



Grant Agreement Number: 731993

Project acronym: AUTOPILOT

Project full title: AUTOMated driving Progressed by Internet Of Things

D. 5.7

TITLE

Due delivery date: 31 May 2017

Actual delivery date:

Organization name of lead participant for this deliverable: Telecom Italia

Project co-funded by the European Commission within Horizon 2020 and managed by the European GNSS Agency (GSA)		
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)	



Document Control Sheet

Deliverable number:	D. 5.7
Deliverable responsible:	TIM
Workpackage:	5
Editor:	Giovanna Larini

Author(s) – in alphabetical order		
Name	Organisation	E-mail
Andrea BASTIANELLI	THALES	andrea.bastianelli@thalesgroup.com
Martin Bauer	NEC	Martin.Bauer@neclab.eu
Enrico BURACCHINI	TIM	enrico.buracchini@telecomitalia.it
Daniele BREVI	ISMB	brevi@ismb.it
Philippe CUENOT	CONTINENTAL	Philippe.Cuenot@continental-corporation.com
Philippe COUSIN	EGM	philippe.cousin@eglobalmark.com
Vincenzo DI MASSA	THALES	vincenzo.dimassa@thalesgroup.com
Miodrag DJURICA	TIM	miodrag.djurica@tno.nl
Mariano FALCITELLI	CNIT	mariano.falcitelli@cnit.it
Enrico FERRERA	ISMB	ferrera@ismb.it;
Anna FIAMMENGO	TIM	annamaria.fiammengo@telecomitalia.it
Guido GAVILANES	ISMB	gavilanes@ismb.it;
Georgios KARAGIANNIS	Huawei	georgios.karagiannis@huawei.com
Giovanna LARINI	TIM	giovanna.larini@telecomitalia.it
Frost LINDSAY	NEC	Lindsay.Frost@neclab.eu;
Daniela LONG	TIM	daniela.long@telecomitalia.it
Paolo PAGANO	CNIT	paolo.pagano@cnit.it;
Jordi PONT	IDIADA	Jordi.Pont@idiada.com
Thomas RESCHKA	CETECOM	Thomas.Reschka@cetecom.com;
Enrico SCARRONE	TIM	enrico.scarrone@telecomitalia.it
Peter SCHMITTING	ERTICO	p.schmitting@mail.ertico.com
Ralf TIEMANN	CETECOM	ralf.tiemann@cetecom.com;
Ovidiu VERMESAN	SINTEF	Ovidiu.Vermesan@sintef.no;
Ralf WILLENBROCK	T-Systems	Ralf.Willenbrock@t-systems.com

Document Revision History			
Version	Date	Modifications Introduced	
		Modification Reason	Modified by
V0.0	07/03/216	Table of Contents	TIM
V0.1	05/04/2017	Draft with first analysis and template	TIM
V0.2	28/04/2017	Draft release with contributions integrated	TIM
V0.3	02/05/2017	Updates on chapter 3 , 4, 5	TIM, NEC
V0.4	11/05/2017	Final release for internal review	TIM
V0.5	25/05/2017	New version taking into account ERTICO and HUAWEI revisions	TIM
V1.0	29/05/2017	Final version	ERTICO

Abstract

This document presents: 1) the standardization plan approach, 2) the main applicable standards in the IoT and ITS domain that shall be taken into account in the architectural framework and design choices in the AUTOPILOT WPs in order to make credible interoperable and future proof decisions, 3) a preliminary standard gaps analysis and a first selection of standards under development of interest for the AUTOPILOT standardization activity.

Legal Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law. © 2017 by AUTOPILOT Consortium.

Abbreviations and Acronyms

Acronym	Definition
3GPP	Third Generation Partnership Project
5GAA	5G Automotive Alliance
ADASIS	Advanced Driver Assistance System
AIOTI	Alliance for IoT Innovation
BBF	BroadBand Forum
CEN	European Committee for Standardization
CIM	Context Information Management
EC	European Commission
EN	European Standard
ERM	EMC and Radio Spectrum Matters
ETSI	European Telecom Standardisation Institute
EG	ETSI Guide
ES	ETSI Standard
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISG	Industry Specification Group
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
NGSI	Next Generation Service Interfaces
OMA	Open Mobile Alliance
OSGi	Open Service Gateway initiative
SDO	Standard Development Organization
SIG	Special Interest Group
TC	Technical Committee
TR	ETSI Technical Report
TS	ETSI Technical Specification
TTT	Transport and Traffic Telematics
WG	Working Group

Table of Contents

Executive Summary	8
1 Introduction	9
1.2 Purpose of Document	10
1.3 Intended audience.....	11
1.4 Document structure	11
2 Methodology used.....	12
2.1 AUTOPILOT and standards	12
2.2 AUTOPILOT relevant standards identification	12
2.3 Standardization activities	16
3 The Standards for AUTOPILOT	17
3.1 Standards Developing Organization (SDO), Alliances and Open Source organizations.....	17
3.1.1 3GPP: Third Generation Partnership Project Standards	17
3.1.2 5GAA: 5G Automotive Alliance	19
3.1.3 ADASIS Forum /ERTICO	22
3.1.4 AIOTI: Alliance for IoT Innovation	23
3.1.5 BBF: BroadBand Forum	24
3.1.6 Bluetooth	27
3.1.7 CEN TC278	28
3.1.8 ETSI TC ITS	29
3.1.9 ETSI TC Cyber	32
3.1.10 ETSI TC ERM.....	33
3.1.11 ETSI ISG CIM.....	34
3.1.12 FI-PPP/FIWARE Foundation.....	35
3.1.13 IEC	36
3.1.14 IEEE	38
3.1.15 IETF.....	40
3.1.16 IRTF	41
3.1.17 ISO TC204	42
3.1.18 ISO/IEC JTC1/SC27	44
3.1.19 LoRaWAN™	46
3.1.20 OneM2M.....	48
3.1.21 OMA	54
3.1.22 OSGi Alliance	55
3.1.23 SENSORIS Forum /ERTICO.....	57
3.2 By Autopilot area of interest.....	59
3.2.1 All areas	59
3.2.2 IoT Platform and architecture.....	61
3.2.3 Vehicle IoT Integration and platform	62
3.2.4 Communication network.....	64

3.2.5	IoT Eco-system	66
3.3	By keywords /knowledge areas.....	67
3.3.1	Communication and Connectivity.....	67
3.3.2	Integration and interoperability	70
3.3.3	Application.....	71
3.3.4	Infrastructure	72
3.3.5	IoT Architecture	74
3.3.6	Devices and sensor technology	74
3.3.7	Security and Privacy	75
3.3.8	Conformance, Testing.....	77
4	Standardization: preliminary activities	78
4.1	Standard gap analysis.....	78
4.2	Standard: ongoing activities	79
4.3	Standardization Activities	83
5	Conclusion	86
6	Annexes	87
6.1	Annex A - Organization overview.....	87
6.1.1	IoT Platform and architecture.....	87
6.1.2	Vehicle IoT Integration and platform	89
6.1.3	Communication network.....	91
6.1.4	IoT Eco-system	93
6.2	Annex B – Standards and Specifications.....	96
6.2.1	3GPP.....	96
6.2.2	ETSI (TC ITS).....	102
6.2.3	ETSI (TC Cyber Security)	120
6.2.4	ETSI (TC ERM)	123
6.2.5	IEEE	126
6.2.6	IETF.....	131
6.2.7	ISO TC204	136
6.2.8	ISO TC 22 / SC 31	139
6.2.9	ISO/IEC JTC1/SC27	140
6.2.10	oneM2M	146
6.3	Annex C – ETSI TR 103 375 v1.1.1 (2016-10).....	156

List of Figures

Figure 1 - The AUTOPILOT overall concept.....	10
Figure 2 - IoT SDOs and Alliances Landscape.....	13
Figure 3 - Mapping of IoT SDOs/Alliances to Knowledge Areas	14
Figure 4 - Mapping of IoT OSSs (Open Source Software) to Knowledge Areas	14

List of Tables

Table 1 - Standard Template	16
Table 2 - Technology gaps.....	79

Executive Summary

This document provides the AUTOPILOT planned activities for standardization. In particular it presents the approach and the methodology that will be used during the project for standardization.

The document provides, as a first result of the standardization activity, a collection of applicable standards in the IoT and ITS domain that shall be taken into account in the architectural framework and design choices for the AUTOPILOT project. This is done in order to find a common solution to assure a smooth and homogeneous way to assure a very high level of interoperability (or at least interworking) among the different systems.

The deliverable presents a preliminary analysis of standard gaps based on existing reports and a first selection of standards under developments that could be of interest for the Project standardization activities.

1 Introduction

1.1 The AUTOPILOT project objectives and concept

Automated driving is expected to increase safety, provide more comfort and create many new business opportunities for mobility services. The market size is expected to grow gradually reaching 50% of the market in 2035.

The Internet of Things (IoT) is about enabling connections between objects or "things"; it is about connecting anything, anytime, anyplace, using any service over any network.

AUTOated driving **Progressed** by **Internet Of Things**" (AUTOPILOT) project will especially focus on utilizing the IoT potential for automated driving.

The overall objective of AUTOPILOT is to bring together relevant knowledge and technology from the automotive and the IoT value chains in order to develop IoT-architectures and platforms which will bring Automated Driving towards a new dimension. This will be realized through the following main objectives:

- Use, adapt and innovate current and advanced technologies to define and implement an IoT approach for autonomous and connected vehicles
- Deploy, test and demonstrate IoT based automated driving use cases at several permanent pilot sites, in real traffic situations with: Urban driving, Highway pilot, Automated Valet Parking, Platooning.
- Create and deploy new business products and services for fully automated driving vehicles, used at the pilot sites: by combining stakeholders' skills and solutions, from the supply and demand side
- Evaluate with the involvement of users, public services and business players at the pilot sites:
 - The suitability of the AUTOPILOT business products and services as well as the ability to create new business opportunities
 - The user acceptance related to using the Internet of Things for highly or fully automated driving
 - The impact on the citizens' quality of life
- Contribute actively to standardization activities as well as consensus building in the areas of Internet of Things and communication technologies

Automated vehicles largely rely on on-board sensors (LiDAR, radar, cameras, etc. ...) to detect the environment and make reliable decisions. However, the possibility of interconnecting surrounding sensors (cameras, traffic light radars, road sensors, etc....) exchanging reliably redundant data may lead to new ways to design automated vehicle systems potentially reducing cost and adding detection robustness.

Indeed, many types of connected objects may act as an additional sources of data, which will very likely contribute to improve the efficiency of the automated driving functions, enable new automated driving scenarios as well as increase the automated driving function safety while providing driving data redundancy and reducing implementation costs. These benefits will enable pushing the SAE level of driving automation to the full automation, keeping the driver out of the loop. Furthermore, by making autonomous cars a full entity in the IoT, the AUTOPILOT project enables developers to create IoT/AD services as easy as accessing any entity in the IoT.

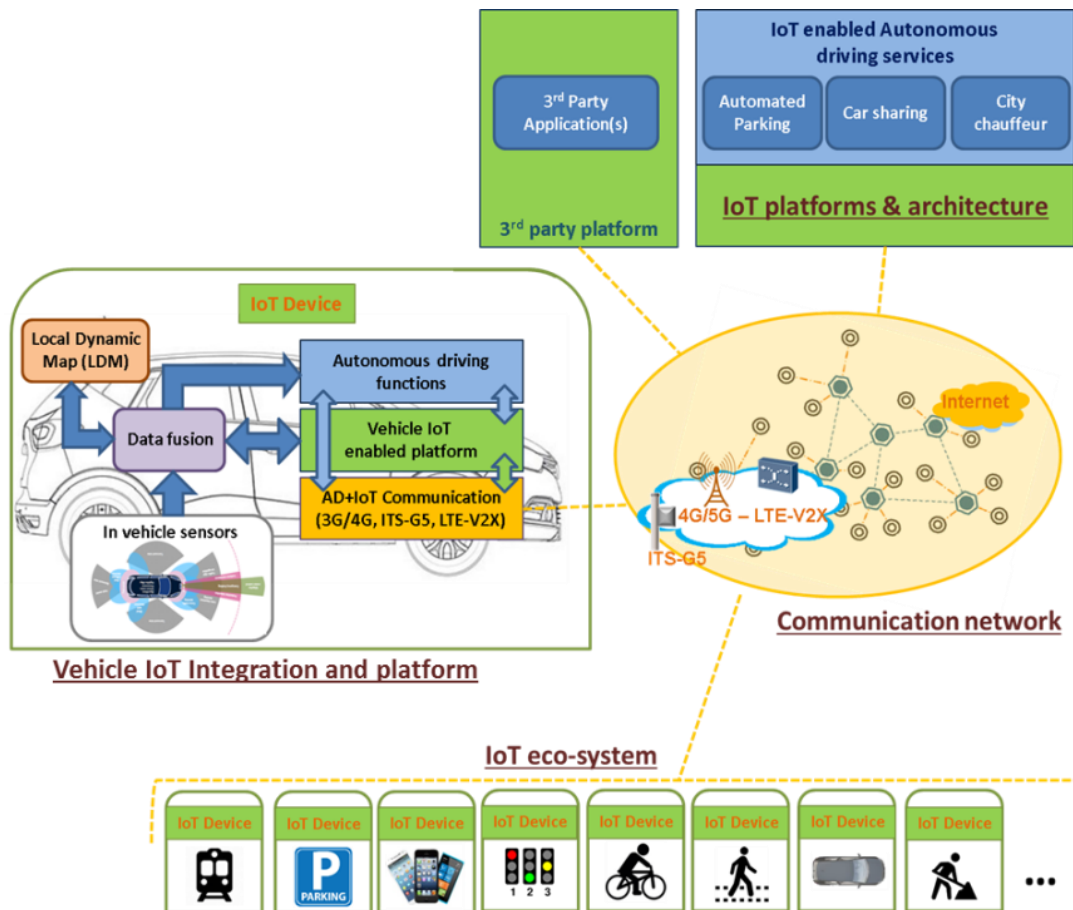


Figure 1 - The AUTOPILOT overall concept

The Figure 1 depicts the AUTOPILOT overall concept including the different ingredients to apply IoT to autonomous driving:

- The overall IoT platforms and architecture, allowing the use of the IoT capabilities for autonomous driving.
- The Vehicle IoT integration and platform to make the vehicle an IoT device, using and contributing to the IoT.
- The Automated Driving relevant sources of information (pedestrians, traffic lights ...) becoming IoT devices and extending the IoT eco-systems to allow enhanced perception of the driving environment on the vehicle.
- The communication network using appropriate and advanced connectivity technology for the vehicle as well as for the other IoT devices.

1.2 Purpose of Document

The objective of this document is to present the activities for contributing to the standardization, planned in AUTOPILOT.

Standardization activity is an essential part of the project strategy. Automated driving solutions will require addressing many issues such as interoperability between systems, security aspects, the IoT ecosystem and applications.

Without standard support the solutions adopted into the project will risk to be marginalized due to lack of market adoption.

The activities of the standardization plan cover the entire duration of the project: in the starting phase they provide an overview of the relevant standards available; during the project development

phases, they analyze the requirements, the specifications and the pilots' results by gathering gaps and needs that can contribute to the evolution of standards.

The standardization plan will address:

- 1) main applicable standards in the IoT and ITS domains to drive the architectural and design choices
- 2) standardization activities e.g. contributions to standards arising from the development and pilots deployment phases about gaps, inconsistencies, aspects to clarify and new requirements, presentations and / or articles on IoT/AD standards.

This deliverable is an initial plan providing an overview of the standardization landscape and the description of the foreseen activities about the possible AUTOPILOT contributions to the standardization.

In particular this document recommends to other AUTOPILOT WPs the main applicable standards in the IoT and ITS domain that shall be taken into account in the architectural framework and design choices in order to make credible interoperable and future proof decisions. Concerning standardization activities, it supplies some initial analysis on standards gaps and the approach that will be adopted to promote the AUTOPILOT results in several SDOs, Alliances and OSSs.

1.3 Intended audience

The document is addressed to project partners working in various WPs, project partners participating in standardization activities, and people working in other projects tackling similar issues.

For project partners working on WP1 "Requirements, Specifications and Architecture" , WP2: "Development, Integration & validation", WP3: "Large scale Pilots", it provides an overview of standards that are potentially of interest and it can therefore be used for the specification and development phases.

For all partners, and in particular for the partners participating in the standardization bodies activities, it offers a first indication on how the AUTOPILOT project intends to contribute to standardization evolutions in order to enhance the project results.

For people external to the project it could offer both a methodological approach and specific technical information.

1.4 Document structure

The document is organized as follows:

In Chapter 1 general information about the project is introduced.

In Chapter 2, the methodology followed for the standardization plan is described; it focuses: the ways to select and to describe standards of interest and the approach to contribute to the standards evolutions.

Chapter 3 describes organizations and the related standards documents of interest for AUTOPILOT and offers aggregated views of the collected information in order to make it more easy to use them in the AUTOPILOT activities.

Chapter 4 presents the results of standards gaps analysis and a first list of standardization activities that are relevant for the AUTOPILOT project.

Chapter 5 presents the conclusions of the work.

The annexes contain:

- an overview of potential organizations of interest for the project based on the partners' experience, organized by AUTOPILOT project area of interest (Annex A)
- the detailed standards and specifications documents description that have been selected as relevant, grouped by organization (Annex B)
- an excerpt of the ETSI Technical Report 103 375 with a list of standards of interest for Mobility vertical services (Annex C)

2 Methodology used

In this chapter the approach followed for the standardization plan activities and documents is presented.

In particular the reason to adopt as much as possible a standard based approach is introduced, then the methodology used to supply guidelines about the already available standards is presented, and finally the approach to contribute to standardization activities is described.

2.1 AUTOPILOT and standards

In the general context of IoT, including Automotive and ITS services, there is a need to exchange information among different ICT systems using combination of technologies. This is also valid for the AUTOPILOT context, where the vehicles have to exchange information with the different IoT systems present in the environment, and with other vehicles. These systems are using a wide range of communication technologies.

The convergence of technologies is a desirable feature, but to assume that it will happen quickly and fully is quite unrealistic, because there are huge legacies that will impact also future deployment in the next years. Additionally, the globalism of IoT, will require dedicated technologies, for performance and cost reasons.

In such environments, there is a need to find a common solution to ensure at least a smooth and homogeneous way to assure a very high level of interoperability (or at least interworking) among the different systems. And more relevantly, this would not be predominantly a protocol/communication technology problem: it is mainly a problem of sharing and understanding the information, achieving interoperability at application level.

In this perspective, standardization activity plays a significant role for the AUTOPILOT project both in offering already available specifications and in providing the opportunity to contribute to standards with new requirements / solutions adopted.

High-quality standards are essential to connect devices and industries through fast, secure and reliable wireless communications and to enable truly interoperable pan-European IoT services. In this view, it is important to encourage standards based on open solutions, developed on a voluntary and consensus approach by industrial stakeholders for the broadest level of marketplace acceptance and interoperability.

Standardization is considered to be the key to establish the credibility for exploitation of the solutions that will be collectively tested by the Large Scale Pilot in the different national Pilots sites.

2.2 AUTOPILOT relevant standards identification

In order to select the relevant standards for the project, the following approach has been applied. The analysis has been performed on the basis of the competence and the experience the partners

developed in the different knowledge areas and through the SDO participations concerning the Autopilot areas of interest.

In addition, two standards organizations overview documents were used in the analysis phase:

- “IoT LSP Standard Framework Concepts” AIOTI WG03 deliverable¹ and
- Technical Report ETSI TR 103 375 “SmartM2M; IoT Standards landscape and future evolutions”².

The **“IoT LSP Standard Framework Concepts”** AIOI WG3 deliverable presents an overview of Standards Developing Organization (SDO), Alliance and Open Source Software (OSS) to be used as input for Large Scale Pilots (LSP) and gap analysis. The objective of the document is to presents which standards and initiatives can be used to leverage on existing IoT standardization; as input to LSP and gap analysis and to provide guidelines for IoT project proposals.

The document introduces the SDO, Alliances, initiatives and OSS providing a brief description of them and presenting with different views focusing on different perspectives that are:

- Technology and Marketing
- Vertical and horizontal domains, see Figure 2

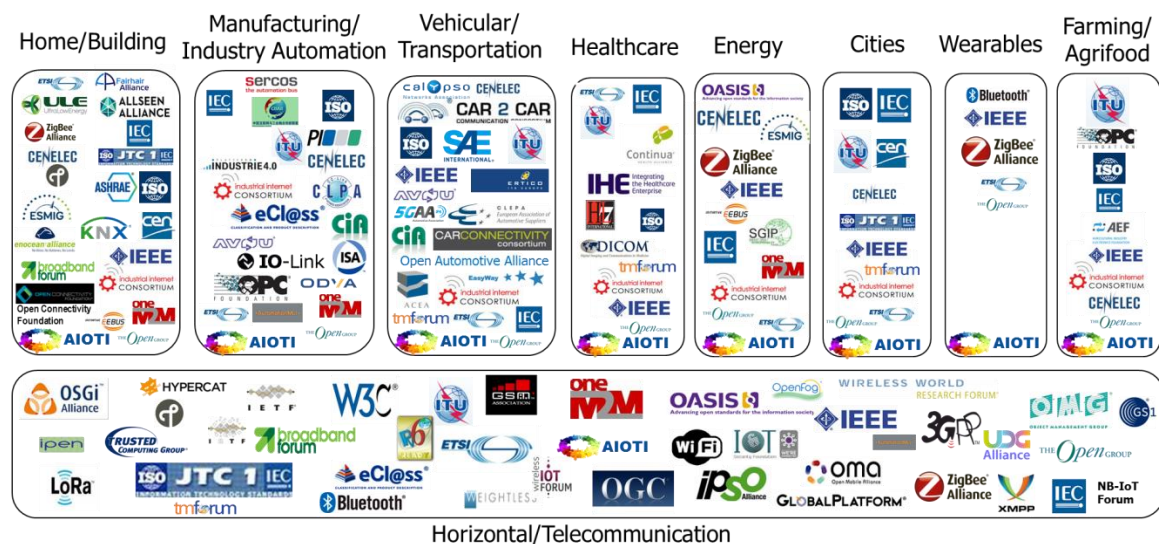


Figure 2 - IoT SDOs and Alliances Landscape³

Each SDO, Alliance, initiative and OSS is mapped into the following knowledge areas, see **Error! Reference source not found.** and **Error! Reference source not found.**, respectively:

- Communication and Connectivity
- Integration and interoperability
- Applications
- Infrastructure
- IoT Architecture
- Devices and sensor technology
- Security and Privacy

¹ https://docbox.etsi.org/SmartM2M/Open/AIOTI/!!20170102Deliverables/AIOTI%20WG3_sdos_alliances_landscape_iiot_lsp_standard_framework_concepts_release_2_v7.pdf

² http://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf

³ Source: AIOTI WG3 (IoT Standardisation) – Release 2.7

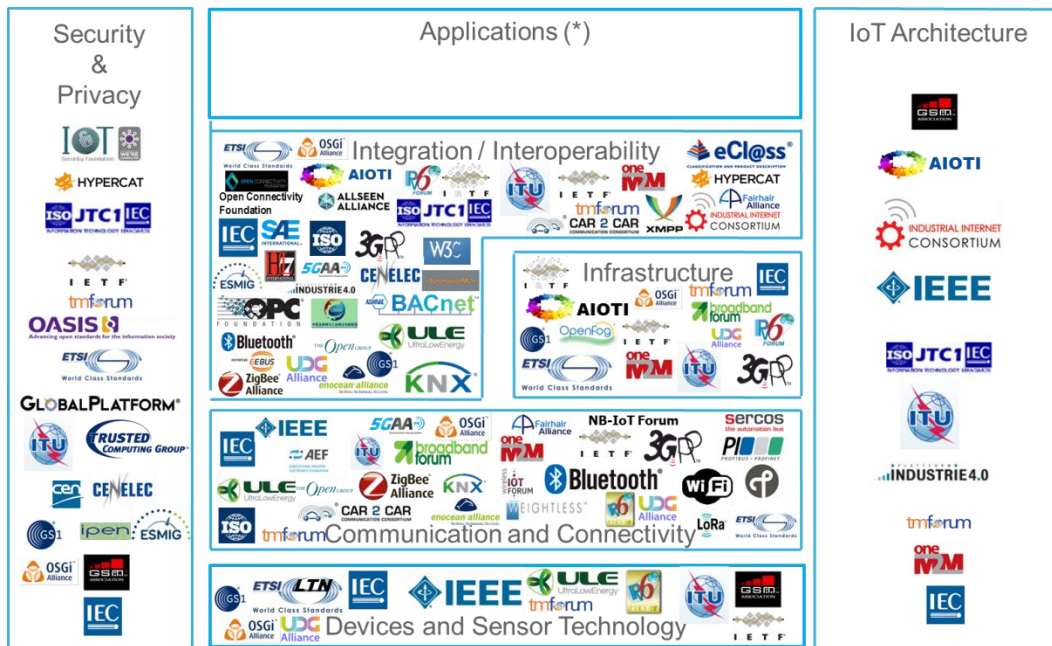


Figure 3 - Mapping of IoT SDOs/Alliances to Knowledge Areas⁴

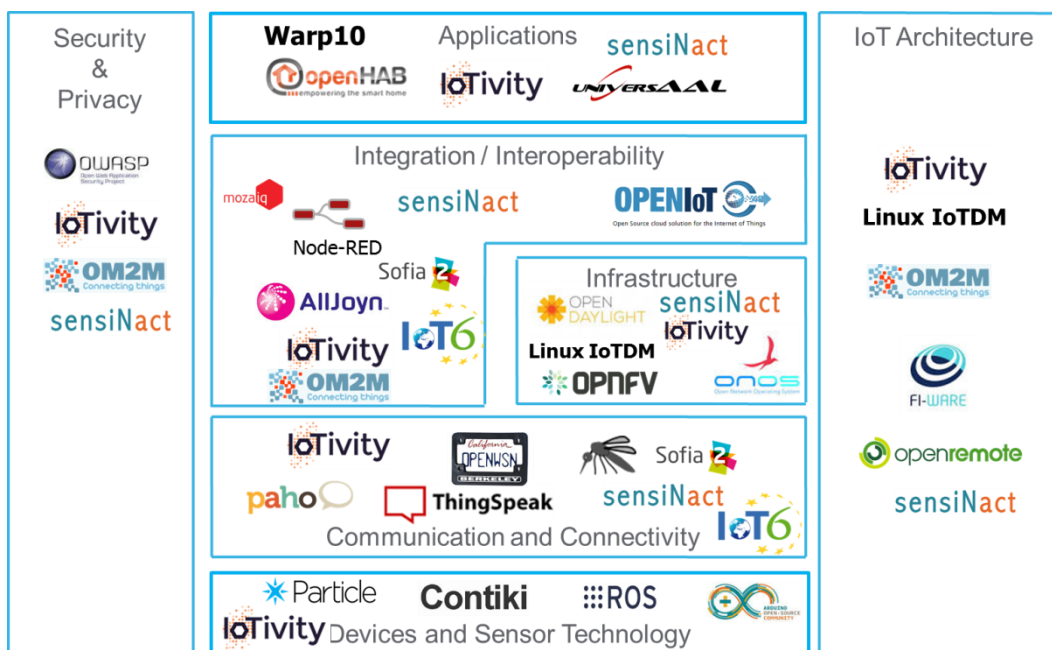


Figure 4 - Mapping of IoT OSSs (Open Source Software) to Knowledge Areas⁵

The Technical Report ETSI TR 103 375 “SmartM2M; IoT Standards landscape and future evolutions” general objectives are to analyze the status of the current IoT standardization and to increase the effectiveness of the IoT standardization. Specific objective is to support Large Scale Pilots (LSPs) taking into account the needs of vertical markets.

For each standard a short description/analysis is given.

Each standard is mapped by Knowledge Area and vertical market.

The Knowledge Areas are the same of the AIOTI document that is:

⁴ Source: AIOTI WG3 (IoT Standardisation) – Release 2.7

⁵ Source: AIOTI WG3 (IoT Standardisation) – Release 2.7

- Communication and Connectivity
- Integration and interoperability
- Applications
- Infrastructure
- IoT Architecture
- Devices and sensor technology
- Security and Privacy

The vertical markets considered are:

- Smart Cities
- Smart Living
- Smart Farming
- Smart Wearables
- Smart Mobility
- Smart Environment
- Smart Manufacturing

Annex C (page156) presents an excerpt of all the standards that are tagged as useful for the Smart Mobility vertical market technical report.

In order to collect the information on the relevant standard organizations and related specifications and recommendations, the template presented into the Table 1 was used.

This template allows organizing the standards information according to a homogeneous structure, facilitating consultation. Information about the areas of project interest, keywords and information on how to use the standard in the project provides further guidance.

Standardization body	
Standard No.	
Standard Title	
URL	
Country	<i>International, Europe, ...</i>
Status	<i>Published, Draft,</i>
Date	
Aim	
Description	<i>Description not more than 2 pages.</i>

Keyword	<i>Knowledge areas (e.g. Communication and Connectivity, Device and sensor Technology, Infrastructure, Integration /Interoperability, IoT Architecture, Security, Privacy, Data)</i>
Autopilot Area involved	<i>IoT Platform, Vehicle IoT Integration and platform, Communication network, IoT eco-system</i>
Use in the Project	<i>Explain how can be used in the AUTOPILOT project</i>
Author /Company	

Table 1 - Standard Template

2.3 Standardization activities

Standardization activities will be addressed through the following approach:

- 1) Standard gaps analysis (based on literature analysis and available standards state of the art).
- 2) Collection of requirements, gaps, needs emerging from pilots projects design and development.
- 3) Collection of information about partners involvement into the SDOs, Alliance, Association and their availability to promote project issues.
- 4) Elaboration of contributions, articles, presentations about IoT/AD standards.

At this phase of the project, the focus has been set on the point 1) results. The other points will follow along the overall life of the project. Particularly relevant for standardization activity will be the documents and results available at the following Project milestones:

- MS2: Specification completed
- MS3: Implementation completed
- MS4: End of Pilot and data collection
- MS5: Evaluation completed.

Concerning standard gaps analysis, from literature the following aspects have been considered:

- analysis of the ETSI document “TR 103 376 SmartM2M; IoT LSP use cases and standards gaps”⁶
- identification of standards of interest for which an evolution is envisaged since they could be the potential targets for the contributions from project standardization activities.

The Technical Report ETSI TR 103 376 “**SmartM2M; IoT LSP use cases and standards gaps**” objective is to provide the collection of missing functionalities that have been identified in standards bodies (SDOs) to offer solutions addressing the IoT use case requirements.

The gaps analysis is conducted for the different vertical markets: Smart Cities, Smart Living, Smart Farming, Smart Wearables, Smart Mobility, Smart Environment, Smart Manufacturing and for the following knowledge areas: Communication and Connectivity, Integration and interoperability, Applications, Infrastructure, IoT Architecture, Devices and sensor technology, Security and Privacy.

The report addresses three categories of gaps: Technology (e.g. communications paradigms, data models, software availability), Societal (e.g. privacy, energy consumption, ease of use), Business (e.g. value chain, investment).

The report presents gaps based on the knowledge areas but also defines the main requirements

⁶ http://www.etsi.org/deliver/etsi_tr/103300_103399/103376/01.01.01_60/tr_103376v010101p.pdf

specific to each vertical sector and analyses how they are covered and what the gaps that have been identified are.

In particular the TR presents for each vertical sector:

- the list of main technological requirements according to the knowledge area which they belong, which SDOs/Alliances address the target requirement and, in case there are no standards, highlights at this level a potential standardization gap;
- the gaps resulting from a survey based on the knowledge areas and conducted on a large sample of users (215 responses) representing different actors of the IoT community.

3 The Standards for AUTOPILOT

This chapter presents the selected organizations and standards of interest for the different parts of the AD ecosystem that could be used in the AUTOPILOT project.

Section **Error! Reference source not found.** summarizes in a list the Standards Developing Organization (SDO), Alliances and Open Source organizations detailing the objective, a short description and in particular some information of potential use in the project.

Section 3.2 and Section 3.3 present them organized by project area of interest: *IoT Platform*, *Vehicle IoT Integration and platform*, *Communication network* and *IoT eco-system* and by Keywords/ Knowledge areas in order to facilitate their use in the AUTOPILOT project activities.

The Annexes contains further information, and in particular:

- Annex A contains an overview of potential organizations of interest for the project based on the partners' experience, organized by AUTOPILOT project area of interest that extend the list presented into this chapter.
- Annex B contains the detailed standards and specifications documents description that have been selected as relevant, grouped by organization
- Annex C contains an excerpt of the ETSI Technical Report 103 375 with a list of standards of interest for Mobility vertical services.

