International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.550

(12/2017)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Vehicular gateways and intelligent transportation systems (ITS) – Architecture for vehicular gateways

Architecture and functional entities of vehicle gateway platforms

Recommendation ITU-T H.550

ITU-T H-SERIES RECOMMENDATIONS

AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	H.240–H.259
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Telepresence	H.420–H.429
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
VEHICULAR GATEWAYS AND INTELLIGENT TRANSPORTATION SYSTEMS (ITS)	
Architecture for vehicular gateways	**H.550–H.559**
Vehicular gateway interfaces	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
Ubiquitous sensor network applications and Internet of Things	H.640–H.649
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779
Digital Signage	H.780–H.789
E-HEALTH MULTIMEDIA SERVICES AND APPLICATIONS	
Personal health systems	H.810–H.819
Interoperability compliance testing of personal health systems (HRN, PAN, LAN, TAN and WAN)	H.820–H.859
Multimedia e-health data exchange services	H.860–H.869

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T H.550

Architecture and functional entities of vehicle gateway platforms

Summary

Recommendation ITU-T H.550 describes the architecture, functional architecture framework and functional entities of vehicle gateway platforms (VGPs). Some signalling flows of VGP are also described in Appendix I.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.550	2017-12-14	16	11.1002/1000/13434

Keywords

Architecture, functional architecture framework, functional entities, signalling flow, vehicle gateway platforms, VGP.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T H.550

Architecture and functional entities of vehicle gateway platforms

1 Scope

This Recommendation specifies the architecture, functional architecture framework and functional entities for vehicle gateway platforms (VGPs). Some signalling flows of VGP are also described in Appendix I.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T F.749.1] Recommendation ITU-T F.749.1 (2015), *Functional requirements for vehicle gateways*.

[ITU-T F.749.2] Recommendation ITU-T F.749.2 (2017), *Service requirements for vehicle gateway platforms*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 driver-vehicle interface (DVI) [ITU-T F.749.2]: The integrated user interface for the vehicle. It includes visual displays, loudspeakers, microphones, manual input controls, etc.

3.1.2 functional entity [b-ITU-T Y.2012]: An entity that comprises an indivisible set of specific functions. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.

3.1.3 intelligent transport systems (ITS) [b-ITU-R handbook]: ITS can be defined as systems utilizing the combination of computers, communications, positioning and automation technologies to improve the safety, management and efficiency of terrestrial transport systems.

3.1.4 nomadic devices [ITU-T F.749.1]: Nomadic devices include all types of information and communication as well as entertainment devices that can be brought into the vehicle by the driver and/or passengers to be used while driving. Examples include mobile phones, portable computers, tablets, mobile navigation devices, portable media players and multi-functional smart phones.

3.1.5 remote user interface (UI) [ITU-T F.749.2]: An approach to realize the interaction between applications in nomadic devices and the driver-vehicle interface (DVI). The UI of applications in nomadic devices can be displayed in the vehicle's touch screen and drivers are able to control the applications through DVIs (touch screen, buttons etc.). A remote UI can help drivers avoid distraction from applications and thus reduce the probability of accidents.

3.1.6 telematics [b-ISO 15638-16]: Telematics is the use of wireless media to obtain and transmit (data) from a distant source.

3.1.7 vehicle gateway (VG) [ITU-T F.749.1]: A VG is a device in a vehicle that enables communications between a device in the vehicle and another device which may be physically located either inside the vehicle or outside the vehicle (e.g., roadside station, cloud-based server, etc.). A VG provides standardized interfaces and protocols, communications across heterogeneous networks, optimized network selection based on application needs and network QoS, arbitration and integration of network communications, security and switching network connections to maintain service continuity.

3.1.8 vehicle gateway platform (VGP) [ITU-T F.749.1]: A VGP is the collection of ICT hardware and software in a vehicle operating as an open platform to provide an integrated runtime environment for delivering the communications services of a VG. A VGP may also provide higher layer communications services such as interaction with the driver through the driver-vehicle access services and so on. Subsystems dedicated solely to vehicle operation are not considered part of the VGP. Supported applications/services include ITS and infotainment.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

CAN Controller Area Network

CI Communication Interface

DLL Data Link Layer

DVA Driver Vehicle Access

EAP Extensible Authentication Protocol

ECU Electronic Control Unit

ETC Electronic Toll Collection

GPS Global Positioning System

GRE Generic Routing Encapsulation

HUD Head Up Display

ICT Information and Communications Technology

IP Internet Protocol

ITS Intelligent Transport System

L2TP Layer 2 Tunnelling Protocol

MAC Medium Access Control

MAN Metropolitan Area Network

MIB Management Information Base

NAT Network Address Translation

OSI Open System Interconnection

POI Point Of Interest

PPTP Point to Point Tunnelling Protocol

PSAP Public Service Answering Point

QoS Quality of Service

RSU Roadside Unit

SAM Situational Awareness Management

SIM Subscriber Identification Module

SSL Secure Sockets Layer

TCP Transmission Control Protocol

TLS Transport Layer Security Protocol

TSP Telematics Service Provider

UDP User Datagram Protocol

UI User Interface

V2I Vehicle-to-Infrastructure

V2V Vehicle-to-Vehicle

VG Vehicle Gateway

VGP Vehicle Gateway Platform

VPN Virtual Private Network

WLAN Wireless Local Area Network

WPAN Wireless Personal Area Network

WWAN Wireless Wide Area Network

5 Conventions

In this Recommendation:

– The keywords "shall" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

– The keywords "should" indicate an optional requirement which is permissible. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the vendor. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Introduction

Figure 1 shows VGP positioning in the intelligent transport system (ITS) reference model: there are six major scenarios, i.e., vehicle to vehicle, vehicle to infrastructure, vehicle to cloud-based server, vehicle to nomadic device, vehicle to pedestrian/bicycle and interaction with in-vehicle network scenarios.

– The vehicle to vehicle (V2V) scenario mainly describes the safety and auto-driving scenarios in which vehicles communicate with each other.

– The vehicle to infrastructure (V2I) scenario mainly describes the safety, electronic toll collection (ETC) and traffic information exchange scenarios in which vehicles communicate with roadside infrastructures.

– The vehicle to cloud-based server scenario mainly describes the emergency call and telematics scenarios in which vehicles communicate with cloud-based services.

– The vehicle to nomadic device scenario mainly describes the telecommunication and remote user interface (UI) scenarios in which vehicles connect to nomadic devices.

– The vehicle to pedestrian/bicycle scenario mainly describes the safety warning scenarios in which vehicles communicate with the devices carried by pedestrian/bicycles.

– Interaction with the in-vehicle network scenario mainly describes the vehicle diagnostics, remote data collection and vehicle remote control scenarios in which a VGP communicates with the proprietary in-vehicle network.

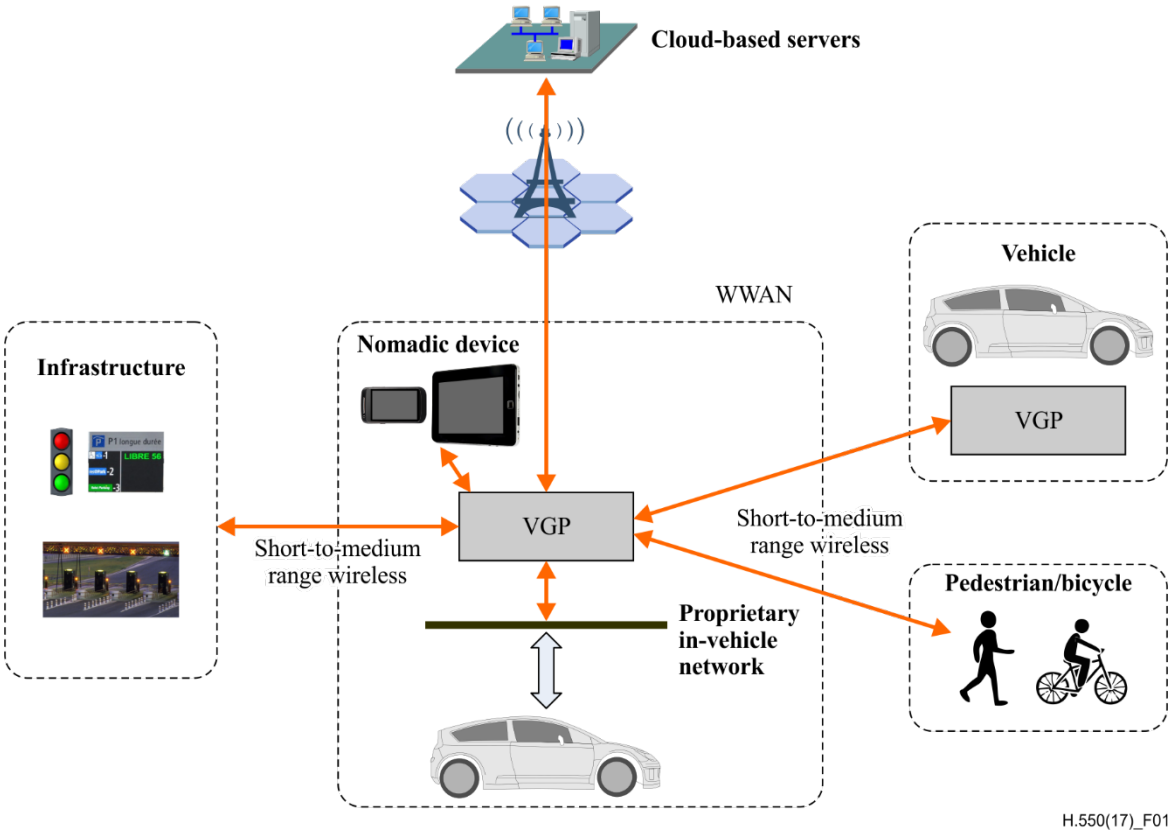

Figure 1 – Location of VGP in the ITS reference model

7 Architecture of VGP

Figure 2 presents the high-layer architecture of VGPs. The functionalities in the various subsystems of a VGP include:

– vehicle gateway

– services

– service functionalities

– management.

