International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.551

(01/2022)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

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

Architecture of vehicular multimedia systems

Recommendation ITU-T H.551

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, immersive environments, virtual and extended reality	H.420–H.439
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
Content delivery and ubiquitous sensor network applications	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 SYSTEMS, 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
Safe listening	H.870–H.879

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

Recommendation ITU-T H.551

Architecture of vehicular multimedia systems

Summary

Recommendation ITU-T H.551 defines the configuration for vehicle multimedia systems (VMSs), the reference model of VMS architecture, and the reference solution for VMS multimedia applications. VMS security issues and personally identifiable information protection and privacy issues are also described.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.551	2022-01-28	16	11.1002/1000/14811

Keywords

Architecture, vehicle multimedia systems.

* 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T H.551

Architecture of vehicular multimedia systems

1 Scope

This Recommendation defines the features and configurations of vehicle multimedia systems (VMSs) and the reference model of VMS architecture. The reference model of vehicular multimedia service platform, the reference protocol stack for convergence transmission, and the reference receiver model of in-vehicle devices for VMS multimedia applications are also defined. VMS security issues and personally identifiable information protection and privacy issues are described as well.

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.749.3] Recommendation ITU-T F.749.3 (2020), *Use cases and requirements for vehicular multimedia networks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 vehicular multimedia networks (VMN) [ITU-T F.749.3]: The VMN consist of the vehicular multimedia service platform (VMSP), broadcast and communication networks, and the vehicle multimedia system (VMS) in the vehicle.

3.1.2 vehicular multimedia service platform (VMSP) [ITU-T F.749.3]: The VMSP is a platform in the cloud that enables the multimedia service for end-user(s) in the vehicle.

3.1.3 vehicle multimedia system (VMS) [ITU-T F.749.3]: The VMS consists of vehicle multimedia system inputs (VM I/P), vehicle multimedia unit (VMU) and vehicle multimedia system outputs (VM O/P).

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 VMS core function: A function that deals with the physical, functional and logical data of VMS.

3.2.2 VMS associated function: A function that only receives and displays functional and logical data from other systems or sub-systems.

3.2.3 VMS shared function: A function that is used by other systems or sub-systems to share the physical, functional and logical data and control information.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ADAS	Advanced Driver Assistance System
AM	Amplitude Modulation
ANC	Active Noise Cancellation
APP	Application
AR	Augmented Reality
AVM	Around View Monitoring
bCall	Breakdown Call
BGS	Background Scan
CA	Conditional Access
CDN	Content Distribution Network
CDR	Convergent Digital Radio
DAB	Digital Audio Broadcasting
DASH	Dynamic Adaptive Streaming over HTTP
DMS	Driver Monitoring System
DNT	Do Not Track
DRM	Digital Rights Management
DTTB	Digital Terrestrial Television Broadcasting
eCall	Emergency Call
ECM	Entitlement Control Message
ECU	Electronic Control Unit
EMM	Entitlement Management Message
FM	Frequency Modulation
GDPR	General Data Protection Regulation
HEO	High Earth Orbit
HLS	HTTP Live Streaming
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
HVAC	Heating, Ventilation and Air Conditioning
IAM	Identity and Access Management
IBOC	In-Band On-Channel
iCall	Information Call
IP	Internet Protocol
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LEO	Low Earth Orbit

MR	Mixed Reality
NAT	Network Address Translation
OBD	On-Board Diagnostics
OEM	Original Equipment Manufacturer
OLED	Organic Light Emitting Diode
OS	Operating System
OTA	Over The Air
PD	Phase Diversity
PII	Personally Identifiable Information
PUF	Physical Unclonable Function
RDS	Radio Data System
RF	Radio Frequency
RVC	Rear View Camera
TCP	Transfer Control Protocol
TMC	Traffic Message Channel
UDP	User Datagram Protocol
V2I	Vehicle-to-Infrastructure
V2P	Vehicle-to-Person
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VM	Vehicular Multimedia
VM I/P	Vehicle Multimedia System Inputs
VM O/P	Vehicle Multimedia System Outputs
VMN	Vehicular Multimedia Network
VMSP	Vehicular Multimedia Service Platform
VMS	Vehicle Multimedia System
VMU	Vehicle Multimedia Unit
VR	Virtual Reality

5 Conventions

In this Recommendation:

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

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

– The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

– The keywords "is not recommended" indicate a requirement which is not recommended but which is not specifically prohibited. Thus, conformance with this Recommendation can still be claimed even if this requirement is present.

6 Background

In this Recommendation, the features and configurations of vehicle multimedia systems (VMSs) and the reference model of VMS architecture are defined in compliance with the requirements in [ITU-T F.749.3]. The reference model of vehicular multimedia service platform (VMSP), the reference protocol stack for convergence transmission, and the reference receiver model of in-vehicle devices for VMS multimedia applications are also defined. VMS security issues, personally identifiable information (PII) protection and privacy issues are defined as well.

The Recommendation is organized as follows:

Clause 7 defines the features and configurations of VMS. Clause 8 defines the reference model of VMS architecture. Clause 9 defines the reference model of VMSP, the reference protocol stack for convergence transmission of multimedia contents over heterogeneous networks, and the reference receiver model of in-vehicle devices. Clause 10 addresses VMS security issues. Clause 11 addresses PII protection and privacy issues.

7 VMS features and configurations

7.1 VMS features

VMS features are determined based on the following principles:

– User experience, entertainment and information features and applications for the driver and the passenger.

– Market, regional and country specific requirements.

– Legal and mandatory requirements.

However, VMS features do not describe the overall network architecture of vehicles or the integration of multiple domains in vehicles.

7.2 VMS configurations

VMS configurations are based on the following principles:

– VMS configurations define standalone requirements for entertainment and information display to driver and passenger.

– VMS configurations are recommended to be defined at the level of features and functions.

– VMS configurations are recommended to include hardware components within the VMS.

– Multiple VMS configurations are possible.

– VMS configurations are recommended to be highly variable. Both OEM-built and after-market plug-in VMS products are recommended to be considered.

However, VMS configurations do not describe the overall network architecture of vehicles or the integration of multiple domains in the vehicle.

7.2.1 Deciding factors

VMS configurations are determined based on the following deciding factors:

– Usage requirements.

– Features, functional requirements.

– Interface requirements.

– Cost requirements.
– Benchmarked requirements.

7.3 List of VMS features

The reference VMS features are summarized in Table 1.

Table 1 – Reference VMS features

Features	Sub-features	Configurable
Human machine interface (HMI)	Display technology	Light emitting diode (LED)/liquid crystal display (LCD)/organic light emitting diode (OLED), etc.
	Number of displays	Multiple (front, central, rear, etc.)
	Control	Traditional controls: Button / knobs / touch controls, etc.
		Intelligent controls: Voice control, face recognition, voice biometric, gesture, personalization, eye movement control, tactile-flexible feedback touch, etc.
	Multi-screen interaction	Push information to different screens
		Video file synchronous or asynchronous display
		Dual navigation display
		Free matching of the display interface
	System language	User interface: Different language requirements as mandated by regulations
	Display for camera	Rear view camera (RVC) / Around view monitoring (AVM)
	Control and display	Heating, ventilation and air conditioning (HVAC) display and controls
		Driver assistance control and displays
Broadcast	Terrestrial	Analogue: Amplitude modulation (AM) broadcasting, frequency modulation (FM) broadcasting, FM broadcasting with dual tuner and phase diversity (PD), FM broadcasting with background scan (BGS), Radio data system (RDS), etc.
		Digital: Digital audio broadcasting (DAB), digital terrestrial television broadcasting (DTTB), in-band on-channel (IBOC) technologies, convergent digital radio (CDR), etc.
	Satellite	Satellite audio/video services (e.g., satellite audio/video streaming service)
External Network Connectivity	Cellular networks	3G/4G/5G
	Satellites bi-directional	Low earth orbit (LEO) satellite bi-directional communication networks
		High earth orbit (HEO) satellite bi-directional communication networks
	Vehicle-to-everything (V2X)	Vehicle-to-vehicle (V2V), Vehicle-to-infrastructure (V2I), Vehicle-to-person (V2P)
	Wireless local area networks	IEEE 802.11 hotspots
		Hands-free calls and music playing using personal area networks