3.1 Standards Developing Organization (SDO), Alliances and Open Source organizations

3.1.1 3GPP: Third Generation Partnership Project Standards

Standardization body	3GPP (Third Generation Partnership Project)
Standard No.	N/A
Standard Title	Third Generation Partnership Project Lte, Lte Adv, Lte Adv Pro, 5G, VTx (V, I, P), Nb-IoT, eMTC
URL	http://www.3gpp.org
Country	Worldwide

Status	Ongoing Work
Date	1998 - Present
Aim	3GPP covers cellular telecommunications network technologies, including radio access, the core network, and service capabilities - including work on codecs, security, quality of service - and thus provides complete system specifications. The specifications also provide hooks for interworking with non 3GPP radio accesses, such as Wi-Fi.
Description	<p>The 3rd Generation Partnership Project (3GPP) unites several telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as “Organizational Partners” and provides their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies.</p> <p>3GPP specifications and studies are contribution-driven, by member companies, in Working Groups and at the Technical Specification Group level.</p> <p>The three Technical Specification Groups (TSG) in 3GPP are;</p> <ul style="list-style-type: none"> • Radio Access Networks (RAN), • Services & Systems Aspects (SA), • Core Network & Terminals (CT) <p>The Working Groups, within the TSGs, meet regularly and come together for their quarterly TSG Plenary meeting, where their work is presented for information, discussion and approval.</p> <p>Each TSG has a particular area of responsibility for the Reports and Specifications within its own Terms of Reference (Details available in: http://www.3gpp.org/specifications-groups).</p> <p>The 3GPP technologies from these groups are constantly evolving through Generations of commercial cellular / mobile systems. Since the completion of the first LTE and the Evolved Packet Core specifications, 3GPP has become the focal point for mobile systems beyond 3G.</p> <p>Although these Generations have become an adequate descriptor for the type of network under discussion, real progress on 3GPP standards is measured by the milestones achieved in particular Releases. New features are ‘functionality frozen’ and are ready for implementation when a Release is completed. 3GPP works on a number of Releases in parallel, starting future work well in advance of the completion of the current Release. Although this adds some complexity to the work of the groups, such a way of working ensures that progress is continuous & stable.</p> <p>Between all the TSG groups, <u>the radio ones</u> are considered of main relevance for AutoPilot work, since they specify the radio solutions considered for communication infrastructure, such as LTE (Rel8) and related</p>

	<p>evolutions (Rel 10 onwards), for vehicular communications (rel14onwards) and upcoming 5G (Rel15 onwards), and for IoT solutions, such Nb-IoT (Rel 13 onwards) and eMTC families (Rel12 onwards).</p> <p>For requirements and use cases for LTE and future 5G based vehicular communications and services, SA WG1 has to be assumed as a reference.</p> <p>For more detail on 3GPP standard documents please refer to Annex B – Standards and Specifications – section 6.2.13GPP</p>
Keyword	Communication and Connectivity, Infrastructure, IoT Architecture, Devices and sensor technology, Integration/Interoperability, Security aspects, security Architecture, Security Requirements, Vehicular Communication Services
Autopilot Area involved	Vehicle IoT Integration and platform, IoT platform, Communication network, IoT eco-system
Use in the Project	<p>The overall Autopilot concept is based on 4G/5G and LTE-V2X, these communication technologies are specified in the 3GPP Global Initiative. 5G is still under specification procedure with regards to standardization, nevertheless narrow-band IOT will play a significant role in parking services planned in AUTOPILOT sites and other ITS field trials due to weak battery life time. Therefore, all mobile communication technologies have to be considered related to narrow-band IOT sensor availability and base station upgrades. These standards can be used both for WP1 and WP3.</p> <p>NB-IoT is a promising brand-new standard which can be considered by AUTOPILOT architecture during the design phase. To be considered also the possibility of development of NB-IoT-enabled sensors.</p> <p>LTE-based V2X services standard will be considered while it is implemented the pilot sites with RSUs complying with 3GPP release 13, migration to R14 first in terms of connected field components (OBUs, RSUs) thus implementing PC5 at 5.9 GHz, and in turn at radio infrastructure level.</p> <p>Security aspect for LTE support of V2X services (release 14) can be used as a guideline in the AUTOPILOT WP1 architecture phase, with reference to the Security Aspect in T1.5 Security, Privacy and Data Specification</p>
Author /Company	<p>CNIT</p> <p>ISMB</p> <p>THALES</p> <p>TIM</p> <p>T-SYSTEMS</p>

3.1.2 5GAA: 5G Automotive Alliance

Standardization body	<p>5GAA (5G Automotive Alliance)</p> <p>http://5gaa.org/</p>
Standard No.	<p>Currently only a white paper (http://5gaa.org/pdfs/5GAA-whitepaper-23-Nov-2016.pdf), but planned to provide various recommendation and guidelines by the 5GAA WGs:</p>

	<ul style="list-style-type: none"> • WG1-Use Cases and Technical Requirements; • WG2- System Architecture and Solution Development; • WG3 Evaluations, Testbeds and Pilots; • WG4- Standards, Policy, Certification and Regulatory; • WG5- Business Models and Go-To-Market Strategies.
Standard Title	See above
URL	http://5gaa.org/
Country	International, Europe
Status	Published, Ongoing
Date	2016 - ongoing
Aim	<p>Develop, test and promote communications solutions, initiate their standardization and accelerate their commercial availability and global market penetration to address society's connected mobility and road safety needs with applications such as autonomous driving, ubiquitous access to services and integration into smart city and intelligent transportation.</p> <p>High level activities to support the mission statement include:</p> <ul style="list-style-type: none"> • Define and harmonize use cases, business and go-to-market models for automotive and intelligent mobility applications, including rental cars, car sharing and electric vehicles • Elaborate technology selection and roadmap evolution strategy including spectrum allocation requirements • Influence standardization and regulatory bodies, certification and approval processes required for the deployment of future connected mobility solutions • Address vehicle-to-x connectivity and communication challenges, including wireless and cellular access networks, security, privacy, authentication, distributed cloud architectures, technology platforms, protocols and data formats required for reliable communication and access to cloud content. Run joint innovation and development projects leading to interoperability testing, large scale pilots and trial deployments.
Description	<p>The 5GAA is a multi-industry association to develop, test and promote communications solutions, initiate their standardization and accelerate their commercial availability and global market penetration to address societal need.</p> <p>The 5GAA was initiated in September 27, 2016 by the following founding members: AUDI AG, BMW Group, Daimler AG, Ericsson, Huawei, Intel, Nokia and Qualcomm Incorporated. Currently, 5GAA is supported by 45 members that represent different types of stakeholders including OEMs, Telecom Operators and vendors. In particular, the 5G Automotive Association is a global association that welcomes stakeholders who are engaged in the automotive industry, the ICT industry or the broader eco-system and value chain for vehicle and road transportation systems.</p>

	<p>The association will develop, test and promote communications solutions, support standardization and accelerate commercial availability and global market penetration. The goal is to address society's connected mobility and road safety needs with applications such as connected automated driving, ubiquitous access to services and integration into smart cities and intelligent transportation.</p> <p>With next generation 5G mobile networks and continued strong LTE evolution, which include Cellular Vehicle-to-everything (C-V2X) communication, the focus of information and communication technologies (ICT) shifts towards the Internet of Things and the digitalization of industries.</p> <p>As an evolution to today's networks, next generation mobile networks are expected to handle much higher data volume, connect many more devices, significantly reduce latency and bring new levels of reliability. For example, 5G can better support mission-critical communications for safer driving and will further support enhanced vehicle-to-everything communications and connected mobility solutions. These new solutions bring new technological and business opportunities for both the automotive and ICT industries, and the members of the association will closely collaborate to realize the full potential together.</p> <p>The association will address key technical and regulatory issues, leveraging next generation mobile networks and integrating vehicle platforms with connectivity, networking and computing solutions. The main activities of the association include:</p> <ul style="list-style-type: none"> • Defining and harmonizing use cases, technical requirements and implementation strategies. • Supporting standardization and regulatory bodies, certification and approval processes. • Addressing vehicle-to-everything technology requirements, such as wireless connectivity, security, privacy, authentication, distributed cloud architectures and more. • Running joint innovation and development projects leading to integrated solutions, interoperability testing, large scale pilots and trial deployments. <p>The above activities will be realized within the following 5GAA WGs:</p> <ul style="list-style-type: none"> • WG1-Use Cases and Technical Requirements; • WG2- System Architecture and Solution Development; • WG3 Evaluations, Testbeds and Pilots; • WG4- Standards, Policy, Certification and Regulatory; • WG5- Business Models and Go-To-Market Strategies. <p>5GAA supports and works in close cooperation with national and regional initiatives, such as the European Connected & Automated Driving Pre-Deployment Project.</p>
Keyword	Interoperability, integration, IoT Architecture, Security, Privacy, Infrastructure, Communication and Connectivity

Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform, Communication network, IoT eco-system
Use in the Project	It can be used in AUTOPILOT WP1, WP2, WP3, WP4 and WP5
Author /Company	HUAWEI

3.1.3 ADASIS Forum /ERTICO

Standardization body	ADASIS forum / ERTICO
Standard No.	-
Standard Title	ADASIS Protocol
URL	http://adasis.org/ http://tracking.vires.com/attachments/download/3911/200v2.0.3-D2.2-ADASIS_v2_Specification.0.pdf
Country	Europe / Worldwide
Status	V2.0.3.0 Released December 2013, V3.0.0 Draft (2017 Release plan)
Date	11.04.2017
Aim	Standardize the interface of Advanced Driver Assistance System to predict the road geometry with its related attributes ahead of a vehicle based on vehicle's position and a digital map, so called ADAS Horizon.
Description	<p>The Advanced Driver Assistance System Interface Specification (ADASIS) forum is an industry driven open initiative handled by ERTICO since 2002. It was established to define a standardized exchange interface between in-vehicle stored data map, Advance Driver Assistance System (ADAS) and automated driving applications. Specifications are defined in relation to Open Auto Drive Forum (OADF) as the cross-domain platform driving standardizations in the area of autonomous driving.</p> <p>The objective is to provide a de facto and reliable worldwide standard to be able to access data generated by map data sources and related data, to build predictive and vehicle environment data based on map, position and other geo-referenced data and therefore improve their performance. The 1st specification 2.0 version was released in 2010 while the 3.0 version is in final review phase.</p> <p>The ADASIS specification defines the concept of an “ADAS Horizon” to extend the horizon beyond what is immediately visible as a means for building road network part and its characteristics as road infrastructure data and road sign information originated from map data along the route ahead of the vehicle. The road network topology represents streets or roads as a</p>

	collection of links (or edges or lines) and street intersections as nodes (or points), whereas “ADAS Horizon” represents a vehicle centric scheme with only those roads in front of the vehicle. The “ADAS Horizon” is constructed using the current vehicle position and a most probable path or trajectory on the road network (as digital map links). The vehicle’s path is defined by an optimized path representation for future possible ways through the links. It represented by the main path and the associated sub-paths describing possible alternative roads for intersection. It includes associated road geometry and related attributes. This “ADAS Horizon” can be serialized and transmitted over the vehicle communication network to facilitate data communication from horizon provider to clients. Moreover the standard embeds with data description and rule definition (introduced in v3.0) for horizon synchronization between provider and receivers. To achieve the interoperability result, the ADASIS protocol is standardized for different media implementation (applicable as OSI layer 7 model and current discussion for 6 and 5 layers). ADASIS v2.0 was designed for CAN bus interface media, while v3.0 extend the concept to larger bandwidth and payload media. In addition it defined data structures for containing this data, using a formal language (IDL defined in the standard).
Keyword	Interface, ADAS, AD
Autopilot Area involved	Vehicle IoT Platform
Use in the Project	Interface from Data fusion block to Environment Re-constructor in block Autonomous Driving functions
Author /Company	CONTINENTAL

3.1.4 AIOTI: Alliance for IoT Innovation

Standardization body	AIOTI (Alliance for IoT Innovation)
Standard No.	Various WG03 (IoT Standards) and WG09 (Smart Mobility) Recommendations and Guidelines (www.aioti.org)
Standard Title	See above
URL	
Country	International, Europe
Status	Published, Ongoing
Date	2015 - ongoing
Aim	WG 03: IoT Standardisation: This Working Group identifies and, where

	appropriate, makes recommendations to address existing IoT standards and analyses gaps in standardization, and develops strategies and use cases aiming for (1) consolidation of architectural frameworks, reference architectures, and architectural styles in the IoT space, (2) (semantic) interoperability, (3) security by design and (4) personal data & persona l data protection to the various categories of stakeholders in the IoT space. WG 09: Smart mobility: The topic for this Working Group refers to IoT solutions that allow for increased multi-modal mobility, more efficient traffic management, a dynamic road infrastructure, automated road tolling, usage based insurance and improved policy making through the analysis of road usage data smart vehicles including autonomous and connected cars.
Description	The main goal of AIOTI is to: (1) develop the IoT eco-system across the Vertical Application Areas which shall include start-up companies and SMEs, and through the Horizontal Activities, and to (2) act as cross cutting organization through the various Vertical Application Areas and Horizontal Activities ongoing in Europe, and build a forum for and cooperate with all relevant ETP's, cPPPs, Joint Undertakings and their private members, EIT KICs, European Innovation Partnerships (EIP's) and other European innovation platforms when IoT innovation issues are concerned.
Keyword	Interoperability, integration, IoT Architecture, Security, Privacy, Infrastructure, Communication and Connectivity
Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform, Communication network, IoT eco-system
Use in the Project	It can be used in AUTOPILOT WP1, WP2, WP3 and WP5
Author /Company	HUAWEI

3.1.5 BBF: BroadBand Forum

Standardization body	BBF (BroadBand Forum)
Standard No.	TR-069 and USP (https://www.broadband-forum.org)
Standard Title	TR-069 CPE WAN Management Protocol (CWMP) and Universal Service Platform (USP)
URL	https://www.broadband-forum.org/cwmp.php . https://www.broadband-forum.org/technical/trlist.php
Country	International, Europe
Status	Published (TR-069), Ongoing (Universal Service Platform (USP))

Date	2006 - 2018
Aim	<p>The BBF BUS Work Area will develop and evolve the TR-069 CPE WAN Management Protocol (CWMP) and a Universal Service Platform (USP) to cover existing use cases, machine-to-machine/IoT use cases, and the virtualization of broadband user services, prioritized by their potential business value.</p> <p>The produced documents related to TR-069 are, listed below. These can be downloaded via: https://www.broadband-forum.org/technical/trlist.php:</p> <ul style="list-style-type: none"> ○ TR-069: Ammendment 1: CPE WAN Management Protocol (December 2006). ○ TR-069: Ammendment 2: CPE WAN Management Protocol v1.1 (December 2007). ○ TR-069: Ammendment 3: CPE WAN Management Protocol (November 2010). ○ TR-069: Ammendment 4: CPE WAN Management Protocol (July 2011). ○ TR-069: Ammendment 5: CPE WAN Management Protocol (November 2013). ○ TR-330: TR-069 UPnP DM Proxy Management Guidelines. ○ TR-181: Device Data Model for TR-069 (February 2010). ○ TR-181 Device Data Model for TR-069 Issue 2, (May 2010). ○ TR-181 Device Data Model for TR-069 Issue 2, Amendment 2 (February 2011). ○ TR-181 Device Data Model for TR-069, Issue 2, Amendment 5 (May 2012). ○ TR-181 Device Data Model for TR-069 Issue 2 Amendment 6 (November 2012). ○ TR-181 Device Data Model for TR-069 Issue 2 Amendment 7 (November 2013). ○ TR-181 Device Data Model for TR-069 Issue 2 Amendment 8 (september 2014). ○ TR-154: TR-069 Data Model XML User Guide (March 2012). ○ TR-142: Framework for TR-069 enabled PON devices (March 2008). ○ TR-142: Framework for TR-069 enabled PON devices Issue 2 (February 2010). ○ TR-140: TR-069 Data Model for Storage Service Enabled Devices, Amendment 1 (April 2010). ○ TR-140: TR-069 Data Model for Storage Service Enabled Devices. Issue 1.1: (December 2007). ○ TR-135: Data Model for a TR-069 Enabled STB (December 2007). ○ TR-106: Amendment 1: Data Model Template for TR-069-Enabled Devices (November 2006). ○ TR-106: DSLHome™ Data Model Template for TR-069 Enabled Devices (September 2006). ○ TR-098: Internet Gateway Device Data Model for TR-069 (December 2006). ○ TR-157: Component Objects for CWMP (March 2009). ● For more details on the CWMP (CPE WAN Management Protocol) protocol, please visit:

	https://www.broadband-forum.org/cwmp.php .
Description	<ul style="list-style-type: none"> • The BBF Work Area: Broadband User Services (BUS) work area is a new area that has been created after the BBF restructuring that took place in 2015. Please note that previously, the Working Group that focused the most on IoT related specifications was the BroadbandHome WG, which was dismissed at the moment that the BUS Work Area has been created. The BroadbandHome WG provided the TR-069 that specifies the CPE WAN Management Protocol, intended for communication between a CPE and Auto-Configuration Server (ACS). • More details on this area can be found via: https://www.broadband-forum.org/technical/technicalwip.php#WABUS. The following text has been copied from the provided URL: • Mission Statement: <ul style="list-style-type: none"> ▪ The Broadband User Services Work Area provides the broadband industry with technical specifications, implementation guides, reference implementations, test plans, and marketing white papers for the deployment, management, and consumption of services by the broadband end user. This Work Area represents the end user perspective when incorporating into the Broadband Forum architecture. • Business Impact: <ul style="list-style-type: none"> • The Broadband User Services Work Area develops specifications and publications to create a new kind of the Broadband experience for the end user and provides new means for service providers and application developers to monetize the broadband user's connection. This ranges from on-demand performance assured business and entertainment services, IoT services related to energy, security, environment, etc. to user control of what can become the data center in the home and small business managed and control with zero- touch diagnostics. All of which opens up large markets and profitable business models. • Scope: <ul style="list-style-type: none"> • Develop and evolve the TR-069 CPE WAN Management Protocol and a Universal Service Platform (USP) to cover existing use cases, machine-to-machine/IoT use cases, and the virtualization of broadband user services, prioritized by their potential business value. • Develop and specify new information models to broaden the range of for which TR-069 and USP can be used. • Develop requirements for broadband user devices and associated software. • Develop test plans and training programs for Work Area protocols and requirements. • Develop marketing white papers that supplement Work Area protocols and requirements.
Keyword	Communication and Connectivity, Infrastructure

Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform, Communication network, IoT eco-system
Use in the Project	It can be used in AUTOPILOT WP1, WP2, WP3 and WP5
Author /Company	HUAWEI

3.1.6 Bluetooth

Standardization body	Bluetooth SIG (The IEEE standardized Bluetooth as IEEE 802.15.1, but no longer maintains the standard. The Bluetooth Special Interest Group (SIG) oversees development of the specification, manages the qualification program, and protects the trademarks.)
Standard No.	Bluetooth Core Specification, version 5.0
Standard Title	See above
URL	https://www.bluetooth.com/
Country	International
Status	Bluetooth 5.0: Published 2016.
Date	See above
Aim	Interoperability among Bluetooth enabled devices worldwide that make short-range, low-power and low-cost wireless communication possible.
Description	Global wireless communication specifications that connects devices. The Bluetooth core specification defines the technology building blocks that developers use to create the interoperable devices that make up the Bluetooth ecosystem. The core specification (Bluetooth 5.0) also offers optional features that allow product/device differentiation. Vol 1: Architecture and terminology overview. Vol 2: Core system package - Basic rate (BR) and enhanced data rate (EDR) controller volume. Vol 3: Core system package - Host volume. Vol 4: Host controller interface - Transport layer. Vol 5: Core system package - Alternate MAC/PHY (AMP) controller volume. Vol 6: Core system package - Low energy controller volume. Vol 7: Core system package - Wireless coexistence volume.
Keyword	V2D, D2D short-range communications.
Autopilot Area involved	Vehicle IoT Integration and platform. Communication network (Piconets).

Use in the Project	Vehicle-to-Device (V2D) and Device-to-Device (D2D) communications. Smartphone or tablet user interfaces.
Author /Company	SINTEF

3.1.7 CEN TC278

Standardization body	CEN TC278		
Standard No.	Various – WG15 - WG6		
Standard Title	Intelligent Transport System - eSafety / eCall - Co-operative systems		
URL	https://www.cen.eu/		
Country	International		
Status	Ongoing		
Date	Since 1992 and ongoing		
Aim	CEN TC 278 is responsible for standardization in the field of telematics for traffic and road transport.		
Description	<p>European Committee for Standardization (CEN) collects the national standards body of 33 European countries, i.e., it is European based. CEN like ETSI, is a recognized SDO by the European Commission. It has a similar structure as ISO with around 400 technical committees divided into subcommittees and some 1600 working groups.</p> <p>CEN TC 278 is the European ITS committee. It started with the name of Road Transport and Traffic Telematics (RTTT), but changed to ITS in 2013. This was the first ITS standardization body, and TC 278 has laid the groundwork for global ITS standards. The initial ideas came from the European framework program called DRIVE, where it became clear that standardization had to be started. In general, CEN has a good representation and participation from industry, service providers, public bodies and road operators/authorities, but less from car makers.</p> <p>The most relevant Working Groups for AUTOPILOT are WG15 (eSafety / eCall) and WG16 (Co-operative systems).</p> <p>In the following Table, an overview of the active working groups in TC278 is outlined.</p> <table data-bbox="486 1948 1404 2016"> <thead> <tr> <th>Working Group Number</th><th>Working Group Name</th></tr> </thead> </table>	Working Group Number	Working Group Name
Working Group Number	Working Group Name		

	<ul style="list-style-type: none"> 1 Electronic fee collection 2 Freight 3 Public transport 7 ITS spatial data 8 Road traffic data 10 Human-machine interfacing 12 Vehicle identification 13 ITS architecture 14 Recovery of stolen vehicles 15 eCall 16 Cooperative ITS <p>TC 278 is working closely with the ISO TC 204 committee, responsible for developing standards in the same field of action. CEN standards are also often ISO standards.</p>
Keyword	eCall, Safety
Autopilot Area involved	Vehicle IoT Integration and platform, Communication network
Use in the Project	The most relevant Working Groups for AUTOPILOT are WG15 (eSafety / eCall) and WG16 (Co-operative systems).
Author /Company	ERTICO TIM

3.1.8 ETSI TC ITS

Standardization body	ETSI TC ITS
Standard No.	various
Standard Title	various
URL	http://www.etsi.org
Country	Europe
Status	Published - ongoing
Date	Since 2007 and ongoing
Aim	ETSI is the European Telecommunications Standardisation Institute and is a commonly known a major contributor to global telecommunications standards such as GSM, LTE and DVB. ETSI does also have a formal and legal

	<p>role in Europe since it produces Harmonised European Norms, which is an operative part of the R&TTE directive that allows sale and operation of radio equipment without type approval.</p> <p>ETSI is a member-driven organization consisting of companies, universities, and research institutes. Members pay an annual fee to ETSI and can then be part of standards development.</p> <p>ETSSTI is organized in a number of Technical Committees (TC), where TC ITS covers the Intelligent Transport aspects.</p>												
Description	<p>ETSI TC ITS concentrates on a subset of the ITS scope with the current focus being on</p> <ul style="list-style-type: none"> • 5.9 GHz communications called ITS-G5 in ETSI terminology, • applying a special multi-hopping network function called GeoNet, and • serving a small number of mainly safety applications for vehicle-to-vehicle and vehicle-to-roadside scenarios. This vehicle-safety-centric scenario is supported by strong security provisions. <table border="1"> <thead> <tr> <th>Working Group Number</th><th>Working Group Name</th></tr> </thead> <tbody> <tr> <td>1</td><td>Application requirements and services</td></tr> <tr> <td>2</td><td>Architecture and Cross-layer</td></tr> <tr> <td>3</td><td>Transport and Network</td></tr> <tr> <td>4</td><td>Media and Medium Related</td></tr> <tr> <td>5</td><td>Security</td></tr> </tbody> </table> <p>The ETSI TC ITS standards that could be of interest for AUTOPILOT project are listed below:</p> <ul style="list-style-type: none"> • ETSI EN 302 636 series ITS; Vehicular Communications; GeoNetworking • ETSI EN 302 637-3 V1.2.2 – DENM • ETSI EN 302 637-2 V1.3.2 – CAM • ETSI EN 302 665 V1.1.1 - ITS; Communications Architecture • ETSI EN 302 895 V1.1.1 - LDM • ETSI TS 101 556-2 V1.1.1 - ITS; Infrastructure to Vehicle Communication; Part 2: Communication system specification to support application requirements for TIS and TPG interoperability • ETSI TS 102 894-1 V1.1.1 - SPAT/MAP • ETSI TS 102 723-8 V1.1.1 - ITS; OSI cross-layer topics; Part 8: Interface between security entity and network and transport layer • ETSI TS 102 940 V1.21 - ITS; Security; ITS communications security architecture and security management • ETSI TS 103 191, TS 103 096, TS 102 869, TS 102 868, TS 102 871, TS 102 870, TS 102 859- ITS Testing, Conformance test specifications • ETSI EG 202 798 V1.1.1 - ITS; Testing; Framework for conformance and interoperability testing <p>For more details about these standards documents please refer to Annex B – Standards and Specifications – section 6.2.2</p>	Working Group Number	Working Group Name	1	Application requirements and services	2	Architecture and Cross-layer	3	Transport and Network	4	Media and Medium Related	5	Security
Working Group Number	Working Group Name												
1	Application requirements and services												
2	Architecture and Cross-layer												
3	Transport and Network												
4	Media and Medium Related												
5	Security												
Keyword	<p>Communication and Connectivity, Integration and interoperability, IoT Architecture, ITS-G5, Applications, Infrastructure, Security and Privacy, ITS, Management, Security, Conformance, Testing</p>												

Autopilot Area involved	Communication network, Vehicle IoT Integration and platform, IoT eco-system, IoT Platform, Security architecture, Vehicle IoT testing, Test specification
Use in the Project	<p>AUTOPILOT will monitor the activities of ETSI TC ITS especially of WG1 (User and Application requirements) as it deals with the topics most relevant to AUTOPILOT.</p> <p>ETSI EN 302 637-3 V1.2.2 – DENM: the Decentralized Environmental Notification Message could be used to communicate any type of hazard with short-range V2x communications</p> <p>ETSI EN 302 637-2 V1.3.2 – CAM: the Cooperative Awareness Message is the base for all the applications that needs to have information about the surrounding of the car</p> <p>ETSI EN 302 895 V1.1.1 – LDM: Local Dynamic Map could be used to store any useful information about the surrounding of a vehicle. Could be extended to host IoT specific information</p> <p>ETSI TS 101 556-2 V1.1.1 - ITS; Infrastructure to Vehicle Communication; Part 2: Communication system specification to support application requirements for TIS and TPG interoperability: this standard can be used as reference for examining vehicle communication to support application requirements not only for tyre pressure interoperability but also general interoperability aspects of autonomous driving and IOT</p> <p>ETSI TS 102 894-1 V1.1.1 - SPAT/MAP: this standard is useful to send standard information about phase/time of traffic lights</p> <p>ETSI TS 102 723-8 V1.1.1 - ITS; OSI cross-layer topics; Part 8: Interface between security entity and network and transport layer: this standard specifies important OSI cross-layer topics and addresses interfaces between security entities and network and transport layers. It is expected that security issues will have a very strong impact on test scenarios of the V2I and I2V communication technologies, i.e. under consideration of IOT security aspects</p> <p>ETSI TS 102 940 V1.21 - ITS; Security; ITS communications security architecture and security management: the security architecture for Intelligent Transport System (ITS) communications, described in this standard, is in general an important requirement for the AUTOPILOT project and the document provides especially important input for WP1.5 (Security, Privacy and Data Specification) and WP1.2 (IoT architecture and specification)</p> <p>ETSI TS 103 191, TS 103 096, TS 102 869, TS 102 868, TS 102 871, TS 102 870, TS 102 859- ITS Testing, Conformance test specifications: the tests specified in this standard are important to validate the AUTOPILOT ITS components</p> <p>ETSI EG 202 798 V1.1.1 - ITS; Testing; Framework for conformance and interoperability testing: the provided guidelines and templates from chapters 7 (Guidelines for interoperability testing), 8.2 (Provision of Test suite structure & Test Purposes) and annex A (Introduction to Interoperability testing) are useful input for the AUTOPILOT WP2.5 (Pilot Readiness Verification) and WP3.1 (Pilot site test specification)</p>
Author /Company	CETECOM EGM ERTICO ISMB

	TIM T-Systems
--	------------------

3.1.9 ETSI TC Cyber

Standardization body	ETSI TC Cyber
Standard No.	various
Standard Title	various
URL	http://www.etsi.org
Country	Europe
Status	Published - ongoing
Date	Since 2014 and ongoing
Aim	ETSI is organized in a number of Technical Committees (TC), where TC Cyber covers the cross-domain cybersecurity aspects.
Description	<p>ETSI is working closely with relevant stakeholders to develop standards to increase privacy and security for organizations and citizens across Europe and worldwide. The aim is to provide standards for horizontal and cross-domain applicability, as well as for the security of infrastructures, devices, services and protocols and security tools and techniques. The addressed areas are:</p> <ul style="list-style-type: none"> • Horizontal cybersecurity • Securing technologies and systems • Security tools and techniques <p>Work is carried out by many ETSI groups. TC CYBER mainly works on cross-domain cybersecurity while addressing more specific domains or security tools and techniques if not addressed by other ETSI groups.</p> <p>In addition, TC CYBER serves as a centre of expertise and offers security advice and guidance to users, manufacturers and network and infrastructure operators as well as other ETSI committees.</p> <p>The ETSI TC Cyber standards relevant to AUTOPILOT project are listed below:</p> <ul style="list-style-type: none"> • ETSI TR 103 303 V1.1.1 - Protection measures for Critical Infrastructure • ETSI TR 103 304 V1.1.1 - Protection in mobile and cloud services <p>For more details about these standards see Annex B – Standards and Specifications – Section 6.2.3</p>
Keyword	Cyber, Access Control, Critical Infrastructure, Critical Infrastructure Protection, Public Key Infrastructure, Anonymization, Cloud Service

	Customer, Cloud Service Partner, Cloud Service Provider, Cloud Service User, PII controller, PII principal, PII process, Threats, Trust
Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform, Communication network, IoT eco-system
Use in the Project	The security architecture, described in these standards, should be used as guideline in the AUTOPILOT architecture design phase, with particular reference to the T1.2, IOT architecture and specification, and T1.5 Security, Privacy and Data Specification
Author /Company	THALES TIM

3.1.10 ETSI TC ERM

Standardization body	ETSI TC ERM
Standard No.	various
Standard Title	various
URL	http://www.etsi.org
Country	Europe
Status	Published - ongoing
Date	See Annex B – Standards and Specifications
Aim	ETSI is organized in a number of Technical Committees (TC), where TC ERM covers the radio product and electromagnetic compatibility aspects
Description	<p>ETSI Technical Committee (TC) EMC and Radio Spectrum Matters (ERM) is responsible for a range of radio product and electromagnetic compatibility (EMC) standards and the overall co-ordination of EMC and radio spectrum matters within ETSI.</p> <p>In addition to its liaison role with other standardization bodies on regulatory affairs, EMC and radio spectrum matters, TC ERM produces a range of ETSI deliverables dealing with radio equipment and systems where they are not undertaken by other ETSI groups of the ETSI Wireless Systems Cluster.</p> <p>TC ERM consists of two horizontal Working Groups (WG) dealing with ElectroMagnetic Compatibility (WGEMC) and Radio Spectrum Matters (WGRM) and a number of vertical Task Groups (TG) which are set up to deal with particular radio issues.</p> <p>The ETSI TC ERM standards relevant to AUTOPILOT project are listed below:</p>

	<ul style="list-style-type: none"> ETSI EN 300 674-2-1 V2.1.1 - TTT; Dedicated Short Range Communication (DSRC)-Harmonized standard - Road Side Units (RSU) ETSI EN 300 674-2-2 V2.1.1 - TTT; Dedicated Short Range Communication (DSRC)-Harmonized standard - On-Board Units (OBU) ETSI EN 302 571 V2.0.0 – ITS; Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band, Harmonized Standard <p>For more details about these standards see Annex B – Standards and Specifications – Section 6.2.3</p>
Keyword	ITS-G5; LTE-V2X; Communication and connectivity
Autopilot Area involved	Mobile Communication network
Use in the Project	<p>ETSI EN 300 674-2-1 V2.1.1 - TTT; Dedicated Short Range Communication (DSRC)-Harmonized standard - Road Side Units (RSU) and ETSI EN 300 674-2-2 V2.1.1 - TTT; Dedicated Short Range Communication (DSRC)-Harmonized standard - On-Board Units (OBU): several Autopilot test sites have to consider the usage of OBU (vehicle based) and RSU equipment. DSRC is a well-established and stable communication technology between road-side equipment and moving vehicles, which can be used for reference for communication purposes</p> <p>ETSI EN 302 571 V2.0.0 – ITS; Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band, Harmonized Standard: the overall AUTOPILOT concept is based on 4G/5G and LTE-V2X in combination with G5 technology of road side units placed along ITS application corridors, mainly roads. With regards to AUTOPILOT test sites special, safety issues taking extreme test source voltages and regulated lead-acid battery power sources used on vehicles have to be considered, so that accident risks are minimized</p>
Author /Company	TIM T-Systems

3.1.11 ETSI ISG CIM

Standardization body	ETSI ISG CIM (ETSI Industry Specification Group on Context Information Management)
Standard No.	Being developed
Standard Title	Being developed
URL	https://portal.etsi.org/tb.aspx?tbid=854&SubTB=854
Country	Europe

Status	Ongoing Work
Date	February 2017 - Present
Aim	The aim of the ETSI Industry Specification Group on Context Information Management is to issue technical specifications to enable multiple organizations to develop interoperable software implementations of a cross-cutting Context Information Management (CIM) Layer. It is about bridging the gap between abstract standards and concrete implementations.
Description	<p>The CIM Layer should enable applications to discover access update and manage context information from many different sources, as well as to publish it through interoperable data publication platforms.</p> <p>The work of ISG CIM will be done in a phased manner. The initial phase will be purely informative and result in an ISG CIM Group Report (GR). It will be followed by a second normative phase resulting in several ISG CIM Group Specifications (GS). In order to avoid duplication of work, close collaborations will be sought with a number of organizations and initiatives such as with ETSI TC SmartM2M and oneM2M.</p> <p>The Phase 1 ISG CIM Group Report will detect and describe the standardization gaps in order to consider any missing features and to ensure interoperable software implementations, including open source implementations. Developing ISG CIM Group Specifications in Phase 2 will subsequently fill these gaps. It is expected that an extension of the RESTful binding of the OMA NGSI API involving expression using JSON-LD could aid interoperability, so this and potentially other extensions will be considered.</p>
Keyword	Integration and Interoperability, IoT Architecture, Context Information Management, Context Brokering, Semantics
Autopilot Area involved	AUTOPILOT IoT Platform (based on Fiware and oneM2M)
Use in the Project	<p>ETSI ISG CIM is developing an API using the OMA NGSI Context Interfaces (3.1.21) as a starting point. The result will likely be taken up in a new version of FIWARE GEs (0), which are going to be used in the AUTOPILOT IoT Platform.</p> <p>This standards is important to specify the Content Information Model and AUTOPILOT will likely use but also influence its content to take into account the particular area of ITS and Automated cars.</p>
Author /Company	EGM

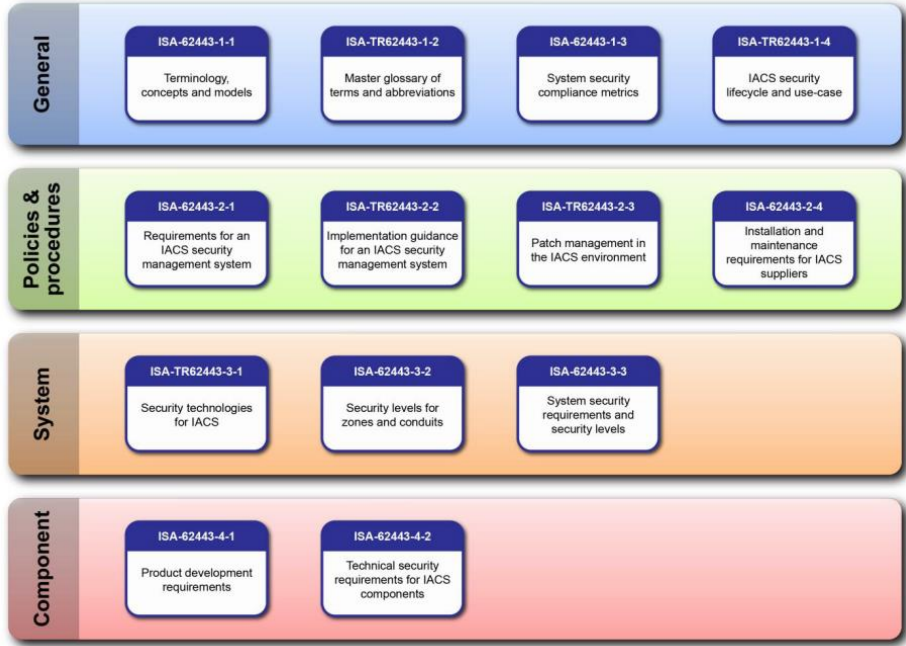
3.1.12 FI-PPP/FIWARE Foundation

Standardization body	Future Internet Public-Private Partnership (FIPPP) - until 2016 FIWARE Foundation e.V. – since 2016
Standard No.	- IoT Broker GE Specification: https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWA

