International Telecommunication Union

ITU-T Technical Report

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(13 April 2021)

Focus Group on Vehicular Multimedia (FG-VM)

FGVM-02
Architecture of vehicle multimedia systems

Focus Group Technical Report

International Telecommunication Union

Acknowledgement

This Technical Report was prepared under the leadership of Mr. Jun Li, Chair of ITU-T FG-VM (TIAA, China) and Yajun Kou, Chair of ITU-T FG-VM Working Group 2 (Global Fusion Media Technology and Development Co. Ltd, China).

It is based on the contributions of numerous authors who participated in the Focus Group activities. Due credit is given to the following Focus Group participants:

Srinivasagan Ayyappan, Yansong Guo (Great Wall Motors, Co, LTD, China); Yajun Kou, Jun Li (Global Fusion Media Technology and Development Co. Ltd, China); Koji Nakao (National Institute of Information and Communications Technology, Japan); Stiepan A. Kovac (QRCrypto SA; CEuniX.eu Project); Paolo Volpato, Francois Fischer (Huawei Technologies); Latif Ladid (IPv6 Forum); Jonas Walter (Technical University of Darmstadt Institute of Ergonomics & Human Factors); Gaëlle Martin-Cocher (InterDigital Canada, Lte, Canada); Prakash Ranganathan (University of North Dakota); Sébastien Ziegler, Anna Brékine, Cédric Crettaz (Mandat International); and Pradipta Biswas (Indian Institute of Science).

Srinivasagan Ayyappan (Great Wall Motors, Co, LTD, China) served as the main Editor of this Technical Report. Stefano Polidori (Advisor), Mythili Menon (Project Officer), and Carolina Lima (Assistant) served as the FG-VM Secretariat.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

CONTENTS

Page

Page

Page

List of Tables

Page

List of Figures

Page

Technical Report

Architecture of vehicle multimedia systems

Summary

This Technical Report is the output of the ITU-T Focus Group on Vehicle Multimedia. It has been prepared by FG-VM/WG2 during its working sessions of 2019- 2021.

Keywords

ITS, Vehicle, Multimedia, Configuration, Architecture, Security

Technical Report

Architecture of vehicle multimedia systems

1 Scope

This Technical Report describes the architecture of vehicle multimedia system (VMS) and the network architectures for vehicular telematics connectivity services and multimedia streaming services.

2 References

None.

3 Terms and definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 vehicular multimedia networks (VMN) [b-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) [b-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) [b-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).

3.1.4 VMN services (VMNS) [b-ITU-T F.749.3]: The VMNS are the vehicular multimedia services provided by the VMSP to the end-user(s) in the vehicle.

3.1.5 VMN application [b-ITU-T F.749.3]: The VMN application uses the underlying VMS capabilities to consume and present a VMNS to end-user(s) in the vehicle.

3.1.6 network convergence transmission [b-ITU-T F.749.3]: Network convergence transmission is an intelligent transmission technique used by the vehicular multimedia service platform (VMSP) to efficiently and timely deliver the VMN services (VMNS) data to the vehicle multimedia system (VMS) via broadcasting and communication networks.

3.2 Terms defined here

This Technical Report defines the following terms:

3.2.1 zonal gateway: ECU or system through which data is exchanged between any kind of ECUs or systems or interface for sensors, actuators, displays (network difference or signals) in a zone or functional area of the vehicle. It may distribute power. Zone is a local vehicle specific portion of the vehicle. Act as gateway, switch and as smart junction box.

3.2.2 central gateway: Central ECU or system through which data is exchanged between all the ECUs or systems or interface for sensors, actuators, displays (network difference or signals). This is the data bridge of the vehicle. Central gateway transmits and evaluates data between busses of various vehicle domains, such as engine management network, chassis network, Power Train network and diagnostic bus for maintenance.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms.

AGL	Automotive Grade Linux
AM	Amplitude Modulation
APP	Application
BT	Bluetooth
CA	Conditional Access
CCC	Connected Car Consortium
CDR	China Digital Radio
DAB	Digital Audio Broadcast
DLNA	Digital Living Network Alliance
DRM	Digital Rights Management
ECM	Entitlement Control Message
ECU	Electronic Control Unit
EMM	Entitlement Management Message
FG	Focus Group
FM	Frequency Modulation
GNSS	Global Navigation Satellite System
HMI	Human Machine Interface
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LEO	Low Earth Orbit (Satellite)
LTE	Long-Term Evolution
NFC	Near Field Communication
OEM	Original Equipment Manufacturer
OLED	Organic Light Emitting Diode
PII	Personally Identifiable Information
PUF	Physical Unclonable Function
RDS	Radio Data System
RF	Radio Frequency
RTOS	Real Time Operating Systems
V2I	Vehicle-To-Infrastructure
V2P	Vehicle-to-Person
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VM I/P	Vehicle Multimedia System Inputs
VM O/P	Vehicle Multimedia System Outputs
VMN	Vehicular Multimedia Networks

VMNS	Vehicular Multimedia Networks Services
VMSP	Vehicular Multimedia Service Platform
VMS	Vehicular Multimedia System
VMU	Vehicular Multimedia Unit
WG	Working Group

5 Conventions

None.

6 Background

In this Technical Report, the configurations of vehicle multimedia system (VMS) and the reference model of VMS architecture are defined in compliance with the requirements in ITU-T Recommendation F.749.3 [b-ITU-T F.749.3]. The network architectures for vehicular telematics connectivity services and vehicular multimedia streaming services are discussed respectively. Security issues, personally identifiable information (PII) protection and privacy issues are discussed as well.

The rest of the Technical Report is organized as follows. In Chapter 7, the VMS configurations are defined. In Chapter 8, the architecture of vehicular multimedia network (VMN) is overviewed. In Chapter 9, the network architecture for vehicular telematics connectivity services is described. In Chapter 10, the reference model of VMS architecture is defined. In Chapter 11, the reference architecture of VMSP, the reference protocol stack for convergence transmission of multimedia streaming data over heterogeneous networks, and the reference architecture of receivers of in-vehicle devices are described, respectively. In Chapter 12, the VMS security architecture is discussed. In Chapter 13, personally identifiable information (PII) protection and privacy issues are discussed.

