



INTERNATIONAL TELECOMMUNICATION UNION

**TELECOMMUNICATION
STANDARDIZATION SECTOR**

STUDY PERIOD 2017-2020

SG16-TD393/WP2
STUDY GROUP 16
Original: English
Question(s): 27/16

Online, 19-30 April 2021

TD
Source: Editor F.VM-VMA

Title: [Clean] F.VM-VMA "Architecture of vehicular multimedia systems" (New): Initial draft (Online, 19-30 April 2021)

Purpose: Admin

Contact: Mr Yajun Kou
TIAA, China
E-mail: yajun.kou@gvmedia.com.cn
Contact: Mr Srinivasagan Ayyappan
TIAA, China
E-mail: asrinivasagan@gmail.com
Keywords: Vehicular multimedia systems; architecture

Abstract: This document contains updates to the initial draft of ITU-T F.VM-VMA "Architecture of vehicular multimedia systems" (Online, 4-5 March 2021)

This document contains updates to the initial draft in SG16 of the new work item ITU-T F.VM-VMA "Architecture of vehicular multimedia systems" and is based to the agreed 1st baseline text that was posted as Q27/16 document: [[Q27/16-DOC5\(210304\)](#)].

NOTE – Editorial adjustments performed by TSB. Formatting changes accepted for better readability.

CONTENTS

	Page
1	Scope.....5
2	References.....5
3	Terms and definitions5
3.1	Terms defined elsewhere5
3.2	Terms defined in this Recommendation5
4	Abbreviations and acronyms.....6
5	Conventions8
6	Background.....8
7	VMS features and configurations8
7.1	VMS features8
7.2	VMS configurations8
7.2.1	Deciding factors8
7.3	List of VMS features9
8	Vehicle Multimedia Network Ecosystem..... 11
9	Network architecture for vehicular telematics connectivity services 11
9.1	Defining factors 11
9.1.1	Media entertainment..... 11
9.1.2	User access control..... 12
9.1.3	Captive portal 12
9.1.4	Bandwidth control 12
9.1.5	Local telecommunications regulations control..... 12
9.1.6	Network access services 12
9.1.7	Vehicle tracking 12
9.1.8	Centralized management 13
9.2	Connected vehicle landscape 13
9.2.1	Major components 13
9.2.2	Services provided by these components..... 13
9.3	Reference architecture for vehicular telematics connectivity services..... 13
9.3.1	Devices 14
9.3.2	Access..... 15
9.3.3	Service providers service delivery 15
9.3.4	Applications and application-level service delivery..... 15
9.3.5	OEM enterprise integration 16
9.3.6	Third party services 17

	Page
9.3.7	Mobile network operators 17
10	VMS architecture 17
10.1	Definitions 17
10.1.1	Core functions 17
10.1.2	Associated functions..... 17
10.1.3	Shared functions 17
10.2	Deciding factors..... 17
10.3	Reference model of VMS architecture 18
10.3.1	Applications..... 18
10.3.2	Application framework..... 19
10.3.3	OS framework 19
10.3.4	OS..... 19
10.3.5	Hypervisor and virtualization 19
10.3.6	Device drivers and peripherals 19
10.3.7	Hardware 19
10.3.8	Cloud data,..... 19
11	Network architecture for vehicular multimedia streaming services 19
11.1	Reference architecture of VMSP 19
11.2	Reference protocol stack for convergence transmission 21
11.3	Reference architecture of receivers 22
11.4	Suggestions for the networking architecture 23
12	VMS Security..... 24
12.1	Overview..... 24
12.2	Assumed threats to VMS and its ecosystem..... 24
12.2.1	Threats regarding vehicle multimedia service platform (VMSP) 24
12.2.2	Threats to vehicles regarding their communication channels 25
12.2.3	Threats to vehicles regarding their update procedures 25
12.2.4	Threats to vehicles regarding their external connectivity and connections 26
12.3	Security capabilities based on identified threats..... 26
12.3.1	Identity and access management (IAM), authentication, authorization and transaction audit..... 26
12.3.2	Interface security 27
12.3.3	Network security 27
12.3.4	Operational security 27
12.3.5	Software and firmware updates 27
12.3.6	Application security 28
12.3.7	Incident management 28

	Page
12.3.8 Cryptography	28
12.3.9 Hardware security	28
12.3.10 General security capabilities	29
13 Personally identifiable information (PII) protection and privacy	30
13.1 Information sources	31
13.2 Implementation of PII protection: General considerations.....	31
13.3 Data visibility and transparency	31
13.3.1 Privacy-by-default	31
13.4 Data accuracy and data integrity.....	32
13.5 Confidentiality	33
13.5.1 Confidentiality impact levels.....	33
13.5.2 Confidentiality protection.....	33
13.6 Data anonymization	33
13.7 Data availability.....	33
Bibliography.....	34

List of Tables

	Page
Table 1 – Reference VMS features	9

List of Figures

	Page
Figure 1 – Vehicular multimedia network ecosystem.....	11
Figure 2 – Reference architecture of vehicular telematics connectivity services	14
Figure 3 – Reference model of VMS architecture	18
Figure 4 – Reference architecture of VMSP	20
Figure 5 – The processing of convergence transmission	21
Figure 6 – The protocol stack for convergence transmission.....	22
Figure 7 – Reference architecture of receivers of in-vehicle devices	23

Draft new ITU-T F.VM-VMA

Architecture of vehicle multimedia systems

AAP Summary

[To be provided before Consent]

Summary

[Mandatory, to be provided before Consent].

