International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.560

(12/2017)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Vehicular gateways and intelligent transportation systems (ITS) – Vehicular gateway interfaces

Communications interface between external applications and a vehicle gateway platform

Recommendation ITU-T H.560

International Telecommunication Union

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.560

Communications interface between external applications and a vehicle gateway platform

Summary

Recommendation ITU-T H.560 specifies functional requirements for vehicle gateway platform (VGP) services, services functionalities and management, including vehicle gateway platform, application and communication network requirements. In particular, it defines the requirements for services running over the vehicle gateway platform and the communication interfaces between those services and some applications running over external devices such as cloud servers, nomadic devices or other in-vehicle devices.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.560	2017-12-14	16	11.1002/1000/13435

Keywords

Communications interface requirements; external applications; Intelligent transportation systems; ITS; service requirements; telematics; vehicle gateway platform; 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

Introduction

The primary goal of the vehicle gateway platform (VGP) is to provide an integrated runtime environment for delivering the communications services of a vehicle gateway. The VGP also provides higher layer communications services in order to support intelligent transportation systems (ITS) and infotainment applications and services for the driver and passengers. Therefore, the VGP provides and controls the access to the driver-vehicle interface (DVI) devices such as displays, speakers and buttons installed inside the car.

In particular, the communication services allow external applications to enhance the user interface of the vehicle. Communication services will also enable the VGP to control the timing and format of all application outputs transmitted to the driver via the DVI, even for applications that are not integrated at the time of vehicle manufacturing. They shall also provide enough capabilities and flexibility to support any kind of application while respecting safety constraints specific to the vehicle environment.

Indeed, there are some safety concerns with drivers interacting with information and communications technology (ICT) applications "brought in" to the vehicle on a nomadic device or "beamed in" via network connectivity. Firstly, interactions with these applications are often performed through a nomadic device's user interface instead of the vehicle's user interface. Nomadic device user interfaces are usually not adapted for in-vehicle usage because of their small size, manual interface and unsecured/uncontrolled/arbitrary position within the vehicle. On the other hand, vehicle user interfaces are usually optimized for safe interaction with drivers by careful placement and design of the user interface.

Secondly, interaction with these devices/applications typically operates independently of the driving situation and other applications the driver may be interacting with. This can result in driver distraction that is not compatible with safe driving. For instance, a social media status update message from an unpaired nomadic device may interfere with a collision avoidance warning.

Consequently, an important aim of this Recommendation is to define services requirements that will address all of these safety concerns, based on a standardized communications interface between the vehicle and all external applications – regardless of where they are physically located. Such an interface will enable drivers to safely interact with external ICT applications through the vehicle's user interface and also allow all interaction with the driver to be managed by a centralized point of control.

Recommendation ITU-T H.560

Communications interface between external applications and a vehicle gateway platform

1 Scope

This Recommendation defines the requirements for vehicle gateway platform (VGP) services, VGP service functionalities and VGP management. The VGP service functions support service capabilities for applications running and data/message processing. The VGP service functionalities support core capabilities used by VGP services such as session management or in-vehicle resource access management. Finally, the VGP management supports functions for VGP configuration and monitoring such as security management.

This Recommendation also defines the network requirements for communication interfaces used between the defined VGP services and external applications. These external applications could be running over nomadic devices brought into the vehicle, roadside infrastructure, or cloud-based servers. Applications downloaded to one of the in-vehicle devices after the time of manufacture are also considered external applications since they may not be fully integrated into the driver-vehicle interface (DVI) and require a communications interface. Advanced driver assistance systems (ADAS) are considered as out of scope of this Recommendation.

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 H.550] Recommendation ITU-T H.550 (2017), *Architecture and functional entities of vehicle gateway platforms*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 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.

3.1.2 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.

3.1.3 nomadic devices [ITU-T F.749.1]: Nomadic devices include all types of information and communication devices 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.

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

3.1.5 quality of service (QoS) [b-ITU-T E.800]: Totality of characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 advanced driver assistance systems (ADAS): Vehicle systems that have a primary function of helping the driver safely control the vehicle. Examples of such systems include lane departure warning systems and adaptive cruise control (ACC).

3.2.2 external applications/services: Applications/services that were not integrated into the vehicle at the time of manufacture. Such applications/services include those that reside on a nomadic device brought into the vehicle, on the roadside infrastructure, or on a cloud-based server. Applications/services that do reside on the vehicle platform, but that were not integrated at the time of manufacture (e.g., downloaded applications), are also considered "external applications/services" as they might not be fully integrated into the DVI.

3.2.3 service functionalities: The service functionalities entities provide a set of basic control functions such as session management and in-vehicle resource access management that are used by other services.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3G	Third Generation of cellular phone technologies
ACC	Adaptive Cruise Control
ADAS	Advanced Driver Assistance Systems
API	Application Programming Interface
CAN	Controller Area Network
DVA	Driver Vehicle Access
DVI	Driver Vehicle Interface
ECU	Electronic Control Unit
GRE	Generic Route Encapsulation
ICT	Information and Communications Technology
IP	Internet Protocol
IPsec	Internet Protocol Security

ITS	Intelligent Transportation Systems
L2TP	Layer 2 Tunnelling Protocol
LDM	Local Dynamic Map
LTE	Long Term Evolution
MIB	Management Information Base
OID	Object Identifier
PPTP	Point-to-Point Tunnelling Protocol
QoS	Quality of Service
RSU	Roadside Unit
SAM	Situational Awareness Management
SMSA	Security Management for Services and Applications
SSL	Secure Sockets Layer
TLS	Transport Layer Security
USB	Universal Serial Bus
VG	Vehicle Gateway
VGP	Vehicle Gateway Platform
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

5 Conventions

None.

6 System description

The VGP framework includes several components such as access networks and devices (known as vehicle gateways or VGs), services, service functionalities and management. Figure 2 in [ITU-T H.550] illustrates the high level architecture of the VGP and presents the VGP services and management within the overall VGP framework. This figure is used as a basis for many of the figures included in this Recommendation.

This Recommendation focuses on VGP services and management.

6.1 Overview of VGP services

6.1.1 VGP services

6.1.1.1 Driver-vehicle access service

This clause introduces the supported services that have interaction with DVI. These services are part of driver vehicle access (DVA) service. DVA service has components for managing input devices, providing an I/O interface for the application to control input and to access the on-board display. The main components and roles related to DVA are as follows:

– Display management service
  - Announcing the list of on-board displays
  - Providing schemes to share access to each display

    - Providing functionality to adapt the displayed content to the targeted display device in the vehicle
    - Selecting an appropriate way to present the application (infotainments and navigation, etc.)
- Input device management service
    - Input device selection
    - Sending input command
    - Command mapping
- Notification message service
    - Providing to external applications a common interface to present message / notification
    - Selecting an appropriate way to present the notification
    - Providing schemes to present the higher priority notification message first and delay the display of lower priority message or applications
- Driver-vehicle (I/O) interface management service
    - Control and access to the in-vehicle DVI devices (e.g., touch panel, push buttons, control knob, microphone and display screen, etc.)
    - Encoding and decoding of the DVI related data

6.1.1.2 Software and application data management services

This clause introduces the VGP services that are useful to manage software and application data for internal services and in-vehicle devices such as electronic control units (ECUs) and sensors. Main components and roles of related services are:

- Software management service used for the deployment and maintenance of software package versions on some updatable modules or software units.
- Application data management service used for the management of the specific data and the associated metadata used by updatable modules or software units.

