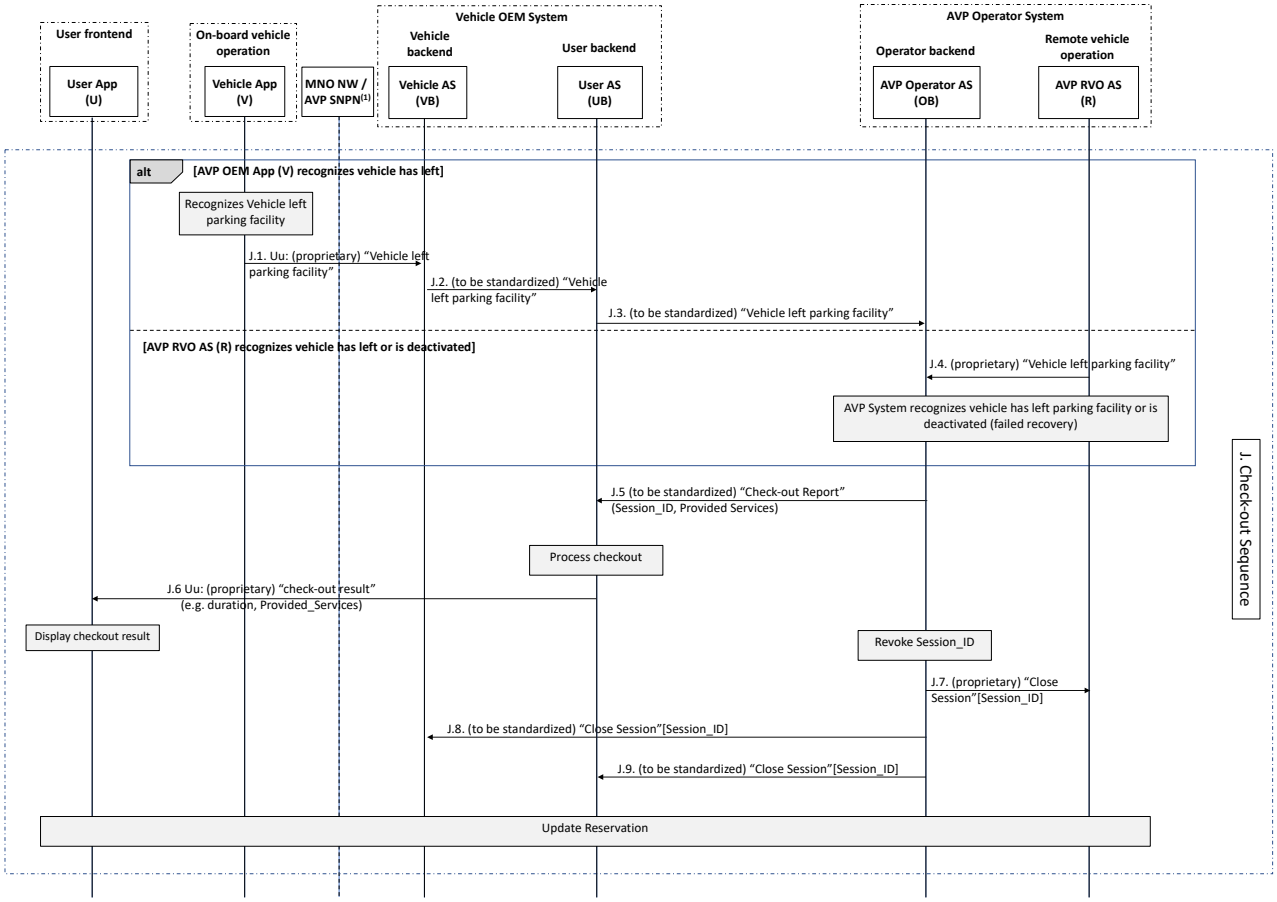


Figure 18: Communication sequence for 'check-out'

8 Implementation considerations for cellular network solutions

Based on the application-level system architecture for AVP Type-2 in Figure 2, Figure 19 illustrates how cellular networks enable the end-to-end IP connectivity for key system interfaces in actual implementations. Particularly, for the VMC interface between AVP RVO AS and Vehicle App, either cellular Public Networks (PN) or Stand-alone Non-Public Networks (SNPN) can transparently transfer VMC messages on top of secure IP connections. This chapter presents the implementation considerations for cellular network solutions covering both PN and SNPN.

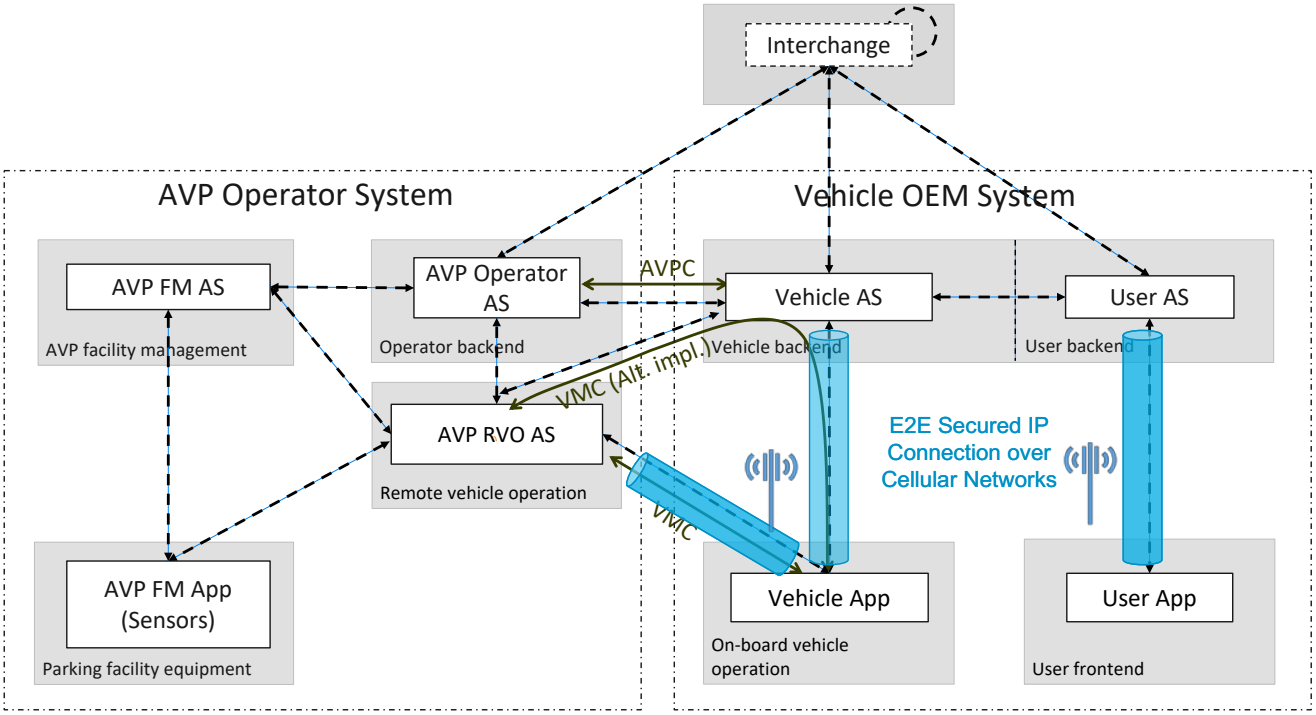


Figure 19: Architecture of cellular network-based AVP implementation

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 served 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 Vehicle Backend system from the parking facility system. The Vehicle 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 Vehicle Backend) about the ‘preferred network’ comprises frequency bands (e.g. 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 so-called 'Network Exposure' interfaces interacting with the cellular network.

8.1.3.1 Network exposure realisations

The 5G system also supports 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.)

8.1.3.2 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: Unless QoS Class Identifier (QCI) or 5G QoS Identifier (5QI) values standardised in 3GPP [10] are used, the same QCI or 5QI value may have different behaviours in different Network Slices. Section 8.1.3.2 provides more details about how UE can use network slicing for applications like AVP.

- PDU session needs to be established, when the UE has packets to transmit. One or more PDU sessions can be established 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[2] 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.

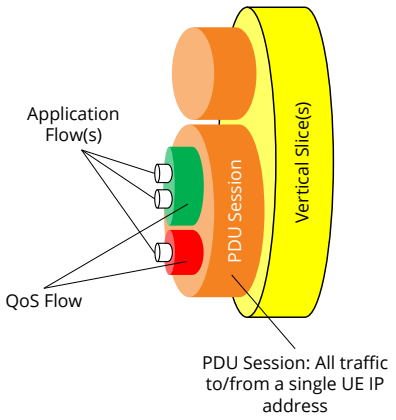


Figure 20: 3GPP QoS assurance mechanisms

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 Vehicle Backend, or a map download is performed).

Even when the network is delivering the requested QoS – the actual QoS performance may change due to RAN being temporary unable to fulfil it. The network has mechanisms to handle such events, e.g. Alternative QoS Profile, QoS Sustainability analytics, QoS monitoring. Additional, proper network planning and QoS/priority assignment can also reduce the probability of such events.

[2] 'Application Flow' refers to data traffic of an application that certain QoS policy can be applied. Application Flow can be described using descriptors e.g. IP 5-Tuple.

8.1.3.3 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.

UE 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.

8.1.4 Global availability and roaming

8.1.4.1 Authentication and roaming

Authentication is required for different layers; network access and the application-level.