Keywords

Vehicular multimedia systems; architecture

1 Scope

This Recommendation 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 Recommendation used 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 in this Recommendation

This Recommendation 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. Also 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 Recommendation uses the following abbreviations and acronyms.

AM	Amplitude modulation
ANC	Active noise cancellation
API	Application programming interface
APP	Application
AR	Augmented reality
AVM	Around view monitoring
bCall	Breakdown call
BGS	Background scan
CA	Conditional access
CCC	Connected car consortium
CDR	Convergent digital radio
CRM	Customer relationship management
DAB	Digital audio broadcasting
DLNA	Digital living network alliance
DMS	Driver monitoring system
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
GNSS	Global navigation satellite system
HEO	High earth orbit
HMI	Human machine interface
HVAC	Heating, ventilation and air conditioning
IBOC	In-band on-channel
iCall	Information call
IoT	Internet of Things

LCD	Liquid crystal display
LED	Light emitting diode
LEO	Low earth orbit
LTE	Long-term evolution
MNOs	Mobile network operators
MR	Mixed reality
OBD	On-board diagnostics
OEM	Original equipment manufacturer
OLED	Organic light emitting diode
OS	Operating system
PD	Phase diversity
PII	Personally identifiable information
PUF	Physical unclonable function
RDS	Radio data system
RF	Radio frequency
RSA	Roadside assistance
RTOS	Real time operating system
RVC	Rear view camera
SIM	Subscriber identity module
TMC	Traffic message channel
TPEG	Transport protocol experts group
TPS	Time-based positioning scheme
UBI	Usage-based insurance
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
VR	Virtual reality

5 Conventions

None. There are no conventions but should is used..

6 Background

In this Recommendation, 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 Recommendation is organized as follows. In clause 7, the VMS configurations are defined. In clause 8, the vehicular multimedia network (VMN) ecosystem is overviewed. In clause 9, the network architecture for vehicular telematics connectivity services is described. In clause 10, the reference model of VMS architecture is defined. In clause 11, the reference architecture of vehicular multimedia service platform (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 clause 12, the VMS security architecture is discussed. In clause 13, personally identifiable information (PII) protection and privacy issues are discussed.

7 VMS features and configurations

7.1 VMS features

VMS features are determined based on the following principles.

- User experience, entertainment and information features/applications to driver and passenger.
- Market, regional, country specific requirements.
- Legal, mandatory requirements.

However, VMS features do not describe the vehicle network or domain architecture integration.

7.2 VMS configurations

VMS configurations are defined by the following principles.

- VMS configuration defines standalone requirements for entertainment and information display to driver and passenger.
- VMS configurations should be defined in the level of features and functions.
- VMS configurations should include hardware components within the VMS.
- Multiple VMS configurations are possible.
- VMS configurations should be highly variable. Both OEM-built and after-market plug-ins VMS products should be considered.

However, VMS configurations do not describe the vehicle network or domain architecture integration.

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.
- etc.

7.3 List of 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	Multiple (front, central, rear, and etc.), independent, interactive, and etc.
	Control	Traditional controls: Button / knobs / touch controls, and 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 broadcasting, FM broadcasting, FM broadcasting with dual tuner and phase diversity (PD), FM broadcasting with background scan (BGS), Radio data system (RDS), and etc.
		Digital: Digital audio broadcasting (DAB), digital terrestrial television broadcasting (DTTD), in-band on-channel (IBOC) technologies, convergent digital radio (CDR), and 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
	V2X	V2V, V2I, V2P, V2X (e.g., LTE-V/5G PC5)
Wireless local area networks	IEEE 802.11 hotspots	
In-vehicle Mobile Connectivity		Hands-free calls and music playing using personal area networks
		Web surfing using IEEE 802.11 local area networks
		Screen sharing using short distance communication networks

Features	Sub-features	Configurable
		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		Software OTA
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/ cellular networks) modem / user mobile data
	Real-time traffic	Traffic message channel (TMC), transport protocol experts group (TPEG), real time traffic centre, and etc.
	Services	Navigation services, real-time weather forecasting services, 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 OTA security
		Hardware security
		Cryptography security

Features	Sub-features	Configurable
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	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

8 Vehicular Multimedia Network Ecosystem

The VMN ecosystem 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.