7 VMS configuration

7.1 VMS features

VMS features are determined based the following principles.

1) These are User Experience Entertainment and Information Features/Applications to driver and passenger.
2) Market, regional, country specific requirements.
3) Legal, mandatory requirements.
4) It does not describe the vehicle network or domain architecture integration.

7.2 Reference VMS features

The reference VMS features are summarized in Table 1.

Table 1 – Reference VMS features

Features	Sub-features	Configurable
HMI	Display Technology	LED /LCD/ OLED, etc.
	Number of Displays	Front, Central, Rear, multiple, independent, interactive, etc.

Features	Sub-features	Configurable
	Control	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/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	Analog - AM
		Analog - FM
		Analog - Dual Tuner (FM2), FM PD (Phase Diversity), FM BGS (Back Ground Scan)
		Analog - FM- RDS (Radio Data System)
		Digital - DAB1 (Digital Audio Broadcast)
		Digital - DAB2 Maximal-Ratio Combining (MRC)
		Digital Terrestrial Television Broadcasting (DTTD)
		In Band On Channel technologies (IBOC) - HD Radio, Digital Radio Mondiale
		Convergent Digital Radio (CDR)
		and many more….
	Satellite	Satellite Digital Audio Radio Service (SDARS) Satellite Audio/Video Services (e.g., Satellite Audio/Video Streaming Service)
External Network Connectivity	Cellular networks	3G/4G/5G
	LEO Satellites	Low earth orbit bi-directional communication networks
	Satellites bi-directional	High earth orbit bi-directional communication networks
	V2X	V2V, V2I, V2P, V2X (e.g., LTE-V/5G PC5)
	Wireless local area networks	IEEE 802.11 Hotspots
In-vehicle Mobile Connectivity		Bluetooth hands-free calls and music
		IEEE 802.11
		Third-party vehicle interface applications
		Wi-Fi Alliance Miracast, CCC Mirror Link, DLNA, NFC, and Wi-Fi direct, and etc.
Telematics Configurations	Remote	Remote monitoring, Control, Vehicle data transfer
	Calls	Emergency Call, Information Call, Breakdown Call

Features	Sub-features	Configurable
Online App Stores/Suites	APP Store	New features downloaded
	Theme Marketplace	Theme Skin Replacement
OTA		Software (SOTA) / Firmware Over the Air (FOTA)
Media	Audio	Normal and High fidelity
	Image	In different formats
	Video	Normal video (High Definition (HD), Full HD (FHD), 4K,8K), Augmented Reality (AR), Virtual Reality (VR), Mixed Reality (MR)
Navigation	Local navigation	
	Cloud navigation	Data from Telematics box (3G/4G/5G/ cellular networks) modem / User mobile data
	Real-time traffic	Traffic Message Channel (TMC) / Transport Protocol Experts Group (TPEG) / Real Time Traffic Centre (RTIC), proprietary technology, and etc.
	Services	Navigation services such as 3D map, HD map, Parking, Fuel Stations, real time weather, and etc.
	Advance features	Intelligent travel applications such as calendar, planners
Voice Recognition (VR)	Local VR and Cloud VR	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 Speakers configurations tweeter (treble speaker) / woofer (bass speaker) / full range speakers
Security		Identity and Access Management, Authentication, Authorization and Transaction Audit
		Network Security
		Operational Security
		Application Security
		Software and Firmware Updates
		Hardware Security
		Cryptography security
Privacy		General Data Protection Considerations
		Personal Information Protection
		Data visibility protection
		Confidentiality, Integrity, and Availability

Features	Sub-features	Configurable
Intelligent Features	Driver Monitoring System (DMS)	Fatigue, Expression and Emotion Recognition
	Health	Bluetooth - Heart beat 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

7.3 VMS configuration

VMS configurations are defined by the following principles.

1) VMS configuration defines standalone requirements for Entertainment and Information display to driver and passenger.
2) Defined in the level of features and functions.
3) Hardware components within the configurations
4) Multiple Configurations possible
5) OEM built, After Market plug-ins. Highly variable.
6) It does not describe the vehicle network or domain architecture integration.

7.3.1 Deciding factors

VMS configurations are determined based on the following deciding factors.

1) Usage requirements
2) Features, Functional requirements
3) Interface requirements
4) Cost requirements
5) Benchmarked requirements
6) etc.

8 Overall architecture of vehicular multimedia network

The overall architecture of vehicular multimedia network (VMN) is illustrated in Figure 1, which consists of cloud service platforms, heterogeneous networks, and in-vehicle devices. For vehicular telematics connectivity services, the conventional broadcast or communication schemes may be used to fulfil the service requirements. For vehicular multimedia streaming services, a convergence transmission scheme is used to improve the transmission efficiency of multimedia streaming services over heterogeneous networks, i.e., satellite broadcast networks and mobile communication networks.

