Grant Agreement Number: 768953

Project acronym: ICT4CART

Project full title: ICT Infrastructure for Connected and Automated Road Transport

D3.1

ICT4CART Reference Architecture

Due delivery date: 30.04.2019

Actual delivery date: 22.05.2019

Organization name of lead participant for this deliverable: UULM

Dissemination level		
PU	Public	X
PP	Restricted to other programme participants (including the GSA)	
RE	Restricted to a group specified by the consortium (including the GSA)	
CO	Confidential , only for members of the consortium (including the GSA)	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 768953

Document Control Sheet

Deliverable number:	D3.1
Deliverable responsible:	UULM
Workpackage:	WP3
Editor:	UULM

Author(s) – in alphabetical order		
Name	**Organisation**	**E-mail**
Anna Adaktylos	ASFINAG	Anna.Adaktylos@asfinag.at
Gottfried Allmer	ASFINAG	Gottfried.Allmer@asfinag.at
Michael Buchholz	UULM	Michael.Buchholz@uni-ulm.de
Birger Hätty	NOKIA	Birger.haetty@nokia.com
Yassine Lassoued	IBM-IE	ylassoue@ie.ibm.com
Guillemette Massot	AIRBUS	guillemette.massot@airbus.com
Jan Strohbeck	UULM	Jan.Strohbeck@uni-ulm.de
Friedrich Vogl	ASFINAG	friedrich.vogl@asfinag.at
Markus Wimmer	NOKIA	Markus.wimmer@nokia.com

Document Revision History			
Version	**Date**	**Modifications Introduced**	
		Modification Reason	**Modified by**
V0.1	20/02/2019	Initial Template	J. Strohbeck (UULM)
V0.2	21/02/2019	Add Cyber-Security & Privacy View	G.Massot (AIRBUS)
V0.4	15/03/2019	Draft Communication View (Section 2.2)	B. Hätty, M. Wimmer (NOKIA)
V0.5	19/03/2019	Data viewpoint section	Y. Lassoued (IBM-IE)
V0.6	26/03/2019	Functional view section	F. Vogl (ASFINAG)
V0.7	28/03/2019	Merge V0.3+V0.4+V0.5+V0.6, add UULM content, change TOC order	J. Strohbeck (UULM)
V0.8	01/04/2019		M. Wimmer (Nokia)
V0.9	02/04/2019	Functional View revision (Section 5)	F. Vogl (ASFINAG)
V0.95	16/04/2019	Merge V0.94-NOKIA and V0.91-AIRBUS	J. Strohbeck (UULM)
V0.96	17/04/2019	UULM internal review	M. Buchholz (UULM)
V0.98	25/04/2019	Merging of Last inputs for Review	M. Buchholz, J, Strohbeck (UULM)
V0.99	14/05/2019	Review of Section 3	A. Adaktylos, G. Allmer, F. Vogl (ASFINAG)
V1.0	21/05/2019	After internal review: Changes according to reviewers' comments and merging of changes by partners, final editing for submission	M. Buchholz, J. Strohbeck (UULM)

Abstract
The purpose of this document is to outline the general architecture that is used to implement the ICT4CART technologies on the different test sites. The aim of this general architecture is to cover all of the different ICT4CART use cases (see D2.1) and to offer the ability for deployment in all test sites and beyond.

Legal Disclaimer

Abbreviations and Acronyms

Acronym	Definition
AA	Authorization Authority
AD	Automated Driving
CAM	Cooperative Awareness Message
CAV	Cooperative Automated Vehicle
C-ITS	Cooperative Intelligent Transport Systems
CPM	Collective Perception Message
Dx.y	Deliverable x.y
EA	Enrolment Authority
EPM	Environment Perception Model
ETSI	European Telecommunications Standards Institute
GLOSA	Green Light Optimized Optimised Speed Advisory
GNSS	Global Navigation Satellite System
GSSL	Group Signature with Selective Linkability
GW	Gateway
HAD	Highly automated driving
IAM	Identity and Access Management
ICT	Information & Communication Technology
IT	Information Technology
ITS	Intelligent Transport Systems
ITS-G5	Wi-Fi (WLAN) communication standard based on IEEE 802.11a
ITS-S	ITS Station
L3, L4	Level 3 and level 4 driving levels of the automated driving system
LTE	Long-Term Evolution
MAPEM	MAP (topology) Extended Message
MEC	Multi-Access Edge Computing
NIS	Network and Information Security
NYM	Pseudonym
OEM	Original Equipment Manufacturer
PDN	Packet Data Network
PDN GW	Packet Data Network Gateway (LTE network element)
PDU	Packet Data Unit
PKI	Public Key Infrastructure
PU	Public
QoS	Quality of Service
RAN	Radio Access Network
RSU	Road-Side Unit
SCN x.y	Scenario x.y
SOC	Security Operation Centre
SPATEM	Signal Phase And Timing Extended Message
SPG	Service Provider Gateway
SSEM	Signal request Status Extended Message
TCC	Traffic Control Centre
TLS	Transport Layer Security
V2X	Vehicle-to-Infrastructure
V-ITS-S	Vehicle ITS Station
Wi-Fi	Wireless Fidelity (WLAN IEEE 802.11 Standard)

WLAN	Wireless local area network (IEEE 802.11 Standard)
WP	Work Package

Table 1: Abbreviations and Acronyms

Table of Contents

List of Figures

List of Tables

List of References

[1] ITS-G5 technology – A Fact Sheet: https://ec.europa.eu/info/law/better-regulation/feedback/18167/attachment/090166e5c12a3443_en

[2] ETSI TS 103 324 (under development): "Intelligent Transport System (ITS); Vehicular Communications; Basic Set of Applications; Specification of the Collective Perception Service".

[3] ETSI TS 103 301 V1.1.1 (2016-11): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services".

[4] ETSI EN 302 637-3 V1.3.0 V1.3.0 (2018-08): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service".

[5] DATEX II Specification: https://datex2.eu/support/downloads

[6] Open Mobility Vocabulary (MobiVoc): https://www.mobivoc.org

[7] ETSI TS 103 301 V1.2.1 (2018-08): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services".

[8] ETSI EN 302 672-2 V1.3.1: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specifications of Cooperative Awareness Basic Serivces".

[9] ETSI TS 102 894-2 V1.3.1: "Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary".

[10] NIS Directive: "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union".

[11] Certificate Policy for Cooperative Intelligent Transport Systems: "Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)". https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf

Executive Summary

The aim of the ICT4CART project is to design, implement and test in real-life conditions a versatile ICT infrastructure that will enable the transition towards higher levels of automation. It focuses on four high-value use cases: Smart Parking & IoT services, dynamic adaptation of vehicle automation level based on infrastructure information, intersection crossing (urban) & lane merging (highway), and Cross Border Interoperability. Work Package 3 (WP3) builds on the findings of WP2, which includes the specification of the use cases (D2.1), the analysis of market needs (D2.2) and the system requirements (D2.3). Within Task 3.1 of WP3, the ICT4CART Reference Architecture was developed, which is reported in this document. The ICT4CART Reference Architecture will be the basis for the subsequent Tasks 3.2, 3.3 and 3.4, where the key aspects of Flexible Networks, IT Environment, and Cyber-Security & Data Privacy will be refined. Their findings will be reported in the deliverables D3.2, D3.3 and D3.4, respectively.