6.1.2 Service functionalities

6.1.2.1 Session management

The role of the session management service comprises:

- Establishing/terminating a session such as for example a virtual private network (VPN) session
- Encapsulating/extraction data including encryption/decryption
- Authentication checking of devices and applications
- Data filtering, attack detection and alarm generation (e.g., firewall functions)

6.1.2.2 In-vehicle resource access management

In-vehicle resource access management service has a two-way directional data transport process between external applications and in-vehicle ECUs and sensors. First, the service provides an interface to access the in-vehicle buses to read data from ECUs and sensors. Second, the service provides an interface to receive data from external applications and send them to the in-vehicle buses. The main roles related to this service are the following:

- Checking and filtering access to on-board resources
- Providing access to the in-vehicle communication buses to other sub-modules

6.1.3 VGP management

VGP management includes three different management functions as detailed in clauses 6.1.3.1 to 6.1.3.3.

6.1.3.1 Device management

The device management function is in charge of:

– collecting and organizing information about the VGP itself for configuration and monitoring purposes.

– providing access to this information to the VGP services, external applications running over nomadic devices and services running over remote servers for configuration, monitoring and maintenance purposes.

6.1.3.2 Security management

The security management function is in charge of:

– managing application certification and authentication

– applying registration and authentication to external devices (e.g., nomadic devices)

– the networking and transport security management

6.1.3.3 Wired and wireless access management

The wired and wireless access management function is in charge of:

– the management of multiple wired and wireless access network protocols

– the management of the communication sessions (e.g., L2TP, GRE, PPTP)

Support of these functions must be provided by the VG and the corresponding requirements are described in [ITU-T F.749.1].

6.2 Overall communication interface description

The session management service provides some core communication functions such as application, device and server authentication and secure connection establishment. These functions are used by external applications (running over the nomadic devices brought into the vehicle, the roadside infrastructure or some cloud-based servers) to communicate with the supported VGP services. The session management service also provides some protection functions such as firewall with data filtering and attack detection. In addition, the session management service provides access for all VGP services and external applications to the situational awareness management (SAM) thanks to a dedicated interface.

NOTE – SAM is considered as out-of-scope of the VGP.

The access to the in-vehicle resources and information is controlled and provided by the in-vehicle resource access management service. The DVA set of services provide functions to access the driver vehicle interface from the external applications. Finally, the software and application management services, as well as future supported services can also communicate with other services in order to provide some more advanced functions for external applications.

Security control functions such as key management or firewall configuration are implemented inside a security management for services and applications sub-module. It is located inside a more global security management module that is also in charge of the security control of the VG access layers.

6.2.1 Communication provisioning and connection activation

Figure 1 shows an example of service flow for establishment of the connection between the VGP and an external application to start application communication.

1) Basic connection establishment

This connection establishment is needed if the external applications are running on nomadic devices brought into the vehicle, roadside infrastructure, or cloud-based servers (nomadic devices can be referred to as external equipment). A link-layer connection such as a wireless local area network (WLAN) or universal serial bus (USB) communication device class connection is established between the VGP and the external equipment. Both VGP and external equipment can be the initiator of the connection.

2) Application authentication and secure connection establishment

VGP authenticates the external application which is running on the external equipment or the VGP. Both VGP and the external application can be the initiator. In the case where the VGP is initiator, the driver should select the external application via DVI. The application authentication is operated by the "Secure management service". VGP establishes secure connection between the VGP and nomadic devices or servers. For the secure authentication, a secure connection shall be established before the application authentication phase. Secure connection is established when the application uses important data. The secure connection establishment is operated by the "Secure management service".

3 Send/Receive DVI information

External applications communicate with DVI devices such as input devices, displays and/or speakers through the VGP. The external application selects the DVI for input and output. Send/Receive DVI information is operated by "Input device management service".

4 Display/Notification

VGP receives information for displaying and notification from the external application. Display/Notification is operated by the "Display management service" and the "Notification message service".

5 Input

When the driver inputs commands through DVI, VGP sends input commands to the external application. Input control is operated by the "Input device management service".

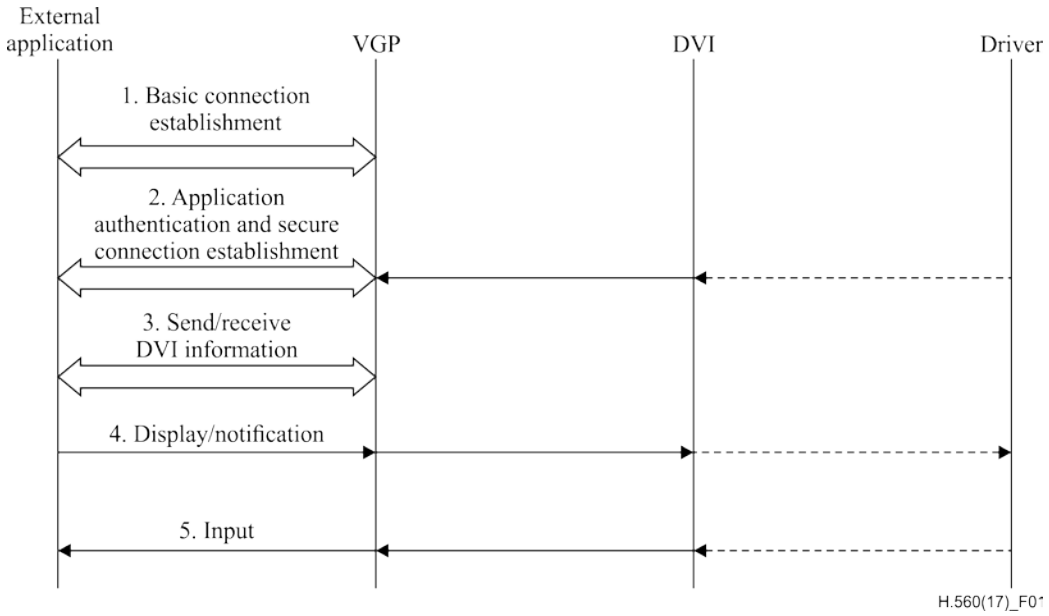

Figure 1 – Service flow

6.2.2 Connection termination

A connection will be terminated when the driver terminates the external application, or the external application terminates itself. In another case, if there is no data transmission and a timeout occurs, the connection with the external application is closed by the VGP.

7 Service requirements

VGP services include services required to connect external devices such as smartphones, tablets, remote servers and roadside units (RSUs) to the VGP and some in-vehicle devices. These services include driver-vehicle access service, in-vehicle resource access management service, software and application data management service and other services within the scope of this Recommendation.

7.1 Driver-vehicle access (DVA) service

DVA service enables the communication between applications running over external devices and on-board equipment that are part of driver-vehicle interface.

7.1.1 VGP requirements

7.1.1.1 Display management service

A display management IP-based service is required to fulfil the following requirements:

– Provide an interface to external applications and internal VGP services to:
  - Announce the list of on-board displays, their features and current status
  - Render application graphical interface on a selected on-board display via the driver-vehicle (I/O) interface management
– Provide support for different IP based protocols for remote application display in order to support a large variety of nomadic devices
– Provide one or more schemes to share access to each display according to the type of applications or devices and the level of priority of displayed information; schemes shall be part of the list of features announced via the common interface
– Provide an access control scheme so that an application or a service has a full or restricted access to some displays for which it has been authorized.