- 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 Considerations for the cellular non-public network

Non-Public Networks (NPNs) are intended for the sole use of a private entity such as an AVP Garage operator and may be deployed in a variety of configurations utilising both virtual and physical elements. Specifically, they may be deployed as completely standalone networks, they may be hosted by a PLMN, or they may be offered as a slice of a PLMN.

In any of these deployment options it is expected that unauthorised UEs (those that are not associated with the AVP service) will not attempt to access the non-public network, which could result in resources being used to reject that UE and thereby not be available for the UEs of the AVP service. It is also expected that UEs of the AVP service will not attempt to access a network they are not authorised to access. For example, some AVP service UEs may be restricted to only access the non-public network of the AVP operator, even if PLMN coverage is available in some parts of the AVP service area. Other AVP service UEs may be able to access both a non-public network and a PLMN where specifically allowed.

There are two NPN types defined in 3GPP:

- Public Network Integrated NPN (PNI-NPN), i.e. a non-public network deployed with the support of a PLMN.
- Stand-alone Non-Public Network (SNPN), i.e. operated by an NPN operator and not relying on network functions provided by a PLMN.

8.2.1 Public network integrated non-public network

Public Network Integrated NPNs are those made available via PLMNs, and the UE shall have a subscription for the PLMN in order to access PNI-NPN. Therefore, the procedures for PNI-NPNs are the same as for PLMNs. From a device as well as from the AVPOS perspective, PNI-NPN can be used agnostic to the use of PLMN. Further information about PLMN is provided within the Public Network implementation description for AVP.

8.2.2 Stand-alone non-public network

SNPN 5G System deployments are based on the architecture shown below, using the architecture for 5G Core with untrusted non-3GPP access for access to services via a PLMN. The SNPN Core is equivalent to the HPLMN Core, and the SNPN RAN is equivalent to the 'Untrusted Non-3GPP Access' entity. The SNPN 5G Core is using the same procedures as for Public Network Core, except as described below. The SNPN 5G RAN is using the same procedures as for Public Network RAN, except as described below. For security and access control then the SNPN 5G RAN is considered by the SNPN 5G Core as an 'Untrusted Non-3GPP Access' and it does not follow the same security and access procedures as a Public Network. The security and access procedures for SNPN are described elsewhere in this document.

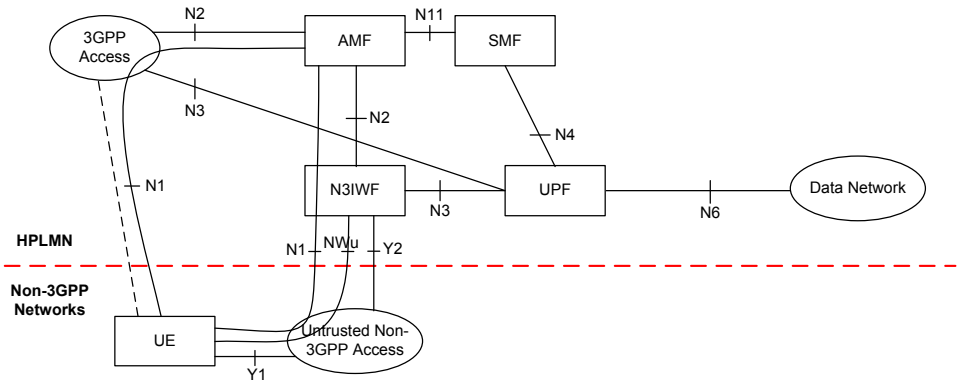


Figure 20a: Non-roaming architecture for 5G core network with untrusted non-3GPP access

8.2.2.1 SNPN core network aspect

SNPN 5G deployments are based on the architecture for the 5G Core, with untrusted non-3GPP type security and access procedures used to access the SNPN services, and with the additional functionality specific to SNPN, as explained.

As an exception, the following 5G System features and functionalities are not supported for SNPNs:

- Interworking with LTE/EPS.
- Emergency services.
- Roaming, e.g. roaming between SNPNs.
- Handover between SNPNs, between SNPN and PLMN or PNI NPN.
- Cellular IoT 5G System optimisations.
- Closed Access Groups (CAG).

8.2.2.2 SNPN RAN aspects

In the current Release 16, direct access to the SNPN services is specified using 3GPP RAN access type only. No other access type is supported for the SNPN Core Network in Release 16.

In general, the same RAN principles as with a PLMN apply to SNPN with several exceptions.

NG-RAN nodes which provide access to SNPNs broadcast the following information:

- One or multiple PLMN IDs.
- List of NIDs per PLMN ID identifying the non-public networks that NG-RAN provides access to.
- Optionally a human-readable network name per NID.

UEs operating in SNPN access mode only (re)select cells within the selected/registered SNPN and a cell can only be considered as suitable if the PLMN and NID broadcast by the cell matches the selected/registered SNPN.

The NG-RAN node is aware of the SNPN ID(s) supported by neighbour cells. At the time of handover, cells that do not support the serving SNPN ID are not considered as candidate target cells by the source NG-RAN node. The target NG-RAN node performs access control. If it cannot accept the handover for the serving SNPN, the target NG-RAN node fails the handover including an appropriate cause value.

8.2.2.3 SNPN UE (device) aspects

An SNPN-enabled UE supports the SNPN access mode. When the UE is set to operate in SNPN access mode the UE only selects and registers with SNPNs over Uu. If a UE is not set to operate in SNPN access mode, even if it is SNPN-enabled, the UE does not select and register with SNPNs. A UE which is not set to operate in SNPN access mode performs normal PLMN selection procedures. Details of activation and deactivation of SNPN access mode are specific to the UE implementation.

For a UE capable of simultaneously connecting to an SNPN and a PLMN, the setting for operation in SNPN access mode is applied only to the Uu interface for connection to the SNPN. When a UE capable of simultaneously connecting to an SNPN and a PLMN is not set to operate in SNPN access mode, the UE only performs PLMN selection (using the Uu interface for connection to the PLMN). A UE supporting simultaneous connectivity to an SNPN and a PLMN applies the network selection and the cell (re-)selection as applicable for the access and network for SNPN and PLMN respectively. Whether the UE uses SNPN or PLMN for its services is implementation dependent.

8.2.2.4 UE network selection in SNPN access mode

When a UE is set to operate in SNPN access mode the UE does not perform normal PLMN selection procedures. UEs operating in SNPN access mode read the available PLMN ID's and list of available NID's from the available broadcast system information and use them for network selection.

For automatic network selection, the UE selects and attempts to register with the available SNPN identified by a PLMN ID and NID for which the UE has SUPI and credentials. If multiple SNPNs are available that the UE has respective SUPI and credentials for, then how the UE selects an SNPN is based on UE implementation.

For manual network selection, the UE will provide to the user the list of SNPNs (each is identified by a PLMN ID and NID) and related human-readable names (if available) of the available SNPNs the UE has respective SUPI and credentials for. The user will then select one of these available SNPN.

8.2.2.5 SNPN authentication methods

8.2.2.5.1 Embedded subscriber identification module (eSIM) profile switching

In eSIM profile switching, the device is equipped with an eSIM and subscription profiles for both the PN and NPN. As the device moves from the coverage area of one network to the other, the device switches profile accordingly to be able to establish connectivity through the appropriate network. Switching eSIM profiles can be triggered either by the user or by the backend system. Network access authentication using eSIM applies the same mechanisms as used in public networks with traditional physical SIM.

eSIM has been considered in the automotive industry, e.g. a vehicle can use one eSIM profile for 5G network in the factory and switch to another eSIM profile (from the contracted MNO) for connected vehicle outside the factory. For the AVP use case, eSIM profile switching can be a technical solution for network authentication when the vehicle switches from the PN to the AVP SNPN network.

GSMA has worked on the framework and solutions of eSIM provisioning [6] [9].

8.2.2.5.2 Extensible authentication protocol – transport layer security (EAP-TLS)

EAP-TLS follows a similar principle as the eSIM profile switching, but instead uses digital certificates and EAP-TLS processes to attach to the NPN.

Extensible Authentication Protocol (EAP) is an authentication framework frequently used in network and internet connections. Defined in RFC 3748 and updated by RFC 5247. EAP framework is introduced in 3GPP 5G networks for use in network access authentication (See 3GPP TS 33.501). EAP-TLS (RFC 5216) using digital certificate may be used in network access authentication when attaching to non-public networks. Note: According to the current 3GPP specification, EAP-TLS cannot be used to access a public network.

To use EAP-TLS for the NPN network supporting the AVP use case, the following three general steps are needed:

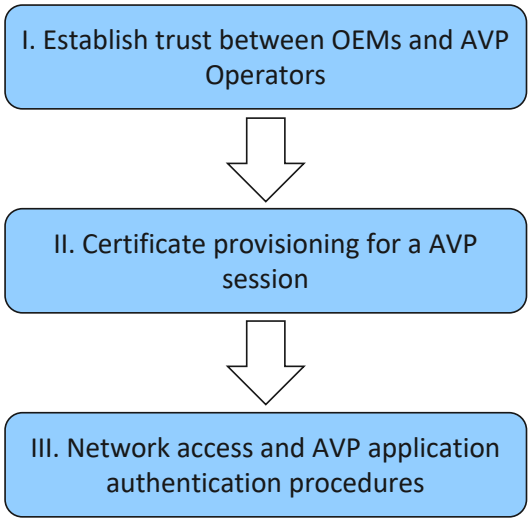


Figure 20b General steps of using EAP-TLS for the NPN network supporting AVP use case

Step I: OEM vehicle models and AVP garages need to be mutually approved or approved by, for example, technical inspection institutes for using/providing AVP services. The OEM vehicle backend and AVP Operator backend establish a trust relationship either directly with each other or via a centralised organisation.

