instituto de telecomunicações

Northern Tyrrhenian Sea Port Authority System

Grant Agreement no.: 2016-EU-TM-0044-M

D1 - Pilot C-ITS infrastructure for the Port of Livorno: architectural components of the pilot C-ITS infrastructure and integration patterns with MoniCA.

Deliverable:	D1
Title:	Pilot C-ITS infrastructure for the Port of Livorno: architectural components of the pilot C-ITS infrastructure and integration patterns with MoniCA.
Due date:	23/11/2018
Lead beneficiary:	IT
Contributing beneficiaries:	IT
Nature:	R
Dissemination level:	CO
Version:	1.2

Abstract:

This deliverable is the outcome of the Article 4.1 of the project URSA MAJOR NEO - Consultancy: “Pilot C-ITS infrastructure for the Port of Livorno: architectural components of the pilot C-ITS infrastructure and integration patterns with MoniCA”. The document defines the description of architectural components of the pilot C-ITS infrastructure and integration patterns with MoniCA.

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK.

Document History

Version	Date	Description	Autor(s)	Reviewer	Organization
0.1	18/09/2018	ToC defined	B. Fernandes J.Almeida J. Ferreira J. Rufino		IT
0.2	26/10/2018	First draft	B. Fernandes J. Almeida J. Ferreira J. Rufino		IT
1.0	31/10/2018	Beta release	B. Fernandes J. Almeida J. Ferreira J. Rufino	J. Ferreira	IT
1.1	20/11/2018	Minor revisions and requests by AdSP/CNIT	B. Fernandes J. Almeida J. Ferreira J. Rufino	P. Pagano M. Falcitelli M. Troscia A. Tesei	AdSP/CNIT
1.2	23/11/2018	Final version	B. Fernandes J. Almeida J. Ferreira J. Rufino	J. Ferreira	IT

Executive Summary

This deliverable is the first outcome of the URSA MAJOR NEO - Consultancy contract with the Northern Tyrrhenian Sea Port Authority System for the development of a Cooperative Intelligent Transportation System (C-ITS) at the port of Livorno. As detailed in Article 4 “Activity Timeline”, this document provides the description of the architectural components for the pilot C-ITS infrastructure and the integration patterns with the Monitoring and Control Architecture (MoniCA) platform.

Table of Acronyms

Acronym	Expanded form
3D	Three-Dimensional
AFV	Alternative Fuel Vehicle
AIS	Automatic Identification System
AMQP	Advanced Message Queuing Protocol
AUTOPILOT	Automated Driving Progressed by Internet of Things
API	Application Programming Interface
CAM	Cooperative Awareness Message
C-ITS	Cooperative Intelligent Transportation Systems
CNIT	Consorzio Nazionale Interuniversitario per le Telecomunicazioni
CoAP	Constrained Application Protocol
DENM	Decentralized Environmental Notification Message
ETSI	European Telecommunications Standards Institute
Fi-Pi-Li	Firenze-Pisa-Livorno
GLOSA	Green Light Optimal Speed Advisory
GPDR	General Data Protection Regulation
GPRS	General Packet Radio Service
H2020	Horizon 2020
HMI	Human Machine Interface
ICT	Information and Communication Technologies
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ITS	Intelligent Transportation Systems

IVI	Infrastructure to Vehicle Information
IVIM	IVI-Message
I2V	Infrastructure-to-Vehicle
LoRa	Long Range
LPWAN	Low-Power Wide Area Network
LSPs	Large-Scale Pilots
LTE	Long-Term Evolution
MAPEM	MapData Messages
M2M	Machine-to-Machine
MONI.C.A or MONICA	Monitoring and Control Architecture
MTC	M2M-Type Communications
OBU	On-Board Unit
PMIS	Port Management Information System
REST	Representational State Transfer
RSU	Road-Side Unit
SGC	Strada di Grande Comunicazione
SPATEM	Signal Phase And Timing Extended Message
TPCS	Tuscan Port Community System
TTG	Time to Green
VMS	Variable Message Sign
V2V	Vehicle-to-Vehicle

Table of Contents:

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK.

1 Introduction

This document provides an overview of the ICT modules required for the implementation of road management and assistance to trucks flows along the access routes of the port of Livorno. The main goal consists in the C-ITS design modelling for the Italian pilot site of the Ursa Major Neo project. The port of Livorno has hosted the ETSI ITS Plugtests™ 2016 and constituted a testbed for the AUTOPILOT H2020 project for autonomous driving in connected environments. As a result, some C-ITS infrastructure has been already deployed in the scope of these projects, being available for integration in the traffic management system foreseen in the Ursa Major Neo project. Besides describing the pre-existing physical infrastructure and software components, the present deliverable details the core modules of a C-ITS system and the required Day 1 and Day 1.5 services for the implementation of the target use cases. At the end of the document, the proposed architecture is presented, together with the operation of the C-ITS infrastructure in the presence of hybrid communications and security features.

2 Objective and Use Cases

The main goal of this pilot project at the port of Livorno is to develop a series of C-ITS services for the Port Authority. This way, it will be possible to provide added value in the logistics sector, enhancing safety and efficiency in the port businesses.
The C-ITS infrastructure to be deployed at the Livorno pilot will enable the following use case scenarios:

- Bottleneck removal: real-time information and early notification about potential traffic congestion, accompanied by the suggestion of alternatives routes;
- Safety information: real-time information about hazards detected ahead on the road;
- Smart truck parking: drivers will be suggested to make use of the freight village smart parking premises for a time lapse optimized on the basis of the real-time traffic along the route and the operational status (i.e. destination terminal handling capabilities) at the port of Livorno.

3 Existing Architecture

3.1 Geographical Scope

The project pilot site encompasses the access routes to the port of Livorno, namely the Livorno-Verona Freight Village corridor, which includes the *strada di grande comunicazione* (SGC)

Firenze-Pisa-Livorno (Fi-Pi-Li) motorway. In total, 70 kms of road infrastructure will be covered by C-ITS services. Figure 1 depicts the region where the C-ITS services will be deployed.

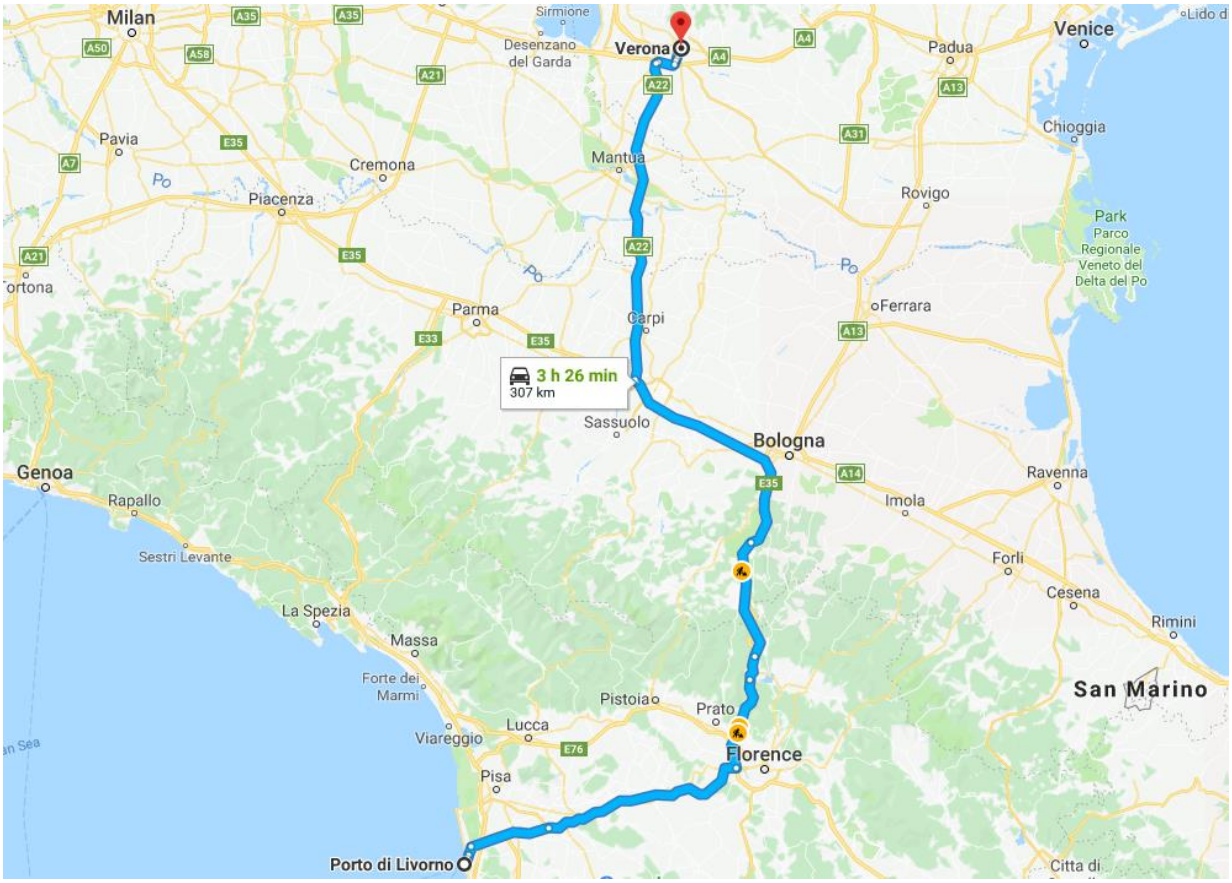

Figure 1 - Geographical scope of the project pilot site

3.2 Pre-existing Infrastructure

The pilot site already has some available infrastructure, previously deployed in the scope of the AUTOPILOT project, one of the European Commission's Large-Scale Pilots (LSPs) for autonomous vehicles in connected environments. As a result, both physical and data infrastructure have been developed to support use cases for autonomous driving.

Regarding the physical infrastructure, a group of sensors and communication units is available both at the Fi-Pi-Li highway, as well as at the Livorno port area. On the Fi-Pi-Li motorway, three road-side units (RSUs) equipped with both LTE and ETSI ITS-G5 technologies are located on kms 12, 69 and 73, as shown in figure 2.

Figure 2 - C-ITS infrastructure available at Fi-Pi-Li motorway

Within the port area, two more RSUs are available, as well as a smart traffic light connected to a camera that is able to detect the presence of pedestrians in a crosswalk. As depicted in figure 3, these devices are installed in a more urban area inside the harbour, close to the CNIT lab. For the use cases of Ursa Major Neo project, this specific part of the infrastructure will probably not be very useful, since the freight corridor and truck parking zone are located in the northern part of the harbour.

