5GAA Automotive Association

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

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

VERSION:	3.0
DATE OF PUBLICATION:	3 February 2025
DOCUMENT TYPE:	Technical Report
EXTERNAL PUBLICATION:	Yes
DATE OF APPROVAL BY 5GAA BOARD:	16 January 2025

Contents

Foreword 5

Executive Summary 6

Introduction 8

1 Scope 8

2 References 9

3 Definitions, symbols and abbreviations 10
3.1 Definitions 10
3.2 Abbreviations 10

4 System architecture 13

5 Working assumptions and requirements for AVP Use Case implementation 18

6 Protocols and implementation profiles 21

7 AVP Use Case implementation flows 23
7.1 Overview of AVP Use Case procedure 23
7.2 High-level communication sequences 23
7.2.1 AVP services discovery, reservation, and payment 23
7.2.2 Vehicle parking process 25
7.2.3 Vehicle re-park to a different location 27
7.2.4 Vehicle retrieval 27
7.3 Detailed communication sequences for AVP Type-2 29
7.3.1 A. Check-in sequence 29
7.3.2 B. Manoeuvring control handover sequence 31
7.3.3 C.1. Mission assignment sequence 33
7.3.4 C.2. Mission initialisation sequence 34
7.3.5 D. Destination and route (automated vehicle operation Type-2) 35
7.3.5.1 Uu-based implementation 35
7.3.5.2 PC5-based implementation 36
7.3.6 E. Destination reached (optional) 39
7.3.7 F. Mission accomplished 39
7.3.8 G. Sleep sequence 40
7.3.9 H. Wake-up sequence 41
7.3.10 I. Hand-back sequence 42
7.3.11 J. Check-out sequence 42
7.3.12 K. Value-adding service request sequence 43
7.3.13 L. Vehicle return request sequence 44
7.4 Time synchronisation in AVP systems 45
7.4.1 Functional time synchronisation 46
7.4.2 Safety time synchronisation 46

8 Implementation considerations for cellular network solutions 48
8.1 Considerations for cellular public networks 49
8.1.1 Network coverage in parking facilities 49
8.1.2 Network switching to the preferred MNO network in a parking facility 50
8.1.3 QoS provisioning in the cellular network 50
8.1.3.1 Network exposure realisations 50
8.1.3.2 3GPP QoS assurance mechanisms 51

8.1.3.3 Network slicing ... 52
8.1.4 Global availability and roaming ... 52
8.1.4.1 Authentication and roaming ... 52
8.1.4.2 Regional breakout ... 53
8.1.5 Additional network features support AVP ... 54
8.1.5.1 Discontinuous reception (DRX) framework ... 54
8.2 Considerations for the cellular non-public network ... 54
8.2.1 Public network integrated non-public network ... 54
8.2.2 Stand-alone non-public network ... 54
8.2.2.1 SNPN core network aspect ... 55
8.2.2.2 SNPN RAN aspects ... 55
8.2.2.3 SNPN UE (device) aspects ... 56
8.2.2.4 UE network selection in SNPN access mode ... 56
8.2.2.5 SNPN authentication methods ... 57
8.2.2.5.1 Embedded subscriber identification module profile switching ... 57
8.2.2.5.2 Extensible authentication protocol – transport layer security ... 57
8.2.2.6 SNPN access to PLMN services ... 58
8.3 Protocol stacks ... 59
8.3.1 Interaction between Vehicle AS and AVP Operator System ... 59
8.3.2 Vehicle motion control interface ... 60
8.4 Communication sequence for IP and security session ... 62

9 Implementation considerations for PC5 Direct Communication-based vehicle motion control ... 64
9.1 Implementation architecture options for PC5 Direct Communication-based AVP vehicle motion control ... 64
9.1.1 Split RSU/RVO architecture ... 64
9.1.2 Co-located RVO-RSU architecture ('smart RSU') ... 66
9.1.3 Guidelines on RSU deployment ... 66
9.2 Selection of PC5 Direct Communication-based vehicle motion control ... 67
9.2.1 PC5 Direct Communication-based vehicle motion control Use Cases ... 67
9.2.2 Requirements for availability of PC5 vehicle motion control ... 68
9.3 Security mechanism for PC5 direct communication ... 68
9.4 Assumptions on cellular coverage ... 69
9.5 Vehicle motion control interface – PC5 Direct Communication-based vehicle motion control ... 70

10 Conclusion ... 73
10.1 Conformance of cellular public network solution ... 73
10.2 Conformance of SNPN network solution ... 74
10.3 Conformance of PC5 direct communication-based vehicle motion control solution ... 75

Annex A: Considerations on messages and protocols among ecosystem stakeholders for AVP service ... 77

Contents

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 with an identifying change of the consistent numbering that all WG meeting documents and files should follow (according to 5GAA rules of procedure).

Contents

Executive Summary

Vision and objectives

This Technical Report outlines the implementation details and technological framework for Automated Valet Parking (AVP) Type-2 systems. It provides an in-depth analysis of AVP Use Case Type-2, focusing on system architecture, wireless communication technologies, protocols, and deployment considerations using cellular public networks, Stand-alone Non-Public Networks (SNPN), and short-range PC5 Direct Communication solutions. The detailed communication sequences for AVP services—ranging from service discovery and reservation to vehicle parking and retrieval—are explained, emphasizing interoperability, security, and safety aspects.

This report serves as a reference for stakeholders in the automotive and telecommunications industries, providing actionable insights into deploying AVP services at scale.

Key findings and recommendations

- Scope and Purpose: The report describes how AVP Type-2 leverages advanced Vehicle-to-Everything (V2X) communication technologies enabling driverless parking operations in predefined facilities. It addresses the interplay between AVP Operator Systems, Vehicle Application Servers, and User Interfaces to deliver seamless and secure parking solutions.
- Technological Framework: Cellular public networks and SNPN are evaluated for their suitability in supporting AVP operations, focusing on Quality of Service (QoS), network slicing, authentication and roaming capabilities. PC5 Direct Communication is explored for its low-latency potential in motion

control but requires dedicated Road-Side Unit (RSU) infrastructure.

- Implementation Considerations: The system must ensure secure communication channels through end-to-end encryption and mutual authentication between vehicles, infrastructure, and backend systems. Mutual authentication between vehicles with their backends and AVP operators is a prerequisite for initiating any parking mission. Functional safety requirements are emphasized, including robust time synchronization mechanisms and the functional driving and safety tasks are separated.
- Protocols and profiles: Detailed communication sequences are provided for core AVP operations, including service discovery and reservation, vehicle check-in, parking, retrieval, and optional value-added services like battery charging or car washing. High-level flowcharts illustrate the interdependencies between various system components and stakeholders.
- Deployment considerations: For cellular networks, enhancements such as improved indoor coverage and local breakout options are suggested to optimize performance in parking facilities. SNPN deployments are positioned as a viable alternative for standalone operators, requiring careful management of spectrum and access controls.
- Interoperability and Standards: The report underscores the need for industry-wide and global harmonized standardization to ensure compatibility across different Original Equipment Manufacturers (OEMs) and AVP service providers. Interface Implementation Profiles (IIPs) are proposed to guide developers in achieving cross-vendor interoperability. The implementation of IIPs is vital to ensuring compatibility across diverse vehicle manufacturers and AVP service operators, facilitating scalable deployments.

Conclusion

The 5GAA Technical Report highlights how AVP technology, underpinned by advanced communication networks, can revolutionize parking experiences while addressing technical as well critical safety and operational challenges. The document serves as a guide for stakeholders aiming to deploy AVP systems, emphasizing the need for standardization, and technological aspects. 5GAA sees a strong need among industry stakeholders to harmonise and i.e., limit the number of AVM IIPs to reduce the complexity of AVP product implementation and avoid fragmented markets. Assuming that most parking areas will have adequate coverage cellular coverage, even partially, and the penetration rate of AVP-capable vehicles increases due to their enablement for Automated Vehicle Marshalling in OEMs factories, the rollout with AVP solutions will possibly appear on the market as predicted by the 5GAA C-V2X Roadmap [13].

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, Stand-alone 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, Stand-alone Non-Public Network and short-range communication technologies. In addition to the 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 on, considering AVP service deployment requirements.

2 References

[1] ISO/FDIS 23374-1 Intelligent Transport Systems – Automated Valet Parking Systems (AVPS) – Part 1: System Framework Requirements for Automated Driving, and Communication Interface, July 2023

[2] 5GAA A-200094, Technical Report, V2X Application Layer Reference Architecture, June 2020 https://5gaa.org/v2x-application-layer-reference-architecture/

[3] C-V2X Use Cases and Service Level Requirements Volume III, v1, January 2023, 5GAA_T-210022 https://5gaa.org/content/uploads/2023/01/5gaa-t-210022-tr-c-v2x-use-cases-and-service-level-requirements-vol-iii.pdf

[4] 5GAA Technical Report, Safety Treatment in Connected and Automated Driving Functions, March 2021 https://5gaa.org/content/uploads/2021/03/5GAA_T-210009_STiCAD_TR-V1-compressed_2.pdf

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

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

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

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

[9] GSMA RSP (Remote SIM Provisioning) Technical Specification, Version 2.4, October 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

[11] ETSI TS 103 882 V2.1.1 – Intelligent Transport Systems (ITS); Automated Vehicle Marshalling (AVM); Release 2, May 2024

[12] German Association of the Automotive Industry, Position: Automated Valet Parking Systems – Requirements for automated valet parking systems, Version 3.0 (Not publicly available at the time of publication).

[13] 5GAA White Paper, A visionary roadmap for advanced driving use cases, connectivity, and technologies, November 2024 https://5gaa.org/a-visionary-roadmap-for-advanced-driving-use-cases-connectivity-and-technologies/

3 Definitions, symbols and abbreviations

3.1 Definitions

The following definitions, given in ISO 22374-1:2021 [1] and ETSI TS 103 882 V2.1.1 (2024-05) [11], apply to the present document:

AVM: Automated Vehicle Marshalling (in the context of road traffic) means automated orchestration and remote vehicle motion control of individual or multiple unoccupied vehicles of several kinds in the lower velocity range.

NOTE: AVM technical solutions can be used to implement Automated Valet Parking as services in parking facilities, automated factory parking services in factories, and other service scenarios that require automated remote vehicle control at low velocity.

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

3.2 Abbreviations

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

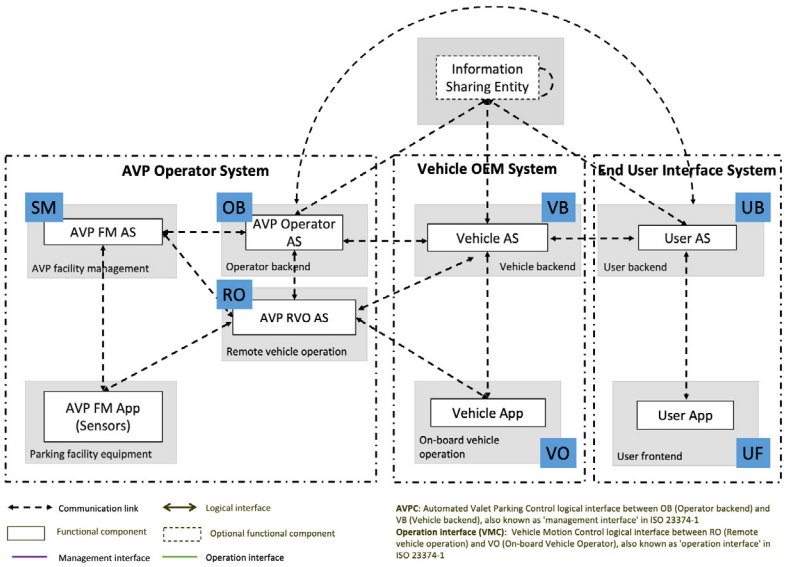
G3GPP	3rd Generation Partnership Project
5GAA	5G Automotive Association
5QI	5G QoS Identifier
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
APP	Application
ARFCN	Absolute Radio-Frequency Channel Number
AS	Application Server
ASP	Application Service Provider
ASIL	Automated Safety Integrity Level
AVM	Automated Vehicle Marshalling
AVP	Automated Valet Parking
AVPC	AVP Control
AVPS	AVP System
AVP FM AS	AVP Facilities Management Application Server
BTP	Basic Transport Protocol
CAG	Closed Access Groups
DRX	Discontinuous Reception
E2E	End-to-End
EAP	Extensible Authentication Protocol

EAP-TLS	Extensible authentication protocol – transport layer security
ECU	Electronic Control Units
EPA	European Parking Association
EPS	Evolved Packet System
eSIM	Embedded Subscriber Identification Module
FW	Firewall
GBR	Guaranteed Bit Rate
GNW	GeoNetWorking
GSMA	GSM Association
HPLMN	Home Public Land Mobile Network
HV	Host Vehicle
IIP	Interface Implementation Profile
ISE	Information Sharing Entity
ITS	Intelligent Transport System
IoT	Internet of Things
KPI	Key Performance Indicators
MEC	Mobile Edge Computing
MEC4AUTO	MEC for Automotive
MIM	Marshalling Infrastructure Message
MNO	Mobile Network Operator
MVM	Marshalling Vehicle Message
N3IWF	Non-3GPP Interworking Function
NAT	Network Address Translation
NEF	Network Exposure Function
NG-RAN	Next Generation Radio Access Network
NID	Network Identifier
NPNs	Non-Public Networks
NW	Network
OB	Operator backend
OEM	Original Equipment Manufacturer
P	AVP Facility Management
PDB	Packet Delay Budget
PDU	Packet Data Unit
PER	Priority Error Rate
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PNI-NPN	Public Network Integrated- Non-Public Network
QCI	QoS Class Identifier
QoD	QoS on Demand
QoS	Quality of Services
RAN	Radio Access Network
REST	Representational State Transfer
RO	Remote Vehicle Operation
RRC	Radio Resource Control
RSSI	Received Signal Strength Indicator
RSU	Roadside Unit
RV	Remote Vehicle
RVO	Remote Vehicle Operation

SCEF	Service Capability Exposure Function
SDO	Standards Developing Organisation
SIM	Subscriber Identity Module
SLR	Service Level Requirements
SNPN	Stand-alone Non-Public Network
SUPI	Subscription Permanent Identifier
ToD	Tele-operated Driving
UE	User Equipment
UDP	User Datagram Protocol
DTLS	Datagram Transport Layer Security
UPF	User Plane Function
URSP	UE Route Selection Policy
User App	User Application
User AS	User Application Server
Uu interface	User-to-User interface
UF	User frontend
UB	User backend
V2X	Vehicle-to-Everything
VB	Vehicle backend
Vehicle AS	Vehicle Application Server
Vehicle App	Vehicle Application
VMC	Vehicle Motion Control
VO	On-board Vehicle Operation
WAVE	Wireless Access in Vehicular Environments
WSMP	WAVE Short Message Protocol

4 System architecture

The system architecture described in this section is based on the Vehicle-to-Everything (V2X) application layer reference architecture agreed upon in 5GAA [2]. The following figure shows the application layer system architecture for implementing the AVP Type-2 Use Case.



5GAA App. Layer System Architecture	ISO 12768-1 System Architecture
AVP Operator Application Server (AVP Operator AS)	Operator backend (OB)
AVP Remote Vehicle Operation Application Server (AVP RVO AS)	Remote vehicle operation (RO)
Vehicle Application Server (Vehicle AS)	Vehicle backend (VB)
Vehicle Application (Vehicle App)	On-board Vehicle Operator (VO)
User Application Server (User AS)	User backend (UB)
User Application (User App)	User frontend (UF)
AVP Facility Management Application Server (AVP FM AS)	Safety Manager (SM)
AVP Facility Management Application (AVP FM App)	
Information Sharing Entity (Interface for service discovery)	(This is out scope of the ISO standard)

Figure 1: Application-level system architecture for AVP Type-2

Note: Figure 1 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 vehicles into driverless operation.
  - Via Vehicle AS, handing over authority (rights and ability to perform tasks on the vehicle) to the user.
  - Forwarding information between AVP RVO AS (remote vehicle operation) and Vehicle AS.

AVP Remote Vehicle Operation Application Server (AVP RVO AS), also known as Remote Vehicle Operation (RO) 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 Vehicle Motion Control (VMC) logical interface. The AVP RVO AS communicates with the AVP Operator AS for AVP service management.

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

- The Vehicle AS at the Original Equipment Manufacturer (OEM) vehicle backend offers services to the vehicles manufactured by the OEM and its drivers and passengers by communicating with the Vehicle App. It communicates with the AVP Operator AS and User AS via backend connectivity.
- The Vehicle AS is responsible for remotely engaging/disengaging the AVP service of the Vehicle App in the vehicle.

Vehicle Application (Vehicle App), also known as On-board Vehicle Operation (VO) in [1]

- The Vehicle App integrates services offered by the Vehicle AS into vehicles. For the AVP service, it performs the VO 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 but will be handled as a third-party separate End User Interface System as it can be hosted by a third party (e.g. a car-sharing or rental company). It offers services for end users by communicating with the User App, e.g. installed on the user's smartphone, the infotainment system of the Host Vehicle (HV) 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 (UF) in [1]

- The User App provides the services offered by User AS to the end user, e.g. via a smartphone App, an App running on the infotainment system of the HV, or the fleet management system.

AVP Facility Management Application Server (AVP FM AS), also recognised as part of the broader 'automated valet Parking facility management' or '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), again recognised as part of 'automated valet Parking facility management' 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.

Information Sharing Entity

- Given the potentially large number of different AVP Operators in real deployment scenarios, Information Sharing Entities (ISE) are needed to automate the discovery of AVP operators and scale up communications between the AVP Operator ASs, User ASs, and the Vehicle ASs, to avoid full mesh connectivity. The ISE is out of the scope of the ISO standard [1].

Figure 2 and Figure 3 illustrate the logical interfaces between the backends, the RVO and the Vehicle App described in the following and completed by the implementation details described in Section 5 of this document.