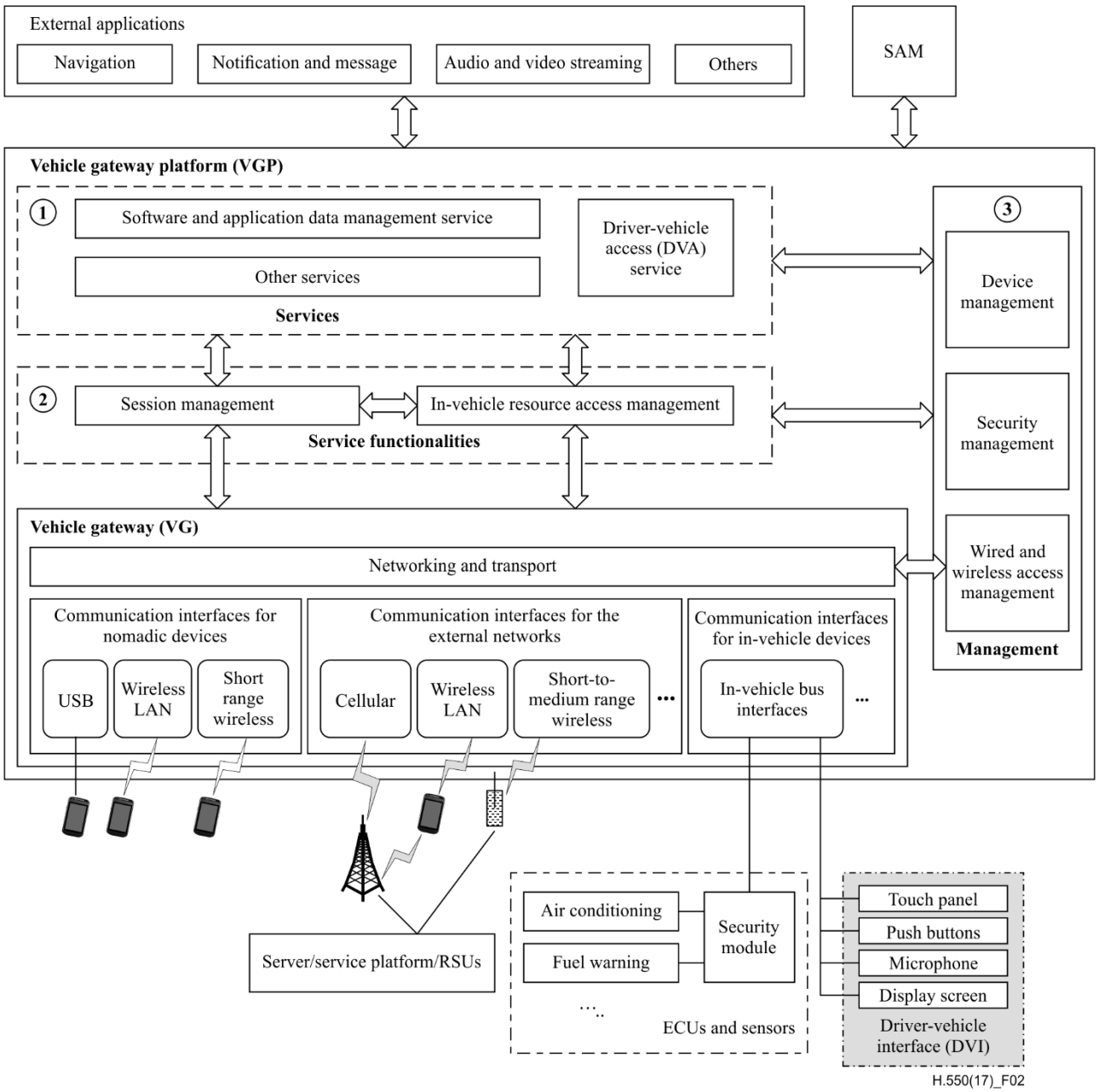

Figure 2 – High-level architecture of a VGP

The VGP services include software and an application data management service, driver-vehicle access service, and other services (see block (1) in Figure 2). Service functionalities include session management and in-vehicle resource access management (see block (2) in Figure 2). Management includes device management; security management and wired and wireless access management (see block (3) in Figure 2). Services support external applications such as navigation and infotainment to accomplish the session establishment, data format conversion and specific processing. A general description of the services and management of a VGP are presented below.

– **Vehicle gateway:** The VG functionality covers OSI layers 1 to 4. It includes transport functions, networking functions and network access functions.

– **Services:** Services support basic service capabilities for applications running and data / message processing. It includes the driver-vehicle access (DVA) service, software and application data management service, and other services.

– **Service functionalities:** Service functionalities support service management functions such as session management and in-vehicle resource access management.

– **Management:** Management supports device management, security management and wired and wireless access management.

7.1 Functional architecture framework

The functional architecture framework of the VGP is shown in the Figure 3. All independent functional blocks are connected with each other through the reference points. There are two types of reference points in the VGP: media and control.