Table 1 – Reference VMS features

Features	Sub-features	Configurable
In-vehicle Mobile Connectivity		Web surfing using IEEE 802.11 local area networks
		Screen sharing using short distance communication networks
		Third-party vehicle interface applications
Telematics Configurations	Remote	Remote monitoring, control, vehicle data transfer
	Calls	Emergency call (eCall), breakdown call (bCall), information call (iCall)
Online APP Stores/Suites	APP store	New features downloaded
	Theme marketplace	Theme skin replacement
Over-the-air (OTA) update		OTA software
Media	Audio	Normal and high fidelity
	Image	In different formats
	Video	Normal video with various resolutions, augmented reality (AR), virtual reality (VR), mixed reality (MR)
Navigation	Local navigation	
	Cloud navigation	Data from telematics box (3G/4G/5G) modem / user mobile data
	Real-time traffic	Traffic message channel (TMC), Transport Protocol Experts Group (TPEG), real time traffic centre, etc.
	Services	Navigation services, real-time weather forecasting services, etc.
	Advanced features	Intelligent travel applications such as calendar, planners, etc.
Voice Recognition (VR) and Synthesis	Local VR, cloud VR and synthesis	Natural language understanding
		Auto speech recognition
		Text to speech
Audio	Audio quality	Volume adjustment of the speed function
		Sound algorithms
		Active noise cancellation (ANC)
		Personalization settings (sound patterns and facial recognition)
		Best listening position adjustment
		Sound quality reduction technology
	Amplifier configurations	Multiple channels integrated amplifiers
		Amplifiers with speakers
	Sound configuration	Multiple speaker configurations tweeter (treble speaker) / woofer (bass speaker) / full range speakers
Security		Identity and access management, authentication, authorization and transaction audit
		Network security
		Operational security

Table 1 – Reference VMS features

Features	Sub-features	Configurable
		Application security
		Software OTA security
		Hardware security
		Cryptography security
Privacy		General data protection considerations
		Personal information protection
		Data visibility protection
		Confidentiality, integrity and availability
Intelligent features	Driver monitoring system (DMS)	Fatigue, expression and emotion recognition
	Health	Heartbeat monitor, blood pressure monitor
	Office environment	Email, video conference calls, holographic projection, gesture recognition, eye movement control, handwritten memo
	Games	Voice based interactive quiz games, holographic interacting games, adventure games
	Social	Social applications in vehicle

NOTE – Security and privacy features are essential to VMSs with configurations M1 to M5, but are configurable to VMS with configuration M0. Examples of VMSs with configuration M0 to M5 are given in Appendix I of [ITU-T F.749.3].

8 VMS architecture

This clause defines the classification of VMS functions, the deciding factors and the reference model of the VMS architecture.

8.1 VMS functions

In general, VMS functions can be classified into three categories, namely, VMS core functions, VMS associated functions and VMS shared functions.

VMS core functions are VMS functions that deal with the physical, functional and logical data of VMS. Examples of VMS core functions include tuner, media processing, display functions, etc.

VMS associated functions are VMS functions that only receive and display functional and logical data from other systems or sub-systems. Examples of VMS associated functions include camera feed from rear vehicle camera, eCall information display initiated by an accident, etc.

VMS shared functions are VMS functions that are used by other systems or sub-systems to share the physical, functional and logical data and control information. Examples of VMS shared functions include HVAC controls through the vehicle multimedia unit (VMU), etc.

8.2 Deciding factors of VMS architecture

The following are deciding factors of the VMS architecture:

– Technical requirements

– Operating system, memory and hardware requirements

– Features, functional, sub-systems, logical and physical requirements

– Interface requirements
– Cost requirements
– Usage requirements
– Benchmarked requirements
– Standard compliance requirement

8.3 Reference model of VMS architecture

The VMS architecture is defined at the interface, the sub-systems and the systems levels. A reference model of VMS architecture is given in Figure 1.

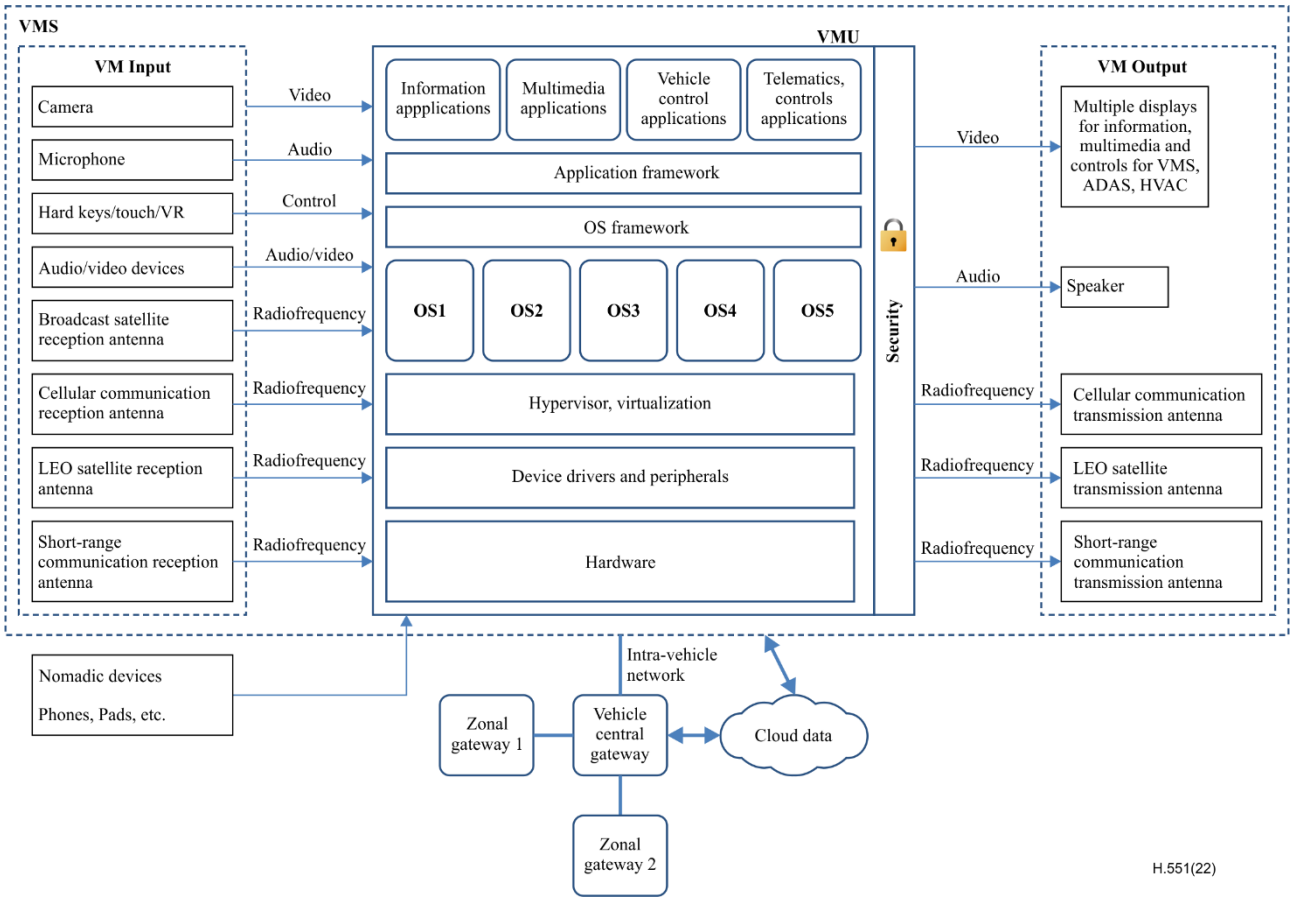

Figure 1 – Reference model of VMS architecture

8.3.1 Applications

Applications of VMS include:

– Information applications, e.g., instrument cluster, head up displays, navigation and weather.
– Multimedia applications, e.g., media, navigation, VR and HMI.
– Vehicle control applications, e.g., HVAC and connected cars.
– Telematics applications, e.g., remote control, diagnostics, and data access.
– Display applications, e.g., front and rear display applications.