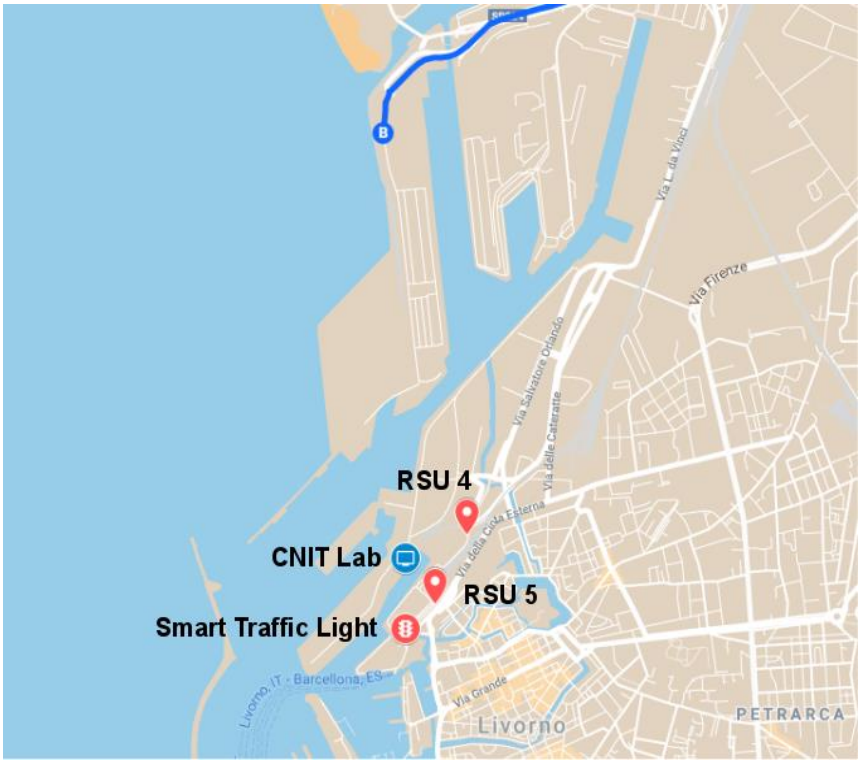

Figure 3 - C-ITS infrastructure available at the port of Livorno

3.3 Pre-Existing Software

A single horizontal platform is used to ensure the exchange and sharing of data among all services, devices, programs and projects running at the seaport. It is capable of providing an interworking framework and enabling the re-use of the already available infrastructure. The architecture chosen for the platform was based on oneM2M, a standardization endeavour on M2M and IoT communication.

This distributed software layer, composed of multiple subsystems, works as an operating system for the seaport. The platform is sustained by an always connected environment constantly feeding real-time heterogeneous information. The gathered data is aggregated, processed, analysed and transformed by the platform, becoming available to different actors through well-defined APIs.

Having a focal point of communication to a panoply of entities enables a comprehensive perception of the seaport status. This cooperative approach allows for a safer, more efficient operation of this complex system. Thereby, starting from this digital port platform, it is possible to monitor, observe, coordinate and orchestrate services related to the seaside (i.e. connected ships), the landside (smart mobility, info-mobility, services for passengers and cruisers) and connected communication routes (enhancing road, rail and maritime mobility).

This solution was named **MONI.C.A.** or **MONICA,** which stands for MONItoring and Control Architecture for the port of Livorno. The acronym refers to the ICT stack as a whole, but in fact, MONI.C.A. can be divided in three cloud computing layers: Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (Saas). Located between applications and devices, the main goal of the platform is to provide consistency in how devices, servers, applications and services communicate. This enables the available infrastructure to be used as a service, allowing sensors and actuators to be tuned to specific needs. Finally, every service or application that relies on the information served by the platform, and in specific cases enhanced by external sources, is in the SaaS layer.

Without the SaaS layer, the usage of the platform is impractical, it needs a set of data visualization tools in order to increase its usability. A core MONI.C.A. application, a dashboard for the port providing a 3D and real-time visualization interface for different seaport operations, offers a set of tools and services for a grained control of the seaport. More specifically, through this application, operators can, for instance, discover the images detected by cameras, set trigger values and discover real-time readings on sensors. They can also be visually notified when dangerous goods are carried by vessels and can look into it at the detail level of a single container.

Different dashboards can co-exist. In fact, another key application is the Tuscan Port Community System (TPCS), which is used for the coordination of public and private agencies responsible for handling and inspecting goods. It allows goods to be tracked, validated, inspected and monitored in real-time. This integration point alienates the need for multiple proprietary solutions to be used, simplifying or even automating most of the validation processes and therefore reducing the overall costs and increasing efficiency. Portofacile is also an integrating part of MONI.C.A., it works as a web portal for managing the main functional practices for port operations. Responsible parties

can make requests through a common interface that exploits the richness of the data available in MONI.C.A. and similar platforms.
With the existing functions it is already possible to interoperate with the PMIS, the portal of the port authorities, with PELAGUS, the database of AIS data managed by the general command of the Port Authorities, as well as to acquire infomobility data from the 3iPlus portal managed by the Tuscany Region. The integration of networks and sensors takes place through the Common Service Layer, the heart of MoniCA.
Although there is a well-founded work in maritime mobility, components for road mobility are still missing from the platform. The next sections and subsections will provide the basic information on the services that need to be added to achieve a fully Cooperative Intelligent Transportation System (C-ITS).

4 Cooperative Intelligent Transportation Systems

4.1 Purpose

The cooperative intelligent transportation systems (C-ITS) are the next trend on safer, more efficient and responsive road vehicles. Instead of focusing on self-centred and proprietary solutions, where vehicles mostly rely on their own capabilities to assess the surrounding environment, C-ITS augments the awareness and decision-making process with information gathered by surrounding road-users. Consequently, such systems urge for concerted information-sharing, cooperation, and coordination between vehicles (V2V), vehicles and infrastructure (V2I), and vehicles and other systems (V2X). Under the ETSI ITS philosophy, vehicles broadcast different types of messages, the most common being Cooperative Awareness Messages (CAMs), comprising vehicle attributes such as physical dimensions, speed, direction, and location, and Decentralized Environmental Notification Messages (DENMs), which convey information regarding hazardous events and other types of relevant sporadic incidents.

4.2 Components

In this section the most important elements of the C-ITS system are introduced. Figure 4 depicts the interconnections between these five core components:

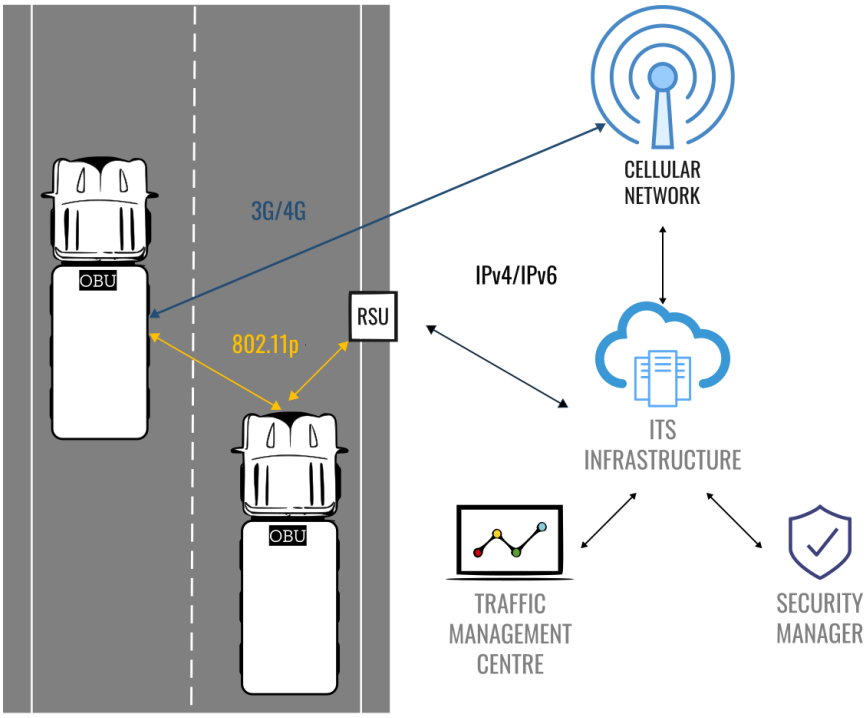

Figure 4 – Components of the ETSI Standard Architecture

On-Board Unit (OBU)
This component is installed on the road user or operator vehicle. It is responsible for sending and receiving information to/from other vehicles (OBUs) or roadside units (RSUs). This information can be: periodically generated (Cooperative Awareness Messages - CAMs) with position, speed, etc.; automatically generated by the on-board sensors (e.g. emergency brake light); or manually triggered through a human-machine interface (HMI) (e.g. reporting an object on the road) using Decentralized Environment Notification messages (DENMs).

Road-Side Unit (RSU)
This unit is the interface between the ITS infrastructure (ITS-I) and the vehicle. It receives the vehicle information, stores it for later analysis, processes it (e.g. aggregates CAMs to reduce the network burden) and then sends it to the infrastructure. The reverse is also done by sending important notifications from the infrastructure to the vehicle.

ITS Infrastructure (ITS-I)
It receives and processes information from all the road side units and makes it available to the traffic management centre (TMC). It also receives data from the TMC to be sent to the users, translating it and using the appropriate channel.

Traffic Management Centre (TMC)
This element is responsible for displaying real time events that may affect traffic safety and gives to the operator the ability of taking actions that will be routed to the user by the ITS-I and RSUs.

Security Manager (SM)
This element is responsible for ensuring the authenticity, accountability, confidentiality, availability and integrity of all entities on the C-ITS domain.

4.3 Communication Systems

Neither ETSI ITS G5 nor cellular systems can provide the full range of necessary services for C-ITS. It is essential to ensure that vehicular messages can be transmitted independently from the underlying communications technology (access-layer agnostic) wherever possible. Consequently, a hybrid communication concept is needed in order to take advantage of complementary technologies. Due to its latency specifications, it is recommended that:

- for short-range communications, the communication system to be used is IEEE 802.11p / ETSI ITS-G5;
- to extend the geographical coverage obligations, the communication system to be used is the existing cellular communications infrastructure, also used as backup communication system.

Using hybrid communications, we can connect more devices and cover a broader area, quicker and more cost efficiently. In this way, the current C-ITS coverage areas can be extended from local regions up to a national level. In the context of the project Ursa Major Neo, a hybrid communication permits, for instance, to cover the full extent of motorways between Verona freight village and the Port of Livorno. On the other hand, by using cellular networks, we add extra communication delays (and jitter) in comparison to VANETS, due to the topology of the cellular network.

The European Commission strategy for ITS states that:

- C-ITS is a starting point; the objective is to move into a Cooperative, Connected and Automated Mobility (CCAM) paradigm (depicted in figure 5).
- Deployment of Day 1 and 1.5 services will be made using hybrid communications starting from 2019.
- Security is a critical point of C-ITS communications.
- It must be assured the continuity of C-ITS services.
- GPDR needs to be implemented for data protection.
- C-ITS needs to be compliant & interoperable.
- Hybrid communication should be used as a complementary communication technology, and they are future-proof.
- Protocols should be communication layer agnostic.
- Current mature technologies are: 3G/LTE and ITS-G5.
- Cellular and ITS-G5 are both needed to adequately cover all Day 1 services.
- Support for safety-related transport services.
- Cross-border interoperability.
- Efficiently use of the spectrum allocated for C-ITS.