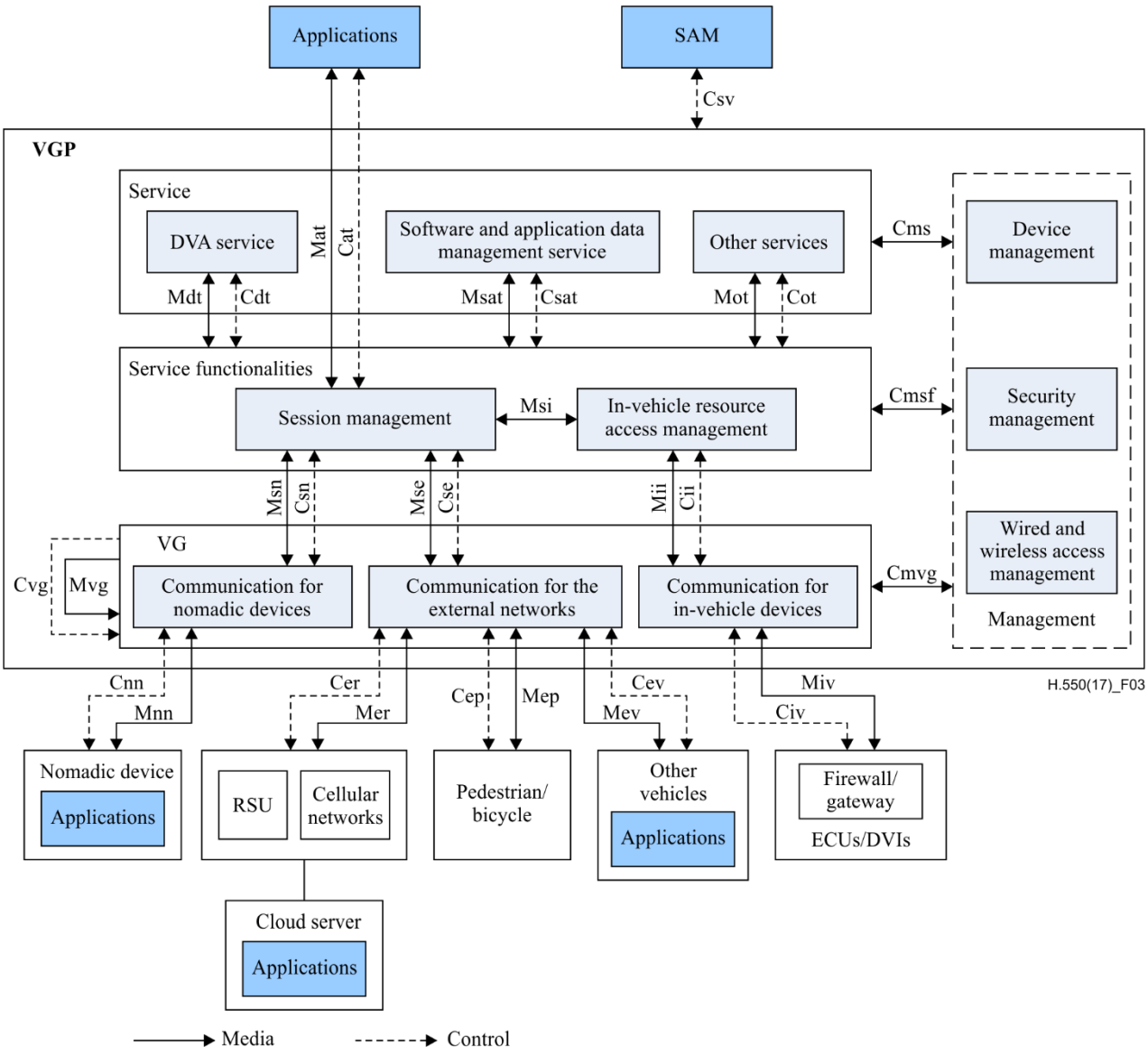

Figure 3 – Functional architecture framework of VGP

Media reference points include:

– Mnn reference point: media reference point between a nomadic device and the VG;

– Mer reference point: media reference point between the roadside unit (RSU)/cellular networks and the VG;

– Mev reference point: media reference point between other vehicles and the VG;

– Mep reference point: media reference point between a pedestrian/bicycle and the VG;

– Miv reference point: media reference point between the electronic control unit (ECU)/DVI and the VG;

– Msn reference point: media reference point between communication for nomadic devices and session management service functionalities;
– Mat reference point: media reference point between session management service functionality and applications;
– Msc reference point: media reference point between communication for external networks and session management service functionalities;
– Mii reference point: media reference point between communication for in-vehicle devices and in-vehicle resource access management service functionalities;
– Msi reference point: media reference point between session management service functionality and in-vehicle resource access management service functionalities;
– Mdt reference point: media reference point between DVA service and in-vehicle resource access management/Session management service functionalities;
– Msat reference point: media reference point between the software and application data management service and in-vehicle resource access management/session management service functionalities;
– Mot reference point: media reference point between other services and in-vehicle resource access management/session management service functionalities;
– Mvg reference point: media reference point between the entities inside the VG.

Control reference points include:

– Cnn reference point: control reference point between a nomadic device and the VG;
– Cer reference point: control reference point between the RSU/cellular networks and the VG;
– Cep reference point: control reference point between a pedestrian/bicycle and the VG;
– Cev reference point: control reference point between other vehicles and the VG;
– Civ reference point: control reference point between the ECU/DVI and the VG;
– Csn reference point: control reference point between communication for nomadic devices and session management service functionality;
– Csc reference point: control reference point between communication for external networks and session management service functionality;
– Cii reference point: control reference point between communication for in-vehicle devices and in-vehicle resource access management service functionality;
– Cat reference point: control reference point between session management service functionality and applications;
– Cdt reference point: control reference point between session management/in-vehicle resource access management service functionality and DVA service;
– Csat reference point: control reference point between in-vehicle resource access management/session management service functionality and the software and application data management service;
– Cot reference point: control reference point between in-vehicle resource access Management/Session management service functionality and other services;
– Csv reference point: control reference point between the VGP and situational awareness management (SAM);
– Cms reference point: control reference point between device management/security management and services;

– Cmsf reference point: control reference point between device management/security management and service functionalities;
– Cmvg reference point: Control reference point between device management/security management/wired and wireless access management and the VG;
– Cvg reference point: control reference point between the entities inside the VG.

8 Functional entities of VGP

8.1 Vehicle gateway

8.1.1 Definition of vehicle gateway

A VG is a function module of a VGP. VGs are devices in a vehicle that enable real-time two-way communication between an object in the vehicle and another object that may be physically located either inside or outside the vehicle (e.g., roadside station, cloud-based server, etc.). It provides standardized interfaces and protocols, communications across heterogeneous networks, optimized network selection based on application needs and network QoS, arbitration and integration of network communications, security and switching network connections to maintain service continuity.

A VG includes networking and transport functions and network access functions.

8.1.2 Networking and transport functions

The networking and transport functions cover the functions of the network and transport layers in the open system interconnection (OSI) model.

The VG should support several network protocols in the network layer, including IP (internet protocol) and non-IP protocols.

– The VG shall support IP protocols, e.g., IPv4 or IPv6 for Internet connectivity including the routing capability to the selected network.
– The VG should support other non-IP network protocols based on the supported interfaces. These protocols are meant to support applications with severe timing constraints and low latency requirements, e.g., time-critical safety-related applications, road safety and traffic efficiency applications.
– The VG should support the establishment of VPN in the network layer, e.g., IP Sec VPN, etc.
– The VG shall support several transport layer protocols in the transport layer, including the transmission control protocol / user datagram protocol (TCP/UDP). The VG should implement data segments and provide end-to-end and reliable/unreliable transportation for the upper layer. In addition, the VG should implement end-to-end flow control and error control in the transport layer. It should also support the network address translation (NAT) function to provide Internet access to every in-vehicle device.

8.1.3 Network access functions

8.1.3.1 Description

Network access covers the OSI model physical layer (PHY), which connects physically to the communication medium and to the data link layer (DLL). The DLL may be subdivided into the medium access control (MAC) sublayer (managing the access to the communication medium) and the logical link control (LLC) sublayer.

A VG should provide wired and wireless communication Interfaces (CIs) as follows:

– wired access (e.g., USB);

– wireless access (e.g., 2G / 3G / 4G, IEEE 802.11 [b-IEEE 802.11] and legacy dedicated short-range communications), which are used to communicate with devices outside the vehicle. Wireless access such as WLAN and short-range wireless CIs (e.g., wireless personal area networks) are used for communicating with in-vehicle nomadic devices (e.g., smartphones).

– A VG should support the establishment of VPN in DLL, e.g., Layer 2 Tunnelling Protocol (L2TP), Generic Routing Encapsulation (GRE), and Point-To-Point Tunnelling Protocol (PPTP).

8.1.3.2 Communications with nomadic devices

A VG should support interfaces for consumers to access in-vehicle modules/network via nomadic devices, such as USB, wireless LAN and short-range wireless CIs.

8.1.3.3 Communication with external networks

A VG should support cellular CIs which include CIs for 2G, 3G, 4G and future cellular technologies, wireless LAN CI, short-to-medium range wireless CIs and other CIs.

A cellular CI shall support the establishment and termination of a medium-dependent session. It is necessary to follow one of the connection establishment procedures defined in cellular communications standards, and the procedures defined in the relevant cellular communications protocols shall be followed.

A VG shall support the wireless LAN CI to get Internet access via a nomadic device (e.g., mobile phone). A VG connects to the nomadic device using a wireless LAN and uses the device as a gateway to access the Internet.

These short-to-medium wireless CIs are used to provide vehicle-to-vehicle (V2V) and vehicle to-infrastructure (V2I) communications in order to satisfy time-critical safety-related applications, traffic efficiency applications, cooperative local services and payment services.

Short-to-medium range wireless CIs may include CIs for IEEE 802.11 or 4G device-to-device.

Besides the cellular communications and short-to-medium range communications listed above, other outside-vehicle communications include global navigation satellite systems, infrared, mm wave communications, etc.

8.1.3.4 Communications with in-vehicle devices

A VGP shall support CIs to connect with the in-vehicle network, e.g., controller area network (CAN) bus interface protocol [b-ISO 11898-1].

A VGP should support the collection of (read-only) vehicle information from ECUs and sensors, e.g., engine control, lighting, air conditioning, power locks, active suspension, power seats, airbag, etc. The CI should also support backend servers and nomadic devices to remotely control (read and write) vehicle behaviour while security is guaranteed and communication authorized.

8.1.4 Reference points with other function entities

The reference points between the VG and other function entities are as follows:

– The reference points between the VG and session management services are as follows:

  1) **Reference point Msn:** This reference point is used to transfer media data that is received from nomadic devices through reference point Mnn to session management services. It is also used to receive media data from session management services which is then transferred to nomadic devices.

  2) **Reference point Csn:** This reference point is used to transfer control messages that are received from nomadic devices through reference point Cnn to session management

services. It is also used to receive control messages from session management services and then transfer them to nomadic devices. The examples of these control messages include the control messages of the remote UI.

3) **Reference point Msc:** This reference point is used to transfer media data that is received from an external network through reference point Mer/Mep/Mev to session management services. It is also used to receive media data from session management services and then transfer it to the RSU/cloud server, pedestrian/bicycle and other vehicles.