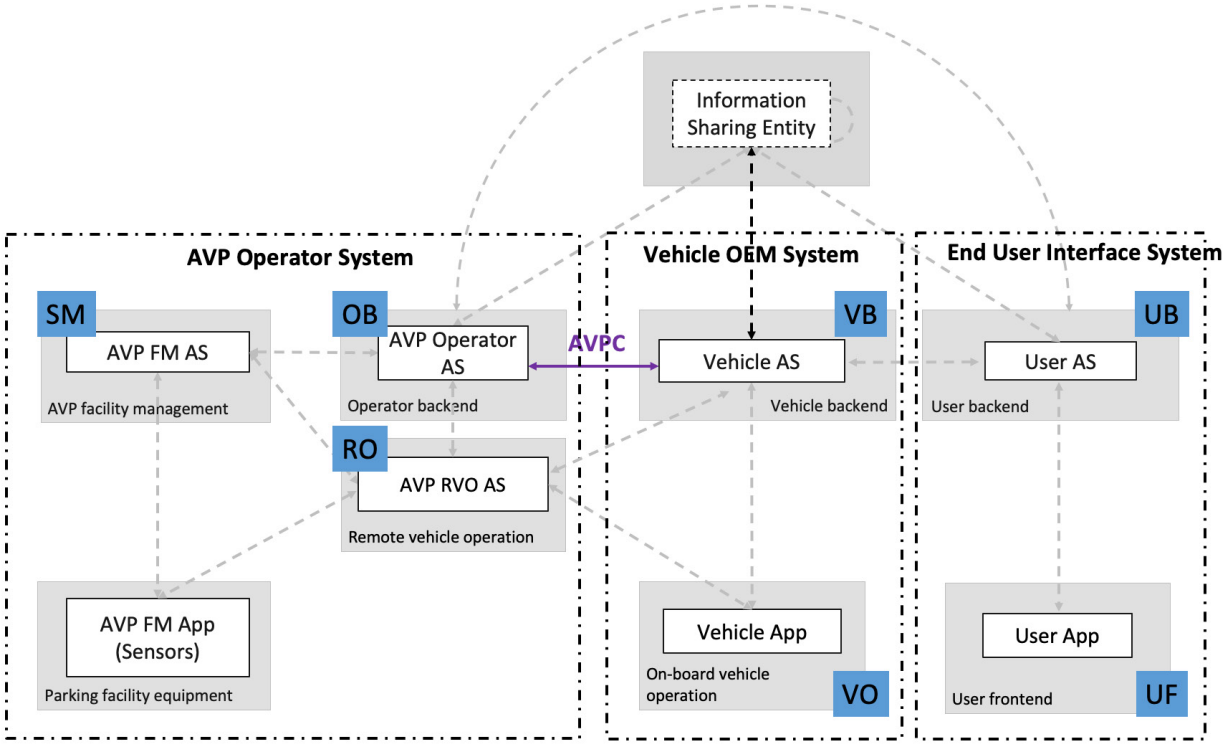


Figure 2: AVP Control (AVPC) logical interface in Application-level system architecture for AVP Type-2

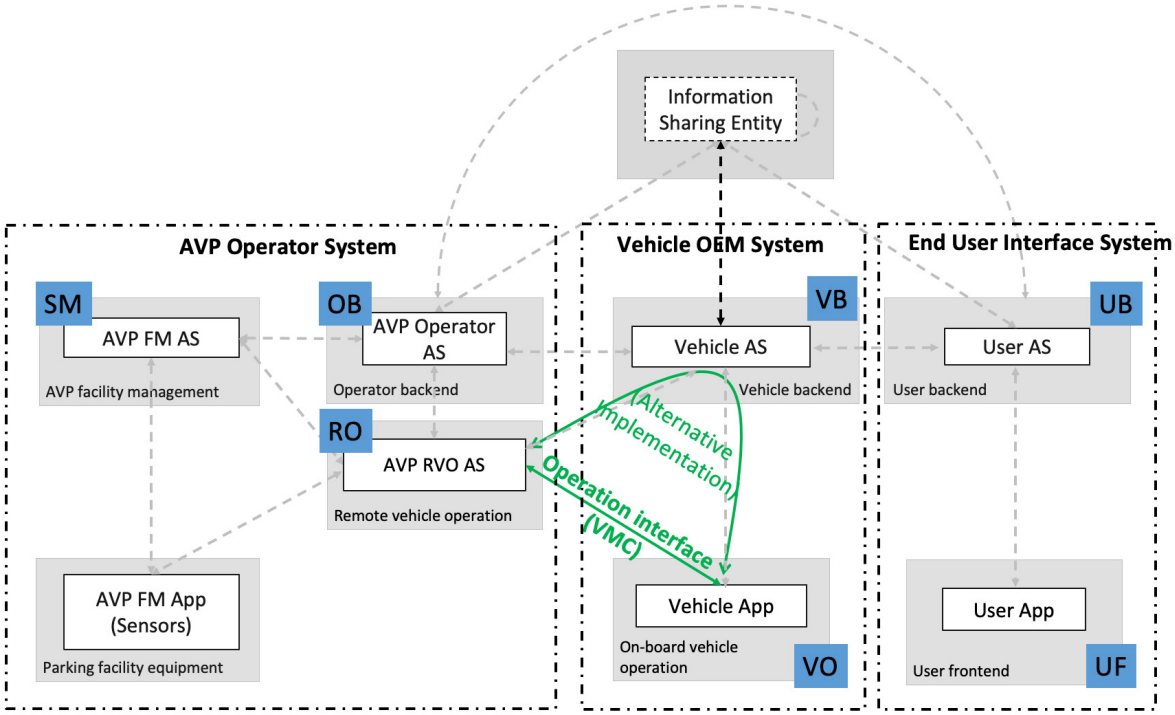


Figure 3: Vehicle Motion Control logical interface in application-level system architecture for AVP Type-2

Automated Valet Parking Control (AVPC) logical interface

The AVPC is the logical interface between the AVP Operator AS (OB), the User AS (UB) and the Vehicle AS (VB) to manage 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 the '**Management Interface'** in ISO 23374-1 [1].

Note: This logical interface may also be implemented via the Information Sharing Entity to improve the system's scalability.

Vehicle Motion Control (VMC) logical interface

The Vehicle Motion Control logical interface between the AVP RVO AS (RO) and Vehicle App (VO) is used to communicate 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 going through Vehicle backend (VB), as shown in Figure 3. 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, it 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 – to utilise existing firewalls, 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 communication between Application Servers and their respective Apps (clients) typically uses 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 1) 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:
        ii. The Vehicle AS and AVP Operator AS shall be mutually authenticated before any AVP session.
        iii. 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 secure access to and control over their connected vehicles at all times.
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 be able 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. Note: Worst-case scenario (e.g. a total power failure of the parking facility), the vehicle can be moved manually.
8. The vehicle shall flash its hazard lights during the mission's initialisation,

supporting safe vehicle identification.

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 the Automated Safety Integrity Level (ASIL) or similar schemes. [4][11]
- 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 the 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 mechanisms to guarantee Key Performance Indicators according to the defined and applicable Service Level Requirement 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 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 downloading, installing, and using 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 the 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 5, Step I.11.

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 the scope of these Work Items.

6 Protocols and implementation profiles

The table below 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 AVP RVO AS HV Automotive OEM: Approves AVP operation of HV by AVP Operator User frontend (UF): User's interface to issue AVP related user requests and confirmations.
	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 the Vehicle App, Vehicle AS, and AVP Operator AS, such as service discovery, reservation, payment, and AVP network information, is needed to enable AVP services
Standards and technology	Access layer technology/ies	1. Cellular Uu interface in 4G and beyond systems for communicating with vehicles 2. In addition, LTE-V2X or NR-V2X PC5 interfaces may be used for VMC procedure (Communication between Vehicle AS and AVP Operator AS is carried out wirelessly)
	Network and transport layer technologies	1. For Uu: IP with TCP/UDP with secure connections, i.e. TLS/DTLS 2. For PC5: (Non-IP) GNW, BTP, WSMP
	Message standards	Besides standardised AVM messages defined in ETSI TS 103 882, AVP application protocols need to be developed and standardised
	Framework	1. Uu: IP protocol stacks 2. 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	1. Cellular coverage in vehicle drop-off area and AVP operation area 2. 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

Interoperability is one of the prerequisites for successful mass deployment and operation of AVP services delivered on open markets. AVP service operation involves different automotive OEM brands and AVP service operators (e.g. parking garage operators). Consequently, interoperable implementations of AVP systems are required, especially for AVM delivered through the operational interface. To this end, the AVM Interface Implementation Profiles (IIPs) are needed. An AVM IIP is a technical specification containing the minimum set of testable requirements to ensure interoperable AVM implementations on both the vehicle (VO) and infrastructure (RO) sides, and over the operation interface for AVP Type-2 service operation. Such technical requirements in an IIP include, for example, the vehicle motion control mode (known as AVM Control Interface), the configuration of the communication protocol stack covering transport, network, and access layers, as well as security and safety solution implementation. Depending on the technical solutions of AVM Implementation, multiple AVM IIPs may exist, and new AVM IIPs may appear. However, interoperability is guaranteed only between implementations following the same AVM IIP and the same version.

AVM IIPs are used by developers and testers of AVP products to ensure AVM interoperability with other products over the operating interface, especially with products from different vendors. Furthermore, the nomenclatures of AVM IIPs, once agreed upon among the industry stakeholders, can be used in communications for AVP service announcements, discovery, negotiation, reservation, billing, etc., to ensure interoperability throughout the service operation.

Although multiple AVM IIPs may exist on the market due to vendors' different choices of technical solutions and communication technologies, 5GAA sees a strong need among industry stakeholders to harmonise and limit the number of AVM IIPs in order to reduce the complexity of AVP product implementation and avoid fragmented markets.

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 diagrams and flows, including the main parameters conveyed. Figure 4 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 including optional value-adding service requests, and vehicle retrieval process including an optional customer vehicle return request.

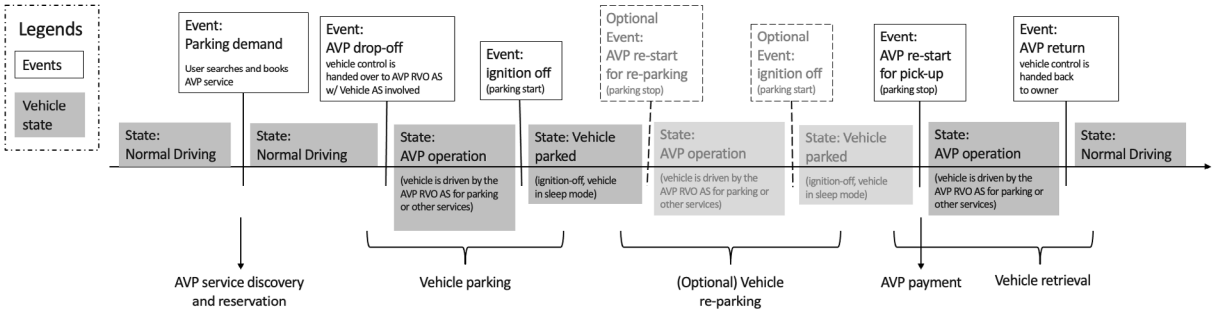


Figure 4: Events and vehicle states in AVP service cycle

7.2 High-level communication sequences

7.2.1 AVP services discovery, reservation, and payment

It is assumed that methods are needed to announce the presence of available AVP parking/slots for a scalable, automated solution. 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 parking slots, known as an AVP service announcement, and the User AS subscribes to this type of information. The AVP service announcement must be standardised or agreed upon among industry players. In this case, the Information Sharing Entity (ISE) can serve as a message broker, e.g. by using AMQP for AVP service announcements. Alternatively, if the User AS does not subscribe to AVP announcements, it can still use the ISE to 'discover' available AVP Operators when a user requests such a service via the User AS. In this case, the ISE 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 User 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 using the AVP Operator's information (e.g. URL) obtained from the AVP service announcement. To make AVP 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 Vehicle App and the AVP Operator AS via the User AS.

For the AVP SNPN network, download and installation of the AVP SNPN, eSIM profiles or certifications must 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.

An example of the reservation processes, as implemented using the latest knowledge and best practices in both the parking and automotive industry, is illustrated in Figure 5.

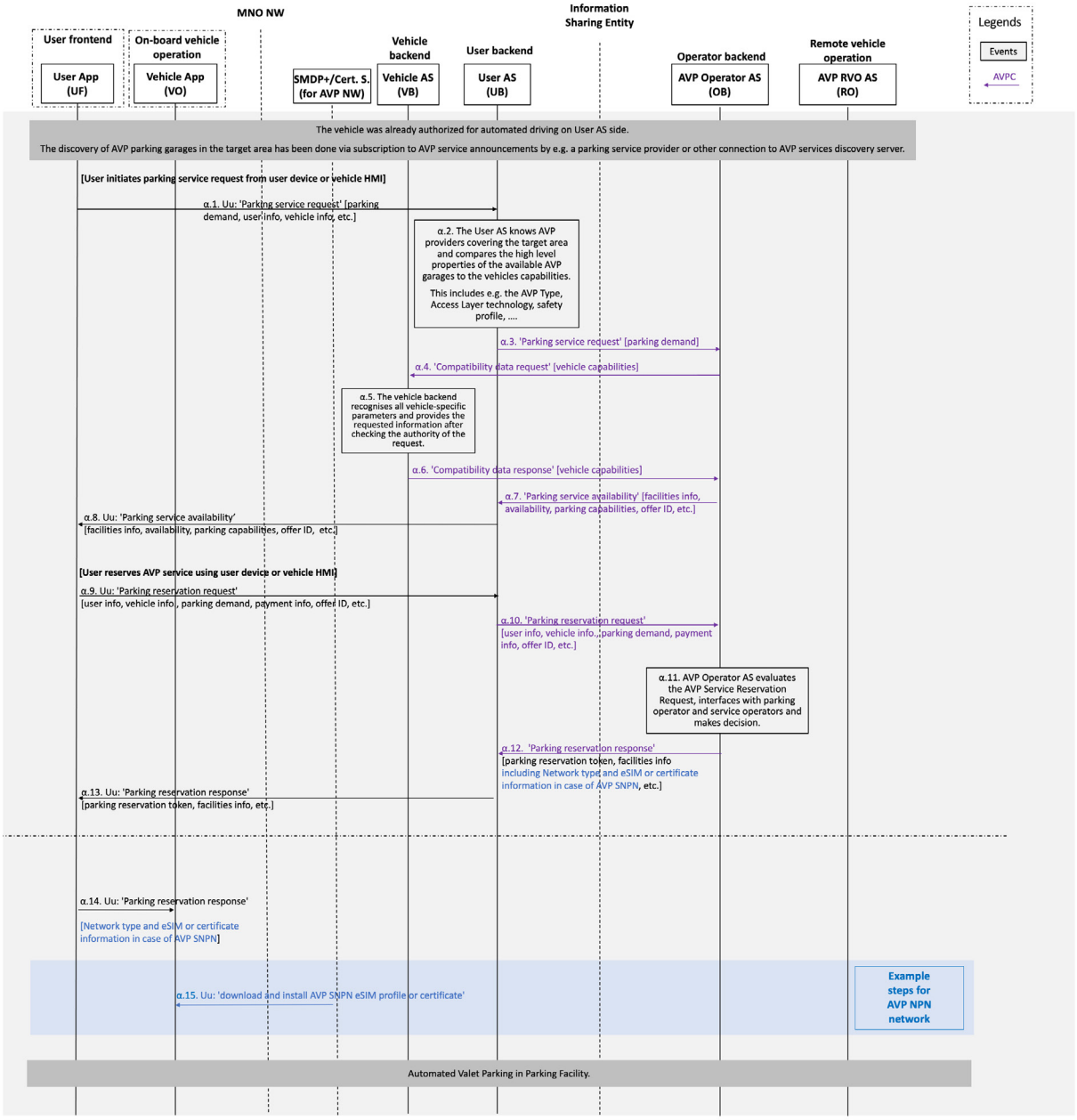


Figure 5: Example communication sequence for AVP service discovery and reservation

7.2.2 Vehicle parking process

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

This description also applies to AVP at or within an OEM logistics zone or 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. Likewise, communication would be limited to interactions between the vehicle and the OEM factory control system, which would incorporate a series of essential functions, such as MAP handling (i.e. where to park the vehicle). This scenario could

also be referred to as Automated Vehicle Marshalling (AVM) in vehicle factories [11][12].

As shown in Figure 1, 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 the Vehicle backend. The Vehicle backend system is thus connected to the AVP Operator backend. [1]

Figure 6 illustrates the high-level process of vehicle parking, starting from check-in to the vehicle being parked and entering sleep mode once in the allotted space. This process is aligned 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, are needed.

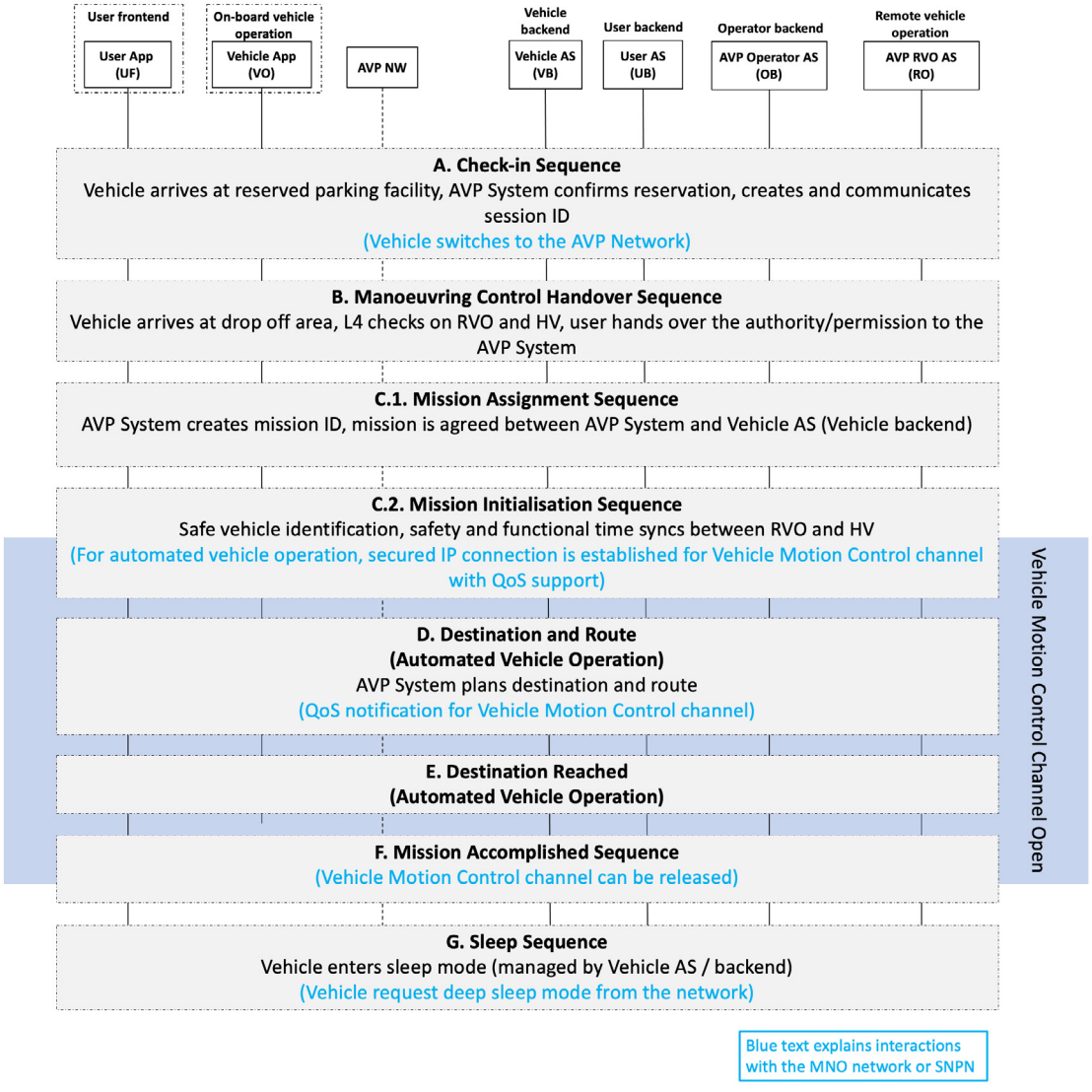


Figure 6: High-level communication sequences for AVP Type-2 parking process

7.2.3 Vehicle re-park to a different location

This section describes the vehicle re-parking process, including the optional value-adding service request of AVP Type-2 [1] from one location to another in the parking facility, as shown in Figure 7. Explanations in blue brackets describe specific steps where interactions with the AVP NW, i.e. the MNO NW or SNPN, are needed.