Figure 2 presents some examples of scenarios of applications running over a nomadic or a cloud server respectively connected via USB or through WLAN or 3G/LTE access to the vehicle. They access the display management service through session management for establishing secure session connection and authenticating these applications via the IP or non-IP based functions provided by the VG. After adapting the displayed content to the targeted display and selecting an appropriate way to present the application, applications such as navigation and infotainments from smartphones are sent to driver-vehicle interface management and then forwarded to display devices through the DVI. Alternatively, an internal service such as local dynamic map (LDM) management running over the VGP is also able to access the display management service in the same way. The display management service accesses the physical displays through the driver-vehicle (I/O) interface management as is illustrated by the display management service flow in Figure 2 (dotted line arrow).

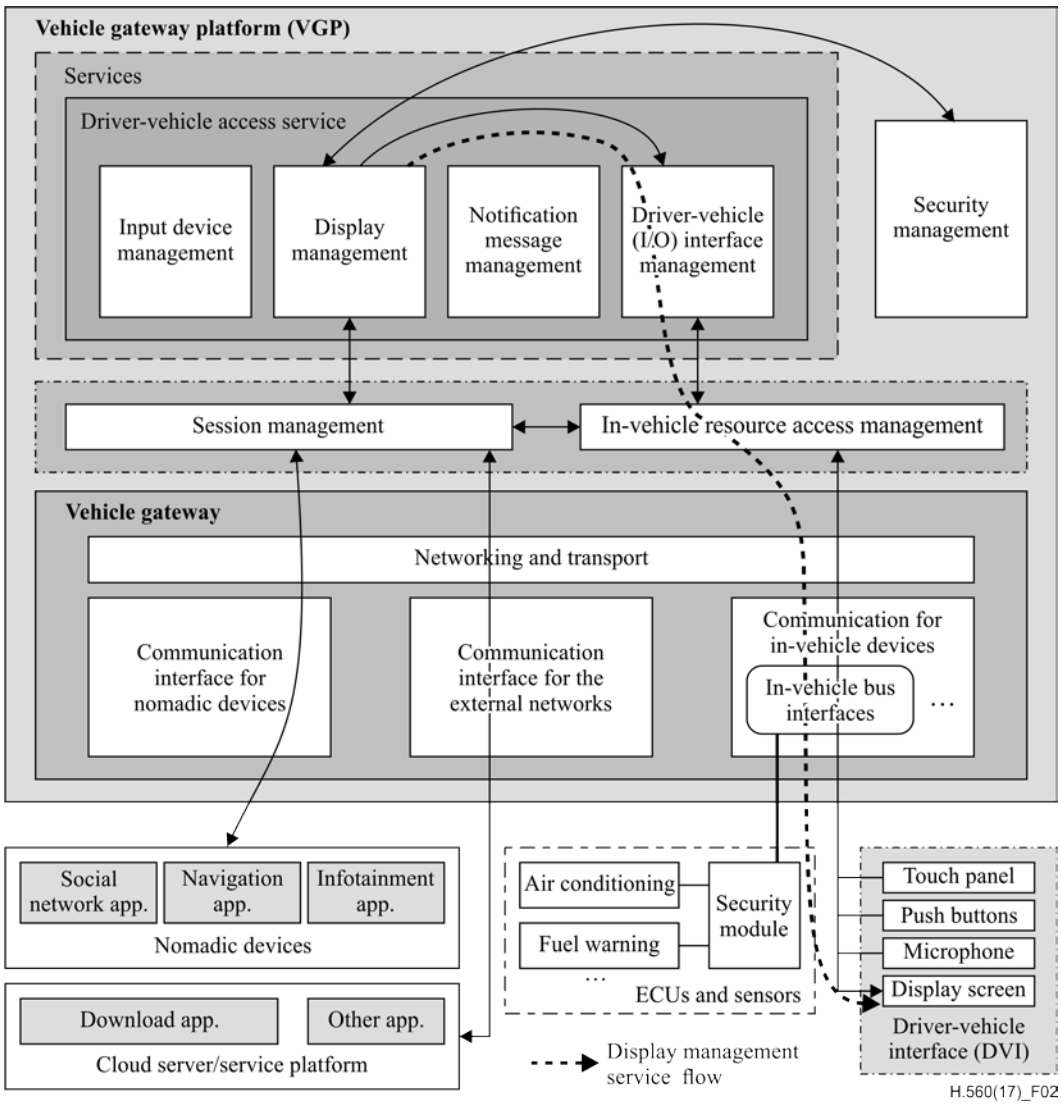

Figure 2 – VGP integration of the display management service

7.1.1.2 Input device management service

An input device management service is required to fulfil the following requirements:

– Provide a common interface to external applications/services to:
  - Announce the list of available control commands and input devices
  - Manage application registration to send some common control commands
– Map on-board input devices to common control commands
– Provide a function for sending input commands to previously registered external applications/devices.

Figure 3 presents some scenarios of applications/services running over a nomadic device, a remote server or the VGP that receive input commands from several on-board input devices. As shown in Figure 3, the "Command transmission" sub-module is in charge of sending translated common control commands to appropriate applications/services. The "External device registration" sub-module is in charge of providing a list of available control commands and managing external devices and it interacts with 'Security management' to realize registration and authentication of external devices. The "Command mapping" sub-module is in charge of translating input commands to common control commands before the input device sends commands to applications/services. The "Input device selection" sub-module is in charge of selecting input devices (e.g., touch panel,

push buttons, control knob, microphone and display screen) for applications/services via the driver-vehicle interface management.

In Figure 3, the dotted line arrows illustrate the input device management service flows for a simple example where an on-board push button is used as an input control for a navigation application running over a consumer nomadic device.