This document describes the ICT4CART Reference Architecture that is used in the ICT4CART project to implement all of the project use cases (see D2.1).
First, the Introduction in Section 1 describes the aims of ICT4CART, i.e. the design and deployment of the ICT4CART technologies on the test sites covering all use cases. Section 2 contains the description of the high-level architecture, which aims to not only encompass the ICT4CART use cases and scenarios, but also to be general enough to be re-used for new, different use cases in other projects as well as in the deployment of ICT-based ITS applications.
It is followed by descriptions of different views of the architecture, which highlight certain aspects of the architecture. First, in Section 3, a functional view on the architecture is presented, which shows and describes the different functional components that are used in the project. Section 4 describes the types of data that can be transmitted in communication with the IT environment as well as the typical data flows. Then, in Section 5, a communication view is described, which outlines the different communication technologies used in the project (Ad-hoc-networks, cellular networks, hybrid communication) and the approach to their implementation during this project. As finding solutions for Cyber-Security and Data Privacy is a key objective of the project, Section 6 describes how the high-level architecture can be enhanced with additional security and privacy components to achieve this objective.
Finally, Section 7 concludes the document with a summary of the main aspects of the ICT4CART reference architecture.

1 Introduction

1.1 Aim of the project

Today, significant and rapid advances in both telecommunication and IT industries can be accredited to fast-growing disruptive technologies. Amongst these, the ETSI ITS G5 technology can be considered a mature and accessible technology with widely accepted norms and easily available products [1]. Moreover, the 5G technology is evolving rapidly, while LTE-Vehicle (LTE-V) features low cost and rapid deployment since it can utilize existing base stations. In the light also of the above, several ICT challenges related to connectivity, data management, cyber-security and ICT infrastructure architectures still play a significant role and need to be addressed in order to enable road vehicle automation. Thus, it is of utmost importance for vehicle automation to work on the direction of advancing the digital and ICT infrastructure, taking also into consideration the limitations in both resources and investments in the physical transport infrastructure.

ICT4CART aims to address the gaps to deployment bringing together key players from automotive, telecom and IT industries, to shape the ICT landscape for Connected and Automated Road Transport and to boost the EU competitiveness and innovation in this area.

The main goal of ICT4CART is to design, implement and test in real-life conditions a versatile ICT infrastructure that will enable the transition towards higher levels of automation (up to L4) addressing existing gaps and working with specific key ICT elements, namely hybrid connectivity, data management, cyber-security, data privacy and accurate localization. ICT4CART builds on high-value use cases (urban and highway), which will be demonstrated and validated in real-life conditions at the test sites in Austria, Germany and Italy. Significant effort will be put also on cross-border interoperability, setting up a separate test site at the Italian-Austrian border. The ICT4CART Reference Architecture reported in this document will be the basis for the realization of the use cases in these test sites.

1.2 Purpose of the document

The purpose of this document is to outline the high-level reference architecture that is used to implement the ICT4CART technologies on the different test sites. The aim of this architecture is to cover all of the different ICT4CART use cases (see D2.1) and to offer the ability for deployment in all test sites and beyond. To achieve this, it has to address the requirements of all the different scenarios while remaining generic enough to be deployed for automated driving in general and to allow more use cases to be integrated. It shows a solution to interoperability of the various heterogeneous networks and software components throughout the architecture. It also defines the high-level data flow in the Communication View and the involved IT services in the Data / IT Environment View. Finally, principles by which cyber-security and privacy will be enforced throughout the architecture are given in the Cyber-Security & Privacy View. These concepts are presented on a high-level basis and elaborated further in the deliverables D3.2 (Flexible Networks Specification and Architecture), D3.3 (IT Environment Specifications and Architecture) and D3.4 (Cyber-Security and data privacy Specifications and Architecture).

1.3 Intended readership

This deliverable is addressed to any interested reader (i.e., PU dissemination level) who wishes to be informed of the general architecture that is used in ICT4CART project to implement the use cases and scenarios defined in D2.1 (also PU dissemination level).

2 ICT4CART High-Level Architecture

2.1 Overview

In this chapter, the general, high-level architecture is described, which encompasses the concepts that are used in the ICT4CART use cases. The architecture is general enough to be applied to new, different automated driving use cases.

2.2 High-Level Architecture

In Figure 1, the general architecture is visualized. It shows which basic components are involved in the ICT4CART system and how they can interact with each other. The main components are the vehicles, infrastructure (sensors and processing units) and IT services (such as an OEM backend or other service providers). The basic communication technologies that are used are LTE/5G (cellular) and ITS-G5 (ad-hoc). Not all use cases need to use all of these technologies, but may only use a subset of them. When using 5G, slicing may be used to provide a Quality of Service (QoS) required for the kind of information to be transported, which is represented by the dashed lines in the figure. There can be slices, e.g., for low-latency communication (short dashes in the figure) or high-throughput communication (lines with longer dashes in the figure). As slicing is a 5G feature, it is not available when using LTE or ITS-G5. For further details on the communication, see Section 5.

Hybrid connectivity, i.e. using ITS-G5 and LTE/5G in parallel, is also depicted in the figure, as the infrastructure can provide the information via both communication channels. Also, vehicles can retrieve information over the different communication paths, either from the same source or from different sources. The vehicles in Figure 1 are either not connected, connected with ITS-G5 (G5), with LTE/5G (5G), or with both (5G+G5). A car-to-car connection is possible via ITS-G5.