4) **Reference point Csc**: This reference point is used to transfer control messages that are received from the RSU/cloud server, pedestrian/bicycle and other vehicles through reference point Cer/Cep/Cev to session management services. It is also used to receive control messages from session management services. The control messages which are received from session management services should include network capabilities request messages (e.g., bandwidth, QoS request) and the messages that will be transferred to the RSU/cloud server, pedestrian/bicycle and other vehicles.

– The reference points between the VG and in-vehicle resource access management services are as follows:

1) **Reference point Mii:** This reference point is used to transfer data that is received from the in-vehicle network through reference point Miv to in-vehicle resource access management services. Mii is also used to receive media data from in-vehicle resource access management services and then transfer it to the in-vehicle network.

2) **Reference point Cii:** This reference point is used to transfer control messages that are received from the in-vehicle network through reference point Civ to in-vehicle resource access management services. It is also used to receive control messages from in-vehicle resource access management services and then transfer them to the in-vehicle network. The examples of these control messages include the vehicle remote control messages, vehicle data collecting control messages and OTA update of ECU control messages.

– The reference points between the VG and management are as follows:

1) **Reference point Cmvg:** This reference point is used to send bidirectional manage messages between the VG and wired and wireless access/security/device management. The control messages should include notifications of connection status in communication networks, indications of handover between the same network and different networks, control of communication connection establish/disconnect. The control messages should include keys/certifications/ciphers acquisition, encryption schemes acquisition and authentication/authorization for the communication process between the VG and external networks/nomadic devices. The control messages should also be used to retrieve the hardware/software running status of the VG.

– The reference points between the VG and nomadic devices are as follows:

1) **Reference point Cnn**: This reference point is used to send bidirectional control messages between the VG and nomadic devices. The control messages should include application control messages (e.g., remote UI control messages, wireless LAN hotspot control messages etc.).

2) **Reference point Mnn**: This reference point is used to send bidirectional media data between the VG and nomadic devices.

– The reference points between the VG and RSU/cellular networks are as follows:

1) **Reference point Cer**: This reference point is used to send bidirectional control messages between the VG and RSU/cellular networks. Through the RSU/cellular networks, the control messages are forwarded to the cloud server.

2) **Reference point Mer**: This reference point is used to send bidirectional media data between the VG and RSU/cellular networks. Through the RSU/cellular networks, the media data is forwarded to the cloud server.

– The reference points between the VG and a pedestrian/bicycle are as follows:

1) **Reference point Cep**: This reference point is used to send bidirectional control messages between the VG and pedestrian/bicycle.

2) **Reference point Mep**: This reference point is used to send bidirectional media data between the VG and a pedestrian/bicycle.

– The reference points between the VG and other vehicles are as follows:

1) **Reference point Cev**: This reference point is used to send bidirectional control messages between the VG and other vehicles.

2) **Reference point Mev**: This reference point is used to send bidirectional control messages between the VG and other vehicles.

– The reference points between the VG and in-vehicle network are as follows:

1) **Reference point Civ**: This reference point is used to send bidirectional control messages between VG and in-vehicle network.

2) **Reference point Miv**: This reference point is used to send bidirectional media data between the VG and in-vehicle network.

– The reference points inside the VG are as follows:

1) **Reference point Cvg:** This reference point is used to send bidirectional control messages between the sub-modules inside the VG.

2) **Reference point Mvg:** This reference point is used to send bidirectional media data between the sub-modules inside the VG.

8.2 Service functionalities

8.2.1 Session management service functionality

8.2.1.1 Definition of session management service functionality

The session management services functionality is a functional module of the VGP. It is in the OSI model session layer and presentation layer. The session management services are the data bus for data exchange between the VG, services, external applications and the security entity.

The session management services shall support session connection management and data processing functions. The session connection management function includes the establishment/ management/termination of session connection, attack detection and alarm generation. The data processing function includes data routing/dispatch, encryption and decryption, compression, data format conversion, data filtering, etc.

8.2.1.2 Session connection management

The session management service functionality should implement establishment/management/ termination of session connections between services/external applications. Session management services should monitor the status of session connections and select proper communication network cooperation with the VG to provide a secure and high-quality connection.

The session management service functionality should provide unified APIs (application programming interfaces) for external applications. Session management services should provide proper communication connection according to the requirements (e.g., QoS, security requirements) of applications.

The session management service functionality should support the establishment of the transport layer security protocol / secure socket layer (TLS/SSL) VPN.

The session management service functionality should support attack detection and alarm generation (e.g., firewall functions) to guarantee the security of a connection.

8.2.1.3 Data processing

The session management service functionality should process data to guarantee the consistency of the data format, high efficiency and security of data transportation.

– The session management service functionality should process two-way data format transformation to transport data between the VG and applications.

– The session management service functionality should compress and decompress two-way data to increase the efficiency of data transportation.

– The session management service functionality should support the technologies of data encryption and decryption, and digital signatures to guarantee the safety of data transportation.

– The session management service functionality should support data exchange management, including the data/message route management function and data/message dispatching management function.

1) The data/message routing management function supports the routing of the data/message. It selects the appropriate interface and protocol to route data/messages between the VG and external applications according to preconfigured routing tables.

2) The data/message dispatching management function should support:

i. permission/rejection for data/message requests of applications according to the instructions of the security management function;

ii. real-time processing of high-priority data/message and pause/resume processing of low-priority data/message.

8.2.2 In-vehicle resource access management service functionality

8.2.2.1 Definition of in-vehicle resource access management service functionality

Because in-vehicle resource access has a strong influence on driving safety, VGPs should have an independent and isolated service to implement data exchange between external applications and an in-vehicle network.

The in-vehicle resource access management service functionality shall support data exchange and connection management between external applications/networks and in-vehicle networks. It shall guarantee security and high-efficiency of data exchange and connection establishment.

8.2.2.2 Component description

The in-vehicle resource access management service functionality should implement data exchange between external applications/devices and the in-vehicle network through the connection to session management services.

The in-vehicle resource access management service functionality should implement external applications access authentication/authorization, and keys/certifications/ciphers acquisition through the connection to the security entity.

The in-vehicle resource access management service functionality should support the establishment of a secure connection to the in-vehicle network through the interaction with a firewall/gateway in a vehicle.

The in-vehicle resource access management service functionality should support data encryption and decryption, data compression, protocol conversion and data format conversion of data exchange between external applications and the in-vehicle network.

The in-vehicle resource access management service functionality should support the access control function of external applications, such as request frequency control. It also should support the access control function according to the driving state that can be acquired from the external SAM function.

8.2.3 Reference points with other function entities

The reference points between service functionalities and other function entities are as follows:

– The reference points between service functionalities and a DVA service are:
  – **Reference point Cdt:** This reference point is used to send bidirectional control messages between service functionalities and DVA services. The control messages should support DVI working status update, DVI capability request, etc.
  – **Reference point Mdt:** This reference point is used to send bidirectional media data between service functionalities and DVA services. The media data should support audio/video stream or other data formats.

– The reference points between service functionalities and the software and application data management service are:
  1) **Reference point Csat:** This reference point is used to send bidirectional control messages between service functionalities and the software and application data management service. The control messages should support modify/delete/add request, storage/read request of application data, etc. The control messages should also support software deployment/update/configuration request, etc.
  2) **Reference point Msat:** This reference point is used to exchange data between service functionalities and the software and application data management service for application data storage/read and software deployment/update.

– The reference points between service functionalities and other services are:
  1) **Mot reference point:** This is the media reference point between service functionalities and other services.
  2) **Cot reference point:** This is the control reference point between service functionalities and other services.

– The reference point between session management service functionality and the in-vehicle resource access management service functionality is:
  1) **Reference point Msi:** This reference point is used to exchange data between the session management service functionality and in-vehicle resource access management service functionality. The data includes vehicle data that is exchanged between external applications and the in-vehicle network (e.g., CAN, [b- ISO 17458-1], [b-MOST]).

– The reference points between the session management service functionality and external applications are:
  1) **Reference point Mat:** This reference point is used to exchange data between the session management service functionality and external applications which run on the VGP.
  2) **Reference point Cat:** This reference point is used to send bidirectional control messages between the session management service functionality and external applications which run on the VGP.

– The reference points between service functionalities and the VG are:

1) **Reference point Msn, Msc, Mii, Csn, Csc, Mii:** These reference points refer to clause 8.1.4.

– The reference point between service functionalities and management is:

1) **Reference point Cmsf:** This reference point is used to send bidirectional manage messages between service functionalities and wired and security/device management. The control messages should include keys/certifications/ciphers acquisition, encryption schemes acquisition and authentication/authorization for session connection, data processing and vehicle resource access. The control messages should also be used to retrieve software running the status of service functionalities.