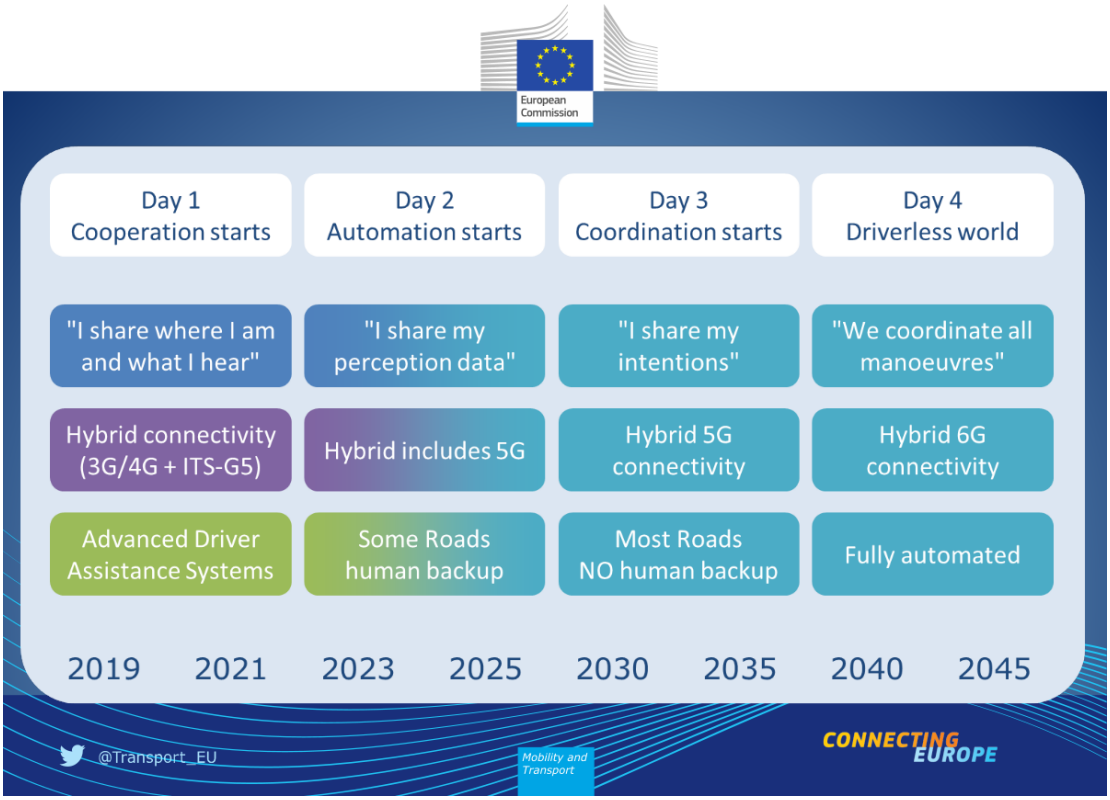

Figure 5 – EU point of view on integration of services and hybrid communications (source:http://goo.gl/DcPn1u)

4.4 ETSI ITS Reference Architecture

As depicted in figure 6 the ETSI proposal for the ITS architecture has three major layers: (i) Access, (ii) Network and Transport, and (iii) Facilities. The access layer is further subdivided into Physical (PHY), Medium Access Control (MAC) and Logic Link Control (LLC), also commonly referenced as MAC extensions.

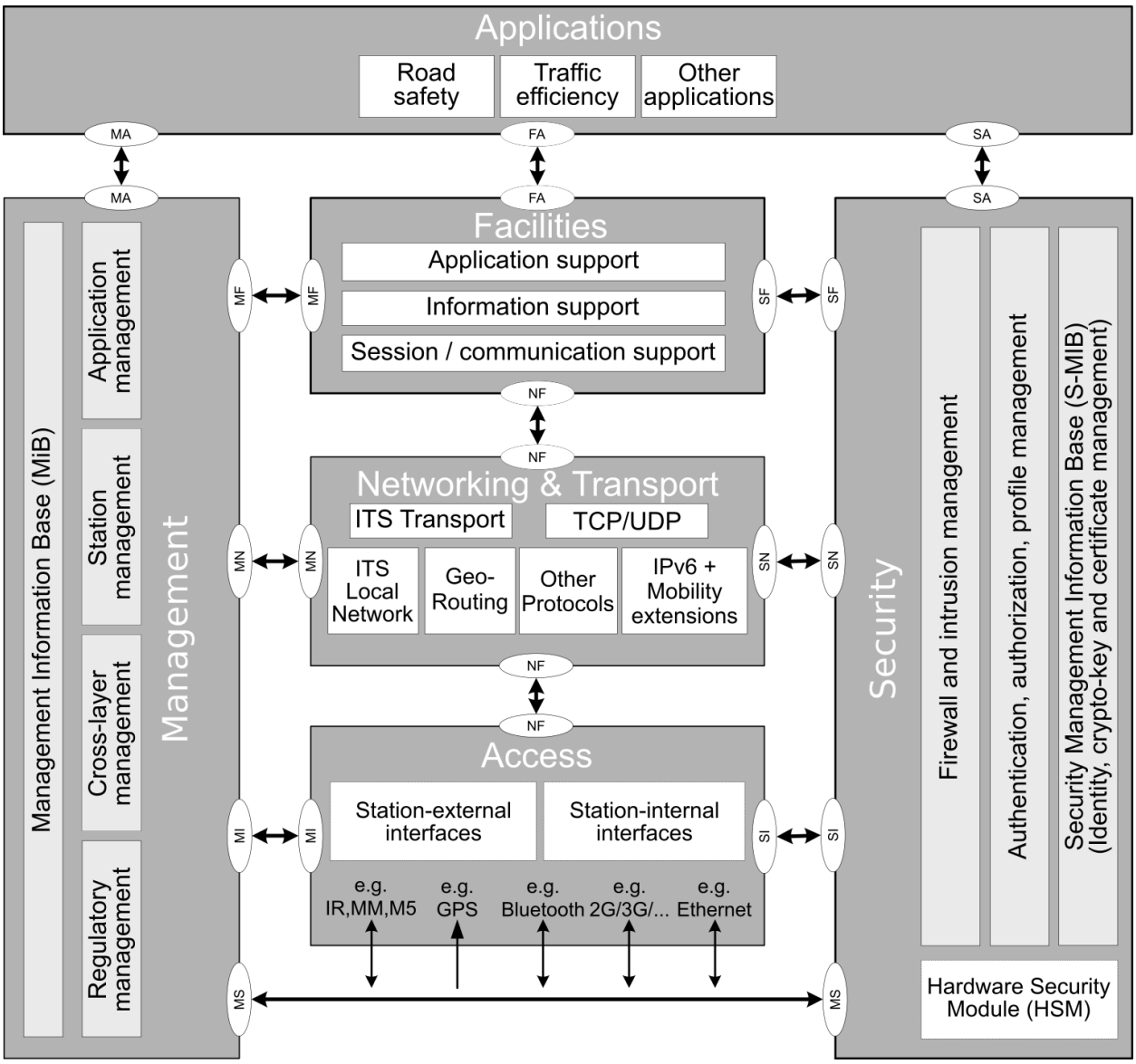

Figure 6 - Overview of the ETSI ITS architecture (source: https://goo.gl/YQToCe)

The Network and Transport layer comprises two different protocol stacks: a standard IP and a lightweight non-IP stack, containing its own set of transport and network protocols which can be used by applications to meet specific requirements. The most commonly used for safety-related applications is the non-IP stack. Safety applications rely on the combination of Geo-networking (GN), a network protocol, with a transport protocol known as Basic Transport Protocol (BTP). While GN provides geographic addressing and forwarding, BTP gives an end-to-end, connectionless transport service to the ITS ad-hoc network. BTP has features similar to those of UDP, offering non-guaranteed delivery through a minimal transport service. Using these protocols

it is possible to, for example, disseminate warning or generic information messages within specific geographic areas.

The Facilities layer offers a set of core functionalities that can be explored by internal and external applications and services. It contains the functionality of the upper OSI layers, i.e. application, presentation, and session layer, with amendments tailored for ITS communications and provides the necessary support for ITS applications to share generic functions and data, improving the interoperability between systems. Facilities include, amongst other utilities, Human-Machine Interface (HMI), data coding/decoding, and most importantly, provide the common messages used for data exchange between ITS applications. An overview of these messages is next presented.

ITS applications are categorised into three main application areas: (i) road safety, (ii) traffic efficiency and (iii) others. Road safety-related applications mainly rely on Cooperative Awareness Message (CAM) and Decentralized Environmental Notification Message (DENM) messages. CAMs contain the ITS station status and physical attributes as well as current location and are periodically broadcast in order to create awareness. CAM broadcast intervals depend on traffic dynamics and communication channel congestion status, however, they must not be inferior to 100 ms and superior to 1000 ms. DENMs are mainly used by ITS applications to alert road users of a detected sporadic event, e.g. car crash. The combination of CAMs and DENMs ensure a cooperative environment perception.

This perception can be further enhanced by MAP Extended Message (MAPEM) and Signal Phase And Timing Extended Message (SPATEM) messages. The former contains information regarding road topology, e.g. available lanes, traffic directions and surrounding crosswalks, while the latter presents operational states of traffic lights and allowed manoeuvres. MAPEM and SPATEM are typically broadcast by infrastructures located at conflict points, e.g. intersections. MAPEM and SPATEM messages may also be used by applications that aim to improve traffic efficiency such as, for example, time-to-green applications, where the time to receive the right-of-passage at an intersection is presented to the user.

For traffic efficiency applications, Infrastructure to Vehicle Information Message (IVIM) messages provide the receiver with mandatory and advisory road signage such as local speed limits and roadwork warnings. With IVIM, infrastructures at conflict points are envisioned to improve, or even replace, physical road signs and lights. This information is summarized in table 1.

Message Type	Description
CAM	A periodic message sent by ITS-Stations indicating its status. CAMs are used to exchange information between ITS stations about the time, motion, position, vehicle type, etc. to build cooperative awareness among the vehicles on the road.
DENM	DENMs are mainly used by ITS applications to alert road users of a detected event that has a potential impact on the roads safety or traffic condition. They can be triggered automatically by the on-board sensors or manually triggered through an HMI (road user or operator)
IVIM	IVIMs allow specific messages to be sent to vehicles, e.g. they can be used to inform road users on actual, static or dynamic (virtual) road signs via in-vehicle systems. The road signs can be mandatory or advisory.
SPATEM	SPATEMs include safety related information for supporting traffic participants (vehicles, pedestrians, etc.) to execute safe manoeuvres in an intersection area. The goal is to enter and exit an intersection "conflict area" in a controlled way. It informs in real-time about the operational states of a specific intersection, the current signal state, the residual time of the state before changing to the next state.
MAPEM	MAPEMs are digital maps defining the topology of a specific area. It includes the lane topology for e.g. vehicles, bicycles, parking, public transportation and the paths for pedestrian crossings and the possible maneuvers within an intersection area or a road segment.

Table 1 - C-ITS message type description

4.5 C-ITS services

Since 2014 the European Commission is bringing together different stakeholders to accelerate the deployment of Cooperative ITS in Europe. In the end of 2016, the European Commission issued a communication on C-ITS indicating the planned actions as well as recommendations on how to achieve European deployment of C-ITS. This was supported by ETSI, a European standardization organization, by updating the relevant specifications.

In the roadmap for C-ITS, two sets of services were presented, day 1 and day 1.5 services. Together they are the building blocks for a fully C-ITS system. In the Ursa Major Neo project for the Livorno pilot site, three different use cases are specified, namely the safety information services that will enable traffic safety due to improved hazard warning, the bottleneck removal

service that will relieve congestion and improve traffic flows by suggesting alternative routes, and the smart truck parking service that will allow trip management and port access planning for freight from/to the port area. The C-ITS services are mapped into the Ursa Major Neo project use cases in tables 2 and 3. As can be seen, there are some services that cannot be mapped to the requested use cases, and therefore will not be defined as mandatory.