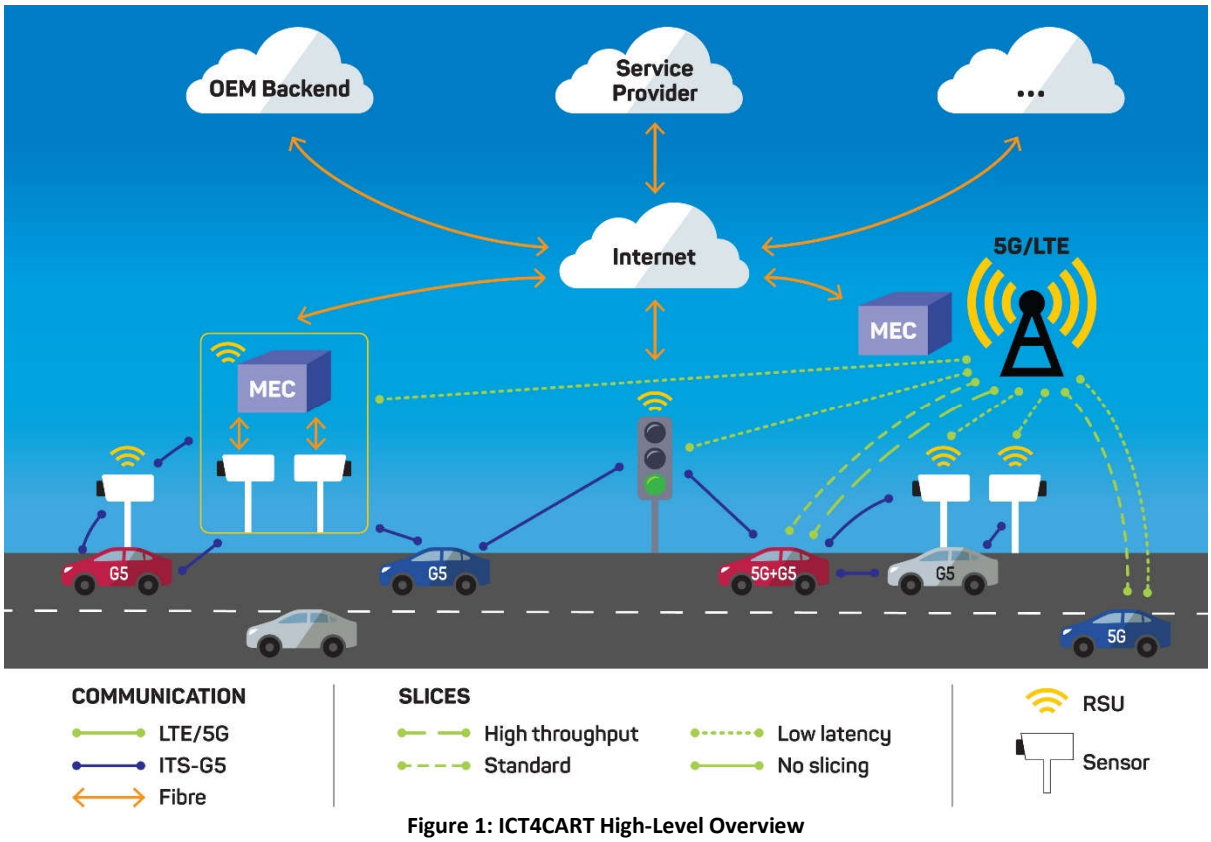

Figure 1: ICT4CART High-Level Overview

The road is equipped with Road Side Units (RSUs), connected sensors, and connected traffic lights. LTE/5G base stations receive and transmit data via cellular network (green lines). ITS-G5 RSUs receive and transmit data via ITS-G5 (blue lines). Sensors and traffic lights are connected either via fibre cables (orange lines), cellular network, or via ITS-G5.

The figure also indicates the concept of Multi-Access Edge Computing (MEC) servers. MEC servers are situated close to a base station of a cellular network, providing computation closer to end devices (in the ICT4CART use cases: vehicles) and thereby avoiding time-consuming transmission of data via the Internet. This concept decreases latency, especially for mission-critical data, when compared to using a cloud server anywhere in the network.

Similar functionality like MEC servers can be provided by processing capabilities of road infrastructure, like sensors in combination with RSUs. This is shown in the left part of the figure. For simplicity, these processing units are also denoted as MEC here. An RSU is an ITS-G5 communication unit on infrastructure side. Such MEC servers in combination with RSUs can run ICT4CART applications or services in close proximity with lower delays than cloud services.

Information from the OEM Backend, Service Providers, and other cloud services ("…" cloud in Figure 1) can be received via the Internet.

The concepts depicted in this general architecture are refined in the following chapters regarding the functional, data/IT environment, communication, as well as cyber-security and privacy viewpoints.

3 Functional View

The ICT4CART architecture consists of a collection of functional blocks. The individual test sites each make use of a selection of these functional blocks. The functional view organizes the functional blocks into groups according to their common purpose: Supporting Services, Sensors and Actuators, Applications, Core Services, Hybrid Wireless Network, Cooperative Automated Vehicle (CAV), Security and Privacy.

3.1 Overview

The Functional View is depicted in Figure 2. Please note that the groups in the diagram are not communication layers, so their location in the diagram below does not have a meaning for that purpose. Core services are essential for HAD on European roads.

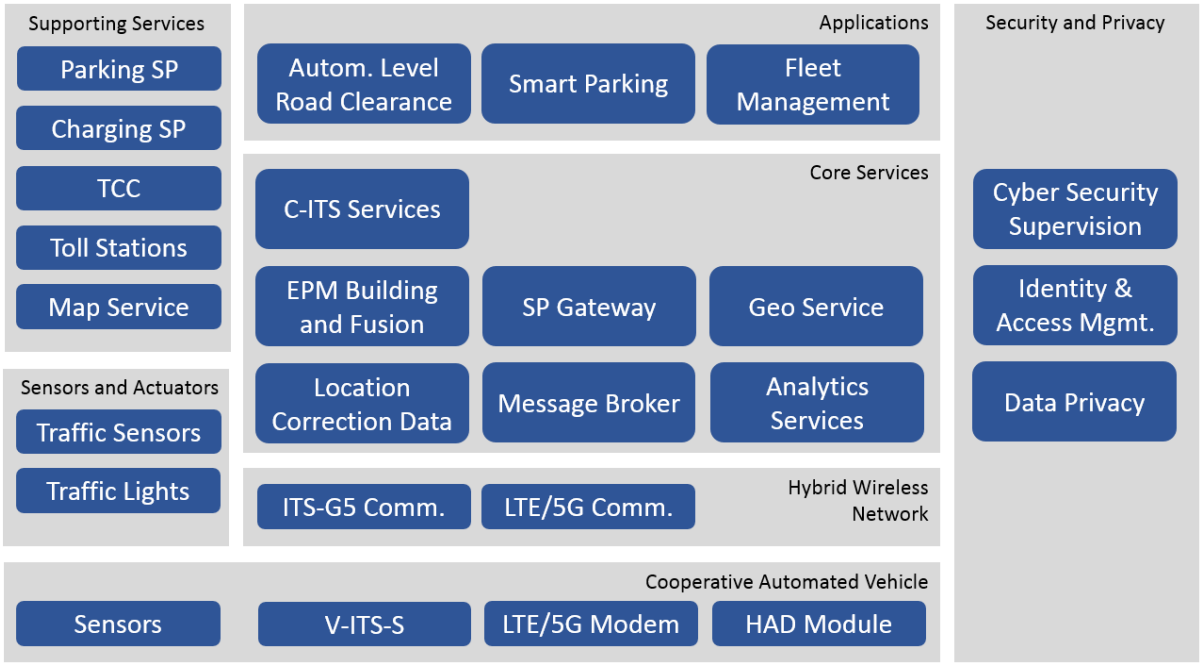

Figure 2: Functions required for ICT4CART use cases

3.2 Description

3.2.1 Supporting Services

The Supporting Services group includes functional modules that are directly or indirectly related to navigation, i.e. parking, charging, etc.

3.2.1.1 Parking Service Provider (SP)

Parking Service Providers supply information regarding currently available parking spots to the Service Provider Gateway (SPG). In addition to the number of vacant parking spaces, their location is provided for navigation purposes. The providers may also make historic data available for prediction purposes.

3.2.1.2 Charging Service Provider (SP)

Charging Service Providers supply data regarding currently available charging stations to the SPG. The locations and the technical characteristics, like available charging plug types and charging modes, are shared. The providers may also make historic data available for prediction purposes.

3.2.1.3 Traffic Control Centre

The Traffic Control Centre (TCC) provides the relevant data from the road infrastructure operator. This includes information like the maximum speed limit, the location of road works zones, or the current weather situation.

3.2.1.4 Toll Stations

Toll Stations provide data regarding operational lanes, their occupancy rate, and available payment methods.

3.2.1.5 Map Services

Map Services provide an HD map that contains highly accurate information about traffic lanes, the location of pedestrian crossings, etc.

3.2.2 Sensors and Actuators

The Sensors and Actuators group contains functions in the infrastructure to gather information about the traffic on roads as well as to manage the traffic.