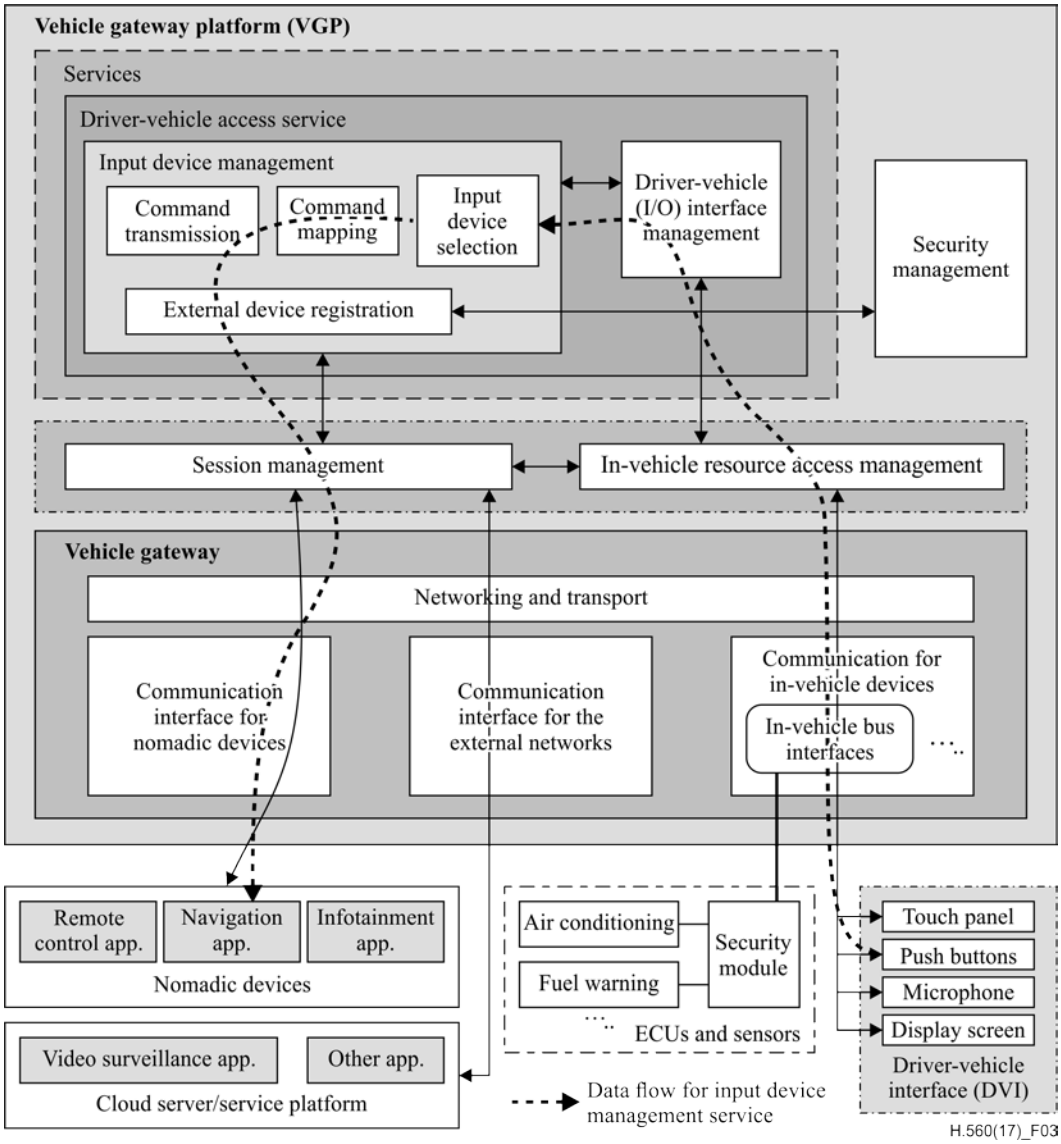

Figure 3 – VGP integration of the input device management service

7.1.1.3 Notification message management service

A notification message management service is required to fulfil the following requirements:

– Provide to external applications a common interface to present notification messages via the DVI (display screen, sounds, etc.)

– Arbitrate and/or integrate notifications to limit driver distraction, based on an importance level set by the applications; the VGP is authorized to modify the importance level in order to limit driver distraction

– Select an appropriate way to present the notification messages depending on the source and importance level; a time-to-live value is used to calculate the end of the notification presentation

– Provide to external applications a common interface to subscribe to the notification messages.

In order to support events issued from devices connected through different network interfaces, a notification message adaptation sub-module may be required to convert events received from the devices through the VG into the proper format supported by the notification message management sub-module as shown in Figure 4. In Figure 4, the dotted line arrow illustrates an example of usage of the notification message management service. The dotted line arrow represents the notification message data flow that is generated by a social network application running over a nomadic device. The message is sent to the notification message manager through one of the communication interfaces for nomadic devices and the session management service functionality. Then, the notification message manager dispatches the notification to one DVI device (display screen in the example) taking into account the driver distraction.

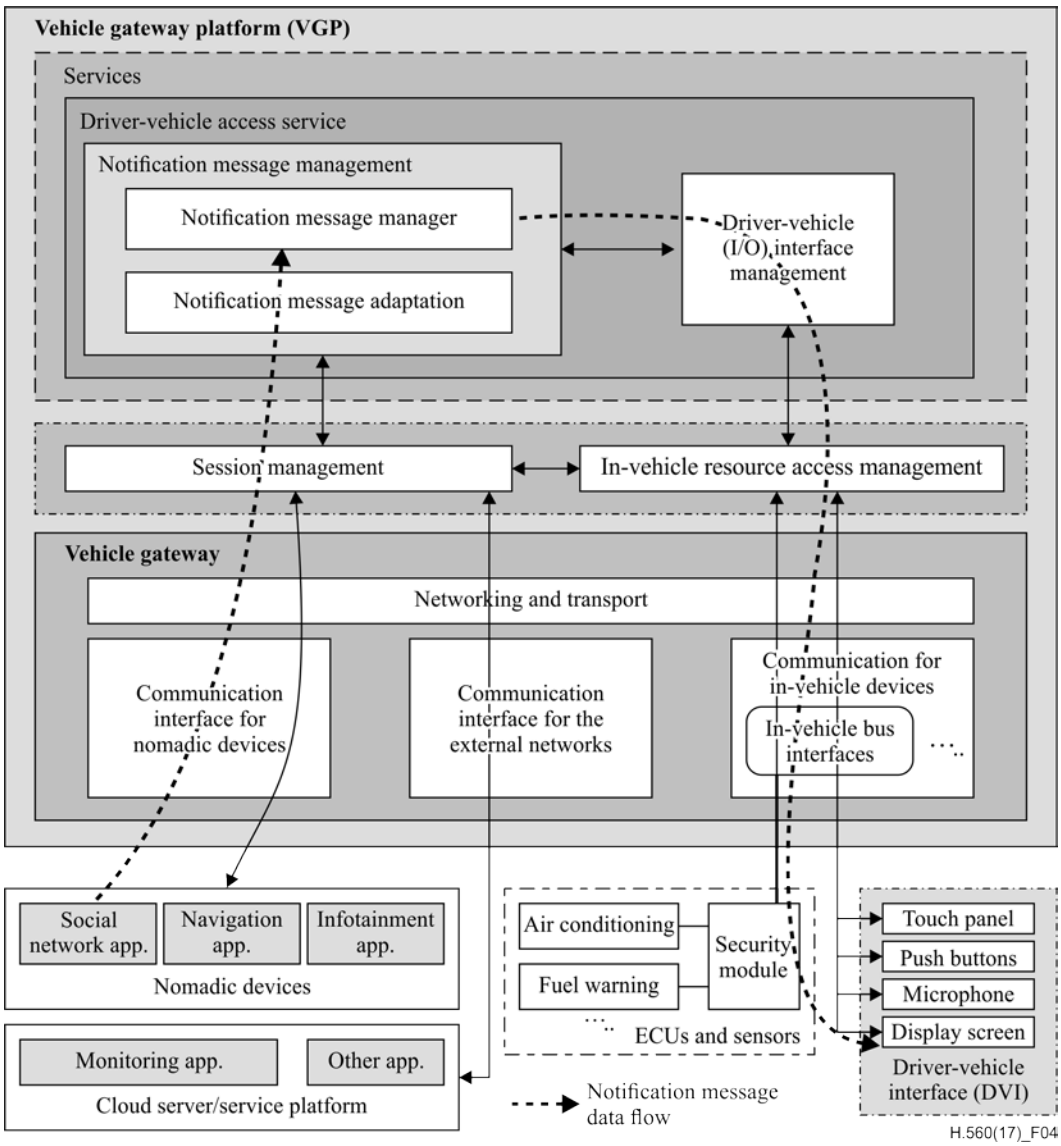

Figure 4 – VGP integration of the notification message management service

7.1.1.4 Driver-vehicle (I/O) interface management service

The driver-vehicle (I/O) interface management provides an interface to other DVA services (display, input device, notification message management) to access the DVI devices. This functional entity must communicate with the DVI devices through the in-vehicle resource access management service functionality.

The role of the driver-vehicle (I/O) interface management is then to provide some uniform control and media interfaces to configure and access the different in-vehicle DVI devices such as display screens, speakers, microphones, touch panel, push buttons and control knobs.