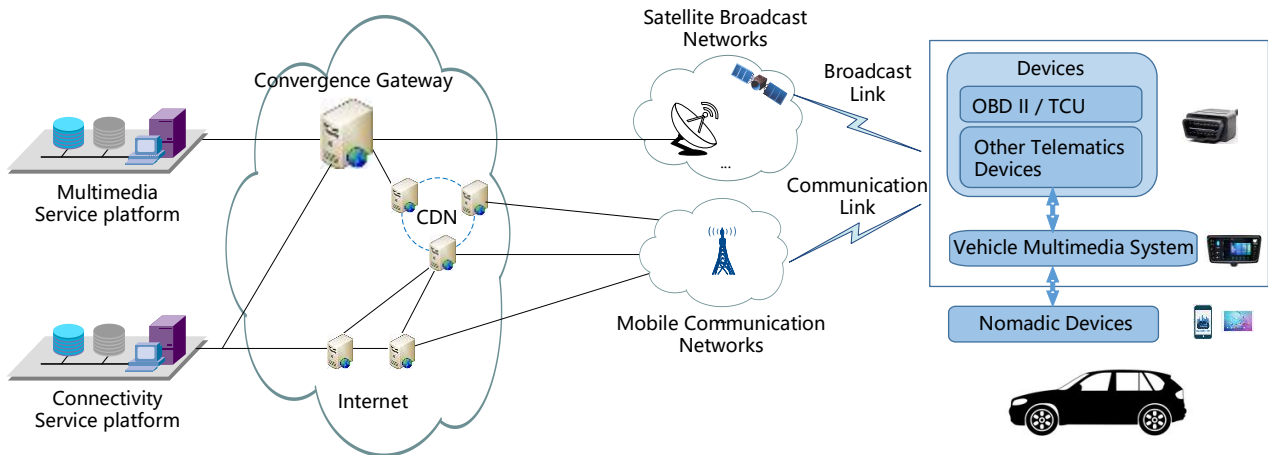


Figure 1 – Vehicular multimedia network ecosystem

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

- In-vehicle entertainment

Audio, video, and data services accessed by VMS from cloud.

- Media store

Media resources accessed by VMS from cloud.

- Periodic content updates

Content updates to VMS from cloud

9.1.2 User access control

9.1.3 Captive portal

- 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

- 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

- Accessed by VMS

It defines the country/regional specific department of telecommunication regulations and control.

9.1.6 Network access services

- 2G/3G/4G/5G backbone

Accessed by VMS.

- Internet access

VMS service by accessing the network

- Outbound/inbound short message services

VMS service by accessing the network

- Voice, eCall, iCall

VMS service by accessing the network

9.1.7 Vehicle tracking

Below are VMS services by accessing the network.

- Tracking vehicle using GNSS

- Securing vehicle using immobilizer trigger
- Driver behaviour log
- Vehicle status record

9.1.8 Centralized management

Below are VMS services by accessing the network.

- Real-time analytics
- Centralized network / infotainment management

9.2 Connected vehicle landscape

9.2.1 Major components

- Telematics control unit (TCU) / On-board diagnostics (OBD) solutions
- Connectivity solutions
- Customer relationship management applications
- Business intelligence

9.2.2 Services provided by these components

- Engine, oil status, charge status
- Vehicle location
- Driving behaviour
- In-vehicle Internet
- Distribution platform
- Content providing

9.3 Reference architecture for vehicular telematics connectivity services

Vehicular telematics connectivity system includes a vehicle tracking device installed in a vehicle that allows the sending, receiving and storing of telemetry data. The telematics data captured can include location, speed, idling time, harsh acceleration or braking, fuel consumption, vehicle faults, and more.

Vehicular telematics connectivity architecture starts with embedded devices in the vehicle such as telematics control unit (TCU) with embedded subscriber identity module (SIM) card. TCU obtains user input information and control information from VMS and connects to the application cloud for various applications, i.e., third-party services such as insurance, information and entertainment services, through mobile or satellite networks. These applications interact with customer relationship and billing which are parts of OEM enterprise integration to provide payment gateway and roadside assistance. Mobile operators and connectivity service providers deliver their services through call centres and mobile or device applications. At the service centre, manual or automated process is used to handle the service requests and the process can be controlled or monitored by the users by using various user interfaces.