3.2.2.1 Traffic Sensors

Traffic sensors provide the TCC with vital sensor information regarding the current traffic in the surveyed area. These sensors include observation sensors like video cameras, vehicle detectors like magnetic coils, and depth sensors like LiDAR sensors.

3.2.2.2 Traffic Lights

Connected traffic lights are used to adaptively control the traffic. They can both display the information and provide it digitally. In addition to the traffic light status, the remaining time to the next signal change may be shared.

3.2.3 Applications

In the Applications group, we have functions that make use of data and services from several other different groups to add business value.

3.2.3.1 Automation Level Road Clearance

The Automation Level Road Clearance application utilises static (e.g. legal regulations, road topology, etc.) and dynamic (e.g. traffic density, weather, etc.) information to determine and prescribe a clearance for a road section and a specific automation level. A human traffic manager can override the actual clearance, if required, before it is distributed.

3.2.3.2 Smart Parking

The Smart Parking application replies to requests from CAVs and Fleet Management Applications to find a suitable parking space. Based on a requested location and a search radius, an available parking space is selected and the precise location is communicated. The application may also assign the parking space to the requesting vehicle and, thus, not consider it for near-term requests from other vehicles.

3.2.3.3 Fleet Management

The Fleet Management application keeps track of all managed vehicles and their statuses. If a low battery level is detected in a vehicle, the Fleet Manager requests information about charging stations and appoints the vehicle to a suitable charging station. The Fleet Manager can also request parking data to relocate an idle vehicle to a different area where high demand is expected.

3.2.4 Core Services

The Core Services group consists of several services that are crucial to make ICT infrastructure a key enabler for a safe and efficient deployment of HAD on European roads.

3.2.4.1 C-ITS Services

C-ITS services such as Common Awareness, Decentralized Environmental Notification, Traffic Light Manoeuvre or Infrastructure-to-Vehicle Information are used to manage the generation, transmission and reception of C-ITS messages.

3.2.4.2 Environment Perception Model Building and Fusion

Data from vehicles and/or infrastructure are received and then processed in the Environment Perception Model (EPM) Building and Fusion function. This way, an EPM of the surveyed area is created, which is then provided to the road users.

3.2.4.3 Service Provider Gateway

The Service Provider Gateway (SPG) collects the data from various different vendors and provides a single downstream interface to the communication infrastructure. Based on historic data, the SPG makes predictions for parking space availability in a specific area and time frame.

3.2.4.4 Geo Service

The Geo Service determines the relevance radius for ITS messages, the group of wireless stations that transmit these ITS messages and the CAVs that are in the relevance radius.

3.2.4.5 Location Correction Data

To allow precise positioning of the CAV, the Location Correction Data function provides correction data for Global Navigation Satellite Systems (GNSS) data by using either physical reference stations or network-based ones.

3.2.4.6 Message Broker

The Message Broker is part of the hybrid C-ITS approach and will be used by CAVs to subscribe for messages of interest based on geographical location. There will be at least one Message Broker per country.

3.2.4.7 Analytics Services

Analytics Services refine data by using algorithms in order to prepare them for other services. The SPG for example will make use of Analytic Services to make predictions of service availability for the future.

3.2.5 Hybrid Wireless Network

The Hybrid Wireless Network consists of the combination of the wireless ad-hoc ITS-G5 network and cellular networks such as LTE and 5G which maximizes coverage. A seamless integration of both technologies enables an increase in reliability, availability and redundancy.

3.2.5.1 ITS-G5 Communication

ITS-G5 utilises Wi-Fi to enable decentralized ad-hoc communication between vehicles and/or infrastructure elements.

3.2.5.2 LTE/5G Communication

Cellular networks, like LTE and 5G, are used to enable wireless communication over a longer range. Techniques like network slicing and the use of Multi Access Edge (MEC) Computing will be used to provide Quality of Service (QoS).

3.2.6 Cooperative Automated Vehicle

The Cooperative Automated Vehicle group describes the vehicle part. Vehicles equipped with both wireless communication technologies (ITS-G5 and LTE/5G) make use of both, the ad-hoc information and the mobile information (hybrid communication).

3.2.6.1 Sensors

The on-board sensors are a major source of information on which the CAV bases its automated driving decisions.

3.2.6.2 V-ITS-S

The Vehicle ITS Station (V-ITS-S) is used for the ITS-G5 ad-hoc Wi-Fi communication with other vehicles and C-ITS infrastructure components.

3.2.6.3 LTE/5G Modem

The LTE or 5G Modem is used for the mobile connection to the radio access network (RAN) of the cellular network.

3.2.6.4 Highly Automated Driving Module

The Highly Automated Driving (HAD) Module summarizes all functionality to implement automated driving using the data from its on-board sensors as well as cooperative information.

3.2.7 Security and Privacy

The Security and Privacy group contains the Identity and Access Management, Cyber Security Supervision and Data Privacy functions. Together they ensure that all data exchanges are safe and secure while personal data privacy is preserved.

3.2.7.1 Cyber Security Supervision

By constant monitoring of the system, the Cyber Security Supervision function ensures that any security threats are identified timely and are reported for mitigation.

3.2.7.2 Identity & Access Management

The Identity and Access Management function ensures that all participants in the data exchanges are authenticated and authorized.

3.2.7.3 Data Privacy

The Data Privacy function allows the collection of data from authenticated endpoints while preserving the user’s privacy.

4 Data / IT Environment View

The Data / IT environment view of the high-level architecture comprises the data flows as well as the data types. This overview will be detailed in Deliverable D3.3 “IT Environment Specifications and Architecture”.

4.1 Overview of Data Flows

Based on the ICT4CART report D2.1, “Specification of Use Cases”, all the use cases share the following common data flows, which are further illustrated in Figure 3.

1. Road users (e.g., vehicles) or sensors may submit data to a road-side unit (RSU) about the current “driving environment”, e.g., cooperative awareness message (CAM) from vehicles, positions, speeds and directions of road users detected by sensors, information about obstacles, traffic signs, parking availability, etc.).
2. Consumer vehicles equipped with communication modules may receive data directly from an RSU or a MEC server, e.g., collective perception message (CPM), decentralized environmental notification message (DENM), signal phase and timing extended message (SPATEM), map extended message (MAPEM). They may also receive data directly from other vehicles, e.g., CAM, CPM. These may be used for short-term decisions and control.
3. One or multiple RSUs and road sensors may push their data to a multi-access edge computing (MEC) server in their vicinity.
4. A vehicle may exchange collective perception messages with a MEC server in its vicinity.
5. A cloud platform receives data from MEC servers, RSUs or ITS stations, and external services (e.g., third-party parking service, traffic service, etc.) to create large-scale maps and predictions (e.g., parking availability predictions, traffic jam analysis, etc.).
6. Vehicles may receive data from the cloud platform about traffic jams in their vicinities, parking availability predictions, etc. These may be used for long-term (strategic) decisions and for automation level adaptation (6).