The control interface shall provide an application programming interface (API) to configure and monitor the DVI devices in a uniform way.

The media interface shall provide an adaptation function of input/output data flow. It shall include media encoding and decoding functions to adapt to the specific format accepted by each different DVI device.

7.1.2 Application requirements

7.1.2.1 Display management service

The application must adapt the internal application data to the external interface format defined by the display management service. An application shall also embed a certificate that is sent to the VGP via the external interface during an initial authentication step. The certificate shall contain the requested rights and priority attached to the application. After verification of the certificate validity, the VGP can apply the requested rights and priority to the information that is displayed/announced by the application through the DVI devices.

7.1.2.2 Input device management service

The applications/services shall translate received common control commands into its internal command types. In addition, it should register control commands on the service to receive specified control commands from the VGP.

7.1.2.3 Notification message management service

The application must adapt the internal application events to the notification message format defined by the notification message interface. The application shall set an appropriate importance level as well as a time-to-live value that are attached to the notification message sent to the VGP.

7.1.3 Communication network requirements

7.1.3.1 Display management service

The external interface defined by the display management service must be implemented over a network transport layer offering a reliable data delivery.

The external interface defined by the display management service may be preferably implemented over a network transport layer offering an encrypted and authenticated data link.

Depending on the on-board resource targeted by the external interface function, the set of quality of service (QoS) parameters used for the transport layer may be selected accordingly.

7.1.3.2 Input device management service

The external interface defined by the input device management service in clause 7.1.1.2 must be implemented over a network transport layer offering a reliable data delivery.

The external interface defined by the input device management service should be implemented over a network transport layer offering an encrypted and an authenticated data link.

Depending on the on-board control commands targeted by the external interface function, the set of QoS parameters used for the transport layer should be selected accordingly.

7.1.3.3 Notification message management

The notification message interface must be implemented over a network transport layer offering a reliable data delivery.

The notification message interface may preferably be implemented over a network transport layer offering an encrypted and authenticated data link.

According to the network transport protocol used to convey notification messages, an importance level may be used to optimize the set of QoS parameters used for the transport layer.

7.3 Software and application data management service

Software may be running in VGP and in-vehicle on for example ECUs and sensors.

7.3.1 VGP requirements

7.3.1.1 Software management service

A software management service is required to fulfil the following requirements:

– Provide a common, fast, secure and flexible interface for software package upload from external devices or servers.

– Provide several interfaces to deploy in a safe way the new software package version on the corresponding updatable modules or software units which can be located inside (e.g., VGP services) or outside the VGP (e.g., ECUs). In particular, these interfaces shall support the specifications implemented in the ECUs for secure update such as the specification defined by [b-TCG TPM2.0].

– Provide a database used for storing in a secure way the different software package versions intended for the different updatable modules or software units.

– Provide a management sub-module in charge of checking the software packages before the deployment, handling their installation, configuration and removal and providing installation traces (journaling). The journal access shall be restricted to only authorized parties and it must be protected with signature and encryption schemes in order to provide reliability and verifiability of the logs.

Integration of the software management service into the VGP is shown in Figure 5. Figure 5 presents some scenarios of ECU and VGP component software updates from either a nomadic device or a remote server. The "External interface" sub-module is in charge of providing several interfaces for external applications and devices uploading software and middleware which are sent to the "Software package management". The "In-vehicle resource interface" sub-module is in charge of providing several interfaces for in-vehicle resource and devices uploading software and middleware which are sent to the "Software package management". The "Software package database" sub-module is in charge of storing the uploaded software and installing or updating software in the VGP and in-vehicle such as on ECUs and sensors. The "Software package management" interacts with "Security management" to realize secure download,certification and authentication and ensures the security of their deployment, handling their installation, configuration and removal.

The dotted line arrows in Figure 5 illustrate a usage example of the software management service. In this example, a maintenance service running over a cloud server makes a software update of the ECU in charge of controlling the on-board air conditioning. The maintenance service communicates with the software management service thanks to a virtual private network (VPN) link established through a communication interface for external networks (for instance LTE) and the session management service functionality. The software update procedure is then triggered by the software package management sub-modules through the in-vehicle resource management service functionality and one of the in-vehicle bus interfaces such as controller area network (CAN) for instance.

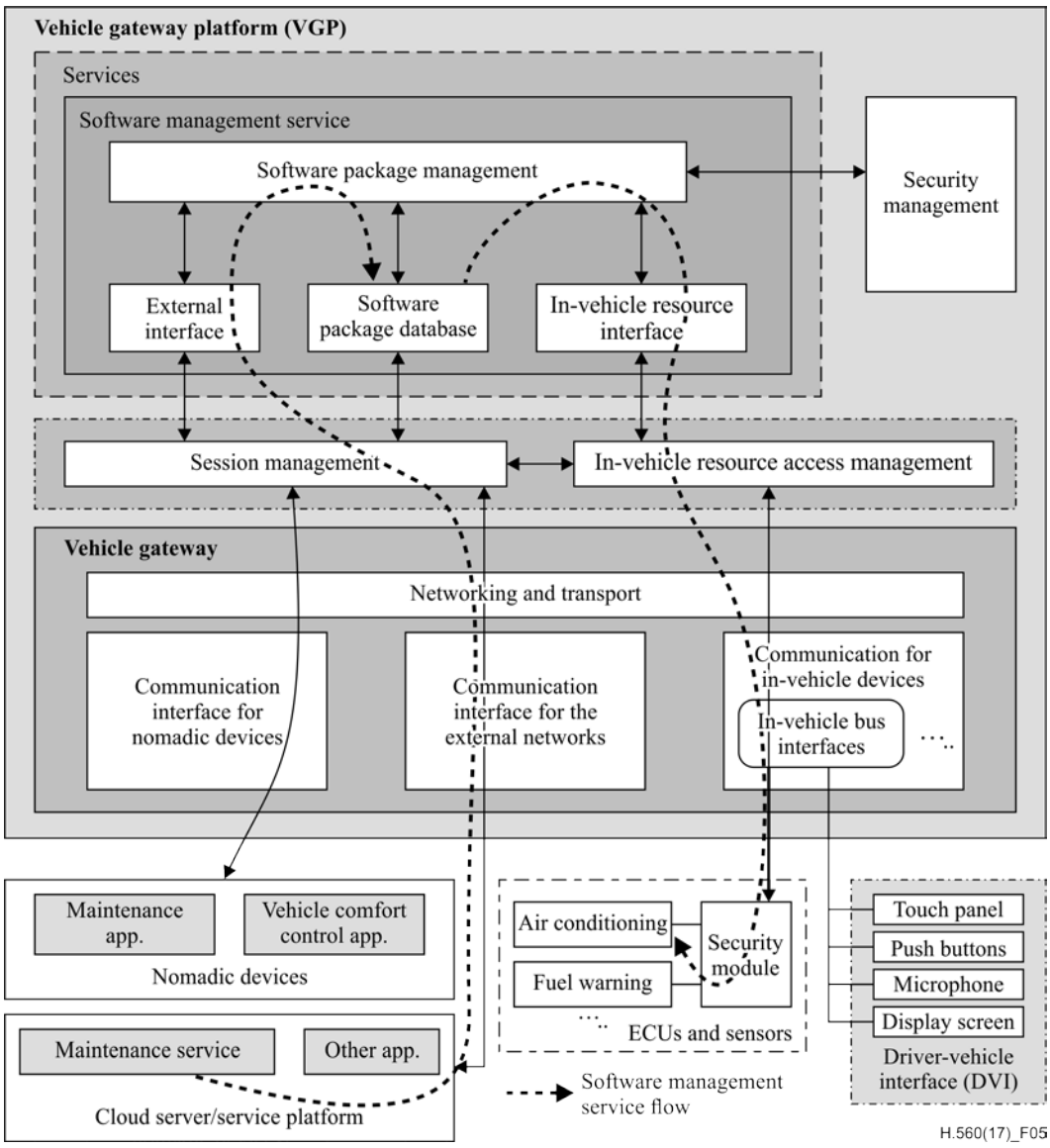

Figure 5 – VGP integration of the software management service

7.3.1.2 Applications data management service

An applications data management service is required to fulfil the following requirements:

– Provide a database used to store the data and the associated metadata used by the different software components in a secure way in order to avoid possible intrusion. This database is also used to store dynamic data related with all kinds of VGP applications, e.g., the local dynamic map (LDM) database contains data necessary to build a LDM. Metadata shall include data type and size, software components owner and access permissions. It should include physical location of data and encryption keys if requested.