8.3.2 Application framework

VMS features and functions are accessed via user interface tools designed according to an application framework.

8.3.3 Operating system (OS) framework

The OS framework handles system services. It could be a proprietary framework of OEMs and VMS developers.

8.3.4 OS

Various embedded operating systems (OSs) and kernels are used depending on processing load, speed and accuracy requirements.

8.3.5 Hypervisor and virtualization

Hypervisor and virtualization techniques are used to support multiple OSs and processing tasks by a single high-power processor through computing resource sharing.

8.3.6 Device drivers and peripherals

Device drivers include vehicle network interface driver, audio and video drivers, display drivers, inter-processors protocol drivers and intra-processor protocol drivers.

8.3.7 Hardware

Hardware includes processors, memory and other components.

8.3.8 Cloud data

Cloud data includes:

– Data for multimedia services

– Data for telematics services, i.e., remote diagnostics services, software OTA update services, bCall / iCall services and navigation services.

9 VMS multimedia applications

Figure 2 depicts a system for VMS multimedia applications, which consists of vehicular multimedia service platform (VMSP) in the cloud, heterogeneous networks and in-vehicle devices. A convergence transmission scheme is used to improve the transmission efficiency of multimedia contents over heterogeneous networks, i.e., satellite broadcasting networks and mobile communication networks. This clause describes the VMSP reference model (clause 9.1), the reference protocol stack for convergence transmission of multimedia contents over heterogeneous networks (clause 9.2), and the reference receiver model of in-vehicle devices (clause 9.3).

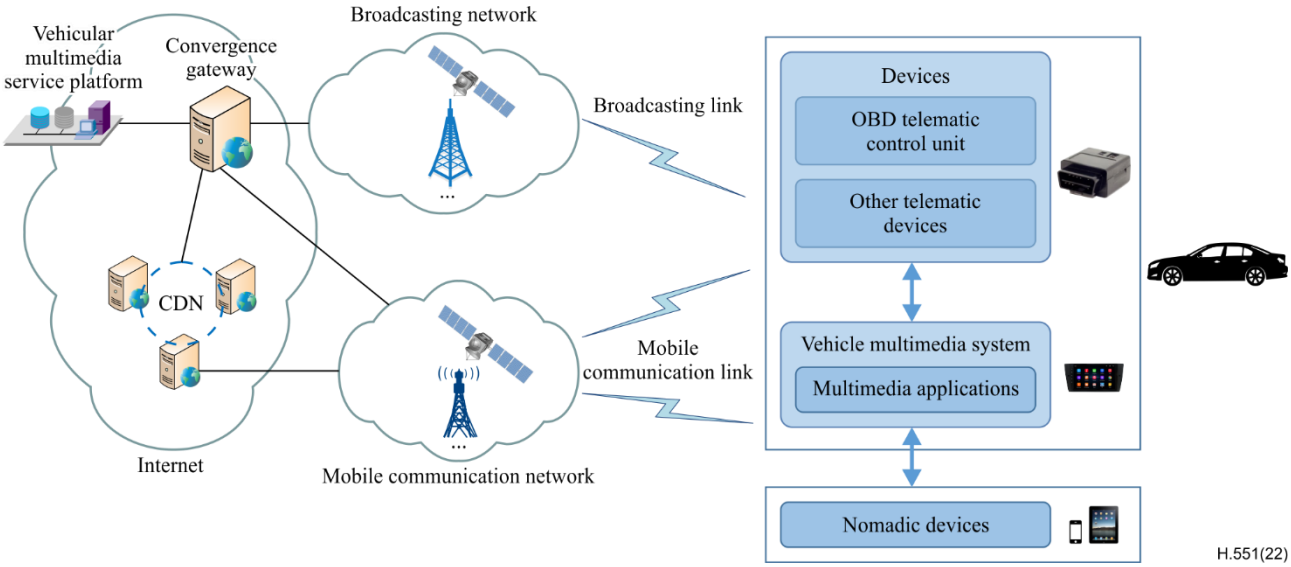

Figure 2 – A system diagram for VMS multimedia applications

9.1 VMSP reference model

The VMSP consists of content server, licence server (optional) and conditional access (CA) server (optional). Its reference model is illustrated in Figure 3.

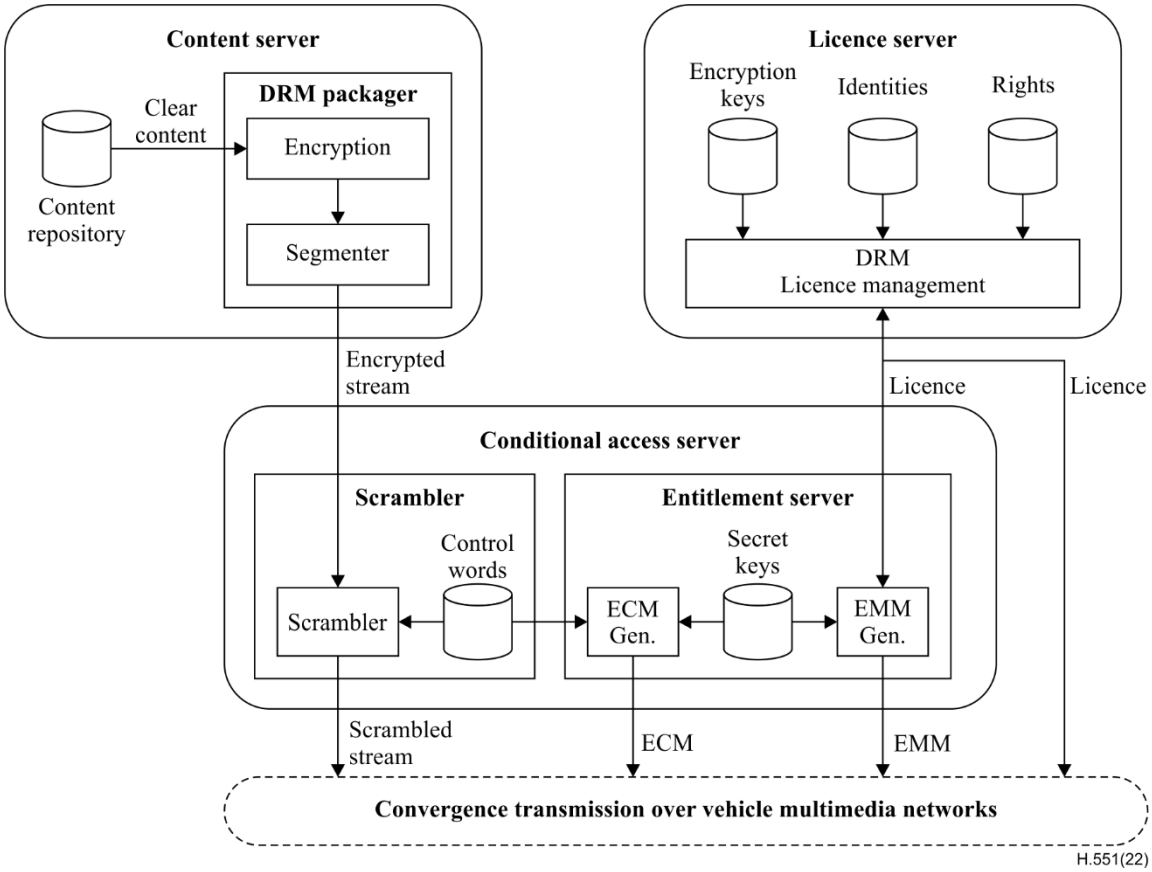

Figure 3 – Reference model of VMSP

The content server consists of the content repository and the digital rights management (DRM) packager. The content repository is used to store the clear contents that the content provider (CP) wants to distribute. Note that the content repository is often built into the DRM solution or is sometimes integrated into a content management system that interfaces to the DRM server. The DRM packager encrypts and packages the multimedia contents for streaming over VMN. The licence server is used to manage the creation, modification, and revocation of the DRM licences. The DRM licence contains identities, rights specification and encryption keys. Usually, DRM clients could acquire their DRM licences from the licence server by using mobile communication network connections. The candidate packaging schemes for streaming in VMN include MPEG-DASH [b-ISO/IEC 23009-1] and HLS [b-IETF RFC 8216].