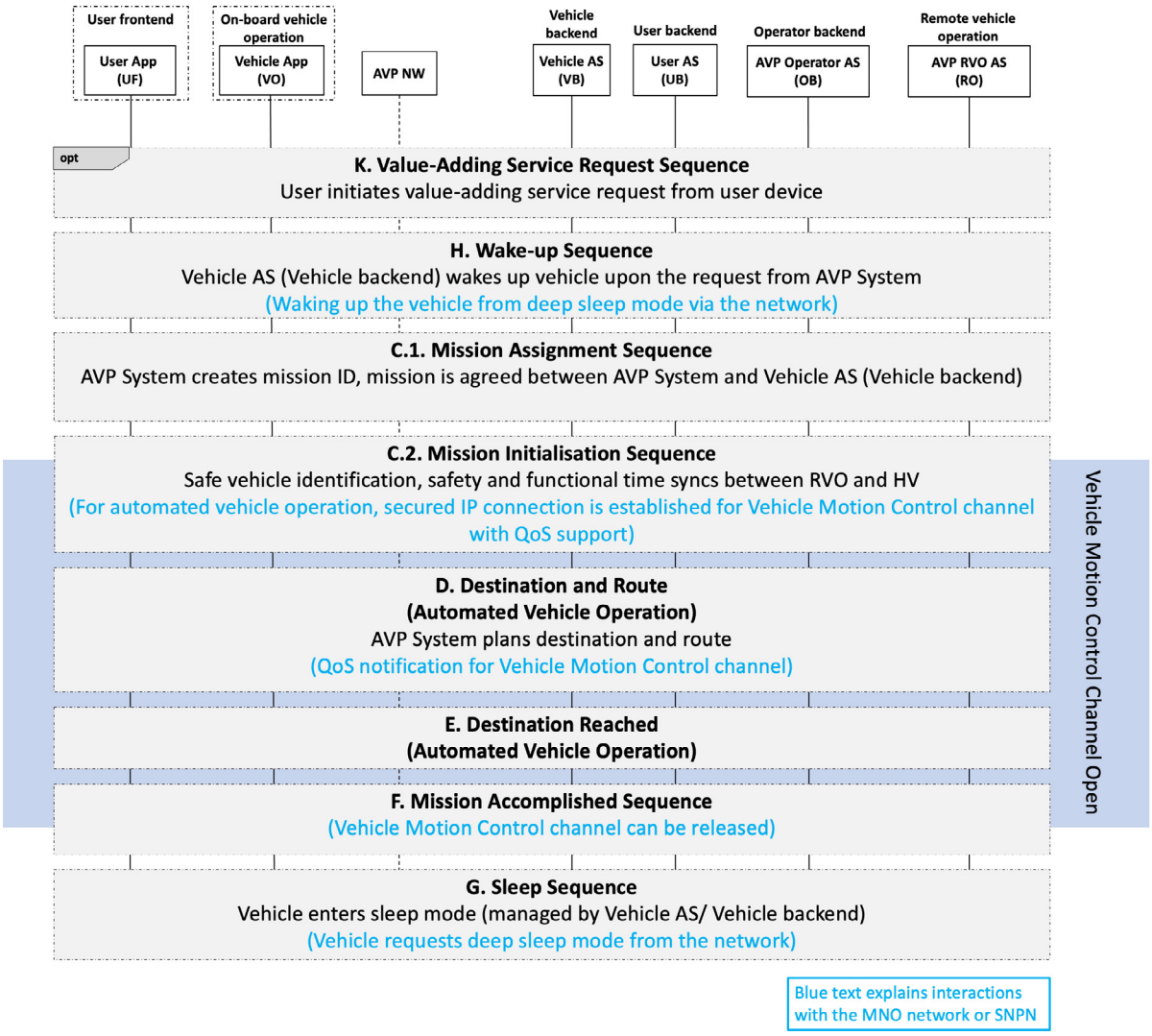


Figure 7: High-level communication sequences for AVP Type-2 re-park process with optional value-adding service request

7.2.4 Vehicle retrieval

This section describes the vehicle pick-up process, illustrated in Figure 8, from the vehicle parking location to the vehicle pick-up area.

This description also applies to AVP at or within an OEM logistics zone/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). Again, this scenario could also be referred to as AVM in vehicle factories [11][12].

Figure 1 illustrates AVP Type-2 in the public parking facility, where the Vehicle backend system is connected to the vehicle, validates AVP requests and collects driving data directly from 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 motion control and feedback information do not 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 how to manoeuvre the vehicle. The system, 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.

Optional: The process of vehicle retrieval can be triggered via the Vehicle Return Request Sequence by the customer using a handheld User App.

Note: The explanations in the blue brackets of Figure 8 describe specific steps where interactions with the AVP NW, i.e. the MNO NW or SNPN in this case, are needed.

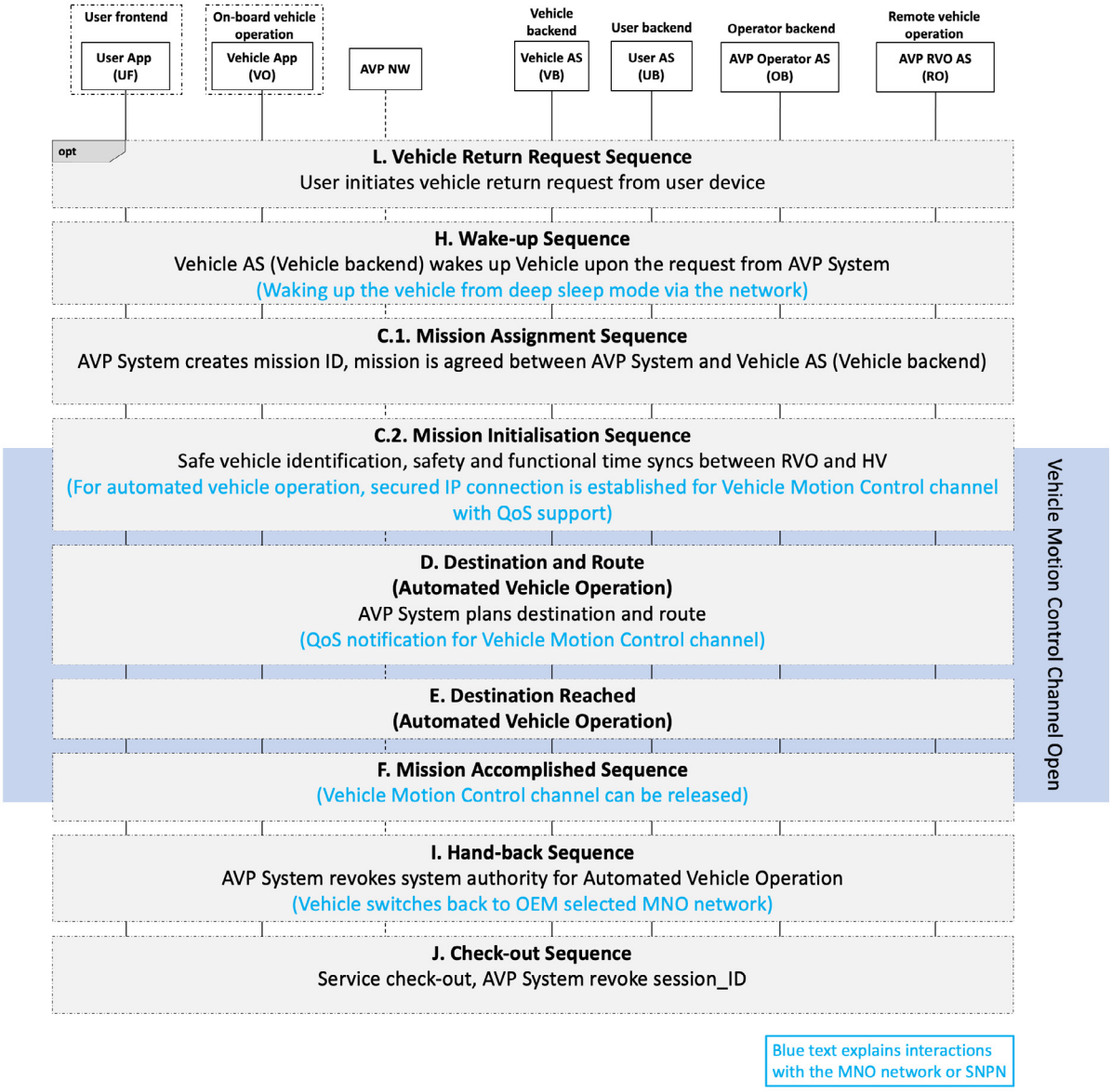


Figure 8: High-level communication sequences for AVP Type-2 retrieval process with optional return request

7.3 Detailed communication sequences for AVP Type-2

7.3.1 A. Check-in sequence

The following Figure 9 is an example of the communication sequence for the HV's check-in as it arrives at the parking facility. When the HV crosses the parking facility barrier it starts the recorded 'parking time' for the billing.

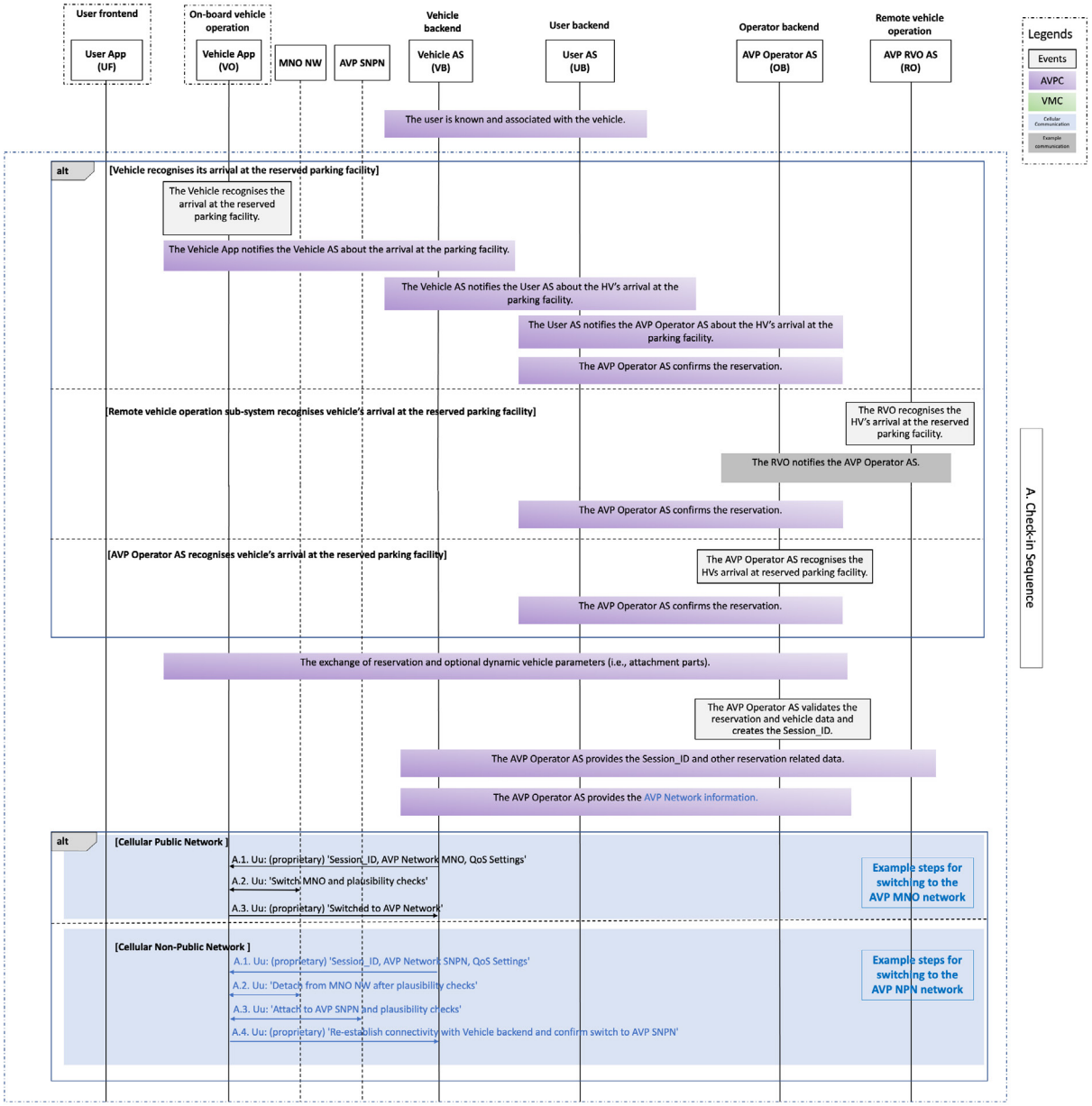


Figure 9: Communication sequence for 'Check-in'

The 'AVP network information' provided by the AVP Operator AS includes the identifier and further information about the AVP network to enable the vehicle to access it.

- 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 an 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, Radio Resource Control, or RRC, configuration) for AVP use.

For cellular public networks, steps A.2 to A.3 are meant for the vehicle's UE to switch to the AVP network.

- A.2 includes 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 must first detach from the MNO network, then switch to SNPN mode and execute a 'network attach' command. The SNPN network has to be known to the UE/modem, and necessary credentials must be exchanged beforehand.

- A.2 includes the step to detach from the MNO network.
- A.3 includes when the vehicle application instructs the modem to switch to an SNPN NW, and the modem attaches to it according to standard 3GPP procedures (Section 8.2.2 explains the SNPN aspects and network selection).
- A.4 confirms the network change to the Vehicle backend and re-establishes the connectivity, including the announcement of new IP after the network change.

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

7.3.2 B. Manoeuvring control handover sequence

Figure 10 gives an example of the communication sequence for manoeuvring control handover in which the authority over the HV's manoeuvring controls (e.g. actuators, etc.) is submitted to the AVP Operator System (i.e. AVP RVO AS).

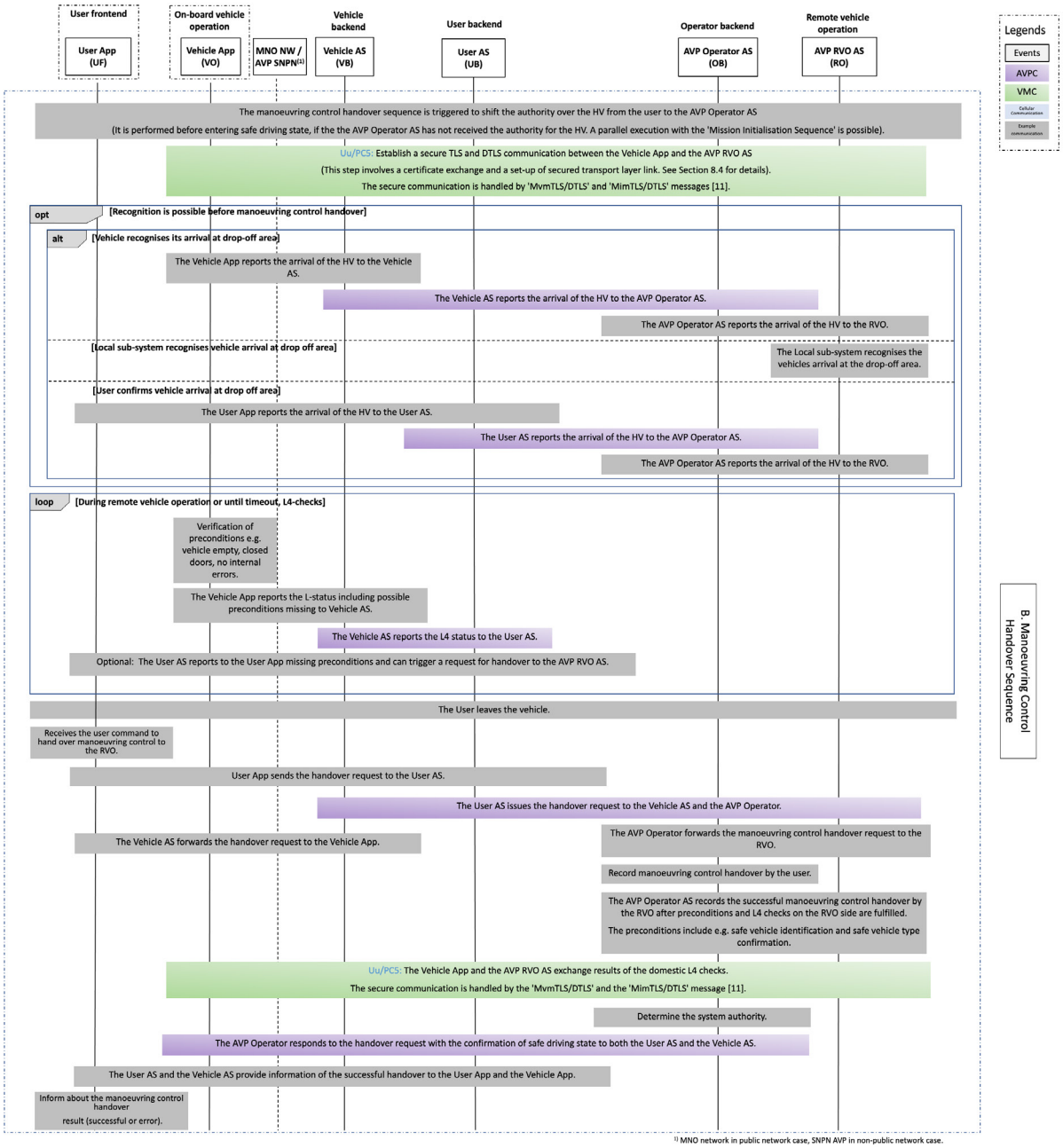


Figure 10: Communication sequence for 'Manoeuvring Control Handover'

Communications between 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.

The communication between the Vehicle App (vehicle) and AVP RVO AS (remote control) uses secured DTLS/IP (or TLS) sessions. Section 8.4 presents the detailed communication sequence for establishing the secured communication session.

Note: The secured IP-based session does not apply to non-IP PC5 Direct Communication since it does not use the IP-based protocol stack or standardised IT security methods described in Section 8.4.

7.3.3 C.1. Mission assignment sequence

Figure 11 gives an example of the communication sequence for the mission assignment, in which the first and every following mission is assigned.

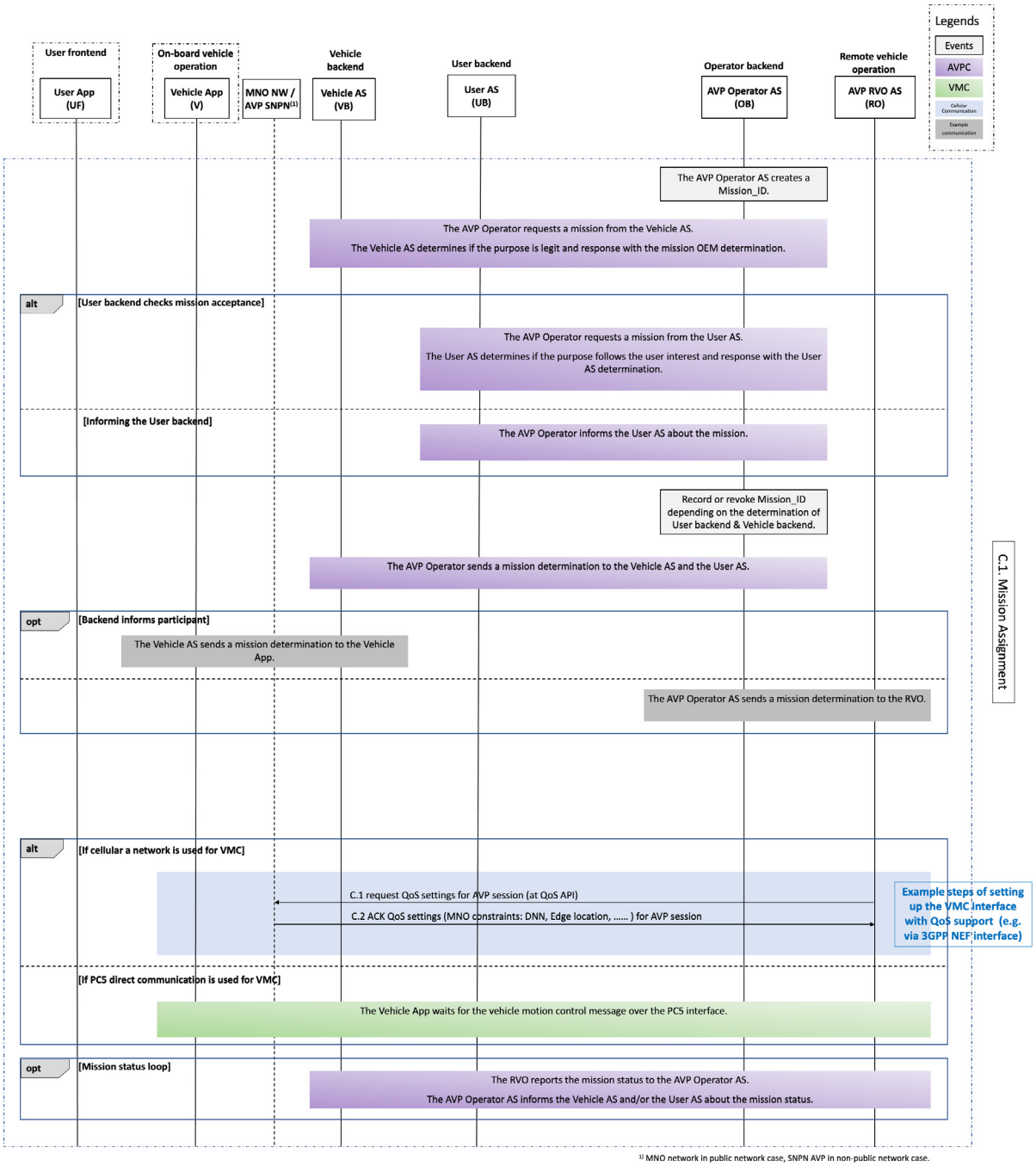


Figure 11: Communication sequence for 'Mission Assignment'

The mission request, issued by the AVP Operator AS, must be approved by either the Vehicle AS or User AS every time there is a new reason for the remote operation of the HV.