8.3 Services

8.3.1 Driver-vehicle access service

8.3.1.1 Definition of driver-vehicle access service

The driver-vehicle access (DVA) service is a functional module of the VGP. The DVA service supports the function of interacting between DVIs inside vehicles and applications, include louder speaker, buttons and visual display equipment (e.g., display screen and head up display).

8.3.1.2 Component description

The DVA service should control which DVIs in a vehicle can be used by different applications (e.g., lower voice, disconnect from display or change display mode etc.) depending on the instructions from the external SAM function.

The DVA service should complete the following functions by interacting with service functionalities:

– The DVA service should analyse and instruct whether the message/data can be routed, delayed or cancelled according to the driving scene that is received from the external SAM function.

– The DVA service should support retrieve working status of DVIs. And DVA service should support changing the data format (e.g., change from video format to audio format) and re-routing to different DVIs according to the working status of DVIs.

– The DVA service should support remote UI between applications and DVIs. The DVA service should support DVI capability authentication/authorization through security management when the external applications request DVI access.

8.3.2 Software and application data management service

8.3.2.1 Software management service

8.3.2.1.1 Description

The software management service allows the deployment and maintenance of software over the different software-based units located inside or outside the VGP in an efficient, flexible and secure way. This service also takes care of the consistency between the software package versions deployed over the different software-based units.

8.3.2.1.2 Component description

The software management service is made up of the following components:

– A common, fast, secure, safe and flexible interface for software package upload from external devices or servers. This interface is used either by external devices such as a nomadic device connected to the VGP using the wireless LAN interface with specific maintenance applications used on the nomadic interface implementing this interface via a

specific API. The interface provides a strong authentication scheme in order to prevent unauthorized users from making modifications that may disrupt the vehicle system. The authentication scheme is able to manage some user rights in order to allow the maintenance application to access only some software modules or units inside the vehicle. The software transfer is implemented over a reliable and fast transport layer, preferably with an encryption feature in order to protect code interception by unauthorized people.

– Several interfaces are used to deploy in a safe way the new software package version on the corresponding updatable modules or software units. These can later be located inside or outside the VGP. Device units inside the vehicle are heterogeneous because of the use of different technologies and communication buses. An IP-based interface is provided to update the different VGP modules or services, and also for IP-based in-vehicle devices such as the head unit or passenger infotainment unit. Some specific interfaces are also provided for non-IP based devices such as ECUs, cameras, etc. As some ECUs may integrate some security modules, it is required that the corresponding non-IP interface shall support the specifications of the underlying secure protocols implemented by these modules.

– A database is used for storing the different software package version, encryption keys, signatures and authorizations for the different updatable modules or software unit.

– There is a management sub-module in charge of checking software packages before deployment, handling their installation, configuration and removal, and providing installation traces (journaling). Journal access is restricted to authorized parties, and it is preferably protected by signature and encryption schemes in order to provide reliability and verifiability of the logs.

8.3.2.2 Application data management service

8.3.2.2.1 Description

The application data management service is used by the different VGP components to store some data that shall be kept intact from one software version to another.

The data can be shared between different components and may also be accessed from external devices (such as nomadic devices or remote servers) for monitoring or maintenance purposes. For instance, a management application running over a nomadic device may require access to the version and publication date of the different navigation maps installed over the head unit.

Some metadata is associated with each defined data entry (such as access permissions, data type and size) and allows flexible and secure data sharing between different components.

8.3.2.2.2 Component description

The application data management service is made up of the following components:

– A common, fast, secure, safe and flexible interface for accessing stored data from external devices or servers. This interface may be used either by applications running over external devices such as a nomadic device or cloud servers, and implementing a specific API derived from the interface specification. The interface provides a strong authentication scheme in order to prevent unauthorized users from making modifications that may disrupt the vehicle system. The authentication scheme allows managing some user rights in accordance with the permission rights associated with each data entry. Thanks to this feature, the different applications only have access to some of the shared data, and have limited rights to operate on them. Permissions may include read, modify, delete.

– Several interfaces are available to allow data access from the corresponding updatable modules or software units. These can later be located inside or outside the VGP. Device units inside the vehicle are heterogeneous because of the use of different technologies and communication buses. The application data management service provides different

"internal access interfaces" to allow the in-vehicle devices, services and applications running over the VGP or outside the VGP to operate on data entries. The type of operations over the data entries and the associated metadata are addition, removal, modifications and reading. An IP-based interface provides data access to the different VGP modules or services, and also for IP-based in-vehicle devices such as a head unit or passenger infotainment unit. Some specific interfaces are provided for non-IP based devices such as ECUs.

– There is a robust database used for storing data, data version, encryption key, signatures and authorizations for the different updatable modules or software units. This database is used to store the data used by the different software components in a secure way in order to avoid possible intrusion, software leaks or malicious modifications that may be critical for vehicle security. Some extra metadata is associated with each application data entry such as data version number, modification date, data type, size, owner application, permissions, physical location of stored data when data is not physically stored in the VGP, encryption key when data requests encryption. They shall be also stored in the database.

– There is a journaling sub-module in charge of providing data access traces. Journal access is restricted to only authorized parties and is protected with signature and encryption schemes in order to provide reliability and verifiability of the logs.

8.3.2.2.3 Interaction with software management service

The application data management service interacts with the software management service described in clause 8.3.2.1 by using the software package management sub-module through the IP-based interface, both being provided by the software management service. In particular, it is useful to get the properties of the in-vehicle components, services and applications that request access to application data.

8.3.3 Reference points with other function entities

The reference points between services and other function entities are as follows:

– The reference points between the driver-vehicle access service and service functionalities are:

  1) **Reference point Mdt: r**efer to clause 8.2.3.

  2) **Reference point Cdt: r**efer to clause 8.2.3.

– The reference points between the software and application data management service and service functionalities are:

  1) **Reference point Msat:** refer to clause 8.2.3.

  2) **Reference point Csat:** refer to clause 8.2.3.

– The reference point between services and SAM is:

  1) **Reference point Csv:** This reference point is used to retrieve the driving states from SAM, and SAM can also obtain the vehicle data from VGP.

– The reference point between service functionalities and management is:

  1) **Reference point Cmsf:** This reference point is used to send bidirectional manage messages between service functionalities and security/device management. The control messages should include keys/certifications/ciphers acquisition, encryption schemes acquisition and authentication/authorization for software deployment/update and application data storage/read. The control messages should also be used to retrieve the software running status of services.

8.4 Management

8.4.1 Security management

8.4.1.1 Description of security management

The security entity in the VGP includes access layer security management functions in OSI 1-4 layer and security management for services/applications in OSI 5-7 layer.

8.4.1.2 Access layer security management

The access layer security management covers the transport, networking and network access security.

The access layer security management shall support functions that prevent non-authorized access or intrusion from external networks and devices. One or several firewall functions, e.g., stateful packet inspection filtering, MAC address filtering, IP address filtering, etc. should be used.

The access layer security management shall support identity, crypto key and certificate management, e.g., identity add/delete/modification, crypto key create/update/storage, certificate create/update/storage/destroy, etc. A VGP shall guarantee the security of the process of management to avoid tampering and stealing. The security data is implemented in the process of MAC authentication, EAP-SIM (Extensible Authentication Protocol – Subscriber Identity Module) authentication, EAP-PEAP (Protected EAP) authentication and VPN (e.g., L2TP, GRE, IPSec), etc.

8.4.1.3 Security management for services/applications

The security management for services/applications cover the security functions in the OSI 5-7.

The security management for services/applications shall support the registration, authentication and authorization functions for external applications' access. Security management for services/applications should support registration of service capabilities/user data that an application can use. An application can only use the service capabilities/user data that have been authorized.

There is some private data about user behaviour which belongs to user privacy, such as location data, driving behaviour data, etc. Besides using encryption technology to protect critical data, a VGP should classify the data according to privacy policy which is managed in security management and allow that only authorized applications can use the private data.

The security management for services/applications shall support identity, crypto key, digital signature and certificate management, e.g., add/delete/modify identity; create/update/store crypto key; create/update/store/delete certificate; etc. A VGP shall guarantee the security of the process of management to avoid tampering and stealing. A VGP should support the secure data/criteria exchange that is implemented in the process of session management; application data storage encryption and decryption; application access authentication; and VPN (e.g., TLS/SSLVPN).

8.4.2 Wired and wireless access management

8.4.2.1 Description

The wired and wireless access management entity supports management of multiple wired and wireless access network protocols and can make optimal use of all these resources to support handover between the same communication interface and different communication interfaces.

8.4.2.2 Component description

A VGP should track the status of the dynamically changing mobile network and provide access to the management information base (MIB) containing the configuration and current status information and be notified when the status of the medium changes.