	<p>RE.OpenSpecification.IoT.Backend.IoTBroker</p> <ul style="list-style-type: none"> - IoT Discovery GE Specification: https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification.IoT.Backend.IoTDiscovery - Context Broker GE Specification: https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification.Data.ContextBroker <p>The GE specifications listed above are based on the OMA NGSI Context (page Error! Bookmark not defined.) Interfaces specification, which are the starting point for the context interface being developed by ETSI ISG CIM (page 32)</p>
Standard Title	FIWARE
URL	https://www.fiware.org/ .
Country	Europe
Status	Published
Date	2011 - ongoing
Aim	To build an open sustainable ecosystem around public, royalty-free and implementation-driven software platform standards that will ease the development of new Smart Applications in multiple sectors.
Description	<p>FIWARE is a middleware platform that was initiated by the European Union as part of the Future Internet PPP, for the development and global deployment of applications for Future Internet. It is now based on the FIWARE open community and lead by the FIWARE Foundation.</p> <p>The API specifications of FIWARE are open and royalty-free to facilitate creation and delivery of Future Internet applications and services in a variety of areas, including smart cities, sustainable transport, logistics, renewable energy, and environmental sustainability.</p>
Keyword	IoT Architecture
Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform
Use in the Project	FIWARE GE implementations based on the specifications listed above are to be used in the AUTOPILOT IoT platform, providing applications with efficient access to IoT-related information, also across different sites.
Author /Company	NEC

3.1.13 IEC

Standardization body	ISA/IEC - http://www.iec.ch
-----------------------------	---

Standard No.	ISA/IEC-62443
Standard Title	Security for industrial automation and control systems
URL	https://webstore.iec.ch/publication/7033
Country	International
Status	Published
Date	2013 – 08 – 12
Aim	IEC 62443 documents addressing policies and procedures vs. functional requirements.
Description	<p>It is a family of standard organized into four general categories called General, Policies and Procedures, System, and Component.</p>  <p>The General category includes foundational information such as concepts, models and terminology, together with descriptions of security metrics and security life cycles for industrial automation and control systems (IACS). The Policies and Procedures category is intended for asset owners. Documents in this category are concerned with various aspects of creating and maintaining an effective IACS security program. The System category describes system design guidance and requirements for the secure integration of control systems. The Component category describes specific product development and technical requirements of control system products. These are primarily intended for control product vendors, but can be used by integrator and asset owners to aid them in acquiring secure products.</p>

	<table><tr><th colspan="4">IEC 62443 / ISA-99</th></tr><tr><td><div>General</div><div>1-1 Terminology, concepts and models</div><div>1-2 Master glossary of terms and abbreviations</div><div>1-3 System security compliance metrics</div><div>Definitions Metrics</div></td><td><div>Policies and procedures</div><div>2-1 Establishing an IACS security program</div><div>2-2 Operating an IACS security program</div><div>2-3 Patch management in the IACS environment</div><div>2-4 Certification of IACS supplier security policies and practices</div><div>Requirements to the security organization and processes of the plant owner and suppliers</div></td><td><div>System</div><div>3-1 Security technologies for IACS</div><div>3-2 Security assurance levels for zones and conduits</div><div>3-3 System security requirements and security assurance levels</div><div>Requirements to a secure system</div></td><td><div>Component</div><div>4-1 Product development requirements</div><div>4-2 Technical security requirements for IACS products</div><div>Requirements to secure system components</div></td></tr><tr><td colspan="4"><div>Functional requirements</div><div>Processes / procedures</div></td></tr></table>	IEC 62443 / ISA-99				<div>General</div> <div>1-1 Terminology, concepts and models</div> <div>1-2 Master glossary of terms and abbreviations</div> <div>1-3 System security compliance metrics</div> <div>Definitions Metrics</div>	<div>Policies and procedures</div> <div>2-1 Establishing an IACS security program</div> <div>2-2 Operating an IACS security program</div> <div>2-3 Patch management in the IACS environment</div> <div>2-4 Certification of IACS supplier security policies and practices</div> <div>Requirements to the security organization and processes of the plant owner and suppliers</div>	<div>System</div> <div>3-1 Security technologies for IACS</div> <div>3-2 Security assurance levels for zones and conduits</div> <div>3-3 System security requirements and security assurance levels</div> <div>Requirements to a secure system</div>	<div>Component</div> <div>4-1 Product development requirements</div> <div>4-2 Technical security requirements for IACS products</div> <div>Requirements to secure system components</div>	<div>Functional requirements</div> <div>Processes / procedures</div>			
IEC 62443 / ISA-99													
<div>General</div> <div>1-1 Terminology, concepts and models</div> <div>1-2 Master glossary of terms and abbreviations</div> <div>1-3 System security compliance metrics</div> <div>Definitions Metrics</div>	<div>Policies and procedures</div> <div>2-1 Establishing an IACS security program</div> <div>2-2 Operating an IACS security program</div> <div>2-3 Patch management in the IACS environment</div> <div>2-4 Certification of IACS supplier security policies and practices</div> <div>Requirements to the security organization and processes of the plant owner and suppliers</div>	<div>System</div> <div>3-1 Security technologies for IACS</div> <div>3-2 Security assurance levels for zones and conduits</div> <div>3-3 System security requirements and security assurance levels</div> <div>Requirements to a secure system</div>	<div>Component</div> <div>4-1 Product development requirements</div> <div>4-2 Technical security requirements for IACS products</div> <div>Requirements to secure system components</div>										
<div>Functional requirements</div> <div>Processes / procedures</div>													
Keyword	SL Security level , SL-A Achieved security level , SL-C Capability security level, SL-T Target security level												
Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform, Communication network, IoT eco-system.												
Use in the Project	This standard (family of) shall be used as references for anyone involved in developing products for or associated with the IoT.												
Author /Company	THALES												

3.1.14 IEEE

Standardization body	IEEE
Standard No.	various
Standard Title	various
URL	https://standards.ieee.org/
Country	International
Status	Published - ongoing
Date	See Annex B – Standards and Specifications
Aim	IEEE mission is to foster technological innovation and excellence for the benefit of humanity. Strategic plan (2015 - 2020) http://www.ieee.org/about/ieee_strategic_plan_2015_to_2020.pdf

Description	<p>IEEE has standards activities in many aspects of ITS, such as vehicle communications and networking (IEEE 802 series). In addition, the IEEE 1609 Family of Standards for Wireless Access in Vehicular Environments (WAVE) define an architecture and a complementary, standardised set of services and interfaces that collectively enable secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications. These standards are designed to provide the foundation for a broad range of applications in the transportation environment, including vehicle safety, automated tolling, enhanced navigation, traffic management and many others.</p> <p>The IEEE standards relevant to AUTOPILOT project are listed below:</p> <p>IEEE 802.11p-2010: Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments</p> <p>IEEE 802.15.1-2005: Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 15.1a: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPAN).</p> <p>IEEE 802.15.4-2015: Standard for Low-Rate Wireless Networks.</p> <p>IEEE 802.20 series - Mobile Broadband Wireless Access (MBWA)</p> <p>IEEE 1609 series P1609 Wireless Access in Vehicular Environments (WAVE)</p> <p>For more details about these standards see Annex B – Standards and Specifications – Section 6.2.5</p>
Keyword	Communication and Connectivity, WLAN, WiFi, V2X Communication (V2V, V2I), V2D Communication, low data rate, short range, MBWA, Security
Autopilot Area involved	Vehicle IoT Integration and platform, Communication network, IoT eco-system, IoT Platform
Use in the Project	<p>IEEE 802.11p - Wireless local area networks - Wireless Access in Vehicular Environments: can be used for Vehicle -to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications.</p> <p>IEEE 802.15 - Wireless Personal Area Network (WPAN): can be used for Vehicle -to-Device (V2D) communications.</p> <p>IEEE 802.20 - Mobile Broadband Wireless Access (MBWA): can be used for Vehicle -to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications.</p> <p>IEEE P1609 Wireless Access in Vehicular Environments (WAVE): This set of services and interfaces collectively enable secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications</p>
Author /Company	SINTEF TIM

3.1.15 IETF

Standardization body	IETF (Internet Engineering Task Force)
Standard No.	Various
Standard Title	Specifications published by several WGs: 6lo (IPv6 over Networks of Resource-constrained Nodes), 6TiSCH (IPv6 over the TSCH mode of IEEE 802.15.4e), detnet (Deterministic Networking), lpwan (Low Power WAN), IPWAVE (), ACE (Authentication and Authorization for Constrained Environments), CORE (Constrained RESTful Environments) WG, COSE (CBOR Encoded Message Syntax), CBOR (Concise Binary Object Representation), Dice (DTLS In Constrained Environments)
URL	www.ietf.org
Country	International
Status	Published, Ongoing
Date	2003 – ongoing
Aim	Provide specifications that are targeted to support the connectivity and communication of IoT constrained devices with the Internet
Description	<p>The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet. The IETF Mission Statement is documented in RFC 3935. The IETF has an IOT directorate to deal with IOT specificities.</p> <p>IETF WG 6lo (IPv6 over Networks of Resource-constrained Nodes) focuses on the work that facilitates IPv6 connectivity over constrained node networks with the characteristics of: limited power, memory and processing resources, hard upper bounds on state, code space and processing cycles, optimization of energy and network bandwidth usage, lack of some layer 2 services like complete device connectivity and broadcast/multicast.</p> <p>The IETF RFC 4944: transmission of IPv6 Packets over IEEE 802.15.4 Networks could be relevant for AUTOPILOT project.</p> <p>For more details about this standard see Annex B – Standards and Specifications – Section 6.2.6</p>
Keyword	Integration/Interoperability, Applications, Devices and sensor technology, Security and Privacy, Communication and Connectivity, Infrastructure
Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform, Communication network, IoT eco-system
Use in the Project	It can be used in AUTOPILOT WP1, WP2, WP3, WP4 and WP5

	In particular 6LowPAN can be used to bridge vehicular networks with IoT infrastructure. 6LowPAN can be also used for low power and short-range networking to enable specific services by the IoT infrastructure.
--	--

3.1.16 IRTF

Standardization body	IRTF (Internet Research Task Force)
Standard No.	Various
Standard Title	Specifications published by T2T RG (Thing to Thing Research Group)
URL	www.irtf.org
Country	International,
Status	Published, Ongoing
Date	2015 - ongoing
Aim	The T2T RG is a proposed IRTF Research Group that will be using and providing input mainly to IETF, but also to the IOT research community.
Description	<ul style="list-style-type: none"> The T2T (Thing to Thing) proposed RG is not yet an official IRTF Research Group, but it can become an official one if there is satisfactory participation. The T2t RG will investigate open research issues in turning a true “Internet of Things” into reality, and on an Internet where low-resource nodes (“Things”, “Constrained Nodes”) can communicate among themselves and with the wider Internet, in order to partake in permissionless innovation. <p>The focus of this RG will be on issues that touch opportunities for standardization in the IETF:</p> <ul style="list-style-type: none"> Start at the adaptation layer connecting devices to IP; End at the application layer with architectures and APIs for communicating and making data and management functions (including security functions) available. <p>The main areas of interest are:</p> <ul style="list-style-type: none"> Understanding and managing the motivation for single purpose silos and gateways; facilitating a move towards small pieces loosely joined (hence “thing-to-thing”); scaling the number of applications in a single network. Deployment considerations; scaling considerations; cost of ownership. Management and Operation of Things. Lifecycle aspects (including, but not limited to, security considerations). Cooperation with W3C, e.g. on data formats and semantics.

Keyword	Communication and Connectivity, Integration/Interoperability, IoT Architecture, Security and Privacy
Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform, Communication network, IoT eco-system
Use in the Project	It can be used in AUTOPILOT WP1, WP2, WP3, WP4 and WP5
Author /Company	HUAWEI

3.1.17 ISO TC204

Standardization body	ISO TC204
Standard No.	Various –
Standard Title	Intelligent Transport System
URL	https://www.iso.org/
Country	International
Status	Ongoing
Date	Since 1992 and ongoing
Aim	ISO TC204 is responsible for the overall system aspects and infrastructure aspects of intelligent transport systems (ITS), as well as the coordination of the overall ISO work programme in this field including the schedule for standards development, taking into account the work of existing international standardization bodies.
Description	<p>International Organization for Standardization (ISO) is a world-wide SDO with 162 member countries. Every member country has a national standards body, which appoints a delegate representing the country during standardization meetings. The national standards body collects companies and other interested parties of the ISO standardization. ISO hosts nearly 300 technical committees (TC) treating a plethora of different subjects. Each TC is usually divided into several working groups (WG).</p> <p>ISO TC204 is the International ITS committee. It was originally called Transport Information Control Systems (TICS), but changed its name to Intelligent Transport Systems some years ago. This was the second ITS standardization body to start after CEN TC278.</p> <p>TC204 was patterned on CEN TC278, and the cooperation is regulated by the Vienna Agreement (VA) between ISO and CEN, which means that many</p>

	<p>working groups have joint meetings to ensure alignment.</p> <p>ISO TC204 is the most active group within the field of ITS standardization and its meetings are attended by 150+ delegates from all over the world, with an about even split between American (US and Canada) Asian (mostly from China, Japan and South Korea) and European delegates. ITS TC204 meets twice a year alternating the meeting venue between the Americas, the Asia Pacific region and Europe.</p> <p>TC204 is further divided into several WG, of which some are dealing with communication – WG 14 Vehicle/roadway warning and control systems, WG 16 Communications and WG 18 Cooperative systems. See following table, for a full overview of the different WG within TC 204.</p> <table border="1"> <thead> <tr> <th>Working Group Number</th><th>Working Group Name</th></tr> </thead> <tbody> <tr> <td>1</td><td>Architecture</td></tr> <tr> <td>3</td><td>ITS database technology</td></tr> <tr> <td>4</td><td>Automatic vehicle and equipment identification</td></tr> <tr> <td>5</td><td>Fee and toll collection</td></tr> <tr> <td>7</td><td>General fleet management and commercial/freight</td></tr> <tr> <td>8</td><td>Public transport/emergency</td></tr> <tr> <td>9</td><td>Integrated transport information, management and control</td></tr> <tr> <td>10</td><td>Traveller information systems</td></tr> <tr> <td>14</td><td>Vehicle/roadway warning and control systems</td></tr> <tr> <td>16</td><td>Communications</td></tr> <tr> <td>17</td><td>Nomadic devices in ITS Systems</td></tr> <tr> <td>18</td><td>Cooperative systems</td></tr> </tbody> </table> <p>The ISO standards relevant to AUTOPILOT project are listed below:</p> <ul style="list-style-type: none"> • ISO/AWI 20900 PAPS Partially automated parking systems • ISO TC204 WG14 - Automated Valet Parking System • ISO/CD 20035 C-ACC Cooperative Adaptive Cruise Control - Performance requirements and test procedures <p>For more details about these standards see Annex B – Standards and Specifications – Section 6.2.7</p>	Working Group Number	Working Group Name	1	Architecture	3	ITS database technology	4	Automatic vehicle and equipment identification	5	Fee and toll collection	7	General fleet management and commercial/freight	8	Public transport/emergency	9	Integrated transport information, management and control	10	Traveller information systems	14	Vehicle/roadway warning and control systems	16	Communications	17	Nomadic devices in ITS Systems	18	Cooperative systems
Working Group Number	Working Group Name																										
1	Architecture																										
3	ITS database technology																										
4	Automatic vehicle and equipment identification																										
5	Fee and toll collection																										
7	General fleet management and commercial/freight																										
8	Public transport/emergency																										
9	Integrated transport information, management and control																										
10	Traveller information systems																										
14	Vehicle/roadway warning and control systems																										
16	Communications																										
17	Nomadic devices in ITS Systems																										
18	Cooperative systems																										
Keyword	International standardization; ITS system aspects; Integration and interoperability; Devices and sensor technology ; Applications; Communication and connectivity																										
Autopilot Area involved	Vehicle IoT Integration and platform; Communication network																										
Use in the Project	The AUTOPILOT project will be presented at the G-ITS (Green-ITS) workshop at the 49th plenary meeting of ISO TC204, which will be held in Paris from April 24 to 28. Furthermore this meeting will be the perfect opportunity to raise awareness of the AUTOPILOT project. Of special interest will be the meeting of WG14 (Vehicle Control Systems) as this group is standardizing performance requirements and test procedures for many of the new ITS																										

	<p>features in cars, such as automatic parking, intelligent cruise control, backing-up aid, lane departure warning, collision warning and so on. Both vehicle manufacturers and authorities are well represented. This is one of the more active and productive WGs of ISO TC204; not in the number of produced standards, but in the consistent deployment of these standards into vehicles on the road today.</p> <p>ISO/AWI 20900 PAPS Partially automated parking systems: this standard is used to manage test procedures and performance requirements related to partially automated parking system use cases. We reference it as a possible baseline for some of the functions of Pilot Sites which PAPS is involved</p> <p>ISO TC204 WG14 - Automated Valet Parking System: this standard is used to manage procedures related to automated valet parking use cases. We reference it as a possible baseline for some of the functions of Pilot Sites which automated valet parking is involved</p> <p>ISO/CD 20035 C-ACC Cooperative Adaptive Cruise Control - Performance requirements and test procedures: This standard is used to manage test procedures and performance requirements related to C-ACC use cases. We reference it as a possible baseline for some of the functions of Pilot Sites which C-ACC is involved</p>
Author /Company	<p>ERTICO</p> <p>IDIADA</p> <p>TIM</p>

3.1.18 ISO/IEC JTC1/SC27

Standardization body	ISO/IEC JTC1/SC27
Standard No.	Various
Standard Title	IT Security techniques
URL	https://www.iso.org/
Country	International
Status	Published - ongoing
Date	Since 1989 and ongoing
Aim	ISO/IEC JTC 1/SC 27 is responsible for the development of International Standards, Technical Reports, and Technical Specifications within the field of information and IT security

Description

ISO/IEC JTC 1/SC 27 is a standardization subcommittee of the Joint Technical Committee ISO/IEC JTC 1 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

The scope of ISO/IEC JTC 1/SC 27 is the development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management systems, security processes, and security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security management systems;
- Security evaluation criteria and methodology.

ISO/IEC JTC 1/SC 27 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas

See following table, for a full overview of the different WG within ISO/IEC JTC 1/SC 27.

Working Group	Title
SWG-M	Special Working Group on Management
SWG-T	Transversal items
WG 1	Information security management systems
WG 2	Cryptography and security mechanisms
WG 3	Security evaluation, testing and specification
WG 4	Security controls and services
WG 5	Identity management and privacy technologies

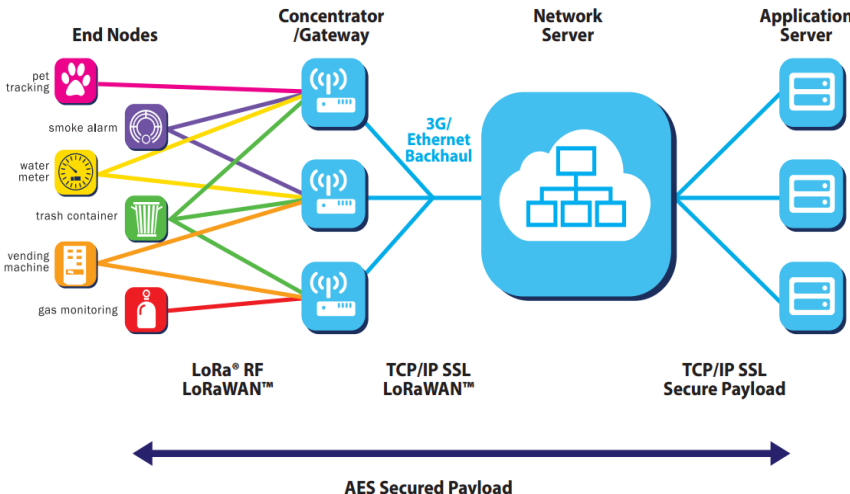
The ISO/IEC JTC1/SC27 standards relevant to AUTOPILOT project are listed below:

- ISO/IEC 27000:2016 Information technology — Security techniques — Information security management systems — Overview and vocabulary
- ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC: 27002 Information technology — Security techniques — Code of practice for information security controls
- ISO/IEC 15408-1 - Evaluation criteria for IT security - Information and General Model
- ISO/IEC 15408-2 - Evaluation criteria for IT security – Security Functional Components

	<ul style="list-style-type: none"> ISO/IEC 15408-3 - Evaluation criteria for IT security T Security Assurance Components <p>For more details about these standards see Annex B – Standards and Specifications – Section 6.2.8</p>
Keyword	ISMS (Information Security Management System); Security; Applications
Autopilot Area involved	IoT Platform; Vehicle IoT Integration and platform; Communication network; IoT eco-system
Use in the Project	<p>ISO/IEC 27000 family of standard (ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002): this family of standards is widely adopted by companies and organizations to manage security related aspects of information systems. We reference it as a possible baseline for overall IT security management by AUTOPILOT service suppliers</p> <p>ISO TC204 WG14 - Automated Valet Parking System: this standard is used to manage procedures related to automated valet parking use cases. We reference it as a possible baseline for some of the functions of Pilot Sites which automated valet parking is involved</p> <p>ISO/IEC 15408-1 - Evaluation criteria for IT security - Information and General Model: this standard shall be the guide for the AUTOPILOT architecture in particular for T1.5 “Security, Privacy and Data Specification” and for T1.2 “IoT Architecture and Specification”</p>
Author /Company	THALES TIM

3.1.19 LoRaWAN™

Standardization body	LoRa Alliance, Inc. - https://www.lora-alliance.org/
Standard No.	201R0
Standard Title	LoRaWAN™ Specification
URL	https://www.lora-alliance.org/portals/0/specs/LoRaWAN%20Specification%201R0.pdf
Country	International
Status	Released
Date	2015
Aim	Low-power and log-range network communication protocol optimized for battery-powered end-devices that may be either mobile or mounted at a fixed location.

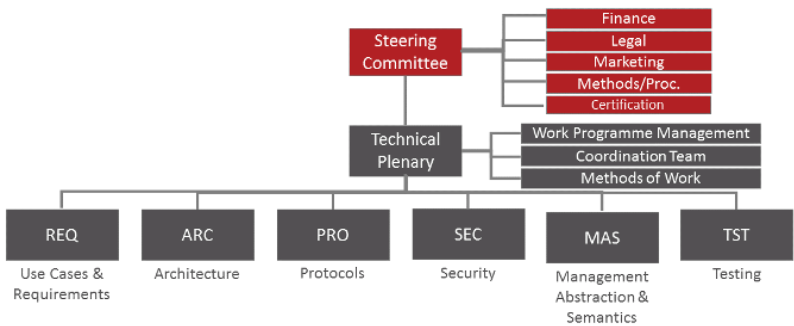
Description	<p>LoRaWAN™ defines the communication protocol and system architecture for the network. It is based on the LoRa® physical layer, which enables the long-range communication link.</p> <p>LoRa® is the physical layer or the wireless modulation utilized to create the long-range communication link. It uses chirp spread spectrum modulation, which has low power characteristics, long communication range and robustness to interferences. A single LoRa® gateway or base station can cover entire cities or hundreds of square kilometers, even if the range highly depends on the environment or obstructions in a given location.</p> <p>LoRaWAN networks typically are laid out in a star-of-stars topology in which gateways relay messages between end-devices and a central network server at the backend. Gateways are connected to the network server via standard IP connections while end-devices use single-hop LoRa™ or FSK communication to one or many gateways. All communication is generally bi-directional, although uplink communication from an end-device to the network server is expected to be the predominant traffic.</p>  <p>The nodes in a LoRaWAN™ network are asynchronous and communicate when they have data ready to send whether event-driven or scheduled. LoRaWAN™ utilizes two layers of security: one for the network and one for the application. The network security ensures authenticity of the node in the network while the application layer of security ensures the network operator does not have access to the end user's application data. AES encryption is used with the key exchange.</p> <p>LoRaWAN™ defines ten channels, eight of which are multi data rate from 250bps to 5.5 kbps, a single high data rate LoRa® channel at 11kbps, and a single FSK channel at 50kbps. The maximum output power allowed by ETSI in Europe is +14dBm, except for the G3 band which allows +27dBm. There are duty cycle restrictions under ETSI but no max transmission or channel dwell time limitations.</p>
Keyword	Communication and Connectivity; Infrastructure; Devices and sensor technology; Security and Privacy
Autopilot Area involved	IoT eco-system
Use in the Project	LoRaWAN offers multi-year battery lifetime and is designed for sensors and

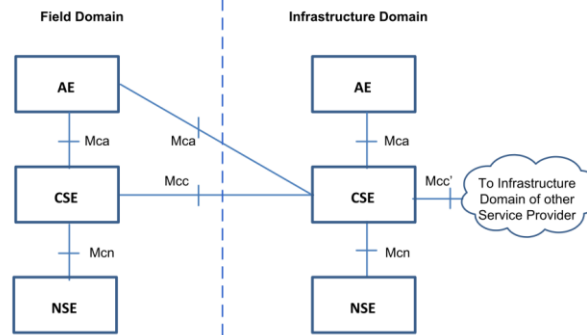
	applications that need to send small amounts of data over long distances a few times per hour from varying environments. In AUTOPILOT, LoRaWAN might be considered as a possible communication protocol, supported by IoT platform, for applications like parking lots monitoring.
Author /Company	Enrico Ferrera / ISMB

3.1.20 OneM2M

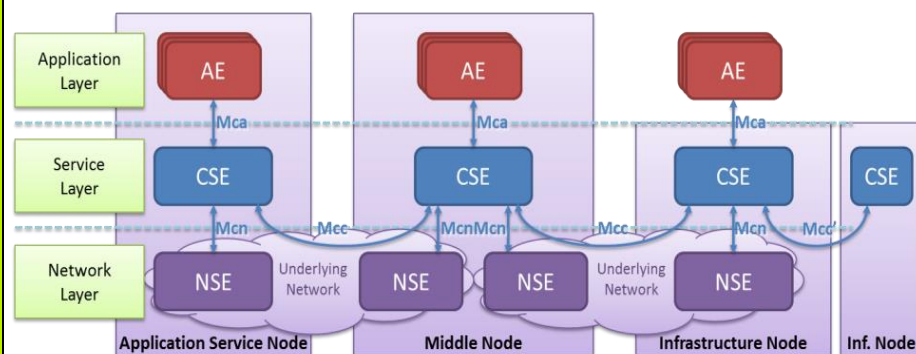
Standardization body	OneM2M
Standard No.	<p>This is the subset of oneM2M specifications potentially relevant For AUTOPILOT:</p> <p>General requirements and architecture</p> <ul style="list-style-type: none"> • TS-0011 Common Terminology • TS-0002 Requirements • TS-0001 Functional Architecture • TS-0003 Security Solutions <p>Management</p> <ul style="list-style-type: none"> • TS-0005 Management Enablement (OMA) • TS-0006 Management Enablement (BBF) • TS-0014 LWM2M Interworking <p>Semantic, general and specic interworking</p> <ul style="list-style-type: none"> • TS-0012 oneM2M Base Ontology • <i>TS-0030 Generic Interworking</i> • TS 0021 oneM2M and AllJoyn® Interworking • TS 0124 oneM2M and OIC Interworking • TS 0023 Home Appliances Information Model and Mapping <p>API transport protocols and bindings:</p> <ul style="list-style-type: none"> • TS-0004 Service Layer Core Protocol • TS-0008 CoAP Protocol Binding • TS-0009 HTTPProtocol Binding • TS-0010 MQTT Protocol Binding • TS-0020 WebSocket Protocol Binding <p>Testing</p> <ul style="list-style-type: none"> • TS-0013 Interoperability Testing • <i>TS-0015 Testing Framework</i> • <i>TS-0017 Implementation Conformance Statements</i> • <i>TS-0018 Test Suite Structure & Test Purposes</i> • <i>TS-0019 Abstract Test Suite & Implementation eXtra information for Test</i> <p>Other documents relevant for AUTOPILOT:</p> <ul style="list-style-type: none"> • <i>oneM2M TR 0026 Vehicular Domain Enablement</i> <p>Please note that these specifications are also transposed into ETSI specifications with no modifications.</p>

Standard Title	See above
URL	<p>Website http://www.onem2m.org/ http://www.onem2m.org/technical/latest-drafts http://www.onem2m.org/technical/published-documents Portal: restricted to members: http://member.onem2m.org/website/homepage.aspx</p> <p>All oneM2M draft specifications , temporary documents and contributions are freely accessible at ftp.oneM2M.org</p>
Country	<p>Worldwide, with about more than 230 organizations involved. oneM2M is not a standard body, it is a partnership project cooperation among ETSI, ARIB, ATIS, CCSA, TIA, TSDSI, TTA, TTC, BBF, OMA, CEN, CENELEC, Global Platform, New generation M2M consortium</p>
Status	<p>Published middle 2016 as release 2. Release 3 expected 1Q 2018 Documents above in <i>Italic</i> are still to be published as release 3, see last stable draft version on the website or ftp site.</p> <p>Release 2 does not support all requirements needed for Autonomous driving (missing timing and reliable delivery requirements). Release 3 in considering some of the requirements, Autopilot may consider contribution to oneM2M to assure that all those elements will be included in Release 3 or future releases.</p>
Date	2012 - ongoing
Aim	<p>oneM2M scope is to develop and maintain a full set of specifications. The necessary set of Technical Specifications and Technical Reports for an IoT service layer capable of acting as a full interworking framework with past and future IoT/M2M solutions.</p> <p>The goal is not only to allow the sharing of data via a communication framework, but also to enable the mutual understanding of the information via semantic interworking/interoperability. It also provides storage capability by historization of the data It includes:</p> <ul style="list-style-type: none"> • Use cases and requirements • Service Layer aspects with high level and detailed service architecture, • Protocols/APIs/information models • semantic and ontology standardization • data management • Identification, Security and privacy aspects • Dynamic access control to the information • Reachability and discovery of applications • Interoperability • Test and conformance specifications; These tests will be used also for the oneM2M certification activity.

	<ul style="list-style-type: none"> • Management aspects (including remote management of entities) <p>oneM2M is not chartered to focus on a particular vertical industry. It provides a standardized common service layer that is applicable to various industry domains including the cross domain interactions, i.e. horizontal industry.</p> <p>However, it also investigates some selected vertical industries (e.g. home, industrial, and vehicle) in deep to ensure that the provided standard/technology can fulfill the vertical requirements and interwork with the applications/network/devices in those industries. More industries may be investigated in the future.</p>
Description	<p>oneM2M was launched in 2012 as a global initiative to ensure the most efficient deployment of Machine-to-Machine (M2M) communications systems and the Internet of Things (IoT), as globalization of the principles and the solutions developed in ETSI M2M specifications.</p> <p>Into the following figure it is presented the organization and structure of oneM2M, the activities are organized into six working group:</p> <ul style="list-style-type: none"> • REQ on use cases and requirements identifies and documents use cases and service and system requirements • ARC develops and specifies an architecture for an M2M system • PRO develops and specifies APIs, protocols and message formats used across oneM2M interfaces, including mapping to commonly used M2M protocols • SEC has the overall responsibility for all technical aspects related to security and privacy within oneM2M • MAS on Management, Abstraction and Semantics deals with the technical aspects related to management of M2M entities and/or functions. It also deals with support for application specific abstraction and semantics • TST identifies and defines test requirements for the oneM2M system and the services related to it. It also develops and maintains a set of specifications for conformance and interoperability testing  <p>The oneM2M functional architecture, detailed in TS 001, can be summarized as follows.</p>



The oneM2M Layered Model for supporting end-to-end (E2E) M2M Services comprises three layers: **Application Layer**, **Common Services Layer** and the underlying **Network Services Layer**.



The common service layer is composed of a set of common service functions providing services to the AEs via the Mca reference point and to other Common Services Entity (CSEs) via the Mcc reference point. CSEs interact with the Network Service Entity (NSE) via the Mcn reference point. An instantiation of a CSE in a Node comprises a subset of the CSFs from the CSFs described in the TS-001.

TS 0012 and TS 0030 complete the architectural interworking framework providing semantic interoperability support.

The security aspects (specified in TS 004) are including:

- Security Integration in oneM2M flow of events
- Security Service Layer:
 - Access Management
 - Authorization Architecture
 - Security Administration
 - Identity Protection
 - Sensitive Data Handling
 - Trust Enabler security functions
- Secure Environment Abstraction Layer Components
- Authorization
- Security Framework
- Security Framework Procedures and Parameters
- Protocol and Algorithm details
- Privacy Protection Architecture using Privacy Policy Manager (PPM)

- Security-Specific oneM2M Data Type Definitions

Security Layer is located between M2M applications and communication HW/SW that provides data transport. It provides the functions that M2M applications across different industry segments commonly need.

For the management support (TS-0005, TS-0006, TS-0014) oneM2M adopts OMA DM (1.x/ 2.0), OMA LWM2M, BBF TR-069 as the alternative device management protocols in the case of reusing underlying network services over oneM2M Mcn reference point.

The protocols and binding specifications are covering how the Mca or Mcc request and response messages are transported (TS-0004, TS-0008, TS-0009, TS-0010)

It maps the primitive used by Reference Point of M2M architecture, on transport layer protocols. Other one is available like HTTP and CoAP. The primitives are independent from the transport Protocols. The protocols are the following:

- CoAP Protocol Binding TS-008
- HTTP Protocol Binding TS-009
- MQTT Protocol Binding TS-010
- WebSocket Protocol Binding TS-0020

Particular attention of AUTOPILOT should be given to the ongoing development of TR 0026: vehicular domain enablement. The Technical Report describes technology trends in the Vehicular Domain and lists organizations and standards related to this field.

15 use cases are included:

- Vehicular Diagnostic & Maintenance Report
- Use Case on Remote Maintenance Services
- Traffic Accident Information Collection
- Fleet Management Service using DTG (Digital Tachograph)
- Use cases for Electronic Toll Collection (ETC) service
- Use cases for Taxi Advertisement
- Use Case on Vehicle Data Service
- Smart Automatic Driving
- Use Case on Vehicle Data Wipe Service
- Vehicle Management based on Geo-Fence
- Use Case on Secure Over-The-Air Firmware Update for Automotive ECUs
- Car/Bicycle Sharing Services
- Smart Parking
- Vehicle Broadcasting without Registration
- Vehicle location privacy protection

defining their potential requirements and providing some examples of potential deployment of the oneM2M architecture mapping for these use cases.