The conditional access (CA) server consists of scrambler and entitlement server. The scrambler is used to scramble the inbound streams using control words. The entitlement server is used to generate the entitlement control message (ECM) and the entitlement management message (EMM). Usually, the outbound scrambled streams, ECMs and EMMs are delivered over satellite broadcast networks. However, there are the following two exceptions:

1) When a user drives to a place with no cell phone coverage, DRM licences cannot be acquired through any mobile communication network. In this case, DRM licences could be integrated into EMMs and be delivered to the user over satellite networks. Thus, service continuity could be achieved.

2) When a service operator starts its business, thousands of new customers may try to activate their devices in a short period of time. However, the bandwidth required for the delivery of EMMs for those devices may not be available in satellite broadcast networks. In such a case, EMMs could be temporally offloaded from satellite broadcast networks to mobile communication networks. Thus, a successful business launch could be guaranteed.

9.2 Reference protocol stack for convergence transmission

Broadcast is generally regarded as the most cost-effective way to deliver linear programs to a large population over vast geographic areas. Despite the success of Ka- and Ku-band fixed DTV broadcast around the world, service provision via broadcast to vehicles has turned out to be challenging. For example, in an urban environment, the reliability of broadcast communications is rather problematic due to moving receivers and frequent signal blockage by high buildings. Although the broadcast urban coverage issue can be addressed by ground repeater networks that fill up the outage gaps, building the gap-filler infrastructure is both expensive and highly time consuming. Another limitation of broadcast communication is that it can only provide one-way services, thus unable to accommodate personalized services or support user interactions.

To deal with these challenges, a convergence transmission scheme is proposed for multimedia contents transmission over VMN, where most media contents are delivered to massive users via broadcast networks, and mobile communication networks are used only to recover packets that have been dropped by the broadcast networks. The scrambled streams from the VMSP are sent to the convergence gateways, where the media segments are further packetized into sequenced packets and broadcast to all users over the satellite network. At the terminal, the missing or erroneous packets of broadcast streams can be easily detected. These dropped packets are recovered by retransmission over the mobile communication network. Once the media streams are seamlessly re-assembled, the terminal can not only play these media streams at the cockpit displays and speakers, but also serve as a local infotainment centre to Wi-Fi-share these media streams with all passengers using their personal devices such as smart phones and tablets. The convergence transmission scheme is illustrated in Figure 4.

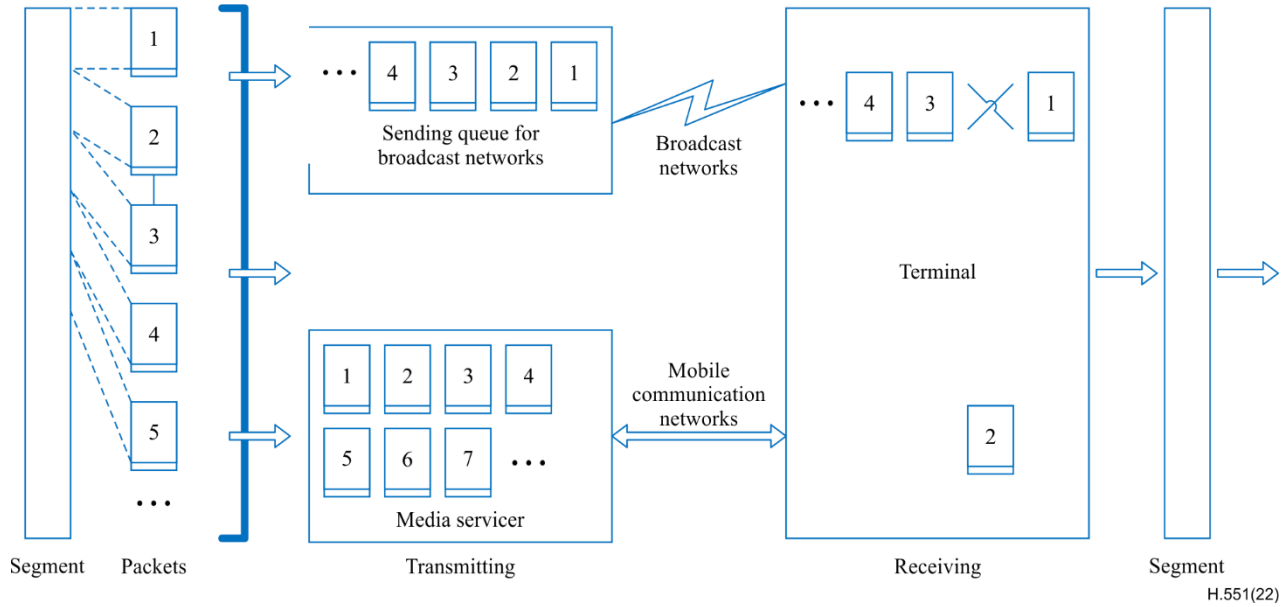

Figure 4 – The processing of convergence transmission

The convergence transmission scheme takes full advantages of the complementary strengths of broadcast networks and mobile communication networks. Hence, the system efficiency of multimedia streaming services over VMN is optimized.

The reference protocol stack for convergence transmission of multimedia contents over VMN is given in Figure 5. Note that the convergence transmission protocols are agnostic to the underlying physical-layer standards and are transparent to the upper-layer standards. Thus, minimum modifications to the existing broadcast or mobile communication infrastructures can be guaranteed.

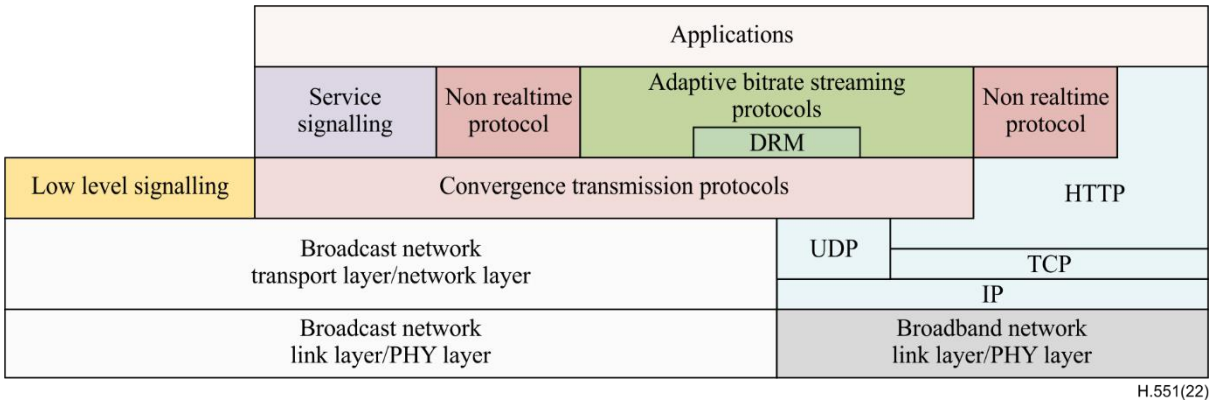

Figure 5 – Reference protocol stack for convergence transmission

The general assumption is that the network layer protocol may be based on both versions of the IP protocol (IPv4 and IPv6). It is advisable to select IPv6 [b-IETF RFC 8200] for direct and secure connectivity between VMS and the cloud platforms, for the following reasons:

– The IETF clearly advises other standards development organizations (SDOs) to prefer IPv6 [b-IAB]. As a result, standardization work is recommended to assume IPv6.