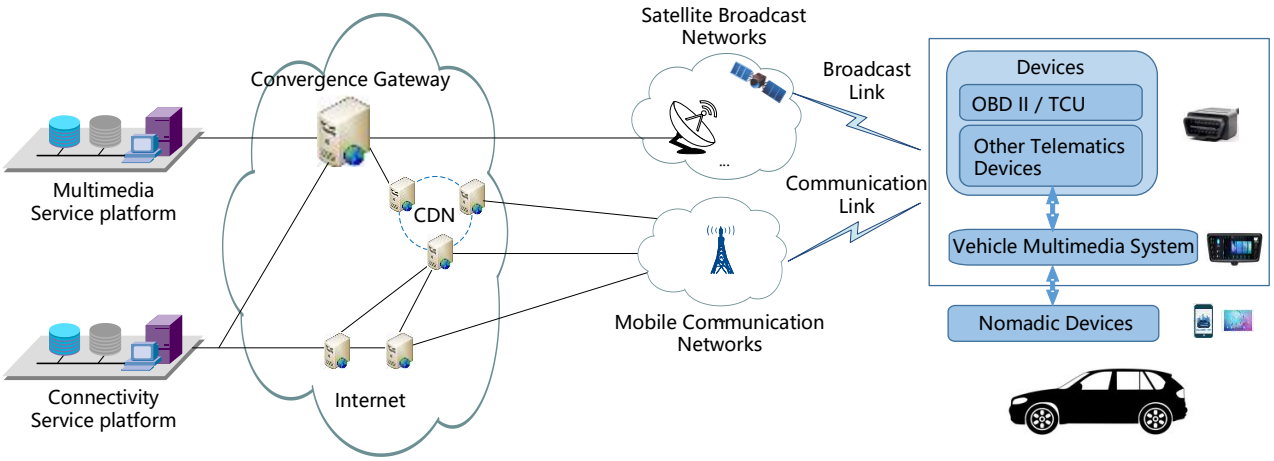

Figure 1 – Overall architecture of vehicular multimedia network

9 Network architecture for vehicular telematics connectivity services

The network architecture for vehicular telematics connectivity services is described with its components, applications, and technologies. Firstly, the deciding factors of the network architecture for vehicular telematics connectivity services are discussed. Secondly, the connected vehicle landscape is given. Lastly, the foundation architecture for vehicular telematics connectivity services is defined.

9.1 Defining factors

9.1.1 Media entertainment

1) In-vehicle Entertainment

   VMS services. Audio, Video, data services

2) Media Store

   Accessed by VMS from cloud.

3) Periodic Content updates

   Accessed by VMS from cloud

9.1.2 User access control

9.1.3 Captive portal

1) Accessed by VMS.

   It is one of the authoritative identity sources supported by the connectivity services provider system. It is an active authentication method where users authenticate onto the network using VMS user authentication. Typically use captive portal to require authentication to access the internet or to access restricted internal resources; can optionally configure guest access to resources. After the system authenticates captive portal users, it handles their user traffic according to access control rules. Captive portal also records failed authentication attempts. A failed attempt does not add a new user to the list of users in the database. The authentication data gained from captive portal can be used for user awareness and user control.

9.1.4 Bandwidth control

1) VMS services

Bandwidth Manager helps to control and limit Internet usage, download and upload, data traffic for VMS.

VMS can be limited with specified time and quota per session, day time when access is allowed and set to logout after inactivity.

9.1.5 Local telecommunications regulations control

1) Accessed by VMS

   It defines the country/regional specific Department of Telecommunication regulations and control.

9.1.6 Network access services

1) 2G/3G/4G/5G Backbone

   Accessed by VMS.

2) Internet Access

   VMS service by accessing the network

3) Outbound/Inbound SMS

   VMS service by accessing the network

4) Voice, Emergency Call (E-Call), Information Call (I-Call)

   VMS service by accessing the network

9.1.7 Vehicle tracking

Below are VMS services by accessing the network.

1) Tracking vehicle using GNSS
2) Securing vehicle using immobilizer trigger
3) Driver behaviour log
4) Vehicle status record

9.1.8 Centralized management

Below are VMS services by accessing the network.

1) Real Time Analytics
2) Centralized Wi-Fi /network /Infotainment management

9.2 Connected vehicle landscape

9.2.1 Major components

1) Telematics Control Unit (TCU) / On Board Diagnostics (OBD) II solutions
2) Connectivity solutions
3) Customer Relationship Management (CRM) Applications
4) Business Intelligence

9.2.2 Services provided by these components

1) Engine, Oil Status, Charge Status

2) Vehicle location
3) Driving behaviour
4) In-vehicle Internet
5) Distribution Platform
6) Content providing

9.3 Reference architecture for vehicular telematics connectivity services

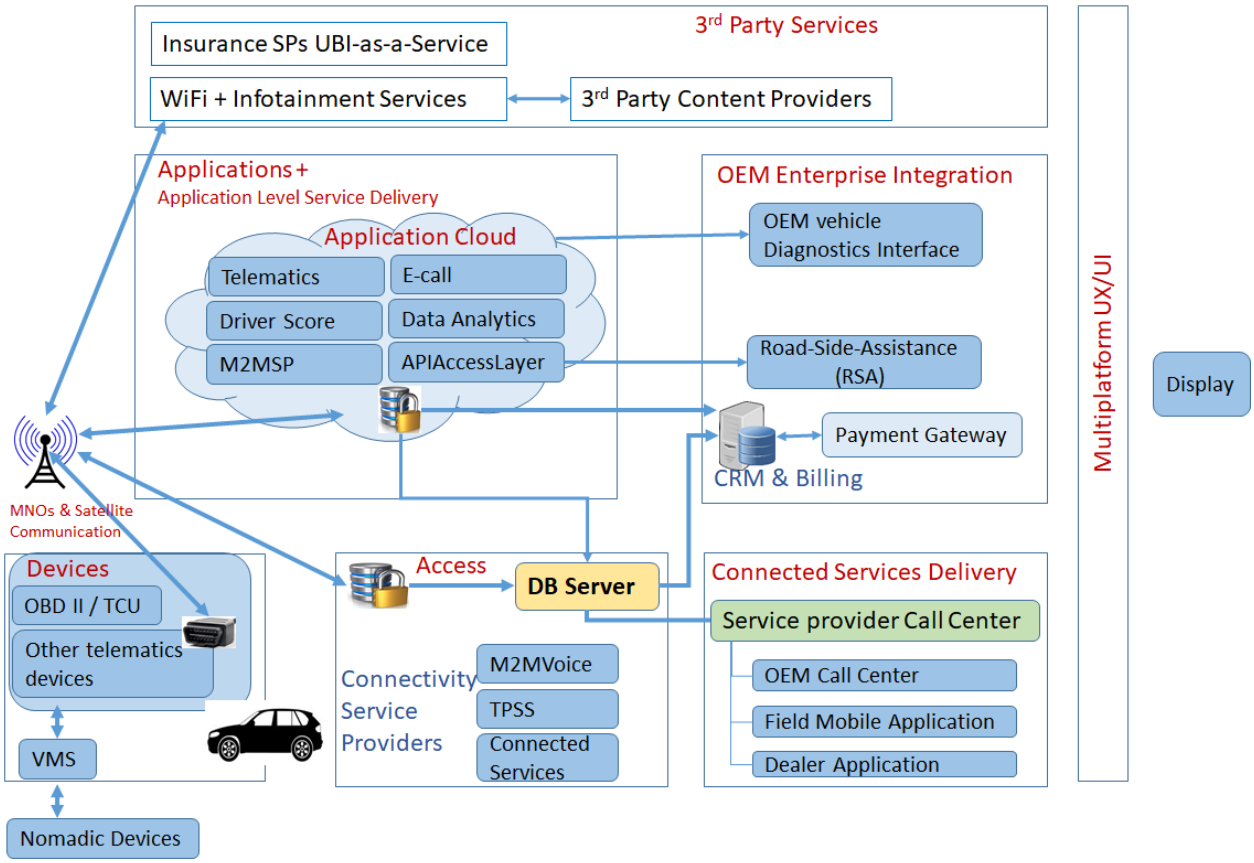

Figure 2 – Reference architecture of vehicular telematics connectivity services

9.3.1 Devices

Devices are connected to Mobile Network Operators (MNOs)