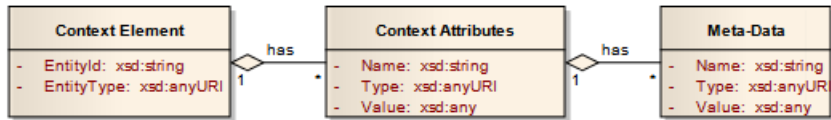
For more details about these standards see Annex B – Standards and Specifications – Section 6.2.10

Keyword	<p>IoT Interworking framework, Information sharing, semantic interoperability, Interoperability, IoT Architecture, Applications, Devices, Security and Privacy, common services layer, Security, Security design and +implementation analysis, Identification, Identity Management, Authentication; Authorization, Access Control, CoAP, MQTT, HTTP, websocket</p> <p>Conformance, Testing.</p>
Autopilot Area involved	<p>Communication network, Vehicle IoT Integration and platform, IoT eco-system, IoT Platform</p>
Use in the Project	<p>It can be used in AUTOPILOT WP1, WP2, WP3 and WP5.</p> <p>The identified standards can be used in AUTOPILOT for architectural, data sharing, interoperability (including semantic interoperability), security and testing aspects.</p> <p>Can contribute into the requirements definition and into the development phase.</p> <p>The oneM2M security architecture could be used as guideline in the AUTOPILOT architecture design phase, with particular reference to the WP1.2, IOT architecture and specification, and WP1.5 Security, Privacy and Data Specification.</p> <p>Furthermore, the availability of a testing frameworks such as the oneM2M one makes it easier for AUTOPILOT to define the tests on the communication framework in particular on the security aspects.</p> <p>Note that there is large number of IoT platforms, making integration challenging. oneM2M is supported by major standardization bodies (ETSI, ARIB, TTA, ...) and therefore oneM2M would provide a good basis for AUTOPILOT. Heterogeneity in available IoT platforms,</p> <p>This would be in the scope of AUTOPILOT federative principle, having cooperation of IoT platforms via standardized interfaces, typically via REST API.</p> <p>oneM2M architecture, data models, and supported protocols are essential to enable standardized IoT data exchanges. While missing time critical elements that may come in release 3, currently published release 2 can support near-real time IoT data exchanges, and can be therefore be used for ‘tactical’ autonomous driving. Examples of tactical AD are platoon management, road status information (traffic jams, ice on road, etc.) , traffic lights information.</p> <p>oneM2M has been designed for information and data sharing, providing a framework for achieving application interoperability via semantic interoperability and communication technology interworking and is therefore a good candidate to be used in AUTOPILOT.</p> <p>oneM2M is probably the only Standard “de Jure” designed to make different</p>

	<p>IoT industrial solutions proprietary and vertical solution to talk to each other. OneM2M also leverages the existing systems, exploiting the network connectivity features to the application layer, and paying attention to the device configuration and the network services offered by the integrated fixed and mobile solutions.</p> <p>Another key element in oneM2M is the security including flexible, dynamic security and authorization. This has been included to relief the burden of manual configuration data access privacy and the setting of security credentials. In oneM2M security is a standards-based tool-box where one can mix and match the security tools according to the use case needs. Security is a cost, and it is necessary to properly satisfy the requirements of the different services in a cost effective manner.</p> <p>IoT is not a simple system: IoT is about applications, system integration and device proliferation. This requires the capacity to integrate different objects from different business domains in a single framework. Semantic interoperability provides a very elegant manner to solve these integration problems. It is not about exchanging data, it is about sharing information.</p>
Author /Company	EGM HUAWEI NEC TIM THALES TNO

3.1.21 OMA

Standardization body	OMA
Standard No.	OMA-TS-NGSI_Context_Management-V1_0-20120529-A
Standard Title	OMA Next Generation Service Interface – Context Management
URL	http://openmobilealliance.org/release/NGSI/V1_0-20120529-A/OMA-TS-NGSI_Context_Management-V1_0-20120529-A.pdf
Country	International
Status	Published
Date	29.05.2012
Aim	The aim of OMA Context Management is to provide standardized interfaces for accessing and managing context information, supporting different architectures, e.g. centralized, distributed, federated etc.

Description	<p>The NGSI-9: Context Entity Discovery Interface enables the registration and discovery of sources of context information, enabling the support in a distributed system.</p> <p>The NGSI-10: Context Information Interface enables the update and retrieval of the context information itself.</p> <p>The Context Information Model details how Context Information is structured and associated to Context Entities in order to describe their situation. In this model, Context Information is organized as Context Elements, which contain set of Context Attributes and associated metadata.</p>  <p>The structure of the Context Information Model is used in the interface to specify the context information of interest to an application.</p>
Keyword	Integration /Interoperability, IoT Architecture, Context Information, FIWARE
Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform
Use in the Project	The interfaces defined in OMA NGSI Context Management have been used as the basis for developing the IoT-related generic enablers in the FIWARE platform (page 54), which is going to be used as part of the IoT Platform in AUTOPILOT. The NGSI interfaces are being used as the starting point in the ETSI ISG CIM (page 34), which is likely to be taken up in the evolution of the FIWARE generic enablers.
Author /Company	NEC

3.1.22 OSGi Alliance

Standardization body	The OSGi Alliance
Standard No.	Various
Standard Title	See above
URL	http://www.osgi.org/
Country	International,
Status	Published, Release 6, Ongoing Release 7 to be completed in 2017. Currently working on the first IoT release, to be published on 2018.
Date	2016 - Ongoing

Aim	The OSGi specifications provide a standardized service platform for interacting with services (both local and remote) using a variety of defined communication and messaging protocols, including UPnP, TR069, enOcean, OMA DM, HTTP/REST, JSON-RPC and many others built by the community.
Description	<p>The OSGi Alliance is a worldwide consortium advancing a proven and mature process to create open specifications. These specifications enable dynamic end-to-end connectivity and facilitate the componentization of software and applications, thus increasing development productivity, reducing time to market and substantially decreasing the long term maintainability costs of the resulting modular solution. The technology also provides flexible remote management and interoperability for applications and services over a broad variety of devices. Member company industries include leading service and content providers, infrastructure/network operators, utilities, enterprise software vendors, software developers, gateway suppliers, consumer electronics/device suppliers (wired and wireless) and research institutions. Features: high level functionalities covered by the initiative</p> <p>OSGi inherently responds to many requirements of the IoT. Its most important features can be listed as:</p> <ul style="list-style-type: none"> • A Modular execution environment enabling functional reuse of components across diverse platforms. • A flexible Capabilities / Requirements model that enables environment-aware deployment and dependency management. • A dynamic environment allowing system components to be updated and/or reconfigured without restarting them. • Lifecycle aware components that are able to respond to changes in their environment, for example the addition/activation of a hardware device. • Support for dynamic deployment of native libraries based on the discovered system capabilities. • A defined security model for determining whether software modules are trusted and the actions they are permitted to perform. • Common API's for device connectivity using various underlying communication protocols. • A standardized common remote management interface using a variety of protocols including JMX and HTTP/REST. • Programming models for distributed environments using synchronous or asynchronous invocations. Suitable for use in edge or cloud environments. <p>OSGi Alliance provides a horizontal platform with API's and device abstraction for specific vertical markets; it also provides specifications for enterprise solutions (app servers; cloud product solutions) and a framework for modular web application development.</p> <p><u>Communication and Connectivity knowledge area:</u> Gateway based architecture, interconnection of devices and the cloud.</p> <p><u>Integration/Interoperability knowledge area::</u> OSGi Alliance provides a device abstraction layer and various APIs for providing common access to external resources (both physical hardware and external services). Framework provides a Java execution environment capable of supporting existing Java applications on small embedded systems, or large server hardware.</p>

	<p><u>Applications knowledge area:</u></p> <p>OSGi Alliance provides a dynamic lifecycle management layer and standardized API that allows users to remotely install, manage, configure and update software components.</p> <p>The OSGi Alliance provides enRoute, a framework for modular development of web applications using OSGi best practices.</p> <p>Numerous tools for dependency management and resource access exist</p> <p>Configuration is able to be pushed to OSGi modules via a common interface, independent of how the configuration is stored.</p> <p><u>Infrastructure knowledge area:</u> OSGi Alliance provides specifications for large-scale enterprise deployments, embedded systems, and edge devices.</p> <p><u>Devices and sensor technology knowledge area:</u></p> <ul style="list-style-type: none"> ○ The OSGi specifications provide dynamic lifecycle management for modules and services, meaning that devices sensors can be dynamically added, removed, discovered, or updated within a running system. ○ Dynamic configuration management is provided for application and infrastructure modules allowing them to be updated without restarting the system. ○ A wide variety of operating platforms are supported. The core requirement is for a Java Virtual Machine implementation. <p><u>Security and Privacy knowledge area:</u></p> <ul style="list-style-type: none"> ● The OSGi specifications include native support for trusted modules, and permission-based access to resources and services. ● Permissions can be dynamically changed at runtime based on configuration.
Keyword	Interoperability, integration, Security, Privacy, Devices and sensor technologies, Infrastructure, Communication and Connectivity
Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform, Communication network, IoT eco-system
Use in the Project	Could be used in AUTOPILOT WP2 and AUTOPILOT WP3 to support IoT Platform, Vehicle IoT Integration and platform, Communication network, IoT eco-system.
Author /Company	HUAWEI

3.1.23 SENSORIS Forum /ERTICO

Standardization body	SENSORIS Forum / ERTICO
Standard No.	
Standard Title	Vehicle Sensor Data Cloud Ingestion Interface Specification
URL	https://its.cms.here.com/static-cloud-

	content/Company_Site/2015_06/Vehicle_Sensor_Data_Cloud_Ingestion_Interface_Specification.pdf
Country	Europe / Worldwide
Status	V2.0.2 licensed by HERE released in 2015, future standardized release under planning for 2017
Date	11.04.2017
Aim	Standardize the data interface of Vehicle sensor for Cloud ingestion.
Description	<p>SENSORIS initiative was initiated by HERE in June 2015 when the company published the first open specification for how vehicle sensor data gathered by connected cars could be sent to the cloud for processing and analysis. ERTICO brings it now into a standardized interface specification with the implication of automotive industry company for a de facto and reliable worldwide standard. The Specifications are defined in relation to Open Auto Drive Forum (OADF) as the cross-domain platform driving standardizations in the area of autonomous driving.</p> <p>The objective is to define a detailed specification with encoding format of data message for sensor interface to be submitted to the analytic processing backend platform.</p> <p>The SENSORIS specification defines data messages with standardized data elements and formats. Each sensor data submission is a Message. A Message has an Envelope, a Path, and optionally (but likely) Path Events. The data messages are timestamp by UTC time ordered in Path and Path events information. The Envelope describes information about the vehicle that is valid for the entire path, as vehicle type information, the vehicle specific meta data The Path describes the logical data type containing one or more position estimates of the vehicle. A position estimate coordinates of the estimated position and is defined by longitude, latitude, speed, lane, etc. Path event describes information of notification about vehicle events that vehicle detect from raw sensor data. The information can be vehicle status (transmission mode, light status...), vehicle dynamics (curvature, slop, etc.), sign recognition (speed limit, etc.), lane boundary detection, exceptional vehicle state (slippage, crash detection, etc...), proprietary information, environment status (light condition, temperature, etc.), object detection (detected object, position, moving vector, etc.), Automated driving service and sensor state (speed control, break control, etc.). Depending of vehicle configuration and electronic performance, the message send policies can be different (event based, synchronous, accumulated. etc.). Messages are encoded using specific serialization mechanisms such as the Protocol Buffers (ProBuf) primary mechanism.</p> <p>According to the AUTOPILOT overall concept, the “ADAS Horizon” matches to the definition Data fusion block with communication interface from Local Dynamic Map and vehicle sensor blocks, whereas environment reconstruction mandatory for autonomous vehicle is included in Autonomous driving function.</p>
Keyword	Cloud, Interface, Sensor data, IoT format

Autopilot Area involved	IoT and cloud based service platforms
Use in the Project	Interface between the vehicle IoT platform, block Vehicle IoT enabled platform, and the IoT Cloud based service platform
Author /Company	CONTINENTAL

3.2 By Autopilot area of interest

This section presents the collected standards according to different groupings in order to facilitate their use in the AUTOPILOT project activities.

The mapping of the organizations, standards and specification documents is presented following the AUTOPILOT areas of interest:

- IoT Platform,
- Vehicle IoT Integration and platform,
- Communication network,
- IoT eco-system.

Furthermore the term "All areas" is applied to group the organizations and related documents that address all the areas of interest of the AUTOPILOT project.

3.2.1 All areas

Organization	Number	Title
3GPP	N/A	3GPP Standards: Lte, Lte Adv, Lte Adv Pro, 5G, VTx (V, I, P), Nb-IoT, eMTC
3GPP	3GPP - Release 14	Technical Specification Group Radio Access Network; Study on LTE-based V2X Services
3GPP	3GPP TS 33.185 V1.0.0	Security aspect for LTE support of V2X services (release 14)
5GAA	N/A	Various specs: WG1 (Use Cases and Tech Req); WG2 (System Architecture); WG3 (Evaluations, Testbeds and Pilots); WG4 (Standards, Policy, Certification and Regulatory); WG5 (Business Models)
AIOTI		Various WG03 (IoT Standards) and WG09 (Smart Mobility) Recommendations and Guidelines
BBF	TR-069 and USP	TR-069 CPE WAN Management Protocol (CWMP) and Universal Service Platform (USP)
ETSI (TC ITS)	TS 103 191, TS 103 096, TS 102 869, TS 102 868, TS 102 871, TS 102 870, TS 102 859	ITS Testing, Conformance test specifications for: Signal Phase And Timing (SPAT) and Map (MAP) ITS Security Decentralized Environmental Notification Basic Service (DEN) Cooperative Awareness Basic Service (CA) GeoNetworking ITS-G5 Geonetworking Basic Transport Protocol (BTP) Transmission of IP packets over GeoNetworking
ETSI (TC Cyber Security)	TR 103 303 V1.1.1	CYBER; Protection measures for ICT in the context of Critical Infrastructure

Organization	Number	Title
ETSI (TC Cyber Security)	TR 103 304 V1.1.1	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services
ISA/IEC	ISA/IEC-62443	Security for industrial automation and control systems
IETF	Various (www.ietf.org)	Specifications published by several WGs: 6lo (IPv6 over Networks of Resource-constrained Nodes), 6TiSCH (IPv6 over the TSCH mode of IEEE 802.15.4e), detnet (Deterministic Networking), lpwan (Low Power WAN), IPWAVE (), ACE (Authentication and Authorization for Constrained Environments), CORE (Constrained RESTful Environments) WG, COSE (CBOR Encoded Message Syntax), CBOR (Concise Binary Object Representation), Dice (DTLS In Constrained Environments)
IRTF	Various (www.irtf.org)	Specifications published by T2T RG (Thing to Thing Research Group) The T2T RG will investigate open research issues in turning a true “Internet of Things” into reality, and on an Internet where low-resource nodes
ISO TC204 WG14	ISO/CD 20035 C-ACC	Cooperative Adaptive Cruise Control - Performance requirements and test procedures
ISO TC204 WG14	ISO/AWI 20900 PAPS	Partially automated parking systems
ISO TC204 WG14	New topic	New Topic (Automated Valet Parking System)
ISO/IEC	27000:2016	Information technology Security techniques Information security management systems Overview and vocabulary
ISO/IEC	27001	Information technology Security techniques Information security management systems Requirements
ISO/IEC	27002	Information technology Security techniques Code of practice for information security controls
oneM2M	TS-0011 TS-0002 TS-0001 TS-0003 TS-0005 TS-0006 TS-0014 TS-0012 TS-0030 TS 0021 TS 0124 TS 0023 TS-0004 TS-0008 TS-0009 TS-0010 TS-0020 TS-0013 TS-0015 TS-0017	Common Terminology Requirements Functional Architecture Security Solutions Management Enablement (OMA) Management Enablement (BBF) LWM2M Interworking oneM2M Base Ontology Generic Interworking oneM2M and AllJoyn® Interworking oneM2M and OIC Interworking Home Appliances Information Model and API transport protocols and bindings: Service Layer Core ProtocolCoAP Protocol Binding HTTPProtocol Binding MQTT Protocol Binding WebSocket Protocol Binding Interoperability Testing Testing Framework Implementation Conformance Statements Test Suite Structure & Test Purposes

Organization	Number	Title
	TS-0018 TS-0019	Abstract Test Suite & Implementation eXtra information for Test
OSGi	Various	The OSGi Alliance specifications provide a standardized service platform for interacting with services (both local and remote) using a variety of defined communication and messaging protocols, including UPnP, TR069, enOcean, OMA DM, HTTP/REST, JSON-RPC and many others built by the community

3.2.2 IoT Platform and architecture

Organization	Number	Title
3GPP	3GPP - Release 13	Narrowband Internet of Things (NB-IoT)
ETSI (TC ITS)	TS 102 940	Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management
ETSI ISG CIM	Being developed	Being developed : technical specifications to enable multiple organizations to develop interoperable software implementations of a cross-cutting Context Information Management (CIM) Layer. It is about bridging the gap between abstract standards and concrete implementations.
FI-PPP/FIWARE Foundation	FIWARE	- IoT Broker GE Specification: - IoT Discovery GE Specification: - Context Broker GE Specification:
IEEE SA	802.15.1-2005 802.15.4-2015	Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 15.1a: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPAN). Standard for Low-Rate Wireless Networks.
IETF	RFC 4944	Transmission of IPv6 Packets over IEEE 802.15.4 Networks
ISO/IEC	15408-1	Information Technology – Security Techniques – Evaluation criteria for IT security – Information and General Model
ISO/IEC	15408-2	Information Technology – Security Techniques – Evaluation criteria for IT security – Security Functional Components
ISO/IEC	15408-3	Information Technology – Security Techniques – Evaluation criteria for IT security – Security Assurance Components
oneM2M	TS-0011 TS-0002 TS-0001 TS-0003 TS-0005 TS-0006 TS-0012 TS-0030 TS-0013 TS-0015 TS-0017 TS-0018 TS-0019	Common Terminology Requirements Functional Architecture Security Solutions Management Enablement (OMA) Management Enablement (BBF) oneM2M Base Ontology Generic Interworking Interoperability Testing Testing Framework Implementation Conformance Statements Test Suite Structure & Test Purposes Abstract Test Suite & Implementation eXtra information for Test
OMA	OMA-TS-	OMA Next Generation Service Interface – Context

Organization	Number	Title
	NGSI_Context_Management-V1_0-20120529-A	Management

3.2.3 Vehicle IoT Integration and platform

Organization	Number	Title
ADASIS forum / ERTICO		ADASIS Protocol
Bluetooth	Bluetooth 5.0	Bluetooth Core Specification, version 5.0
CEN TC278	Various – WG15 - WG6	Intelligent Transport System - eSafety / eCall Co-operative systems
ETSI (TC ITS)	EN 302 637-3 V1.2.2	DENM
ETSI (TC ITS)	EN 302 637-2 V1.3.2	CAM
ETSI (TC ITS)	EN 302 895 V1.1.1	LDM
ETSI (TC ITS WG1)	TS 102 894-1 V1.1.1	SPAT/MAP
ETSI (TC ITS)	EG 202 798	Intelligent Transport Systems (ITS) Testing; Framework for conformance and interoperability testing
ETSI (TC ITS)	EN 302 665	Intelligent Transport Systems (ITS); Communications Architecture of ITS stations
ETSI (TC ITS)	EN 302 636-1 EN 302 636-2 EN 302 636-3 EN 302 636-4-1 V1.2.1 (2014-07) EN 302 636-5-1 V1.2.1 (2014-08) EN 302 636-6-1 V1.2.1 (2014-05)	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements GeoNetworking; Part 2: Scenarios GeoNetworking; Part 3: Network Architecture 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 GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols
FI-PPP/FIWARE Foundation	FIWARE	- IoT Broker GE Specification: - IoT Discovery GE Specification: - Context Broker GE Specification:
IEEE SA	802.11p-2010	Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments
IEEE SA	802.15.1-2005	Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 15.1a: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPAN).

Organization	Number	Title
	802.15.4-2015	Standard for Low-Rate Wireless Networks.
IEEE SA	802.20-2008:	Standard for Local and metropolitan area networks - Part 20: Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility - Physical and Media Access Control Layer Specification.
	802.20.2-2010	Standard for Conformance to IEEE 802.20 Systems--Protocol Implementation Conformance Statement (PICS) Proforma.
	802.20.3-2010	Standard for Minimum Performance Characteristics of IEEE 802.20 Terminals and Base Stations/Access Nodes.
	IEEE 802.20a-2010	Standard for Local and metropolitan area networks--Part 20: Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility--Physical and Media Access Control Layer Specification Amendment 1: Management Information Base Enhancements and Corrigenda Items.
	802.20b-2010	Standard for Local and metropolitan area networks--Virtual Bridged Local Area Networks - Amendment 15: Bridging of IEEE 802.20.
IEEE	1609.0	1609.0 IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture
	1609.2	1609.2 IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages
	1609.3	1609.3 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services
	1609.4	1609.4 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation
	1609.11	1609.11 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)-- Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS)
	1609.12	1609.12 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Identifier Allocations
IETF	RFC 4944	Transmission of IPv6 Packets over IEEE 802.15.4 Networks
ISO	Various TC 204	Cover overall system aspects and infrastructure aspects of intelligent transport systems (ITS)
ISO	ISO/AWI 20900 PAPS	Partially automated parking systems
ISO	New Topic	Automated Valet Parking System
ISO (TC 22/SC31)	15118-1:2013	Road vehicles -- Vehicle to grid communication interface -- Part 1: General information and use-case definition.
	15118-2:2014	Road vehicles -- Vehicle-to-Grid Communication Interface -- Part 2: Network and application protocol requirements.
	15118-3:2015.	Road vehicles -- Vehicle to grid communication interface -- Part 3: Physical and data link layer requirements.
ISO (TC204 WG14)	ISO/CD 20035 C-ACC res	Cooperative Adaptive Cruise Control - Performance requirements and test procedure
ISO/IEC	18092:2013	Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1)
ISO/IEC	21481:2012	Information technology -- Telecommunications and information exchange between systems -- Near Field Communication Interface and Protocol -2 (NFCIP-2)

Organization	Number	Title
oneM2M	TS-0011 TS-0002 TS-0001 TS-0003 TS-0005 TS-0006 TS-0012 TS-0030 TS-0013 TS-0015 TS-0017 TS-0018 TS-0019 TR-0026	Common Terminology Requirements Functional Architecture Security Solutions Management Enablement (OMA) Management Enablement (BBF) oneM2M Base Ontology Generic Interworking Interoperability Testing Testing Framework Implementation Conformance Statements Test Suite Structure & Test Purposes Abstract Test Suite & Implementation eXtra information for Test Vehicular Domain Enablement
OMA	OMA-TS- NGSI_Context_Management-V1_0- 20120529-A	OMA Next Generation Service Interface – Context Management
SENSORIS Forum / ERTICO		Vehicle Sensor Data Cloud Ingestion Interface Specification

3.2.4 Communication network

Organization	Number	Title
3GPP	3GPP - Release 13	Narrowband Internet of Things (NB-IoT)
Bluetooth	Bluetooth 5.0	Bluetooth Core Specification, version 5.0
CEN TC278	Various – WG15 - WG6	Intelligent Transport System - eSafety / eCall Co-operative systems
ETSI (TC ITS)	various	ETSI TC ITS
ETSI (TC ITS)	EN 302 637-3 V1.2.2	DENM
ETSI (TC ITS)	EN 302 637-2 V1.3.2	CAM
ETSI (TC ITS)	EN 302 895 V1.1.1	LDM
ETSI (TC ITS WG1)	TS 102 894-1 V1.1.1	SPAT/MAP
ETSI (TC ITS)	TS 102 940	Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management
ETSI	various	ETSI TC ITS concentrates on a subset of the ITS scope with the current focus being on <ul style="list-style-type: none"> • 5.9 GHz communications called ITS-G5 in ETSI terminology, • applying a special multi-hopping network function called GeoNet, and • serving a small number of mainly safety applications for vehicle-to-vehicle and vehicle-to-roadside scenarios. This vehicle-safety-centric scenario is supported by strong security provisions.
ETSI (TC ITS)	EN 302 665	Intelligent Transport Systems (ITS); Communications

Organization	Number	Title
		Architecture of ITS stations
ETSI (TC ITS)	EN 302 636-1 EN 302 636-2 EN 302 636-3 EN 302 636-4-1 V1.2.1 (2014-07) EN 302 636-5-1 V1.2.1 (2014-08) EN 302 636-6-1 V1.2.1 (2014-05)	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements GeoNetworking; Part 2: Scenarios GeoNetworking; Part 3: Network Architecture 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 GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols
ETSI (TC ITS)	TS 101 556-2	Intelligent Transport Systems (ITS); Infrastructure to Vehicle Communication; Part 2: Communication system specification to support application requirements for Tyre Information System (TIS) and Tyre Pressure Gauge (TPG) interoperability
ETSI (TC ITS)	TS 102 723-8	Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 8: Interface between security entity and network and transport layer
ETSI (TC ERM)	EN 300 674-2-2	TTT - Dedicated Short Range Communication (DSRC)-Harmonized standard - On-Board Units (OBU)
ETSI (TC ERM)	EN 300 674-2-1	TTT - Dedicated Short Range Communication (DSRC)-Harmonized standard - Road Side Units (RSU)
ETSI (TC ERM)	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
IEEE SA	802.11p-2010	Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments
IEEE SA	802.20-2008: 802.20.2-2010 802.20.3-2010 802.20a-2010	Standard for Local and metropolitan area networks - Part 20: Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility - Physical and Media Access Control Layer Specification. Standard for Conformance to IEEE 802.20 Systems-- Protocol Implementation Conformance Statement (PICS) Proforma. Standard for Minimum Performance Characteristics of IEEE 802.20 Terminals and Base Stations/Access Nodes. Standard for Local and metropolitan area networks--Part 20: Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility--Physical and Media Access Control Layer Specification Amendment 1: Management Information Base Enhancements and

Organization	Number	Title
	802.20b-2010	Corrigenda Items. Standard for Local and metropolitan area networks--Virtual Bridged Local Area Networks - Amendment 15: Bridging of IEEE 802.20.
IEEE	1609.0	1609.0 IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture
	1609.2	1609.2 IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages
	1609.3	1609.3 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services
	1609.4	1609.4 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation
	1609.11	1609.11 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)-- Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS)
	1609.12	1609.12 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Identifier Allocations
ISO	Various TC 204	Cover overall system aspects and infrastructure aspects of intelligent transport systems (ITS)
ISO (TC22/SC31)	15118-1:2013	Road vehicles -- Vehicle to grid communication interface -- Part 1: General information and use-case definition.
	15118-2:2014	Road vehicles -- Vehicle-to-Grid Communication Interface -- Part 2: Network and application protocol requirements.
	15118-3:2015.	Road vehicles -- Vehicle to grid communication interface -- Part 3: Physical and data link layer requirements.
oneM2M	TS-0001	Functional Architecture
	TS-0003	Security Solutions
	TS-0004	Service Layer Core Protocol
	TS-0008	CoAP Protocol Binding
	TS-0009	HTTPProtocol Binding
	TS-0010	MQTT Protocol Binding
	TS-0020	WebSocket Protocol Binding

3.2.5 IoT Eco-system

Organization	Number	Title
3GPP	3GPP - Release 13	Narrowband Internet of Things (NB-IoT)
ETSI (TC ITS WG1)	TS 102 894-1 V1.1.1	SPAT/MAP
IETF	RFC 4944	Transmission of IPv6 Packets over IEEE 802.15.4 Networks
IEEE SA	802.15.1-2005	Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 15.1a: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPAN).
	802.15.4-2015	Standard for Low-Rate Wireless Networks.
ISO (TC 22/SC31)	15118-1:2013	Road vehicles -- Vehicle to grid communication interface -- Part 1: General information and use-case definition.
	15118-2:2014	Road vehicles -- Vehicle-to-Grid Communication Interface -- Part 2: Network and application protocol requirements.
	15118-3:2015.	Road vehicles -- Vehicle to grid communication interface -- Part 3: Physical and data link layer requirements.

Organization	Number	Title
LoRaWAN	201R0	LoRaWAN™ Specification
oneM2M	TS-0005	Management Enablement (OMA)
	TS-0006	Management Enablement (BBF)
	TS-0014	LWM2M Interworking
	TS-0012	oneM2M Base Ontology
	TS-0030	Generic Interworking
	TS 0021	oneM2M and AllJoyn® Interworking
	TS 0124	oneM2M and OIC Interworking
	TS 0023	Home Appliances Information Model and mapping

3.3 By keywords /knowledge areas

This section presents the collected standards according to different groupings in order to facilitate their use in the AUTOPILOT project activities.

The standard documents and organizations that have been detailed in chapter 3 are summarized on the basis of the following keywords / knowledge areas:

- Communication and Connectivity
- Integration and interoperability
- Applications
- Infrastructure
- IoT Architecture
- Devices and sensor technology
- Security and Privacy
- Conformance, Testing

3.3.1 Communication and Connectivity

Organization	Number	Title
3GPP	N/A	3GPP standards: Lte, Lte Adv, Lte Adv Pro, 5G, VTx (V, I, P), Nb-IoT, eMTC
3GPP	3GPP - Release 13	Narrowband Internet of Things (NB-IoT)
3GPP	3GPP - Release 14	Technical Specification Group Radio Access Network; Study on LTE-based V2X Services
3GPP	3GPP TS 33.185 V1.0.0	Security aspect for LTE support of V2X services (release 14)
5GAA	N/A	Various specs: WG1 (Use Cases and Tech Req); WG2 (System Architecture); WG3 (Evaluations, Testbeds and Pilots); WG4 (Standards, Policy, Certification and Regulatory); WG5 (Business Models)
AIOTI		Various WG03 (IoT Standards) and WG09 (Smart Mobility) Recommendations and Guidelines
BBF	TR-069 and USP	TR-069 CPE WAN Management Protocol (CWMP) and Universal Service Platform (USP)
Bluetooth	Bluetooth 5.0	Bluetooth Core Specification, version 5.0
CEN TC278	Various – WG15 - WG6	Intelligent Transport System - eSafety / eCall Co-operative systems
ETSI (TC ITS)	various	ETSI TC ITS
ETSI (TC ITS)		Intelligent Transport Systems (ITS); Vehicular Communications;

Organization	Number	Title
	EN 302 636-1 EN 302 636-2 EN 302 636-3	GeoNetworking; Part 1: Requirements GeoNetworking; Part 2: Scenarios GeoNetworking; Part 3: Network Architecture
	EN 302 636-4-1 V1.2.1 (2014-07)	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
	EN 302 636-5-1 V1.2.1 (2014-08)	GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol
	EN 302 636-6-1 V1.2.1 (2014-05)	GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols
ETSI (TC ITS)	EN 302 637-3 V1.2.2	DENM
ETSI (TC ITS)	EN 302 637-2 V1.3.2	CAM
ETSI (TC ITS)	EN 302 665	Intelligent Transport Systems (ITS); Communications Architecture of ITS stations
ETSI (TC ITS)	EN 302 895 V1.1.1	LDM
ETSI (TC ITS)	TS 101 556-2	Intelligent Transport Systems (ITS); Infrastructure to Vehicle Communication; Part 2: Communication system specification to support application requirements for Tyre Information System (TIS) and Tyre Pressure Gauge (TPG) interoperability
ETSI (TC ITS WG1)	TS 102 894-1 V1.1.1	SPAT/MAP
ETSI (TC ITS)	TS 102 723-8	Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 8: Interface between security entity and network and transport layer
ETSI (TC ERM)	EN 300 674-2-2	TTT - Dedicated Short Range Communication (DSRC)-Harmonized standard - On-Board Units (OBU)
ETSI (TC ERM)	EN 300 674-2-1	TTT - Dedicated Short Range Communication (DSRC)-Harmonized standard - Road Side Units (RSU)
ETSI (TC ERM)	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
IEEE SA	802.11p-2010	Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments
IEEE SA	802.15.1-2005 802.15.4-2015	Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 15.1a: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPAN). Standard for Low-Rate Wireless Networks.
IEEE SA	802.15.1-2005	Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 15.1a: Wireless Medium Access Control (MAC) and Physical

Organization	Number	Title
	802.15.4-2015	Layer (PHY) specifications for Wireless Personal Area Networks (WPAN). Standard for Low-Rate Wireless Networks.
IEEE SA	802.20-2008:	Standard for Local and metropolitan area networks - Part 20: Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility - Physical and Media Access Control Layer Specification.
	802.20.2-2010	Standard for Conformance to IEEE 802.20 Systems--Protocol Implementation Conformance Statement (PICS) Proforma.
	802.20.3-2010	Standard for Minimum Performance Characteristics of IEEE 802.20 Terminals and Base Stations/Access Nodes.
	802.20a-2010	Standard for Local and metropolitan area networks--Part 20: Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility--Physical and Media Access Control Layer Specification Amendment 1: Management Information Base Enhancements and Corrigenda Items.
	802.20b-2010	Standard for Local and metropolitan area networks--Virtual Bridged Local Area Networks - Amendment 15: Bridging of IEEE 802.20.
IEEE	1609.0	1609.0 IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture
	1609.2	1609.2 IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages
	1609.3	1609.3 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services
	1609.4	1609.4 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation
	1609.11	1609.11 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)-- Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS)
	1609.12	1609.12 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Identifier Allocations
IETF	RFC 4944	Transmission of IPv6 Packets over IEEE 802.15.4 Networks
IRTF	Various (www.irtf.org)	Specifications published by T2T RG (Thing to Thing Research Group) The T2T RG will investigate open research issues in turning a true "Internet of Things" into reality, and on an Internet where low-resource nodes
ISO	Various TC 204	Cover overall system aspects and infrastructure aspects of intelligent transport systems (ITS)
ISO (TC204 WG14)	ISO/CD 20035 C-ACC res	Cooperative Adaptive Cruise Control - Performance requirements and test procedure
ISO/IEC	18092:2013	Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1)
ISO/IEC	21481:2012	Information technology -- Telecommunications and information exchange between systems -- Near Field Communication Interface and Protocol -2 (NFCIP-2)
LoRaWAN	201R0	LoRaWAN™ Specification
oneM2M	TS-0030 TS-0004	Generic Interworking Service Layer Core Protocol