Step II: A digital certificate is created and provisioned to a vehicle for a booked AVP session. This step happens during the AVP service booking process well before the vehicle arrives at the parking facility.

Step III: When the vehicle is at the parking facility (drop-off/pick-up areas), an EAP-TLS network authentication process is performed for access to the NPN following 3GPP TS 33.501. This covers mutual authentication between the vehicle and AVP network using AVP session certificate from step II. The AVP session certificate for vehicle can also be used for AVP application authentication and security, e.g. establishment of a TLS session between vehicle and AVP Operator System.

8.2.2.6 SNPN access to PLMN services

A UE that is connected to an SNPN may still be able to access services which are only available in a PLMN. To access PLMN services, a UE in SNPN access mode that has successfully registered with an SNPN may perform an additional registration via the SNPN User Plane to a PLMN, using the credentials of that PLMN. This follows the architectural principles in 3GPP shown below (including the optional support for PDU Session continuity between PLMN and SNPN using the Handover of a PDU Session) and with the SNPN taking the role of 'Untrusted Non-3GPP Access'.

In order to obtain access to PLMN services when the UE is camping in RAN of an SNPN, the UE obtains IP connectivity, discovers and establishes connectivity to an N3IWF in the PLMN. In the figure below, the N1 (for NPN) represents the reference point between UE and the AMF in SNPN. The NWu (for PLMN) represents the reference point between the UE and the N3IWF in the PLMN for establishing secure tunnel between UE and the N3IWF over the Stand-alone Non-Public Network. N1 (for PLMN) represents the reference point between UE and the AMF in PLMN.

QoS differentiation in the SNPN can be provided on per-IPsec child Security Association basis by using the UE or network requested PDU Session Modification procedure. The N3IWF is preconfigured by PLMN to allocate different IPsec child security associations for QoS Flows with different QoS profiles.

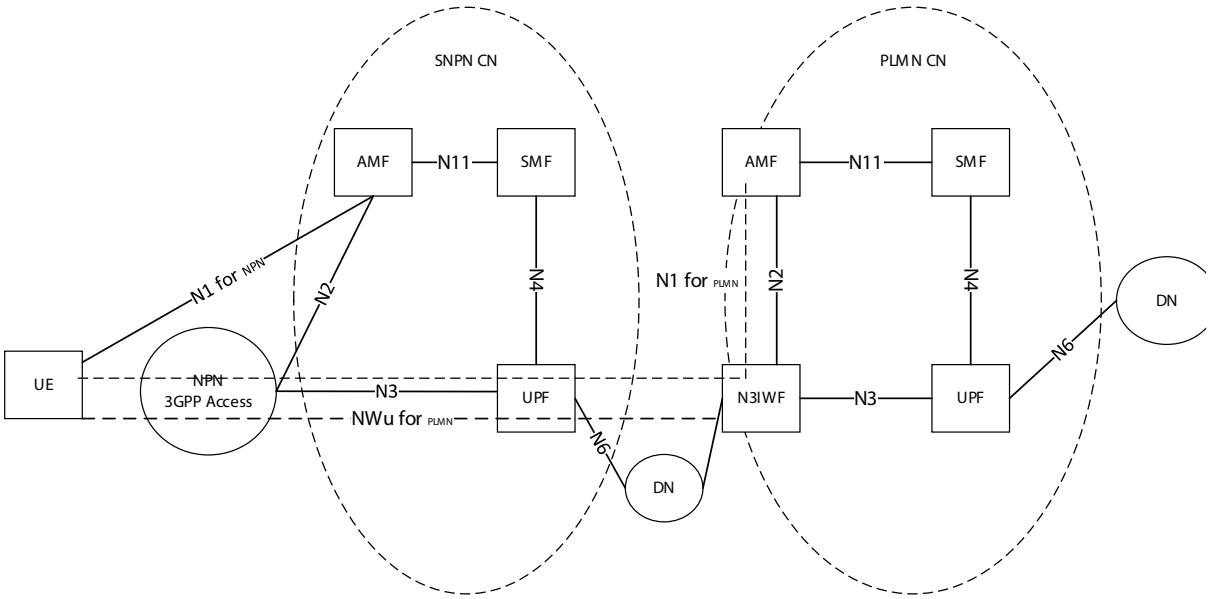


Figure 20c: Access to PLMN services via stand-alone non-public network

8.3 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.

8.3.1 Vehicle AS and AVP Operator System interaction

As shown in the initial architecture (Figure 2), the AVP Control (AVPC) interface between AVP operator backend (AVP Operator System) and Vehicle 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.

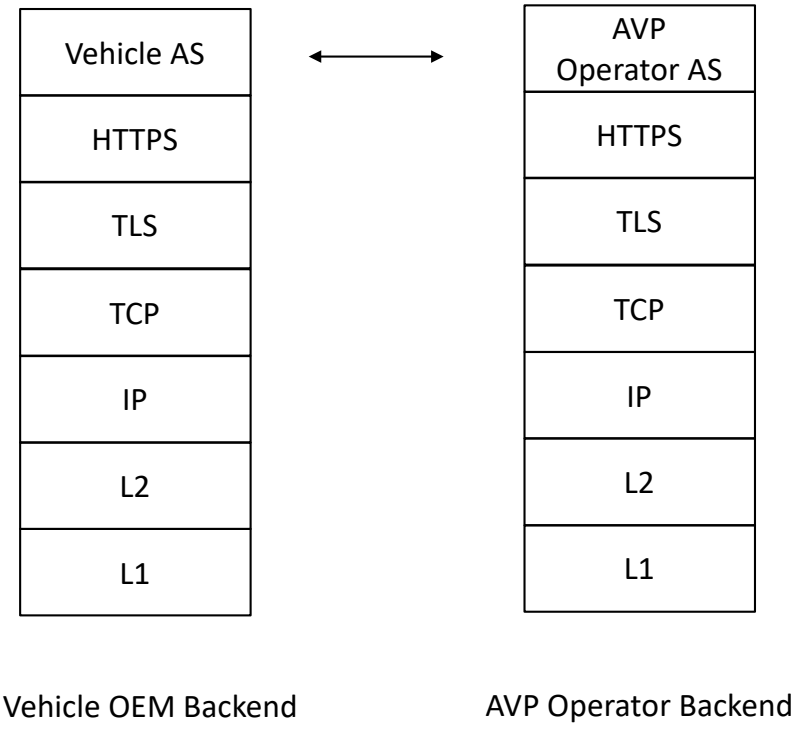


Figure 21: Example protocol stacks for Vehicle AS and AVP Operator AS interaction

As an example, Figure 21 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.

8.3.2 Vehicle motion control interface

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

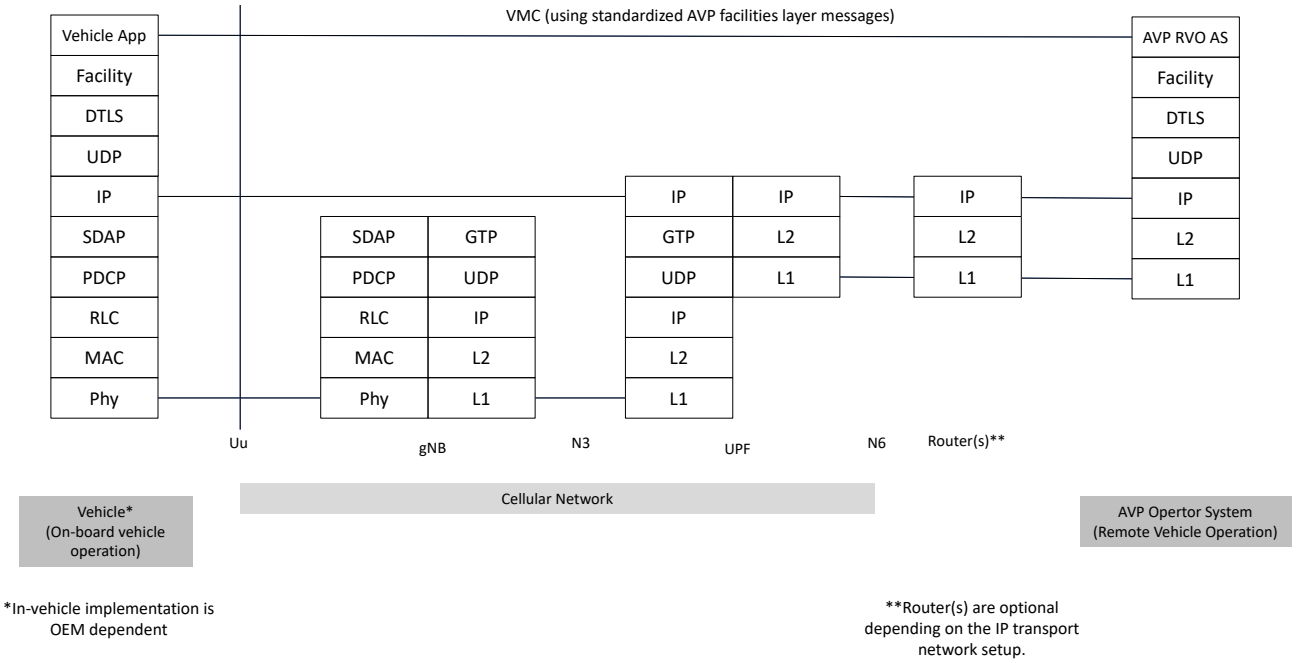


Figure 22: Example protocol stacks for vehicle motion control

Figure 22 shows an example end-to-end protocol stacks when a vehicle AVP Vehicle App (left) communicates with an AVP Operator 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.