Steps C.1 and C.2 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.

Note: Before the mission status loop starts, the first VMC message from the RVO must be sent to the Vehicle App. This only applies to PC5 Direct Communication, where the vehicle awaits the reception of a VMC message over the PC5 interface.

7.3.4 C.2. Mission initialisation sequence

Figure 12 provides an example of the communication sequence for the mission initialisation used to ensure that secure and functional clocks on both the Vehicle App and the AVP RVO AS are synchronised, and that all safety-related measures are in place before the HV enters the safe driving state.

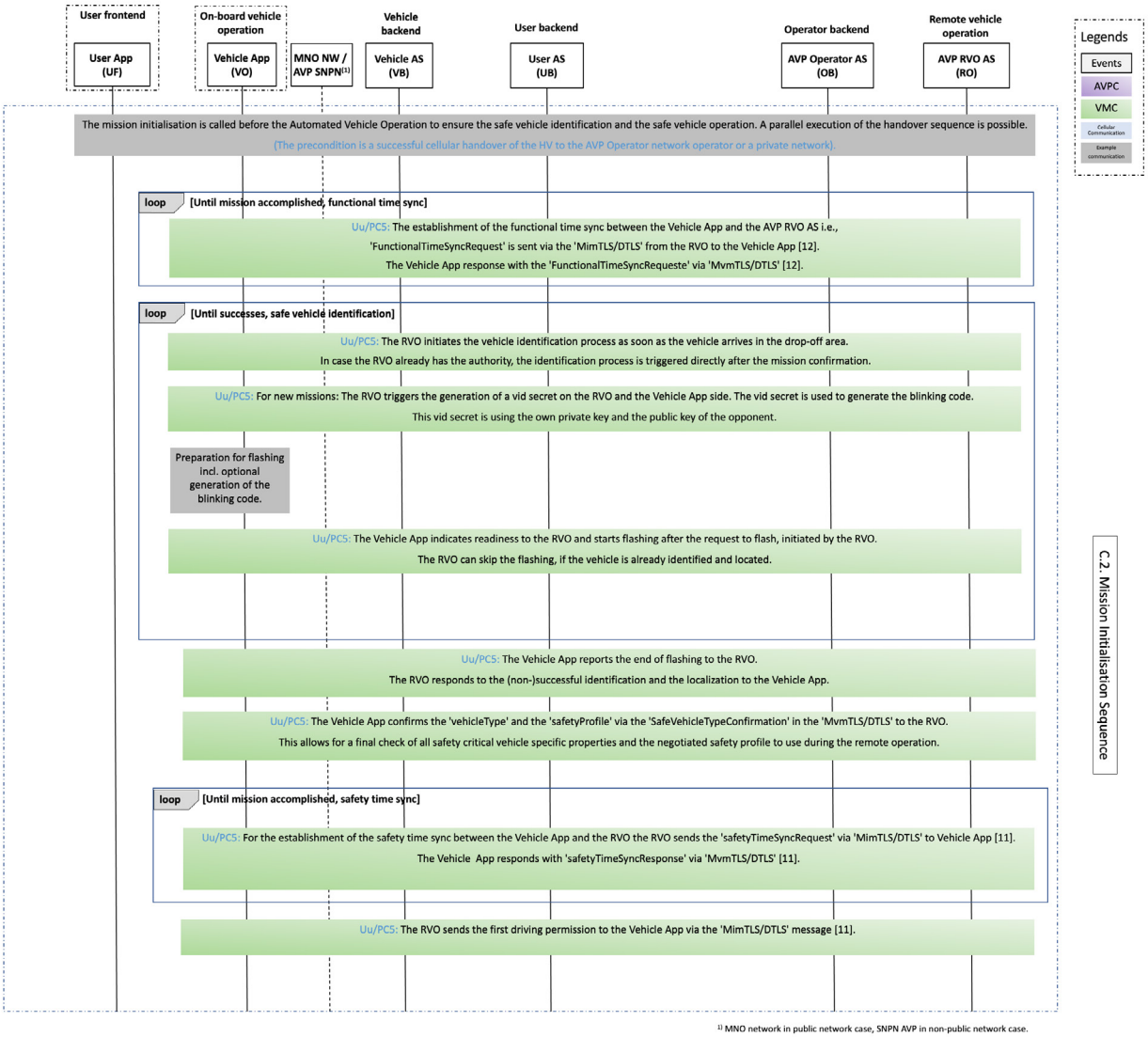


Figure 12: Communication sequence for 'Mission Initialisation'

For the process of clock synchronisation, refer to Chapter 7.4.1 Functional Time Synchronisation.

Note: The full sequence can run before every mission, or a subset can be executed in parallel with other sequences, e.g. the manoeuvring control handover.

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

The communication sequence diagram of 'destination and route' is shown in Figure 13, Figure 14 and Figure 15 or respective implementation options using the Uu and PC5 interfaces. In this process, the functional driving and safety tasks are separated. Each task has its own clock synchronisation and communication loops between the Vehicle App and AVP RVO AS (remote control), established in the mission initialisation sequence found in Figure 12.

The 'driving permissions' in Figures 13 to 15, defined in ISO 23307-1 [1] and ETSI 103 882 [11], are 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 ensures safety requirements are fulfilled, even if the connectivity between the vehicle and remote control fails.

For specification of the facility layer, refer to [11] and for detailed requirements on implementation to [12].

7.3.5.1 Uu-based implementation

For cellular networks and IP-based implementation, Figure 13 shows the communication sequence over the VMC, where the VMC messages terminate at the facilities layer of the AVP RVO AS and Vehicle App, respectively. Figure 31 in Section 8.3.2 shows the end-to-end protocol stacks.

Step D.1 is only applicable for cellular network-based implementations. In a cellular network, the QoS notification in step D.1 utilises the network exposure interface described in Section 8.1.3.

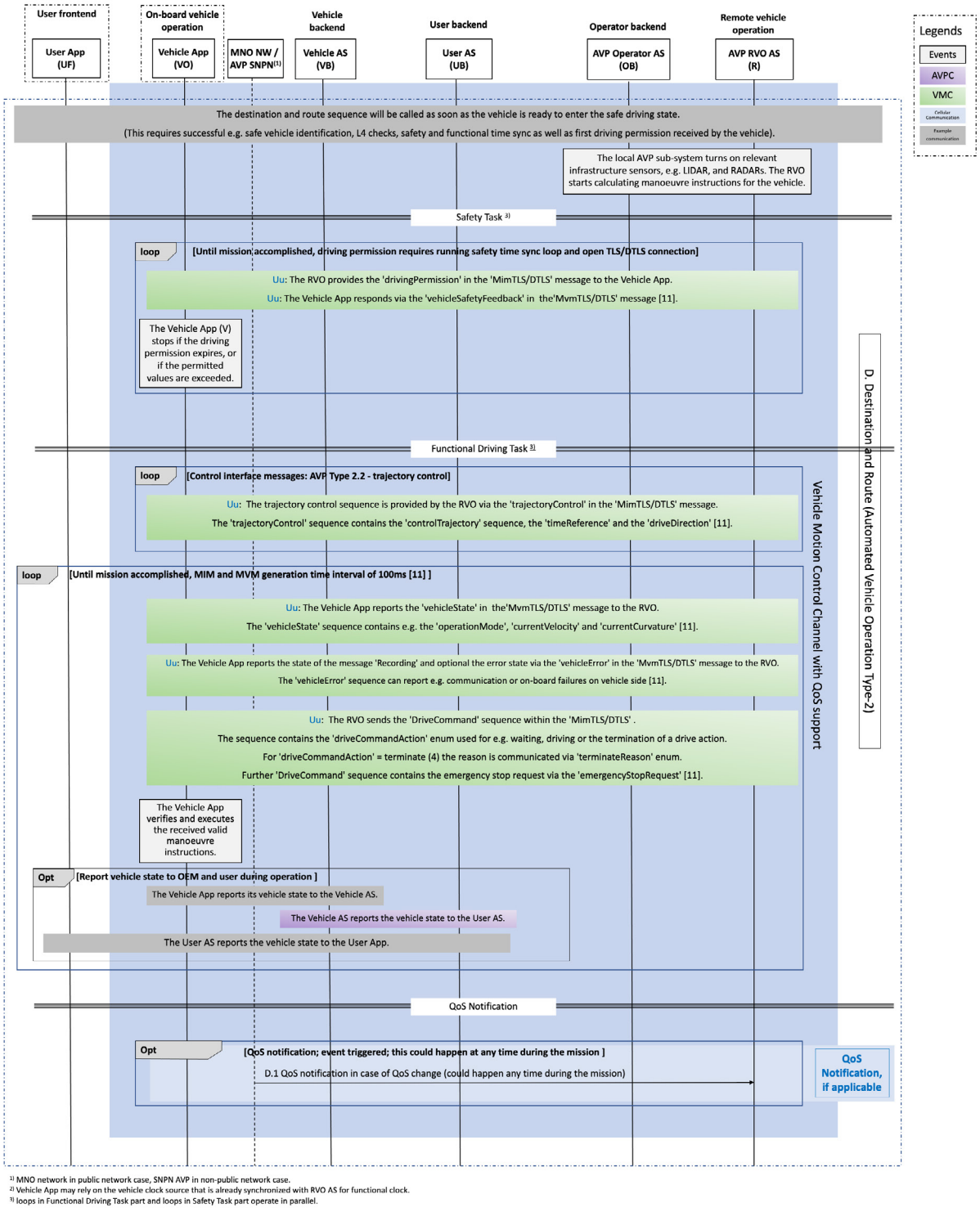


Figure 13: Communication sequence for 'destination and route' – Uu-based implementation

7.3.5.2 PC5-based implementation

For PC5 Direct Communication-based solutions, several implementation options have different locations of the facilities layer functions that terminate the VMC messages between AVP RVO AS and Vehicle App.

- Figure 14 shows the sequence diagram for the implementation option where the facilities layer functions are located at AVP RVO AS. Figure 36 in Section 9.5 shows the corresponding E2E protocol stacks.
- Figure 15 shows the sequence diagram for another implementation option, in which the facilities layer functions are located at the RSU ITS Service instead of AVP RVP AS. Figure 35 shows the E2E protocol stacks.

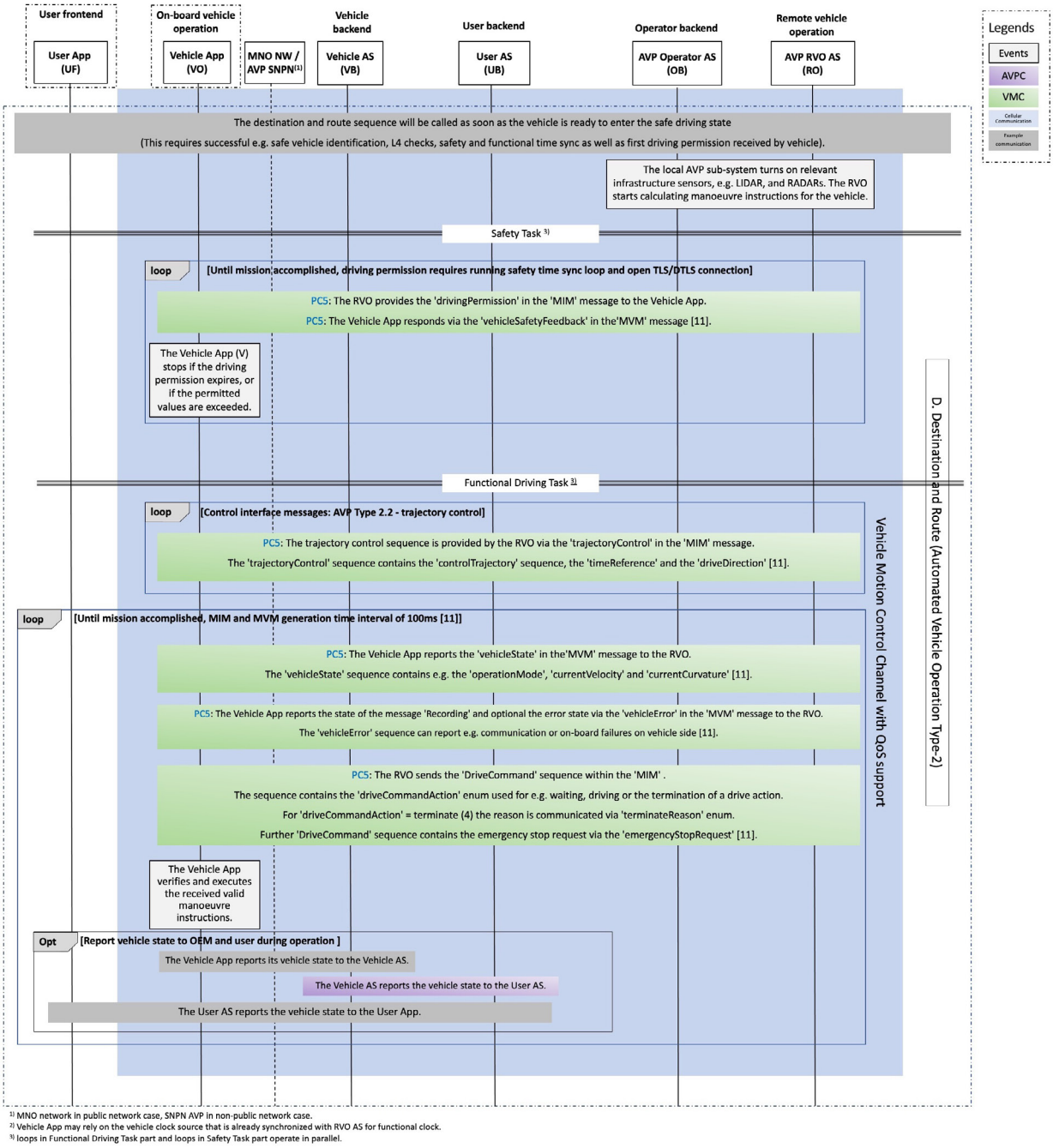


Figure 14: Communication sequence for 'Destination and Route' – PC5 Direct Communication AVP RVO AS-based facilities layer

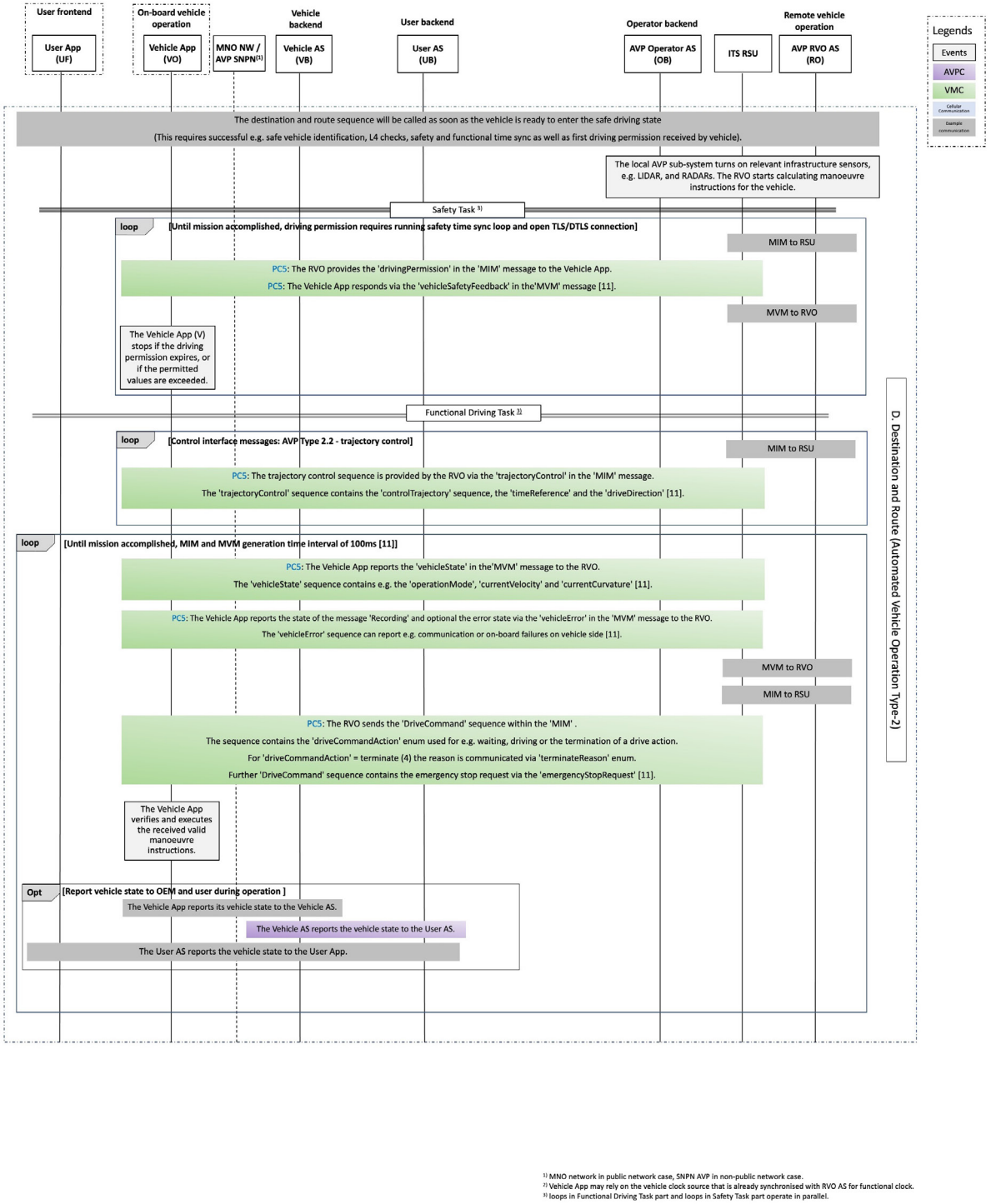


Figure 15: Communication sequence for 'Destination and Route' – PC5 Direct Communication RSU-based facilities layer