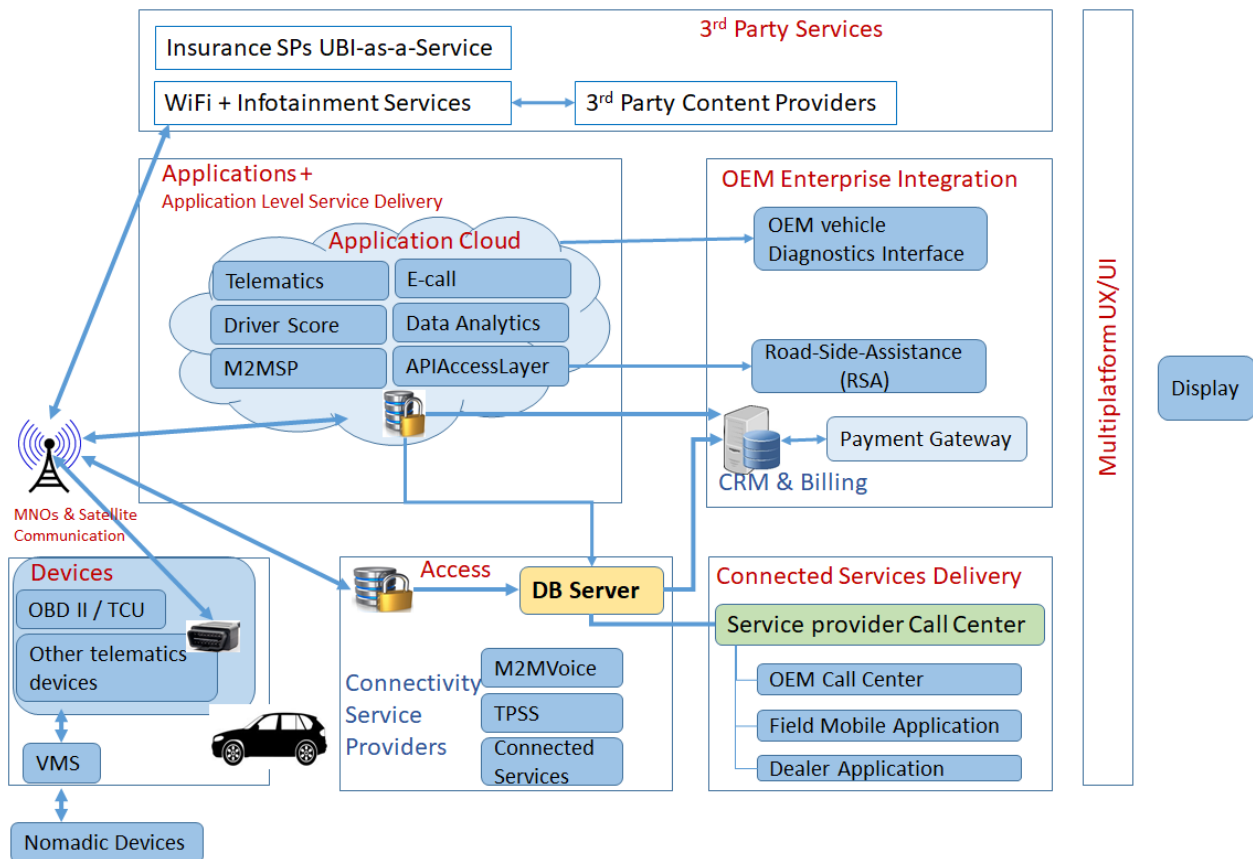


Figure 2 – Reference architecture of vehicular telematics connectivity services

9.3.1 Devices

Devices are connected to mobile network operators (MNOs).

9.3.1.1 Telematics control unit

A TCU is an embedded system on board of a vehicle that wirelessly connects the vehicle to cloud services or other vehicles over a cellular network. The TCU collects telemetry data from the vehicle, such as position, speed, engine data, connectivity quality, and etc. through interfacing with various sub-systems over data and control buses in the vehicle. It may also provide in-vehicle connectivity via wireless local area networks or short-distance communication networks and implements the emergency call (eCall) function on applicable markets.

A TCU consists of:

- A global navigation satellite system (GNSS) unit which keeps track of the latitude and longitude values of the vehicle
- An external interface for mobile communication which provides the tracked values to a centralized geographical information system database server
- An electronic processing unit

9.3.1.2 On-board diagnostics devices II

OBD-II provides access to data from the engine control unit (ECU) and offers a valuable source of information when troubleshooting problems inside a vehicle.

9.3.1.3 Nomadic devices

Nomadic devices are portable electronic devices for information, entertainment, or communication.

9.3.1.4 Devices as per global/regional/country specific regulation

9.3.2 Access

MNOs and application cloud access database server of telematics service provider.

9.3.2.1 Database server

Telematics data stored in the cloud telematics server is accessed by the end-users through a web APP or a mobile APP.

9.3.2.2 Machine2Machine voice/video data

As per local regulation/OEM/customer requirements.

9.3.2.3 TPS

Time-based positioning scheme (TPS) is a scheme used by sensors with short range beacons to broadcast its own location and help other sensors for position detection.

9.3.3 Service providers service delivery

Access database servers feed to telematics service provider's call centre services.

9.3.3.1 OEM call centre

OEM call centre is obligated to provides information about the service, diagnostics, vehicles/device operations and etc.

9.3.3.2 Field mobile APP

Field mobile APP provides insight into where vehicles and assets are, what they are doing, and allows users to easily and cost effectively communicate with their mobile workforce. It helps users to find out whether managers are in the office, on the road or in the field. It also provides users with the fleet intelligence they need to track and manage their entire fleet.