– Provide a common, fast, secure, safe and flexible external access interface for accessing stored data and associated metadata from external devices or servers, in accordance with the access permissions defined in the database.

– Provide several internal access interfaces to allow the software components to operate on data and associated metadata. Types of supported operations on the data entries and the associated metadata are addition/removal/modifications/reading. In particular, these interfaces shall support the specifications implemented in the ECUs for secure update such as the specification defined by [b-TCG TPM2.0]. At least one internal access interface for the IP protocol shall be provided.

– Provide a journaling sub-module in charge of maintaining an on-board journal containing all accesses and operations done on any data entries and associated metadata. The journal access shall be restricted to only authorized parties and it must be protected with signature and encryption schemes in order to provide reliability and verifiability of the logs.

The integration of the application data management service into the VGP is shown in Figure 6. Figure 6 presents some scenarios of access to data shared by ECU and VGP software components from either a nomadic device or a remote server.

The dotted line arrows illustrate how a maintenance application running over a nomadic device has access to the configuration data of the air-conditioning ECU. The application connects to the database managed by application data management service through one communication interface for nomadic devices (for instance WLAN interface) and the session management service functionality. The database contains information data obtained from the air conditioning ECU through the in-vehicle resource access management service functionality and an in-vehicle bus interface (for instance CAN).

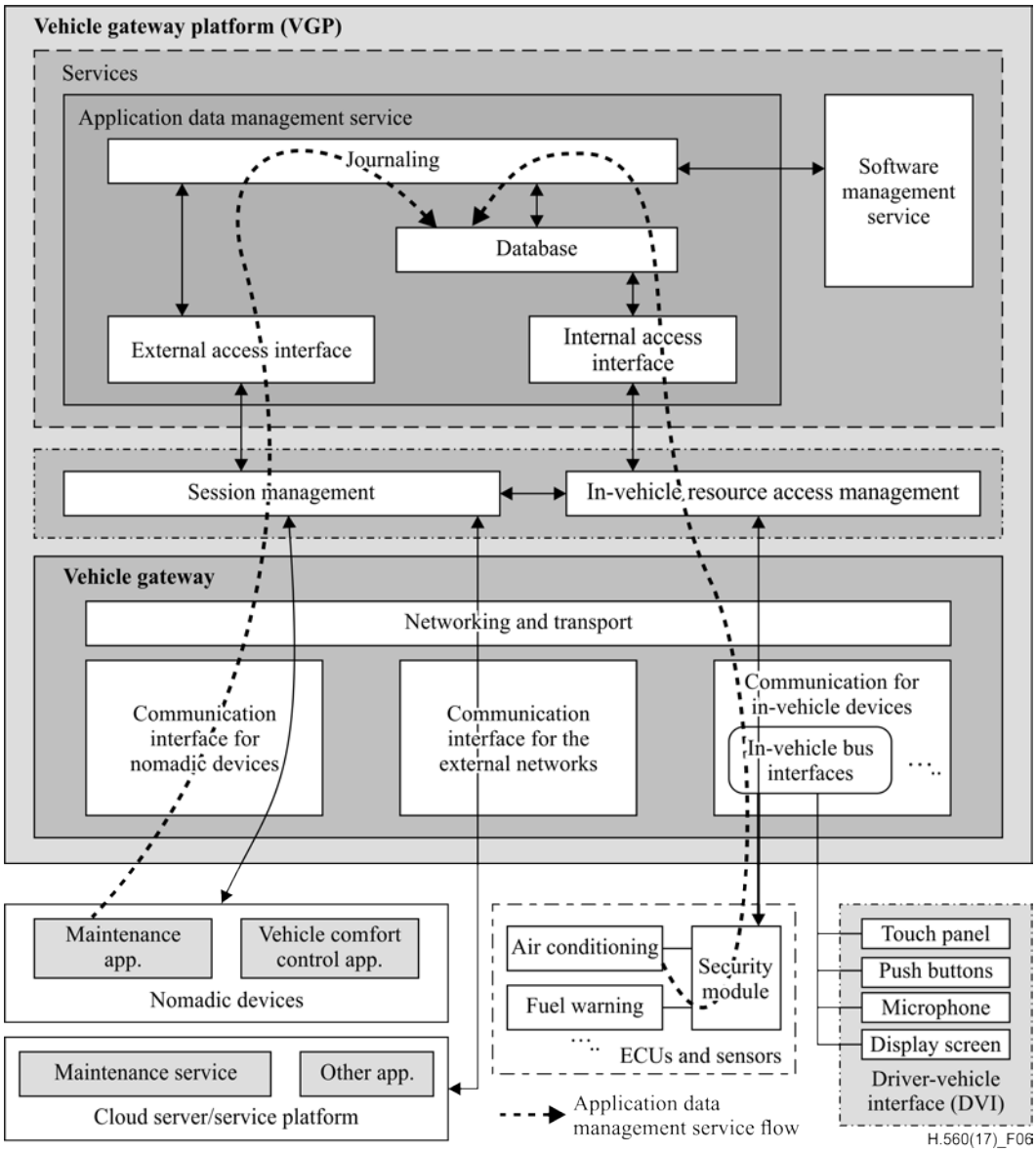

Figure 6 – VGP integration of the application data management service

The applications data management service may interact with the software management service by using the software package management sub-module through the update interface dedicated to IP protocol, both being provided by the software management service as described in clause 7.3.2.1.

7.3.2 Application requirements

7.3.2.1 Software management service

The applications must use the software upload interface provided by the VGP, implement the proper user authentication scheme and reflect correct management on their human-machine interface.

7.3.2.2 Applications data management service

The applications must use the external access interface provided by the VGP, implement the proper user authentication scheme and reflect correct management on their human-machine interface.

7.3.3 Communication network requirements

7.3.3.1 Software management service

The external interface defined by the software management service must be implemented over a network transport layer offering a reliable and fast data delivery.

The external interface defined by the software management service must be preferably implemented over a network transport layer offering an encrypted and authenticated data link.

7.3.3.2 Applications data management service

The external access interface defined by the applications data management service must be implemented over a network transport layer offering a reliable and fast data delivery.

The external access interface defined by the applications data management service must preferably be implemented over a network transport layer offering an encrypted and authenticated data link.

8 Requirements for service functionalities

Service functionalities are VGP entities that provide helpers for other VGP services. They do not constitute a basic service for applications but are required to run other services. They include service management functions such as session management and in-vehicle resource access management.