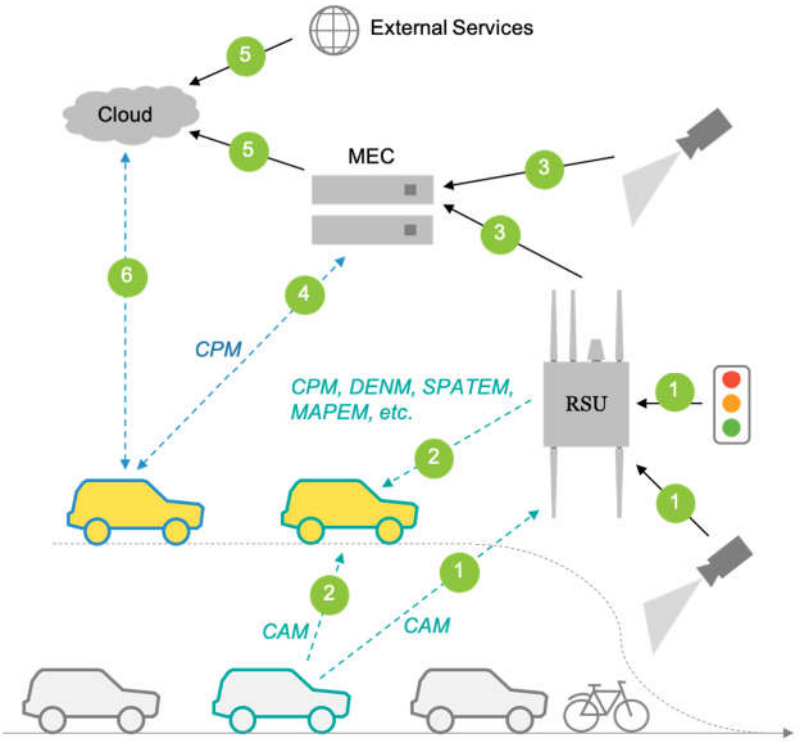

Figure 3: Common Data Flows across ICT4CART Use Cases

4.2 Data Types

Based on the use case specifications, the following data will be exchanged throughout the ICT architecture (table below). Data types are split into two categories: those provided by the IT environment to the vehicles, and those consumed by the IT environment. The data standards and use cases pertaining to each data type are listed.

	Data Type	Relevant Standards	Relevant Use Cases
Provided by the IT Environment	Environment perception models (EPMs) for use by the automated driving (AD) vehicles	CPM as will be specified in ETSI TS 103 324 [2]	Virtual mirror (e.g., vehicles and road users around intersections/junctions) Lane merging (e.g., vehicles and road users in a given lane) Adaptation of vehicle automation level (e.g., vehicles and road users around toll stations)
	Intersection map and topology	MAPEM as specified by ETSI TS 103 301 [3]	Virtual mirror, lane merging, green light optimised speed advisory (GLOSA)
	Traffic light data	SPATEM as specified by ETSI TS 103 301 [[3]	Intersection crossing, GLOSA
	Situations and events (e.g., accident, road closure, etc.)	DENM [4], DATEX II [5]	Lane merging, adaptation of vehicle automation level
	Real-time parking spot and charging station availability	DATEX II [5], Open Mobility Vocabulary (MobiVoc) [6]	Smart parking
	Extracted or aggregated information and predictions, such as parking predictions, traffic jams, etc.	To be defined depending on the type of output data	All use cases
	Correction data for GNSS-based localisation	ETSI TS 103 301 [7]	All use cases
	HD Maps	To be defined	All use cases
Consumed by the IT	EPMs, or data required to build EPMs, from RSUs and road signs and sensors	CPM, CAM as specified by ETSI EN 302 672-2 [8]	Virtual mirror, lane merging, adaptation of vehicle automation level
	Data directly received from road signs and sensors in the absence of RSUs	CPM, DENM	Virtual mirror, lane merging, adaptation of vehicle automation level
	Data received from traffic and parking services	DATEX II	Adaptation of vehicle automation level, smart parking
	Data received from vehicles either directly or indirectly through RSUs	CPM, CAM	All use cases

5 Communication View

In the following, the Communication View of the high-level architecture is presented. After a short overview of the ITS message handling, the following subsections describe the wireless ad-hoc communication and the cellular communication. Finally, the hybrid communication based in the combination of both communication channels is sketched. Details will be available in the Deliverable D3.2 “Flexible Networks Specification and Architecture”.

5.1 ITS message handling

An ITS Station interacts with one or multiple ITS Stations. This activity includes:

- the generation and transmission of ITS messages to be sent to selected ITS Stations;
- the reception of ITS messages from ITS Stations,
- the processing of incoming ITS messages, and
- the storage of received, generated, and/or transmitted information;

ITS messages can be exchanged using wireless ad-hoc and cellular communication systems, as shown in Figure 4 with SPATEM as exemplary ITS message.

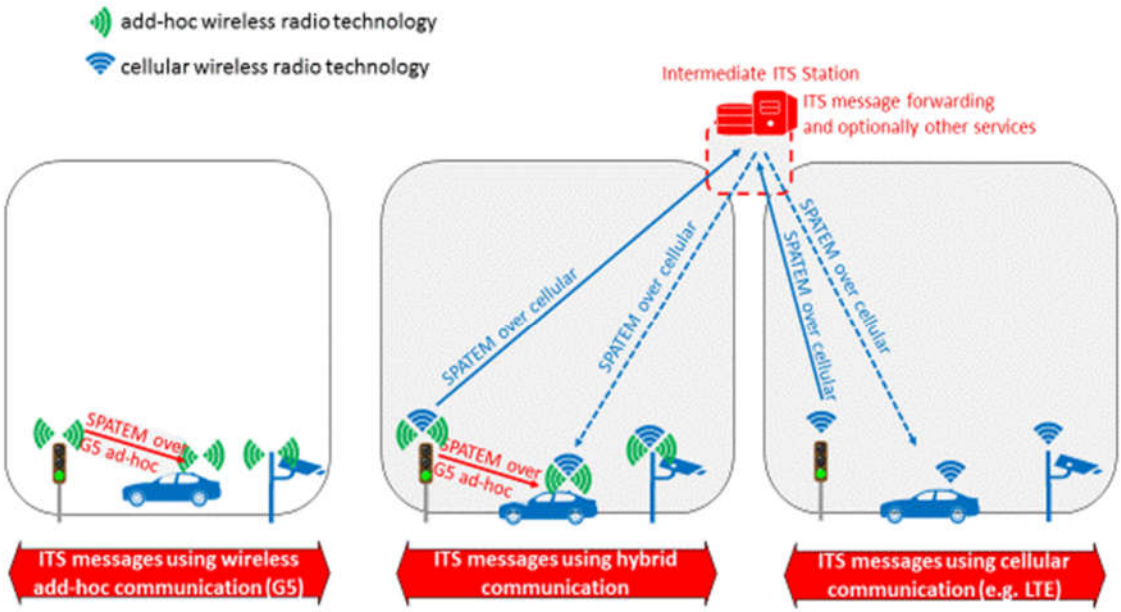

Figure 4: ICT4CART wireless ad-hoc, cellular, and hybrid communication architecture. The transmission paths of ITS messages are exemplified with SPATEM

5.2 Wireless ad-hoc communication

Wireless ad-hoc networks such as Wi-Fi operating in ad-hoc mode offer decentralized communication, which allows network elements to communicate directly with each other. ITS Stations can use wireless ad-hoc communication as defined in ETSI ITS-G5 systems to broadcast ITS messages to any other ITS Station within their proximity. For instance, if a Roadside ITS Station equipped with a traffic light signalling system supports an ITS-G5 wireless ad-hoc access technology, then it can broadcast an ITS message such as a SPATEM directly to (vehicle) ITS Stations in its proximity. The ITS message can be received by those (vehicle) ITS Stations supporting the same access technology, as indicated on the left-hand side in Figure 4.