1) Telematics Control Unit (TCU) / On Board Diagnostics Devices (OBD) II
2) Devices as per global/regional/country specific regulation

9.3.2 Access

MNOs and Application Cloud access Database server of telematics service provider

1) Database Server
2) Solution Implementer Control systems
3) Access to telecom operator services
   a) Machine2Machine Services Providers(M2MSP)
   b) Local regulation requirements

TPSS: A Time-based Positioning Scheme for Sensor Networks with Short Range Beacons

9.3.3 Service providers service delivery

Access Database Servers feed to telematics service provider's call centre

Call centre services

1) OEM call centre
2) Field Mobile App
3) Dealer Application

9.3.4 Applications and application level service delivery

Application Cloud provider below services to MNOs and to database server

1) Telematics
2) Driver Score
3) Machine-to-Machine Service Providers (M2MSP)
4) Emergency / Breakdown/Information Call (e/b/I Call)
5) Data Analytics
6) API Access Layer

9.3.5 OEM enterprise integration

1) OEM Vehicle Diagnostics Interface access the application cloud
2) Telematics service provider provides Customer Relationship Management (CRM) and Billing through database server
3) Data Analytics & e/b/I –Call to Road-side-Assistance (RSA)
4) Payment Gateway which is based on OEM or service provider's strategy

9.3.6 Third party services

Information accessing Application cloud and MNOs

1) 3rd party Content providers
2) Wi-Fi + Infotainment Services
3) Insurance Service Providers (SP)/Usage Based Insurance (UBI)
4) 3rd Party Services

9.3.7 Mobile network operators (MNOs)

MNOs facilitate Third party services, application cloud, Telematics service providers data communication and to access the database by Vehicle Multimedia Service (VMS) Devices.

10 VMS Architecture

1) Physical and logical requirements
2) Defines in the level of Sub-systems and Systems
3) Network Interfaces

10.1 Definitions

Definition of VMS **Core**, **Associated** and **Shared** features & functions

10.1.1 Core functions

Physical, Functional and logical data processed by VMS

Example:

Tuner, Media, Display functions etc.

10.1.1.1 Associated functions

Receive functional / Logical data from other systems, sub-systems to display data, status only

Examples:

1) Camera Feed from Rear vehicle camera,
2) eCall information display initiated by accident

10.1.1.2 Shared functions

Sharing Physical, Functional and logical data and controls

Examples:

1) Heating, Ventilation and Air conditioning (HVAC) controls are through VMU, data processed by HVAC. Status display in VMS.
2) V2X data received, processed by ADAS /other ECUs but Navigation Map layout integration done by VMS

10.1.2 VMS architecture deciding factors

1) Technical requirements, advancement
2) Operating System, memory, hardware requirements
3) Features, Functional, sub-systems, logical and physical requirements
4) Interface requirements
5) Cost requirements
6) Usage requirements
7) Benchmarked requirements
8) Standard compliance, including SDO directions (e.g., recommendations for advancement in networking)
9) etc.