8.1 Session management service functionality

8.1.1 VGP requirements

As shown in Figure 7, the VGP must manage security tasks such as protecting against attacks from outside the vehicle and authenticating external applications. The VGP is required to fulfil the following requirements:

– Provide a function to authenticate the devices and external applications configured from the security management for services and applications sub-module (e.g., using certificates, common password, etc.).

– Provide normal connection management (i.e., non-encrypted connection) function to send/receive non-critical or public data (e.g., infotainment).

– Provide a secure connection management function to send/receive the important vehicle and/or personal information safety (e.g., establishing VPN connection, using TLS/SSL, etc.) based on the security keys provided by the security management for services and applications sub-module.

– Prohibit the transmission of unnecessary vehicle and/or personal information to the external applications by applying device authorization rights and firewall rules defined by the security management for services and applications sub-module.
– Receive the data from external applications securely. For instance, the VGP should block access to safety critical units such as engine control from unauthorized devices.
– Protect in-vehicle devices from unauthenticated external application and/or servers (firewall functionality) based on firewall rules defined by the security management for services and applications sub-module.

It shall be noticed that application authorizations used by each VGP service to define application rights for the access to service resources, are managed by the security management for services and applications sub-module. These authorization rights are then used by the session management service and all other VGP services to filter and regulate access to some particular critical data. This scheme allows for a flexible VGP service deployment and a resource access control specific to each service, depending on the type of managed resources.

Figure 7 shows the integration of the session management service inside the VGP. It illustrates the previous requirements for a non-encrypted session opened between a trusted application running over a nomadic device and a VGP service (long dotted line arrows). In a second example, it also shows a secured session opened from a nomadic device that gets information from the air conditioning ECUs (short dotted line arrows).

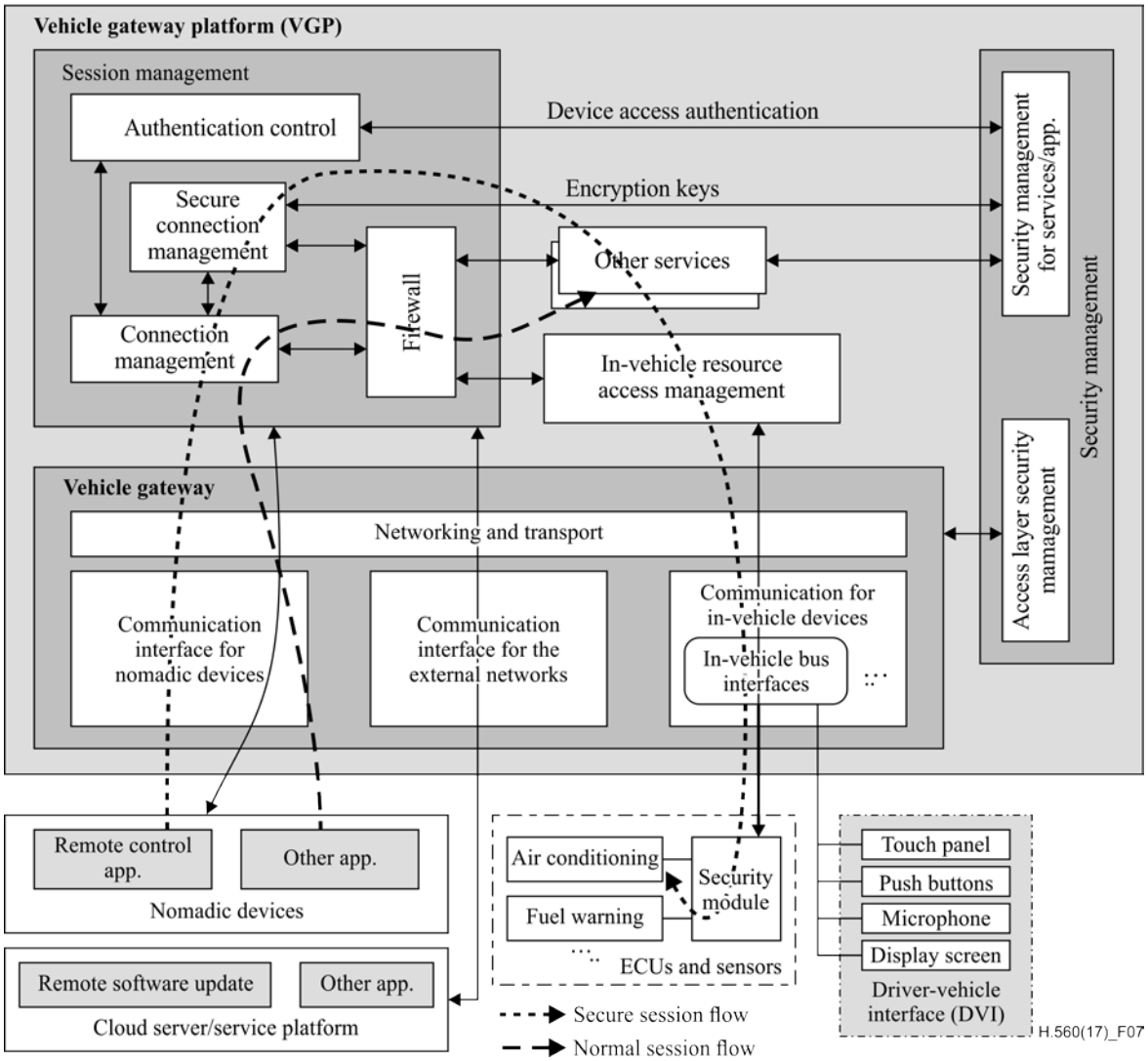

Figure 7 – VGP integration of the session management service

8.1.2 Application requirements

The applications and the VGP shall provide the functions to authenticate each other. Before starting any communication between the applications and in-vehicle devices (e.g., sensors, displays, speakers, controls, etc.), applications and the VGP shall authenticate each other using the defined method.

External applications shall also provide the function to establish secure connections. At the end of the authentication process, if the applications require secure connections (e.g., for critical data exchanges), external applications and the VGP shall use secure connections such as VPN or secure sockets layer (SSL).

8.1.3 Communication network requirements

Unsecure and secure connection management functions, as well as the authentication function defined by the session management service shall be implemented over network and transport layer offering a fast data delivery.

One or more protocols used for secure association and encryption such as transport layer security (TLS) or Internet protocol security (IPsec) shall be supported for the authentication and secure connection functions.

Intermediate firewall shall allow forwarding of all protocols that are used for authentication and secure connection functions.

8.2 In-vehicle resource access management service functionality

In-vehicle resource access management service enables communication between the external devices and applications and the in-vehicle resources such as ECUs and sensors.

8.2.1 VGP requirements

As shown in Figure 8, an advanced access service to in-vehicle resources is required to fulfil the following requirements:

– Provide to external applications a common interface to access on-board resources (power train information, body control, infotainment controls, devices through DVI, etc.). This interface shall support synchronous and asynchronous methods so that a service may receive in a secure, flexible and reliable way every information coming from a selected set of resources.

– Select, organize and convert in-vehicle data required for each managed function types (e.g., air conditioning, infotainment system, seat control, power train, etc.) in order to present data in an uniform and generic way.

– Provide an access control scheme so that an application or a service has access to only in-vehicle resources for which it has been authorized. Access control is based on application authorization provided by the Security management for Services and applications sub-module.

– Provide to external applications access to in-vehicle resources (power train information, seat control, air-conditioning control, etc.) in a uniform way whatever the type of in-vehicle buses.