A VGP should provide functions to manage communication sessions according to the methods specified in the relevant wireless network standards. A VGP should also support mechanisms or strategies to establish, manage and disconnect networks based on user profiles. A strategy profile may be configured based on time, location, preferred communication channels (all accesses are transparent to applications), etc. in the hybrid network environment.

The VG is in charge of supporting communication layers 1 to 4 and shall control the above listed functions through the Cmvg reference point.

8.4.3 Device management

8.4.3.1 Description

The device management entity supports the management of hardware/software running and data communication status, hardware/software parameters configuration and fault management, etc.

8.4.3.2 Component description

A VGP should track the hardware/software running status/data communication status and generate records. A VGP should support the records uploaded to the cloud server through external networks and support the records local storage.

A VGP should support configuring the MIB and hardware/software parameters remotely/locally.

A VGP should support hardware/software fault diagnostics and disposal (e.g., restart, recovery).

8.4.4 Reference points with other function entities

– The reference point between the VG and management is:
  1) **Reference point Cmvg**: refer to clause 8.1.4.
– The reference point between service functionalities and management is:
  1) **Reference point Cmsf**: refer to clause 8.2.3.
– The reference point between services and management is:
  1) **Reference point Cms**: refer to clause 8.3.3.

Appendix I

Signalling flows of VGP

(This appendix does not form an integral part of this Recommendation.)

NOTE – The dotted arrows are control messages and the solid arrows are media messages.

I.1 Signalling flows for emergency information display in V2V scenario

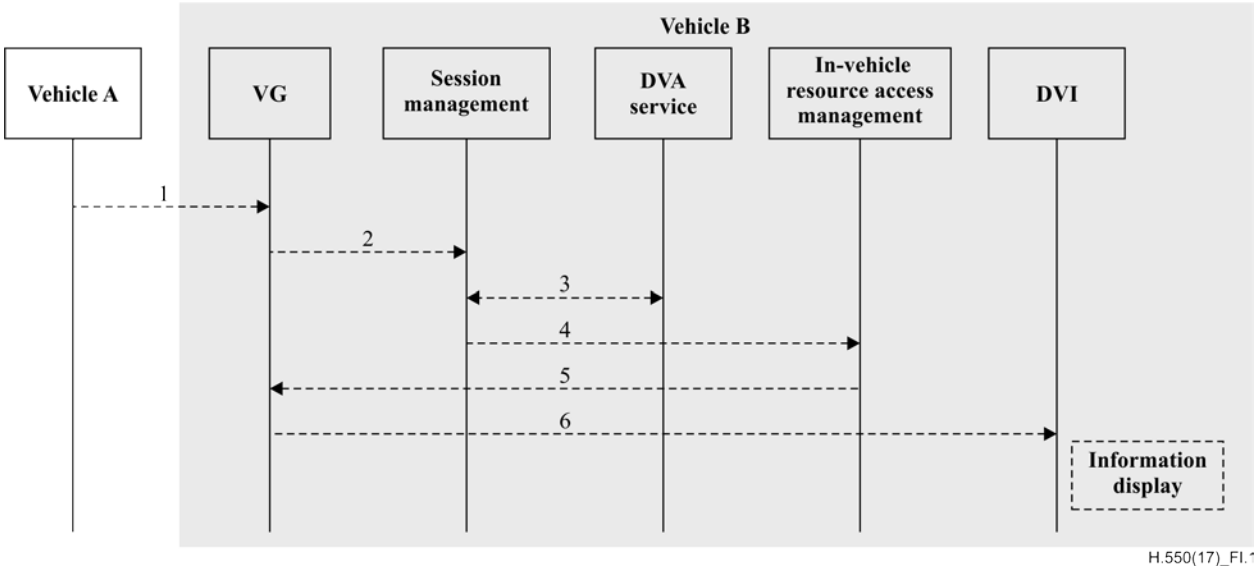

Figure I.1 – Signalling flows for emergency information display in the V2V scenario

1. Vehicle A communicates with vehicle B at an intersection. Vehicle A sends a message to the VG.
2. The VG transfers the message to session management.
3. Session management transfers the message to the DVA service with high priority. The DVA service determines which DVI can be used to display the message according to the working status of each DVI. Then the DVA service changes the message format to adapt the DVI.
4. Session management transfers the message to the in-vehicle resource access management. In-vehicle resource access management determines whether the message can be transferred to the vehicle bus.
5. The in-vehicle resource access management transfers the message to the VG.
6. The VG sends the message to the vehicle bus, and the message can be displayed through the DVI.

I.2 Signalling flows for traffic data download in V2I scenario

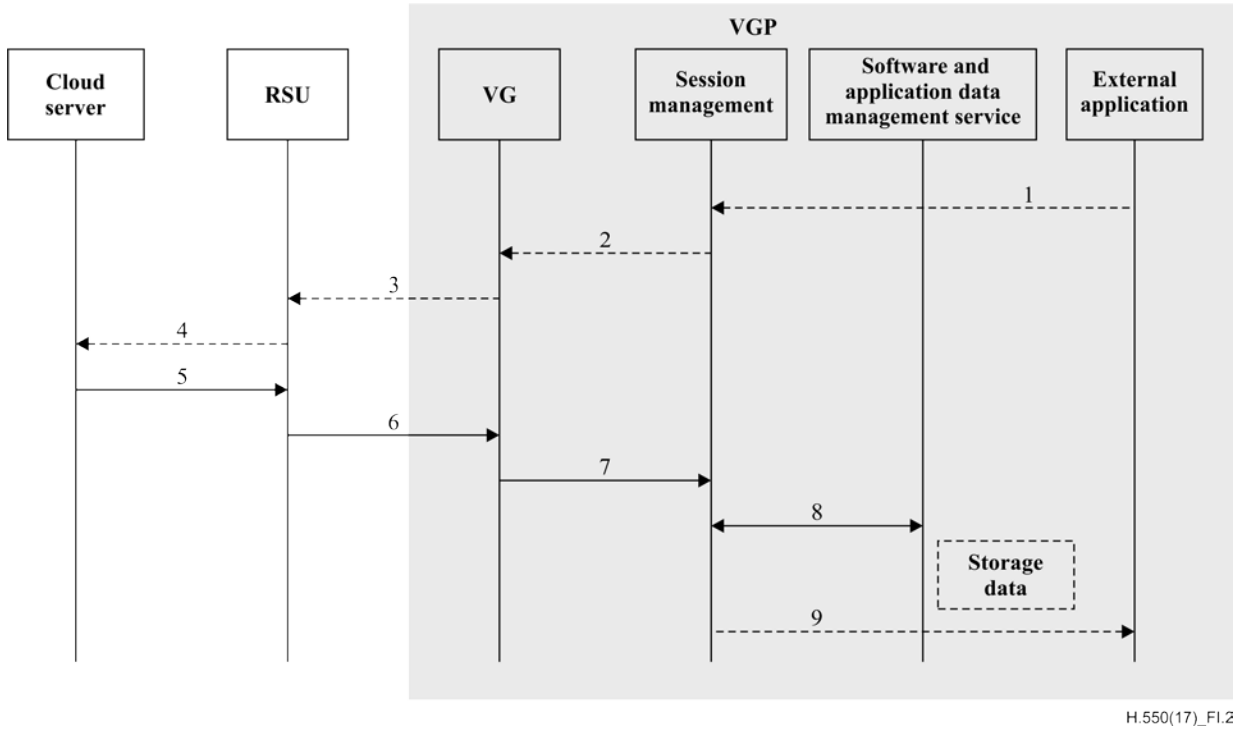

Figure I.2 – Signalling flows for traffic data download in the V2I scenario

1. An external application applies to download the latest traffic data from the cloud server. The external application initializes a request message to session management.
2. Session management transfers the message to the VG.
3. The VG selects the RSU to download the traffic data.
4. The RSU transfers the message to the cloud server.
5. The cloud server sends the traffic data back to the RSU.
6. The RSU transfers the traffic data to the VG.
7. The VG transfers the traffic data to session management.
8. Session management sends the traffic data to the software and application data management service. The software and application data management service unpacks and checks the traffic data, and then stores the data.
9. Session management sends the metadata of the traffic data to the external application.