Services		Use Cases		
ID	Designation	Safety information	Bottleneck removal	Smart truck parking
1	Emergency electronic brake light	x		
2	Emergency vehicle approaching	x		
3	Slow or stationary vehicle(s)	x	x	
4	Traffic jam ahead warning	x	x	
5	Hazardous location notification	x	x	
6	Road works warning	x	x	
7	Weather conditions	x		
8	In-vehicle signage	x		
9	In-vehicle speed limits	x		
10	Probe vehicle data	x	x	
11	Shockwave damping		x	
12	GLOSA / Time to Green (TTG)			
13	Signal violation/Intersection safety			
14	Traffic signal priority request by designated vehicles			

Table 2 - Day 1 C-ITS services

Services		Use Cases		
ID	Designation	Safety information	Bottleneck removal	Smart truck parking
1	Off street parking information			x
2	On street parking information and management			x
3	Park & Ride information			
4	Information on AFV fuelling & charging stations			
5	Traffic information and smart routing		x	
6	Zone access control for urban areas			
7	Loading zone management			x
8	Vulnerable road user protection (pedestrians and cyclists)			
9	Cooperative collision risk warning	x		
10	Motorcycle approaching indication			
11	Wrong way driving	x		

Table 3 - Day 1.5 C-ITS services

4.5.2 Day 1 Services

Day 1 services can be divided in two different categories: Hazardous Location Notifications (HLN) and Signage Applications (SA). The first ones include the “Emergency electronic brake light”, the “Emergency vehicle approaching”, the “Slow or stationary vehicle(s)”, the “Traffic jam ahead warning”, the “Hazardous location notification”, the “Road work warnings” and the “Weather conditions”.

All of these services are important for the implementation of at least one of two use cases, namely the safety information and the bottleneck removal. Figure 7 depicts the operation of some HLN services in a highway scenario. For instance, in case of the emergency vehicle approaching, the freight vehicle can receive this information directly through a CAM message if the emergency vehicle is equipped with an On-Board Unit (OBU). Otherwise, if the traffic control center is aware of the emergency vehicle’s position, the cloud platform can disseminate this information through the roadside infrastructure or the cellular network, using DENM messages. A similar flow of information takes place with notifications of hazardous events, such as the presence of puddles, slow or stationary vehicles or traffic jams. However, for some specific services, like the emergency brake light or a traffic crash, the direct vehicle-to-vehicle (V2V) communications link is fundamental, in order to transmit the DENM message within strict time bounds for the following vehicles.

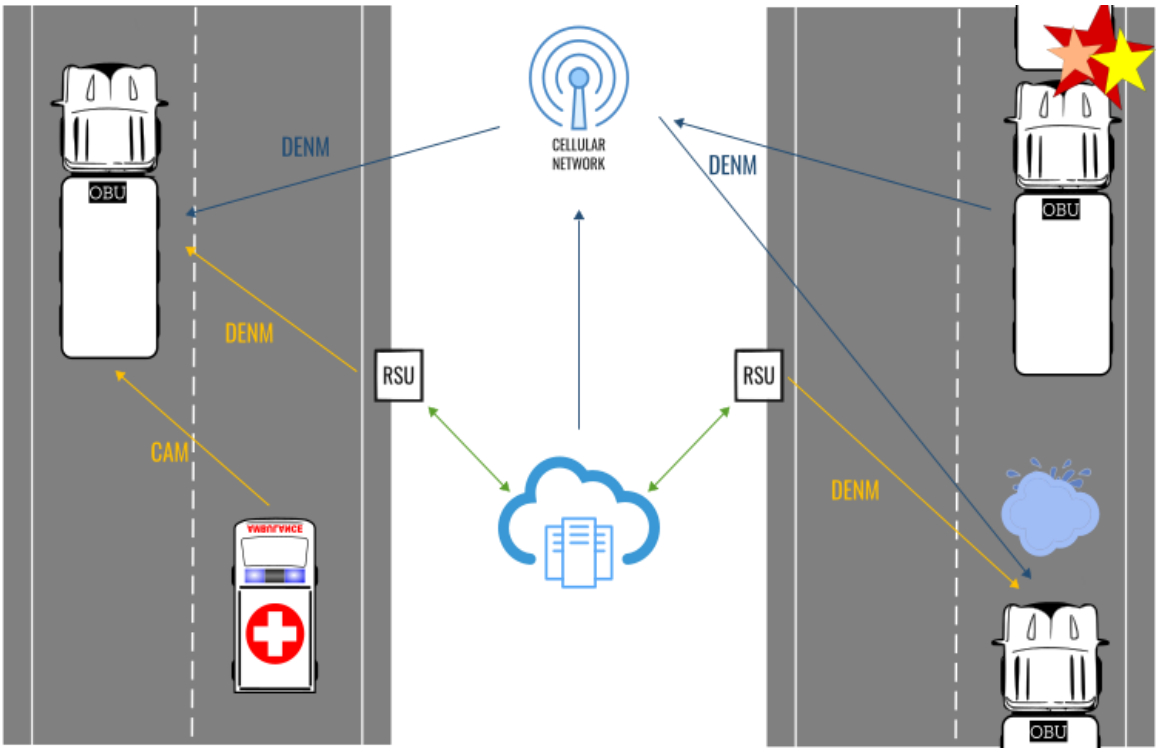

Figure 7 - Hazard Location Notifications (Day 1 C-ITS services)

On the other hand, the Signage Applications include the “In-vehicle signage”, “In-vehicle speed limits”, “Probe vehicle data”, “Shockwave damping”, “GLOSA / Time to Green (TTG)”, “Signal violation/Intersection safety”, “Traffic signal priority request by designated vehicles”. In the scope of URSA Major Neo project, the last three services will not be necessary, since they are specific for central urban areas, with road intersections and traffic lights. Figure 8 shows how the in-vehicle signage and speed limits can be deployed. Basically, the network only needs to disseminate SPATEM, MAPEM and IVIM messages to the freight vehicles, typically using the roadside infrastructure located close to the transit signals. Regarding the “Probe vehicle data” and the “Shockwave damping” services, these services require the collection of CAM messages from the vehicles and additional data analysis at the cloud platform.

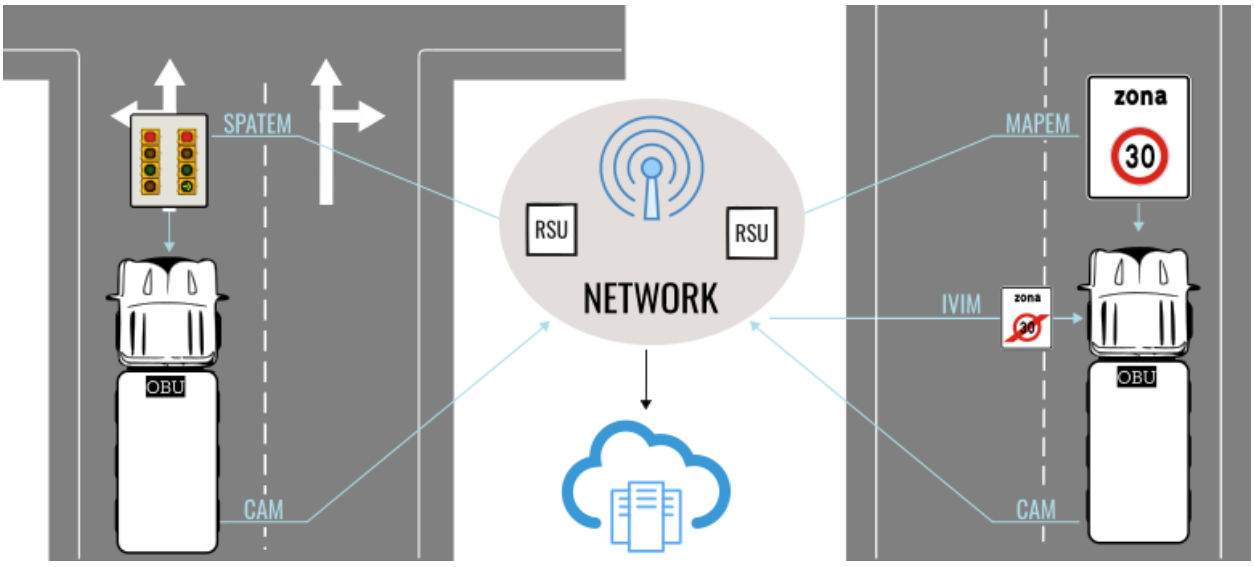

Figure 8 - Signage Application (Day 1 C-ITS services)

4.5.3 Day 1.5 Services

With respect to the Day 1.5 services, again there are some services that are not required. The “Park & Ride information”, “Zone access control for urban areas” and “Vulnerable road user protection (pedestrians and cyclists)” are related to the urban use cases, which are outside the scope of this project. Additionally, the “Information on AFV fuelling & charging stations” consists in the broadcast of information for charging electric or alternative fuel vehicles. Regarding the services of interest for this pilot site, the “Cooperative Collision Risk Warning” and the “Wrong Way Driving” can be implemented similarly to the HLN Day 1 services, as well as the “Traffic information and smart routing”, useful for the bottleneck removal use case. The latter

service may require external sources of information to the ITS system, such as a Traffic Control Centre, Google Traffic, Waze, etc.

Finally, the “Off street parking information”, the “On street parking information and management” and the “Loading zone management” are the services required for the implementation of the smart trucking parking use case. The first two services allow the freight vehicles to receive information regarding parking topology, capacity and availability, through the dissemination of IVIM and MAPEM messages in an infrastructure-to-vehicle (I2V) communications link. The “Loading zone management” service supports the driver, fleet manager and road operator in the booking, monitoring and management of the parking zones for freight driver activities. The driver/fleet operator can book in advance a parking spot, specifying the delivery mission, the planned delivery time, the loading/unloading time required, the vehicle type, any flexibility (e.g. ±15 mins) in the delivery time and the estimated time to reach the parking zone (interaction with traffic management). The fleet operator can optimize delivery times, reduce driver stress, anticipate congestion problems and optimize the management of parking zones through better knowledge of the delivery time period and duration.