Key features include:

- Real-time location tracking to find a vehicle or asset anywhere, anytime and view whether it's active, where it is and what speed it's traveling.
- Query to get instant statistics about a particular vehicle's status.
- Messaging to easily communicate with one or multiple vehicle operators.
- Maps that integrate standard or satellite maps.
- Routing where managers can instantly send a destination address with navigation instructions to a vehicle operator, providing turn-by-turn directions.

9.3.3.3 Dealer APP

Applications to improve OEM and dealer loyalty for after-sales service and new purchases

9.3.4 Applications and application-level service delivery

Application cloud provide below services to MNOs and to database server.

9.3.4.1 Telematics applications

Several road transport telematics applications have been regulated or imposed on most vehicles to improve road safety, prevent fraud and ensure interoperability such as fleet/asset management,

navigation and location-based system, infotainment system, insurance telematic, safety & security, V2X, and others.

9.3.4.2 Driver score applications

Driver score uses the sensor data from the connected vehicle to calculate a driver score for each trip. This sensor data includes odometer reading, acceleration and speed. The driving performance for every trip is mapped to a score on a scale of 0-100. The key metrics for a trip score calculation is acceleration behaviour, braking behaviour and cornering behaviour. Apart from the trip score, an aggregated overall score based on all the past trips is calculated to have a better representation of driving behaviour.

9.3.4.3 Machine-to-machine service providers applications

Machine to machine (M2M) services can be used by OEMs and vehicles to exchange the information they record such as weather conditions, traffic information, etc

9.3.4.4 Emergency / breakdown calls

9.3.4.4.1 eCall

eCall is a system that phones the emergency services automatically if the vehicle it's fitted to is involved in an incident or accident.

9.3.4.4.2 bCall

bCall refers to a service, which allows the driver to call local road assistance in case of a breakdown. At the same time, bCall makes it possible for the call centre to gather information about the vehicle. This helps them locate the car and pin down the breakdown reasons.

9.3.4.5 Data analytics applications

Telematics is enabling automotive manufacturers, sellers, and insurers to gather information from different geographical locations and usage patterns. The data generated by sensor-driven cars about driving behaviour, speed, braking habits, turning styles, acceleration, and abidance with the traffic rules in a country is then used to create driver profiles.

9.3.4.6 API access layer

Application programming interface (API) is technical interfaces for software programs where one software program calls another software program for four key drivers: speed, reach, Internet of Things (IoT) and domains. For example, an auto dealership can reach new customers through independent car-shopping applications. The dealership gets access to a set of potential vehicle buyers who may not have contacted them directly.

9.3.5 OEM enterprise integration

9.3.5.1 OEM vehicle diagnostics interface

OEM vehicle diagnostics interface is used by OEMs to accesses the application cloud for real-time monitoring of the vehicles for any safety issues, making necessary alerts, fault prevention, and maintenance.

9.3.5.2 Roadside assistance

Roadside assistance (RSA) services and breakdown coverage services can be used to provide assistance to vehicles which suffered a mechanical failure that leaves the vehicles stranded.

9.3.5.3 Customer relationship management and billing

Customer relationship management (CRM) and billing services are services related to accounting, customer relationships, auctions, inventory, digital marketing and more.

9.3.5.4 Payment gateway which is based on OEM or service provider's strategy

Payment gateway is a secure technology that is used to communicate payment information between OEMs and customers.

9.3.6 Third party services

Third party services may include the following services:

- Third party content services
- Third party infotainment services
- Third party insurance services, i.e., usage based insurance (UBI)

9.3.7 Mobile network operators

Mobile network operators (MNOs) provide communication services to the telematics service providers and third party service providers.

10 VMS architecture

In this clause, the classification of VMS functions, the deciding factors and the reference model of VMS architecture are defined as below.

10.1 Definitions

Definition of VMS core, associated and shared functions are given as below.

10.1.1 Core functions

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

10.1.2 Associated functions

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

10.1.3 Shared functions

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 shared functions include HVAC controls through VMU and etc.

10.2 Deciding factors

Deciding factors of VMS architectures are listed as below.

- 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
- etc.

10.3 Reference model of VMS architecture

VMS architecture is defined in the level of interface, sub-systems and systems. A reference model of VMS architecture is given as below.