I.3 Signalling flows of remote UI scenario

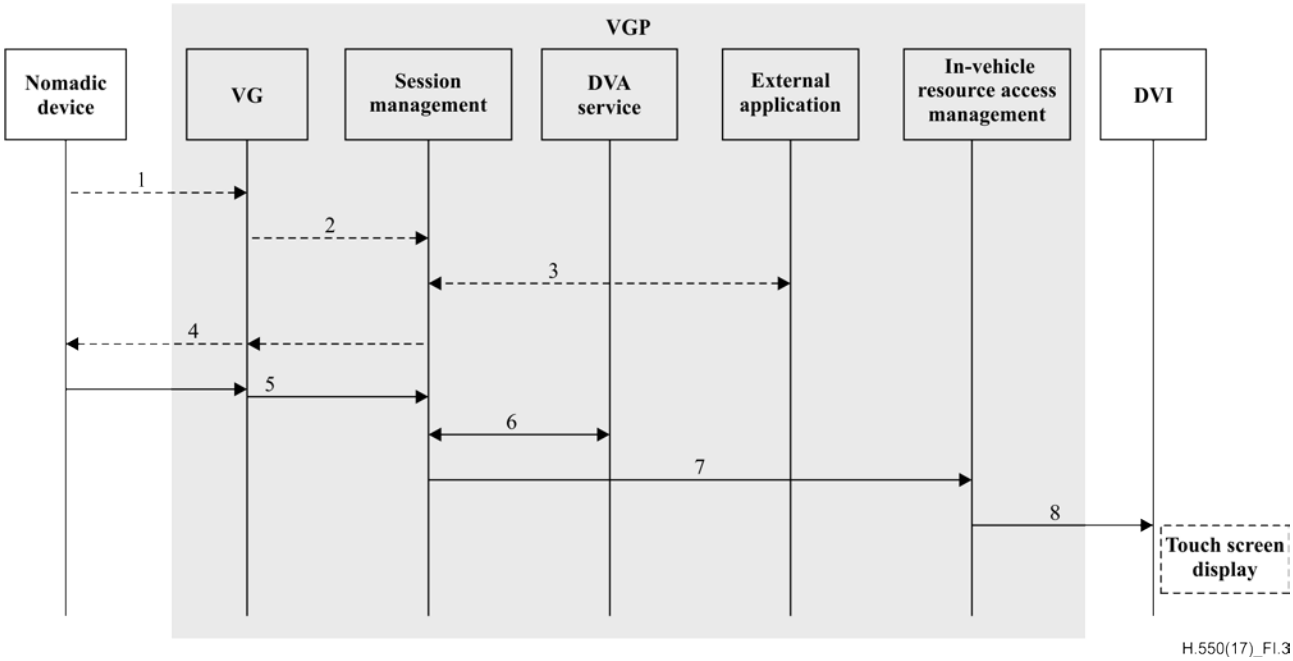

Figure I.3 – Signalling flows of the remote UI scenario

1. A nomadic device sends a request to the remote UI on the screens of the vehicle. The nomadic device connects to the VG and sends the request message.
2. The VG sends the request message to session management.
3. Session management transfers the message to the external application. The external application ensures that the remote UI request is technically feasible. The external application sends the remote UI parameters back to session management.
4. Session management sends the message back to the VG and the nomadic device.
5. The nomadic device sends a media stream to the VG and session management.
6. Session management transfer the media stream to the DVA service. The DVA service determines whether the media stream can be display on the screens according to the driving scene which is obtained from SAM and the running status of the screen. And the DVA service also can change the format and resolution of the media stream.
7. Session management transfers the media stream to in-vehicle resource access management. In-vehicle resource access management determines whether the media stream can be transferred to the vehicle bus.
8. The in-vehicle resource access management transfers the media stream and displays on the screens.

I.4 Signalling flows of emergency call scenario

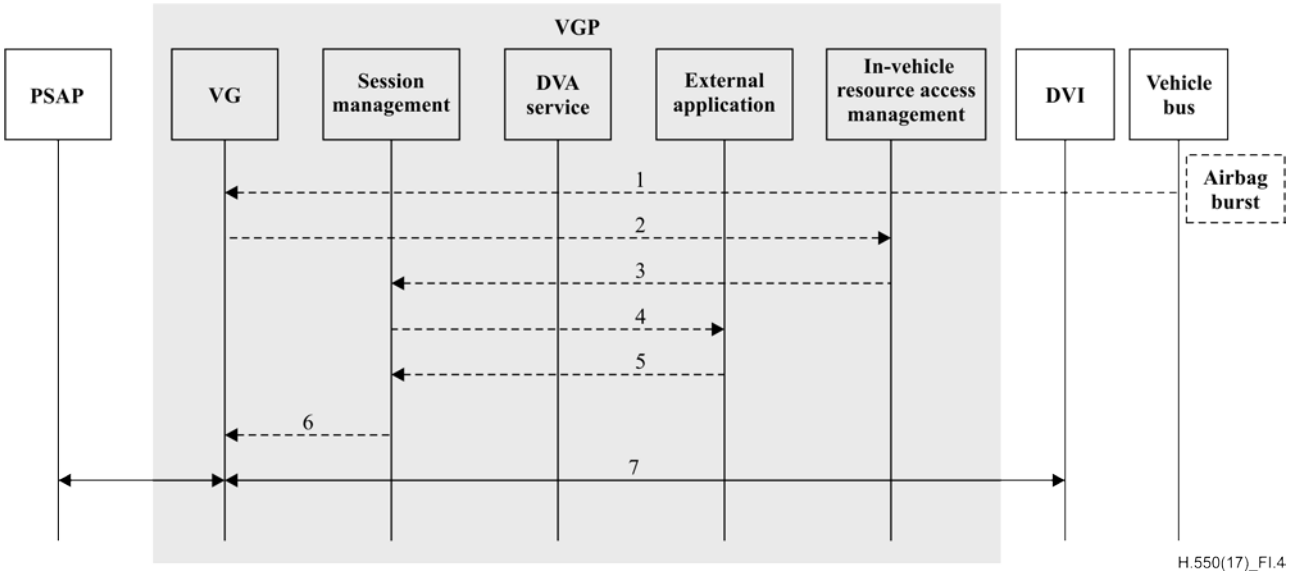

Figure I.4 – Signalling flows of the emergency call scenario

1. When an accident happens the airbag bursts. The vehicle bus sends a message to the VG.
2. The VG transfers the message to the in-vehicle resource access management.
3. The in-vehicle resource access management sends the message to session management.
4. Session management transfers the message to an external application with high priority.
5. The external application obtains the global positioning system (GPS) information and vehicle information, and sends the information to session management.
6. Session management sends the message to the VG.
7. The VG cuts off the existing call and establishes a call to the public service answering point (PSAP) with GPS/vehicle information.

I.5 Signalling flows of anti-stolen scenario

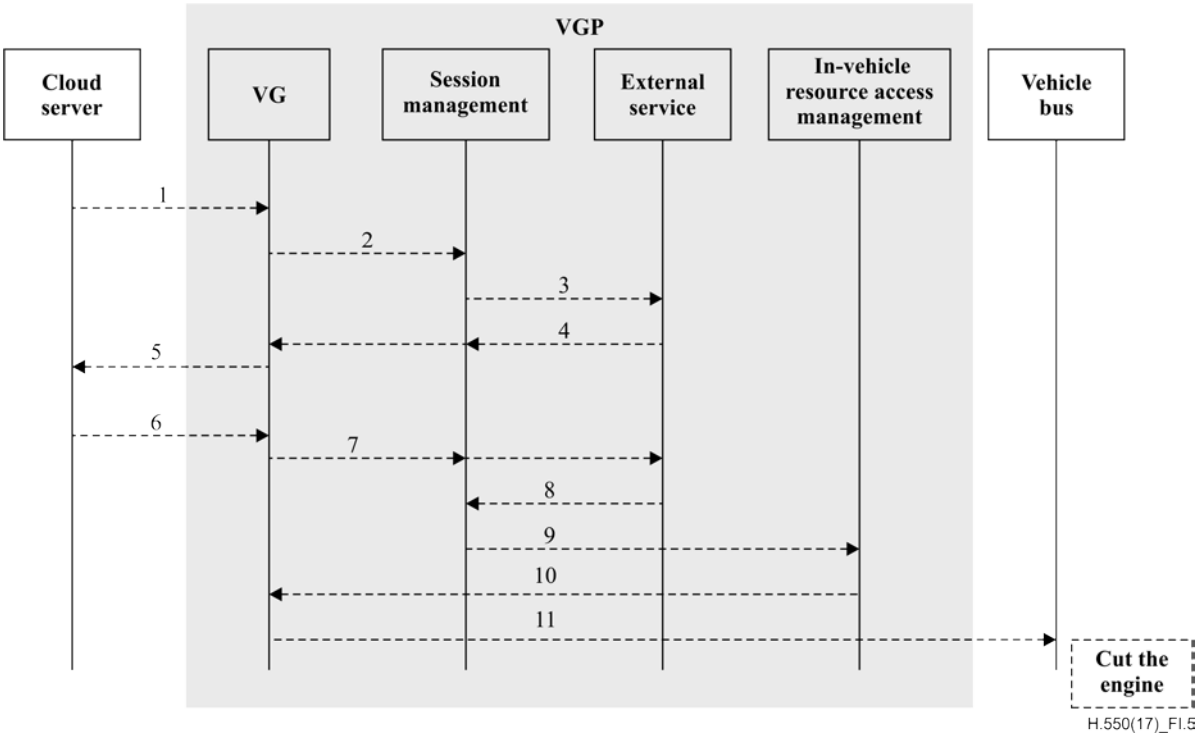

Figure I.5 – Signalling flows of the anti-stolen scenario

1. After the vehicle has been stolen, the driver owner calls the telematics server and asks for tracking. The cloud server sends the request message to the VG.
2. The VG transfers the message to session management.
3. Session management transfers the message to an external service. The external service obtains the GPS information of the vehicle.
4. The external service sends the response message to session management and the VG.
5. The VG transfers the message to the cloud server.
6. When the speed of the vehicle turns to 0 km/h, the cloud server sends a message to cut the engine.
7. The VG sends the message to session management and the external service.
8. The external service transfers the message to session management.
9. Session management transfers the message to the in-vehicle resource access management.
10. The in-vehicle resource access management transfers the message to the VG.
11. The VG transfers the message to the vehicle bus and the vehicle cuts the engine.