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

7.3.6 E. Destination reached (optional)

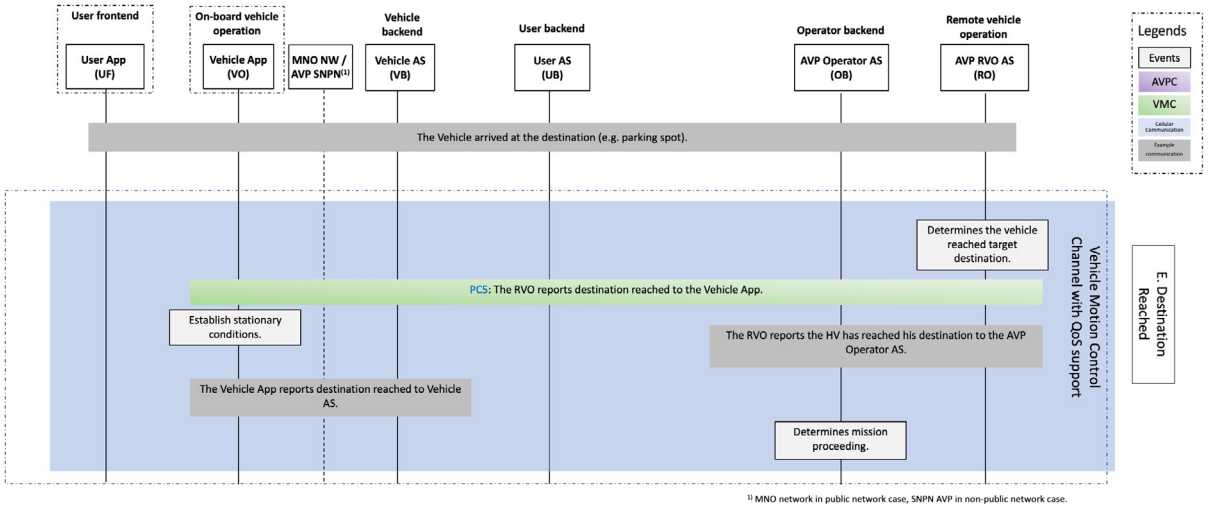


Figure 16: Communication sequence for 'Destination Reached'

7.3.7 F. Mission accomplished

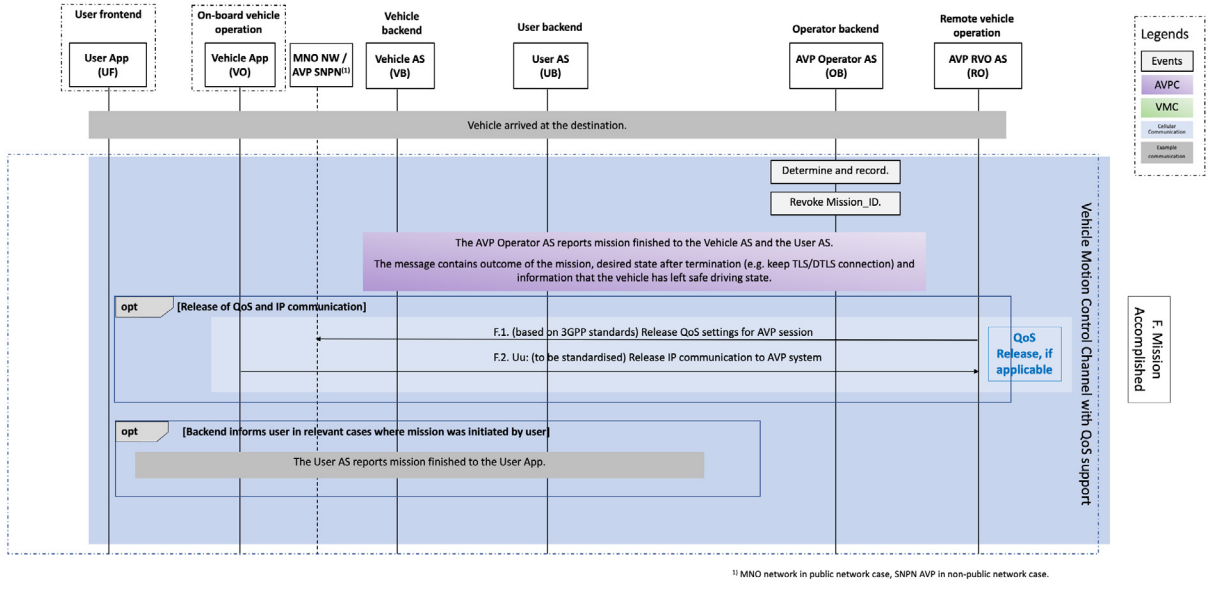


Figure 17: Communication sequence for 'Mission Accomplished'

Step F.1 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: Steps F.1 and F.2 are not applicable for PC5 Direct Communication.

7.3.8 G. Sleep sequence

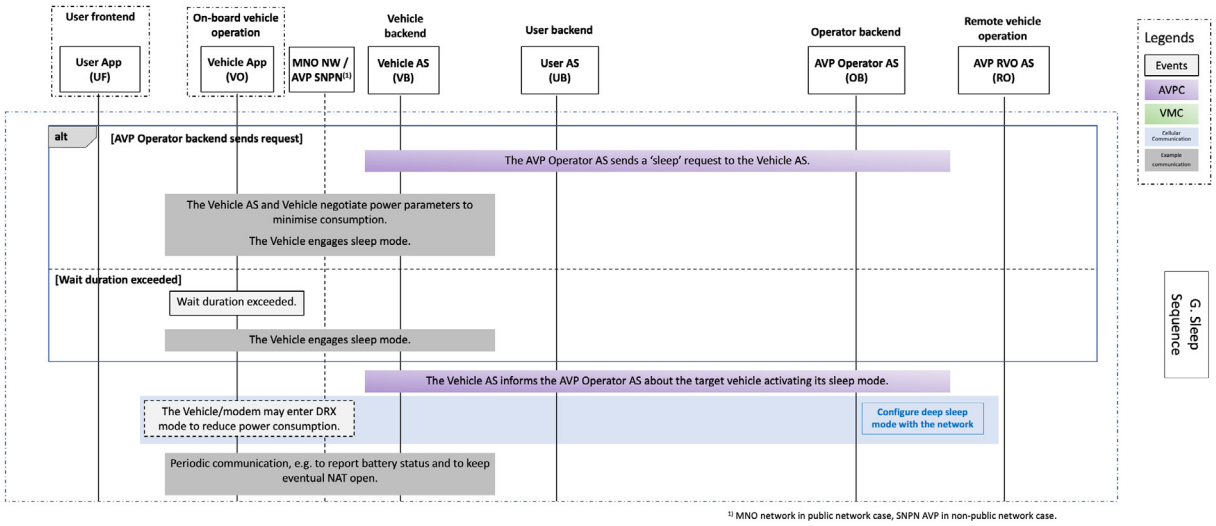


Figure 18: Communication sequence for 'Sleep'

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

To know the vehicle's valid IP address 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 periodic communication with MNO NW/AVP SNPN, the vehicle may send 'keep alive' messages with optional additional status information.

7.3.9 H. Wake-up sequence

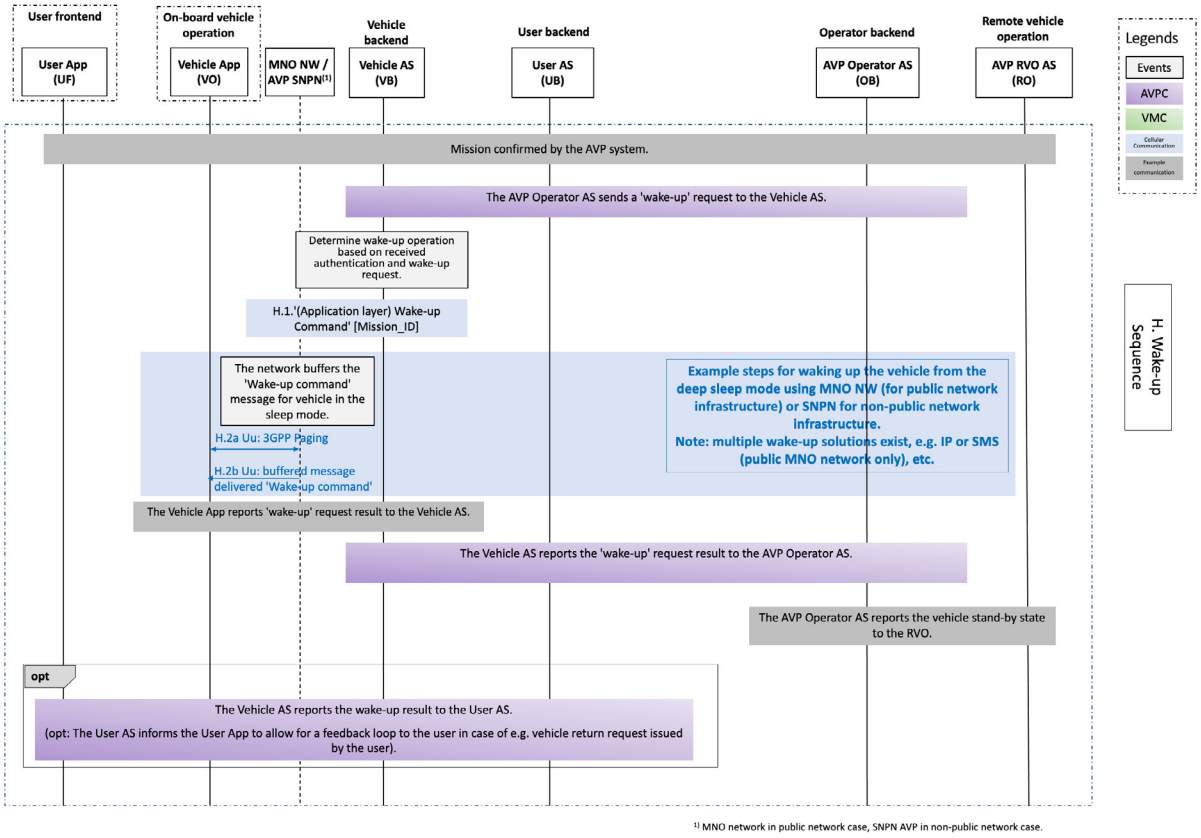


Figure 19: Communication sequence for 'Wake-up'

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'. Triggered by the wake-up received from the cellular network, the vehicle acts according to the OEM procedure, performs the desired action and reports the result to the AVP Operator AS (i.e. the vehicle replies with a *Wake-Up_Result* message).

7.3.10 I. Hand-back sequence

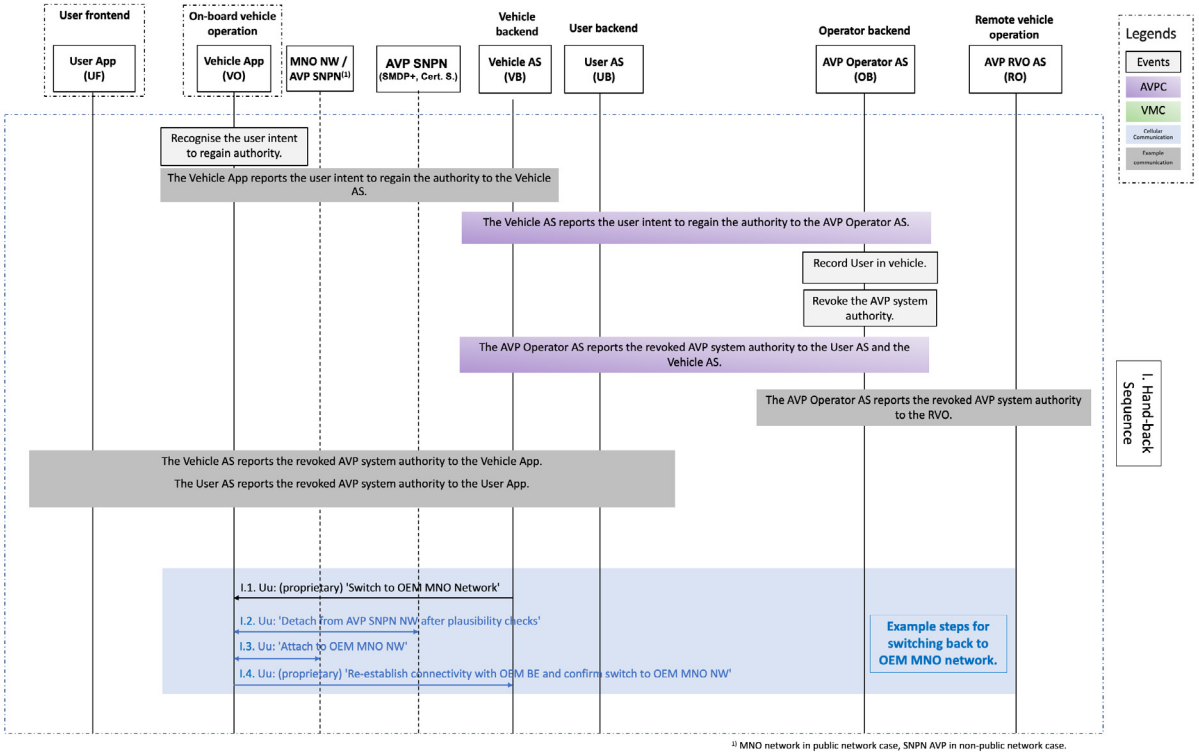


Figure 20: Communication sequence for 'Hand-back'

Message I.1 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.1, if the vehicle needed to switch to an 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 the MNO used prior to the AVP session.

In I.2, which is specific to SNPN, the application on the vehicle side instructs the modem to deactivate the SNPN mode and detach from the SNPN network.

While in I.3, 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.

Lastly, in I.4, the application on the vehicle side confirms the network switch and re-establishes connectivity with the Vehicle backend (e.g. announcing a new IP address) after the network has changed.

7.3.11 J. Check-out sequence

Figure 21 provides an example of the communication sequence for the check-out of the HV by the time it leaves the parking facility. The time by which the HV crosses the barrier of the parking facility can be used as the end of the overall parking time and is used for billing.

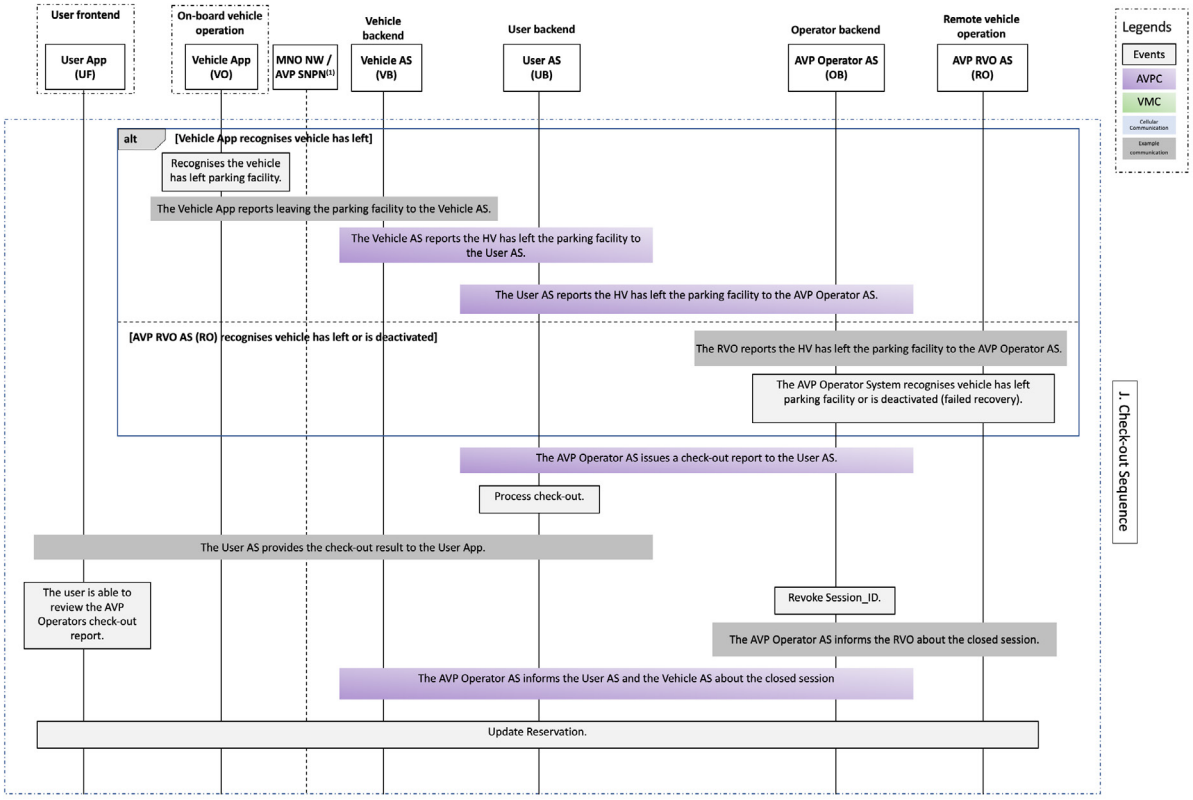


Figure 21: Communication sequence for 'Check-out'

7.3.12 K. Value-adding service request sequence

The value-adding service request sequence allows the delivery of services, e.g. charging or car-washing during the parking process without pre-reservation during the service discovery and reservation phase. The evaluation of the requests is processed on AVP Operator AS and might include vehicle parameters, such as the charging state of the vehicle battery.

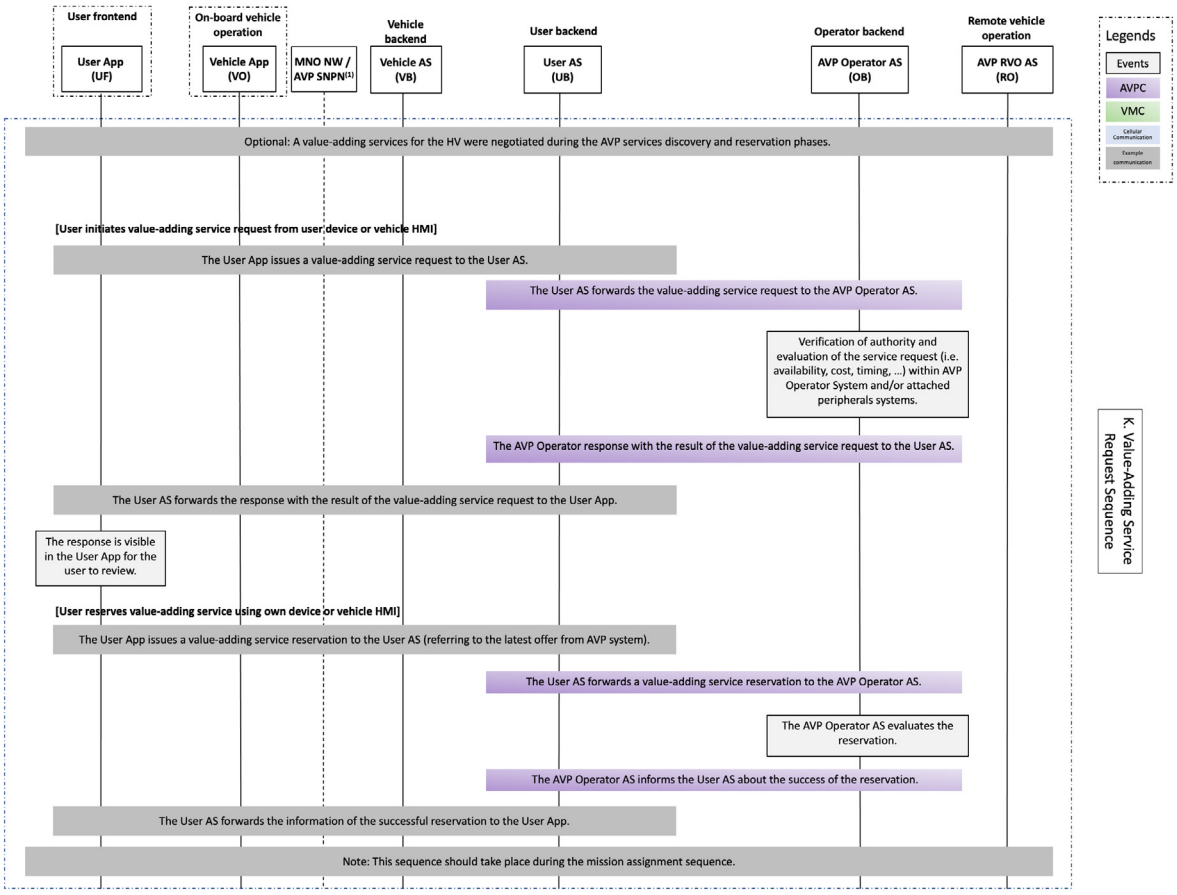


Figure 22: Communication sequence for 'Value-adding Service Request'

7.3.13 L. Vehicle return request sequence

The vehicle return request sequence allows for delivery of the vehicle to the drop-off zone if and when the driver arrives at the parking facility. The request sequence can be used as a general trigger of the vehicle retrieval process (illustrated in Figure 8), assuming the vehicle is in a 'parked' state by the time of the request, as illustrated by Figure 4.