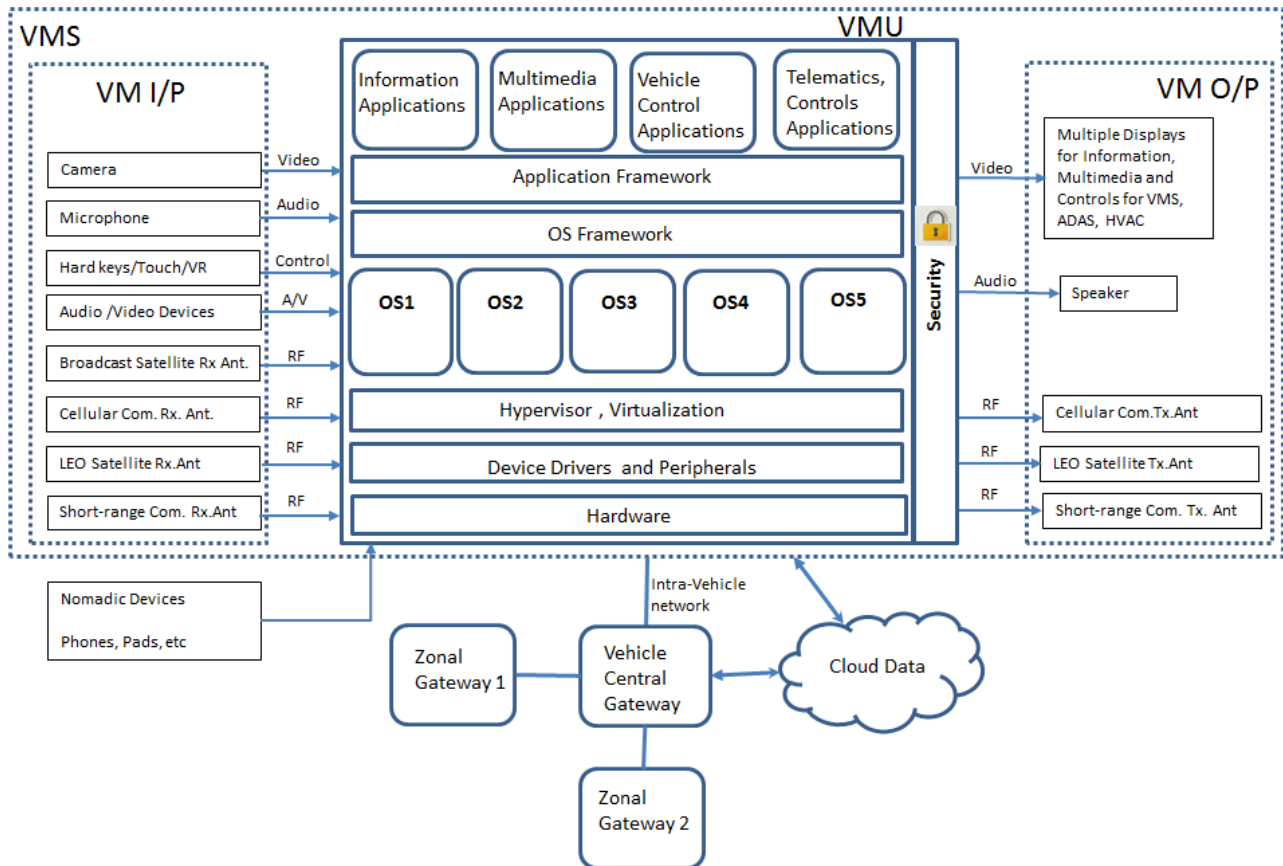


Figure 3 – Reference model of VMS architecture

10.3.1 Applications

Applications of VMS include:

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

10.3.2 Application framework

To access and control the VMS features and functions, user interface tools and design methodologies are formed as application framework.

10.3.3 OS framework

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

10.3.4 OS

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

10.3.5 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.

10.3.6 Device drivers and peripherals

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

10.3.7 Hardware

Hardware includes processors, memory, and other components, and etc.

10.3.8 Cloud data,

Cloud data includes:

- Data for multimedia services
- Data for telematics services, i.e., remote diagnostics services, software OTA update services, eCall / bCall / iCall services, navigation services, and etc.

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 clause, 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.