In Figure 22, the protocol stacks at or within the vehicle and the AVP Operator System are simplified examples. In real implementation, the AVP Vehicle App and facilities layer can be implemented, e.g. in the Electronic Control Unit (ECU), which receives and transmits the AVP facilities layer messages from/to the AVP Operator System via a different in-vehicle component, e.g. the Telematics Control Unit (TCU) and in-vehicle network. In this example, the TCU acts as the gateway for access to other in-vehicle functions. The exact implementation is up to the car OEMs. Similarly, the AVP Operator System may include multiple IP routers forwarding the AVP facilities layer messages to/from the AVP RVO AS.

If the alternative implementation of VMC in Figure 2 is used, i.e. Vehicle AS acts as proxy/FW between vehicle and AVP Operator System, then proprietary protocols can be used to transport the facilities layer message between Vehicle AS and vehicle (i.e. only the Vehicle AS needs to be compliant with all protocol layers).

UDP (DTLS) is used to transfer the facility layer message as a payload on an IP connection between the vehicle and AVP Operator System, i.e. only one vehicle is addressed per IP connection. The AVP Operator System can simultaneously support multiple IP connections with different vehicles. IP connection is initiated by the vehicle to avoid potential NAT problems. After establishment, the IP connection can be used bi-directionally. The encrypted DTLS session will protect the data privacy of AVP users. The certificate handling for DTLS is explained in Section 8.4.

8.4 Communication sequence for IP and security session

This section presents the example sequence for establishing secured session for IP-based communication protocol stacks using digital certificates. This sequence can used in the communication sequences where secured IP communication sessions are needed. Figure 21 illustrates an example communication sequence for IP session with security.

Three prerequisites for this security sequence are:

- Pre-requisite 1: The secured communication between Vehicle and Vehicle Backend exists, e.g. OEM TLS, between Vehicle App and Vehicle AS.
- Pre-requisite 2: Trust relation has been established between Vehicle Backend (Vehicle AS) and AVP Operator Backend (AVP Operator AS). This may include the necessary information exchange for certificates, addresses, etc.
- Pre-requisite 3: Secure connection has been established, e.g. TLS, between Vehicle Backend (Vehicle AS) and AVP Operator Backend (AVP Operator AS).

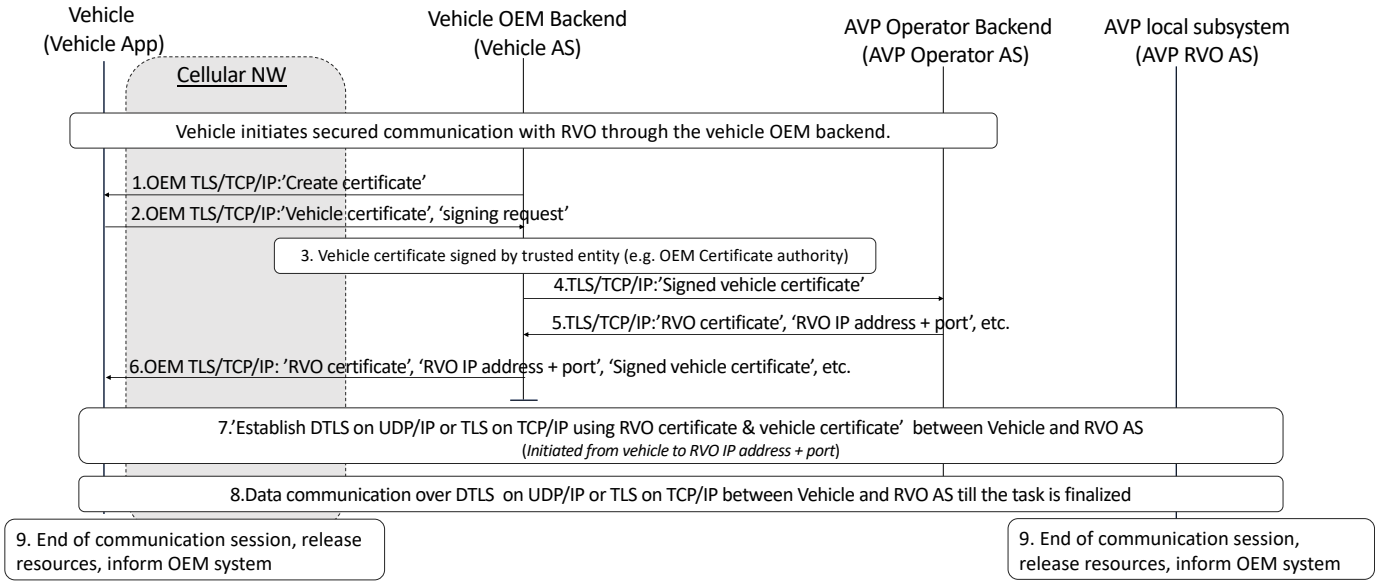


Figure 23: Example of communication sequence for IP session with security

Notes:

- In this example, the AVP Operator AS also owns the 'RVO certificate', i.e. the digital certificate of AVP RVO AS.
- UDP or TCP can be used between AVP Vehicle App and AVP RVO AS depending on the need of application layer protocols. This communication sequence for creating and exchanging digital certificates is applicable for both DTLS and TLS sessions.
- In step 7, standard IT security principles for establishing and operating DTLS and TLS using X.509 certificates are used.
- In step 9, one or both sides may end the secured communication session.

9 Implementation considerations for PC5 direct communication-based vehicle motion control

This chapter describes the implementation of PC5 Direct Communication for the VMC interface between the AVP RVO AS and the (AVP) Vehicle App as illustrated in Figure 2.

Two main implementation architectures are considered:

- Split RSU/RVO architecture described in Section 9.1.1.
- Collocated RSU/RVO architecture ('Smart RSU') described in Section 9.1.2.

The following sections details the above implementation architectures as well as considerations for using direct communication-based VMC and related ITS security mechanism and protocol stacks.

The interfaces indicated by dashed lines in Figure 24 and Figure 25, except for the interface over PC5, are proprietary.

9.1 Implementation architecture options for PC5 direct communication-based AVP vehicle motion control

9.1.1 Split RSU/RVO architecture

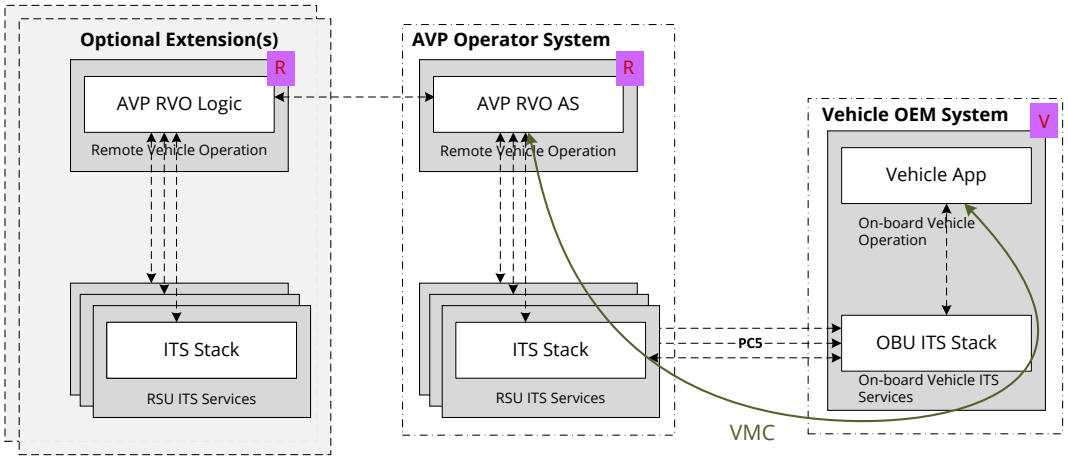


Figure 24: Split RSU/RVO architecture

The basic implementation architecture of AVP with PC5 Direct Communication-based VMC would consist of an AVP RVO AS controlling one or more RSUs (depending on coverage conditions).

In this type of deployment, the AVP RVO AS would need to be aware of the coverage area of each RSU and deliver the vehicle control messages to the RSU under which coverage the vehicle is currently located.

Additionally, in this implementation architecture the facilities layer, responsible for encoding and decoding the VMC messages, can be implemented in several locations:

- On the AVP Operator System side:
  - As part of the AVP RVO AS (as in the cellular-based implementation described in Section 8). In this case, the RSU forwards encoded VMC messages between AVP RVO AS and AVP Vehicle App.
  - Reusing the existing ITS stack in the RSU: when utilising the existing ITS stack in the RSU, the RSU's facilities layer encodes and decodes the VMC messages to/from vehicles. The AVP RVO AS and RSU exchange the content of the VMC messages using proprietary or standardised format selected by the implementor (see Figure 12b).
- On the vehicle side:
  The location of the facilities layer on the vehicle side may vary between different vehicle OEMs and vehicle models (depending on OEM decision and the overall vehicle V2X architecture) and, as such, is out of scoup of this document.

In addition, this architecture can be scaled up to accommodate larger areas by adding multiple AVP RVO AS units and grouping RSUs under different AVP RVO AS. This would allow the processing load of RSU/vehicle management to be offloaded between several AVP RVO ASs and thus expand the AVP coverage area.

For example, in a large multi-story parking facility deploying a dedicated AVP RVO AS for each floor controls the RSUs within its area. In this case, the AVP RVO AS would need to be inter-connected using wired (ethernet, etc.) or wireless links, to allow handover of vehicles from one AVP RVO AS to the next as the vehicle progresses along the route.