10.1.3 Reference model of VMS architecture

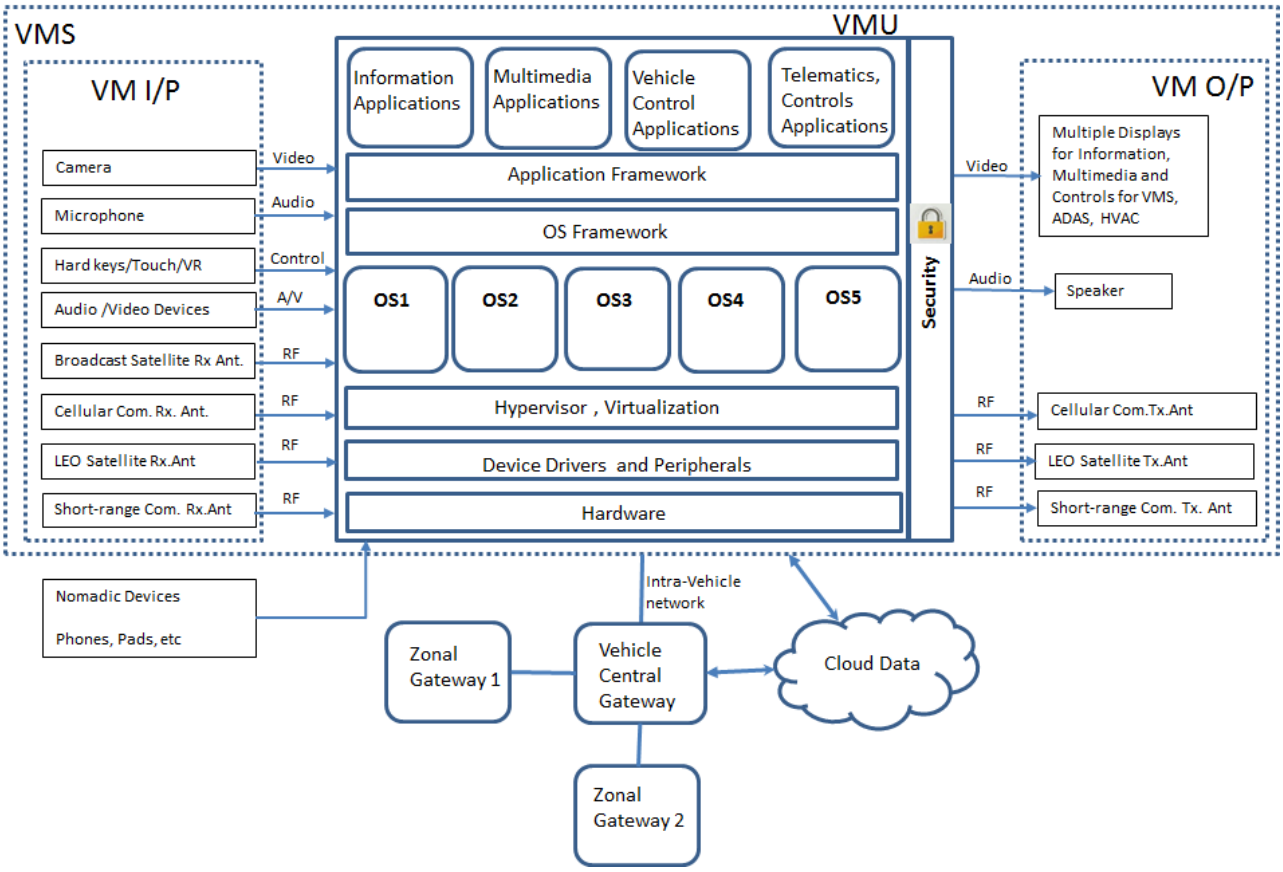

Figure 3 – Reference architecture of VMS

10.1.3.1 Applications

1) Information application: Instrument cluster, head up displays, navigation, weather
2) Multimedia application: Tuner, media, HMI, VR, navigation
3) Vehicle control: ADAS, HVAC, connected cars
4) Telematics: Remote control, diagnostics, data access
5) Front, rear display applications
6) Audio, video control applications

10.1.3.2 Application framework

To access, control the Applications such as Java script, HTML5, Flash Air, X11, Win32.

10.1.3.3 OS framework

Handling System Services, proprietary framework of OEM, VMS developers

10.1.3.4 OS

QNX RTOS and Microkernel, Linux kernel, AGL, Android Automotive OS, VxWorks RTOS, Windows CE, INTEGRITY etc.

10.1.3.5 Devices and peripherals

Network and Internal and External Peripherals Control

10.1.3.6 Hypervisor and virtualization

Single high-power processor to handle sharing the resources to support multiple OSs, processing

10.1.3.7 Device drivers

Vehicle network, Audio & Video drivers, Display drivers, vehicle network interface drivers, inter-processors such as inter-processor protocol drivers, intra-processor protocol drivers, wireless system drivers, sensor & actuators interface drivers.

10.1.3.8 Hardware

Processors, Memory, Sensors, Cameras, Radars and Interface Controllers

10.1.3.9 Cloud data

1) Online Voice Recognition for Natural Language Understanding data base access
2) Big data for telematics services
3) Remote Diagnostics, vehicle services database
4) Over-The-Air (OTA) software update
5) Emergency Call (E-Call), Breakdown Call (B-Call), Information Call (I-Call) services
6) Payment gateway services
7) Cloud internet services
8) Online Navigation, HD map, Traffic information
9) Infotainment services, Applications
10) Car Connectivity- V2V, V2I, V2X

11 Network architecture for vehicular multimedia streaming services

The network architecture for vehicular multimedia streaming services consists of vehicular multimedia service platform (VMSP) in the cloud, heterogeneous networks, and in-vehicle devices. In this chapter, the reference architecture of VMSP, the reference protocol stack for convergence transmission of multimedia streaming data over heterogeneous networks, and the reference architecture of receivers of in-vehicle devices are described, respectively.

11.1 Reference architecture of VMSP

The VMSP consists of content server, license server (optional), and conditional access server (optional). Its reference architecture is illustrated in Figure 4.