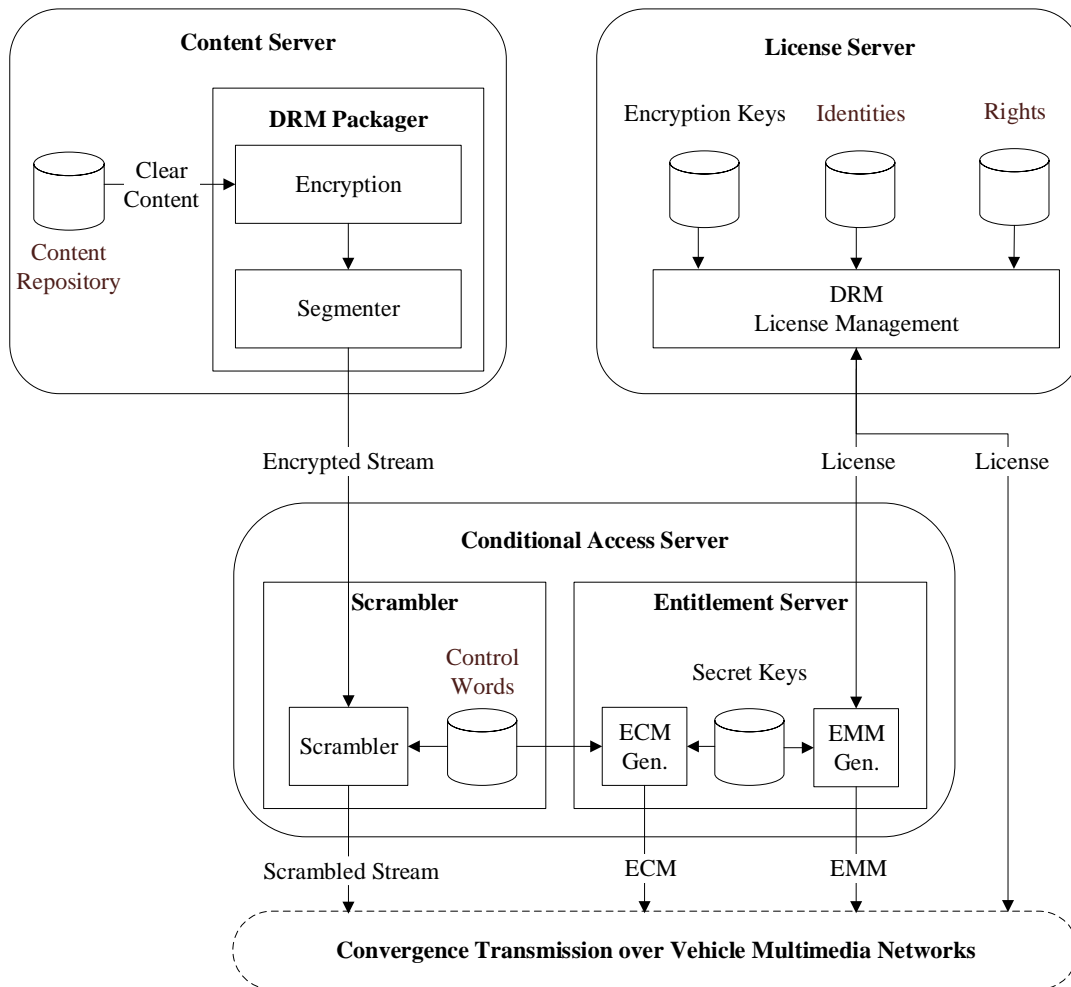


Figure 4 – Reference architecture of VMSP

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.

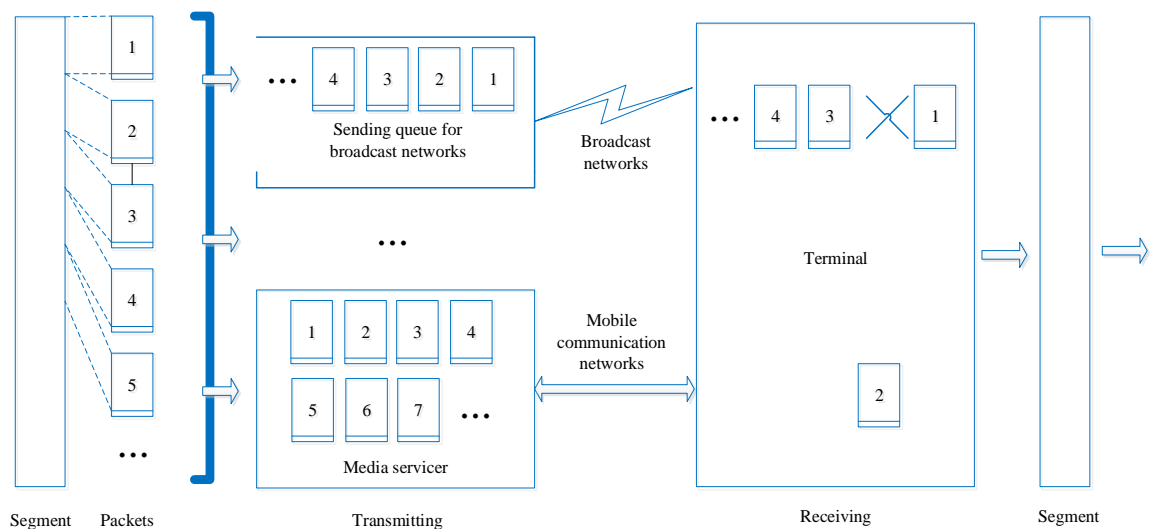


Figure 5 – The processing of convergence transmission

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.