An unlicensed frequency spectrum is typically used, such as 5.9 GHz for ETSI ITS-G5. Factors such as the used wireless ad-hoc technology and the surrounding geographical topology determine range, within which the ITS message can be received. The typical communication range is in the order of hundreds of meters.

5.3 Cellular communications

Cellular networks, also called mobile networks, such as LTE and 5G, provide a centralized communication network with a wireless access technology. ITS Stations using a cellular communication system typically do not broadcast ITS messages directly to other ITS Stations in their geographical proximity. Instead, the ITS message is sent to an intermediate ITS Station, which provides ITS message forwarding as a service. It may provide a range of additional services, such as message fusing. For ITS message forwarding, the intermediate ITS Station operates a geo-location function. A geo-location function stores e.g. the latest known location of ITS Stations based on incoming ITS messages; geo-location information may also be stored directly by an ITS service provider for stationary ITS Stations such as signalling traffic light systems. With the help of the geo-location function, the intermediate ITS Station can determine the group of ITS Stations that are currently located in the proximity of the sender of the ITS message, and then forward this ITS message to this group of ITS Stations using the cellular network.

For example, if a Roadside ITS Station such as a traffic light signalling system at an intersection supports only a cellular access technology, then an ITS message such as a SPATEM can be sent via the cellular network to the intermediate ITS Station, which then forwards the ITS message, as shown on the right-hand side in Figure 4.

Being a centralized communication network, transmission resources for an ITS Station or a group of ITS Stations can be controlled. This allows the mobile network operator to provide Quality of Service (QoS) between edge nodes of its network. (Edge nodes of a mobile network are the mobile phone, and the Packed Data Network Gateway (PDN GW), which interconnects the mobile operator's network to other networks.) The key QoS attributes are:

- latency, i.e. the transmission delay between mobile phone and PDN GW; and
- reliability, i.e. the packet error loss rate between mobile phone and PDN GW.

If an ITS service for connected automated driving (L3/L4) requires very low latency, then the transmission delay between the ITS Station and the intermediate ITS Station needs to be minimized. This can be achieved by

- minimizing the transmission delay on the wireless link by deploying radio resource management tactics, such as pro-active scheduling and reduced block error rate in LTE; and by

- minimizing the wireline transmission delay between the base stations and intermediate ITS station by placing it in close proximity of the base stations over which the (vehicle) ITS Stations send their ITS messages. The intermediate ITS Station can e.g. be hosted on a **MEC Server** placed within or next to radio access network (RAN) of the cellular network.

Users and applications can have very specific requirements with respect to transport QoS and ITS service processing and storage capabilities. **Network slicing** allows providing **dedicated virtual networks** with functionalities specifically selected to meet the service or customer requirements. ITS service specific network slices can be generated, in which

- the allocated virtual infrastructure resources like cloud nodes and transmission resources are isolated; and in which
- an ITS service provider can manage the virtual infrastructure resources allocated to it; and the latency and reliability can be configured by the ITS service provider to meet the demands of the ITS service.

5.4 Hybrid communications

Hybrid communication deploys multiple communication networks to extend network coverage for ITS Stations and to improve ITS service availability. When an ITS Station such as a traffic light signalling system supports both ITS-G5 wireless ad-hoc and a cellular access technology, then

- an ITS message such as a SPATEM can be broadcasted directly via the wireless ad-hoc network to those neighbouring ITS Stations which are capable to receive ITS messages via this wireless access technology; and
- an ITS message can be sent via the cellular network to the intermediate ITS Station. The intermediate ITS station processes the incoming information, and it can e.g. determine those vehicular ITS Stations in the proximity of the light signalling system which can be accessed via the cellular communications system. It can then trigger the forwarding of ITS messages to those vehicular ITS Station.

The example with the light signalling system is indicated in the middle and on the right-hand side of Figure 4.

6 Cyber-Security & Privacy View

The Cyber-Security & Privacy View of the high-level architecture comprises a Cyber Security Supervision Service, an Identity and Access Management Service, and Data privacy mechanisms. The given overview will be detailed in Deliverable D3.4 “Cyber-Security and data privacy Specifications and Architecture”.

6.1 Overview

One of the objectives of the ICT4CART project is to define and implement cyber-security means for end-to-end protection, integrity, privacy, and reliability of the data used for automated driving purposes, in compliance with ITS standards and regulations, enhanced by surveillance mechanisms. This applies to Vehicle-to-Infrastructure (V2X) communications and communication from/to services provided by OEMs, third parties, and even security service providers themselves. To achieve this objective, two cyber security services provide role-based identity and access management (IAM) and cyber-security supervision for C-ITS message exchanges. Supervision in cyber security is a function available within a Security Operation Centre (SOC), and proposed to decision-makers and analysts. Preserving privacy is a major need formulated by the European Union. Thus, privacy dedicated capacities are proposed, too. For example, information correlated by the supervision service is anonymised with a mechanism preserving privacy while allowing linkability. Along with cyber-security cloud services, cyber-security modules are integrated within vehicles, infrastructure and services with various features that depend on their role and the type of messages they deliver. These features include access control, accounting, encryption, authentication, and privacy protection.

Figure 5 depicts the general architecture of cyber security services that will be designed within the ICT4CART project.

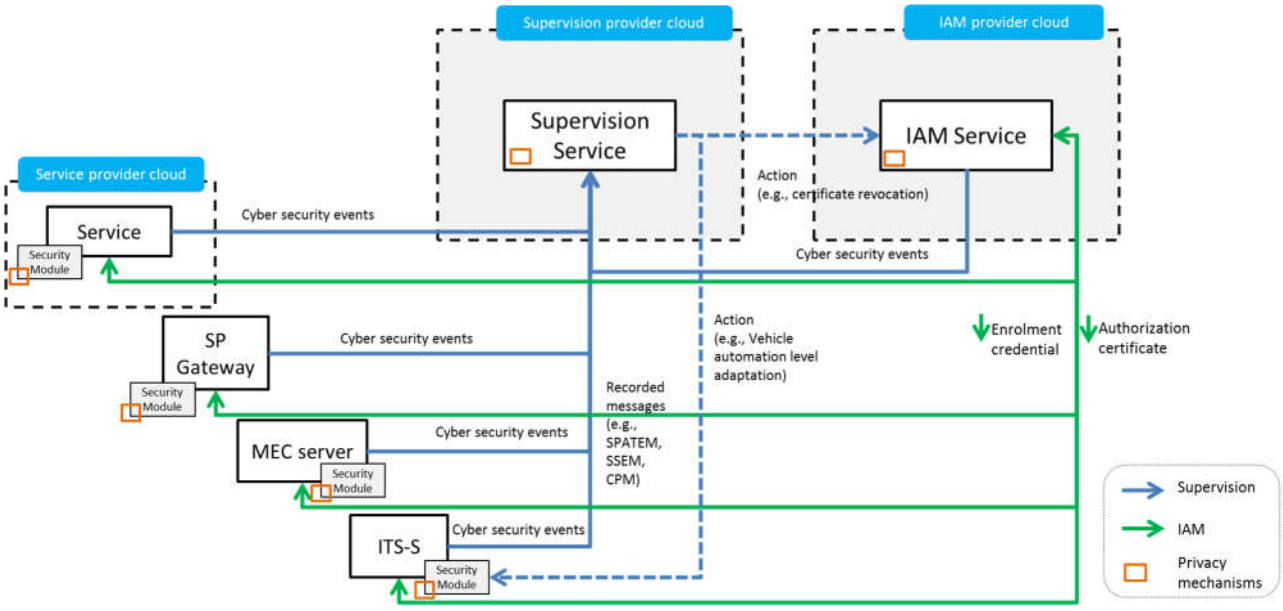

Figure 5: Cyber security architecture overview

6.2 Cyber Security Supervision Service

Road transport operators are categorized as operators of essential services. Consequently, they have to comply with the Network and Information Security (NIS) Directive [10]. This European directive states that every member state has to set national cyber security capabilities, cross-border collaboration, and cyber security supervision of critical sectors including transport. The supervision service proposed in this section fulfils this need with the capacity to get aware of the cyber security situation on ITS communications.