Organization	Number	Title
	TS-0008 TS-0009 TS-0010 TS-0020	CoAP Protocol Binding HTTPProtocol Binding MQTT Protocol Binding WebSocket Protocol Binding
OSGi	Various	The OSGi Alliance specifications provide a standardized service platform for interacting with services (both local and remote) using a variety of defined communication and messaging protocols, including UPnP, TR069, enOcean, OMA DM, HTTP/REST, JSON-RPC and many others built by the community

3.3.2 Integration and interoperability

Organization	Number	Title
3GPP	N/A	3GPP standards: Lte, Lte Adv, Lte Adv Pro, 5G, VTx (V, I, P), Nb-IoT, eMTC
3GPP	3GPP - Release 13	Narrowband Internet of Things (NB-IoT)
3GPP	3GPP - Release 14	Technical Specification Group Radio Access Network; Study on LTE-based V2X Services
5GAA	N/A	Various specs: WG1 (Use Cases and Tech Req); WG2 (System Architecture); WG3 (Evaluations, Testbeds and Pilots); WG4 (Standards, Policy, Certification and Regulatory); WG5 (Business Models)
ADASIS forum / ERTICO		ADASIS Protocol
AIOTI		Various WG03 (IoT Standards) and WG09 (Smart Mobility) Recommendations and Guidelines
ETSI (TC ITS)	various	ETSI TC ITS
ETSI (TC ITS)	EN 302 637-3 V1.2.2	DENM
ETSI (TC ITS)	EN 302 637-2 V1.3.2	CAM
ETSI (TC ITS)	EN 302 895 V1.1.1	LDM
ETSI (TC ITS WG1)	TS 102 894-1 V1.1.1	SPAT/MAP
ETSI (TC ITS)	TS 102 940	Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management
ETSI (TC ITS)	TS 103 191, TS 103 096, TS 102 869, TS 102 868, TS 102 871, TS 102 870, TS 102 859	ITS Testing, Conformance test specifications for: Signal Phase And Timing (SPAT) and Map (MAP) ITS Security Decentralized Environmental Notification Basic Service (DEN) Cooperative Awareness Basic Service (CA) GeoNetworking ITS-G5 Geonetworking Basic Transport Protocol (BTP) Transmission of IP packets over GeoNetworking
ETSI (TC ITS)	EG 202 798	Intelligent Transport Systems (ITS) Testing; Framework for conformance and interoperability testing
ETSI ISG CIM	Being developed	Being developed : technical specifications to enable multiple organizations to develop interoperable software implementations of a cross-cutting Context Information

Organization	Number	Title
		Management (CIM) Layer. It is about bridging the gap between abstract standards and concrete implementations.
IETF	Various (www.ietf.org)	Specifications published by several WGs: 6lo (IPv6 over Networks of Resource-constrained Nodes), 6TiSCH (IPv6 over the TSCH mode of IEEE 802.15.4e), detnet (Deterministic Networking), lpwan (Low Power WAN), IPWAVE (), ACE (Authentication and Authorization for Constrained Environments), CORE (Constrained RESTful Environments) WG, COSE (CBOR Encoded Message Syntax), CBOR (Concise Binary Object Representation), Dice (DTLS In Constrained Environments)
ISO	Various TC 204	Cover overall system aspects and infrastructure aspects of intelligent transport systems (ITS)
ISO	ISO/AWI 20900 PAPS	Partially automated parking systems
ISO	New Topic	Automated Valet Parking System
ISO (TC 22/SC31)	15118-1:2013 15118-2:2014 15118-3:2015.	Road vehicles -- Vehicle to grid communication interface -- Part 1: General information and use-case definition. Road vehicles -- Vehicle-to-Grid Communication Interface -- Part 2: Network and application protocol requirements. Road vehicles -- Vehicle to grid communication interface -- Part 3: Physical and data link layer requirements.
ISO (TC204 WG14)	ISO/CD 20035 C-ACC res	Cooperative Adaptive Cruise Control - Performance requirements and test procedure
oneM2M	TS-0001 TS-0003 TS-0005 TS-0006 TS-0014 TS-0012 TS-0030 TS 0021 TS 0124 TS 0023 TS-0013 TS-0015	Functional Architecture Security Solutions Management Enablement (OMA) Management Enablement (BBF) LWM2M Interworking oneM2M Base Ontology Generic Interworking oneM2M and AllJoyn® Interworking oneM2M and OIC Interworking Home Appliances Information Model and Interoperability Testing Testing Framework
OMA	OMA-TS-NGSI_Context_Management-V1_0-20120529-A	OMA Next Generation Service Interface – Context Management
OSGi	Various	The OSGi Alliance specifications provide a standardized service platform for interacting with services (both local and remote) using a variety of defined communication and messaging protocols, including UPnP, TR069, enOcean, OMA DM, HTTP/REST, JSON-RPC and many others built by the community

3.3.3 Application

Organization	Number	Title
5GAA	N/A	Various specs: WG1 (Use Cases and Tech Req); WG2 (System Architecture); WG3 (Evaluations, Testbeds and Pilots); WG4 (Standards, Policy, Certification and Regulatory); WG5 (Business Models)
ADASIS forum /		ADASIS Protocol

Organization	Number	Title
ERTICO		
CEN TC278	Various – WG15 - WG6	Intelligent Transport System - eSafety / eCall Co-operative systems
ETSI (TC ITS)	various	ETSI TC ITS
ETSI (TC ITS)	EN 302 637-3 V1.2.2	DENM
ETSI (TC ITS)	EN 302 637-2 V1.3.2	CAM
ETSI (TC ITS)	EN 302 895 V1.1.1	LDM
ETSI (TC ITS WG1)	TS 102 894-1 V1.1.1	SPAT/MAP
IETF	Various (www.ietf.org)	Specifications published by several WGs: 6lo (IPv6 over Networks of Resource-constrained Nodes), 6TiSCH (IPv6 over the TSCH mode of IEEE 802.15.4e), detnet (Deterministic Networking), lpwan (Low Power WAN), IPWAVE (), ACE (Authentication and Authorization for Constrained Environments), CORE (Constrained RESTful Environments) WG, COSE (CBOR Encoded Message Syntax), CBOR (Concise Binary Object Representation), Dice (DTLS In Constrained Environments)
IRTF	Various (www.irtf.org)	Specifications published by T2T RG (Thing to Thing Research Group) The T2T RG will investigate open research issues in turning a true “Internet of Things” into reality, and on an Internet where low-resource nodes
ISO	ISO/AWI 20900 PAPS	Partially automated parking systems
ISO	New Topic	Automated Valet Parking System
ISO (TC 22/SC31)	15118-1:2013 15118-2:2014 15118-3:2015.	Road vehicles -- Vehicle to grid communication interface -- Part 1: General information and use-case definition. Road vehicles -- Vehicle-to-Grid Communication Interface -- Part 2: Network and application protocol requirements. Road vehicles -- Vehicle to grid communication interface -- Part 3: Physical and data link layer requirements.
ISO (TC204 WG14)	ISO/CD 20035 C-ACC res	Cooperative Adaptive Cruise Control - Performance requirements and test procedure
ISO/IEC	27001	Information technology Security techniques Information security management systems Requirements
ISO/IEC	27002	Information technology Security techniques Code of practice for information security controls
oneM2M	TR-0026	Vehicular Domain Enablement

3.3.4 Infrastructure

Organization	Number	Title
3GPP	N/A	3GPP standards: Lte, Lte Adv, Lte Adv Pro, 5G, VTx (V, I, P), Nb-IoT, eMTC
3GPP	3GPP - Release 13	Narrowband Internet of Things (NB-IoT)
3GPP	3GPP - Release 14	Technical Specification Group Radio Access Network; Study on LTE-based V2X Services
5GAA	N/A	Various specs: WG1 (Use Cases and Tech Req); WG2 (System Architecture); WG3 (Evaluations, Testbeds and Pilots); WG4 (Standards, Policy, Certification and

Organization	Number	Title
		Regulatory); WG5 (Business Models)
AIOTI		Various WG03 (IoT Standards) and WG09 (Smart Mobility) Recommendations and Guidelines
BBF	TR-069 and USP	TR-069 CPE WAN Management Protocol (CWMP) and Universal Service Platform (USP)
ETSI (TC ITS)	various	ETSI TC ITS
ETSI (TC ITS)	EN 302 636-1 EN 302 636-2 EN 302 636-3 EN 302 636-4-1 V1.2.1 (2014-07) EN 302 636-5-1 V1.2.1 (2014-08) EN 302 636-6-1 V1.2.1 (2014-05)	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements GeoNetworking; Part 2: Scenarios GeoNetworking; Part 3: Network Architecture 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 GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols
ETSI (TC Cyber Security)	TR 103 303 V1.1.1	CYBER; Protection measures for ICT in the context of Critical Infrastructure
ETSI (TC ERM)	EN 300 674-2-2	TTT - Dedicated Short Range Communication (DSRC)-Harmonized standard - On-Board Units (OBU)
ETSI (TC ERM)	EN 300 674-2-1	TTT - Dedicated Short Range Communication (DSRC)-Harmonized standard - Road Side Units (RSU)
ETSI (TC ERM)	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
IEEE SA	802.11p-2010	Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments
IETF	RFC 4944	Transmission of IPv6 Packets over IEEE 802.15.4 Networks
LoRaWAN	201R0	LoRaWAN™ Specification
oneM2M	TS-0001 TS-0003 TS-0030 TS-0004 TS-0008 TS-0009 TS-0010 TS-0020	Functional Architecture Security Solutions Generic Interworking Service Layer Core Protocol CoAP Protocol Binding HTTPProtocol Binding MQTT Protocol Binding WebSocket Protocol Binding
OSGi	Various	The OSGi Alliance specifications provide a standardized service platform for interacting with services (both local and remote) using a variety of defined communication and messaging protocols, including UPnP, TR069, enOcean, OMA DM, HTTP/REST, JSON-RPC and many others built by

Organization	Number	Title
		the community

3.3.5 IoT Architecture

Organization	Number	Title
3GPP	N/A	3GPP standards: Lte, Lte Adv, Lte Adv Pro, 5G, VTx (V, I, P), Nb-IoT, eMTC
3GPP	3GPP - Release 13	Narrowband Internet of Things (NB-IoT)
3GPP	3GPP - Release 14	Technical Specification Group Radio Access Network; Study on LTE-based V2X Services
3GPP	3GPP TS 33.185 V1.0.0	Security aspect for LTE support of V2X services (release 14)
5GAA	N/A	Various specs: WG1 (Use Cases and Tech Req); WG2 (System Architecture); WG3 (Evaluations, Testbeds and Pilots); WG4 (Standards, Policy, Certification and Regulatory); WG5 (Business Models)
AIOTI		Various WG03 (IoT Standards) and WG09 (Smart Mobility) Recommendations and Guidelines
ETSI (TC ITS)	EN 302 665	Intelligent Transport Systems (ITS); Communications Architecture of ITS stations
ETSI (TC Cyber Security)	TR 103 304 V1.1.1	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services
oneM2M	TS-0011 TS-0002 TS-0001 TS-0003 TS-0012 TS-0030	Common Terminology Requirements Functional Architecture Security Solutions oneM2M Base Ontology Generic Interworking
ETSI ISG CIM	Being developed	Being developed : technical specifications to enable multiple organizations to develop interoperable software implementations of a cross-cutting Context Information Management (CIM) Layer. It is about bridging the gap between abstract standards and concrete implementations.
FI-PPP/FIWARE Foundation	FIWARE	- IoT Broker GE Specification: - IoT Discovery GE Specification: - Context Broker GE Specification:
IRTF	Various (www.irtf.org)	Specifications published by T2T RG (Thing to Thing Research Group) The T2T RG will investigate open research issues in turning a true "Internet of Things" into reality, and on an Internet where low-resource nodes

3.3.6 Devices and sensor technology

Organization	Number	Title
3GPP	N/A	3GPP standards: Lte, Lte Adv, Lte Adv Pro, 5G, VTx (V, I, P), Nb-IoT, eMTC
3GPP	3GPP - Release 13	Narrowband Internet of Things (NB-IoT)
3GPP	3GPP - Release 14	Technical Specification Group Radio Access Network; Study on LTE-based V2X Services
Bluetooth	Bluetooth 5.0	Bluetooth Core Specification, version 5.0
oneM2M	TS-0001 TS-0003 TS-0005	Functional Architecture Security Solutions Management Enablement (OMA)

Organization	Number	Title
	TS-0006 TS-0012 TS-0030 TS 0021 TS 0124 TS 0023 TS-0013	Management Enablement (BBF) oneM2M Base Ontology Generic Interworking oneM2M and AllJoyn® Interworking oneM2M and OIC Interworking Home Appliances Information Model and Interoperability Testing
OMA	OMA-TS-NGSI_Context_Management-V1_0-20120529-A	OMA Next Generation Service Interface – Context Management
OSGi	Various	The OSGi Alliance specifications provide a standardized service platform for interacting with services (both local and remote) using a variety of defined communication and messaging protocols, including UPnP, TR069, enOcean, OMA DM, HTTP/REST, JSON-RPC and many others built by the community
IETF	Various (www.ietf.org)	Specifications published by several WGs: 6lo (IPv6 over Networks of Resource-constrained Nodes), 6TiSCH (IPv6 over the TSCH mode of IEEE 802.15.4e), detnet (Deterministic Networking), lpwan (Low Power WAN), IPWAVE (), ACE (Authentication and Authorization for Constrained Environments), CORE (Constrained RESTful Environments) WG, COSE (CBOR Encoded Message Syntax), CBOR (Concise Binary Object Representation), Dice (DTLS In Constrained Environments)
IETF	RFC 4944	Transmission of IPv6 Packets over IEEE 802.15.4 Networks
ISO	ISO/AWI 20900 PAPS	Partially automated parking systems
ISO	New Topic	Automated Valet Parking System
ISO (TC204 WG14)	ISO/CD 20035 C-ACC res	Cooperative Adaptive Cruise Control - Performance requirements and test procedure
LoRaWAN	201R0	LoRaWAN™ Specification
SENSORIS Forum / ERTICO		Vehicle Sensor Data Cloud Ingestion Interface Specification

3.3.7 Security and Privacy

Organization	Number	Title
3GPP	3GPP TS 33.185 V1.0.0	Security aspect for LTE support of V2X services (release 14)
5GAA	N/A	Various specs: WG1 (Use Cases and Tech Req); WG2 (System Architecture); WG3 (Evaluations, Testbeds and Pilots); WG4 (Standards, Policy, Certification and Regulatory); WG5 (Business Models)
AIOTI		Various WG03 (IoT Standards) and WG09 (Smart Mobility) Recommendations and Guidelines
ETSI (TC ITS)	various	ETSI TC ITS
ETSI (TC ITS)	TS 102 940	Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management
ETSI (TC ITS)	TS 103 191,	ITS Testing, Conformance test specifications for: Signal Phase And Timing (SPAT) and Map (MAP)

Organization	Number	Title
	TS 103 096, TS 102 869, TS 102 868, TS 102 871, TS 102 870, TS 102 859	ITS Security Decentralized Environmental Notification Basic Service (DEN) Cooperative Awareness Basic Service (CA) GeoNetworking ITS-G5 Geonetworking Basic Transport Protocol (BTP) Transmission of IP packets over GeoNetworking
oneM2M	TS-0002 TS-0001 TS-0003	Requirements Functional Architecture Security Solutions
OSGi	Various	The OSGi Alliance specifications provide a standardized service platform for interacting with services (both local and remote) using a variety of defined communication and messaging protocols, including UPnP, TR069, enOcean, OMA DM, HTTP/REST, JSON-RPC and many others built by the community
ETSI (TC Cyber Security)	TR 103 303 V1.1.1	CYBER; Protection measures for ICT in the context of Critical Infrastructure
ETSI (TC Cyber Security)	TR 103 304 V1.1.1	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services
ISA/IEC	62443	Security for industrial automation and control systems
IEEE	1609.0 1609.2 1609.3 1609.4 1609.11 1609.12	1609.0 IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture 1609.2 IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages 1609.3 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services 1609.4 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation 1609.11 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)-- Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS) 1609.12 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Identifier Allocations
IETF	Various (www.ietf.org)	Specifications published by several WGs: 6lo (IPv6 over Networks of Resource-constrained Nodes), 6TiSCH (IPv6 over the TSCH mode of IEEE 802.15.4e), detnet (Deterministic Networking), lpwan (Low Power WAN), IPWAVE (), ACE (Authentication and Authorization for Constrained Environments), CORE (Constrained RESTful Environments) WG, COSE (CBOR Encoded Message Syntax), CBOR (Concise Binary Object Representation), Dice (DTLS In Constrained Environments)
IRTF	Various (www.irtf.org)	Specifications published by T2T RG (Thing to Thing Research Group) The T2T RG will investigate open research issues in turning a true "Internet of Things" into reality, and on an Internet where low-resource nodes
ISO/IEC	27001	Information technology Security techniques Information security management systems Requirements
ISO/IEC	27002	Information technology

Organization	Number	Title
		Security techniques Code of practice for information security controls
ISO/IEC	15408-1	Information Technology – Security Techniques – Evaluation criteria for IT security – Information and General Model
ISO/IEC	15408-2	Information Technology – Security Techniques – Evaluation criteria for IT security – Security Functional Components
ISO/IEC	15408-3	Information Technology – Security Techniques – Evaluation criteria for IT security – Security Assurance Components
LoRaWAN	201R0	LoRaWAN™ Specification
oneM2M	TS-0002 TS-0001 TS-0003	Requirements Functional Architecture Security Solutions

3.3.8 Conformance, Testing

Organization	Number	Title
ETSI (TC ITS)	TS 103 191, TS 103 096, TS 102 869, TS 102 868, TS 102 871, TS 102 870, TS 102 859	ITS Testing, Conformance test specifications for: Signal Phase And Timing (SPAT) and Map (MAP) ITS Security Decentralized Environmental Notification Basic Service (DEN) Cooperative Awareness Basic Service (CA) GeoNetworking ITS-G5 Geonetworking Basic Transport Protocol (BTP) Transmission of IP packets over GeoNetworking
ETSI (TC ITS)	EG 202 798	Intelligent Transport Systems (ITS) Testing; Framework for conformance and interoperability testing
ISO/IEC	27000:2016	Information technology Security techniques Information security management systems Overview and vocabulary
oneM2M	TS-0013 TS-0015 TS-0017 TS-0018 TS-0019	Interoperability Testing Testing Framework Implementation Conformance Statements Test Suite Structure & Test Purposes Abstract Test Suite & Implementation eXtra information for Test

4 Standardization: preliminary activities

In this chapter are presented the results of preliminary activities foreseen for the Standardization Plan.

In particular, the standard gaps analysis based on literature and standards state of the art (presented in chapter 3).

Moreover a first collection of information about partners involvement into the SDOs, Alliance, Association and their availability to promote project issues is presented.

4.1 Standard gap analysis

The technical report ETSI TR 103 376 **“SmartM2M; IoT LSP use cases and standards gaps”** presents a detailed reports addressing potential standard gaps in the different vertical markets.

In this section only the main results of the technical report for the mobility vertical market are reported, in particular the requirements list with potential gaps and the general results arising from the theoretical analysis and the questionnaire conducted over a large sample of users.

Regarding the gaps analysis the report uses a list of requirements extracted from vertical-specific AIOTI reports and other available documentation. The selected requirements are classified by knowledge areas.

For each main requirement, the document reports the list of standards that address such a requirement. In case no standards are identified, a potential gap is reported.

In Table 2 the technology requirements identified for the smart mobility vertical market with potential standard gaps are reported.

Knowledge area	Requirements	Comment
Connectivity at network layer	High network availability performance behaviour	Potential gap
Application layer level, APIs, data models and ontologies	Customization and user-specified adaptation	Potential gap
Application layer level, APIs, data models and ontologies	Decision-making processes (cognitive and robotics)	Potential gap (left to market competition)
Application layer level, APIs, data models and ontologies	Standards for data handling and organization	Potential gap
Application layer level, APIs, data models and ontologies	Traffic data handling and analysis (fusion, cleaning, processing, mining, etc.)	Potential gap
Integration/ interoperability	Interoperability for equivalent messages defined at regional level (e.g. CAM and BSM)	Potential gap
Applications management	Continued support to the client after purchase	CCC only cover part of the requirements
Applications management	Tools to enable ease of	CCC only cover part of the

Knowledge area	Requirements	Comment
	installation, configuration and personalization; usability and convenience	requirements
Infrastructure	Enhanced proper infrastructure to support automated driving	Potential gap
IoT Architecture	Global-level standards (international)	ISO, oneM2M, only cover part of the requirements. Harmonization of regional standards is a potential gap
Devices and sensor technology	Performance behaviour: robustness, accuracy, reliability and resilience over long period of time	Potential gap

Table 2 - Technology gaps

The main gaps for the smart mobility vertical market resulting from theoretical analysis and questionnaires are as follows:

1. **Connectivity:** a smart vehicle is a place where very different network technologies and communications protocols are used. Securing high network availability, with certified performance figures, is necessary, making sure that no safety-related message is lost.
2. **Position accuracy:** to locate with sufficient precision the position of the vehicle, based on the application requirement.
3. **Data handling:** A lack of global data model and/or translation mechanisms between different specific models is clearly a big issue. Vehicles will generate a huge amount of data, that need to be processed and shared with all relevant stakeholders.
4. **Interoperable decision-making processing rules:** to process the sensor data and received messages in an identical manner across heterogeneous platforms.
5. **Decision-making processes:** To design autonomous control loops, defining the decisions and actions to be taken under the reception of specific sensor data and messages.
6. **Devices and sensors:** certification rules according their consumption, accuracy, reliability, probably into classes of devices.
7. **Security and privacy:** data security, data privacy and ownership, rules to ensure trust in a common good objective and avoid vehicle spoofing.
8. **Duplication of standards according to different regions of the globe:** to enable the interoperability of the regional standards and allow the usage of devices from one region in the others.
9. **Fragmentation of the technology according to the target application:** to ensure consistency and if possible similarity between the technologies addressing the same needs, but in different market sub-segments.
10. **Usability and customization of the solutions:** to address these different market sub-segments and simplify their usage by the large public.

4.2 Standard: ongoing activities

This section presents a list of standard with ongoing activities that could be of interest for the AUTOPILOT standardization activities. These standard are selected from the standard described into chapter 3.

Standard/standard Body	Evolution/work in progress
3GPP (Third Generation Partnership Project)	The radio TSG groups specify the radio solutions such as LTE (Rel8) and related evolutions (Rel 10 onwards), for vehicular communications (rel14 onwards) and upcoming 5G (Rel15 onwards), and for IoT solutions, such as Nb-IoT (Rel 13 onwards) and eMTC families (Rel12 onwards).
3GPP - Release 14 "Technical Specification Group Radio Access Network; Study on LTE-based V2X Services"	The purpose of this TR is to document the identified LTE enhancements and corresponding evaluations for LTE-based V2X services
3GPP TS 33.185 V1.0.0 "Technical Specification Group Services and System Aspects: Security aspect for LTE support of V2X services (release 14)"	This document specifies the security aspects of V2X features in LTE
5GAA: 5G Automotive Alliance	<p>The main activities of the association include:</p> <ul style="list-style-type: none"> • Defining and harmonizing use cases, technical requirements and implementation strategies. • Supporting standardization and regulatory bodies, certification and approval processes. • Addressing vehicle-to-everything technology requirements, such as wireless connectivity, security, privacy, authentication, distributed cloud architectures and more. • Running joint innovation and development projects leading to integrated solutions, interoperability testing, large scale pilots and trial deployments. <p>The above activities will be realized within the following 5GAA WGs</p> <ul style="list-style-type: none"> • WG1-Use Cases and Technical Requirements; • WG2- System Architecture and Solution Development; • WG3 Evaluations, Testbeds and Pilots; • WG4- Standards, Policy, Certification and Regulatory; • WG5- Business Models and Go-To-Market Strategies
ADASIS Protocol	<p>V3.0.0 of ADASIS (Advanced Driver Assistance System Interface Specification) Protocol (in final review phase)</p> <p>In V3.0.0 data description and rule definition, for horizon synchronization between provider and receivers, are introduced.</p> <p>To achieve the interoperability result, the ADASIS protocol is standardized for different media implementation. ADASIS v2.0 was designed for CAN bus interface media, while v3.0 extend the concept to larger bandwidth and payload media</p>

Standard/standard Body	Evolution/work in progress
AIOTI recommendations and guidelines	<p>WG 03: IoT Standardization: this Working Group identifies and, where appropriate, makes recommendations to address existing IoT standards and analyses gaps in standardization, and develops strategies and use cases aiming for (1) consolidation of architectural frameworks, reference architectures, and architectural styles in the IoT space, (2) (semantic) interoperability, (3) security by design and (4) personal data & personal data protection to the various categories of stakeholders in the IoT space.</p> <p>WG 09: Smart mobility: The topic for this Working Group refers to IoT solutions that allow for increased multi-modal mobility, more efficient traffic management, a dynamic road infrastructure, automated road tolling, usage based insurance and improved policy making through the analysis of road usage data smart vehicles including autonomous and connected cars</p>
BBF Standards	<p>The scope of BBF BUS Work Area;</p> <ul style="list-style-type: none"> • Develop and evolve the TR-069 CPE WAN Management Protocol and a Universal Service Platform (USP) to cover existing use cases, machine-to-machine/IoT use cases, and the virtualization of broadband user services, prioritized by their potential business value. • Develop and specify new information models to broaden the range of for which TR-069 and USP can be used. • Develop requirements for broadband user devices and associated software. • Develop test plans and training programs for Work Area protocols and requirements. • Develop marketing white papers that supplement Work Area protocols and requirements.
ETSI ISG CIM standards	<p>The aim of the ETSI Industry Specification Group on Context Information Management is to issue technical specifications to enable multiple organizations to develop interoperable software implementations of a cross-cutting Context Information Management (CIM) Layer. It is about bridging the gap between abstract standards and concrete implementations</p> <p>The Phase 1 ISG CIM Group Report will detect and describe the standardization gaps in order to consider any missing features and to ensure interoperable software implementations, including open source implementations. Developing ISG CIM Group Specifications in Phase 2 will subsequently fill these gaps. It is expected that an extension of the RESTful binding of the OMA NGSI API involving expression using JSON-LD could aid interoperability, so this and potentially other extensions will be considered</p>
FIWARE	FIWARE is a middleware platform that was initiated by the

Standard/standard Body	Evolution/work in progress
	<p>European Union as part of the Future Internet PPP, for the development and global deployment of applications for Future Internet. It is now based on the FIWARE open community and lead by the FIWARE Foundation.</p> <p>The API specifications of FIWARE are open and royalty-free to facilitate creation and delivery of Future Internet applications and services in a variety of areas, including smart cities, sustainable transport, logistics, renewable energy, and environmental sustainability.</p>
ISO TC204	WG 14 (Vehicle/roadway warning and control systems) of ISO TC204 is standardizing performance requirements and test procedures for many of the new ITS features in cars, such as automatic parking, intelligent cruise control, backing-up aid, lane departure warning, collision warning and so on
ISO/AWI 20900 PAPS Partially automated parking systems (ISO TC204 WG14)	This standard for Partially Automated Parking System (PAPS) addresses light-duty vehicles, it is Under development. The aim of the standard is to help with the performance requirements and test procedures of Partially Automated Parking System (PAPS), which completes the whole task of the parking maneuvers controlling both longitudinal and lateral movement of the vehicle to mitigate driver's burden.
ISO TC204 WG14 - Automated Valet Parking System	This standard, that is under development, will be used to manage procedures related to automated valet parking use cases
ISO/CD 20035 C-ACC Cooperative Adaptive Cruise Control - Performance requirements and test procedures (ISO TC204 WG14)	<p>Cooperative Adaptive Cruise Control (CACC) system International Standard is an expansion to existing ACC control strategy by using wireless communication with preceding vehicles (V2V) and/or the infrastructure (I2V). Both multi vehicle V2V data and I2V infrastructure data are within the scope of this standard.</p> <p>The Scope of the CACC System International Standard will address two types of CACC: V2V, and I2V. Both CACC systems require active sensing using for example radar, lidar, or camera systems. The combined V2V and I2V CACC are not addressed in this standard. The following requirements will be addressed in this standard:</p> <ul style="list-style-type: none"> – Classification of the types of CACC. – Definition of the performance requirements for each CACC type. – CACC state transitions diagram. – Minimum set of wireless data requirements. – Test procedures. <p>Motor vehicle including light vehicle and heavy vehicle are covered in the scope of this standard.</p>
oneM2M standards	<p>General requirements and architecture</p> <ul style="list-style-type: none"> • TS-0011 Common Terminology

Standard/standard Body	Evolution/work in progress
	<ul style="list-style-type: none"> • TS-0002 Requirements • TS-0001 Functional Architecture • TS-0003 Security Solutions <p>Semantic, general and specic interworking</p> <ul style="list-style-type: none"> • <i>TS-0030 Generic Interworking</i> <p>Testing</p> <ul style="list-style-type: none"> • <i>TS-0015 Testing Framework</i> • <i>TS-0017 Implementation Conformance Statements</i> • <i>TS-0018 Test Suite Structure & Test Purposes</i> • <i>TS-0019 Abstract Test Suite & Implementation eXtra information for Test</i> <p>Other documents relevant for AUTOPILOT:</p> <ul style="list-style-type: none"> • <i>oneM2M TR 0026 Vehicular Domain Enablement</i> <p>Documents listed above are still to be published as release 3; release 3 expected 1Q 2018</p> <p>Release 2 does not support all requirements needed for Autonomous driving (missing timing and reliable delivery requirements). Release 3 in considering some of the requirements</p>
OSGi standards	<p>The OSGi specifications provide a standardized service platform for interacting with services (both local and remote) using a variety of defined communication and messaging protocols, including UPnP, TR069, enOcean, OMA DM, HTTP/REST, JSON-RPC and many others built by the community</p> <p>Published, Release 6, Ongoing Release 7 to be completed in 2017.</p> <p>Currently working on the first IoT release, to be published on 2018</p>
SENSORIS Standards	<p>SENSORIS initiative standardizes the data interface of Vehicle sensor for Cloud ingestion</p> <p>V2.0.2 was released in 2015, future standardized release under planning for 2017</p>

4.3 Standardization Activities

The following table summarizes the SDOs, Alliance and OSS activities followed by project partners. This information can be used to:

- (1) obtain more details on the standards and specification documents of interest for AUTOPILOT,
- (2) to have information on the expected evolutions, or
- (3) even more to present any need or gaps that may arise in the AUTOPILOT activities.

Partner	Organization followed
ERT	ERTICO follows currently the following SDO activities: ETSI: TC ITS: Active attendance to all meeting with focus on WG1; OneM2M: ERTICO has planned to contribute to OneM2M CEN TC278: Following the developments and standardization activities. So far not attendance of meetings yet. ISO TC204: Active attendance to all meeting with focus on WG14, 16 and 18 IETF: Following the ITS e-mail exploder mailings
CET	CETECOM is contributing to 3GPP WG RAN5 (LTE RF test case development) and ETSI MSG (eCall test case development).
CNIT	CNIT and ETSI Centre for Testing and Interoperability team up to implement large-scale field trials (as it was done in 2016 for the ETSI ITS Cooperative Mobility Services Event 5, the so-called Plugtest™, in Livorno). CNIT will support a large-scale field trial (a forthcoming Plugtest™) focusing on vehicular communications implemented through 3GPP V2X protocols.
EGM	EGM is member of ETSI, oneM2M and founding member of the ETSI ISG CIM. <ul style="list-style-type: none"> - EGM is contributing to ETSI TC ITS in testing framework and in particular working under ETSI Specialist Task Force (STF) 525 “Intelligent Transports Systems Interoperability Validation Framework” on validating development of tests under new TTCN-3 tool called TITAN. EGM participated to several ITS interoperability events. - EGM is also working in oneM2M tests cases (rapporteur on security tests specifications) and oneM2M test tools. EGM is currently member of the ETSI STF 531 “ SmartM2M conformance testing for oneM2M specifications” to develop tests cases for oneM2M. EGM is also following and contributing to oneM2M TST (Testing) committee on tests and MAS (Management of Abstraction and Semantic) on semantic issues. EGM is regularly participating to oneM2M interoperability events and is planning to organize a new Semantic Interoperability event . - EGM is founding member of the ETSI Industry Specific Group CIM (Context Information Management) working on Data Model and Context information Management relying on past experience of FIWARE and OMA NGSI specifications which are contributed to this group.
HUA	Huawei is contributing worldwide to more than 170 SDOs, Alliances and Open Software Source initiatives including AIOTI, OneM2M, 3GPP, ETSI, ITU-T, BBF, OSGi Alliance, IETF, IEEE, 5GAA. In the context of AUTOPILOT, Huawei is planning to contribute, based on AUTOPILOT recommendations, in AIOTI, OneM2M, OSGi Alliance and IETF.
IDI	IDIADA is contributing to ISO (International Organization for Standardization) <ul style="list-style-type: none"> - IDIADA contributes on several working groups with the definition of safety standards and methodologies for connected and automated driving vehicles. IDIADA is contributing to Euro NCAP (European New Car Assessment Program) <ul style="list-style-type: none"> - IDIADA contributes on the definition of safety standards and standardized test methodologies for connected and automated driving vehicles via Euro NCAP where IDIADA represents the Catalan Government in the board of directors UNECE where IDIADA represents the Spanish Government. IDIADA is also contributing to ETSI (European Telecommunications Standards Institute).
ISMB	ISMB contributes in ETSI-TC-ITS, the working group on Intelligent Transport System (ITS) of ETSI Standardization Body; more specifically ISMB is active in WG3 and WG4,

Partner	Organization followed
	where it covered also member of a Specialist Task Force (STF395).
NEC	<p>NEC is contributing to oneM2M</p> <ul style="list-style-type: none"> - NEC supported TNO in bringing in use case and requirements related to Autopilot to better support automotive use cases in the future in oneM2M. - NEC is working in the oneM2M MAS working group on semantic aspects which are highly relevant for connecting oneM2M and FIWARE IoT systems as it is envisioned for the IoT infrastructure of AUTOPILOT. <p>NEC is contributing and chairing (Lindsay Frost) ETSI ISG CIM. ETSI IST CIM is highly relevant for the evolvement of the context interfaces in FIWARE which are to be used in the IoT infrastructure of AUTOPILOT.</p>
THA	<p>THALES is contributing to CENELEC:</p> <ul style="list-style-type: none"> - TC9XA SGA16 report recommends introduction of IEC 62443 standards. - TC9X SG24 Survey group proves applicability of IEC 62443 standards via gap-analysis <p>THALES is member of certMILS. certMILS develops a security certification methodology for Cyber-physical systems (CPS). Homepage: https://certmils.eu/</p>
TI	<p>Telecom Italia is present in the following SDOs that are expected to be relevant for AUTOPILOT:</p> <ul style="list-style-type: none"> - 3GPP, where the work on vehicular requirements and solutions is ongoing (in particular the V2X one), but also the general connectivity offered by 4G and 5G, with active participation in requirements, architectural, security, and radio groups. - OneM2M, where the contribution is concentrated on the architecture, the Access control and the interworking framework, in particular the general interworking and the interworking with 3GPP system. Telecom Italia is also taking leading role in the organization as VC of the steering committee and leader of the groups dealing with the organizational procedure and the methods of work. - ETSI TC SmartM2M, dealing with anthologies that are related to the oneM2M framework, leading the work as Chari of the TC. - GSMA following the activity related to ITS and Automotive requirements, including the ones related to the security and business models aspects of reconfigurable UICCC. <p>Telecom Italia is member and following actively the work of ERTICO and AIOTI in relation to activity potentially related to AUTOPILOT. Telecom Italia is also active in BBF, IETF, ITU-T and ITU-R, even not directly following the ITS/Automotive activities.</p>
TNO	<p>TNO has provided a number of contributions to oneM2M aimed at requirements for vehicular domain. Some of those requirements are included into requirements for the (just started) release 3 of oneM2M. Goal was to introduce time-critical and reliable delivery of IoT data, which is needed for autonomous driving (REQ-2017-0020 – “Requirements for TS0002”, REQ-2017-0017 – “Autonomous Driving section for introduction”, REQ-2017-0001R03 – “Autonomous driving”).</p>

5 Conclusion

This document describes the Standardization Plan approach to be followed by the AUTOPILOT project in order to take care of the standardization issues, during the specification and the development process in order to ensure interoperability, replicability and sustainability of the AUTOPILOT results.