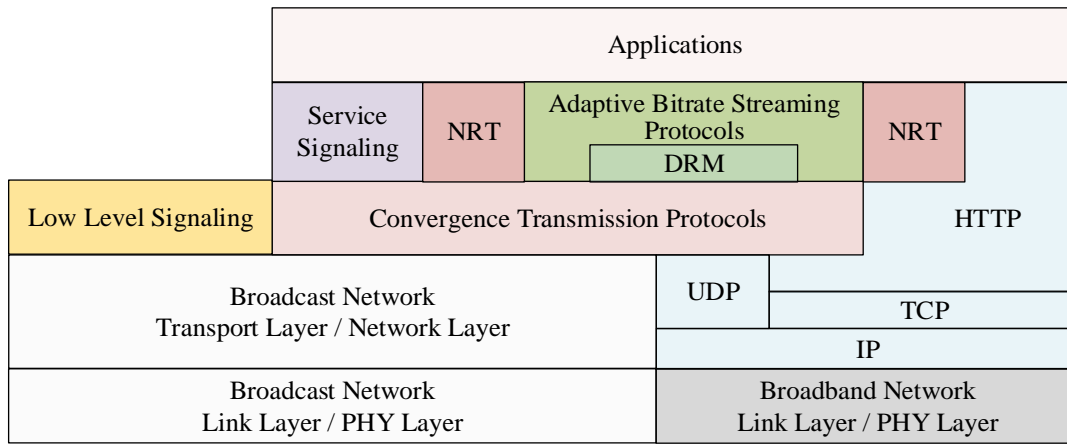


Figure 6 – The protocol stack for convergence transmission

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.

- Broadcast connections and broadband connections that provide the connectivity for the receiver to receive signaling and data.
- 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.
- 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.
- Service Signaling: Service-related signaling 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 signaling.
- 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.
- 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.

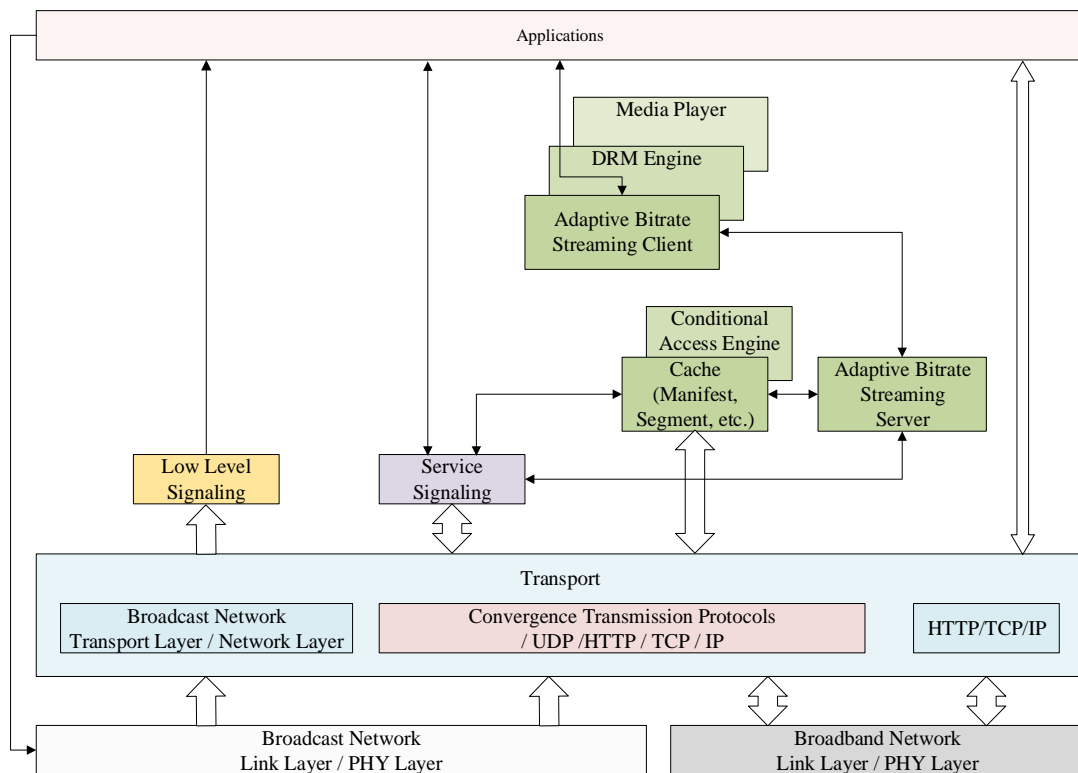


Figure 7 – Reference architecture of receivers of in-vehicle devices

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

- 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.
- 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.
- 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.
- 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.
- 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:

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

- 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

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:

- 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 ITU-T Recommendation F.749.3 [b-ITU-T F.749.3], clause 9.

- 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.
- 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.
- 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:

- 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.

- 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:

- 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 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:

- 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.

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 analysed 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 Recommendation. However, those capabilities can be effectively utilized for improving security of VMS.

- 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, VMSP 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 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,

- Sensors (motion detectors, location detectors, etc...),
- Camera (personalization, face 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/SD 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.

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.

- Personalized access based on user selection of services and interest
- VMS designed to allow for its use as per difference privacy regulatory requirements
- VMS software, hardware and network design allow only authenticated access.
- 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:

- Implementing access control mechanism by pass code 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 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*.
-