The supervision service, as shown in Figure 6, collects, processes, and reports anomalies on vehicles, RSUs, MEC servers, and cloud services communications. It also manages alerts from embedded security modules and the IAM service about unwanted situations such as the use of revoked certificates, abuse of rights, etc. The supervision service has the following functionalities:
Collection: Collecting data is the foundation of the cyber security monitoring. This is a real-time and one-way process, from the data source to the collection point. Collected data may be security events from embedded or network sensors or ITS messages such as CAM, DENM, CPM, etc.
Detection: The supervision service includes a rule-based correlation engine and an anomaly detection engine based on artificial intelligence.
Response orchestration: The role of this capacity is to provide the necessary functions to cyber security experts to **investigate**, to create an incident report, and to gather relevant information. It also interfaces with the **reaction enforcement** capacity to request incident mitigation countermeasures.
Reporting: Various dashboards and reports are needed to be aware of the cyber situation. They are built by the reporting capacity based on stored data, including correlation alerts.

In compliance with the privacy requirements defined in ITS standards, data handled in the supervision service are anonymised. However, the event correlation and anomaly detection process requires analysed data to be linkable. That is why the Group Signature with Selective Linkability (GSSL) technology proposed by IBM may solve this issue as not only it anonymises data but it also enables to link data. Consequently, a GSSL decoder will be deployed to grant anonymised data could be linked. This mechanism will be studied within the technology assessment task. For more details about the GSSL feature, cf. Section 6.4.

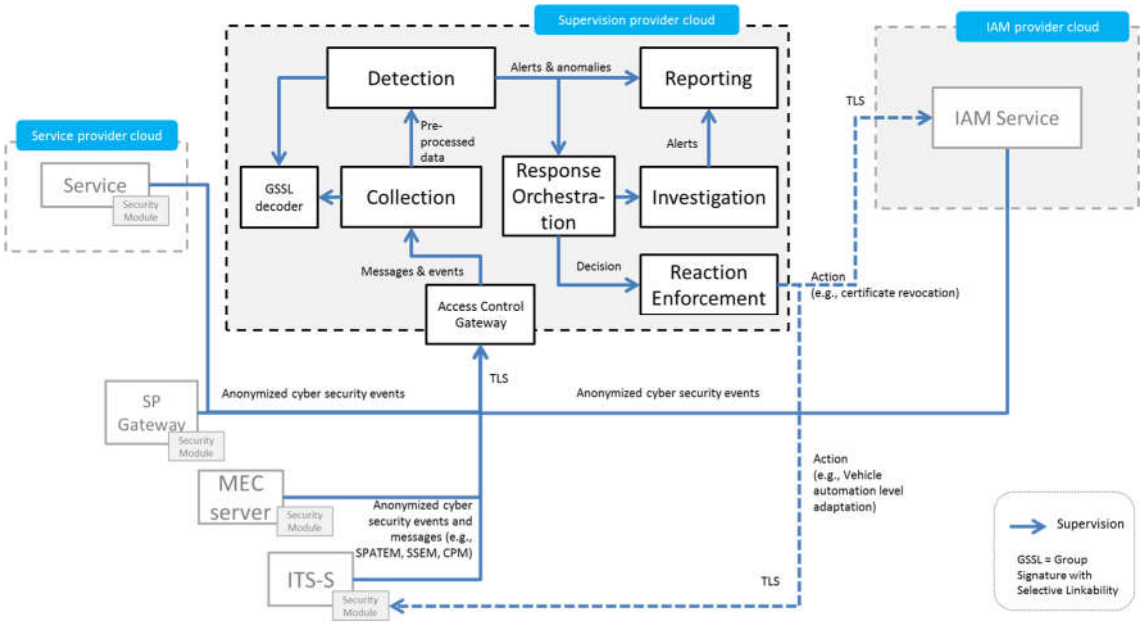

Figure 6: Cyber Security Supervision Service

6.3 Identity and Access Management Service

In compliance with the Certificate Policy for Cooperative Intelligent Transport Systems [11], to ensure that ITS-related services are accessible only by authenticated and authorized devices (vehicles, RSUs, etc.), an identity and access management service is deployed. Secured communications rely on a public key infrastructure (PKI) that enables certificate-holding entities to securely exchange data and verify their legitimacy by supporting the distribution, revocation and verification of public keys used for encryption and linking identities with public key certificates. The PKI follows the C-ITS PKI standards defined in Certificate Policy for C-ITS. Communicating entities are authenticated by getting enrolment credentials from an enrolment authority (EA) and permitted to access services by getting an authorization ticket from an authorization authority (AA).

The authorization ticket pseudonymises the device identity to ensure privacy. Devices can then exchange data pseudonymously with other devices and services. Any communications with an enrolment authority and an authorization authority is encrypted to ensure confidentiality and signed to ensure authentication and integrity. To mitigate communication latency issues, time overhead due to the security layer is limited as much as possible by the implementation of specific technology in security modules and access control gateways. The structure is shown in Figure 7.