9.1.2 Co-located RVO-RSU architecture ('smart RSU')

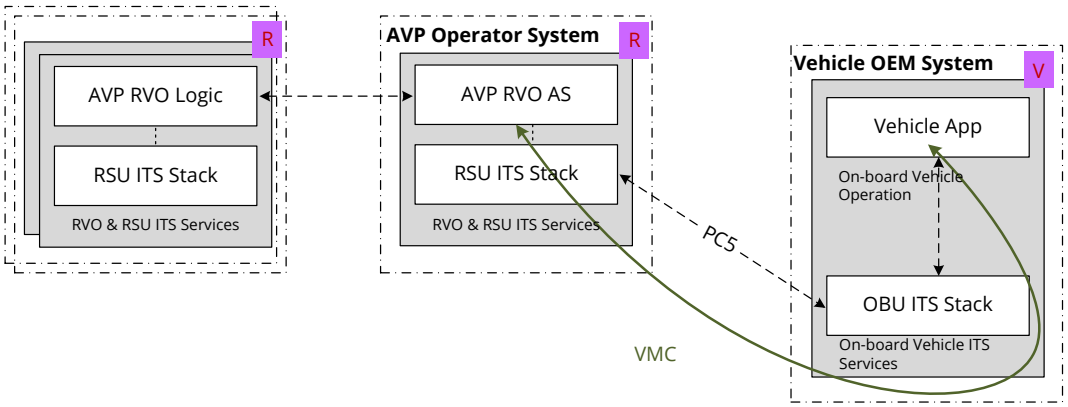


Figure 25: Co-located RVO-RSU architecture

Another possible implementation architecture would include deployment of so-called 'smart-RSUs', which integrate both the AVP RVO AS and RSU functionalities. The single box solution can carry the communications (PC5) and computing hardware (CPU + Accelerators), and all the required firmware, AI, vision analytics, AVP RVO AS and V2X software stack within the same enclosure. It might be beneficial in some scenarios in terms of deployment, operational and maintenance cost. The multiple sensor measurements are input to the AI and vision analytics, fusion software stack to perform the environment perception, localisation and produce metadata. The AVP RVO AS takes the metadata and performs the scheduling, decision-making, path planning tasks, etc. It sends the vehicle control messages over the air through the V2X stack, C-V2X modem and RF frontend.

For larger areas, multiple smart RSUs may be deployed and connected to each other using wired (ethernet, etc.) or wireless links. A software framework may be running on the AVP RVO AS for information sharing between Smart RSUs. The decision-making may be done in a distributed manner and the decisions are shared between smart RSUs. In this scenario, handover from one AVP RVO AS to the next as the vehicle progress along the route is envisaged.

In some large deployments, all the smart RSUs may be connected to a centralised node (preferably an on-premises edge node) to collect metadata from each one, and preform localisation, path planning, scheduling and remote vehicle operation over a larger area. In some cases, the edge node may even create a digital twin of the parking area to perform these functions.

9.1.3 Guidelines on RSU deployment

RSU deployment in general is always location and service dependent. The coverage area of an RSU is influenced by:

- RSU location in relation to obstacles and the area to cover (e.g. in a parking facility scenario the best location would be a centre point on the parking floor, far from concrete columns).
- Availability of required power and network access, locations allowing RSU mounting.
- Antenna placement (i.e. extended from the RSU housing) and type (i.e. directional or omnidirectional).

Furthermore, the coverage and location of RSUs in urban and highway deployments are usually planned by local contractors working for the road operators, and depending on the scope of the deployment (e.g. RSU installation only or upgrade of the road network itself) various 3D modelling and simulation tools are also used.

Parking facilities tend to be complex to cover, especially ones with many columns and low height specifications, both of which tend to make signal propagation harder – crowded underground parking facilities face similar limitations to urban coverage scenarios). Using simulation software is advisable for initial planning and field testing on-site – thus creating an RSSI heatmap.

Regarding vehicle handling, depending on the size of the parking facility and number of possible vehicles served, several handover and networking mechanisms can be used. In general, RSUs are capable (if Basic Awareness or similar is active) to maintain a database of ITS Stations within coverage and, signal strength can then also be monitored. Based on the final message properties, multiple RSUs nearby can broadcast messages to the intended vehicles or implement a more sophisticate approach for efficiency.

9.2 Selection of PC5 Direct Communication -based vehicle motion control

9.2.1 PC5 direct communication-based vehicle motion control use cases

The following use cases are considered for direct communication-based AVP vehicle motion control:

PC5 Direct Communication-Based Vehicle Motion Control as a Redundant System

In this scenario, direct communication is used as a backup system for the Uu-based VMC described above. Possible use cases that may require a fallback to direct communication for VMC are:

- Temporary degradation in QoS on the cellular network (e.g. due to network load, cell outage etc.)
- Insufficient QoS in some locations of the garage (e.g. limited cellular coverage on the underground levels). In this case, the VMC targeted to parking spots on these levels will be performed using PC5 Direct Communication .

Note: A hybrid mode where VMC is switched from Uu-based to PC5 Direct Communication-based motion control and vice versa is out of scope of this document.

PC5 Direct Communication-Based Vehicle Motion Control as a Primary System

In this scenario, PC5 Direct communication is the only system for AVP Vehicle Motion Control.

Possible use cases that would require this are:

- Insufficient cellular QoS to allow Uu-based VMC.
- PC5 Direct Communication is preferred for commercial reasons (e.g. utilising an existing RSU infrastructure in the parking facility).
- Other market or regional regulatory incentives and/or requirements.

Note: In all cases, cellular coverage is still required throughout the premise as explained in Section 9.4.

9.2.2 Requirements for availability of PC5 direct communication vehicle motion control

The following requirements should be met to allow PC5 Direct Communication Vehicle Motion Control:

- Spectrum/regulatory conditions permit PC5 Direct Communication VMC.
- Compliance with privacy regulations when using broadcast communication for AVP Type 2 VMC.
- Vehicle supports PC5 Direct Communication.
- There is sufficient RSU coverage throughout the AVP premises.

9.3 Security mechanism for PC5 direct communication

Security services for standardised direct V2X communications are defined in IEEE1609.2. The main objectives of these services are:

- Authenticity – assurance that the sender is who they claim to be.
- Authorisation – assurance that the sender is entitled to the privileges they request.
- Integrity – assurance that any changes to the packet after it is signed can be detected.
- Anonymity – mitigating privacy risk of the vehicle user.

Authenticity, authorisation, and integrity are achieved by using a scheme based on digital signatures and certificates which are received from a trusted authority recognised by all network users.

However, use of fixed certificates to prove authorisation would allow an undetected third party to use the transmitted certificates to keep track of a particular vehicle; all that is needed is reception of the packets – the certificate and the data are available in plaintext. This would violate the need for privacy (as the tracker would know the whereabouts of any particular vehicle). As a result, vehicles do not receive or use permanent certificates, but instead use short-term pseudonym certificates that are changed every few minutes.

A high-level summary of the scheme is as follows:

- A valid V2X station (e.g. OBU, RSU) undergoes a registration process at the relevant PKI Certificate Authority (CA).
- As part of the above process, there is an exchange of public keys between the V2X station and the CA.
- The relevant CA provides a large number of pseudonym certificates to the V2X station, which are themselves signed by the CA; each certificate contains a different V2X station public key.
- During the operational stage, the V2X station signs the outgoing message using its private keys, and sends them along with the relevant certificate (or a hash of it).
- Receiving vehicles must validate the received certificate, and if valid, use it to than validate the digital signature for each received message. At this point the messages are cryptographically verified (there are further validation tests to the message, including time and location feasibility checks).
- At some point the V2X station will run out of short-term certificates and a renewed session with the PKI CA will be necessary to replenish them.

Note: If needed for compliance with privacy regulations, additional mechanisms can be added to help mitigate privacy issues. For example, employing User Consent Agreement for AVP use.

9.4 Assumptions on cellular coverage

Cellular coverage is required throughout the parking area to ensure vehicle connectivity for the following tasks:

- Session management:
  - Vehicle wake up
  - Tasks management: Managing the different tasks: washing, charging station etc…
  - Re-parking
  - Vehicle pick-up procedure
- Vehicle recovery:
  - Recover a vehicle due to a malfunction
  - Recover a vehicle due to a blocked path

Note: The cellular coverage should ensure sufficient QoS to allow the above functionalities.