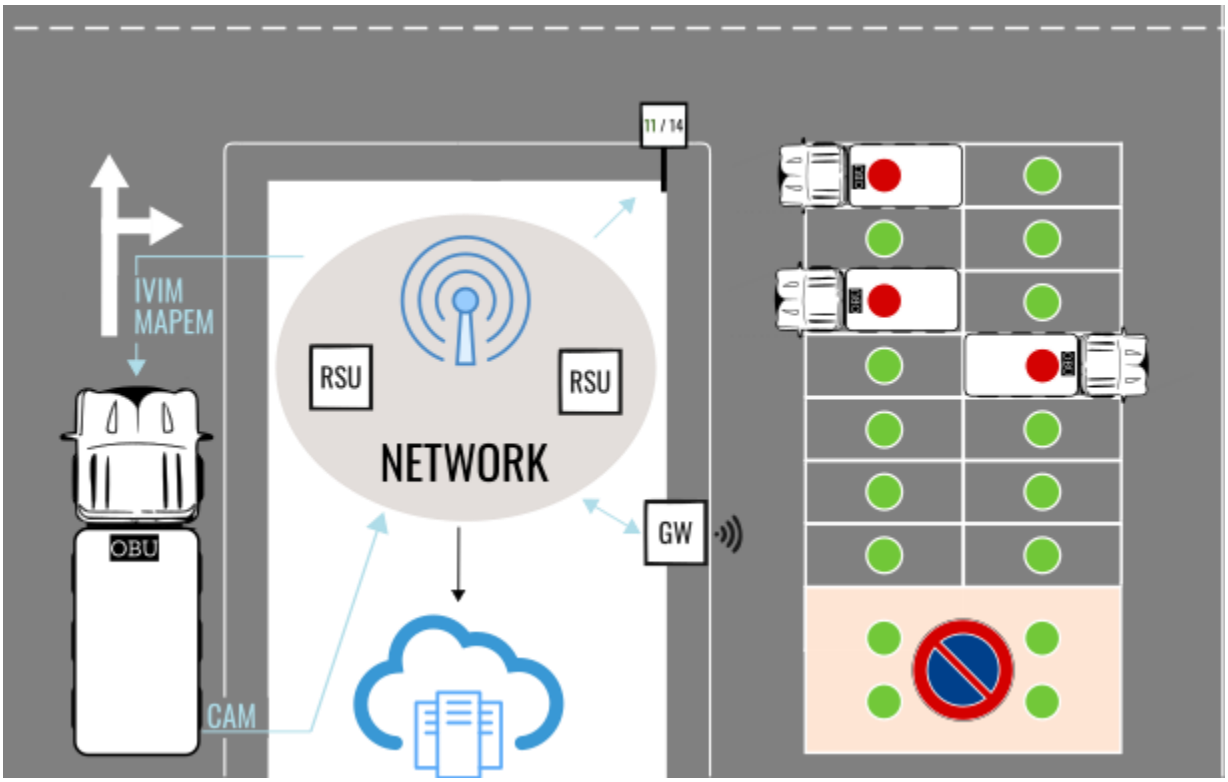

Figure 9 - Smart Truck Parking use case (Day 1.5 C-ITS services)

Figure 9 depicts the smart truck parking scenario, where each parking lot is equipped with occupancy detection sensors. This information is constantly being collected through a low-power

wide area network (LPWAN) that uses a gateway to publish this data in the cloud platform. This information is then disseminated by the RSUs or the cellular network (IVIM and MAPEM messages) to the freight vehicles (OBUs). It can also be displayed in Variable Messages Signs with real-time availability of the parking lots. For pre-reservation/booking of a parking place before the truck arrives to the destination, there are two possible ways. Either the port authority automatically attributes a spot for every vehicle travelling to the local area with some time in advance and does not have any interaction with the driver, or the system allows the driver to make a request for a parking place in a specific time window.

5 Proposed Architecture

The proposed architecture is based on the common Internet of Things (IoT) paradigm, being characterized by the relevant features of this approach, namely openness, flexibility and interoperability. It provides global coverage of the C-ITS pilot site, integrating distinct types of sensors and communication units. This IoT-based architecture also takes advantage of well disseminated standards for the communication purposes and for the definition of its interfaces. It encompasses a variety of devices, from the parking sensors and Variable Message Signs (VMS) to the Road-Side Units (RSUs) and in-vehicle platforms (On-Board Units or OBUs).

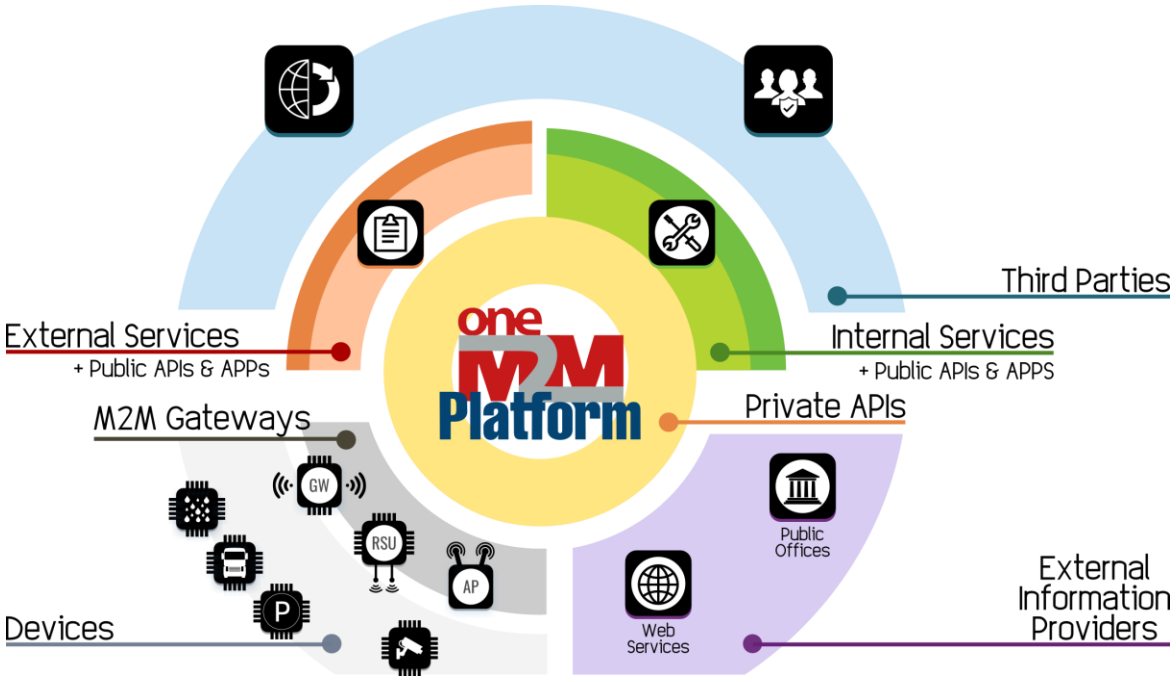

Figure 10 - Overview of the proposed C-ITS architecture.

Figure 10 presents the several domains of the envisioned C-ITS framework. The field domain includes all the different sensors and actuators present in the physical infrastructure, e.g. cameras, radars, parking occupancy detectors, weather stations, smartphones, VMS, RSUs and OBUs. All these devices exchange information through Machine-to-Machine (M2M) type communications (MTC), using gateways (LoRa, ETSI ITS-G5, ...) or other technologies (e.g. GPRS, LTE) to connect with the platform. Additionally, there are external sources of information to the system, comprised by the data available from external providers, for instance Meteo Aerounatica, Waze, AccuWeather and Google Traffic.

A central IoT platform based on the oneM2M standard is used to exchange IoT messages and to store all data. On this platform, there are also buildings blocks responsible for device management, process and service management, security, etc. It is possible to get access to the oneM2M platform through private APIs. For instance, internal services are embedded on the platform making some public APIs available to the end user, while other external services such as the Port Monitoring Centre (MoniCA - Monitoring and Control Architecture) are directly connected to the oneM2M platform. On top of this, third parties applications and services can be developed using public APIs to access the central platform, through either internal or external services.

5.1 Components

As explained before the proposed solution can be seen as an extension to the oneM2M MONICA standard architecture. Figure 11 depicts the different components of the architecture. At the lower level, devices and sensors can communicate directly with the platform or through a mediator. The latter option allows them to function in a network-agnostic manner, exchanging information with a gateway. These middle nodes not only become a connection point to multiple devices but also a communication point with the platform. The platform offers a set of common services, functions and interfaces that provide consistency in how devices, servers and applications communicate. External entities and third-party applications can have the same privileges by registering to these services or exploiting public available interfaces. Each level will be depicted in the following subsections.

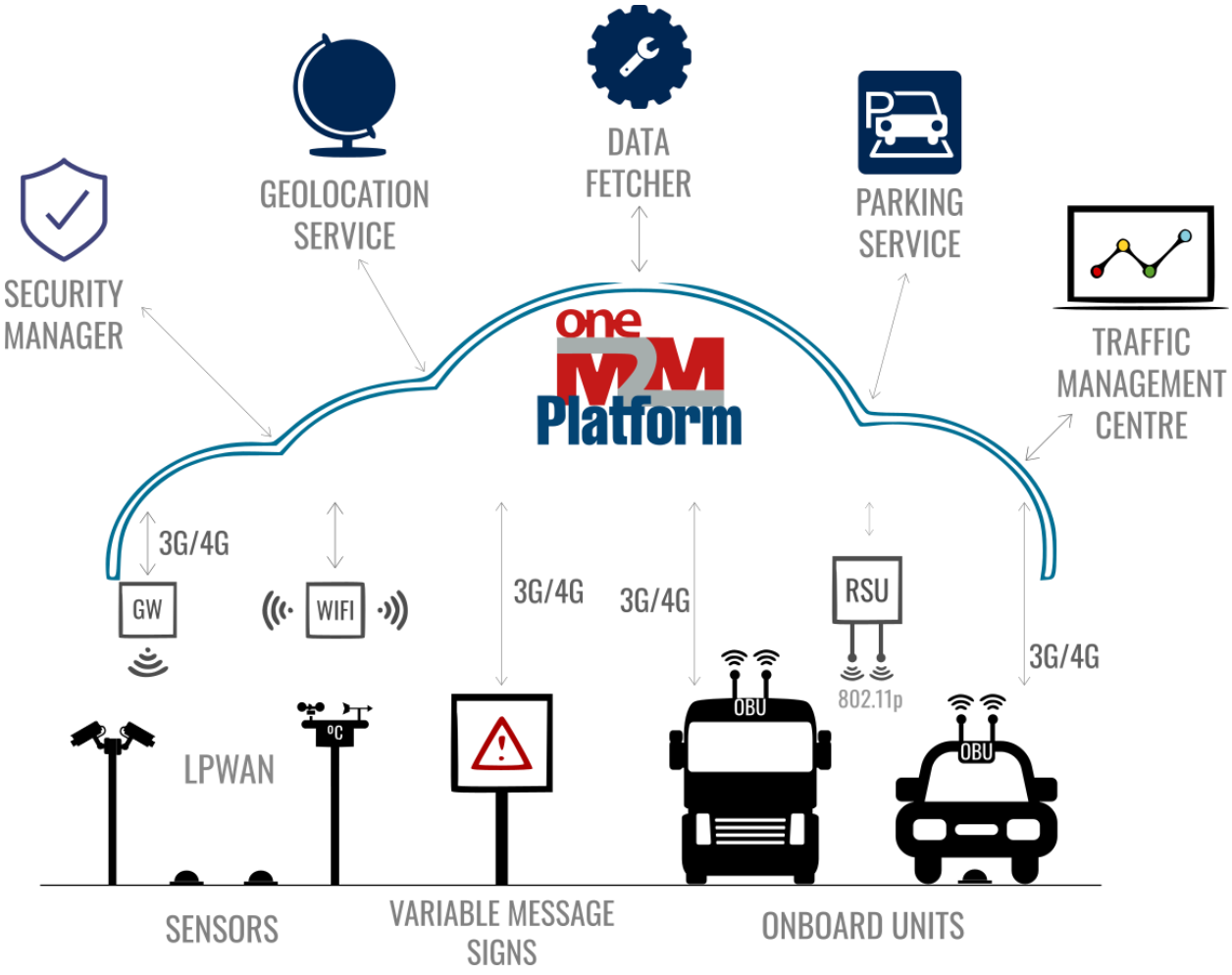

Figure 11 – Components of the proposed architecture

5.1.1 The field domain

This domain is characterized by devices with low or reduced budget in terms of energy, processing power, storage, etc.

5.1.1.1 OBUs

OBUs are units responsible for collecting information regarding the vehicle status. OBUs are deployed inside vehicles and work as gateways to the vehicle integrated sensors. Additionally, they are connected to an HMI, used as communication interface with the user. In more extreme scenarios, vehicles can be the ones to predict an imminent accident and broadcast it. The driver can use the HMI to share information regarding his surrounding environment. The information

perceived by the OBU is translated in CAMs or DENMs and sent to the platform (directly or through an RSU).