Figure 8 illustrates the integration of the different sub-modules required by the access service to in-vehicle resources into the VGP. The "External interface" sub-module is in charge of providing a uniform way for external applications and services. The "Access control" is in charge of providing access control scheme for an application or a service that has been authorized. The "Access control" interacts with "Security management" to get the application access rights.

The "Data abstraction" fulfils checking and package data from in-vehicle ECUs and sensors and checking and un-package data and control data from external application. The "In-vehicle resource interface" provides to external applications access to in-vehicle resources in a uniform way whatever the type of in-vehicle buses.

Figure 8 also presents some scenarios of in-vehicle resource access management service exchange between nomadic devices, remote servers and the in-vehicle resources such as ECUs and sensors. The dotted line arrow shows a synchronous query/response communication between a monitoring service running over a nomadic device and the in-vehicle resource access management service to get air-conditioning status.

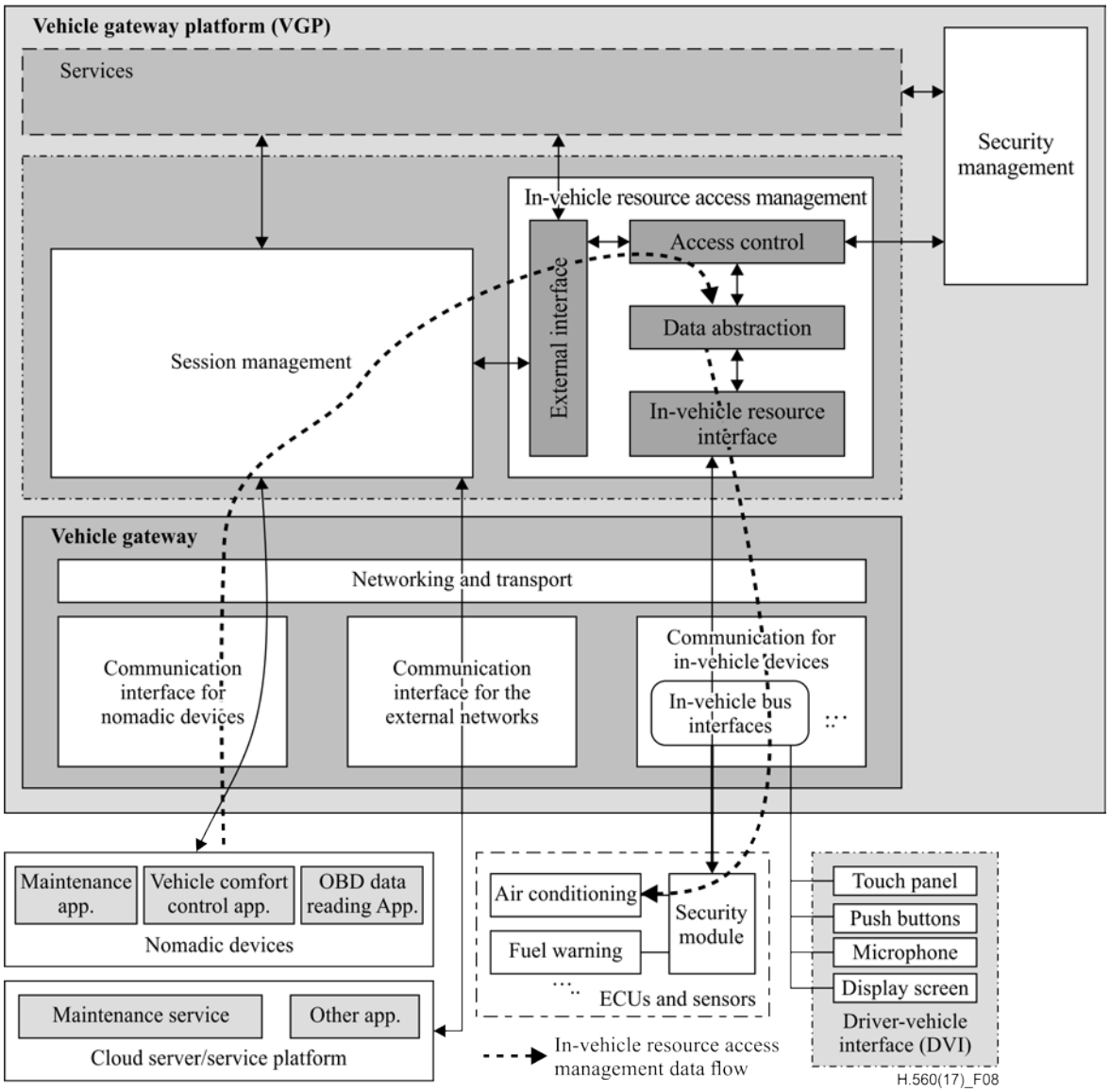

Figure 8 – VGP integration of the in-vehicle resource access management

8.2.2 Application requirements

The application must adapt the internal application data to the external interface format defined by the access service to in-vehicle resources.

8.2.3 Communication network requirements

The external interface defined by the access service to in-vehicle resources must be implemented over a transport layer offering a reliable data delivery.

The external interface defined by the access service to in-vehicle resources may be preferably implemented over a transport layer offering an encrypted and authenticated data link.

Depending on the in-vehicle resource targeted by the external interface function, the set of QoS parameters used for the transport layer may be selected accordingly.

9 Management requirements

9.1 Device management

9.1.1 VGP requirements

The VGP management data shall be organized in a management information base (MIB) that contains VGP status and configuration. The MIB shall expose variable data and their associated metadata (type, size, access right, creation time, last update time, etc.).

The MIB should organise the data in a hierarchic way using object identifiers (OIDs) to identify the variables.

Each VGP entity such as services and service functionalities shall be able to extend the MIB, defining their own hierarchies, variables and associated metadata. The MIB shall contain the description of the management data.

Authorization rights to access and extend the MIB are managed and provided by the security management for the services and applications sub-module. Those authorization rights are applied by the device management function to allow/deny read/write access to some particular variables inside the MIB.

9.1.2 Communication network requirements

The VGP shall support one or several management protocols for collecting and organizing information about the VGP itself for configuration and monitoring purposes. The VGP shall provide access to the MIB to the VGP services, external applications running over nomadic devices and services running over remote servers for configuration, monitoring and maintenance purposes.

The external interface defined for the device management may preferably be implemented over a network transport layer offering an encrypted and authenticated data link.

9.2 Security management for services and applications

The security management for services and applications (SMSA) is the part of security management that covers the security functions in the OSI protocol layers 5 to 7.

9.2.1 VGP requirements

The security management for services and applications (SMSA) shall support the registration, authentication and authorization functions for internal VGP services, external applications running over nomadic devices and services running over some remote cloud servers.

The SMSA shall support the registration of service capabilities/user data that an application is allowed to use. It includes application certificate checking, that involves the support of identity, crypto key, digital signature and certificate management, e.g., identity add/delete/modification, crypto key create/update/storage, certificate create/update/storage/destroy.

Application authorizations provided by the SMSA function are used by the different VGP services to filter and regulate access to some particular critical data. This scheme allows a flexible VGP service deployment and a resource access control specific to each service, depending on the type of managed resources.

Bibliography

[b-ITU-T E.800] Recommendation ITU-T E.800 (2008). *Definitions of terms related to quality of service*.

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

[b-TCG TPM2.0] *TCG TPM 2.0 Library Profile for Automotive-Thin*. https://www.trustedcomputinggroup.org/resources/tcg_tpm_20_library_profile_for_automotivethin

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