– The IPv4 address space was formally exhausted in January 2011, when the Internet Assigned Numbers Authority (IANA) assigned its last IPv4 top-level address space (i.e., /8). Therefore, adopting IPv6 as the only network protocol represents the only viable solution to guarantee the evolution of network services and applications.

– The transition to IPv6 only is considered a strategic initiative by several governmental agencies. An example, among the others, is represented by [b-USG OMB], where the US Federal Government poses specific deadlines and targets to migrate the National Agencies networks to IPv6.

– User devices located in a vehicle may require end-to-end reachability, e.g., to connect to any applications and platforms. This is a case where network address translation (NAT) [b-IETF RFC 2663] coupled with private IPv4 addressing cannot be employed. Conversely, IPv6 provides full support of a global addressing scheme where the user devices are always reachable.

Although people are more familiar with IPv4, and IPv6 deployment has certain new challenges, IPv6's user and traffic growth are much faster than those of IPv4. This means that, with all things considered, the collective wisdom of the industry has selected IPv6 for the future [b-ETSI WP35].

9.3 Reference receiver model

The reference receiver model of in-vehicle devices is given in Figure 6, where the following functions are identified:

– Broadcast connections and broadband connections that provide the connectivity for the receiver to receive signalling and data.

– Convergence transmission protocol/UDP/HTTP/TCP/IP stack and HTTP/TCP/IP stack that provide object-oriented transport protocols for the receiver to receive adaptive bit rate streaming (e.g., DASH or HLS) resources for multimedia streaming services.

– Low-level Signalling: Signalling delivered over broadcast networks that enable the receiver to build a basic service list and bootstrap the discovery of the service signalling for each multimedia service.
– Service signalling: Service-related signalling that enables the receiver to discover and access multimedia streaming services and their content components.
– Cache: Temporary storage and handling of the manifests, initialization segments and media segments whose reception are facilitated by service signalling.
– Adaptive bit rate streaming (i.e., DASH/HLS) server: A local adaptive bit rate streaming server that is used to abstract the underlying layers to the adaptive bit rate streaming client. For the adaptive bit rate streaming client, manifests, initialization segments and media segments are provided through the adaptive bit rate streaming server.
– Adaptive bit rate streaming client: A function that consumes manifests and segments, and communicates with other components in the receiver to personalize the media experience based on platform capabilities, user preferences and user interaction.
– Application: A native or downloaded application that makes use of broadcast or broadband delivered data in order to provide a rich and interactive presentation to the end user.

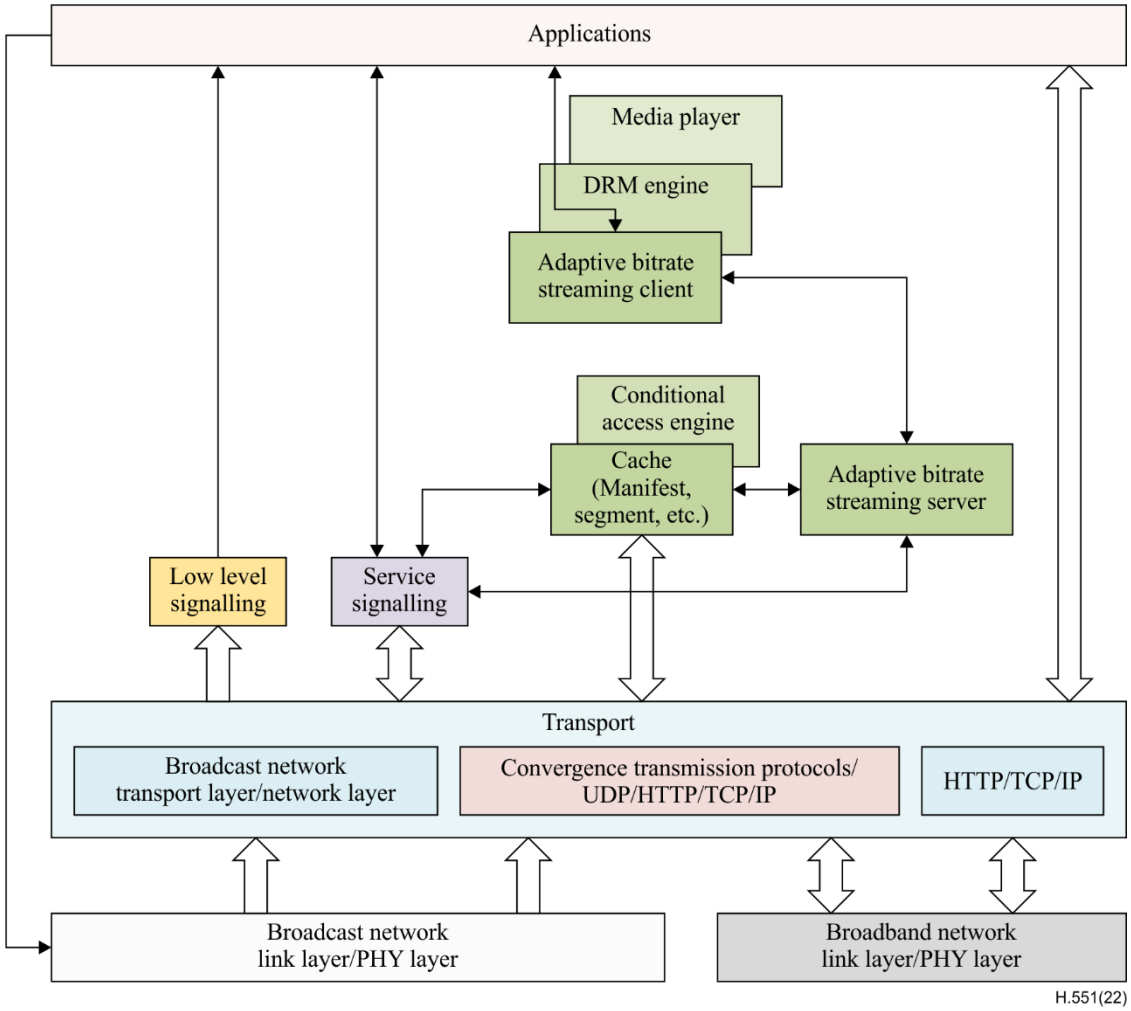

Figure 6 – Reference receiver model of in-vehicle devices

A typical bootstrapping sequence of the reference receiver is presented as below:

– The application requests a pre-configured service list in low level signalling. The service list is delivered to the application, which then provides a user interface for the selection of multimedia streaming services. User chooses a multimedia streaming service to consume.

– The application uses the service signalling entry point information carried in the service list for the selected service to provide access information to the convergence transmission protocol/UDP /HTTP/TCP/IP stack to retrieve the service signalling. Service signalling is delivered to the application.

– By using service signalling, the application provides access information to the convergence transmission protocol/UDP/HTTP/TCP/IP stack for downloading the adaptive bit rate streaming-formatted media components of the selected service, which are sent to the cache to be stored, de-scrambled and subsequently forwarded to the adaptive bit rate streaming server.

– Upon the selection of a service, the application activates the adaptive bit rate streaming client, causing the DASH/HLS client to request and receive media segments from the adaptive bit rate streaming server at or after the media segments availability start times.

– Upon reception of media segments, the composite function comprising the adaptive bit rate streaming client, DRM engine and media player decodes the received media segments, and the decoded media is returned to the application for play out.

10 VMS security

The interactions between the VMS and the other components involved in the security of a car (typically the electronic control unit (ECU)) is recommended to be limited to the shared functions mentioned in clause 8.1.

Details are given in Annex A.