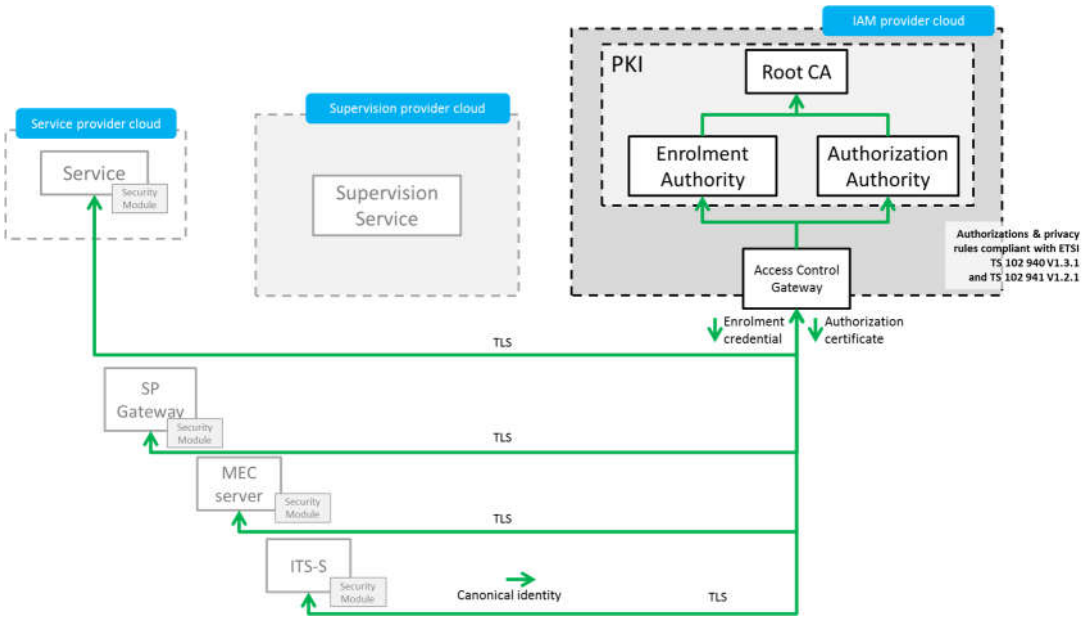

Figure 7: Identity and Access Management Service

6.4 Data privacy mechanism

Preserving privacy is a major concern for the European Union. C-ITS communications have to comply with regulations and standards requiring privacy protection. In ICT4CART, services exploiting data from ITS-S must grant that this is considered. A technology issue is the need by these services to potentially work on relations these data have with each other. To deal with that, an innovation brought by ICT4CART consists in the development of a mechanism to generate group signatures with selective linkability.

Group signatures allow members of a group to anonymously produce signatures on behalf of the group. They are an important building block for privacy-enhancing applications, e.g., enabling user data to be collected in authenticated form while preserving the user's privacy. The linkability between the signatures thereby plays a crucial role for balancing utility and privacy: knowing the correlation of events significantly increases the utility of the data but also severely harms the user's privacy. IBM introduces a new type of group signatures that provides a more flexible and privacy-friendly access to such selective linkability than existing solutions, see Figure 8. When created, all signatures are fully unlinkable. Only when strictly needed or desired, the required pieces should be made linkable with the help of a central entity. For privacy, this linkability is established in an oblivious and non-transitive manner.

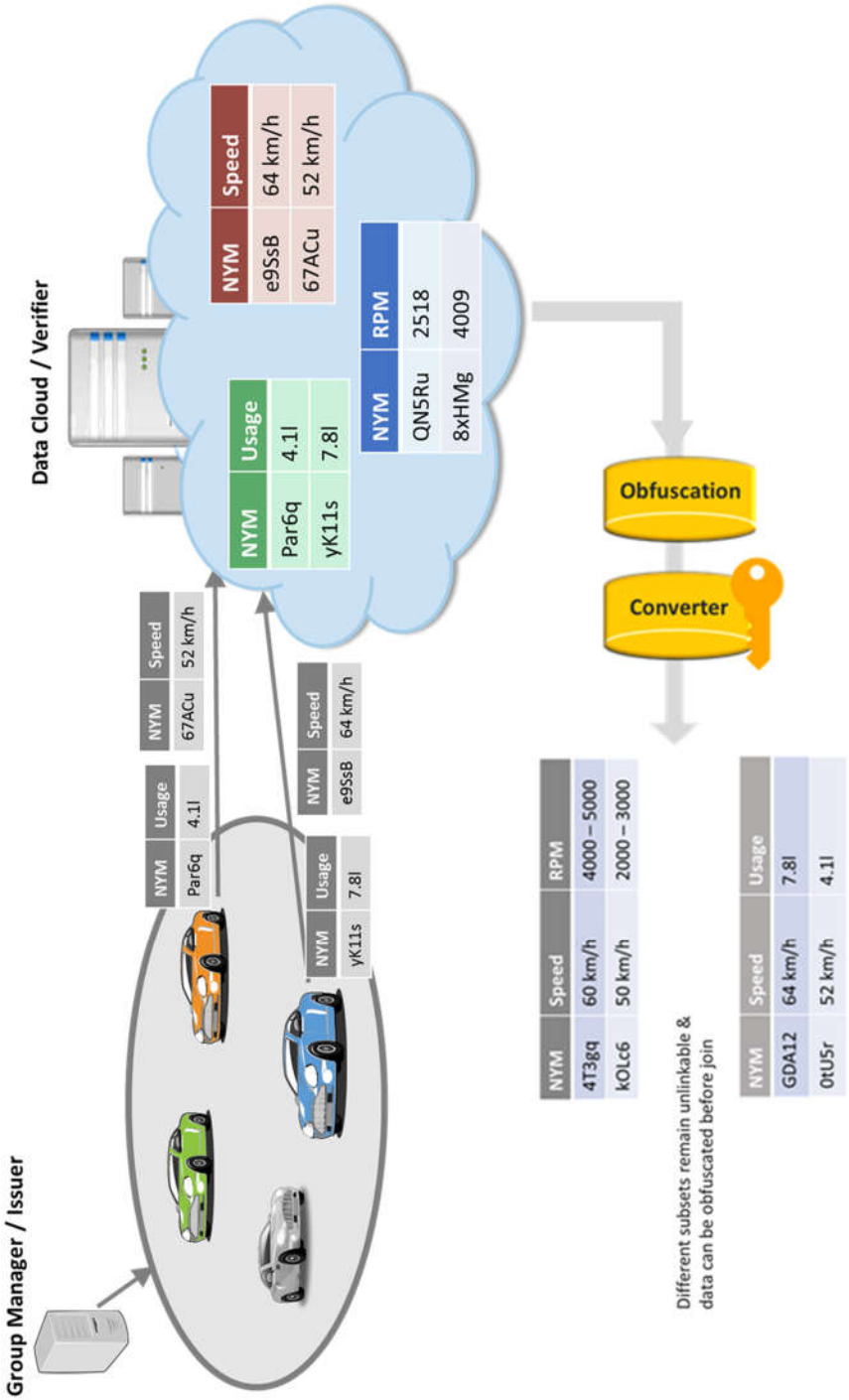

Figure 8: Group Signature with Selective Linkability

7 Conclusion

The ICT4CART Reference Architecture, which has been described in this document, addresses the challenges to enable automated driving by infrastructure means. Therefore, recent developments in communication technology and the IT industry are combined to present solutions like services available via hybrid communication, i.e. using ad-hoc (ITS-G5) and cellular networks (LTE/5G). It embraces these upcoming technologies and presents a unified architecture, which can be used to realize all ICT4CART use cases and beyond.

This deliverable, therefore, first presented a high-level architecture, which showed the basic components that are involved in the ICT4CART system and how they can interact with each other. This was followed by a functional view on the architecture, which explained the functional components in detail. The outlined communication architecture incorporates upcoming technologies such as MEC, ITS-G5, 5G and network slicing. We then identified the key data flows, which occur in the ICT4CART system, and defined the standards, which will be used for the different types of data. A Geo Service will allow vehicles and services to discover MEC servers and Message Brokers in their vicinity. We also introduced new services to address challenges in Cyber-Security, Data Privacy and Communication, e.g., the Identity and Access Management Service, the Supervision Service. Data Privacy is addressed by new concepts based on group signatures with selective linkability.

In the subsequent deliverables D3.2 ‘Flexible Networks Specifications and Architecture’, D3.3 ‘IT environment Specifications and Architecture’ and D3.4 ‘Cyber-security and data privacy Specifications and Architecture’, the ICT4CART Reference Architecture will be further elaborated in the aspects of the Communication architecture, the Data/IT environment and Cyber Security / Data Privacy. The architecture will be implemented, demonstrated and evaluated in WP7 and WP8.