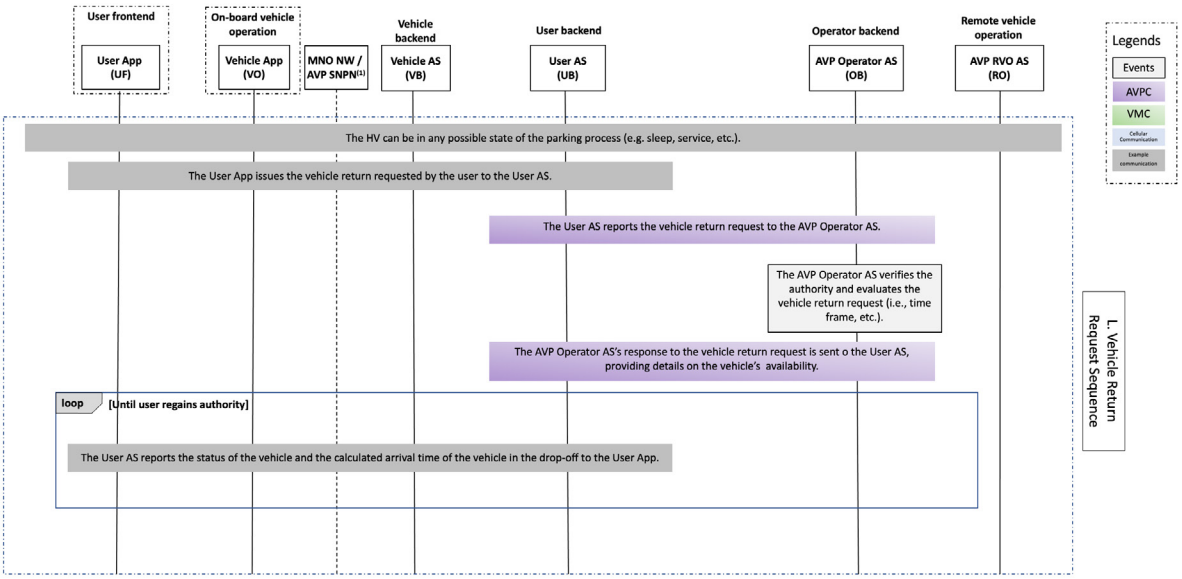


Figure 23: Communication sequence for 'Vehicle Return Request'

7.4 Time synchronisation in AVP systems

Remote-operated driving of the HV within the parking facility relies on synchronised clocks running on the RVO and HV sides. This is necessary to allow the HV to control the actuators by applying the right values at any point in time and enables the RVO to safely move the HV.

Figure 24 illustrates a possible example of a clock architecture based on three clocks. Two of them are used for time-stamp generation in communication with the RVO. Besides the functional clock responsible for general operations, a safety clock can be implemented to handle safety-related messages exchanged with ASIL-capable electronic control units (ECU). A possible implementation of a vehicle safety clock synchronization can be found in [12] (see chapter 4.2.8.). The containers to exchange the required request and response information are defined in [11] (see 7.4.6 and 8.3.6).

In the following chapters, the synchronisation of the functional and safety clocks between HV and RVO is described at high level. More detailed information and requirements can be found in [12].

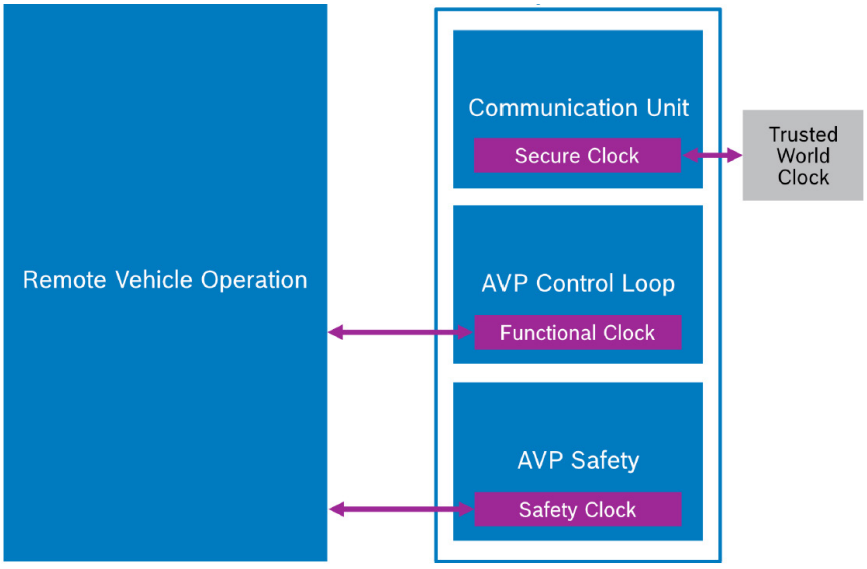


Figure 24: Example architecture of clocks in HV [12]

7.4.1 Functional time synchronisation

Serving as a common time base between the RVO and HV for all non-safety-related functions, the functional clock shall be synchronised. This can be done e.g. via a request- and response-method, e.g. using the messages *FunctionalTimeSyncRequest* and *FunctionalTimeSyncResponse* [12]. Other examples and options are by using Network Time Protocol (NTP) or by synchronizing clocks at RF level between an RSU and the HV.

As soon as the RVO and HV are synchronised, the functional clock can be used to generate, for example, time-stamps of non-safety related message or vehicle state

During a mission, the *functional time synchronisation* shall be repeated in such a way that 100 ms round-trip time can be guaranteed by both the RVO and HV. Receiving the *response* from HV, the RVO is calculating the offset between the functional clock running on the HV and the Remote Vehicle operation clock to ensure precise remote control of the HV. For a more detailed description, time budget calculations and further requirements, refer to [12].

7.4.2 Safety time synchronisation

Safety time synchronisation for Automated Vehicle Manoeuvring (AVM) can be implemented based on the messages and containers defined in ETSI TS 103 882, which is designed to allow for flexible implementations of a safety driving concept in AVM services.

Part of every safety driving concept is to ensure safe vehicle motion during the remote-operated driving process, including the ability to determine the validity of driving command and the concept to automatically stop within a safe distance in case the connection between RVO and a vehicle is lost and e.g. driving commands time out. For this a synchronised time between RVO and the vehicle needs to be established.

A specific implementation based on the messages and containers defined in [11] can be found in [12], chapter 4.2.8.

The messages *safetyTimeSyncResponse* and *safetyTimeSyncResponse* are part of the vehicle motion control sequences found in the Chapter 7.3.4 D. Destination and route (automated vehicle operation Type-2).

8 Implementation considerations for cellular network solutions

Based on the application-level system architecture for AVP Type-2 in Figure 1, Figure 25 illustrates how cellular networks enable end-to-end IP connectivity for key system interfaces in actual implementations, and particularly for the VMC interface between AVP RVO AS and Vehicle App, 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.

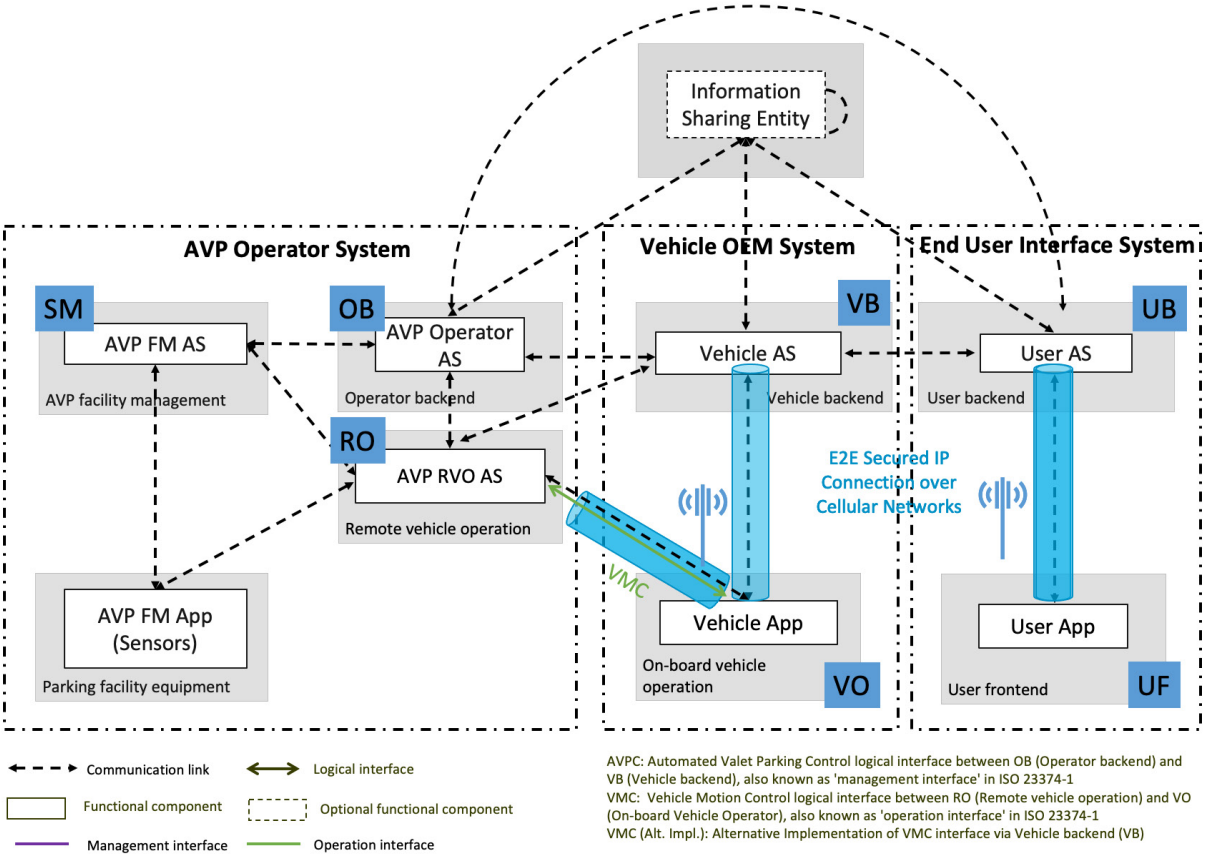


Figure 25: Architecture of cellular network-based AVP implementation

8.1 Considerations for cellular public networks

8.1.1 Network coverage in parking facilities

In many cases, parking facility owners have an agreement with MNOs in place. If the parking facility needs to extend or enhance its existing cellular public network to support AVP, the agreement can be updated, or new agreements can be made with these MNOs.

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 located at 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 the 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 good network coverage exists.

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 is under the responsibility of the parking facility owner and supported by the MNOs.

This AVP Type-2 Use Case implementation description assumes 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 and/or 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 MNOs 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 sent 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 information about the network used from the modem and store it 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 must be in place, which is mostly the case.

If no permanent roaming is in place, MNOs with AVP-capable vehicles among their subscribers will need to be accommodated. Alternatively, national roaming would have to be applied, or the coverage 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 must be established for the AVP application, specifically controlling the vehicle's motion.

This section first introduces the 3GPP features for prioritising dedicated application traffic flows and introduces 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, allowing more dynamic interaction. The 5G system 'exposes' different network services that can be viewed, configured or modified by authorised Application Service Providers (ASP).

The network exposure interfaces follow the HTTP REST model 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 using 3GPP network features, e.g. for 'QoS on Demand'. CAMARA enables simple and seamless access

by hiding the complexity of telecommunications behind APIs and making them available across telco networks and countries. CAMARA is an open-source project within the Linux Foundation that defines, develops, and tests APIs. It works in close collaboration with the GSMA Operator Platform Group to align API requirements and definitions. APIs are harmonised 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 26 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 SLAs 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 must be established when the UE has packets to transmit. One or more PDU sessions can be established within a single Network Slice.
- For one PDU session, multiple QoS Flows can be defined. The number of simultaneously active QoS Flows is typically limited.
  - One or more application flows[1] 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.

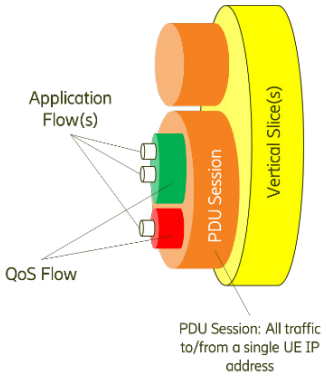


Figure 26: 3GPP QoS assurance mechanisms

[1] 'Application Flow' refers to data traffic of an application where a certain QoS policy can be applied. Application Flow can be described using descriptors, e.g. IP5-Tuple.

With respect to Quality on Demand (QoD)/Quality of Service (QoS), APIs 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 **work on an application level, not a device level.** So, different applications might use 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 the Radio Access Network (RAN) being temporarily unable to fulfil it. The network has mechanisms to handle such events, such as Alternative QoS profile, QoS sustainability analytics, and QoS monitoring. Additionally, proper network planning and QoS/priority assignment can also reduce the probability of such events.

8.1.3.3 Network slicing

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

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

The network offers information about available slice types to the device via URSPs, which in effect 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 access the relevant slice type for the AVP application. Applicable slice(s) must 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 networks, 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 networks 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. For 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 supports mutual authentication on top of the IP connection and 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) must be in place to ensure mutual trust between authenticated entities. This is out of the 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 QoD 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 to be able to take care of the appropriate roaming contracts. 5G slicing applied via URSP is a 3GPP technology and thus aligned inherently. From an operational perspective, the slice types need to be aligned so 5GAA and its partners can aim for profiles to be used globally (see camaraproject.org).

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

8.1.4.2 Regional breakout

A regional breakout (or local breakout) allows the Mobile Network Operator to breakout internet sessions of visiting (roaming) users and offer data services directly via the visiting MNO home network instead of running the user plane back to the user's home network. This 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 already operates 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 works 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 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, it consistently includes its preferred values during initial registration and mobility registration procedures.

8.2 Considerations for the cellular non-public network

Non-Public Networks are intended for the sole use of a private entity, such as an AVP garage operator, and may be deployed in various configurations utilising both virtual and physical elements. Specifically, they may be deployed as completely stand-alone networks, hosted by a PLMN, or 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 NPN, which could result in resources being used to reject that UE and, thereby, not being available to the UEs of the AVP service. It is also expected that UEs of the AVP service will not attempt to access a network without the authority to do so. For example, some AVP service UEs may be restricted to only accessing the NPN 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 a NPN 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 must have a subscription for the PLMN to access them. Therefore, the procedures for PNI-NPNs are the same as for PLMNs. From a device and AVP Operator perspective, PNI-NPN can be used agnostically when accessing PLMNs. 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 using services via PLMN. The SNPN Core is equivalent to the Home Public Land Mobile Network (HPLMN) Core, and the SNPN RAN is equivalent to the 'Untrusted Non-3GPP Access' entity. The SNPN 5G Core uses the same procedures as the Public Network Core, except as described

below. Meanwhile, the SNPN 5G RAN uses the same procedures as the 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.

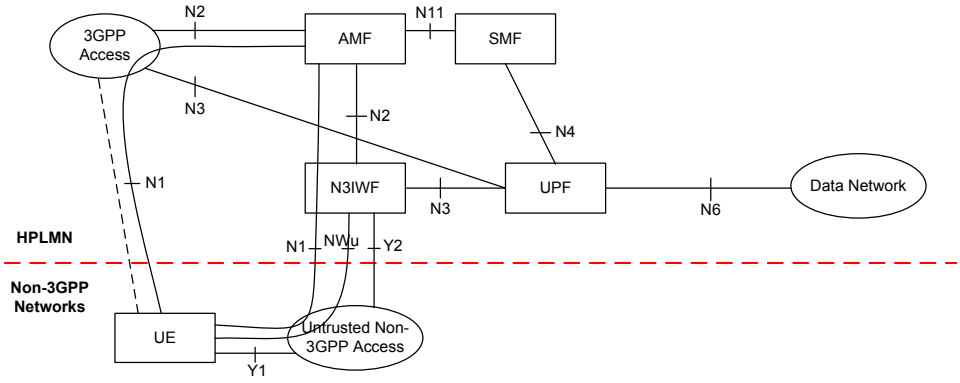


Figure 27: Non-roaming architecture for 5G core network with untrusted non-3GPP access [10]

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

In general, the same RAN principles as those for 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 suitable if the PLMN and NID broadcast by the cell match the selected/registered SNPN.

The NG-RAN node knows the SNPN ID(s) supported by neighbour cells. At the time of mobile communication handover, cells that do not support the serving SNPN ID are not considered candidate target cells by the source NG-RAN node. The target NG-RAN node performs access control. If it cannot accept the mobile communication handover for the serving SNPN, the target NG-RAN node fails, offering 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, it 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, it does not select and register with SNPNs. A UE that 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 operation settings in SNPN access mode are applied only to the Uu interface for connection to the SNPN. When a UE is 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 connecting to the PLMN). A UE supporting simultaneous connectivity to an SNPN and PLMN applies the network selection and the cell (re-) selection as applicable for accessing and operating through 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, it does not perform normal PLMN selection procedures. UEs operating in SNPN access mode read the available PLMN IDs and list of available NIDs from the available broadcast system information and use them for network selection.

For automatic network selection, the UE chooses 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 for which the UE has a Subscription Permanent Identifier (SUPI) and credentials, then how the UE selects an SNPN is based on UE implementation.

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

8.2.2.5 SNPN authentication methods

8.2.2.5.1 Embedded subscriber identification module profile switching

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

Applied to the automotive industry, a vehicle can use one eSIM profile for the 5G network in the factory and switch to another eSIM profile (from the contracted MNO) for the 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 for eSIM provisioning [6] [9].

8.2.2.5.2 Extensible authentication protocol – transport layer security

Extensible Authentication Protocol – Transport Layer Security (EAP-TLS) follows a similar principle to the eSIM profile switching, but uses digital certificates and EAP-TLS processes to attach to the NPN.