11 Personally identifiable information (PII) protection and privacy

VMS is recommended to provide end-to-end protection as vehicles become connected and offer more interactive services. More user data and privacy related information need to be protected to ensure confidentiality and integrity of the user data that is stored in the VMS, in the vehicle and the VMS cloud or backend servers.

Details are given in Annex B.

Annex A

VMS security

(This annex forms an integral part of this Recommendation.)

A.1 Overview

The interactions between the VMS and the other components involved in the security of a car (typically the ECU) is recommended to be limited to the shared functions mentioned in clause 8.1. Indeed, it is recommended that the VMS does not negatively influence the functions of the other components that ensure the required security of a car, notably in the case of autonomous driving vehicles.

Regarding VMS security, assumed threats to VMS and its eco-system are summarized in clause A.2, and security capabilities against threats are provided as an informative reference in clause A.3.

A.2 Assumed threats to VMS and its ecosystem

A.2.1 Threats regarding vehicular multimedia service platform (VMSP)

In recent years, diversification of connectivity in vehicles has increased remarkably, and in particular, connectivity with various servers located at VMSP is highly required. In the context of VMS, back-end servers are recognized as a VMSP, including OEM-provided servers, supplier-provided servers and ICT service-provided servers to support vehicle eco-system from the remote backend. The following threats can be identified in relation to VMSP:

– Servers in VMSP used as a means to attack a vehicle or extract data.

– Services provided by VMSP being disrupted

– Data held on servers in VMSP being lost or compromised

A.2.2 Threats to vehicles regarding their communication channels

Vehicle communication includes external communications through cellular, LEO satellite, broadcast networks and short-range networks. Channels used in the above communications may be targets of attacks like spoofing, eavesdropping, message manipulation, etc. The following threats can be identified in relation to communication channels:

– Unauthorized manipulation, deletion or other amendments to vehicle-held code/data

– VM interfaces can be used to gain access to further (intelligent) infrastructure within the vehicle (e.g., ECU unrelated to VMS)

– Use of untrusted/unreliable messages and session hijacking/replay attacks

– As VM applications can be updated using over the air, those attacks can apply to VM as well.

– Information disclosure

  See clause 9 of [ITU-T F.749.3].

– Denial of service attacks

– VM itself may not have access to critical infrastructure within the vehicle, but can serve as gateway for those attacks.

– Privileged access by an unprivileged user

– As personalized user accounts can be associated with VM applications, unprivileged access is possible. Unprivileged access via VM may not provide direct access to critical infrastructure (e.g., root access; access to braking system), but can again serve as gateway to access the vehicular infrastructure.

– Malware embedded in communication media

– Intelligent VM rely on data transfer between the VMS and a VMSP in the cloud. By penetrating this communication channel, attackers might use messages/data transfers from the VMSP to the VMS to deploy malware.

– Messages with malicious content

– Intelligent VM rely on data transfer between the VMS and e.g., a VMSP in the cloud. By penetrating this communication channel, attackers might alter messages/data transfers from the VMSP to the VMS to gain access to VMS and/or ECUs within the targeted intelligent vehicle.

A.2.3 Threats to vehicles regarding their update procedures

There are two ways to update vehicle systems, namely, wired update through an on-board diagnostics (OBD) port, portable devices such as an SD card, or a USB flash drive, and wireless update by over-the-air. The software to be updated can be firmware or configuration data of the vehicle. Most electronic problem and software defects can be updated and solved electronically without physical access, e.g., via OBD tester. Furthermore, over-the-air (wireless) updates help in shortening the update cycle to minimize attack exposure for known vulnerabilities of the software. The following threats can be identified in relation to update procedures:

– Misuse or compromise of update procedures

  Regardless of whether the over-the-air update or local/physical update is used, the update procedure can include threats that use fabricated system update programs or compromised firmware.

  The software can be manipulated before the update process, although the update process is intact. The software provider creates/prepares their software for the update, and the software is delivered to the target systems that require the update. Therefore, there can be a serious threat that the software can be manipulated and corrupted before it served.

  Especially during the update procedure, cryptographic materials such as cryptographic keys and certificates used in the software update can be compromised and consequently it may cause an invalid or malicious software update.

– Denial of service and denial of a legitimate update

  Denial of service attack against the update server or network to prevent the rollout of critical software updates and/or unlocking customer-specific features can be a possible attack in the software update procedure. It is also possible to deny legitimate updates.

A.2.4 Threats to vehicles regarding their external connectivity and connections

For a variety of convenient services, vehicles can be equipped with components to communicate with servers in VMSP, and can communicate to everything enabled by road users over a wireless connection. Besides convenience features, there are safety benefits such as the automatic emergency call functionality and those supported by V2X communication. However, the more vehicles connect to external entities for enhancing connectivity, the more threats and vulnerabilities show up because attack surfaces are expanded due to the additional interfaces. The following threats can be identified in relation to external connectivity and connections:

– Manipulation of the connectivity of vehicle functions

  VMS does not provide direct access to critical vehicle functions but can be used as gateway to access those critical components, e.g., dedicated ECUs.

– Hosted third-party software

  VMS applications can be included in the class of "hosted third-party software".

– Devices connected to external interfaces

As outlined in [ITU-T F.749.3], connectivity can be based on brought-in devices such as smart phones.

A.3 Security capabilities based on identified threats

A.3.1 Identity and access management (IAM), authentication, authorization and transaction audit

Multiple administrators and users are involved in VMS services, and these services are accessed and used internally and externally. Identity management is needed, not only to protect identities, but also to facilitate the access management, authentication, authorization and transaction audit processes in such a dynamic and open VMS infrastructure.

One or more common trust models are needed by IAM for the authentication of identities, and by developers, hypervisors and other system components for the authentication of system components such as downloaded software modules, applications or datasets.

IAM contributes to the confidentiality, integrity and availability of services and resources, and thus becomes essential in VMS. Furthermore, IAM may enable the implementation of single sign-on and identity federation for VMS using different authentication mechanisms or distributed in different security domains.

Transaction audit protects against repudiation, enables forensic analysis after a security incident, and acts as a deterrent to attacks (both intrusion and insider). Transaction audit implies more than simple logging, but also includes active monitoring to flag up suspicious activities.

A.3.2 Interface security

This capability secures interfaces open to VMS developers and/or other contracted VMSP vendors through which various kinds of VMSs are delivered, and secures communications based on these interfaces. Mechanisms available to ensure interface security include, but are not limited to: unilateral/mutual authentication, integrity checksum, end-to-end encryption and digital signature.

A.3.3 Network security

In a VMS environment, network security enables both physical and virtual network isolation, and secures communications among all participants. It enables network security domain partition, network border access controls (e.g., firewall), intrusion detection and prevention, network traffic segregation based on security policies, and it protects the network from attacks in both the physical and virtual network environments.

A.3.4 Operational security

This capability provides security protection for the daily operation and maintenance of VMS and VMSP infrastructure.

This operational security capability includes:

– Defining sets of security policies and security activities such as configuration management, patch upgrade, security assessment, incident response;

– Monitoring the VMSP's security measures and their effectiveness and giving appropriate reports to affected VMSs.

In the event that the VMSP's security measures or their effectiveness changes, all downstream VMSs will be alerted to such changes.

These reports and alerts enable authorized VMSs to see appropriate incidents, audit information, and configuration data relating to their VMSs.

A.3.5 Software and firmware updates

Secure OTA updates need to conform to baseline security standards. It is recommended that the update process take into account operational factors (e.g., timing of updates and encryption/decryption processes). The presence of multiple OEMs and third-party vendors contribute to different sub-system interfaces within a vehicle. As such, any vulnerability or cyber risk-targeted towards these OEMs or suppliers can effectively hijack a legitimate software OTA update, which is then sent as cloud data to be deployed to vehicles.

Mechanism for updating software and firmware of VMS (ECUs and related systems) is recommended to be designed, implemented and operated.

In the development of VMS service, mechanism for updating software and firmware of VMS is recommended to be designed and implemented as a basic function. The mechanism for rolling back software and firmware is recommended to also be implemented by design, to be used when an update fails.