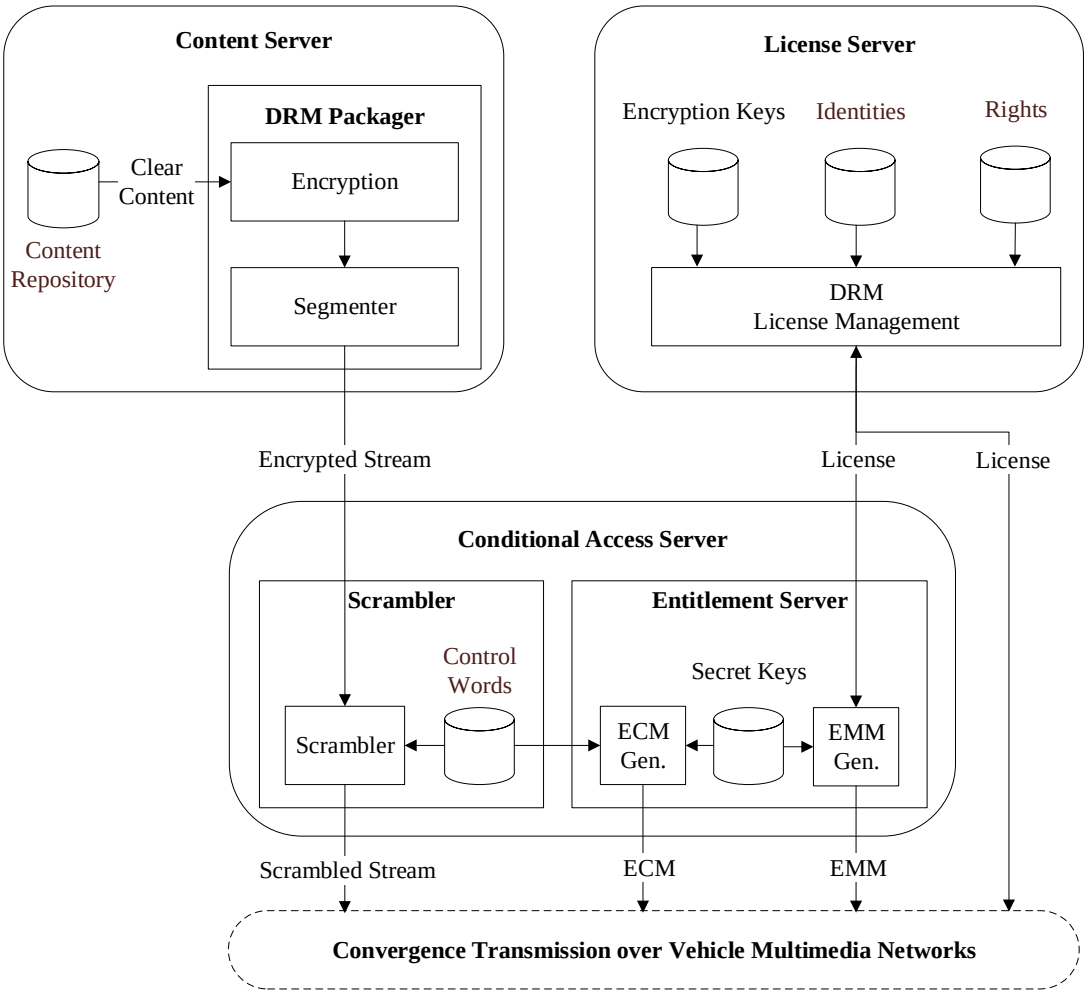

Figure 4 – Reference architecture of VMSP

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 which interfaces to the DRM server. The DRM packager encrypts and packages the multimedia contents for streaming over VMN. The license server is used to manage the creation, modification, and revocation of the DRM licenses. The DRM license contains identities, rights specification, and encryption keys. Usually, DRM clients could acquire their DRM licenses from the license server by using mobile communication network connections. The candidate packaging schemes for streaming in VMN include MPEG-DASH [b-ISO/IEC 23009-1:2019] 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 the 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 some exceptions. (1) When a user drives to a place with no cell phone coverage, DRM licenses cannot be acquired through any mobile communication network. In this case, DRM licenses could be integrated into EMMs and be delivered to the user over satellite networks. Thus, the persistence of service 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.

11.2 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 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 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 streaming services over VMN, where the great majority of media contents are delivered to massive users via broadcast networks and mobile communication networks are used only to recover dropped packets in 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 WIFI-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 5.

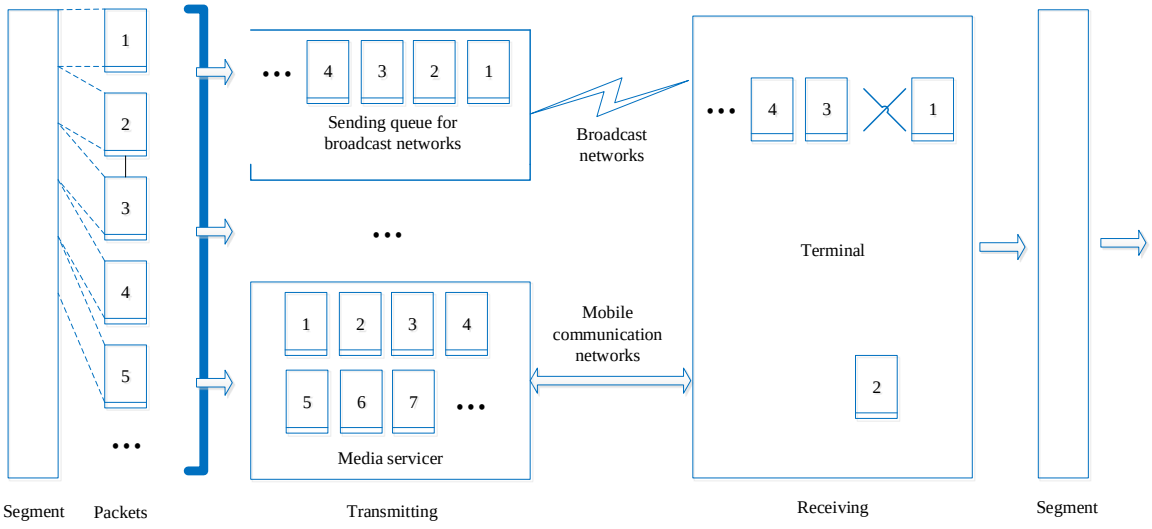

Figure 5 – The processing of convergence transmission

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 protocol stack for convergence transmission of multimedia streaming data over VMN is given in Figure 6. 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.

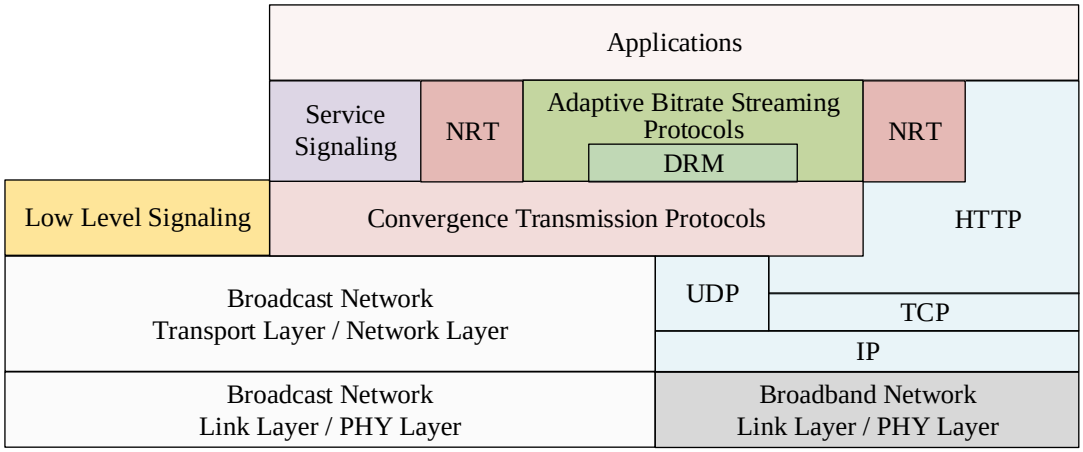

Figure 6 – The protocol stack for convergence transmission

The general assumption is that the networking architecture may be based on both versions of the IP protocol (IPv4 and IPv6). As further explained in 11.4, IPv6 may be considered as the preferred choice for future readiness.

11.3 Reference architecture of receivers

Reference architecture of receivers of in-vehicle devices is given in Figure 7, where the following functions are identified.