The standardization plan activities cover the entire duration of the project: in the starting phase they provide an overview of the relevant standards available; during the project development phases, they analyse the requirements, the specifications and the pilots' results by gathering gaps and needs that can contribute to the evolution of standards.

The document contains an overview of the standards that can be relevant for the project requirements specification and development activities of AUTOPILOT. The standard overview is the result of the standards analysis activity based on the competence and experience of the partners in the different knowledge areas and into the SDO participations; it takes into account two standards overview documents issued by AIOTI WG03 and ETSI.

The selected standards and organizations are presented with a number of established information that allow to identify and recover the document, moreover for each of them the aim and the description is provided together with some hint on how to use it into the project. The material is aggregated using different criteria (organization, areas of interest for the project, knowledge area). This should facilitate the use of the material collected.

The document presents a preliminary analysis results on standard gaps and a first selection of standards under development that could be of interest for the Project. This preliminary information will be further developed in the next ongoing task activities taking into account the results of use cases specifications and AUTOPILOT requirements.

6 Annexes

6.1 Annex A - Organization overview

This section presents an overview of potential organizations of interest for the project based on the partners' experience, organized by AUTOPILOT project area of interest. Organizations which are covered in more detail in the present document (chapter 3) are marked (*).

Please note that the meaning of the type of organization is the following:

- **Alliance** - A forum organization promoting a topic, not developing technical specifications
- **Specs.** - Committee or group developing technical specifications
- **OpenSource** - Eclipse or some other project with free licensing
- **Project** - EC-funded project, usually FP7 or H2020
- **d** - (some deliverables are public, but exact work not clear at time of writing)

6.1.1 IoT Platform and architecture

Acronym	Reference/Link	Name/Comment(s)	Type
AGILE	http://agile-iot.eu/	Topics: Environment / Energy Monitoring, Recycling, Livestock Monitoring, Port / Vessel Monitoring, Smart Retail, Product Monitoring, Mass Market PLM, Smart Healthcare, Quantified Self Results: http://agile-iot.eu/resources	Project
AllJoyn	https://allseenalliance.org/developers	Transferred to OCF (Open Connectivity Foundation)	OpenSource
Allseen Alliance	https://allseenalliance.org	The Open Connectivity Foundation (OCF) is creating a specification and sponsoring an open source project enabling billions of connected devices (devices, phones, computers and sensors) to communicate with one another regardless of manufacturer, operating system, chipset or physical transport.	Alliance
BBF (*)	https://www.broadband-forum.org	(Broadband Forum) The Forum is the industry's defining body for Broadband networking.	Specs.
ETSI SmartM2M	https://portal.etsi.org/TBSiteMap/SmartM2M/SmartM2MToR.aspx	TC Smart M2M provides specifications for M2M services and applications. It supports and identifies European policy and regulatory requirements including mandates in the area of M2M and the Internet of Things. It works on the conversion of the oneM2M specifications into European Standards.	Specs.
HYPER/CAT	http://www.hypercat.io	Hypercat is a Global Alliance and standard driving secure and interoperable Internet of Things (IoT) for Industry and cities. The Hypercat specification allows Internet of Things (IoT) clients to discover information about IoT assets over the web.	Specs.
iCore	http://www.iot-icore.eu/	Internet Connected Objects for Reconfigurable	Project

Acronym	Reference/Link	Name/Comment(s)	Type
		Ecosystems	
IEEE P2413	http://grouper.ieee.org/groups/2413	Standard for an Architectural Framework for the Internet of Things (IoT)	Specs.
IIC	http://www.industrialinternetconsortium.org	(Industrial Internet Consortium) The Industrial Internet Consortium's mission is to deliver a trustworthy IIoT in which the world's systems and devices are securely connected and controlled to deliver transformational outcomes.	Alliance
IoT Security Foundation	https://www.iotsecurityfoundation.org	IoTSec is a collaborative, non-profit, international alliance addressing the complex challenges posed by security in the expansive hyper-connected world.	Alliance
IPSO	http://www.ipso-alliance.org	(Internet Protocol for Smart Object) The IPSO Alliance is a global forum comprising a diverse international membership focused on enabling IoT devices to communicate, understand and trust each other with global interoperability based on open standards.	Specs.
ITU JCA-IoT and SC&C	http://www.itu.int/en/ITU-telecom/ica/iot/Pages/default.aspx	Joint Coordination Activity on Internet of Things and Smart Cities and Communities (JCA-IoT and SC&C)	Specs.
Mosquitto	https://projects.eclipse.org/projects/technology.mosquitto	Eclipse Mosquitto provides a lightweight server implementation of the MQTT protocol that is suitable for all situations from full power machines to embedded and low power machines.	OpenSource
OIC	http://openinterconnect.org	(Open Interconnect Consortium) Transferred to OCF (Open Connectivity Foundation)	Specs.
OM2M	http://www.eclipse.org/om2m	The Eclipse OM2M project is an open source implementation of oneM2M and SmartM2M standard. It provides a horizontal M2M service platform for developing services independently of the underlying network, with the aim to facilitate the deployment of vertical applications and heterogeneous devices.	OpenSource
oneM2M (*)	http://www.onem2m.org	oneM2M develops technical specifications which address the need for a common M2M Service Layer. oneM2M specifications provide a framework to support a wide range of applications and services such as smart cities, smart grid, connected car, home automation, public safety, and health.	Specs.
OpenIoT	https://github.com/OpenIoTOrg/openiot	Open Source Solution for the Internet of Things into the Cloud OpenIoT is an open source platform for interoperability between sensor data silos and focuses on enabling interoperable semantically-annotated IoT cloud applications. OpenIoT comprises utility-driven security and tools for zero-programming development of applications. ' ' The vocabularies are formally represented using Ontologies and it uses OWL	OpenSource

Acronym	Reference/Link	Name/Comment(s)	Type
		(Ontology Web Language) and references namespaces.	
OpenRemote	http://www.openremote.com	OpenRemote is an open source middleware for the Internet of Things.	OpenSource
OSGi Alliance (*)	http://www.osgi.org	The OSGi Alliance specifications provide a standardized service platform for interacting with services (both local and remote) using a variety of defined communication and messaging protocols, including UPnP, TR069, enOcean, OMA DM, HTTP/REST, JSON-RPC and many others built by the community.	Specs.
Plattform Industrie 4.0	http://www.plattform-i40.de	Plattform Industrie 4.0's is a German alliance targeting industrial manufacturing. The platform aims to promote digital structural change and to provide the consistent and reliable framework necessary for this.	Alliance
ULE	http://www.ulealliance.org	(The Ultra Low Energy Alliance) The ULE develops, certifies and promotes low-power wireless technology.	Specs.
VICINITY2020	http://vicinity2020.eu/vicinity/	Topics: Smart City, Environment / Energy Monitoring, Recycling, Smart Mobility, Smart Healthcare, Quantified Self Results: http://vicinity2020.eu/vicinity/public-deliverables	Project
W3C	http://www.w3.org	(World Wide Web Consortium) W3C standards define an Open Web Platform for application development.	Specs.
W3C WoT	https://www.w3.org/WoT/IG/	(Web of Things Interest Group) We need platform independent APIs for application developers, and a means for different platforms to discover how to inter-operate with one another. The approach we are taking is based upon rich metadata that describes the data and interaction models exposed to applications, and the communications and security requirements for platforms to communicate effectively.	Specs.

6.1.2 Vehicle IoT Integration and platform

Acronym	Reference/Link	Name/Comment(s)	Type
ADASIS (*)	http://adasis.org	Advancing map-enhanced driver assistance systems	Alliance
Bluetooth (*)	http://www.bluetooth.com	Bluetooth technology is enabling a global vision to connect more devices in more places—from mobile phones to automobiles, medical equipment to manufacturing plants and fulfillment centers.	Specs.
CANCIA	http://www.can-cia.org	(CAN IN Automation) CAN in Automation (CiA) is the international users' and manufacturers' group for the CAN network (Controller Area Network), internationally standardized in the ISO 11898	Specs.

Acronym	Reference/Link	Name/Comment(s)	Type
		series.	
C2C-CC	https://www.car-2-car.org	(Car-2-Car Communication Consortium) The C2C-CC develops an open European standard for C-ITS.	Specs.
CCC	http://carconnectivity.org	(Car Connectivity Consortium) The CCC is an organization driving global technologies for smartphone-centric car connectivity solutions.	Alliance
CEN TC278 (*)	https://www.cen.eu/	CEN TC 278 is responsible for standardization in the field of telematics for traffic and road transport.	Specs.
ERTICO	http://ertico.com	(ERTICO - ITS Europe) ERTICO - ITS Europe is a partnership of around 100 companies and institutions involved in the production of Intelligent Transport Systems (ITS). Together, ERTICO Partners conduct a range of activities to develop and deploy ITS to save lives, protect the environment and sustain mobility in the most cost-effective way.	Alliance
ETSI TC ITS (*)	http://www.etsi.org	ETSI TC ITS concentrates on a subset of the ITS scope with the current focus being on 5.9 GHz communications called ITS-G5 in ETSI terminology, applying a special multi-hopping network function called GeoNet, and serving a small number of mainly safety applications for vehicle-to-vehicle and vehicle-to-roadside scenarios.	Specs.
GEONOVUM	http://www.geonovum.nl	(GEO standards NL) Provide standards that are necessary to make geographical information accessible.	d
OAA	http://www.openautoalliance.net	(Open Automotive Alliance) The OAA is a global alliance of technology and auto industry leaders committed to bringing the Android platform to cars.	Alliance
OPC	https://opcfoundation.org	(Open Platform Communications Foundation) OPC develops an interoperability standard for the secure and reliable exchange of data in the industrial automation space and in other industries.	Alliance
RailML	http://www.railml.org	Allow day-to-day railway operations, these editors also allow sharing of data among traffic control systems and passenger information systems at stations, on websites, and for mobile phones.	d
RIOT	http://www.riot-os.org	(Real time OS for sensor networks) RIOT is a free, open source operating system developed by a grassroots community gathering companies, academia, and hobbyists, distributed all around the world. RIOT implements relevant open standards supporting an Internet of Things that is connected, secure, durable, and privacy-friendly.	OpenSource
ROS	http://www.ros.org	(Robot Operating System)	OpenSource

Acronym	Reference/Link	Name/Comment(s)	Type
		The Robot Operating System (ROS) is a set of software libraries and tools that helps building robot applications.	
SAE International	http://www.sae.org	Globally active professional association and standards developing organization for engineering professionals in various industries. Principal emphasis is placed on transport industries such as automotive, aerospace, and commercial vehicles.	Specs.
SENSORIS Forum (*)	http://erticonetwork.com/ertico-coordinate-standard-development-vehicle-cloud-data	SENSORIS – a platform that will develop a global standard for vehicle-to-cloud data.	Alliance
VDA	http://www.vda.de	Product-specific standards for road vehicles and the standardization of multimodal transport containers like freight containers and swap container bodies.	d

6.1.3 Communication network

Acronym	Reference/Link	Name/Comment(s)	Type
3GPP (*)	http://www.3gpp.org	(3rd Generation Partnership Project) 3GPP covers cellular telecommunications network technologies, including radio access, the core network, and service capabilities - including work on codecs, security, quality of service - and thus provides complete system specifications. The specifications also provide hooks for interworking with non 3GPP radio accesses, such as Wi-Fi.	Specs.
5GAA (*)	http://5gaa.org/	(5G Automotive Alliance) Develop, test and promote communications solutions, initiate their standardization and accelerate their commercial availability and global market penetration to address society's connected mobility and road safety needs with applications such as autonomous driving, ubiquitous access to services and integration into smart city and intelligent transportation.	Alliance
Enocean	https://www.enocean-alliance.org/	(Enocean Alliance) The Enocean Alliance develops specifications for self-powered wireless switches, sensors and controls for sustainable buildings.	Specs.
ETSI	http://www.etsi.org	(European Telecommunications Standards Institute) ETSI, the European Telecommunications Standards Institute, produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and Internet technologies.	Specs.
ETSI ERM (*)	http://www.etsi.org/deliver/etsi_en/302500_302	ETSI Technical Committee (TC) EMC and Radio Spectrum Matters (ERM) is responsible for a	Specs.

Acronym	Reference/Link	Name/Comment(s)	Type
	599/302571/02.00.00_20/en_302571v020000a.pdf	range of radio product and electromagnetic compatibility (EMC) standards and the overall co-ordination of EMC and radio spectrum matters within ETSI.	
GSMA	http://www.gsma.com	The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with almost 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organizations in adjacent industry sectors.	Alliance
IEC (*)	http://www.iec.ch	(International Electrotechnical Commission) The IEC (<i>International Electrotechnical Commission</i>) is the world's leading organization for the preparation and publication of <i>International Standards</i> for all electrical, electronic and related technologies.	Specs.
IEEE (*)	http://www.ieee.org	(Institute of Electrical and Electronics Engineers) IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity. With an active portfolio of nearly 1,300 standards and projects under development, IEEE is a leading developer of industry standards in a broad range of technologies that drive the functionality, capabilities, and interoperability of products and services, transforming how people live, work, and communicate.	Specs.
IEEE 802 (*)	http://www.ieee802.org	(IEEE 802 LAN/MAN Standards Committee) IEEE 802 is a family of IEEE standards dealing with local area networks and metropolitan area networks.	Specs.
IETF (*)	http://www.ietf.org	(Internet Engineering Task Force) The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.	Specs.
ISO (*)	http://www.iso.org	(International Organization for Standardization) ISO is an independent, non-governmental international organization with a membership of 163 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges.	Specs.
ITU	http://www.itu.int	(International Telecommunication Union) ITU is the United Nations specialized agency for information and communication technologies – ICTs. It allocates global radio spectrum and satellite orbits, develops the technical	Specs.

Acronym	Reference/Link	Name/Comment(s)	Type
		standards that ensure networks and technologies seamlessly interconnect, and strives to improve access to ICTs to underserved communities worldwide.	
LoRa (*)	https://www.lora-alliance.org/	(LoRa Alliance) The LoRa Alliance is an open, non-profit association of members who are collaborating together and sharing experience to drive the success of the LoRa protocol, LoRaWAN, as the open global standard for secure, carrier-grade IoT LPWA connectivity.	Specs.
OMA (*)	http://openmobilealliance.org	(Open Mobile Alliance) OMA is a non-profit organization that delivers open specifications for creating interoperable services that work across all geographical boundaries, on any bearer network.	Specs.
OpenWSN	https://openwsn.atlassian.net/wiki/pages/viewpage.action?pageId=688187	The goal of the OpenWSN project is to provide open-source implementations of a complete protocol stack based on Internet of Things standards, on a variety of software and hardware platforms.	OpenSource
Weightless	http://www.weightless.org	Weightless is the name of a set of LPWAN open wireless technology standards for exchanging data between a base station and thousands of machines around it. These technologies allow developers to build Low-Power Wide-Area Networks (LPWAN). It is managed by Weightless SIG.	Specs.
Wi-Fi Alliance	http://www.wi-fi.org	Wi-Fi Alliance is a worldwide network of companies that provides Wi-Fi. Wi-Fi Alliance defines innovative, standards-based Wi-Fi technologies and programs, certifies products that meet quality, performance, security, and capability standards.	Specs.
XMPP	http://xmpp.org/	XMPP is an open standard for messaging and presence.	Specs.
ZigBee	http://www.zigbee.org	(The ZigBee Alliance) The ZigBee alliance provides an IoT solution, from mesh networks to a universal language that allows smart objects to work together, and certifies implementations.	Specs.

6.1.4 IoT Eco-system

Acronym	Reference/Link	Name/Comment(s)	Type
ACEA	http://www.acea.be	(European Automobile manufacturing Association)	Alliance
ACORD	http://www.acord.org	Exchange of insurance data	d
AIAG	http://www.aiag.org	An open forum where members cooperate in developing and promoting solutions (standards) that enhance the prosperity of the automotive industry).	d
AIOTI (*)	www.aioti.eu	(Alliance for Internet of Things Innovation)	Alliance

Acronym	Reference/Link	Name/Comment(s)	Type
		The "Smart mobility" working group WG9 considers applications of the Internet of Things (IoT) to the mobility domain with short-termed European wide economic potential and applicability. The IoT holds the potential for major disruptive effects across a wide variety of market sectors, where mobility applications comprise e. g. rapidly emerging self-driving and connected vehicles, multi-modal transport systems and ability to develop intelligent transportation systems.	
BIG IoT	http://big-iot.eu/	Topics: Smart City, Smart Mobility Results: http://big-iot.eu/index.php/media/ http://big-iot.eu/index.php/media/deliverables/	Project
DCAT	https://joinup.ec.europa.eu/asset/dcat_application_profile/description	(Application profile for data portals in Europe) The DCAT Application profile for data portals in Europe (DCAT-AP) is a specification based on the Data Catalogue vocabulary (DCAT) for describing public sector datasets in Europe.	Specs.
ebbits	http://www.ebbits-project.eu/news.php	Enabling the Business-Based Internet of Things and Services.	Project
EDXL	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency	The Emergency Data Exchange Language (EDXL) is a suite of XML-based messaging standards that facilitate emergency information sharing between government entities and the full range of emergency-related organizations.	d
FIWARE (*)	www.fiware.org	(FIWARE Community & FIWARE Foundation) The FIWARE Community is an independent open community whose members are committed to materialise the FIWARE mission, that is: "to build an open sustainable ecosystem around public, royalty-free and implementation-driven software platform standards that will ease the development of new Smart Applications in multiple sectors".	OpenSource
IRTF (*)	www.irtf.org	The T2T RG is a proposed IRTF Research Group that will be using and providing input mainly to IETF, but also to the IOT research community.	Specs.
IoTivity	https://www.iotivity.org	IoTivity is an open source software framework enabling seamless device-to-device connectivity to address the emerging needs of the Internet of Things.	OpenSource
ITU SG-20	http://www.itu.int/en/ITU-T/studygroups/2013-2016/20/Pages/default.aspx	Study Group 20 is working to address the standardization requirements of Internet of Things (IoT) technologies, with an initial focus on IoT applications in smart cities and communities (SC&C).	Specs.
OASIS	https://www.oasis-open.org	OASIS is a nonprofit consortium that drives the development, convergence and adoption of open standards for the global information society.	Specs.
Odette	http://www.odette.org	Improve the flow of goods, services, product data and business information across the whole	d

Acronym	Reference/Link	Name/Comment(s)	Type
		supply chain, throughout the entire product life-cycle.	
OTA	http://www.opentravel.org	Business information and transaction standards for the travel industry	d
SGIP	http://sgip.org	(Smart Grid Interoperability Panel) 'SGIP is an industry consortium representing a cross-section of the energy ecosystem focusing on accelerating grid modernization and the energy Internet of Things through policy, education, and promotion of interoperability and standards to empower customers and enable a sustainable energy future. Our members are utilities, vendors, investment institutions, industry associations, regulators, government entities, national labs, services providers and universities.	Specs.
SIVI	http://www.sivi.org	Standards for insurance companies and intermediaries	d
symbloTe	https://www.symbiote-h2020.eu/	H2020 project in areas: -Smart City, Environment / Energy Monitoring, Recycling, Port / Vessel Monitoring, Smart Mobility, Smart Healthcare, Quantified Self	Project
WS-ISDEM	http://www.cen.eu/cenorm/sectors/sectors/iss/activity/ws-isdem.asp	Specifying a message structure for sharing situation awareness in the frame of Disaster and emergency management.	d

6.2 Annex B – Standards and Specifications

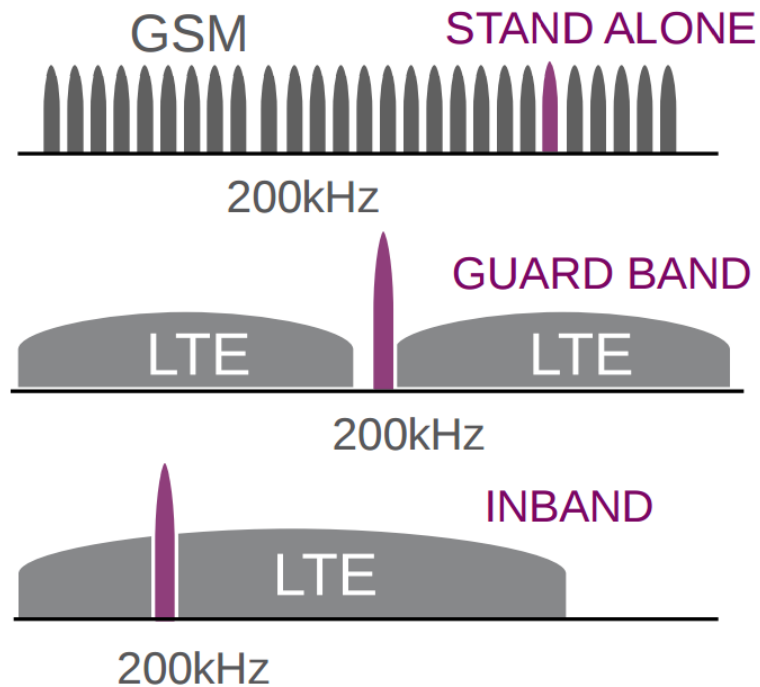
This section presents the standards and specifications documents that have been selected as relevant, grouped by organization.

6.2.1 3GPP

3GPP: Release 13 -Narrowband Internet of Things (NB-IoT)

Standardization body	3rd Generation Partnership Project (3GPP)
Standard No.	3GPP - Release 13
Standard Title	Narrowband Internet of Things (NB-IoT)
URL	ftp://ftp.3gpp.org/tsg_ran/TSG_RAN/TSGR_69/Docs/RP-151621.zip
Country	International
Status	Published
Date	09/2015
Aim	Narrowband-IoT is a Low-Power Wide-Area (LPWA) network technology developed to enable efficient communication for mass distributed devices across wide geographical footprints and deep within urban infrastructure. It is ideal for devices that generate low data traffic, rely on batteries and typically have a long device life cycle.
Description	NB-IoT (Narrowband Internet of Things) represents a solution based on a new radio interface, which can be used both in a portion of the LTE signal band (or in its guard band), or even in an autonomous way in portions of spectrum made available by the release of frequencies (e.g. in the case of a refarming of GSM band). NB-IoT is a self-contained carrier that can be deployed with a system bandwidth of only 200kHz and is specifically tailored for ultra-low-end IoT applications. It is enabled using new network software on an existing LTE network, which will result in rapid time to market. NB-IoT is a new 3GPP radio-access technology in the sense that it is not fully backward compatible with existing 3GPP devices. It is however designed to achieve excellent co-existence performance with legacy GSM, General Packet Radio Service (GPRS) and LTE technologies. A GSM operator can replace one GSM carrier (200 kHz) with NB-IoT. An LTE operator can deploy NB-IoT inside an LTE carrier by allocating one of the Physical Resource Blocks (PRB) of 180 kHz to NB-IoT. NB-IoT reuses the LTE design extensively, including the numerologies, downlink orthogonal frequency-division multiple-access (OFDMA), uplink single-carrier frequency division multiple-access (SC-FDMA), channel coding, rate matching, interleaving, etc. NB-IoT provides lean setup procedures, and a capacity evaluation indicates

that each 200kHz NB-IoT carrier can support more than 200,000 subscribers. NB-IoT also comes with an extended coverage of up to 20dB, and battery saving features, Power Saving Mode and eDRX for more than 10 years of battery life. NB-IoT can be used to connect simple devices, such as sensors, to drive new data streams, reduce operational costs and create new business models. Smart Meters, Smart Bins, environmental monitoring and precision agriculture are just a few applications of NB-IoT.



The Basic technical characteristics are the following:

- Targeting implementation in an existing 3GPP network
- Applicable in any 3GPP defined (licensed) frequency band
- Three deployment modes
- Processing along with wideband LTE carriers implying OFDM secured orthogonality and common resource utilization
- User rates ranging from 300 bps up to 200 kbps
- Maximum coupling loss 164 dB which has been reached with assumptions given in the table below
 - ~ 55000 devices per cell
 - Urban: deep in-building penetration
 - Rural: long range (10-15 km)

M2M access technology contained in 200 kHz with 3 deployments modes:

- Stand-alone operation
- Operation in LTE “guard band”
- Operation within wider LTE carrier (aka in-band)

Keyword

Communication and Connectivity; Devices and sensor technology; Infrastructure; Integration/interoperability; IoT Architecture.

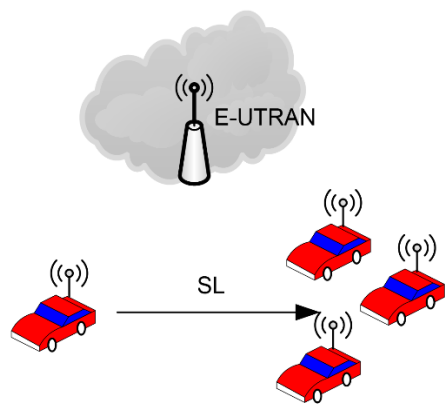
Autopilot Area involved

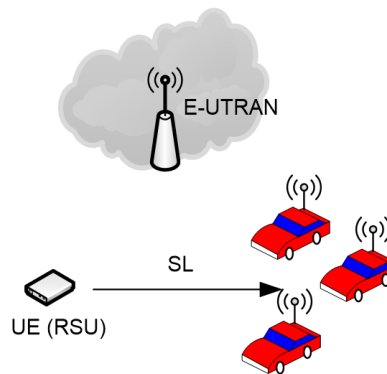
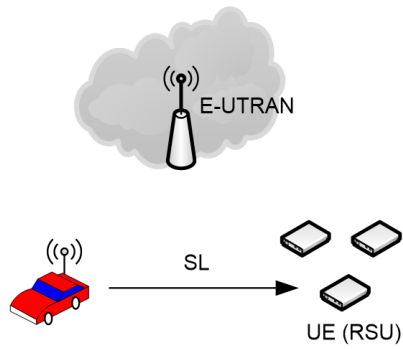
IoT Platform, Communication network, IoT eco-system

Use in the Project	NB-IoT is a promising brand-new standard which can be considered by AUTOPILOT architecture during the design phase. To be considered also the possibility of development of NB-IoT-enabled sensors.
Author /Company	ISMB

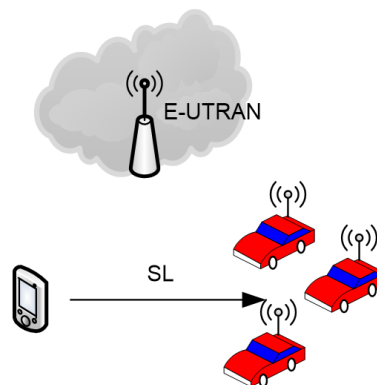
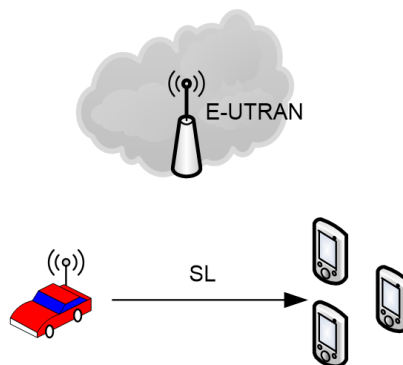
3GPP: Release 14 LTE-based V2X Services

Standardization body	3rd Generation Partnership Project (3GPP)
Standard No.	3GPP - Release 14
Standard Title	Technical Specification Group Radio Access Network; Study on LTE-based V2X Services
URL	http://www.3gpp.org/dynareport/36885.htm
Country	International
Status	Draft. To be published with R14
Date	03/2017
Aim	<p>The document contains the results and findings from the study item, “Feasibility Study on LTE-based V2X Services”. The purpose of this TR is to document the identified LTE enhancements and corresponding evaluations for LTE-based V2X services defined in as follows:</p> <ul style="list-style-type: none"> - V2V (vehicle-to-vehicle): covering LTE-based communication between vehicles. - V2P (vehicle-to-pedestrian): covering LTE-based communication between a vehicle and a device carried by an individual (e.g. handheld terminal carried by a pedestrian, cyclist, driver or passenger). - V2I/N (vehicle-to-infrastructure/network): covering LTE-based communication between a vehicle and a roadside unit/network. A roadside unit (RSU) is a stationary infrastructure entity supporting V2X applications that can exchange messages with other entities supporting V2X applications. Note: RSU is a term frequently used in existing ITS specifications, and the reason for introducing the term in the 3GPP specifications is to make the documents easier to read for the ITS industry. RSU is a logical entity that combines V2X application logic with the functionality of an eNB (referred to as eNB-type RSU) or UE (referred to as UE-type RSU). <p>This document addresses LTE-based V2X both with and without LTE network coverage, and covers both the operating scenario where the carrier(s) is/are</p>

	<p>dedicated to LTE-based V2X services (subject to regional regulation and operator policy including the possibility of being shared by multiple operators) and the operating scenario where the carrier(s) is/are licensed spectrum and also used for normal LTE operation.</p> <p>This technical report contains the evaluation methodology for LTE-based V2V, V2I/N and V2P services to compare the performance of different technical options.</p> <p>This document identifies necessary enhancements to LTE for support of PC5 transport for V2V services.</p> <p>This document captures identification and evaluation of Uu transport for V2V and PC5/Uu transport for V2I/N and V2P services.</p> <p>This document is a 'living' document, i.e. it is permanently updated and presented to TSG-RAN meetings.</p> <p>The document is also linked to two Work Items:</p> <ul style="list-style-type: none"> • Support for V2V services based on LTE sidelink (RP-161272) • Support for LTE-based V2X Services (RP-161298) <p>A liaison statement has been issued by 3GPP (RP-161788) towards ETSI TC ITS in 2017 and labelled as ITS(17)0000002 in the ETSI portal. A reply has been sent to 3GPP and is available as ITS(17)0000026 in the ETSI portal.</p>
<p>Description</p>	<p>As part of the expansion of the LTE platform to new services, and to keep track with the increasing needs of the automotive industry, 3GPP started to work on developing functionality to provide enhancements specific for vehicular communications both in terms of direct communication between vehicles, and vehicles to pedestrian/infrastructure, and cellular communications with networks as sketched in the following Figures.</p> <div data-bbox="710 1232 1157 1646">  </div> <p>(a) V2V operation</p>



(b) V2I operation



(c) V2P operation

Keyword	Communication and Connectivity, Devices and sensor technologies, Integration and Interoperability, Infrastructure, IoT Architecture
Autopilot Area involved	IoT Platform, Communication network, Vehicle IoT Integration and platform, IoT eco-system
Use in the Project	This standard will be considered while it is implemented the pilot sites with RSUs complying with 3GPP release 13, migration to R14 first in terms of connected field components (OBUs, RSUs) thus implementing PC5 at 5.9 GHz, and in turn at radio infrastructure level.
Author /Company	CNIT

3GPP: Security aspect for LTE support of V2X services (release 14)

Standardization body	3 rd Generation Partnership Project – 3GPP http://www.3gpp.org/
Standard No.	3GPP TS 33.185 V1.0.0
Standard Title	Technical Specification Group Services and System Aspects: Security aspect for LTE support of V2X services (release 14)
URL	http://www.3gpp.org/ftp//Specs/archive/33_series/33.185/33185-100.zip
Country	International,
Status	Draft – Presented for Information
Date	2017 – March
Aim	This document specifies the security aspects of V2X features in LTE, including <u>security architecture</u> , <u>security requirements</u> on the network entities that are used to support V2X services, as well as the <u>procedures</u> and <u>solutions</u> which are provided to meet those requirements.
Description	<p>V2X Security Architecture: The overall architecture describing LTE enhancements for V2X services is given in TS 23.285.</p> <p>V2X Security Requirements: the service requirements for V2X services are specified in 3GPP TS 22.185; <u>requirements for V2X</u>:</p> <ul style="list-style-type: none"> • Interface between network elements • Interface between UE and V2X control function (V3) • Interface between external provider and 3GPP network (MB2) • Security requirements of V2X application data

	<ul style="list-style-type: none"> Privacy related requirements V2X Security Solutions: features that are available for V2X services <ul style="list-style-type: none"> V2X communication between network elements V2X communication between UE and V2X Control Function (V3) Interface between V2X application server and 3GPP network (MB2) Security of V2X application data Privacy in V2X Services
Keyword	Security aspects, security Architecture, Security Requirements, Vehicular Communication Services
Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform, Communication network, IoT eco-system
Use in the Project	This document can be used as a guideline in the AUTOPILOT WP1 architecture phase, with reference to the Security Aspect in T1.5 Security, Privacy and Data Specification
Author /Company	THALES

6.2.2 ETSI (TC ITS)

ETSI EN 302 636 series ITS; Vehicular Communications; GeoNetworking

Standardization body	ETSI (TC ITS)
Standard No.	ETSI EN 302 636-1 Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements ETSI EN 302 636-2 Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 2: Scenarios ETSI EN 302 636-3 Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network Architecture ETSI EN 302 636-4-1 V1.2.1 (2014-07) 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 ETSI EN 302 636-5-1 V1.2.1 (2014-08) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol ETSI EN 302 636-6-1 V1.2.1 (2014-05) Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols
Standard Title	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network architecture See above

URL	http://www.etsi.org/deliver/etsi_en/302600_302699/30263601/01.02.01_60/en_30263601v010201p.pdf http://www.etsi.org/deliver/etsi_en/302600_302699/30263602/01.02.01_60/en_30263602v010201p.pdf http://www.etsi.org/deliver/etsi_en/302600_302699/30263603/01.02.01_60/en_30263603v010201p.pdf http://www.etsi.org/deliver/etsi_en/302600_302699/3026360401/01.02.01_60/en_3026360401v010201p.pdf http://www.etsi.org/deliver/etsi_en/302600_302699/3026360501/01.02.01_60/en_3026360501v010201p.pdf http://www.etsi.org/deliver/etsi_en/302600_302699/3026360601/01.02.01_60/en_3026360601v010201p.pdf
Country	Europe
Status	ETSI EN 302 636-1 V1.2.1: published (2014-04) ETSI EN 302 636-2 V1.2.1: published (2013-11) ETSI EN 302 636-3 V1.2.1: published (2014-12) ETSI EN 302 636-4-1 V1.2.1published (2014-07) ETSI EN 302 636-4-1 V1.2.1: published (2014-07) ETSI EN 302 636-5-1 V1.2.1: published (2014-08) ETSI EN 302 636-6-1 V1.2.1: published (2014-05)
Date	See above
Aim	ETSI EN 302 636 is a series of European norms that specify the networking and transport layer protocols, namely GeoNetworking protocol and the Basic Transport Protocol (BTP), for dissemination of messages over geographical areas. GeoNetworking is a network-layer protocol for mobile ad hoc communication based on wireless technology. GeoNetworking utilizes geographical positions for dissemination of information and transport of data packets. Variants of GeoNetworking have been proposed for vehicular ad hoc networks (VANETs); in VANETs, GeoNetworking provides wireless communication among vehicles and among vehicles and fixed stations along the roads.
Description	<p><u>ETSI EN 302 636-1</u> specifies, at an abstract level, the general, functional and performance requirements that apply to the GeoNetworking protocols for use in ETSI ITS G5 access technology.</p> <p><u>ETSI EN 302 636-2</u> classifies and specifies all communication scenarios that are supported by GeoNetworking. The communication scenarios for GeoNetworking can be classified in two ways:</p> <ul style="list-style-type: none"> by connection multiplicity and addressing mode (address or location): <ul style="list-style-type: none"> Point-to-point: communication from an ITS station to another; Point-to-multipoint: communication from an ITS station to multiple ITS stations; GeoAnycast: communication from an ITS station to an arbitrary ITS station within a geographical target area; GeoBroadcast: communication from an ITS station to all ITS stations within a geographical target area; by direct or indirect usage of the GeoNetworking protocol: <ul style="list-style-type: none"> Direct mode: applications directly access the ITS network and

- transport layer, e.g. safety and traffic efficiency applications;
- Indirect mode: applications indirectly access the ITS network and transport layer, i.e. applications access the ITS network and transport layer via an intermediate layer such as IPv6.