In the utilization and support of VMS service, the software/firmware update package has its digital signature, signing certificates and signing certificate chain verified by the device, before the update process begins.

Cryptographic keys used to update integrity protection and confidentiality are recommended to be securely managed and appropriately operated. When updates are conducted over the air (OTA), the updates are recommended to be performed over encrypted communication channels.

Updates using OTA are recommended to either succeed completely or fail in a recoverable manner. In the case of a failed update, the device is recommended to be rolling back to the last known good configuration, and it is recommended to have no ability to disable a device's connection to the update server.

A.3.6 Application security

These security capabilities are often taken to improve the security of a "VMS application" often by finding, fixing and preventing security vulnerabilities in VMS and its eco-system. Different techniques are used to surface such security vulnerabilities at different stages of an applications lifecycle such as design, development, deployment, upgrade, maintenance.

A.3.7 Incident management

Incident management provides incident monitoring, prediction, alerting and response. In order to know whether the VMS is operating as expected through the whole infrastructure, continuous monitoring is necessary (e.g., monitoring the real-time performance of servers used in VMSP). This enables systems to capture the service security status, identify abnormal conditions, and provide early warning of security system overloads, breaches, service discontinuity, etc. After the occurrence of security incidents, the problem is identified and the incident is quickly responded to, either automatically or with the intervention of a human administrator. Closed incidents are logged and analysed for possible underlying patterns which can then be proactively addressed.

A.3.8 Cryptography

This capability ensures confidentiality and integrity of data used and exchanged in VMS and its eco-systems. This is the basic method for storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. This capability not only protects VMS data from theft or alteration but can also be used for user authentication, etc.

As a good example for implementing cryptography, guidelines on the selection of cryptographic primitives for IPTV systems are given in [b-ITU-T X.1197 Amd1] and can be applied to multimedia streams in vehicular systems, insofar as those are of the same level of importance/criticality as multimedia streams in non-vehicular IPTV systems. Likewise, for vehicles with 5G connectivity,

[b-ITU-T X.1811] provides further guidance on how to implement the baseline security levels of [b-ITU-T X.1197 Amd1], including but not limited to multimedia streams.

Furthermore, with a DRM solution based on strong, authenticated encryption, meant to allow only legitimate, copyrighted content to be consumed by the infotainment system, only legitimate line-of-sight external multimedia streams would be taken into account by the infotainment and assisted driving system, therefore allowing traffic to proceed without any disruption.

A.3.9 Hardware security

This capability aims at eliminating the vulnerabilities and security weaknesses inherent to VMS hardware, and provides a secure environment for hardware-level implementation. In particular, it has become essential to implement many fundamental cryptographic functions in hardware, such as cryptographic key management, execution of encryption/decryption, and provision of digital signatures and strong authentication, which are importantly utilized for ensuring security in VMS. For that purpose, it is necessary to securely design and verify the operation of related hardware from the hardware design stage, in consideration of possible threats and attacks.

For example, to ensure ECU-level security in the VMS architecture, each implemented ECU is recommended to be protected by HSMs and PUFs, which are typical components of hardware security modules.

A.3.10 General security capabilities

NOTE – The following security capabilities are optional for this Recommendation. However, those capabilities can be effectively utilized for improving VMS security.

– Security assessment and audit

  This capability enables the security evaluation of VMS. It enables an authorized party to verify that a VMS complies with the applicable security requirements. Security assessment or security audit could be performed by the VMS, VSMP or a third party, and security certification could be performed by an authorized third party.

  Appropriate security criteria are implemented to provide a mutual understanding of the security level between the VMS and VMSP.

– Trust model

  A common trust model is necessary for any system where multiple providers cooperate to provide a trustworthy service.

  Because of the highly multi-stakeholder nature of VMS, the VMS environment will need to incorporate an overall trust model. This trust model will enable the creation of islands and/or federations of trusted entities, such that disparate elements of the system will be able to authenticate the identity and authorized rights of other entities and components. Each island or federation of trust will be based on one or more trusted authorities (e.g., a public key infrastructure (PKI) certificate authority).

– Data isolation and protection

  a) Data isolation

     Data isolation may be realized logically or physically, depending on the required isolation granularity and the specific deployment of VMS software and hardware.

  b) Data protection

     Data protection ensures that VMS data and derived data held in a VMSP are appropriately protected so that it can only be accessed or changed as authorized by the VMS. This protection may include some combination of access control lists, integrity verification, error correction/data recovery, encryption and other appropriate mechanisms.

When a VMSP provides storage encryption for VMSs, this function can be client-side encryption (e.g., within a CSP application) or server-side encryption.

– Security coordination

Since different VMSs imply different implementations of security controls, this security capability coordinates heterogeneous security mechanisms to avoid protection conflicts.

Parties playing different roles in the VMS ecosystem have different degrees of control over the physical or virtual resources and services, including the control of security.

For each party, there will be various security mechanisms, including hypervisor isolation, IAM.

Network protection, etc. Security coordination depends on the interoperability and harmonization of diverse security mechanisms.

– Supply chain security

A VMSP uses several suppliers to build their services. Some of these will be VMS industry participants, while others will be traditional information technology (IT) equipment or service suppliers, e.g., hardware manufacturers with no direct relationship with VMS. This capability enables the establishment of a trust relationship between the VMSP and all participants in the supply chain by security activities. These supply chain security activities involve identifying and gathering information about the VMSP's acquired components and services that are used to provide VMSs and enforcing supply chain security policies.

For example, typical supply chain security activities in a VMSP may include:

a) Confirmation of background information about the participants in the supply chain;

b) Validation of hardware, software and services employed by the VMSP;

c) Inspection of the hardware and software purchased by the VMSP to ensure that it was not tampered with while in-transit;

d) Providing mechanisms to verify the provenance of VMS software, for example, code provided by a software vender.

This capability is continuous to cover ongoing system evolution and updates.

– Secure development environment and procedures

This capability is to avoid introduction of insecurity to VMS and its eco-systems during development. A development environment includes people, processes, technology and facilities associated with a system development. The VMS service developer is recommended to assess risks in individual VMS development efforts and establish secure development environments considering:

a) Personnel working in the environment;

b) Applied development methodologies and software and data handling processes;

c) Use of outsourced products and services;

d) Physical and network environment; and

e) Coexistence with other development and operational efforts.

The VMS service developer also needs to determine development environment and associated procedures to mitigate the risks. The procedures are recommended to be disseminated to individuals involved in the development efforts.

Annex B

Personally identifiable information (PII) protection and privacy

(This annex forms an integral part of this Recommendation.)

VMS is recommended to provide end-to-end protection as vehicles become connected and offer more interactive services. More user data and privacy related information need to be protected to ensure confidentiality and integrity of the user data that is stored in the VMS, in the vehicle and the VMS cloud or backend servers.

According to National Institute of Standards and Technology (NIST) of the US, PII is ‘any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means' [b-NIST SP 800-79-2].

There is no single definition of the term "privacy". The meaning of privacy depends on legal, political, societal, cultural and socio-technological contexts.

Generally, informational privacy can be defined as follows:

1) An individual has informational privacy if she/he is protected against the penetration, interference or the access to own data by unauthorized others.

PII protection is one aspect to assure privacy.

VMS might store PII or might function as a gateway to access PII of the vehicle owner, driver and/or further occupants.

B.1 Information sources

VMS comprises multiple information input sources such as:

– Sensors (motion detectors, location detectors, etc.),

– Camera (personalization, feature recognition, etc.)

– Microphone – Audio (might be further used for voice recordings and voice recognition, voice biometrics, etc.)

– Network communication protocols identifiers such as IP address, MAC address, etc.

– Media sources such as USB memory stick, Secure Digital card, external hard disk, etc.

– Third party applications, payment gateways, services, devices, accessories, etc.

VMS stores and share the information with other systems in the vehicle or cloud based on vehicle architecture, regional, legislative, certification requirements.