1) Broadcast connections and broadband connections that provide the connectivity for the receiver to receive signaling and data.
2) Convergence Transmission Protocols/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 (i.e., DASH/HLS) resources for multimedia streaming services.
3) Low-Level Signaling: Signaling delivered over broadcast networks that enable the receiver to build a basic service list and bootstrap the discovery of the service signaling for each multimedia streaming service.
4) Service Signaling: Service-related signaling that enables the receiver to discover and access multimedia streaming services and their content components.
5) Cache: Temporary storage and handling of the manifests, initialization segments and media segments whose reception are facilitated by service signaling.
6) 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.
7) 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.
8) Applications: 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.

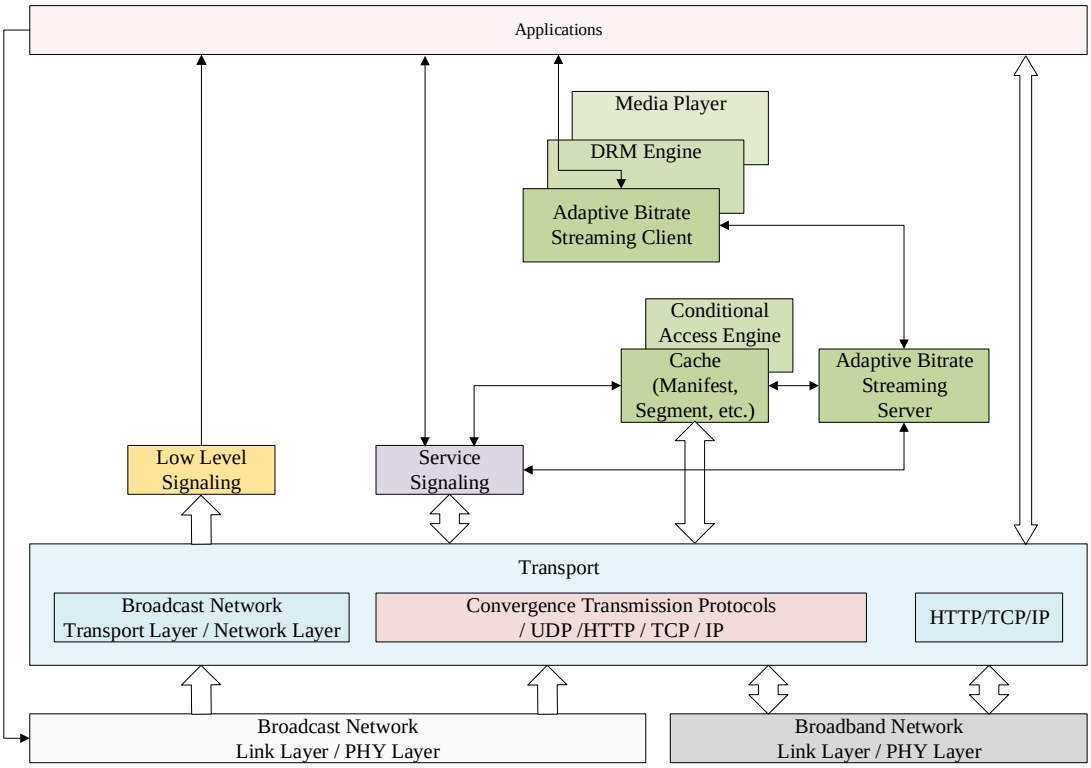

Figure 7 – Reference architecture of receivers of in-vehicle devices

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

1) The application requests a pre-configured service list in low level signaling. 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.

2) The application uses the service signaling entry point information carried in the service list for the selected service to provide access information to the Convergence Transmission Protocols/UDP /HTTP/TCP/IP stack to retrieve the service signaling. Service signaling is delivered to the application.

3) By using the service signaling, the application provides access information to the Convergence Transmission Protocols/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.

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

5) 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.

11.4 Suggestions for the networking architecture

Figure 6 showed the protocol stack for convergence transmission of multimedia streaming data over heterogeneous networks. The core of the protocol stack is IP (Internet Protocol).

While IPv4 and IPv6 can both be considered, 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:

1) The IETF clearly advises other Standards Development Organizations (SDOs) to prefer IPv6 [b-IAB]. As a result, standardization work should assume IPv6.

2) The IPv4 address space 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.

3) 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.

4) The 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 RFC2663] 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 growth and traffic growth are much faster than IPv4's. This means that, with all things considered, the collective wisdom of the industry has selected IPv6 for the future [b-ETSI WP35].

12 VMS Security

12.1 Overview

The interactions between the VMS and the other components involved in the security of a car (typically ECU) should be limited to the shared functions mentioned above in this Technical Report. Indeed, the VMS should not badly influence the functions of the other components ensuring the required security of a car, notably in the case of an autonomous driving.

VMS should 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 user data which is stored in VMS in the vehicle and VMS cloud (VMSP) or backend servers. Personally identifiable information (PII) protection is described in Chapter 13.

Regarding VMS security, assumed threats to VMS and its eco-system are summarized in 12.2 and security capabilities against threats are provided in 12.3 as an informative reference.

12.2 Assumed threats to VMS and its ecosystem

12.2.1 Threats regarding vehicle 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:

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

2) Services provided by VMSP being disrupted

3) Data held on servers in VMSP being lost or compromised

12.2.2 Threats to vehicles regarding their communication channels

Vehicle communication includes external communications through Cellular, LEO satellite, Broadcast and short-range networks. Channels used in the above communications may be targets of attacks like spoofing, eavesdropping, manipulating messages, and so on. The following threats can be identified in relation to communication channels:

1) Unauthorized manipulation, deletion or other amendments to vehicle-held code/data
2) VM interfaces can be used to gain access to further (intelligent) infrastructure within the vehicle (e.g., ECU unrelated to VMS)
3) Use of untrusted/unreliable messages and session hijacking/replay attacks
4) As VM applications can be updated using over the air, those attacks can apply to VM as well.
5) Information disclosure

   See ITU-T Recommendation F.749.3 [b-ITU-T F.749.3], Chapter 9.
6) Denial of service attacks

   VM itself may not have access to critical infrastructure within the vehicle, but can serve as gateway for those attacks.
7) 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.
8) Malwares 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 employ malwares.
9) 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.