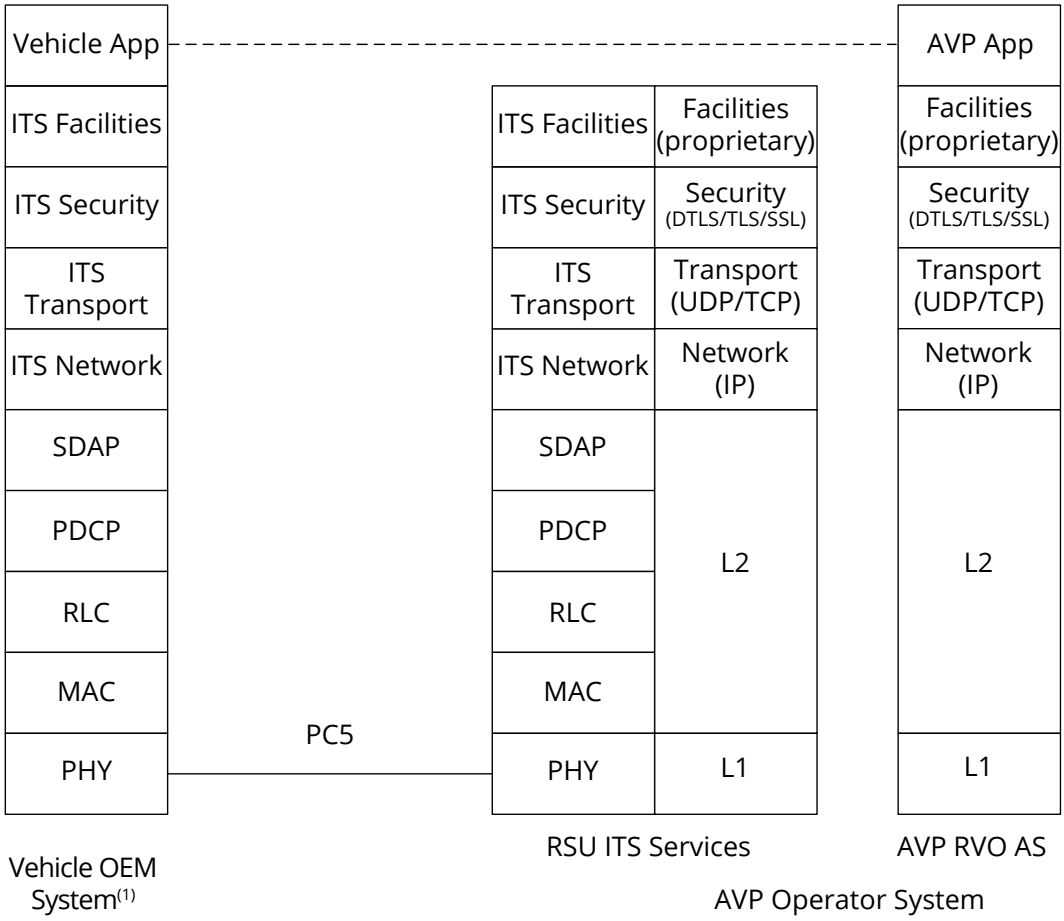
9.5 Vehicle motion control interface – PC5 direct communication-based vehicle motion control

The following figures describe the interaction needed when PC5 Direct Communication is used for the VMC interface. As shown in the application-level system architecture (Figure 2), information about vehicle movement is communicated through the VMC logical interface between the remote vehicle operation and the vehicle.

Figure 26 and Figure 27 below describes the protocol stack for RSU-based and AVP RVO AS-based facilities layer implementation architecture option (respectively).

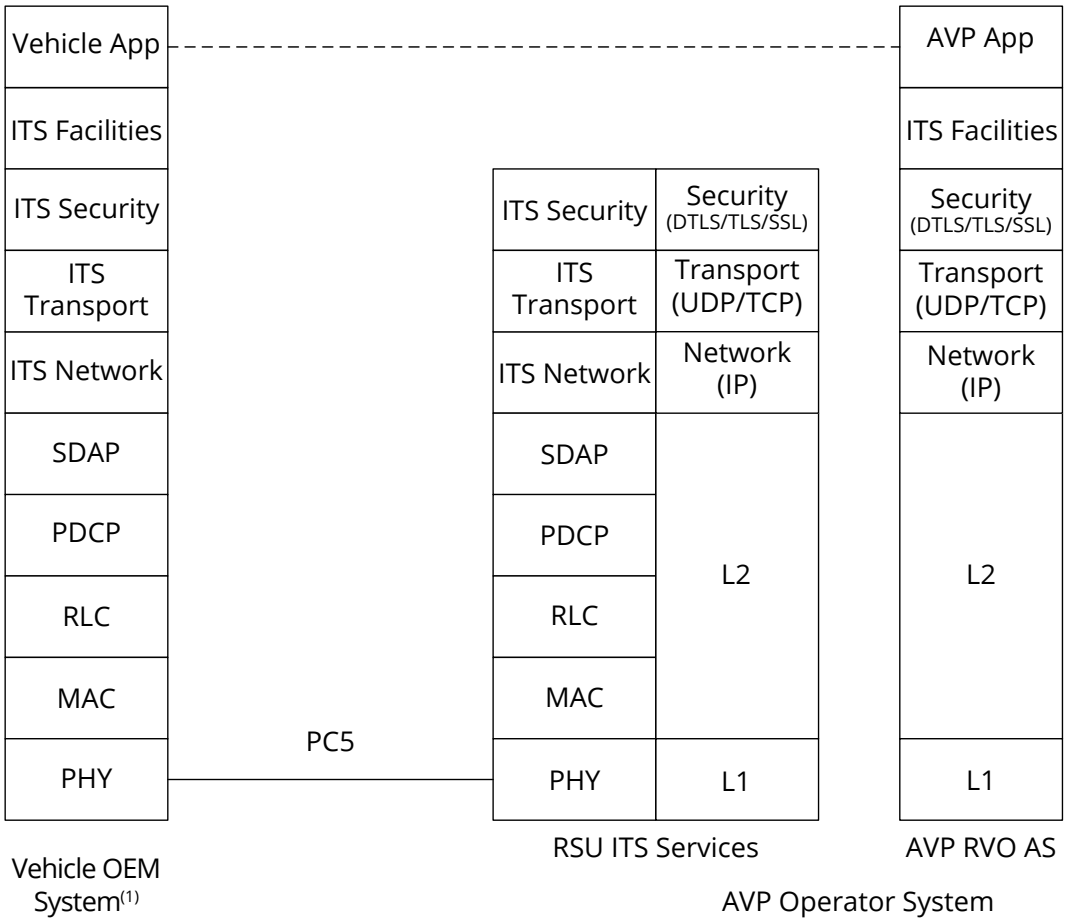
Figure 28 describes the protocol stack of 'Smart RSU' implementation architecture where the AVP RVO AS and the RSU are collocated.

As noted above, vehicle side protocols are implementation specific and may vary between vehicle OEMs and/or vehicle models and is out of scoup of this document.



(1) In vehicle protocol stack is OEM implementation specific

Figure 26: Protocol stack for RSU based facilities layer vehicle motion control interface



(1) In vehicle protocol stack is OEM implementation specific

Figure 27: Protocol stack for AVP RVO AS-based facilities layer vehicle motion control interface

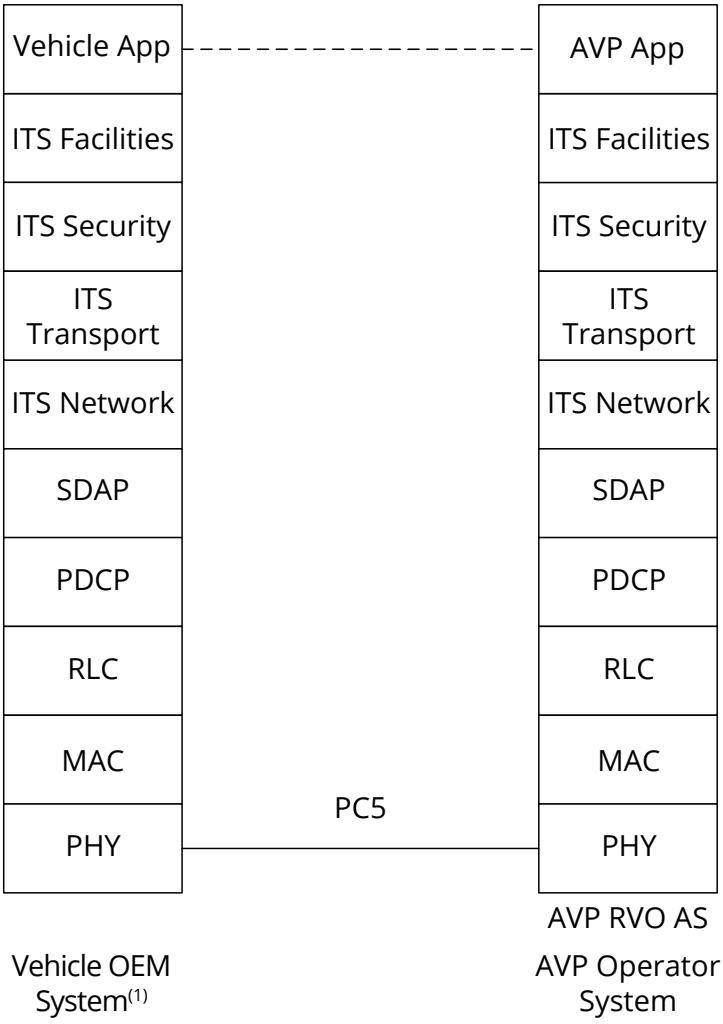


Figure 28: Protocol stack for 'smart RSU' interface

10 Conclusion

This 5GAA Technical Report describes implementation solutions using cellular public and non-public SNPN 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 and non-public SNPN networks in the implementation and operation of AVP services are also discussed.

Section 10.1, 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.

Section 10.2, Table 2 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 non-public SNPN networks.

Section 10.3, Table 3 summarises the technical requirements of ABP Type-2 use cases, as outlined in Section 5, and how they are fulfilled by the described implementation solution using PC5 Direct Communication for VMC.

10.1 Conformance of cellular public network solution

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 Operator 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 Vehicle Backend.	The access to the Vehicle Backend is provided via a cellular public network.	

Short interruption to connectivity between vehicle and Vehicle 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].

10.2 Conformance of SNPN network solution

Table 2: Conformance of SNPN network solution to AVP Type-2 requirements outlined in Section 5

AVP deployment requirements	Cellular non-public SNPN 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.	Same as Section 9.1.
Trust between vehicle OEM and AVP Operator domain.	For AVP network access, SNPN provide SIM or certificate 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.	Please refer to Section 8.2.2.5 for SNPN 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 Vehicle Backend.	The access to the Vehicle Backend is provided via SNPN network.	Vehicle App and Vehicle AS need to maintain a valid IP route to the vehicle.