5.1.1.2 RSUs

The RSUs, located in strategic positions along the roadside, are connection points to multiple devices (namely OBUs, road works stations and traffic cameras). Roadside units are the middle-points between the vehicle and the platform, they can detect trajectories, speed and heading of the approaching vehicles in real time. In the case of eminent danger, the RSU can alert users directly by triggering a warning DENM. In resume they work as mediators to OBUs, enhancing their overall perception of the complex road environment through CAMs, DENMs, IVIMs, SPATEMs and MAPEMs.

5.1.1.3 Parking Sensors

Parking sensors are used to monitor the occupancy of specific zones in the port. They are deployed on the ground, in each parking space, for the respective occupancy detection. They can also be deployed in areas where parking, stopping or standing is strictly prohibited in order to quickly detect any illegal occupancy. The status of the affected area is communicated periodically in order to save energy. The sensor does not require cabling, as it features wireless communications and internal batteries for power. If possible, the sensor should also provide a visual output (e.g. with different light colours) to the drivers at the parking place. This way, one can announce that a specific spot is reserved, even for vehicles not belonging to the fleet operator.

There are two mandatory parking sensor types of communication:

- Status change notification: following a sampling event, the data is analysed and, in case a status change is detected, the sensor sends the respective communication/notification to the system;
- Keep alive notification: if no status change is verified for a defined period of time, the sensor sends an “Keep alive” message.

5.1.1.4 Parking System Dedicated Gateway

Each gateway receives information from nearby parking sensors, aggregates and sends it to the platform. Besides collecting data regarding the individual parking occupancy status, it also informs the central platform about malfunctioning sensors, for instance the ones that stop transmitting “Keep alive” messages.

5.1.1.5 Variable Message Signs

VMS are used to visually inform the users about the occupancy status of nearby parking spaces, guiding them to the most suitable parking spot. This information is typically useful for vehicles not belonging to the fleet operator, since they are not able to book a parking spot in advance.

5.1.2 The platform domain

The oneM2M platform is a generalization of the standard MONI.C.A. platform. It is a software layer, consisting of all cloud-based components responsible for data collection, parsing, storage and provision from the databases to the connection points to other services and multiple platforms.

It is a central point of communication that consistently stores the information and provides different endpoints for retrieval, update, injection and deletion of data. In addition, it provides information triggering and notification through messaging protocols that can be used for device, services, servers and other platforms interworking.

5.1.3 The services domain

Five different services need to be implemented in order to provide the basic functionalities for C-ITS applications.

5.1.3.1 Data Fetcher

In order to receive fully updated information it is crucial for different Traffic Management Entities to share data. The Data Fetcher works as a translator between different platforms, it collects and transforms the received information into predefined structures that can be published to specific oneM2M platform endpoints. One of the most used examples are DATEX II messages that are published periodically by National ITS Systems, these messages are converted into CAMs, IVIMs and DENMs in order to be consumed by other applications and services, or even devices.

5.1.3.2 Geolocation Service

The Geolocation Service provides all vehicles connected to the platform with validated up-to-date information. It consumes the latest CAMs published to the platform and stores the most recent positions of vehicles. Doing so, it can send incoming data regarding specific areas to the affected vehicles. It can decide what is the best communication system to contact the endpoint.

5.1.3.3 Traffic Management Centre

The TMC works as a frontend application for traffic management. A web platform offering a set of tools for monitoring, controlling and managing the traffic on the seaport and is most important road accesses. TMC integrates the images of different traffic cameras in order to validate, create or revoke events. It can also be used to probe vehicle data, checking the past positions of a specific vehicle, or global traffic statistics.

5.1.3.4 Security Manager

Security is a major concern in vehicular communications. Anonymity alone is insufficient for protection of an ITS user's privacy and unsuitable as a solution for ITS. ITS Stations should be observable in order to provide improved safety. Consequently, pseudonymity and unlinkability offer the appropriate protection of the privacy of a sender of basic ITS safety messages (CAM and DENM). The security manager is responsible for the life cycle management of enrolment credentials and certificates. Additionally, it issues, monitors and authenticates different actors credentials in the C-ITS domain, granting him access to ITS communications and services.

5.1.3.5 Parking Service

The parking service is a union point for multiple parking lots to be monitored. It offers a single communication point for different services to interact with the parking system. It is essential for the smart parking use case, since, enhanced with the available traffic information, it can provide the best parking spot for the current operational status.
These services are furtherly depicted in the next sections.

5.2 Integrating C-ITS Services

In order to enable C-ITS services for the required use cases (Bottleneck removal, Safety information and Smart Truck Parking in the affected pilot site areas of the Port of Livorno and adjacent motorways) two ITS technologies are crucial: ITS hybrid communications and ITS security. These technologies contribute to a more secure, efficient and smart logistic corridor among the Port of Livorno, distribution centers and neighboring freight villages. ITS security is a vertical technology that addresses confidentiality, integrity, availability, accountability and authenticity in ITS systems.

5.2.1 ITS Hybrid Communications

In the context of Cooperative Intelligent Transport Systems (C-ITS), hybrid communications represent an extension to the existing ITS communications (ITS-G5), adding cellular communications (3G, 4G, 5G) to current Vehicle Ad-Hoc Networks (VANETS). As depicted in figure 12, vehicles (ITS-S) instead of only relying on a vehicular network connection to the

oneM2M platform (through the RSU and the respective backbone connection), also enjoy from a direct link through a telecom operator's cellular network.

Several problems arise from adding a cellular connection: cellular networks use IP based communications (IPv4/IPv6) which do not permit geolocation routing on opposition to vehicular networks. In addition, the extra complexity of cellular networks leads to longer traffic delays and jitter, compromising safety critical applications.

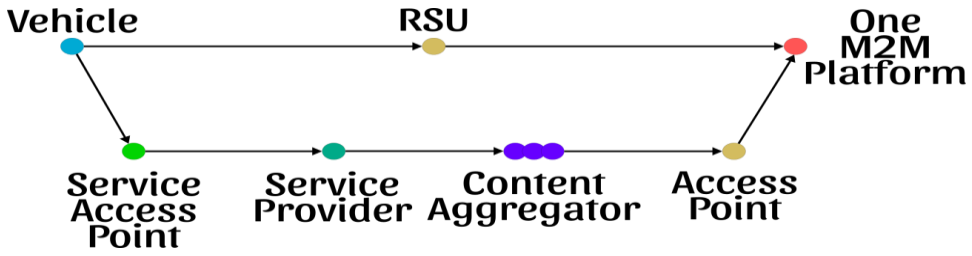

Figure 12 – Hybrid communications

5.2.1.1 Connection to current infrastructure:

- The oneM2M platform should have an extra service (GeoLocation service) which handles the translation between IP/cellular based connections and geo-position connections/services.
- C-ITS messages (in particular CAMs) exchanged between OBUs and the oneM2M platform (originated from cellular or ITS-G5) should be analysed in order to extract geographical position and then used to update the Geolocation service.
- The Geolocation service should keep geographical positions and the connection information of all active nodes.
- Current RSUs are connected via backbone connection, there is no advantage in upgrading existing RSUs with hybrid communications.
- New RSUs can take advantages from hybrid communications when no backbone connection is available.
- oneM2M platform should permit IPv4 and IPv6 connections - future-proof.
- The AMQP messaging protocol should be used in links between OBUs and the oneM2M platform.

5.2.2 ITS Security

ETSI ITS security makes use of a Public Key Infrastructure (PKI) architecture (depicted in figure 13), on which long-term certificates are issued to achieve identification and accountability on ITS stations. These long term certificates are denominated: Root CA certificates, self emitted by the Root Certification Authority (Root CA); Enrolment Authority (EA) certificates, emitted by Root CA;

Authorization Authority (AA) certificates, emitted by Root CA; Distribution Center (DC) certificates, emitted by Root CA and Enrolment Credential (EC), emitted by AA. The second type of certificates emitted by the ETSI PKI structure are the short-lived or anonymized certificates for V2V/V2I communications, named Authorization Tickets (AT) or Pseudonym Certificates (PC) which are emitted by the AA upon validation of the PCs/ATs request.

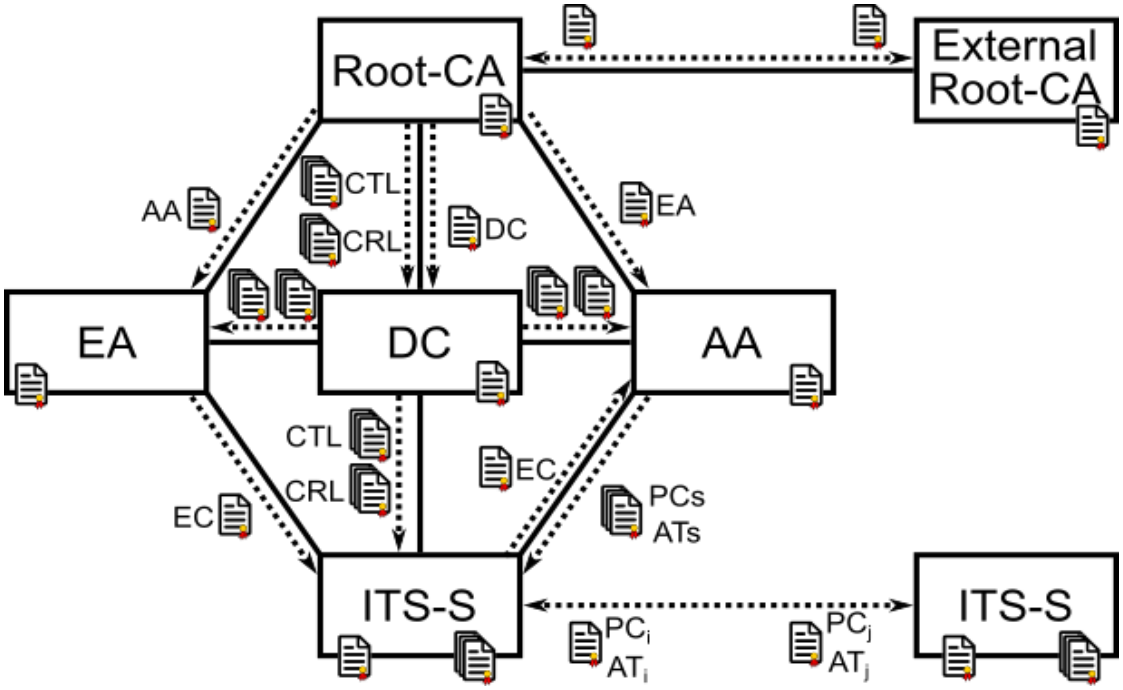

Figure 13 – ETSI ITS trust model (PKI)

Functional element	Description
Root Certification Authority (Root-CA)	The Root CA is the highest level CA in the certification hierarchy. It provides EA, AA certificates with proof that they may be used to issue Enrolment Credentials (EC) and Authorization Tickets (ATs) / Pseudonym Certificates (PCs) respectively. Root CA is also responsible from issuing and signing Certificate Trust List (CTL) and Certificate Revocation List (CRL). These lists indicate which Certificates are trusted in the PKI chain and/or the ones that were revoked. These lists are stored at the Distribution Centre (DC).