12.2.3 Threats to vehicles regarding their update procedures

There are two ways to update vehicle systems, e.g., wired update through 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:

1) 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 using fabricating system update programs or compromised firmware.

The software can be manipulated before the update process, although the update process is intact. Software provider creates/prepares their software for the update and the software is delivered to the target systems which 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, the cryptographic materials such as cryptographic keys and certificates used in the software update can be compromised and consequently it may cause invalid software update.

2) Denial of service and denial of a legitimate update

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

12.2.4 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 which are led by additional interfaces. The following threats can be identified in relation to external connectivity and connections:

1) 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.

2) Hosted third-party software

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

3) Devices connected to external interfaces

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

12.3 Security capabilities based on identified threats

12.3.1 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.

12.3.2 Interface security

This capability secures interfaces open to VMS developers and/or other contracted VMSP (Vehicle Multimedia Service Platform) 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, digital signature, etc.

12.3.3 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.

12.3.4 Operational security

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

This operational security capability includes:

1) Defining sets of security policies and security activities such as configuration management, patch upgrade, security assessment, incident response;
2) 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.

12.3.5 Software and firmware updates

Secure OTA updates need to conform to baseline security standards. They should take 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) should be designed, implemented and operated.

In the development of VMS service, mechanism for updating software and firmware of VMS should be designed and implemented as a basic function. The mechanism for rolling back software and firmware should also be designed and implemented when failed its update.

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

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

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

12.3.6 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.

12.3.7 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 analyzed for possible underlying patterns which can then be proactively addressed.

12.3.8 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 and so on.

As a good example for implementing cryptography, guidelines on the selection of cryptographic primitives for IPTV systems are given in ITU-T Recommendation X.1197 Amd1 [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, ITU-T Recommendation X.1811 [b-ITU-T X.1811] provides further guidance on how to implement the baseline security levels of ITU-T X.1197 Amd1 [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 legit, copyrighted content to be consumed by the infotainment system, only legit 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.

12.3.9 Hardware security

This capability is aiming to eliminate the vulnerabilities and security weaknesses inherent in the hardware used in VMS 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 in consideration of possible threats and attacks from the hardware design stage.

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

12.3.10 General security capabilities

Note: the following security capabilities may not be used for this Technical Report. However, those capabilities can be effectively utilized for improving security of VMS.

1) 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.

2) 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).

3) 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.

4) 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.

5) 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.

6) 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 should 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 should be disseminated to individuals involved in the development efforts.

13 Personally identifiable information (PII) protection and privacy

VMS should 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 user data which is stored in VMS in the vehicle and 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’ (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.

13.1 Information sources

VMS comprises multiple information input sources such as,

1) Sensors (motion detectors, location detectors, etc.),
2) Camera (personalization, face recognition, etc.)
3) Microphone – Audio (might be further used for voice recordings and voice recognition, voice biometrics, etc.)
4) Network communication protocols identifiers such as IP address, MAC address, etc.
5) Media sources such as USB/SD card, External Hard Disk etc.
6) 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.

13.2 Implementation of PII protection: General considerations

Personal data in formats such as data, text, audio, video, images and other content that user than intended customer, or requested by any end user such as remote cloud, stores or processes using the VMS systems to be protected.

There need to be agreement for data sharing for personal data relating to that customer, its end users or third parties. Any such Customer Agreement, or any other relevant agreement governing the use of VMS service to be based on below criteria.

1) Personalized access based on user selection of services and interest
2) VMS designed to allow for its use as per difference privacy regulatory requirements
3) VMS software, hardware and network design allow only authenticated access.
4) VMS PII and privacy protection designed for private vehicle with one single user and shared vehicle with multi users

13.3 Data visibility and transparency

Well known, highly scrutinized security standards should be implemented. Proprietary encryption algorithms should be avoided.

Well-known processes should be adopted.

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

13.3.1 Privacy-by-default

User should have control to limit the data download and option opt-in /opt-out of the data download and storing. Opt-out strategies are more privacy-preserving and align better with the principles of privacy-by-default. Therefore, opt-out strategies are recommended.

VMS should 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 should 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. Another option for VMS might be a "Do Not Track" ("DNT") signal which 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 should be able to change their choice at any time in the settings. If applied to a service which operates also within the EU, 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 which data for which purpose and under which conditions) or denial (which specific functions are restricted).

If applications granted access to use a certain data point, at any time make use of this permission in background mode, users need to be reminded of their approval and may change an application's access

VMS architecture should be robust to prevent applications from accessing only that information the user has explicitly granted his/her permission for.

13.4 Data accuracy and data integrity

VMS should maintain all the aspects of the data, such as, data upload, download, communication, deletion in specific manner.

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

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

User should 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 should be established. Appropriate measures should ensure information non-repudiation and authenticity.

In settings, users should 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 should provide restrictions that prevent data movement between applications and accounts installed by an effective Data Management solution and those installed by user.

User 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.

Implement systems, applications and procedures 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 Cloud should be detected and notified to user.

13.5 Confidentiality

Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

13.5.1 Confidentiality impact levels

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

Confidentiality impact levels should be assessed as low, medium and high based on identifiability, data sensitivity, obligation to protect according to regulations.

13.5.2 Confidentiality protection

Confidentiality protection should be realized by the following measures:

1) Implementing access control mechanism by pass code to access the data from VMS.
2) Multilayer access to high impact confidential PII.
3) Multi-level access control from mobile phones, laptops and Personal Digital devices.
4) Encrypting the PII before transmission. Detailed measures are described in 12.3.9 (Cryptography).

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

13.6 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.

13.7 Data availability

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

Authorized occupants should 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 should control each Applications access to the cloud in settings.

If PII are accessed remotely by telematics, connected services should operate with multi-level authentications.

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

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

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

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

[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-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].

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

[b-ETSI WP35] ETSI White Paper 35 (August 2020), *IPv6 Best Practices, Benefits, Transition Challenges and the Way Forward*.

[b-ITU-T X.1197 Amd1] ITU-T X.1197 Amd.1 (2019), *Guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection*.

[b-ITU-T X.1811] ITU-T X.1811 (2020), *Security guidelines for applying quantum-safe algorithms in 5G systems*.