Short interruption to connectivity between vehicle and Vehicle Backend at drop-off and pick-up areas.	Connectivity interruption only happens when the vehicle switches from the OEM MNO network to SNPN network. Such interruption caused by network switching can be optimised down to a few seconds interruption, if information about the SNPN can be provided to the UE in advance.	See Section 8.2.2.4 for switching to SNPN network.
Vehicle power-saving mode.	The cellular network supported by the Discontinuous Reception (DRX) framework promote UE energy saving.	See Section 8.1.5 for DRX. DRX is a radio interface feature to allow the UE to pause reception in order to save power and battery. The cycles are up to 10,240 ms and so they are relatively short compared to IP address lease times. Hence, this technology and the requirement is not in conflict with the requirement that the IP address needs to be maintained valid in Vehicle Backend as the IP lease time is hours or even days.
Vehicle remote wake-up.	As the SNPN network is available in parking facilities, the remote wake-up feature can be implemented via a cellular Uu modem.	Assumption is that there is a valid IP connection between Vehicle AS and Vehicle App.
Service Level Requirements of the Vehicle Motion Control.	SLR values in the 5GAA Use Case Description [3] can be fulfilled by SNPN networks.	

10.3 Conformance of PC5 direct communication-based vehicle motion control solution

Table 3: Conformance of direct communication-based solution to AVP Type-2 requirements outlined in Section 5

AVP deployment requirements	PC5 Direct Communication	Note
Security and privacy requirements.	PC5 Direct Communication links are secured using a certificate-based ITS security scheme. All communication links between the RSU and AVP RVO AS and 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.	Short-term pseudonym certificates are used to mitigate the privacy risk. See Section 9.3. If needed for compliance with privacy regulations, additional mechanisms can be added to help mitigate privacy issues. For example, employing User Consent Agreement for AVP use.
Trust between vehicle OEM and AVP Operator domain.	Trust between vehicle OEM and AVP operator should be established as defined in Table 1 and 2.	
Trust between the vehicle and the AVP Operator domain.	The trust relationship between the OEM and AVP operator should be extended to the PC5 Direct Communication link.	The mechanism for transferring and ensuring trust between the vehicle and AVP operator is out of scope of this document.
Access for vehicle to Vehicle Backend.	The access to the Vehicle Backend is provided via a cellular public or SNPN network.	
Short interruption to connectivity between vehicle and Vehicle Backend at drop-off and pick-up areas.	Connectivity interruption should conform with the definition in Table 1 and 2.	
Vehicle power-saving mode.	PC5 Direct Communication is not used after the vehicle is switched off.	
Vehicle remote wake-up	Vehicle 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 PC5 Direct Communication protocol (for example, PC5 interface).	

Annex A: Considerations on messages and protocols among ecosystem stakeholders for AVP service

This document focuses on the cellular and PC5 Direct Communication solution framework for AVP Type 2 use case. The solution framework has been developed to be generic, to support any application layer message and protocol that follows the interface and information definitions in ISO 23374-1 [1].

The following tables summarise the messages used in the communication solution framework and the candidate SDOs or industry associations, to our best knowledge, where such messages and related protocols can potentially be defined. The actual standardisation work or industry agreement have to be discussed among ecosystem stakeholders and it is out of scope of this 5GAA work item.

Interface		**Message name**	**Step no. in communication sequence chart**	**Type**	**Notes**
From	To				
AVP User App	User AS	Parking service request	II.1	Proprietary Subject to User SP's decision	
		Parking reservation request	III.1		
User AS	AVP User App	Parking Service Availability	II.10		
		Parking reservation response	III.8		
AVP Vehicle App	Vehicle AS	Parking service request	II.3	Proprietary Subject to OEM's decision	
		Parking reservation request	III.3		
Vehicle AS	AVP Vehicle App	Parking service availability	II.11		
		Parking reservation response	III.9		
User AS	Vehicle AS	Parking service request	II.2	To be standardised, to enable User backend and vehicle backend interoperability	EPA
		Parking reservation request	III.2		EPA
Vehicle AS	User AS	Parking service availability	II.9		EPA
		Parking reservation response	III.7		EPA

Vehicle AS	AVP Operator AS	Parking service request	II.7	To be standardised, to enable OEM and AVP operator interoperability	EPA
		Parking reservation request	III.4		EPA
AVP Operator AS	Vehicle AS	Parking service availability	II.8		EPA
		Parking reservation response	III.6		EPA
Vehicle AS	Interchange Function	Service discovery request	II.5	To be standardised, to enable Vehicle AS and Interchange interoperability	EPA and C-Roads (for message transport)
Interchange Function	Vehicle AS	Service discovery response	II.6		EPA and C-Roads (for message transport)
AVP Vehicle App	SMDP+/Cert. S. (for AVP NW)	Download and install AVP SNPN profile or certificate	III.10	To be standardised, to enable Vehicle App and SMDP+/ Cert. Server interoperability	3GPP, GSMA
SMDP+/Cert. S. (for AVP NW)	AVP Vehicle App	Download and install AVP SNPN profile or certificate	III.10		3GPP, GSMA

Interface		**Message name**	**Step no. in communication sequence chart**	**Type**	**Notes**
From	To				
AVP Vehicle App	Vehicle AS	Vehicle reached parking facility	A.2	Proprietary	
Vehicle AS	User AS	Vehicle reached parking facility	A.3	To be standardised	5GAA, EPA
User AS	AVP User App	User confirms arrival	A.4	Proprietary	
AVP User App	User AS	User confirms arrival	A.4	Proprietary	
User AS	AVP Operator AS	Vehicle reached parking facility	A.6	To be standardised	5GAA, EPA
AVP Operator AS	AVP RVO AS	Vehicle reached parking facility	A.7	Proprietary	
AVP RVO AS	AVP Operator AS	Vehicle reached parking facility	A.10	Proprietary	
AVP Operator AS	User AS	Vehicle reached parking facility	A.11	To be standardised	5GAA, EPA
User AS	Vehicle AS	Reservation data	A.12	To be standardised	5GAA, EPA
Vehicle AS	AVP Vehicle App	Vehicle dynamic parameter request	A.13	Proprietary	
AVP Vehicle App	Vehicle AS	Vehicle dynamic parameter response	A.14	Proprietary	
Vehicle AS	User AS	Vehicle dynamic parameter	A.15	To be standardised	5GAA, EPA
User AS	AVP Operator AS	Reservation data	A.16	To be standardised	5GAA, EPA
AVP Operator AS	AVP RVO AS	Communication Session_ID	A.18	Proprietary	

AVP Operator AS	User AS	Communication Session_ID	A.19	To be standardised	5GAA, EPA
User AS	Vehicle AS	Communication Session_ID	A.20	To be standardised	5GAA, EPA
Vehicle AS	AVP Vehicle App	Session_ID, AVP network MNO, QoS settings	A.21 (Public NW)	Proprietary	
AVP Vehicle App	MNO NW	Switch MNO and plausibility checks	A.22 (Public NW)		This procedure follows the 3GPP standards
MNO NW	AVP Vehicle App	Switch MNO and plausibility checks	A.22 (Public NW)		This procedure follows the 3GPP standards
AVP Vehicle App	Vehicle AS	Switched to AVP network	A.23 (Public NW)	Proprietary	
Vehicle AS	AVP Vehicle App	Session_ID, AVP network SNPN, QoS settings	A.21 (SNPN)	Proprietary	
AVP Vehicle App	MNO NW	Detach from MNO NW after plausibility checks	A.22 (SNPN)		This procedure follows the 3GPP standards
MNO NW	AVP Vehicle App	Detach from MNO NW after plausibility checks	A.22 (SNPN)		This procedure follows the 3GPP standards
AVP Vehicle App	AVP SNPN	Attach to AVP SNPN and plausibility checks	A.23 (SNPN)		Depending on the authentication methods for SNPN, the procedures can follow the 3GPP specifications
AVP Vehicle App	Vehicle AS	Re-establish connectivity with OEM BE and confirm switch to AVP SNPN	A.24 (SNPN)	Proprietary	

Interface		**Message name**	**Step no. in communication sequence chart**	**Type**	**Notes**
From	To				
AVP Vehicle App	AVP RVO AS	Vehicle in drop area	B.1	To be standardised	5GAA
AVP RVO AS	AVP Vehicle App	Vehicle in drop off area	B.2	To be standardised	5GAA
AVP Vehicle App	Vehicle AS	Notify readiness	B.3	Proprietary	
Vehicle AS	User AS	Notify Readiness	B.4	To be standardised	5GAA, EPA
User AS	AVP User App	Notify readiness	B.5	Proprietary	
AVP User App	User AS	Handover request	B.6	Proprietary	
User AS	AVP Operator AS	Handover request	B.7	To be standardised	5GAA, EPA
AVP Operator AS	AVP RVO AS	Handover request	B.8	Proprietary	
User AS	Vehicle AS	Handover request	B.9	to be standardised	5GAA, EPA
Vehicle AS	AVP Vehicle App	Handover request	B.10	Proprietary	
AVP RVO AS	AVP Vehicle App	R-System L4Check results	B.11	To be standardised	5GAA