Enrolment Authority (EA)	Security management entity responsible for the life cycle management of enrolment credentials (EC), these credentials (long term certificates) are stored at ITS-S and are used to authenticate ATs/PCs requests or request a new EC by the ITS-S prior to EC expiration.
Authorization Authority (AA)	Security management entity responsible for issuing and monitor the use of Authorization Tickets (AT) / Pseudonym Certificates (PC). It provides an ITS-S with authoritative proof that it may use specific ITS services in an anonymous manner. By keeping a list of which ATs/PCs were emitted to every ITS-S, it guarantees accountability to ITS-S in case of need.
Distribution Centre (DC)	This entity keeps the updated lists: Certificate Trusted List (CTL) and Certificate Revocation List (CRL) to any node that requests it. It also guarantees the authorization of the originator of an updated list.
External Root-CA	External entity which permits interconnection between PKIs, to authenticate and validate another PKI based nodes, the External Root-CA Certificate must be trusted (published in CTL) and not revoked (not published in CRL), as well as the remain of the certificate chain of trust.
ITS-S	The ITS Stations (ITS-S) use V2V/V2I communications based on the received ATs/PCs.

5.2.2.1 Connection to current infrastructure.

There are two options to integrate C-ITS security into Port of Livorno existing architecture. The first assumes that a National PKI structure is already available. The latter can be used if no National PKI is available (by integrating a full C-ITS PKI into oneM2M platform).

Option 1: Integration with already available Italian ROOT-CA:

- The Port of Livorno emits a request to be associated as an Italian Enrolment Authority (EA).
- After obtaining the certificate, each C-ITS device needs to be registered by requesting Enrolment Credentials (ECs) (emitted by the Security Manager).
- These devices should then request a list of ATs/PCs to the available AA.
- ITS-S need also a connection to available DC in order to obtain the updated CTL and CRL.

- After obtaining the pseudonyms and DC lists, ITS-S can send and validate messages using its certificate.
- A service inside the oneM2M platform should be used in order to speed up / cache the acquisition of TSL and CTL lists.

Option 2: Port of Livorno own ROOT-CA.

- An ETSI ITS PKI should be implemented and maintained inside oneM2M platform as a service (e.g., integrating it in the Security Manager).
- This service has to handle device registration, emission of certificates, maintenance of trusted and revoked certificate lists, emission of certificate pseudonyms and maintaining the list of all certificates emitted.

5.2.3 ITS Security in Hybrid Communications

- A Security Manager service should be implemented in order to validate all C-ITS messages originated from ITS-S by cellular communication.
- The Security Manager service needs to have its own and valid ETSI ITS security certificate in order to validate ITS-S messages working similar to an RSU.
- Since ITS security is integrated at geonetworking layer, all geonetworking headers and trailers have to be sent via AMQP to oneM2M platform.
- The Security Manager have to distinguish between PKIs

5.4 Interfaces and API Specification

Figure 14 depicts all interfaces described in this section. Interfaces 1, 2, 9 are cellular or eth based. Interfaces 3, 4, 6, and 7 are cellular based and they connect devices with the platform, 5 and 8 are device to device communications, 14 and 12 are connections to third-party services and the remaining are restful or messaging IP based communications. Interfaces are depicted in the tables below.

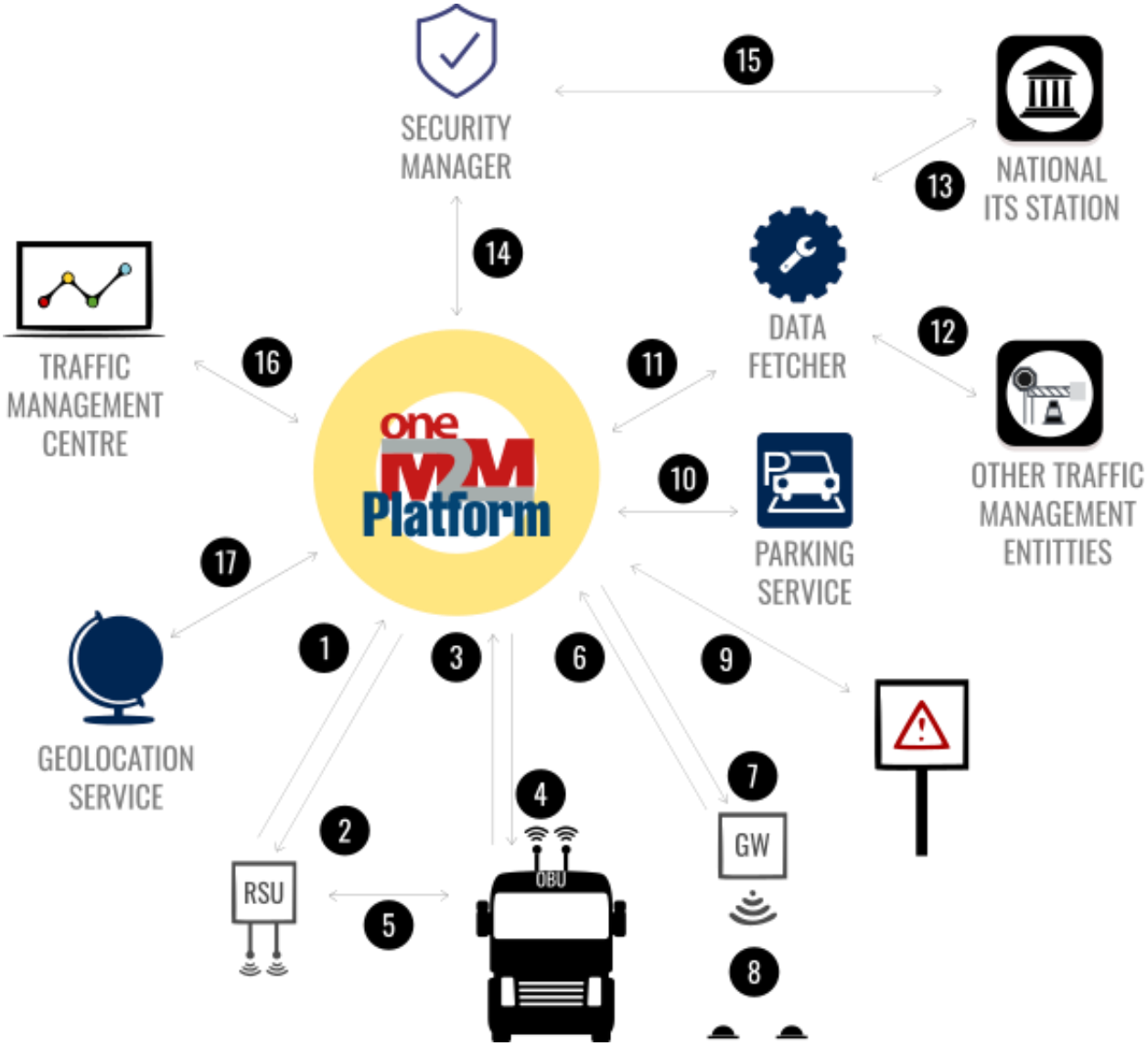

Figure 14 – Architecture Interfaces.

Interface Number	Access	Network	Transport	Application Layer	Data
1	cellular, eth	IPv4/IPv6	TCP	HTTPs, MQTTs	CAM/DENM/IVIM/MAPEM/ SPATEM (JSON)
2	cellular, eth	IPv4/IPv6	TCP	HTTPs, MQTTs	CAM/DENM/IVIM/MAPEM/ SPATEM (JSON)
3	cellular	IPv4/IPv6	TCP	AMQP	CAM/DENM/IVIM/MAPEM/ SPATEM
4	cellular	IPv4/IPv6	TCP	AMQP	CAM/DENM/IVIM/MAPEM/ SPATEM
5	802.11p CCH	GN	BTP		CAM/DENM/IVIM/MAPEM/ SPATEM
6	cellular	IPv4/IPv6	TCP	AMQP, HTTPs, MQTTs	Defined by Service
7	cellular	IPv4/IPv6	TCP	AMQP, HTTPs, MQTTs	Defined by Service
8	LPWAN				Defined by Service
9	cellular, eth	IPv4/IPv6	TCP	AMQP	Defined by Service
10		IPv4/IPv6	TCP	AMQP, HTTPs, MQTTs	Defined by Service
11		IPv4/IPv6	TCP	AMQP, HTTPs	CAM/DENM/IVIM/MAPEM/ SPATEM
12		IPv4/IPv6	TCP	Websocket, HTTPs	DATEX II or 3rd Party Data Types
13		IPv4/IPv6	TCP	Websocket, HTTPs	DATEX II or 3rd Party Data Types
14		IPv4/IPv6	TCP	REST	CTL, CRL, Pseudonym Certificate List
15		IPv4/IPv6	TCP	REST	CTL, CRL

16		IPv4/IPv6	TCP	Websocket, HTTPs	Defined by Service + CAM/DENM/IVIM/MAPEM/ SPATEM
17		IPv4/IPv6	TCP	AMQP, HTTPs, MQTT	Defined by Service + CAM/DENM/IVIM/MAPEM/ SPATEM

ID	1
Components	RoadSide Unit, oneM2m Platform
Communication	HTTPs or MQTTs
Description	Upflow link between RoadSide Unit and the oneM2M platform The data workflow shall follow the ensuing sequence: 1. RSU receives messages from interface 5. 2. The messages are validated through the GN headers 3. Message aggregation is performed whenever necessary (e.g. CAM aggregation) 4. The Facilities layers is stripped from the messages and converted in oneM2M protocol (JSON) 5. The resulting information is published to the platform oneM2M AE (pre-defined facilities endpoint) using HTTPs or MQTTPs oneM2M protocol. 6. The information is stored and shared among different consumers. Message Structure: 1. /FACILITIES(ASN1 UPPER)/HTTPs/TCP/IPV4 2. /FACILITIES(ASN1 UPPER)/MQTTs/TCP/IPV4
Additional information	In specific cases this communication can be cellular-based or eth-based. All ITS-G5 facilities messages gathered by the RSU shall be converted in oneM2M protocols before the publication to the oneM2M platform.