Broadly, EAP is an authentication framework frequently used in network and internet connections. It was defined in RFC 3748 and updated by RFC 5247. The EAP framework is introduced in 3GPP 5G networks for use in network access authentication (See 3GPP TS 33.501). More specifically, EAP-TLS (RFC 5216) can use a digital certificate for network access authentication when attaching to NPNs. 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:

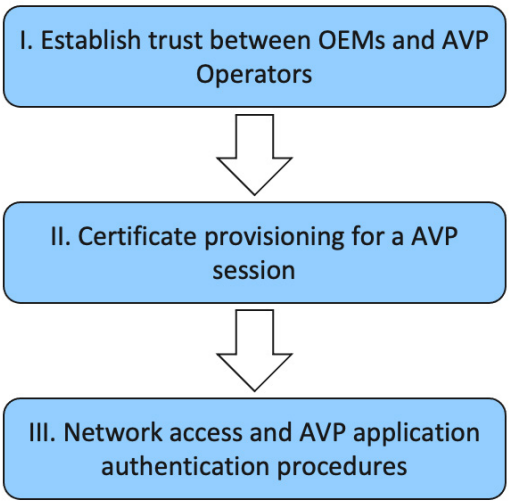


Figure 28: General steps of using EAP-TLS for the NPN network supporting AVP Use Case

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

Step II: A digital certificate is created and provisioned to a vehicle for a booked AVP session. This step occurs during the AVP service booking process, and 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 is performed to access the NPN, following 3GPP TS 33.501. This covers mutual authentication between the vehicle and the AVP network using the AVP session certificate from step II. The AVP session certificate for the vehicle can also be used for AVP Application authentication and security, e.g. establishing a TLS session between the vehicle and the AVP Operator System.

8.2.2.6 SNPN access to PLMN services

A UE connected to an SNPN may still be able to access services 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 mobile communication 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 the RAN of an SNPN, the UE obtains IP connectivity and 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 Non-3GPP Interworking Function (N3IWF) in the PLMN for establishing a secure tunnel between them 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 a 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.

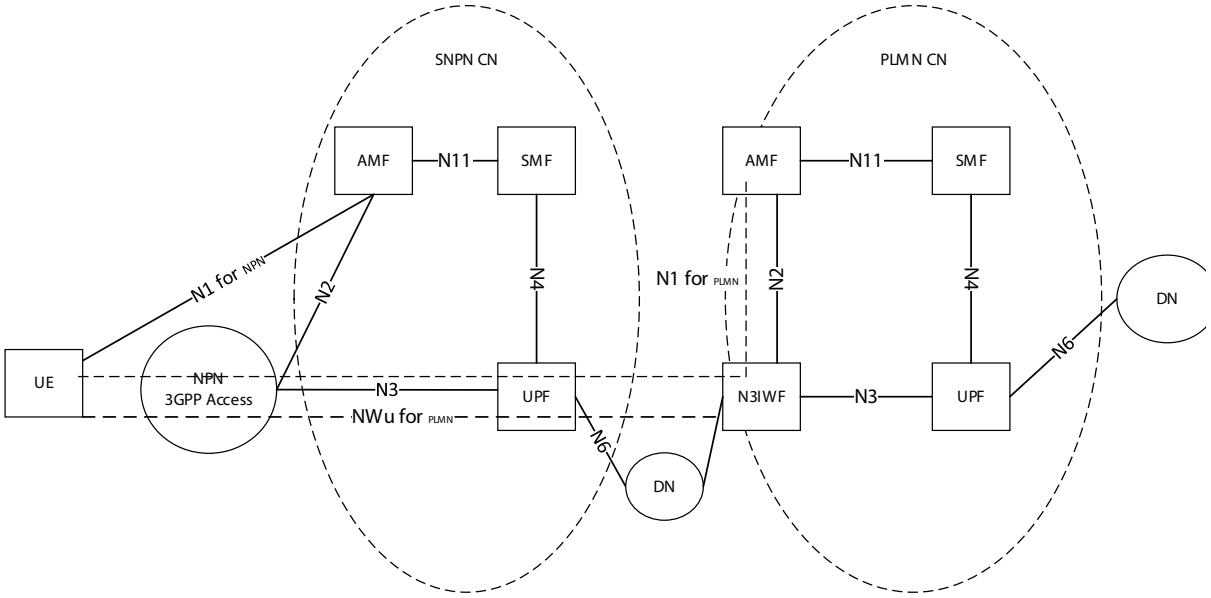


Figure 29: Access to PLMN services via stand-alone non-public network

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. Higher layer protocols (e.g. 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 reused.

8.3.1 Interaction between Vehicle AS and AVP Operator System

As shown in the initial architecture (Figure 1), the AVP Control (AVPC) interface between the 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.

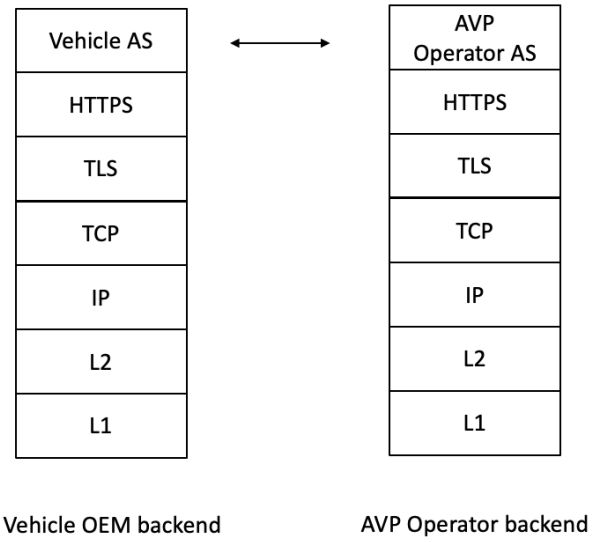


Figure 30: Example protocol stacks for Vehicle AS and AVP Operator AS interaction

As an example, Figure 30 shows that HTTP POST messages – sending data to a server to create/update a resource – and JSON encoding are used for the AVPC interface. Procedures of the AVP Type-2 Use Case are described in Section 7.

8.3.2 Vehicle motion control interface

This section describes the interaction needed for Vehicle Motion Control (VMC). As shown in the AVP Operator System architecture (Figure 1), information about vehicle movement is communicated through the VMC logical interface (or 'operation interface', as introduced in [1] and [12]) between the Remote Vehicle Operation and the vehicle. This logical interface can be implemented via the Vehicle AS or without traversing the Vehicle AS.

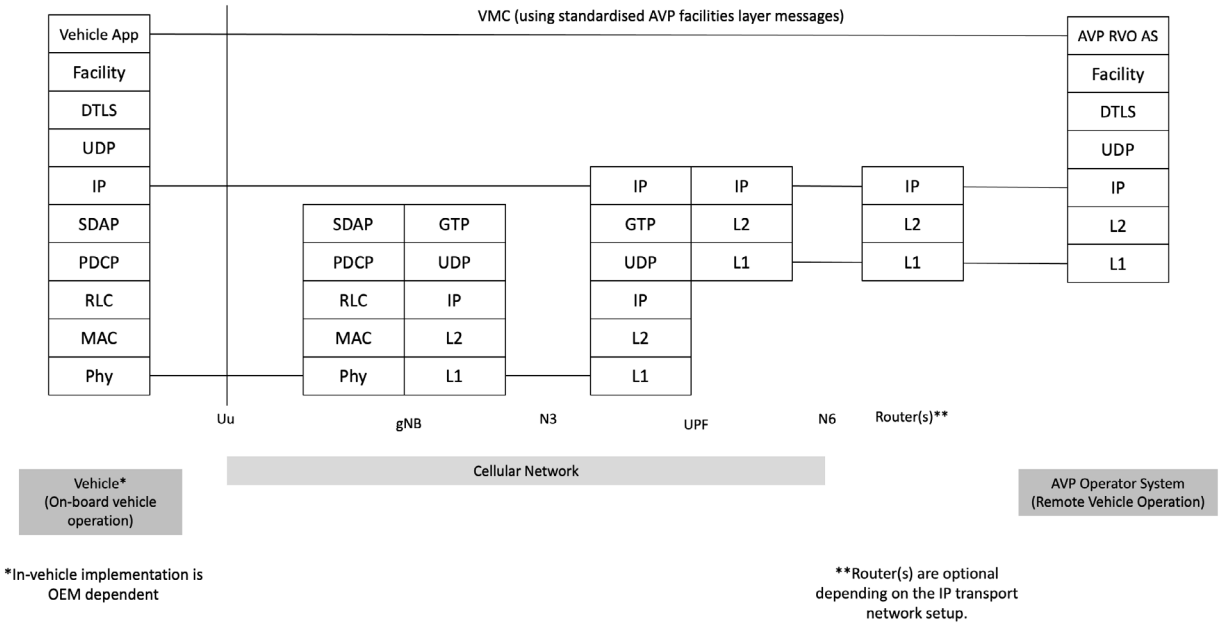


Figure 31: Example protocol stacks for vehicle motion control

Figure 31 shows an example of end-to-end protocol stacks when a 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 31, the protocol stacks at or within the Vehicle App, and the AVP Operator System are simplified examples. In actual implementation, the Vehicle App and facilities layer can be implemented, e.g. in the Electronic Control Unit, 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 is 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 1 is used, i.e. Vehicle AS acts as a proxy/FW between the vehicle and the AVP Operator System, then proprietary protocols can be used to transport the facilities layer message between them (i.e. only the Vehicle AS needs to be compliant with all protocol layers).

The User Datagram Protocol (UDP, or in this case via the Datagram Transport Layer Security, DTLS) transfers the facility layer message as a payload on an IP connection between the vehicle and the 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. The IP connection is initiated by the vehicle to avoid potential Network Address Translation (NAT) problems. After establishment, the IP connection can be used bidirectionally. 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 an example of a sequence for establishing a secured session for IP-based communication protocol stacks using digital certificates. This sequence can be used where secured IP communication sessions are needed. Figure 32 illustrates the security sequence for an IP session.

Three prerequisites for this security sequence are:

- Prerequisite 1: The secured communication between the vehicle and Vehicle backend exists, e.g. OEM TLS using OEM Certificate Authority (CA) signed certificates, between Vehicle App and Vehicle AS.
- Prerequisite 2: Trust has been established between the Vehicle backend (Vehicle AS) and AVP Operator backend (AVP Operator AS). This may include the necessary information exchange for certificates, addresses, etc.
- Prerequisite 3: Secure connection has been established (e.g. TLS) between the Vehicle backend (Vehicle AS) and AVP Operator backend (AVP Operator AS).

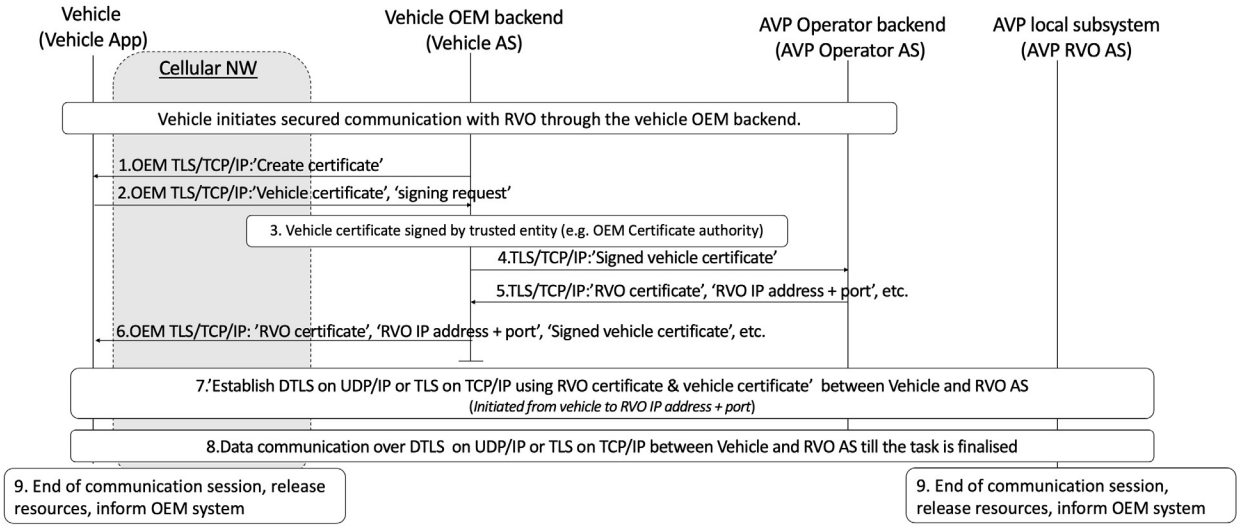


Figure 32: Example of a communication sequence for IP session with security

Notes:

- Figure 32 illustrates the general sequence for creating and exchanging digital certificates for secured TLS or DTLS communication between the Vehicle App and AVP RVO AS, which complies with [12]. In case multiple digital certificates are required, e.g. for different AVM missions or different ECUs in the vehicle, the sequence in Figure 32 can be recalled on demand.
- In this example, the AVP Operator AS also owns the 'RVO certificate', i.e. the digital certificate of AVP RVO AS.

  - Note: In an alternative implementation, the AVP RVO AS possesses a certificate jointly signed by the OEM Root Certificate Authority and AVP Operator CA. (See the example certificate chain in Annex F of [12].) In this case, Step 6 does not need to include the 'RVO certificate' because in Step 7 the Vehicle App can receive and verify the RVO certificate using the root certificate from its OEM.

- UDP or TCP can be used between the Vehicle App and AVP RVO AS, depending on the application layer protocols. This communication sequence for creating and exchanging digital certificates applies to 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 Vehicle App, as illustrated in Figure 1.

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 detail the above implementation architectures and considerations for using Direct Communication-based VMC and related ITS security mechanisms and protocol stacks.

The interfaces are indicated by dashed lines in Figure 33 and Figure 34, except for the interface over PC5, which is proprietary.

Note: This document currently doesn't cover details on how the PC5 Direct communication between the RSU/s and Vehicle/s are impacted and handled during the congestion scenarios.

9.1 Implementation architecture options for PC5 Direct Communication-based AVP vehicle motion control

9.1.1 Split RSU/RVO architecture

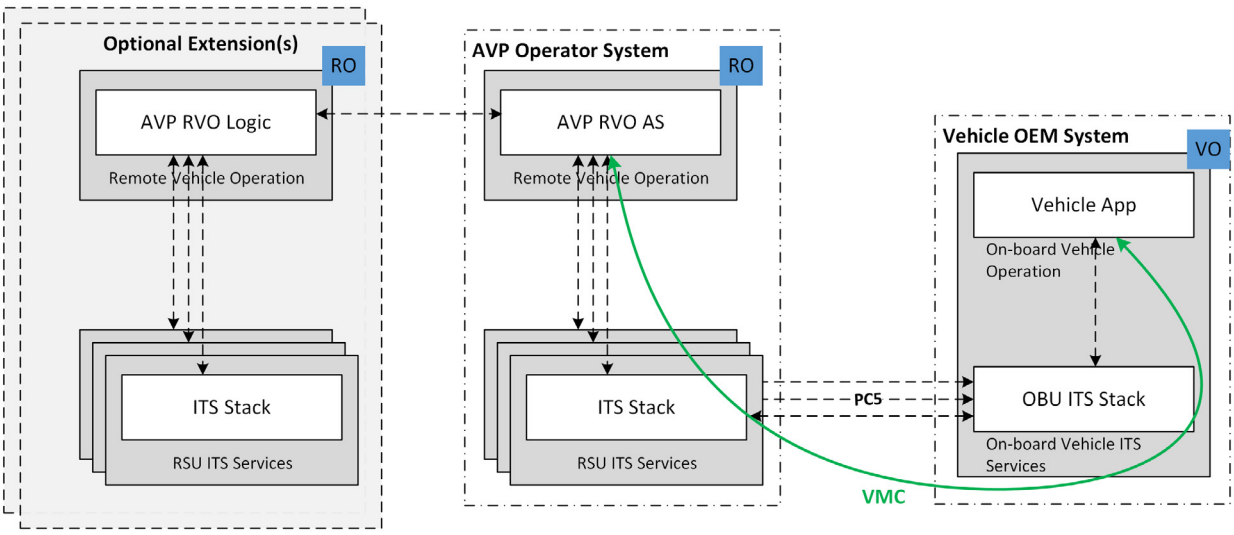


Figure 33: Split RSU/RVO architecture

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 of the vehicle is currently located.

Additionally, in this implementation architecture, the facilities layer responsible for encoding and decoding the VMC messages (as defined in [11]) can be implemented in several locations:

- On the AVP Operator System side:
  - As part of the AVP RVO AS (see the cellular-based implementation described in Section 8); and in this case, the RSU forwards encoded VMC messages between the AVP RVO AS and 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; further, the AVP RVO AS and RSU exchange the content of the VMC messages using a proprietary or standardised format selected by the implementer (see Figure 15b).
- 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 the scope 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, the dedicated AVP RVO AS deployed 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 manoeuvring control 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')

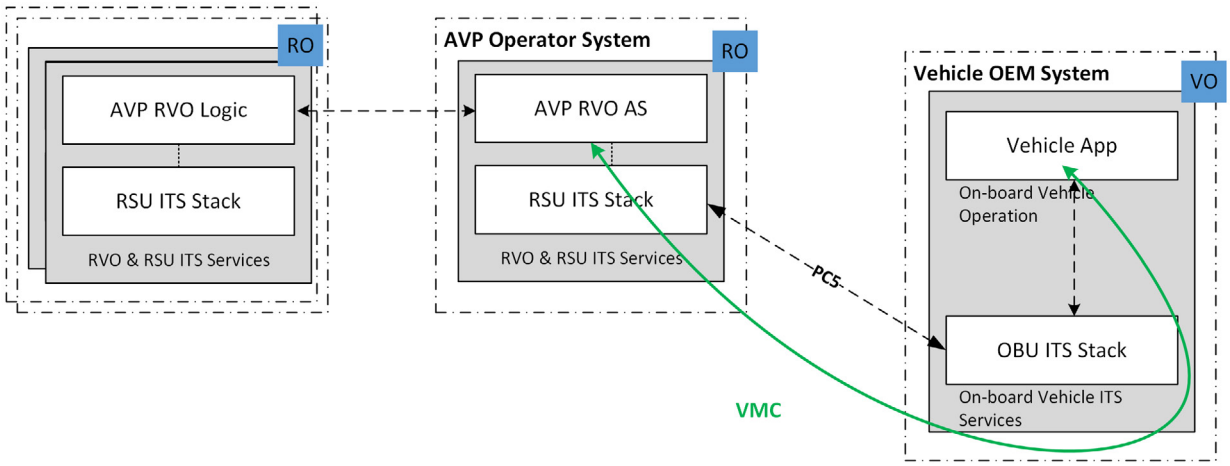


Figure 34: Co-located RVO-RSU architecture

Another possible implementation architecture would include the 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), computing hardware (CPU + Accelerators), and all required firmware, AI, vision analytics, AVP RVO AS and V2X software stack within the same enclosure. It might be beneficial in some scenarios regarding deployment, operational and maintenance costs. The multiple sensor measurements are input to the AI and vision analytics, and the fusion software stack is used to perform the environment perception, localisation, and metadata production. 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 using wired (Ethernet, etc.) or wireless links. A software framework may be running on the AVP RVO AS for information sharing between Smart RSUs. Decision-making may be distributed, and the decisions are shared between smart RSUs. In this scenario, mobile communication handover from one AVP RVO AS to the next as the vehicle progresses 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 perform 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 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 central 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. Depending on the scope of the deployment (e.g. RSU installation only or upgrading 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 a Received Signal Strength Indicator (RSSI) heatmap.