AVP Vehicle App	AVP RVO AS	V-System L4Check results	B.12	To be standardised	5GAA
AVP RVO AS	AVP Operator AS	R-System & vehicle L4Checks results	B.13	Proprietary	
AVP Vehicle App	Vehicle AS	R-System & vehicle L4Checks results	B.14	Proprietary	
AVP Operator AS	Vehicle AS	System authority	B.15	To be standardised	5GAA
AVP Operator AS	User AS	System authority	B.16	To be standardised	5GAA, EPA
AVP Operator AS	AVP RVO AS	System authority	B.17	Proprietary	
Vehicle AS	AVP Vehicle App	System authority	B.18	Proprietary	
User AS	AVP User App	System authority	B.19	Proprietary	

Interface		**Message name**	**Step no. in communication sequence chart**	**Type**	**Notes**
From	**To**				
AVP Operator AS	Vehicle AS	Mission request	C.1	To be standardised	5GAA
Vehicle AS	AVP Operator AS	Mission OEM determination	C.2	To be standardised	5GAA
AVP Operator AS	User AS	Mission request	C.3	To be standardised	5GAA, EPA
User AS	AVP Operator AS	Mission user backend determination	C.4	To be standardised	5GAA, EPA
AVP Operator AS	User AS	Mission information	C.5	To be standardised	5GAA, EPA
AVP Operator AS	Vehicle AS	Mission determination	C.6	To be standardised	5GAA
AVP Operator AS	User AS	Mission determination	C.7	To be standardised	5GAA, EPA
AVP Operator AS	AVP RVO AS	Mission determination	C.8	Proprietary	
Vehicle AS	AVP Vehicle App	Mission determination	C.9	Proprietary	
Vehicle AS	AVP Operator AS	Authorisation of communication AVP Operator System/ vehicle app without Vehicle AS	C.10	To be standardised	5GAA
AVP Operator AS	Vehicle AS	ACK (to authorisation of communication AVP Operator System/ vehicle app without Vehicle AS)	C.11	To be standardised	5GAA
Vehicle AS	AVP Vehicle App	Authorisation of communication AVP Operator System/vehicle app without Vehicle AS/ preferred MNO	C.12	Proprietary	
AVP Vehicle App	AVP RVO AS	Establishing IP communication AVP Operator System/ vehicle app without Vehicle AS	C.13	To be standardised	5GAA

AVP RVO AS	MNO NW / AVP SNPN	Request QoS settings for AVP session (at QoS API)	C.14	To be standardised	5GAA
MNO NW / AVP SNPN	AVP RVO AS	Ack QoS settings for AVP session	C.15	To be standardised	5GAA

Interface		**Message name**	**Step no. in communication sequence chart**	**Type**	**Notes**
From	**To**				
AVP Vehicle App	Vehicle AS	Vehicle state	D.7	Proprietary, subject to OEM's decision	
User AS	AP User App	Vehicle state	D.9	Proprietary, subject to User SP's decision.	
AVP Vehicle App	AVP RVO AS	Functional rime sync request	D.1	To be standardised, to enable OEM and AVP operator interoperability	ETSI ITS
		Vehicle state	D.5		ETSI ITS
		Vehicle debug	D.5a		(Optional) ETSI ITS
		Recorded messages	D.5b		(Optional) ETSI ITS
		Safety time sync request	D.10		ETSI ITS
		Driving permission ACK	D.13		(Optional) ETSI ITS
AVP RVO AS	AVP Vehicle App	Functional time sync response	D.2		ETSI ITS
		PathSnippet	D.3		ETSI ITS
		Coordination permission	D.4		(Optional) ETSI ITS
		Drive command	D.6		ETSI ITS
		Safety time Sync response	D.11		ETSI ITS
		Driving permission	D.12		ETSI ITS
Vehicle AS	User AS	Vehicle state	D.8	To be standardised, to enable Vehicle backend and User backend interoperability.	5GAA, EPA
MNO NW / AVP SNPN	AVP RVO AS	QoS notification in case of QoS change	D.14	To be standardised, to enable network operator and AVP operator interoperability.	3GPP, CAMARA,

Interface		Message name	Step no. in communication sequence chart	Type	Notes
From	To				
AVP RVO AS	AVP Vehicle App	Destination reached	E.1	To be standardised	5GAA
AVP RVO AS	AVP Operator AS	Destination reached	E.2	Proprietary	
AVP Vehicle App	Vehicle AS	Destination reached	E.3	Proprietary	

Interface		Message name	Step no. in communication sequence chart	Type	Notes
From	To				
AVP Operator AS	Vehicle AS	Mission finished	F.1	To be standardised	5GAA
AVP Operator AS	User AS	Mission finished	F.2	To be standardised	5GAA, EPA
AVP Operator AS	AVP RVO AS	Mission finished	F.3	Proprietary	
Vehicle AS	AVP Vehicle App	Mission finished	F.4	Proprietary	
User AS	AVP User App	Mission finished	F.6	Proprietary	
AVP RVO AS	MNO NW / AVP SNPN	Release QoS settings for AVP session	F.7		The procedure is based on 3GPP standards.
AVP Vehicle App	AVP RVO AS	Release IP communication to AVP Operator System	F.8	To be standardised	

Interface		Message name	Step No. in communication sequence chart	Type	Notes
From	To				
AVP Operator AS	Vehicle AS	Request Sleep	G.1	To be standardised protocol	5GAA
Vehicle AS	AVP Vehicle App	Negotiate minimal power consumption	G.2	Proprietary	
AVP Vehicle App	Vehicle AS	Engaging sleep	G.3	Proprietary	
AVP Vehicle App	Vehicle AS	Engaging sleep	G.4	Proprietary	
Vehicle AS	AVP Operator AS	Sleep Engaged	G.5	To be standardised	5GAA
AVP Vehicle App	Vehicle AS	Status information (periodic communication)	G.6	Proprietary	

Interface		Message name	Step no. in communication sequence chart	Type	Notes
From	To				
AVP Operator AS	Vehicle AS	Request wake-up	H.1	To be standardised	5GAA
Vehicle AS	MNO NW/ AVP SNPN	(Application layer) wake-up command	H.2	(proprietary) up to the decision of the OEM	Message buffered at the network
AVP Vehicle App	MNO NW/ AVP SNPN	3GPP paging process	H.2a		According to 3GPP process
MNO NW/ AVP SNPN	AVP Vehicle App	(Application layer) wake-up command	H.2b		Buffered message delivered
AVP Vehicle App	Vehicle AS	Result wake-up	H.3	(proprietary) up to the decision of the OEM	
Vehicle AS	AVP Operator AS	Result wake-up	H.4	To be standardised	5GAA
AVP Operator AS	AVP RVO AS	Vehicle in standby state	H.5	Proprietary	
Vehicle AS	AVP User AS	Result wake-up	H.6	To be standardised	5GAA, EPA
User AS	AVP User App	Result wake-up	H.7	Proprietary	

Interface		Message name	Step no. in communication sequence chart	Type	Notes
From	To				
AVP Vehicle App	Vehicle AS	User intent to regain authority	I.1	Proprietary	
Vehicle AS	AVP Operator AS	User intent to regain authority	I.2	To be standardised	5GAA
AVP Operator AS	Vehicle AS	AVP Operator System authority (revoked)	L3	to be standardised	5GAA
AVP Operator AS	User AS	AVP Operator System authority (revoked)	I.4	To be standardised	5GAA, EPA
AVP Operator AS	AVP RVO AS	AVP Operator System authority (revoked)	I.5	Proprietary	
Vehicle AS	AVP Vehicle App	AVP Operator System authority (revoked)	I.6	Proprietary	
User AS	AVP User App	AVP Operator System authority (revoked)	I.7	Proprietary	
Vehicle AS	AVP Vehicle App	Switch to OEM MNO network	I.8	proprietary	
AVP Vehicle App	AVP SNPN	Detach from AVP SNPN NW after plausibility checks	I.9		The procedure is based on 3GPP standards.
AVP Vehicle App	MNO NW	Attach to OEM MNO NW	I.10		The procedure is based on 3GPP standards.
AVP Vehicle App	Vehicle AS	Re-establish connectivity with OEM BE and confirm switch to OEM MNO NW	I.11	Proprietary	

Interface		Message name	Step no. in communication sequence chart	Type	Notes
From	To				
AVP Vehicle App	Vehicle AS	Vehicle left parking facility	J.1	Proprietary	
Vehicle AS	User AS	Vehicle left parking facility	J.2	To be standardised	5GAA, EPA
User AS	AVP Operator AS	Vehicle left parking facility	J.3	To be standardised	5GAA, EPA
AVP RVO AS	AVP Operator AS	Vehicle left parking facility	J.4	Proprietary	
AVP Operator AS	User AS	Check-out report	J.5	To be standardised	5GAA, EPA
User AS	AVP User App	Check-out result	J.6	Proprietary	
AVP Operator AS	AVP RVO AS	Close session	J.7	Proprietary	
AVP Operator AS	Vehicle AS	Close session	J.8	To be standardised	5GAA
AVP Operator AS	User AS	Close session	J.9	To be standardised	5GAA, EPA

Annex B: Change history

Date	Meeting	TDoc	Subject/Comment
2022.05.09	5GAA F2F#22	5GAA T-220002	V1.0 First public release
2022.12.19		5GAA T-220002	V2.0 Second public release.
2023.02.08	5GAA F2F#25	5GAA T-220002	TR finalization
2023.02.16	Board 23.02.16	5GAA T-220002	Board approval

5GAA is a multi-industry association to develop, test and promote communications solutions, initiate their standardisation and accelerate their commercial availability and global market penetration to address societal need. For more information such as a complete mission statement and a list of members please see https://5gaa.org


5GAA
Automotive Association