I.6 Signalling flows of remote software update scenario

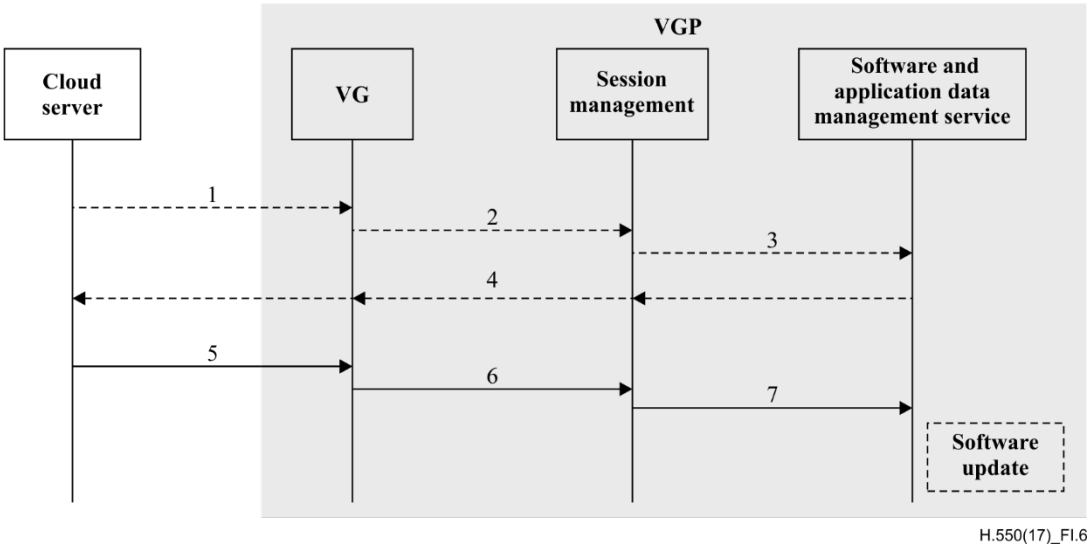

Figure I.6 – Signalling flows of the remote software update scenario

1. After a new software version is published, the cloud server sends a software update request message to the VG.
2. The VG transfers the message to session management.
3. Session management transfers the message to the software and application data management service. The software and application data management service checks the software version and authenticates the server.
4. The software and application data management service sends the response message to the cloud server.
5. The cloud server sends the software data to the VG.
6. The VG transfers the software data to session management.
7. The session management sends the software data to the software and application data management service. The software and application data management service checks/decrypts the data and deploys the new version software in the VGP or sends the data to the vehicle bus through the in-vehicle resource access management.

I.7 Signalling flows of navigation scenario

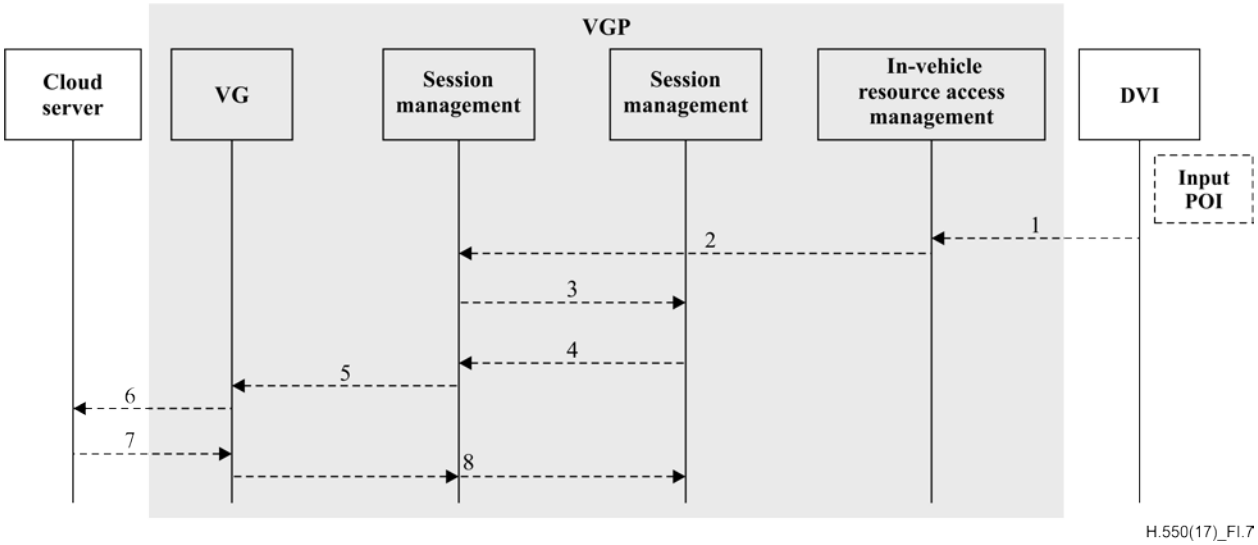

Figure I.7 – Signalling flows of the navigation scenario

1. The driver inputs the point of interest (POI) through the DVI. The DVI sends the POI to the in-vehicle resource access management through the VG.
2. The in-vehicle resource access management transfers the POI to session management.
3. Session management transfers the POI to an external service. If the external service cannot find the POI information in the local database, it should search the POI from the cloud server.
4. The external service sends the request message to session management.
5. Session management sends the message to the VG.
6. The VG sends the message to the cloud server. The cloud server searches the POI in the remote database.
7. The cloud server sends the POI to the VG.
8. The VG sends the message to session management/external service.

Bibliography

[b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

[b-ITU-R handbook] ITU-R Handbook (2006), Land Mobile (including wireless access) – Volume 4: *Intelligent Transport Systems*.

[b-IEEE 802.11] IEEE 802.11-2016, *IEEE Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.
<https://standards.ieee.org/findstds/standard/802.11-2016.html>

[b-ISO/IEC 7498-1] ISO/IEC 7498-1 (1994), *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model.*

[b-ISO 11898-1] ISO 11898-1:2015, *Road vehicles – Controller area network (CAN) – Part 1: Data link layer and physical signalling*.
https://www.iso.org/standard/63648.html

[b-ISO 15638-16] ISO 15638-16:2014, *Intelligent transport systems – Framework for cooperative telematics applications for regulated vehicles (TARV) – Part 16: Vehicle speed monitoring.*

[b-ISO 17458-1] ISO 17458-1:2013, *Road vehicles – FlexRay communications system – Part 1: General information and use case definition.*
<https://www.iso.org/standard/59804.html>

[b-ISO 21210] ISO 21210:2012, *Intelligent Transport Systems (ITS) – Communications access for land mobiles (CALM) – IPv6 Networking.*

[b-ISO 21212] ISO 21212:2008, *Intelligent Transport Systems (ITS) – Communications access for land mobiles (CALM) – 2G Cellular systems.*

[b-ISO 21213] ISO 21213:2008, *Intelligent Transport Systems (ITS) – Communications access for land mobiles (CALM) – 3G Cellular systems.*

[b-ISO 21214] ISO 21214:2006, *Intelligent Transport Systems (ITS) – Communications access for land mobiles (CALM) – Infra- red systems.*

[b-ISO 21216] ISO 21216: 2012, *Intelligent Transport Systems (ITS) – Communication access for land mobiles (CALM) – Millimetre wave air interface*
<https://www.iso.org/standard/59703.htm>

[b-ISO 24102-1] ISO 24102-1:2013, *Intelligent transport systems (ITS) – Communications access for land mobiles (CALM) – ITS station management – Part 1: Local management.*
<https://www.iso.org/standard/61561.html>

[b-ISO 29281] ISO 29281:2011, *Intelligent Transport Systems (ITS) – Communications access for land mobiles (CALM) – Non-IP networking.*

[b-MOST] MOST (2010), *Media Oriented Systems Transport*.
https://www.mostcooperation.com/publications/specifications-organizational-procedures/

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	**Audiovisual and multimedia systems**
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2018