Regarding vehicle handling, several mobile communication handovers and networking mechanisms can be used depending on the size of the parking facility and the number of possible vehicles served. In general, RSUs are capable (if basic awareness or similar is active) of maintaining a database of ITS stations within which coverage and signal strength can then be monitored. Based on the final message properties, multiple RSUs nearby can broadcast messages to the intended vehicles or implement a more sophisticated 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 VMC:

PC5 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 garage locations (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: This document does not cover a hybrid mode in which VMC is switched from Uu-based to PC5 Direct Communication-based motion control or vice versa.

PC5 vehicle motion control as a primary system

In this scenario, PC5 Direct communication is the only system for AVP VMC.

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 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 AVP Type 2 VMC broadcast communication.
- 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 senders are who they claim to be.
- Authorisation – assurance that senders are entitled to the privileges they request.
- Integrity – assurance that any changes to packets after they are signed can be detected.
- Anonymity – mitigating privacy risk of vehicle users.

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

However, using 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 the 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; instead, they use short-term pseudonyms 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.
- As part of the above process, there is an exchange of public keys between the V2X station and the CA.
- The relevant CA provides the V2X station with a large number of 'pseudonym certificates', which are 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, in turn, use that to validate the digital signature for each received message. At this point, the messages are cryptographically verified (there are further validation tests for 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 necessary to comply with privacy regulations, additional mechanisms can be added to help mitigate privacy issues, such as employing a 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: Cellular coverage should ensure sufficient QoS to allow for the above functionalities.

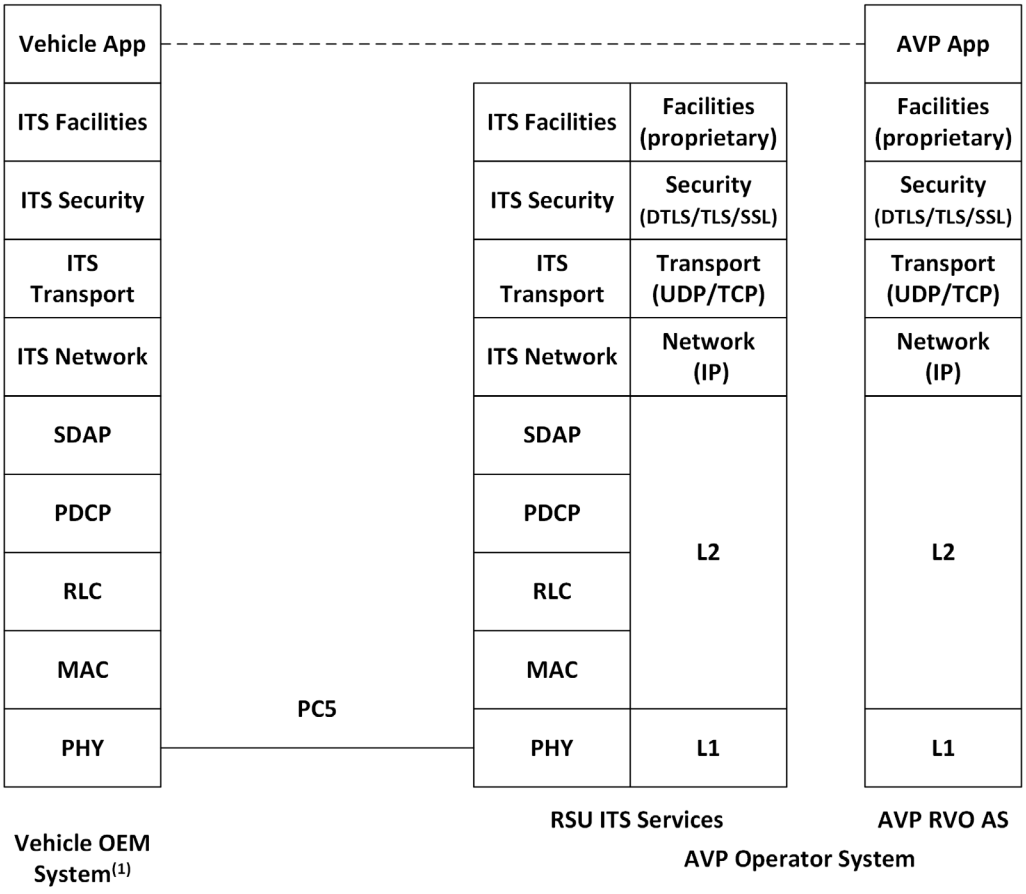
9.5 Vehicle motion control interface – PC5 Direct Communication-based vehicle motion control

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 1), information about vehicle movement is communicated through the VMC logical interface between the Remote Vehicle operation and the vehicle.

Figure 35 and Figure 36 below describe the protocol stack for RSU-based and AVP RVO AS-based facilities layer implementation architecture options (respectively).

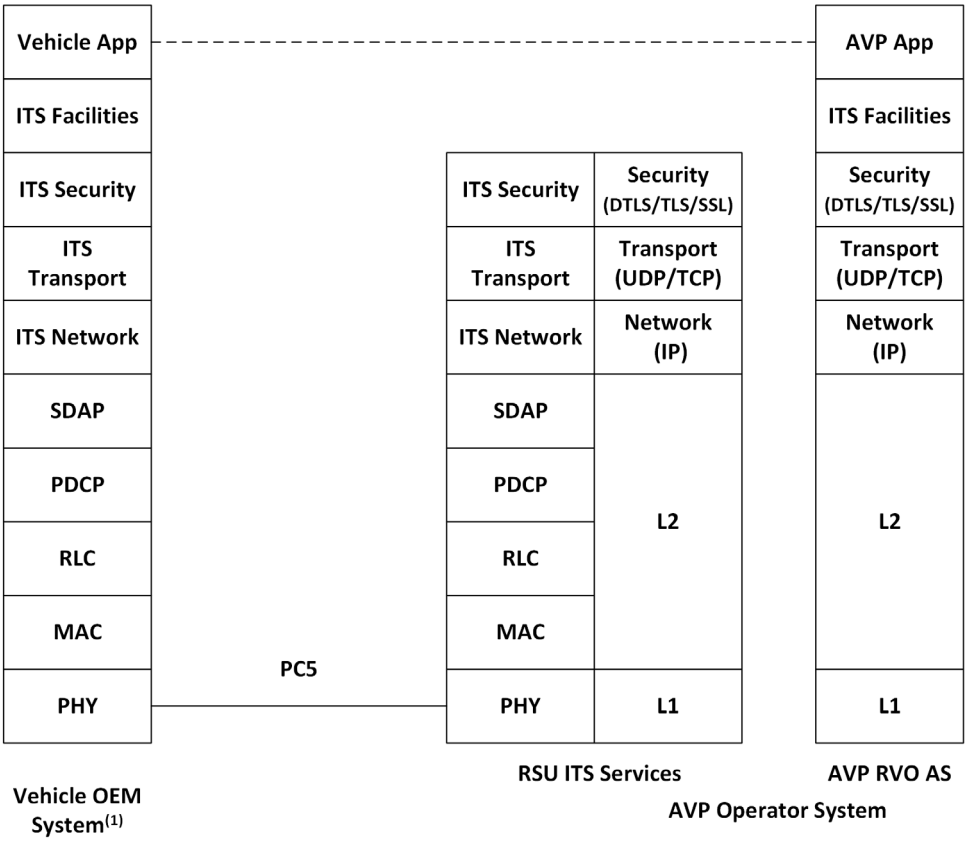
Figure 37 describes the protocol stack of the smart RSU implementation architecture where the AVP RVO AS and the RSU are collocated.

As noted above, vehicle-side protocols are implementation-specific and may vary between vehicle OEMs and/or vehicle models, which are outside the scope of this document.



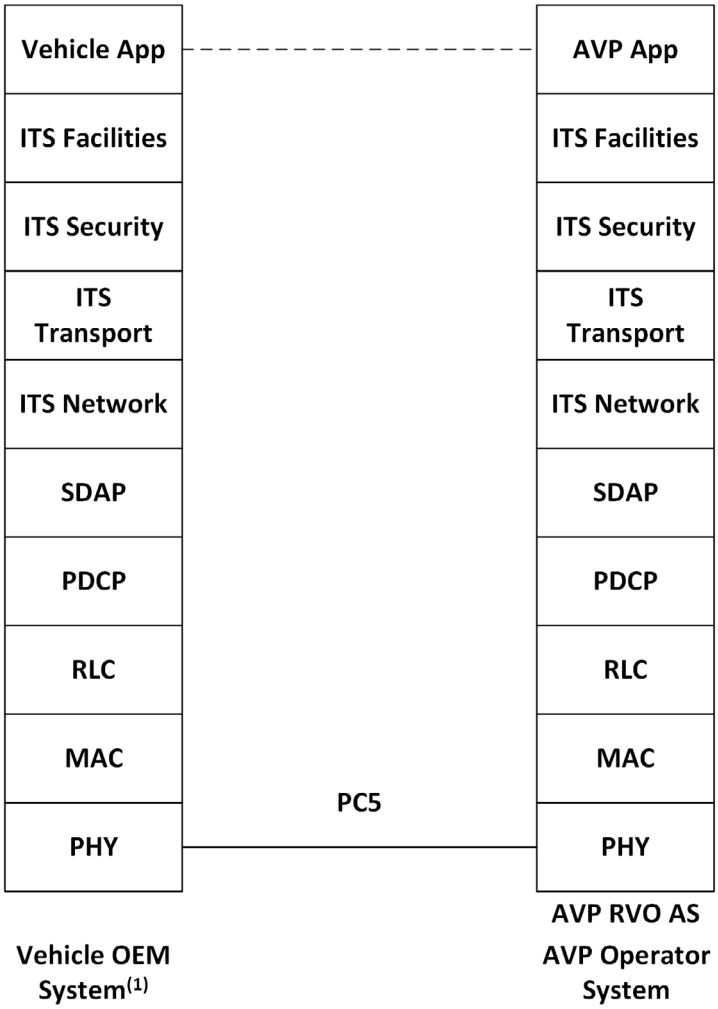
(1) In-vehicle protocol stack is OEM implementation specific

Figure 35: Protocol stack for RSU-based facilities layer vehicle motion control interface



(1) In-vehicle protocol stack is OEM implementation specific

Figure 36: Protocol stack for AVP RVO AS-based facilities layer vehicle motion control interface



(1) In-vehicle protocol stack is OEM implementation specific

Figure 37: 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 have been 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 AVP 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 networks 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.	Cellular networks provide SIM-based authentication for AVP network access. 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 outside the scope of the present document.
Access for vehicle to Vehicle backend.	The access to the Vehicle backend is provided via a cellular public network.	

There is a short interruption to connectivity between the vehicle and Vehicle backend at drop-off and pick-up areas.	Connectivity interruption only happens when the AVP network's preferred MNO differs from the one used for connecting the vehicle on 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 promotes UE energy saving.	See Section 8.1.5.
Vehicle remote wake-up.	The cellular public network is available in parking facilities, so 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.	Cellular networks can fulfil SLRs, which has been previously demonstrated 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 networks 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 provides SIM or certificate-based authentication. Cellular networks support any authentication solution using IP-based connections, such as TLS, DTLS, digital certificated, or user credential-based authentication, for transport and application layer 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 outside the scope of the present document.
Access for vehicle to Vehicle backend.	Access to the Vehicle backend is provided via the SNPN network.	Vehicle App and Vehicle AS must maintain a valid IP route to the vehicle.

There is a short interruption to connectivity between the 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 the SNPN network. Such interruption caused by network switching can be optimised 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 the SNPN network.
Vehicle power-saving mode.	The cellular network supported by the discontinuous reception (DRX) framework promotes UE energy saving.	See Section 8.1.5 for DRX. DRX is a radio interface feature that allows the UE to pause reception to save power and battery. The cycles are up to 10.240 ms, 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 as valid in the Vehicle backend because 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.	The assumption is that there is a valid IP connection between the 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 a 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 a User Consent Agreement for AVP use.

Trust between vehicle OEM and AVP Operator domain.	Trust between vehicle the OEM and AVP Operator should be established as defined in Tables 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 the scope of this document.
Access for vehicle to Vehicle backend.	Access to the Vehicle backend is provided via a cellular public or SNPN network.	
There is a short interruption to connectivity between the vehicle and Vehicle backend at drop-off and pick-up areas.	Connectivity interruption should conform with the definition in Tables 1 and 2.	
Vehicle power-saving mode.	PC5 Direct Communication is not used after the vehicle is switched off.	
Vehicle remote wake-up	The 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 the PC5 Direct Communication protocol (for example, a PC5 interface).	

Annex A: Considerations on messages and protocols among eco-system stakeholders for AVP service

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

For the standardisation of communication used in the AVP process, three categories can be identified:

Category 1: The communication between the backbends via the AVPC logical interface, also referred to as 'Management Interface' in ISO 23374-1 [1]

The AVPC logical interface enables communication between AVP Operator AS (OB), the User AS (UB) and the Vehicle AS (VB) for management and control signalling communications among AVP services.

The AVPC is used in the following examples (illustrated in the purple boxes within the sequences):

- Reporting from the VB to the OB that the HV has arrived at the reserved parking facility, as illustrated in Figure 9.
- Communication of the *Session_ID* and the AVP Network information from the OB to the VB, as illustrated in Figure 9.
- Mission status reported from the OB to the VB, as illustrated in Figure 11.
- The VB reports to the OB the intention of the user to regain authority over the vehicle, as illustrated in Figure 20.

When this document was published, the authors could not access a standard that detailed all required management interface messages or their content.

Besides the overall conditions applied to the management interface found in Chapter 7 of ISO 23374-1 [1], general requirements and message content are partly covered within the detailed implementation requirements found in [12].

Further, [12] also refers to a future document published by the same authors that is supposed to cover the full, detailed requirements of the management interface for AVP.

In the case of service discovery and reservation, no ongoing standardisation activities are known to 5GAA at the time of publication. An example sequence for this process can be found in Figure 5 and was derived from detailed discussions with EPA, ERTICO, VDA, and ISO. It should be highlighted that this interface is not only subject to detailed standardisation of the management interface in the automotive sector, but must also be complemented by parallel activities in the parking industry.

From this, 5GAA concludes that there is a clear need for a standardisation body to specify the management interface and its messages in detail, to keep up with current state development activities.

Category 2: The communication between the Vehicle App and the AVP RVO AS via the VMC logical interface also referred to as 'Operation Interface' in ISO 23374-1 [1]

The VMC logical interface is used to transmit driving commands and instructions from AVP RVO AS (RO) to the Vehicle App (VO) and can be implemented without going through the Vehicle AS (VB), as shown in Figure 3.

The VMC is used for example (illustrated in the green boxes within the sequences):

- To establish secure TLS/DTLS communication between the VO and the RO, as illustrated in Figure 10.
- To establish the functional time sync and the safety time sync between the VO and the RO, as illustrated in Figure 12
- To exchange the *drivingPermission* and trajectory control sequence via the MIM from the RO to the VO, as illustrated in Figure 12
- To provide the *drivingCommand* sequence within the MIM from the RO to the VO, as illustrated in Figure 12
- To report the *vehicleState* within the MVM from the VO to the RO, as illustrated in Figure 12

At the time of publication, the VMC messages, their content, and the requirements on VMC communication used for AVP Type-2 are covered mostly by the facility layer specifications found in ETSI TS 103 882 [11]. Together with [12], which contains more detailed descriptions and requirements, and ISO 23374-1 [1], this interface is covered by standardisation organisations, industry associations, or appropriate authorities.

Category 3: The communication covered by mobile communication within the AVP System

The following tables summarise the messages used in the mobile communication solution framework and candidate Standards Developing Organisations (SDO) or industry associations where such messages and related protocols can potentially be defined, to our best knowledge. The actual standardisation work or industry agreement has to be discussed among ecosystem stakeholders, and it is out of the scope of this 5GAA Work Item.

Interface			Message name	Step no. in communication sequence chart	Type	Notes
From	To					
SMDP+/Cert. S. (for AVP NW)	Vehicle App		Download and install AVP SNPN profile or certificate	α.15	To be standardised, to enable Vehicle App and SMDP+/ Cert. Server interoperability	3GPP, GSMA

Interface		Message name	Step no. in communication sequence chart	Type	Notes
From	To				
Vehicle AS	Vehicle App	Session_ID, AVP network MNO, QoS settings	A.1 (Public NW)	Proprietary	
Vehicle App	MNO NW	Switch MNO and plausibility checks	A.2 (Public NW)		This procedure follows the 3GPP standards.
MNO NW	Vehicle App	Switch MNO and plausibility checks	A.2 (Public NW)		This procedure follows the 3GPP standards.
Vehicle App	Vehicle AS	Switched to AVP network	A.3 (Public NW)	Proprietary	
Vehicle AS	Vehicle App	Session_ID, AVP network SNPN, QoS settings	A.1 (SNPN)	Proprietary	
Vehicle App	MNO NW	Detach from MNO NW after plausibility checks	A.2 (SNPN)		This procedure follows the 3GPP standards.
MNO NW	Vehicle App	Detach from MNO NW after plausibility checks	A.2 (SNPN)		This procedure follows the 3GPP standards.
Vehicle App	AVP SNPN	Attach to AVP SNPN and plausibility checks	A.3 (SNPN)		Depending on the authentication methods for SNPN, the procedures can follow the 3GPP specifications.
Vehicle App	Vehicle AS	Re-establish connectivity with OEM BE and confirm switch to AVP SNPN	A.4 (SNPN)	Proprietary	

Interface		Message name	Step no. in communication sequence chart	Type	Notes
From	To				
AVP RVO AS	MNO NW/ AVP SNPN	Request QoS settings for AVP session (at QoS API)	C.1	Standardised	3GPP
MNO NW / AVP SNPN	AVP RVO AS	ACK QoS settings for AVP session	C.2	Standardised	3GPP

Interface		Message name	Step no. in communication sequence chart	Type	Notes
From	To				

MNO NW/ AVP SNPN	AVP RVO AS	QoS notification in case of QoS change	D.1	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	MNO NW/ AVP SNPN	Release QoS settings for AVP session	F.1		The procedure is based on 3GPP standards.
Vehicle App	AVP RVO AS	Release IP communication to AVP Operator System	F.2	To be standardised	

Interface		Message name	Step no. in communication sequence chart	Type	Notes
From	To				
Vehicle AS	MNO NW/ AVP SNPN	(Application layer) wake-up command	H.1	(proprietary) up to the decision of the OEM	Message buffered at the network.
Vehicle App	MNO NW/ AVP SNPN	3GPP paging process	H.2a		According to 3GPP process.
MNO NW/ AVP SNPN	Vehicle App	(Application layer) wake-up command	H.2b		Buffered message delivered.

Interface		Message name	Step no. in communication sequence chart	Type	Notes
From	To				
Vehicle AS	Vehicle App	Switch to OEM MNO network	I.1	proprietary	
Vehicle App	AVP SNPN	Detach from AVP SNPN NW after plausibility checks	I.2		The procedure is based on 3GPP standards.
Vehicle App	MNO NW	Attach to OEM MNO NW	I.3		The procedure is based on 3GPP standards.
Vehicle App	Vehicle AS	Re-establish connectivity with OEM BE and confirm switch to OEM MNO NW	I.4	Proprietary	

The 5G Automotive Association (5GAA) is a global, cross-industry organisation of over 115 members, including leading global automakers, Tier-1 suppliers, mobile operators, semiconductor companies, and test equipment vendors.
5GAA members work together to develop end-to-end solutions for future mobility and transport services.
5GAA is committed to helping define and develop the next generation of connected mobility, automated vehicles, and intelligent transport solutions based on C-V2X.
For more information, please visit https://5gaa.org


5GAA
Automotive Association