Interface Number	2
Components	RoadSide Unit, OneM2M Platform

Communication	HTTPs or MQTTs
Description	Downflow link between RoadSide Unit and the oneM2M platform The data workflow shall follow the ensuing sequence: 1. The oneM2M Platform issues a new message on a pre-defined container. 2. The RSU is subscribed to the pre-defined container and receives the information (ETSI ITS G5 facility) in JSON format. 3. The RSU adds GN and BTP headers and encodes using ASN1 unaligned PER. 4. The resulting information is broadcasted through interface 5 Message Structure: 1. /SERVICE_STRUCTURE/HTTPs/TCP/IPV4 2. /SERVICE_STRUCTURE/MQTTs/TCP/IPV4
Additional information	In specific cases this communication can be cellular based. All facilities messages broadcasted from the RSU shall be encoded using ASN1 unaligned PER, as defined in the ITS-G5 profiles

ID	3
Components	On-board Unit, OneM2M Platform
Communication	AMQP over IP (Cellular based)
Description	Upflow link between On-board Unit and the oneM2M platform The data workflow shall work in one of the ensuing sequences: 1. The vehicle is out of an IEEE 802.11p coverage area 2. The communication system is switched to cellular 3. The message is published with GN and BTP headers to the platform AMQP broker (pre-defined GN channel) 4. The rate of transmission of periodic messages (e.g. CAMs) is reduced from the standard 1-10 Hz, in order to adapt to the limitations of current cellular communications or 1. The vehicle wants to request a specific service (namely request a new set of pseudonyms, updating CRL or CTL or even request a parking spot)

	2. The communication system is switched to cellular 3. The request is sent to the platform Message Structure: 1. /FACILITIES(ASN1 UPPER)/AMQP/TCP/IPV4/Cellular 2. /SERVICE_STRUCTURE/AMQP/TCP/IPV4/Cellular
Additional information	

ID	4
Components	On-board Unit, oneM2M Platform
Communication	AMQP over IP (Cellular based)
Description	Downflow link between On-board Unit and the oneM2M platform The data workflow shall follow the ensuing sequence: 1. The AMQP broker issues a new message (pre-defined OBU channel) 2. The OBU consumes the information. 3. The message is presented to the user through the HMI Message Structure: 1. /FACILITIES(ASN1 UPPER)/AMQP/TCP/IPV4/Cellular 2. /SERVICE_STRUCTURE/AMQP/TCP/IPV4/Cellular
Additional information	All facilities messages shall be encoded using ASN1 unaligned PER, as defined in the ITS-G5 profiles

ID	5
Components	RoadSide Unit, On-board Unit
Communication	BTP + GN

Description	Communication between RSU and the OBU. The data workflow shall follow the ensuing sequence: Uplink 1. The RSU observes the in-memory messages time validity and periodicity 2. It broadcasts messages accordingly Downlink 1. The vehicle is in a 802.11p coverage area 2. The OBU starts periodically broadcasting CAMs through the ETSI ITS G5 interface Message Structure: Uplink - /(IVIM,MAPEM,SPATEM,CAM,DENM)/BTP/GN/802.11p(CCH) Downlink - /(CAM,DENM)/AMQP/BTP/GN/802.11p(CCH)
Additional information	All facilities messages shall be encoded using ASN1 unaligned PER, as defined in the ITS-G5 profiles

ID	6
Components	Gateway, oneM2m Platform
Communication	AMQP over IP (Cellular based) or HTTPs, or MQTTs
Description	Upflow link between Parking dedicated gateway and the oneM2M platform The data workflow shall follow the ensuing sequence: 1. The GW aggregates the status of the surrounding parking spots 2. The information is periodically published to the platform AMQP broker (on the pre-defined parking lot channel) Message Structure: TBD
Additional information	

ID	7

Components	oneM2m Platform, Gateway
Communication	AMQP over IP (Cellular based)
Description	Downflow link between Parking dedicated gateway and the oneM2M platform The data workflow shall follow the ensuing sequence: 1. The platform issues a request message regarding the status of a group or a specific parking spot 2. The information is transformed and relayed to the respective endpoint 3. A confirmation message is sent through interface 6 Message Structure: TBD
Additional information	

ID	8
Components	Gateway, Parking Sensors
Communication	Low Power Wide Area Network
Description	Communication between Parking Sensors and the Gateway The data workflow shall follow the ensuing sequence: Uplink 1. The sensor checks if the parking spot is occupied (e.g. magnetic sensor or gateway previous information) 2. The information is sent to the gateway Downlink 1. The gateway contacts the sensor to change status 2. It waits for the sensor/next-sensor communication 3. A confirmation message is sent through interface 6 Message Structure: TBD
Additional information	

ID	9
Components	VMS, oneM2M Platform
Communication	AMQP over IP (Cellular based) of HTTPs over eth
Description	Communication between VMS and the oneM2M Platform The data workflow shall follow the ensuing sequence: Downlink 1. The platform publishes new information 2. The VMS consumes the information 3. The VMS presents the information on the display
Additional information	The Uplink is optional, it can be used for management operations, confirmation messages or periodic status updates

ID	10
Components	Parking Service, oneM2m Platform
Communication	AMQP over IP
Description	Communication between Parking Service and the oneM2M Platform The data workflow shall follow the ensuing sequence: 1. A new service request is received (e.g., parking reservation request) 2. The Parking Service verifies parking spaces availability 3. It sends request for parking sensor status modification to platform which relays through interface 7 4. It waits for GW next update 5. It sends information to vehicle through the Geolocation Service
Additional information	

ID	11
Components	Data Fetcher, oneM2m Platform
Communication	AMQP over IP, HTTPs
Description	Communication between the Data Fetcher and the oneM2M Platform The data workflow shall follow the ensuing sequence: Uplink 1. New updated information regarding the seaport is received (e.g., DATEX II, other traffic information related messages) 2. It is translated into Facilities messages and published to the platform
Additional information	The Downlink is optional, depending on the existence of any subscription from the National ITS Station or Other Traffic Management Entities. If exists, it should follow the ensuing sequence: 1. The most recent Facilities messages are aggregated 2. Messages are translated into DATEX II or other message structure. This information is afterwards forwarded through interfaces 13 and/or 12.

ID	12
Components	Data Fetcher, Other Traffic Management Entities
Communication	REST
Description	Communication between the Data Fetcher and the Other Traffic Management Entities The data workflow shall follow the ensuing sequence: Downlink 1. A new message is received 2. It is translated into the respective Facilities messages 3. The messages are published to the platform

Additional information	The Uplink is optional, depending on the existence of any subscription from the Other Traffic Management Entities. If exists, it should follow the ensuing sequence: 1. The most recent Facilities messages are aggregated by the Data Fetcher 2. They are transformed and distributed in accordance to the service endpoint

ID	13
Components	Data Fetcher, National ITS Station
Communication	DATEX over websocket
Description	Communication between the Data Fetcher and the National ITS-S The data workflow shall follow the ensuing sequence: Downlink 1. A new DATEX II message is received 2. It is translated into the respective Facilities messages 3. The messages are published to the platform
Additional information	The Uplink is optional, depending on the existence of any subscription from the National ITS-S. If exists, it should follow the ensuing sequence: 1. The most recent Facilities messages are aggregated by the Data Fetcher 2. They are transformed into DATEX II messages and periodically broadcasted

ID	14
Components	Security Manager, oneM2m Platform
Communication	REST over IP
Description	Communication between the Security Manager and the oneM2M Platform Data flow and the number of connectors will depend where ETSI ITS PKI will be integrated. Uplink

	1. The ETSI ITS related security responses. Downlink The ETSI ITS related security requests.
Additional information	

ID	15
Components	Security Manager, National ITS Station
Communication System	REST over IP
Description	Communication between the Security Manager and the National ITS-S Data flow and the number of connectors depends on where ETSI ITS PKI will be integrated. Uplink 1. The ETSI ITS related security requests. Downlink 1. The ETSI ITS related security responses.
Additional information	

ID	16
Components	Traffic Management Centre, oneM2m Platform
Communication System	AMQP over IP
Description	Communication between TMC and the oneM2M platform The data workflow shall follow the ensuing sequence:

	Uplink 1. A new event is published to the platform 2. The TMC consumes the information 3. The TMC presents the event in the map Downlink 1. A new event is created in the dashboard 2. It is published to the platform 3. A response is received through the uplink
Additional information	

ID	17
Components	Geolocation Service, oneM2m Platform
Communication System	MQTTs, AMQP over IP
Description	Communication between GS and the oneM2M platform The data workflow shall follow the ensuing sequence: 1. The service stores the most recent position of each vehicle and RSU 2. A new event is published to the platform 3. The GC consumes the information 4. Compares the information coverage area with the station positions 5. Publishes it in the respective channels
Additional information	

6 Standards to adopt

Standard	**Description**	**Version**	**Date**

EN 302 665	Intelligent Transport Systems (ITS); Communications Architecture	1.1.1	2010-09
IEEE 802.11	IEEE Standard for Information Technology - Telecommunications and Information exchange between systems - Local and metropolitan area networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications	802.11™(2007)	2007-06-12
ANSI / IEEE 802.2 ISO/IEC 8802-2:1998	IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific Requirements - Part 2: Logical Link Control	802.2™ (1998)	1998-05-7
ES 202 663	Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band	1.1.0	2010-01
EN 302 663	Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band	1.2.1	2013-07
TS 102 687	Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part	1.1.1	2011-07
TS 102 792	Intelligent Transport Systems (ITS); Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (CEN DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range	1.2.1	2015-06

TS 102 724	Intelligent Transport Systems (ITS); Harmonized Channel Specifications for Intelligent Transport Systems operating in the 5 GHz frequency band	1.1.1	2012-10
EN 302 571	Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU	2.1.1	2017-02
TS 102 636-3	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network architecture	1.1.1	2010-03
EN 302 636-3	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network Architecture	1.2.1	2014-12
EN 302 636-1	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements	1.2.1	2014-04
TS 102 636-1	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements	1.1.1	2010-03
EN 302 636-2	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 2: Scenarios	1.2.1	2013-11
TS 102 636-2	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 2: Scenarios	1.1.1	2010-03

EN 302 636-4-1	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality	1.3.1	2017-08
TS 102 636-4-2	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 2: Media-dependent functionalities for ITS-G5	1.1.1	2013-10
EN 302 636-5-1	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol	2.1.1	2017-08
TS 102 636-5-1	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol	1.1.1	2012-02
EN 302 636-6-1	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols	1.2.1	2014-05
TS 102 636-6-1	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocol	1.1.1	2011-03
TS 102 637-2	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification	1.2.1	2011-03

	of Cooperative Awareness Basic Service		
EN 302 637-2	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service	1.3.2	2014-11
EN 302 931	Intelligent Transport Systems (ITS); Vehicular Communications; Geographical Area Definition	1.1.1	2011-07
TS 103 248	Intelligent Transport Systems (ITS); GeoNetworking; Port Numbers for the Basic Transport Protocol (BTP)	1.1.1	2016-11
TS 102 637-3	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service	1.1.1	2010-09
EN 302 637-3	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service	1.2.2	2014-11
TS 102 894-1	Intelligent Transport Systems (ITS); Users and applications requirements; Part 1: Facility layer structure, functional requirements and specifications	1.1.1	2013-08
TS 102 894-2	Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary	1.2.1	2014-09

TS 102 965	Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration list	1.3.1	2016-11
TS 101 539-1	Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signaling (RHS) application requirements specification	1.1.1	2013-08
TR 102 638	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions	1.1.1	2009-06
TS 102 940	Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management	1.2.1	2016-11
TS 102 731	Intelligent Transport Systems (ITS); Security; Security Services and Architecture	1.1.1	2010-09
TS 102 941	Intelligent Transport Systems (ITS); Security; ITS; Trust and Privacy Management	1.1.1	2012-06
TR 102 893	Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)	1.2.1	2017-03
TS 102 942	Intelligent Transport Systems (ITS); Security; Access Control	1.1.1	2012-03
TS 102 943	Intelligent Transport Systems (ITS); Security; Confidentiality services	1.1.1	2012-06
TS 102 867	Intelligent Transport Systems (ITS); Security; Stage 3 mapping for IEEE 1609.2	1.1.1	2012-06

TS 103 097	Intelligent Transport Systems (ITS); Security; Security header and certificate formats	1.2.1	2015-06
TR 102 965	Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration list	1.1.1	2013-03
TR 102 962	Intelligent Transport Systems (ITS); Framework for Public Mobile Networks in Cooperative ITS (C-ITS)	1.1.1	2012-02
ITU E.212(11/98)	List of Mobile Country or Geographical Area Codes	1	2001-06
ISO/TS17419:2014	Intelligent transport systems -- Cooperative systems -- Classification and management of ITS applications in a global context	1	2014-04
ISO/TS19321:2015	Intelligent transport systems -- Cooperative ITS -- Dictionary of in-vehicle information (IVI) data structures	1	2015-04
ISO/TS19091:2017	Intelligent transport systems -- Cooperative ITS -- Using V2I and I2V communications for applications related to signalized intersections	1	2017-03