B.2 Implementation of PII protection: General considerations

Personal data (e.g., in data, text, audio, video or images) is to be protected, as well as any content that users other than the intended customer or any end user (such as remote cloud, stores or processes) using the VMS may request.

There needs to be agreement for data sharing for personal data relating to each customer, the end users and third parties. Any such customer agreement, or any other relevant agreement governing the use of VMS service is to be based on the following criteria:

– Personalized access based on user selection of services and interest

– VMS designed to allow for its use in accordance with the privacy regulatory requirements

– VMS software, hardware and network design it to allow only authenticated access.

– VMS PII and privacy protection is to be designed for private vehicles with one single user, and for shared vehicle with several users.

B.3 Data visibility and transparency

Well-known, highly scrutinized security standards are recommended to be implemented. Proprietary encryption algorithms are recommended to be avoided.

Well-known processes are recommended to be adopted.

Users are recommended to be notified about the data stored /accessible through the VMS. As transparency enhances user acceptance, user notification is recommended to comprise information about data type, purpose of collection, identity of data processing entities and duration of data storage.

B.3.1 Privacy-by-default

It is recommended that users be able to control the limit of data download, as well as to opt-in/opt-out of data download and storage. Opt-out strategies are more privacy-preserving and align better with the principles of privacy-by-default. Therefore, opt-out strategies are recommended.

VMS is recommended to identify the list of use cases that fulfils the data privacy requirements and settings.

Applications might use multiple resources for specific use cases. For example, in the case of location services, Bluetooth, GPS, crowd-sourced Wi-Fi hotspots or cellular tower locations might be used to determine the user's approximate locations. VMS is recommended to provide users with the possibility to turn off specific tracking possibilities. Global settings control might be used to realize this by defining privacy policies for all applications. Alternatively, occupants might be enabled to control data access on a single application level. Privacy controls like PRICON posit approaches, which combine both approaches, can be used. Another option for VMS might be a "Do Not Track" ("DNT") signal that is already used by web browsers. A DNT signal is a HTTP header field indicating user preference for tracking user activities on a service or through cross-site user tracking.

Applications or controls may request to receive e.g., location data only while the application is being used or to allow it at any time. Occupants may choose not to allow this access and are recommended to be able to change their choice at any time in the settings. If applied to a service that operates also within the European Union, the General Data Protection Regulation (GDPR) demands to enable the user to make informed privacy decisions. An informed privacy decision is possible if the decider is aware of the consequences of data disclosure (who gets what data, for what purpose, and under which conditions) or denial (which specific functions are restricted).

If an application has been granted access to certain data, and to use them in background mode, users need to be reminded of their approval and be allowed to change the application's access.

VMS architecture is recommended to be robust to prevent applications from accessing information to which the user has not explicitly granted access permission.

B.4 Data accuracy and data integrity

VMS is recommended to maintain all the aspects of the data, such as data upload, download, communication and deletion in specific manner.

End-to-end security – Full lifecycle protection. Regular code review and rigorous security testing are recommended to be done. Moreover, protection strategies on a broadcasting level, database level and receiver level are recommended to be implemented.

Software security assurance is recommended to be provided in order to prevent loss, inaccuracy, alteration, unavailability or misuse of the data and resources that are used, controlled and protected.

Users are recommended to be allowed to verify PII accuracy and the lawfulness of its processing;

Integrity implies that the consistency, accuracy and trustworthiness of data are maintained over time. Hence, a guard against improper information modification or destruction is recommended to be established. Appropriate measures are recommended to ensure information non-repudiation and authenticity.

In settings, users are recommended to be able to see which applications they have permitted access to certain information, as well as grant or revoke any future access.

Additionally, VMS OS is recommended to provide restrictions that prevent data movement between applications and accounts installed by a trustworthy data management solution and those installed by the user.

Users can request the correction, amendment or deletion of their personally identifiable information if it is inaccurate or if they believe that the processing of their personally identifiable information is in violation of applicable law.

Systems, applications and procedures should be implemented to secure user personally identifiable information, to minimize the risks of theft, damage, loss of information, or unauthorized access or use of information.

Any unauthorized changes to PII in VMS or the cloud are recommended to be detected and notified to the user.

B.5 Confidentiality

Confidentiality consists in preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

B.5.1 Confidentiality impact levels

PII is recommended to be evaluated to determine its confidentiality impact level, so that appropriate safeguards can be applied. Not all PII data stored or created is recommended to be treated equally.

Confidentiality impact levels are recommended to be assessed as low, medium or high depending on identifiability, data sensitivity and obligation to protect according to regulations.

B.5.2 Confidentiality protection

Confidentiality protection is recommended to be realized through the following measures:

– Implementing an access control mechanism using a password to access the data from VMS.

– Multilayer access to high impact confidential PII.

– Multi-level access control from mobile phones, laptops and personal digital devices.

– Encrypting the PII before transmission. Detailed measures are described in clause A.3.8 (Cryptography).

Moreover, risk assessments prior to the deployment of new requirements are recommended to be performed. A continuous risk monitoring mechanism for evaluating changes in the VMS or the identification of new risks associated with the VMS is recommended to be implemented.

B.6 Data anonymization

Data anonymization is the process of irreversibly altering classified data in order to protect PII data subjects.

By anonymizing the data handled in the VMS environment, it is possible to realize a wide range of data analysis and data sharing.

B.7 Data availability

Availability demands ensuring timely and reliable access to and use of information.

Authorized occupants are recommended to be given detailed control over system services use of location information. This includes their ability to turn off the inclusion of location information in information collected by internal applications, navigation search history, and Bluetooth and Wi-Fi access information. If the user signs-in to OEM cloud, functionally necessary applications are granted access by default to OEM cloud. Users are recommended to control each application's access to the cloud in settings.

If PII is accessed remotely by telematics, connected services are recommended to operate with multi-level authentication.

Since data is available by performing various data processing (calculation, statistical processing, etc.) in an encrypted format (for example, using homomorphic encryption), similar data processing can be performed on the data in VMS.

Bibliography

[b-ITU-T X.1197 Amd1] Recommendation ITU-T X.1197 Amd.1 (2019), *Guidelines on Criteria for Selecting Cryptographic Algorithms for IPTV Service and Content Protection, Amendment 1*.

[b-ITU-T X.1811] Recommendation ITU-T X.1811 (2020), *Security Guidelines for Applying Quantum-Safe Algorithms in 5G Systems*.

[b-ETSI WP35] ETSI White Paper 35 (2020), *IPv6 Best Practices, Benefits, Transition Challenges and the Way Forward*. https://www.etsi.org/images/files/ETSIWhitePapers/etsi_WP35_IPv6_Best_Practices_Benefits_Transition_Challenges_and_the_Way_Forward.pdf

[b-IEEE 802.11] IEEE 802.11-2020, *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*.

[b-IETF RFC 2663] IETF RFC 2663 (1999), *IP Network Address Translator (NAT) Terminology and Considerations*.

[b-IETF RFC 8200] IETF RFC 8200 (July 2017), *Internet Protocol, Version 6 (IPv6) Specification.*

[b-IETF RFC 8216] IETF RFC 8216 (2017), *HTTP Live Streaming*.

[b-ISO/IEC 23009-1] ISO/IEC 23009-1:2019, *Information technology – Dynamic adaptive streaming over HTTP (DASH) – Part 1: Media presentation description and segment formats*.

[b-IAB] Internet Architecture Board (IAB) statement on IPv6 address exhaustion (November 2016). https://www.iab.org/2016/11/07/iab-statement-on-ipv6/ [Online].

[b-NIST SP 800-79-2] NIST Special Publication 800-79-2 (2015), *Guidelines for the Authorization of Personal Identity Verification Card Issues (PCI) and Derived PIV Credential Issuers (DPCI)*.

[b-USG OMB] US Office of Management and Budget (November 2020), *Memorandum for heads of executive departments and agencies*. https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf [Online].

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, 2022