ETSI EN 302 636-3 specifies the network architecture for communication-based Intelligent Transport Systems (ITS) using different ITS access technologies. The network architecture is focused on, but not limited to, vehicular communication. The architecture enables a wide range of ITS applications for road safety, traffic efficiency as well as for infotainment and business. The standard first introduces a generic, high-level system view of the network architecture, that is based on the ITS architecture specified in ETSI EN 302 665 and represents the networking viewpoint of the overall architecture. The network architecture comprises internal and external networks; external networks interconnect ITS stations among each other or connect ITS stations to other network entities. Four basic deployment scenarios are then defined, to adapt to specific economical and regulatory conditions and to facilitate a gradual introduction of ITS. A deployment scenario is a subset of the overall architecture created by a combination of the different network types in support of the communication scenarios specified in ETSI EN 302 636-2. Based on the system view, the standard identifies and describes the main network components and specifies network reference points among them. The central component of the architecture is the ITS station; for this component, an overview of its protocol architecture is given and different options of using the GeoNetworking protocol in combination with transport protocols and protocols of the IP suite are described; the protocol stack of an ITS station basically follows the ISO/OSI reference model. Finally, the standard defines high-level logical functions to be considered in the design of ITS networking and transport protocols, such as ad hoc communication, addressing, resource management and data congestion control, integration with protocols of the IP suite and others.

ETSI EN 302 636-4-1 specifies the media-independent functionality of the GeoNetworking protocol. The GeoNetworking protocol is a network layer protocol supports the communication among individual ITS stations by providing the transport of packets in the ITS ad hoc network. It shall support the requirements specified in ETSI EN 302 636-1 and the scenarios specified in ETSI EN 302 636-2. The GeoNetworking protocol provides services to upper protocol entities, i.e. the ITS Transport Protocol, such as the Basic Transport Protocol (BTP) as specified in ETSI EN 302 636-5-1, and the GeoNetworking to IPv6 Adaptation Sub-Layer (GN6ASL) as specified in ETSI EN 302 636-6-1. GeoNetworking can be executed over different ITS access technologies for short-range wireless technologies. The standard defines the functionalities common to all ITS access technologies for short-range wireless communication to be used for GeoNetworking. In particular the standard defines:

- the services provided by the the GeoNetworking protocol;
- the basic convention for the specification of packet formats;
- the GeoNetworking packet structure and formats, providing further details about the GeoNetworking address;
- the data structures that a GeoAdhoc router shall maintain (the GeoAdhoc router is the ad hoc router that implements the

	<p>GeoNetworking protocol);</p> <ul style="list-style-type: none"> the media-independent operations of the GeoNetworking protocol. <p><u>ETSI EN 302 636-5-1</u> specifies the Basic Transport Protocol (BTP) for the transport of packets among ITS stations. The Basic Transport Protocol (BTP) shall support the requirements specified in ETSI EN 302 636-1 and the scenarios specified in ETSI EN 302 636-2. The BTP is a lightweight protocol that provides an end-to-end, connection-less transport service in the ITS ad hoc network. It provides an unreliable transport of packets, i.e. packets can arrive out-of-order, appear duplicated or can be lost. The BTP provides services to ITS facilities layer protocol entities, such as cooperative awareness basic service and DEN basic service. In order to provide its packet transport services, BTP uses the services of the GeoNetworking protocol (ETSI EN 302 636-4-1). The standard defines:</p> <ul style="list-style-type: none"> the services provided by the Basic Transport Protocol; the basic convention for the specification of packet formats; the BTP packet structure, providing further details about the BTP header; the operations of a BTP entity for sending and receiving a BTP-PDU (Protocol data Unit) <p><u>ETSI EN 302 636-6-1</u> specifies the transmission of IPv6 packets over the ETSI GeoNetworking protocol as defined in ETSI EN 302 636-4-1 via a protocol adaptation sub-layer referred to as the GN6ASL (GeoNetworking to IPv6 Adaptation Sub-Layer).</p> <p>The GeoNetworking protocol satisfies the requirements of several ITS services, whose application domain is limited to networks that are disconnected from large existing network infrastructures. However, several ITS applications require the integration of ITS stations with larger networks such as private transport networks or the Internet. In order to connect networks based on GeoNetworking to networks running the Internet Protocol (IP) it is necessary to allow GeoNetworking ITS stations to act like Internet hosts or routers. The ETSI Technical Committee ITS recognizes IP version 6 as the primary version of IP to be necessarily supported by ITS stations. The GN6ASL allows the GeoNetworking protocol, given in ETSI EN 302 636-4-1, to transport IPv6 packets without introducing modifications to existing IPv6 protocol implementations. Furthermore the GN6ASL allows for geocasting of IPv6 multicast packet.</p>
Keyword	Infrastructure, Communication and Connectivity
Autopilot Area involved	Communication network, Vehicle IoT Integration and platform
Use in the Project	This standard can be used both for WP1 and for WP3
Author /Company	TIM

ETSI EN 302 637-3 V1.2.2 - DENM

Standardization	ETSI (TC ITS)
------------------------	---------------

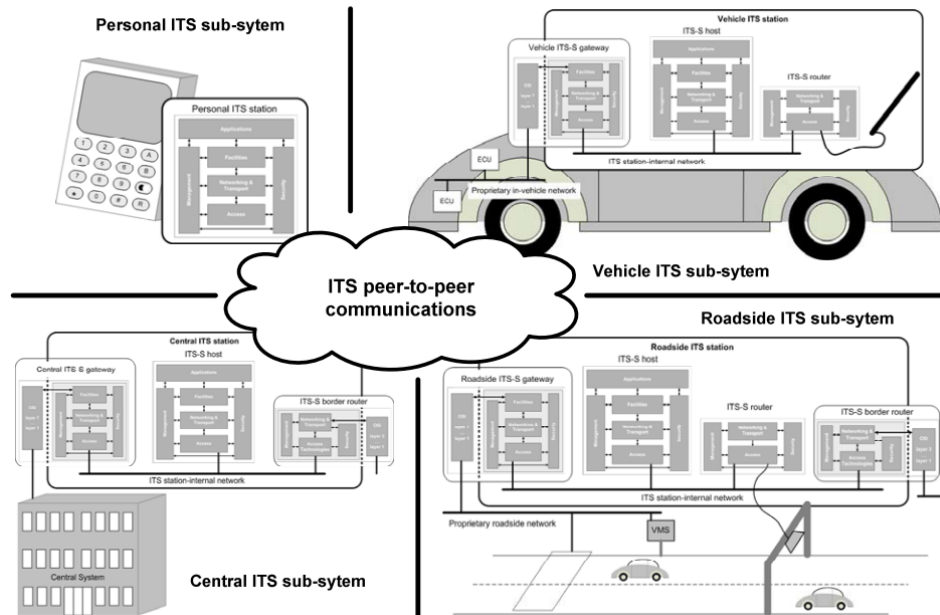
body	
Standard No.	ETSI EN 302 637-3 V1.2.2
Standard Title	DENM Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service
URL	http://www.etsi.org/deliver/etsi_en/302600_302699/30263703/01.02.02_60/en_30263703v010202p.pdf
Country	Europe
Status	Published
Date	11/2014
Aim	To disseminate information related to the abnormalities on the road
Description	The Decentralized Environmental Notification Message (DENM) is a message format that implements the decentralized environmental notification (DEN) basic service. The objective of this service along with its DENM message is to provide the functionality of Road Hazard Warning (RHW) within the ETSI ITS Basic Set of Applications framework. DENM messages are created and triggered by an ITS application and contain information related to anomalies on the road. Such anomalies include a hazard on the road or abnormal traffic conditions. The information included in the DENM message includes the type of abnormality, which enables to identify the road situation and also to evaluate the criticality of the abnormality. Moreover, the position of the occurrence of such abnormality is also indicated in the DENM message. The DENM messages are typically generated by any ITS station and are disseminated via the ITS networking & transport layer to vehicles located in a geographical area through direct vehicle-to-vehicle or vehicle-to-infrastructure communications. An ITS application receiving this information may then initiate an appropriate procedure based on this information, such as to warn a driver about the hazard - if the information is relevant to the driver.
Keyword	Communication and Connectivity; Integration and interoperability; Application.
Autopilot Area involved	Vehicle IoT Integration and platform, Communication network
Use in the Project	This message could be used to communicate any type of hazard with short-range V2x communications.
Author /Company	ISMB

ETSI EN 302 637-2 V1.3.2 - CAM

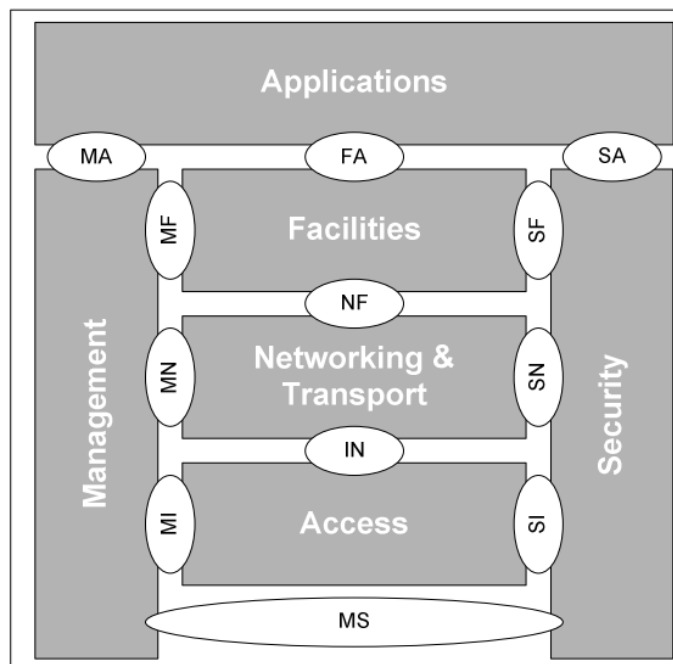
Standardization body	ETSI (TC ITS)
Standard No.	ETSI EN 302 637-2 V1.3.2
Standard Title	CAM Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service
URL	http://www.etsi.org/deliver/etsi_en/302600_302699/30263702/01.03.02_60/en_30263702v010302p.pdf
Country	Europe
Status	Published
Date	11/2014
Aim	To disseminate information related to the car and its dynamics
Description	Cooperative Awareness Messages implement the cooperative awareness within the road traffic. The information contained in the CAM messages is used to indicate to other users and roadside units about each other's position, dynamics and attributes. The information contained in CAM messages serves as a basis for several road and traffic efficiency applications. These messages are generated and processed by all kind of road users, which include but are not limited to cars, bicycles, trucks, roadside units, traffic lights and pedestrians, etc. These messages are typically generated at regular intervals to update the information on other actors on the road. Such exchange of messages is typically achieved by V2X and V2I communications. The generation, management and processing of the CAM messages is done by the Cooperative Awareness basic service (CA basic service) and is mandatory for all ITS stations, which take part in the road traffic.
Keyword	Communication and Connectivity; Integration and interoperability; Applications
Autopilot Area involved	Vehicle IoT Integration and platform, Communication network
Use in the Project	This message is the base for all the applications that needs to have information about the surrounding of the car.
Author /Company	ISMB

ETSI EN 302 665 V1.1.1 - ITS; Communications Architecture

Standardization body	ETSI (TC ITS)
Standard No.	EN 302 665 v1.1.1
Standard Title	Intelligent Transport Systems (ITS); Communications Architecture of ITS stations
URL	http://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf
Country	Europe
Status	Published (v1.1.1),
Date	2010-09
Aim	ETSI EN 302 665 specifies the global communication architecture of communications for Intelligent Transport Systems (ITSC) supporting a variety of existing and new access technologies and ITS applications. The term ITSC denotes communications protocols, related management and additional functionality.
Description	<p>ETSI EN 302 665 specifies the global framework of ITS communications in the road transport domain. The standard specifies:</p> <ul style="list-style-type: none"> • basic architectural elements of ITSC; • the general management of ITS applications with respect of ITSC; • general parts of the: <ul style="list-style-type: none"> ○ ITSC OSI protocol stack; ○ ITSC management entity; ○ ITSC security entity. <p>The standard also describes examples of possible implementations of ITS stations. With reference to the basic architectural elements of ITSC the following ITS sub-systems are identified (see below):</p> <ul style="list-style-type: none"> • personal ITS sub-system: in hand-held devices • central ITS sub-system: part of an ITS central system • vehicle ITS sub-system: in cars, trucks, etc., in motion or parked • roadside ITS sub-system: on gantries, poles, etc.



The ITS station reference architecture (see below) explains the functionality contained in the above listed ITS stations.



Related to ITS applications, the general management of ITS applications, e.g. classification, prioritization and channel assignment, registration and secure maintenance, is specified. ITS-S applications reside in the block Applications of the ITS station reference architecture (see above). ITS applications are initially grouped into Road Safety, Traffic Efficiency and Other Applications. With reference to ITSC OSI protocol stack the standard provides general details of the ITSC access layer (AL), ITSC networking & transport layer and the ITSC facilities layer. These layers are parts of the ITS station reference architecture (see above).

The standard also specifies general details of the ITSC management entity, that is part of the ITS station reference architecture (see above) and the ITSC security entity that contains security functionality related to the ITSC

	communication protocol stack, the ITS station and ITS applications.
Keyword	IoT Architecture, Communication and Connectivity
Autopilot Area involved	Vehicle IoT Integration and platform, Communication network
Use in the Project	These standards can be used both for WP1 and for WP3
Author /Company	TIM

ETSI EN 302 895 V1.1.1 - LDM

Standardization body	ETSI (TC ITS)
Standard No.	ETSI EN 302 895 V1.1.1
Standard Title	LDM Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM)
URL	http://www.etsi.org/deliver/etsi_en/302800_302899/302895/01.01.01_60/en_302895v010101p.pdf
Country	Europe
Status	Published
Date	09/2014
Aim	To store information related to the objects that affect traffic on the road.
Description	In Intelligent Transport Systems (ITS), the Local Dynamic Map (LDM) maintains information of the objects that influence or are influenced by the road traffic. Road traffic signs and vehicles are some examples of the objects that are maintained in an LDM. The LDM provides information about these objects to other ITS applications, which utilize this information to perform the required functionality. The LDM is in fact a conceptual data store placed within an ITS station that contains information related to the ITS applications running on the station. Using this information the ITS application can provide service of road safety and traffic efficiency. The LDM is generated and created by data coming from various sources such as vehicles, infrastructure units, traffic centres, personal ITS stations, and on-board sensors and applications. Finally, the information stored in the LDM can be requested and accessed by authorized application to improve road mobility.
Keyword	Communication and Connectivity; Integration and interoperability; Applications

Autopilot Area involved	Vehicle IoT Integration and platform, Communication network
Use in the Project	Used to store any useful information about the surrounding of a vehicle. Could be extended to host IoT specific information.
Author /Company	ISMB

ETSI TS 101 556-2 V1.1.1 - ITS; Infrastructure to Vehicle Communication; Part 2: Communication system specification to support application requirements for TIS and TPG interoperability

Standardization body	ETSI (TC ITS)
Standard No.	TS 101 556-2 V1.1.1
Standard Title	Intelligent Transport Systems (ITS); Infrastructure to Vehicle Communication; Part 2: Communication system specification to support application requirements for Tyre Information System (TIS) and Tyre Pressure Gauge (TPG) interoperability
URL	http://www.etsi.org/deliver/etsi_ts/101500_101599/10155602/01.01.01_60/ts_10155602v010101p.pdf
Country	International
Status	Published
Date	2017-02
Aim	The standard provides a specification of the communication system required to support the requirements of Tyre Information System (TIS) application, TPG (Tyre Pressure Gauge) application and TPG operator application.
Description	The TIS application has the objective to monitor in real time the pressure of the vehicle tyres, to advise the driver and to support him for the tyre(s) refilling if one or several tyre(s) are not at the recommended pressure. TPG application and TPG operator application have the objective to notify the TPG to road users and provide tyre pressure refilling service to vehicles, either manually, or automatically. Consequently, the communication system specification considers the various phases of the driver support process starting with the provisioning of available Tyre Pressure Gauge (TPG) locations, pairing the vehicle with a selected TPG and ensuring the data elements exchange required for the selected TPG to refill the concerned tyre(s) until reaching recommended pressure(s). The present document is developed in accordance with requirements defined in CEN EN 16661 [1].
Keyword	ITS-G5

Autopilot Area involved	Mobile Communication network
Use in the Project	This standard can be used as reference for examining vehicle communication to support application requirements not only for tyre pressure interoperability but also general interoperability aspects of autonomous driving and IOT.
Author /Company	T-Systems

ETSI TS 102 894-1 V1.1.1 - SPAT/MAP

Standardization body	ETSI (TC ITS WG1)
Standard No.	ETSI TS 102 894-1 V1.1.1
Standard Title	SPAT/MAP Intelligent Transport Systems (ITS); Users and applications requirements; Part 1: Facility layer structure, functional requirements and specifications
URL	http://www.etsi.org/deliver/etsi_ts/102800_102899/10289401/01.01.01_60/ts_10289401v010101p.pdf
Country	Europe
Status	Published
Date	08/2013
Aim	To allow traffic light timing and phase information to be transmitted to, and decoded by a vehicle approaching at an intersection
Description	The SPAT service is related to the ITS applications requiring information about the phase and timing of the traffic light at the intersection of the road. This information can be transmitted by a road side ITS station to an approaching vehicle in the form of a standardized Signal Phase and Timing Message (SPAT). In particular, the message can indicate the current and planned traffic phase and timing information to the approaching vehicle. The vehicle's ITS station can then decode this message and provide it to the higher applications, which allow to use this information for safety at intersection or green light speed advisory applications. The roadside ITS station, should be connected to the traffic light controller system, in order to retrieve and transmit this information. While the vehicle's ITS station must match the SPAT with the intersection topology to correctly identify the intersection and lane to which the SPAT message is related. This mapping functionality is provided by the MAP service. The MAP service provides a mapping of the geographical information to the data requested by the application. Thus, in order for a vehicle to correctly identify the geographical location the SPAT message corresponds to, the vehicle's ITS application must

	utilize the MAP service.
Keyword	Communication and Connectivity; Integration and interoperability; Applications
Autopilot Area involved	Vehicle IoT Integration and platform, Communication network, IoT eco-system
Use in the Project	Useful to send standard information about phase/time of traffic lights
Author /Company	ISMB

ETSI TS 102 723-8 V1.1.1 - ITS; OSI cross-layer topics; Part 8: Interface between security entity and network and transport layer

Standardization body	ETSI (TC ITS)
Standard No.	TS 102 723-8 V1.1.1
Standard Title	Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 8: Interface between security entity and network and transport layer
URL	http://www.etsi.org/deliver/etsi_ts/102700_102799/10272308/01.01.01_60/ts_10272308v010101p.pdf
Country	International
Status	Published
Date	2017-02
Aim	ITS stations are complex systems that may be implemented in different ways. The standard aims to address the security interface from a functional point of view.
Description	The standard specifies interfaces between the ITS security entity and the ITS network and transport layers, including interface services and service primitives which are extensible in order to achieve general applicability. Additionally, it specifies related procedures and common parameters. The SN-SAP description in the present document is functional as according to the ISO model as modified by ETSI EN 302 665 [1].

Keyword	ITS-G5
Autopilot Area involved	Mobile Communication network
Use in the Project	This standard specifies important OSI cross-layer topics and addresses interfaces between security entities and network and transport layers. It is expected that security issues will have a very strong impact on test scenarios of the V2I and I2V communication technologies, i.e. under consideration of IOT security aspects.
Author /Company	T-Systems

ETSI TS 102 940 V1.21 - ITS; Security; ITS communications security architecture and security management

Standardization body	ETSI (TC ITS)
Standard No.	TS 102 940 V1.2.1
Standard Title	Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management
URL	http://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.02.01_60/ts_102940v010201p.pdf
Country	Europe
Status	Published
Date	2016-11 (V1.2.1)
Aim	The document specifies a security architecture for Intelligent Transport System (ITS) communications.
Description	<p>The purpose of the present document is to describe an architecture for the communication security of ITS.</p> <p>ETSI TS 102 940 identifies the functional entities required to support security in an ITS environment and the relationships that exist between the entities themselves and the elements of the ITS reference architecture defined in ETSI EN 302 665, based on the security services defined in ETSI TS 102 731.</p> <p>The document also identifies the roles and locations of a range of security services for the protection of transmitted information and the management of essential security parameters. These include identifier and certificate management, PKI processes and interfaces as well as basic policies and guidelines for trust establishment.</p> <p>The annex A.1 presents a functional description of the Cooperative-ITS Security Management System (CSMS) and the needed services and interfaces</p>

	that should be provided by the CSMS to support the life-cycle management of Trusted ITS Stations.
Keyword	Interoperability, ITS, Management, Security
Autopilot Area involved	Security architecture, Communication
Use in the Project	The described security architecture for Intelligent Transport System (ITS) communications is in general an important requirement for the AUTOPILOT project and the document provides especially important input for WP1.5 (Security, Privacy and Data Specification) and WP1.2 (IoT architecture and specification).
Author /Company	CETECOM

ETSI TS 103 191, TS 103 096, TS 102 869, TS 102 868, TS 102 871, TS 102 870, TS 102 859- ITS Testing, Conformance test specifications

Standardization body	ETSI (TC ITS)
Standard No.	<p>TS 103 191-1 V1.2.1- Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Facilities layer protocols and communication requirements for infrastructure services; Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma</p> <p>TS 103 191-2 V1.2.1 - Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Signal Phase And Timing (SPAT) and Map (MAP); Part 2: Test Suite Structure and Test Purposes (TSS & TP)</p> <p>TS 103 191-3 V1.2.1 - Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Signal Phase And Timing (SPAT) and Map (MAP); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)</p> <p>TS 103 096-1 V1.3.1 - Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 1: Protocol Implementation Conformance Statement (PICS)</p> <p>TS 103 096-2 V1.3.1 - Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 2: Test Suite Structure and Test Purposes (TSS & TP)</p> <p>TS 103 096-3 V1.3.1 - Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)</p> <p>TS 102 869-1 V1.5.1 - Intelligent Transport Systems (ITS); Testing;</p>

	<p>Conformance test specifications for Decentralized Environmental Notification Basic Service (DEN); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma</p> <p>TS 102 869-2 V1.5.1 - Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Decentralized Environmental Notification Basic Service (DEN); Part 2: Test Suite Structure and Test Purposes (TSS & TP)</p> <p>TS 102 869-3 - V1.5.1 - Intelligent Transport Systems (ITS); Testing; Conformance test specification for Decentralized Environmental Notification Messages (DENM); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)</p> <p>TS 102 868-1 V1.4.1 - Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Cooperative Awareness Basic Service (CA); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma</p> <p>TS 102 868-2 V1.4.1 - Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Cooperative Awareness Basic Service (CA); Part 2: Test Suite Structure and Test Purposes (TSS & TP)</p> <p>TS 102 868-3 V1.4.1 Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Cooperative Awareness Basic Service (CA); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)</p> <p>TS 102 870-1 V1.1.1 - Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking Basic Transport Protocol (BTP); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma</p> <p>TS 102 870-2 V1.1.1 - Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking Basic Transport Protocol (BTP); Part 2: Test Suite Structure and Test Purposes (TSS&TP)</p> <p>TS 102 870-3 V1.1.1 - Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Geonetworking Basic Transport Protocol (BTP); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)</p> <p>TS 102 871-1 V1.1.1 – Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma</p> <p>TS 102 871-2 V1.3.1 - Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 2: Test Suite Structure and Test Purposes (TSS & TP)</p> <p>TS 102 871-3 V1.3.1 - Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)</p> <p>TS 102 859-1 V1.2.1 - Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Transmission of IP packets over GeoNetworking; Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma</p> <p>TS 102 859-2 V1.2.1 - Intelligent Transport Systems (ITS); Testing;</p>
--	--

	<p>Conformance test specifications for Transmission of IP packets over GeoNetworking; Part 2: Test Suite Structure and Test Purposes (TSS&TP)</p> <p>TS 102 859-3 V1.2.1 - Intelligent Transport Systems (ITS); Testing;</p> <p>Conformance test specification for Transmission of IP packets over GeoNetworking; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)</p>
Standard Title	<p>ITS Testing, Conformance test specifications for:</p> <ul style="list-style-type: none"> • Signal Phase And Timing (SPAT) and Map (MAP) • ITS Security • Decentralized Environmental Notification Basic Service (DEN) • Cooperative Awareness Basic Service (CA) • GeoNetworking ITS-G5 • Geonetworking Basic Transport Protocol (BTP) • Transmission of IP packets over GeoNetworking
URL	<p>http://www.etsi.org/</p> <p>http://www.etsi.org/deliver/etsi_ts/103100_103199/10319101/01.02.01_60/ts_10319101v010201p.pdf</p> <p>http://www.etsi.org/deliver/etsi_ts/103100_103199/10319101/01.02.01_60/ts_10319101v010201p.pdf</p> <p>http://www.etsi.org/deliver/etsi_ts/103100_103199/10319102/01.02.01_60/ts_10319102v010201p.pdf</p> <p>http://www.etsi.org/deliver/etsi_ts/103100_103199/10319103/01.02.01_60/ts_10319103v010201p.pdf</p> <p>http://www.etsi.org/deliver/etsi_ts/103000_103099/10309601/01.03.01_60/ts_10309601v010301p.pdf</p> <p>http://www.etsi.org/deliver/etsi_ts/103000_103099/10309602/01.03.01_60/ts_10309602v010301p.pdf</p> <p>http://www.etsi.org/deliver/etsi_ts/103000_103099/10309603/01.03.01_60/ts_10309603v010301p.pdf</p> <p>http://www.etsi.org/deliver/etsi_ts/102800_102899/10286901/01.05.01_60/ts_10286901v010501p.pdf</p> <p>http://www.etsi.org/deliver/etsi_ts/102800_102899/10286902/01.05.01_60/ts_10286902v010501p.pdf</p> <p>http://www.etsi.org/deliver/etsi_ts/102800_102899/10286903/01.05.01_60/ts_10286903v010501p.pdf</p> <p>http://www.etsi.org/deliver/etsi_ts/102800_102899/10286801/01.04.01_60/ts_10286801v010401p.pdf</p> <p>http://www.etsi.org/deliver/etsi_ts/102800_102899/10286802/01.04.01_60/ts_10286802v010401p.pdf</p> <p>http://www.etsi.org/deliver/etsi_ts/102800_102899/10286803/01.04.01_60/ts_10286803v010401p.pdf</p> <p>http://www.etsi.org/deliver/etsi_ts/102800_102899/10287001/01.01.01_60/ts_10287001v010101p.pdf</p> <p>http://www.etsi.org/deliver/etsi_ts/102800_102899/10287002/01.01.01_60/ts_10287002v010101p.pdf</p>

	http://www.etsi.org/deliver/etsi_ts/102800_102899/10287003/01.01.01_60/ts_10287003v010101p.pdf http://www.etsi.org/deliver/etsi_ts/102800_102899/10287101/01.01.01_60/ts_10287101v010101p.pdf http://www.etsi.org/deliver/etsi_TS/102800_102899/10287102/01.03.01_60/ts_10287102v010301p.pdf http://www.etsi.org/deliver/etsi_TS/102800_102899/10287103/01.03.01_60/ts_10287103v010301p.pdf http://www.etsi.org/deliver/etsi_ts/102800_102899/10285901/01.02.01_60/ts_10285901v010201p.pdf http://www.etsi.org/deliver/etsi_ts/102800_102899/10285902/01.02.01_60/ts_10285902v010201p.pdf http://www.etsi.org/deliver/etsi_ts/102800_102899/10285903/01.02.01_60/ts_10285903v010201p.pdf
Country	Europe
Status	Published
Date	
Aim	These are test specifications for the different services and messages defined in the ITS standard.
Description	These specifications are the tests description for the various protocols (CA, MAP, SPAT, DEN, etc) that are used to validate if the implementations correctly employ the aforementioned protocols
Keyword	Conformance, Testing, Interoperability, Security
Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform, Communication network, IoT eco-system
Use in the Project	<p>These tests are important to validate the Autopilot ITS components. EGM contributes to the different Test Specifications and TTCN-3 tests which cover different parts of the specification and types of messages, like CAM, SPAT and DENM. To further enrich its experience, EGM participated in the last ITS Cooperative Mobility Services Plugtests Event 5, from 09-18 November 2016 at the port of Livorno, Italy.</p> <p>EGM is actually working with ETSI to port the tests into an open environment (eg the TITAN tool) and this can be used within Autopilot</p>
Author /Company	EGM

ETSI EG 202 798 V1.1.1 - ITS; Testing; Framework for conformance and interoperability testing

Standardization body	ETSI (TC ITS)
Standard No.	ETSI EG 202 798
Standard Title	Intelligent Transport Systems (ITS); Testing; Framework for conformance and interoperability testing
URL	http://www.etsi.org/deliver/etsi_eg/202700_202799/202798/01.01.01_60/eg_202798v010101p.pdf
Country	Europe
Status	Published
Date	2011-01 (V1.1.1)
Aim	<p>The scope of the present document is to support ITS projects on the development of test specifications for ITS base standards from ETSI, ISO, CEN and other "Standard Developing Organizations" (SDOs) by providing:</p> <ul style="list-style-type: none"> - An ITS testing framework for conformance testing. - An ITS testing framework for interoperability testing. <p>The testing framework proposed in the present document provides guidance for development of conformance and interoperability test strategies, test systems and the resulting test specifications for ITS.</p>
Description	<p>A protocol conformance and interoperability testing framework for ITS thus is essential for a systematic and consistent approach towards testing of globally applicable ITS communications equipment.</p> <p>The presented ITS testing framework is a set of guidelines for conformance testing and interoperability testing. It is based on the common architecture for communications in ITS from ETSI and ISO.</p> <p>It is referring explicitly to a consistent set of ITS base standards from ETSI and ISO but is not restricted to this set of ITS base standards. Further on, it is enabling in a sense, that a manufacturer can implement and test those functionalities, considered to be important for market access.</p> <p>Clause 5 provides an introduction to the ITS testing framework.</p> <p>Clause 6 provides guidelines for conformance testing, which includes:</p> <ul style="list-style-type: none"> • Identification of candidate "Implementations Under Test" (IUT); • Identification of reference points; • Identification of the ATM: <ul style="list-style-type: none"> - abstract protocol tester; - functional TTCN-3 test architecture. <p>Clause 7 provides guidelines for interoperability testing, which includes:</p> <ul style="list-style-type: none"> • Identification of candidate EUTs. • Identification of test scenarios. • Definition of test bed architecture. • Identification of test bed interfaces. <p>Clause 8 provides guidance to write test specifications and to develop TTCN-3 test suites:</p>

	<ul style="list-style-type: none"> • Developing "Implementation Conformance Statements" (ICS) or "Interoperable Functions Statement" (IFS) from base standards, if not already provided as part of the base standard. • Developing "Test Suite Structure and Test Purposes" (TSS&TP) from ICS and base standards. • Developing "Test Descriptions" (TDs) from base standards. • Developing ITS TTCN-3 test suite, e.g. naming conventions, code documentation, test case structure. <p>Annex A provides information on the generic approach for interoperability testing.</p>
Keyword	ITS, Testing, Conformance, Interoperability
Autopilot Area involved	Vehicle IoT Integration and testing, test specification
Use in the Project	The provided guidelines and templates from chapters 7 (guidelines for interoperability testing), 8.2 (Provision of Test suite structure & Test Purposes) and annex A (Introduction to Interoperability testing) are useful input for the AUTOPILOT WP2.5 (Pilot Readiness Verification) and WP3.1 (Pilot site test specification).
Author /Company	CETECOM

6.2.3 ETSI (TC Cyber Security)

ETSI TR 103 303 V1.1.1 - Protection measures for Critical Infrastructure

Standardization body	ETSI (TC Cyber Security) http://www.etsi.org
Standard No.	TR 103 303 V1.1.1
Standard Title	CYBER; Protection measures for ICT in the context of Critical Infrastructure
URL	http://www.etsi.org/deliver/etsi_tr/103300_103399/103303/01.01.01_60/tr_103303v010101p.pdf
Country	International
Status	Published
Date	2016 – April
Aim	This document reviews the roles and subsequent measures for the protection of any infrastructure for which loss or damage in whole or in part will lead to significant negative impact on one or more of the economic activity of the Stakeholders, the safety, security or health of the population, where such

	<p>infrastructure is hereinafter referred to as Critical Infrastructure (CI). The resulting measures and processes for Critical Infrastructure Protection (CIP) where the CI in whole or in part is composed of ICT technologies using Cyber-Security mechanisms are defined and relevant mechanisms to be implemented are identified.</p>
Description	<p>Definition of CI: In order to identify Critical Infrastructure(CI), this standard gives an initial clear definition of what constitutes a critical service.</p> <p>Identification of CI: Once definitions and criteria have been established, it is crucial to design and implement a process to create and maintain an up-to-date record of CI.</p> <p>Notification of CI: any organization believing that they either meet the relevant definition of CI or will do so in the near future, should notify the relevant government body.</p> <p>CIA (Confidentiality, Integrity, Availability): the conventional paradigm for provision of security features</p> <ol style="list-style-type: none"> 1. Confidentiality: ensure information remain confidential 2. Integrity: data modifications were detectable 3. Availability: this element covers a wide range of aspects, including: access control, identification, authentication, reliability, resilience and monitoring – for the purpose of assuring availability. <p>In like manner to CI integrity the problem of CI resilience is that the system is inherently mutable and in normal operations will be subject to stress that it will be expected to recover from.</p> <p>Measures for CIP:</p> <ul style="list-style-type: none"> • Protection lifecycle: <ul style="list-style-type: none"> ○ Plan ○ Detect ○ React ○ Recover • Planning measures • Detection measures • CIA based reaction measures <ul style="list-style-type: none"> ○ Integrity measures ○ Availability measures • Resilience and recovery measures: when a system has been compromised it is reasonable to assume that when it recovers it will perform the same set of functions – but the means to perform those functions will be different from those used prior to the compromise.
Keyword	Cyber, Access Control, Critical Infrastructure, Critical Infrastructure Protection, Public Key Infrastructure.
Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform, Communication network, IoT eco-system
Use in the Project	The described security architecture should be used as guideline in the AUTOPILOT architecture design phase, with particular reference to the T1.2, IOT architecture and specification, and T1.5 Security, Privacy and Data Specification.
Author /Company	THALES

ETSI TR 103 304 V1.1.1 - Protection in mobile and cloud services

Standardization body	ETSI (TC Cyber Security) http://www.etsi.org
Standard No.	TR 103 304 V1.1.1
Standard Title	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services
URL	http://www.etsi.org/deliver/etsi_tr/103300_103399/103304/01.01.01_60/tr_103304v010101p.pdf
Country	International
Status	Published
Date	2016 – July
Aim	<p>This document proposes a number of scenarios focusing on today's ICT and develops an analysis of possible threats related to PII in mobile and cloud based services. It also presents technical challenges and needs derived from regulatory aspects (lawful interceptions).</p> <p>The aim is to consolidate a general framework, in line with regulation and international standards, on top of which technical solutions for PII protection can be developed.</p>
Description	<p>This standard describes threats derived from the analysis of the nine different scenarios representing the most common and relevant situations described in the Annexes of the document.</p> <p>After having identified a number of criticalities in PII, the standard provides a summary of the general protection principles that have been defined in ISO/IEC 29100.</p> <p>The standard continues introducing two general Use Cases focusing on architectural aspects; the main distinction between the two Use Cases lays on the role of the Device Platform Provider, a Cloud Service Provider.</p> <p>There were defined actors and roles:</p> <p>Actors:</p> <ul style="list-style-type: none"> • Cloud Service Provider (CSP) • Cloud Service Partner (CSPa) • Cloud Service Customer (CSC) <p>Roles:</p> <ul style="list-style-type: none"> • PII Controller • PII Processor • Law Enforcement Authority (LEA) • Device Platform Provider (DPP) • Cloud Service User (CSu)
Keyword	Cyber, Anonymization, Cloud Service Customer, Cloud Service Partner, Cloud Service Provide, Cloud Service User, PII controller, PII principal, PII process, Threats, Trust.

Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform, Communication network, IoT eco-system.
Use in the Project	The described security architecture should be used as guideline in the AUTOPILOT architecture design phase, whit particular reference to the T1.2, IOT architecture and specification, and T1.5 Security, Privacy and Data Specification.
Author /Company	THALES

6.2.4 ETSI (TC ERM)

ETSI EN 300 674-2-1 V2.1.1 - TTT; Dedicated Short Range Communication (DSRC)-Harmonized standard - Road Side Units (RSU)

Standardization body	ETSI (TC ERM)
Standard No.	ETSI EN 300 674-2-1 V2.1.1
Standard Title	Transport and Traffic Telematics (TTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5 795 MHz to 5 815 MHz frequency band; Part 2: Harmonised Standard covering the essential requirements of article 3.2 of the Directive 2014/53/EU; Sub-part 1: Road Side Units (RSU)
URL	http://www.etsi.org/deliver/etsi_en/300600_300699/3006740201/02.01.01_60/en_3006740201v020101p.pdf
Country	International
Status	Published
Date	2017-02
Aim	<p>The document applies to Transport and Traffic Telematics (TTT) systems:</p> <ul style="list-style-type: none"> • with a Radio Frequency (RF) output connection and specified antenna or with an integral antenna; • for data transmission only; • operating on radio frequencies in the 5,725 GHz to 5,875 GHz Short Range Devices frequency band. <p>The applicability of the present document covers only the Road Side Units (RSU).</p>
Description	<p>This Harmonised European Standard (EN) has been produced by ETSI Technical Committee Electromagnetic compatibility and Radio spectrum Matters (ERM).</p> <p>The document has been prepared under the Commission's standardization request C(2015) 5376 final [i.6] to provide one voluntary means of conforming to the essential requirements of Directive 2014/53/EU on the harmonization of the laws of the Member States relating to the making</p>

	<p>available on the market of radio equipment and repealing Directive 1999/5/EC [i.5].</p> <p>Once the document is cited in the Official Journal of the European Union under that Directive, compliance with the normative clauses of the document given in table A.1 confers, within the limits of the scope of the document, a presumption of conformity with the corresponding essential requirements of that Directive and associated EFTA regulations.</p> <p>The document is part 2, sub-part 2 of a multi-part deliverable covering Transport and Traffic Telematics (TTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5 795 MHz to 5 815 MHz frequency band, as identified below:</p> <p>Part 1: "General characteristics and test methods for Road Side Units (RSU) and On-Board Units (OBU)";</p> <p>Part 2: "Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU";</p> <p>Sub-part 1: "Road Side Units (RSU)";</p> <p>Sub-part 2: "On-Board Units (OBU)".</p>
Keyword	ITS-G5
Autopilot Area involved	Mobile Communication network
Use in the Project	Several Autopilot test sites have to consider the usage of OBU (vehicle based) equipment. DSRC is a well-established and stable communication technology between road-side equipment and moving vehicles, which can be used for reference for communication purposes
Author /Company	T-Systems

ETSI EN 300 674-2-2 V2.1.1 - TTT; Dedicated Short Range Communication (DSRC)-Harmonized standard - On-Board Units (OBU)

Standardization body	ETSI (TC ERM)
Standard No.	ETSI EN 300 674-2-2 V2.1.1
Standard Title	Transport and Traffic Telematics (TTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5 795 MHz to 5 815 MHz frequency band; Part 2: Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU; Sub-part 2: On-Board Units (OBU)
URL	http://www.etsi.org/deliver/etsi_en/300600_300699/3006740202/02.01.01_60/en_3006740202v020101p.pdf

Country	International
Status	Published
Date	2017-02
Aim	<p>The document applies to Transport and Traffic Telematics (TTT) systems:</p> <ul style="list-style-type: none"> - with a Radio Frequency (RF) output connection and specified antenna or with an integral antenna; - for data transmission only; - operating on radio frequencies in the 5 725 MHz to 5 875 MHz Short Range Devices frequency band. <p>The applicability of the present document covers only the On Board Units (OBU).</p> <p>The document does not necessarily include all the characteristics which may be required by a user, nor does it necessarily represent the optimum performance achievable.</p>
Description	<p>The present document complies with the Commission Implementing Decision 2013/752/EU [1] and CEPT/ERC Recommendation 70-03 [2]. It is a specific standard covering various TTT applications.</p> <p>The present document applies to the following radio equipment types operating in all or in part of the following service frequency bands given in table 1.</p> <p>Table 1: Frequency bands and centre frequencies fTx allocated for DSRC</p> <p>Pan European Service Frequencies National Service Frequencies</p> <p>Channel 1 5,795 GHz to 5,800 GHz, fTx = 5,7975 GHz</p> <p>Channel 2 5,800 GHz to 5,805 GHz, fTx = 5,8025 GHz</p> <p>Channel 3 5,805 GHz to 5,810 GHz, fTx = 5,8075 GHz</p> <p>Channel 4 5,810 GHz to 5,815 GHz, fTx = 5,8125 GHz</p> <p>The present document contains requirements to demonstrate that radio equipment</p>
Keyword	ITS-G5
Autopilot Area involved	Mobile Communication network
Use in the Project	Several Autopilot test sites have to consider the usage of OBU (vehicle based) equipment. DSRC is a well-established and stable communication technology between road-side equipment and moving vehicles, which can be used for reference for communication purposes
Author /Company	T-Systems

ETSI EN 302 571 V2.0.0 – ITS; Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band, Harmonized Standard

Standardization	ETSI (TC ERM)
------------------------	---------------

body	
Standard No.	ETSI EN 302 571 V2.0.0
Standard Title	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
URL	http://www.etsi.org/deliver/etsi_en/302500_302599/302571/02.00.00_20/en_302571v020000a.pdf
Country	International
Status	Published
Date	2017-02
Aim	The document specifies technical characteristics and methods of measurement for radio transmitters and receivers operating in the frequency range 5 855 MHz to 5 925 MHz.
Description	The spectrum usage conditions are set out in ECC Decision (08)01 for the frequency range 5 875 MHz to 5 925 MHz (with 5 905 MHz to 5 925 MHz considered as a future ITS extension) and in ECC Recommendation (08)01 for the frequency range 5 855 MHz to 5 875 MHz. The Commission Decision 2008/671/EC [i.3] mandates a harmonized use of the frequency band 5 875 MHz to 5 905 MHz dedicated to safety-related applications of ITS throughout the member states of the European Union.
Keyword	ITS-G5, LTE-V2X, Communication and connectivity
Autopilot Area involved	Mobile Communication network
Use in the Project	The overall Autopilot concept is based on 4G/5G and LTE-V2X in combination with G5 technology of road side units placed along ITS application corridors, mainly roads. With regards to Autopilot test sites special, safety issues taking extreme test source voltages and regulated lead-acid battery power sources used on vehicles have to be considered, so that accident risks are minimized.
Author /Company	T-Systems

6.2.5 IEEE

IEEE 802.11p - Wireless local area networks - Wireless Access in Vehicular Environments

Standardization body	IEEE SA
Standard No.	IEEE 802.11p-2010: Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN

	Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments
Standard Title	See above
URL	https://standards.ieee.org/develop/wg/WG802.11.html
Country	International
Status	IEEE 802.11p: Published 2010 (Superseded standard)
Date	See above
Aim	This amendment specifies the extensions to IEEE Standard 802.11 for wireless local area networks (WLANs) providing wireless communications while in a vehicular environment.
Description	IEEE 802.11p is an approved amendment to add wireless access in vehicular environments (WAVE). It defines enhancements to 802.11 (Wi-Fi) required to support Intelligent Transportation Systems (ITS) applications. This includes data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure (V2X communication), in the licensed ITS band of 5.9 GHz. Both IEEE 1609 and ETSI ITS-G5 are based on IEEE 802.11p.
Keyword	WLAN, WiFi, V2X Communication (V2V, V2I).
Autopilot Area involved	Vehicle IoT Integration and platform. Communication network.
Use in the Project	Vehicle -to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications.
Author /Company	SINTEF

IEEE 802.15 - Wireless Personal Area Network (WPAN)

Standardization body	IEEE SA
Standard No.	IEEE 802.15.1-2005 IEEE 802.15.4-2015
Standard Title	Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 15.1a: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPAN).

	IEEE 802.15.4-2015: Standard for Low-Rate Wireless Networks.
URL	https://standards.ieee.org/develop/wg/WG802.15.html
Country	International
Status	IEEE 802.15.1: Published 2005 (Active standard) IEEE 802.15.4: Published 2015 (Active standard)
Date	See above
Aim	Wireless Personal Area Networks (WPAN) for short distance communications.
Description	<p>IEEE 802.15.1-2005: Methods for communicating devices in a personal area network (PAN) are covered in this standard. Prior basis for Bluetooth. (The IEEE standardized Bluetooth as IEEE 802.15.1, but no longer maintains the standard. The Bluetooth SIG oversees development of the specification, manages the qualification program, and protects the trademarks).</p> <p>IEEE 802.15.4-2015: The protocol and compatible interconnection for data communication devices using low-data-rate, low-power, and low-complexity short-range radio frequency (RF) transmissions in a wireless personal area network (WPAN) are defined in this standard. A variety of physical layers (PHYs) have been defined that cover a wide variety of frequency bands. Basis for the ZigBee, ISA100.11a, WirelessHART specifications.</p>
Keyword	V2D Communication, low data rate, short range,
Autopilot Area involved	IoT Platform. Vehicle IoT Integration and platform. IoT eco-system.
Use in the Project	Vehicle -to-Device (V2D) communications.
Author /Company	SINTEF

IEEE 802.20 - Mobile Broadband Wireless Access (MBWA)

Standardization body	IEEE SA
Standard No.	<p>IEEE 802.20-2008: Standard for Local and metropolitan area networks - Part 20: Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility - Physical and Media Access Control Layer Specification.</p> <p>IEEE 802.20.2-2010: Standard for Conformance to IEEE 802.20 Systems-- Protocol Implementation Conformance Statement (PICS) Proforma.</p>

	<p>IEEE 802.20.3-2010: Standard for Minimum Performance Characteristics of IEEE 802.20 Terminals and Base Stations/Access Nodes.</p> <p>IEEE 802.20a-2010: Standard for Local and metropolitan area networks--Part 20: Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility--Physical and Media Access Control Layer Specification Amendment 1: Management Information Base Enhancements and Corrigenda Items.</p> <p>IEEE 802.20b-2010: Standard for Local and metropolitan area networks--Virtual Bridged Local Area Networks - Amendment 15: Bridging of IEEE 802.20.</p>
Standard Title	See above
URL	https://standards.ieee.org/develop/wg/WG802.20.html
Country	International
Status	<p>IEEE 802.20: Published 2008 (Active standard)</p> <p>IEEE 802.20.2: Published 2010 (Active standard)</p> <p>IEEE 802.20.3: Published 2010 (Active standard)</p> <p>IEEE 802.20a: Published 2010 (Active standard)</p> <p>IEEE 802.20b: Published 2010 (Active standard)</p>
Date	See above
Aim	Specification for an efficient packet based air interface that is optimized for the transport of IP based services. The goal is to enable worldwide deployment of affordable, ubiquitous, always-on and interoperable multi-vendor mobile broadband wireless access (MBWA) networks that meet the needs of business and residential end user markets.
Description	Specification of physical and medium access control layers of an air interface for interoperable mobile broadband wireless access systems, operating in licensed bands below 3.5 GHz, optimized for IP-data transport, with peak data rates per user in excess of 1 Mbps. It supports various vehicular mobility classes up to 250 Km/h in a metropolitan area network (MAN) environment and targets spectral efficiencies, sustained user data rates and numbers of active users that are all significantly higher than achieved by existing mobile systems.
Keyword	MBWA, V2X Communication (V2V, V2I).
Autopilot Area involved	Vehicle IoT Integration and platform. Communication network.
Use in the Project	Vehicle -to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications.

Author /Company	SINTEF
------------------------	--------

IEEE P1609 Wireless Access in Vehicular Environments (WAVE)

Standardization body	IEEE
Standard No.	<p>1609.0 IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture</p> <p>1609.2 IEEE Standard for Wireless Access in Vehicular Environments-- Security Services for Applications and Management Messages</p> <p>1609.3 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services</p> <p>1609.4 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation</p> <p>1609.11 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)-- Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS)</p> <p>1609.12 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Identifier Allocations</p>
Standard Title	See above
URL	http://standards.ieee.org/develop/wg/1609_WG.html
Country	International
Status	<p>1609.0: published (2013)</p> <p>1609.2: published (2016)</p> <p>1609.3: published (2010)</p> <p>1609.4: published (2016)</p> <p>1609.11: published (2010)</p> <p>1609.12: published (2016)</p>
Date	See above
Aim	IEEE P1609 is a suite of standards for Wireless Access in Vehicular Environments (WAVE). They define architecture and standardizes a set of services and interfaces that enable secure wireless communication and physical access for high speed, short range and low latency wireless communication in the vehicular environment. This set of services and interfaces collectively enable secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications
Description	<p><u>IEEE 1609.0</u> describes the architecture and service necessary for WAVE devices to communicate in a mobile vehicular environment.</p> <p><u>IEEE P1609.2</u> defines secure message formats and processing for use by WAVE devices, including methods to secure WAVE management messages and methods to secure application messages. It also describes</p>

	<p>administrative functions necessary to support the core security functions. IEEE P1609.3 describes standard messages that support higher layer communication stacks, including TCP/IP. The WAVE Networking Services, defined in this standard, provides services to WAVE devices and systems. Layers 3 and 4 of the OSI model and the Internet Protocol (IP), User Datagram Protocol (UDP), and Transmission Control Protocol (TCP) elements of the Internet model are represented. Management and data services within WAVE devices are provided.</p> <p>IEEE P1609.4 describes various standard message formats for DSRC applications at 5.9 GHz; in particular this standard describes multi-channel wireless radio operations, WAVE mode, medium access control (MAC), and physical layers (PHYs), including parameters for priority access, channel switching and routing, management services, and primitives designed for multi-channel operations</p> <p>IEEE P1609.11 specifies the electronic payment service layer and profile for Payment and Identity authentication, and Payment Data transfer for DSRC based applications in Wireless Access in Vehicular Environments. This standard defines a basic level of technical interoperability (vehicle-to-roadside) for electronic payment equipment, i.e., onboard unit (OBU) and roadside unit (RSU) using WAVE. It does not provide a full solution for interoperability, and it does not define other parts of the electronic payment system, other services, other technologies and non-technical elements of payment interoperability. This standard is not intended to define technology and processes to activate and store data into the OBU (personalization), nor the applications using the payment service.</p> <p>IEEE P1609.12 specifies allocations of WAVE identifiers defined in the IEEE 1609 series of standards. Within the IEEE 1609 family of standards a number of identifiers are used; this standard describes the use of these identifiers, indicates identifier values that have been allocated for use by WAVE systems and specifies the allocation of values of identifiers specified in the WAVE standards</p>
Keyword	Communication and Connectivity, Security
Autopilot Area involved	Vehicle IoT Integration and platform, Communication network,
Use in the Project	These standards can be used both for WP1 and for WP3
Author /Company	TIM

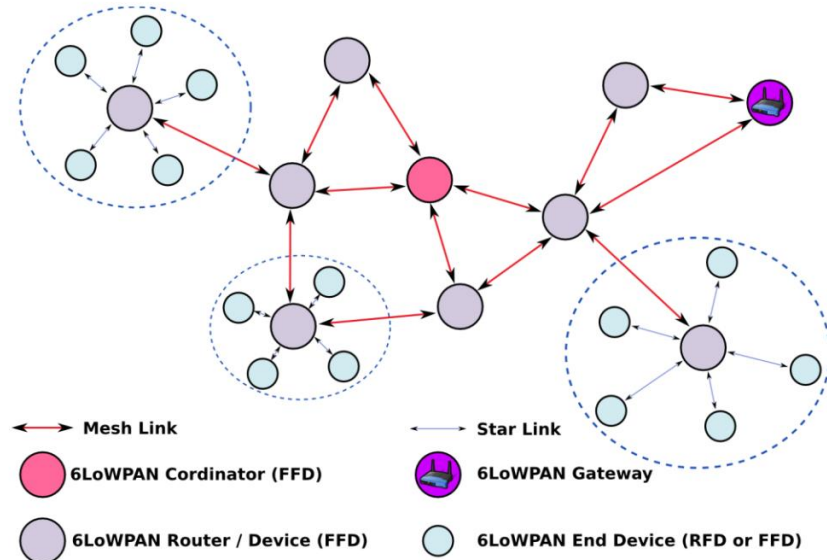
6.2.6 IETF

IETF: RFC 4944 Transmission of IPv6 Packets over IEEE 802.15.4 Networks

Standardization body	Internet Engineering Task Force (IETF)
-----------------------------	--

Standard No.	RFC 4944
Standard Title	Transmission of IPv6 Packets over IEEE 802.15.4 Networks
URL	https://www.rfc-editor.org/rfc/rfc4944.txt
Country	International
Status	Proposed
Date	February 2017
Aim	This document describes the frame format for transmission of IPv6 packets and the method of forming IPv6 link-local addresses and statelessly autoconfigured addresses on IEEE 802.15.4 networks. Additional specifications include a simple header compression scheme using shared context and provisions for packet delivery in IEEE 802.15.4 meshes.
Description	<p>The original goal of 6LoWPAN was to run IP on smart objects. For that purpose, an adaptation layer for IPv6 has been designed for 802.15.4 Low-power and Lossy Networks (LoWPANs or LLNs) on simple embedded devices. LLNs are constrained environments with special characteristics such as small packet size, low bandwidth (802.15.4) and low cost devices deployed in large scales. These embedded devices are low-power, small and cheap. They also use short-range, low-power wireless radios which have limited data rates, frame sizes and radio duty cycles. Thanks to the upper layer protocols running over IPv6/6LoWPAN, users/applications can perform restful interactions with the devices to manipulate the hosted.</p> <p>6LoWPAN architectures often consist of host and router nodes connected to one or several edge routers which share a common IPv6 address prefix. In fact, all network interfaces of 6LoWPAN nodes share the same IPv6 prefix distributed by the edge router and thereafter routers throughout the 6LoWPAN network.</p> <p>Three modes are available:</p> <ul style="list-style-type: none"> • Simple 6LoWPAN: nodes are connected through a single 6LoWPAN edge router to another IP network. The edge router (6LoWPAN Gateway) is in general directly connected to the Internet. It is responsible of 6LoWPAN compression and neighbour discovery. It also handles IPv6 forwarding on behalf of the nodes inside and outside the 6LoWPAN network. Reduced Function devices (RFDs) are simple nodes that are only capable to sense their environment and communicate this information to Full-Function Devices (FFDs). RFDs are extremely simple devices with low resources and communication requirements. FFDs can play the role of RFDs, but they support additional features. In fact, FFDs can serve as PAN coordinators, and relay data packets from one source node toward one destination node. • Extended 6LoWPAN: in that mode, several edge routers are used and shared a common backbone link. • Ad-hoc 6LoWPAN: this mode requires no infrastructure. In fact, this

type of 6LoWPAN is not connected to the Internet. For that purpose, one router must be configured as a simplified edge router, implementing Unique Local Unicast Address (ULA) generation and handling 6LoWPAN Neighbour Discovery registration. An IPv6 local prefix is advertised. Consequently, there are no routes outside the 6LoWPAN network.



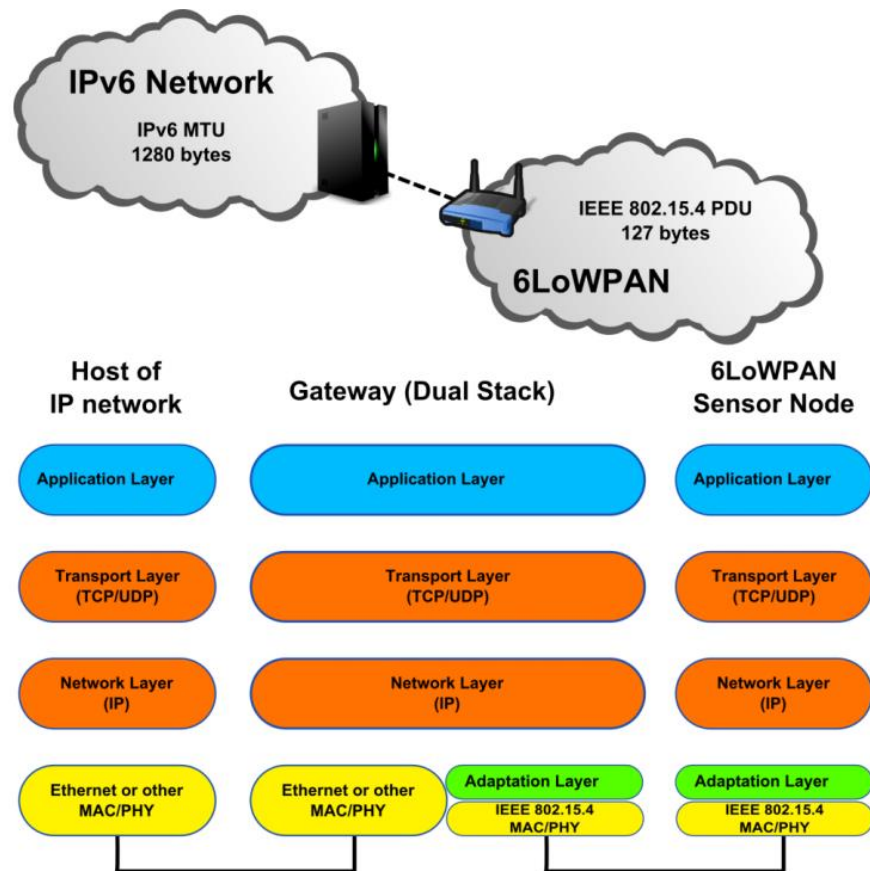
Simple 6LoWPAN network topology.

In fact, nodes register with an edge router through a Neighbour Discovery process that defines available interactions between hosts and routers on the same link. Nodes can be attached to more than one 6LoWPAN at the same time (multi-homing). They can be mobile. This will have a direct impact on the network topology that can also change due to the evolution of wireless channel conditions. Nodes can communicate with other IP nodes in an end-to-end manner. In fact, each 6LoWPAN node is identified by a unique IPv6 address, and can send and receiving IPv6 packets. In general, 6LoWPAN nodes

support ICMPv6 traffic such as ping, and use UDP as transport, due to their limitation in payload and processing capabilities. IP addressing with 6LoWPAN works just like in any IPv6 network. IPv6 addresses are typically formed automatically from the prefix of the 6LoWPAN and the link-layer address of the wireless interfaces. For

6LoWPAN technologies, a direct mapping between the link layer address and the IPv6 address is used for achieving compression. Adaptation between full IPv6 and the 6LoWPAN format is performed by edge routers. The 6LoWPAN gateway supports two protocol stacks, e.g. IP and 6LoWPAN stacks. The adaptation layer is located between the 802.15.4 link layer and the IP layer. It is the main component of 6LoWPAN. It enables TCP/IP communications above it. In fact, the adaptation layer is mandatory as the size of 802.15.4 frames do not permit to use conventional IPv6 packets. Within a 6LoWPAN network, IEEE 802.15.4 frame size is limited to 127 bytes. The Maximum Transfer Unit (MTU) within IPv6 networks rates 1280 bytes. So, header compression, fragmentation and re-assembling are handled by the adaptation layer. The adaptation layer also supports routing between the

6LoWPAN network and the remaining Internet.



Dual stack Gateway in a 6LoWPAN network.

6LoWPAN applications most often involve completely autonomous devices and networks which must auto-configure themselves. Bootstrapping (channel setting, default security key and address settings), performed by the link layer, permits to enable basic communication between nodes within a defined radio range. After this initialization, devices can operate single-hop communications. Afterwards 6LoWPAN Neighbour Discovery (ND) is used to bootstrap the whole network. In fact, the original IPv6 ND supports most basic bootstrapping and maintenance issues between nodes on IPv6 links. But without any modification, IPv6 ND remains not suitable for 6LoWPAN networks. Thus, 6lowpan-nd has been designed to describe auto-configuration and the operation of hosts, routers and edge routers. It is an important part of the bootstrapping process. A node uses ND to discover other nodes on the same links, to determine their link addresses, to find routers and to maintain reachability information about the paths to neighbours that the node is actively communicating with. The edge router updates a registry of the 6LoWPAN nodes to simplify IPv6 operations across the network and reduce the amount of flooding.

Contrary to WLAN commissioning where SSID (Service Set Identifier) and security information (key material) are used, a 6LoWPAN device can assume that it is connected to its network when the security parameters and keying material match. In that case Integrity check of incoming packets does not

	<p>fail. As a matter, of course, providing the network prefix, at the commissioning time would reduce the need for neighbor discovery router advertisements as nodes will automatically be aware of the 6LoWPAN where they are attached. The edge routers include the context information in their Route Advertisement (RA), making it available to all first hop routers, which disseminate it further down on the topology and so on. Addressing is also an important process that aims at assigning the IP address of 6LoWPAN nodes. During the design of IEEE 802.15.4, a 64-bit MAC address is assigned to each device, and afterwards it can be used as EUI-64. This identifier must be unique and can also be used as device ID by applications. A simple mechanism can be used for address configuration: Stateless Address Auto-configuration. In fact, it is based on Interface Identifier IID that is performed with each interface on the link, ensuring uniqueness at least per link. This IID is combined with a prefix to form an address.</p> <p>Security highlights:</p> <ul style="list-style-type: none"> – Applications: security can be handled by TLS or DTLS. – IPv6: IPSec is possible at the network layer but it consumes a lot of resources. Limitations in 6LoWPANs prevent the use of the full IPSec suite. The management of cryptographic keys using the minimum payload, and the limitation of exchanged messages between nodes are required. – 6LoWPAN: LSEND (Lightweight Secure Neighbour Discovery) is an extension of the protocol SEND that permits to secure the Neighbour Discovery mechanisms in 6LoWPAN networks. – 802.15.4 MAC: AES permits to secure the link layer. Link-layer security inside 6LoWPANs, based on the IEEE 802.15.4 128-bit AES encryption, provides some protection. – Authentication: resurrecting duckling model. – Confidentiality OK – Integrity OK – AES symmetric Encryption is used for confidentiality and integrity. AES/CCM is a quite efficient and very secure algorithm if the same nonce never occurs twice with the same key. So many applications will require rekeying within the lifetime of the 6LoWPAN network.
Keyword	Communication and Connectivity, Device and sensor Technology, Infrastructure
Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform, IoT eco-system
Use in the Project	6LowPAN can be used to bridge vehicular networks with IoT infrastructure. 6LowPAN can be also used for low power and short-range networking to enable specific services by the IoT infrastructure.
Author /Company	ISMB

6.2.7 ISO TC204

ISO/AWI 20900 PAPS Partially automated parking systems

Standardization body	ISO TC204 WG14
Standard No.	ISO/AWI 20900 PAPS
Standard Title	Partially automated parking systems
URL	https://www.iso.org/standard/69405.html
Country	International
Status	Under development
Date	2017
Aim	The aim of this standard is to help with the performance requirements and test procedures of Partially Automated Parking System (PAPS), which completes the whole task of the parking maneuvers controlling both longitudinal and lateral movement of the vehicle to mitigate driver's burden.
Description	<p>This International Standard for Partially Automated Parking System (PAPS) addresses light-duty vehicles, e.g. passenger cars, pick-up trucks, light vans and sport utility vehicles (motorcycles excluded), equipped with such PAPS. This standard establishes minimum functionality requirements that the driver/operator can expect and the manufacturer should take into account. Possible system configuration includes the following two types.</p> <ul style="list-style-type: none"> -Type 1: System being supervised by the driver located in the driver's seat. -Type 2: System being supervised by an operator (present within or outside the vehicle) that is not necessarily located in the driver's seat. <p>For both types, minimum requirements and conditions of safety, system performance and function including HMI information content and every system operating mode of searching, engaging, controlling, and ending are addressed.</p> <p>The requirements include the driver or operator who supervises the safety throughout the system manoeuvres.</p> <p>Also system test requirements are addressed including test criteria, method, and conditions.</p>
Keyword	<ul style="list-style-type: none"> - Integration and interoperability - Devices and sensor technology - Applications
Autopilot Area involved	Vehicle IoT Integration and platform

Use in the Project	This standard is used to manage test procedures and performance requirements related to partially automated parking system use cases. We reference it as a possible baseline for some of the functions of Pilot Sites which PAPS is involved.
Author /Company	IDIADA

ISO TC204 WG14 - Automated Valet Parking System

Standardization body	ISO TC204 WG14
Standard No.	New Topic (Automated Valet Parking System)
Standard Title	Unknown (New Topic)
URL	Not available yet.
Country	International
Status	Under development
Date	Not released (2017).
Aim	This information will be provided once the standard is released.
Description	This information will be provided once the standard is released.
Keyword	<ul style="list-style-type: none"> - Integration and interoperability - Devices and sensor technology - Applications
Autopilot Area involved	Vehicle IoT Integration and platform
Use in the Project	This standard is used to manage procedures related to automated valet parking use cases. We reference it as a possible baseline for some of the functions of Pilot Sites which automated valet parking is involved.
Author /Company	IDIADA

ISO/CD 20035 C-ACC Cooperative Adaptive Cruise Control - Performance requirements and test procedures

Standardization body	ISO TC204 WG14
-----------------------------	----------------

Standard No.	ISO/CD 20035 C-ACC res
Standard Title	Cooperative Adaptive Cruise Control - Performance requirements and test procedure
URL	https://www.iso.org/standard/66879.html
Country	International
Status	Under development
Date	2017
Aim	Cooperative Adaptive Cruise Control is fundamentally intended to provide longitudinal control of equipped vehicles while travelling on highways (roads where non-motorized vehicles and pedestrians are prohibited) under free-flowing traffic conditions. ACC can be augmented with other capabilities, such as forward obstacle warning.
Description	<p>Cooperative Adaptive Cruise Control (CACC) system International Standard is an expansion to existing ACC control strategy by using wireless communication with preceding vehicles (V2V) and/or the infrastructure (I2V). Both multi vehicle V2V data and I2V infrastructure data are within the scope of this standard. When V2V data is used CACC could enable shorter time gaps and more accurate gap control, which can help increase traffic throughput and reduce fuel consumption. It can also receive data from the infrastructure, such as recommended speed and time gap setting, to improve traffic flow and safety. The Scope of the CACC System International Standard will address two types of CACC: V2V, and I2V. Both CACC systems require active sensing using for example radar, lidar, or camera systems. The combined V2V and I2V CACC are not addressed in this standard. The following requirements will be addressed in this standard:</p> <ul style="list-style-type: none"> – Classification of the types of CACC. – Definition of the performance requirements for each CACC type. – CACC state transitions diagram. – Minimum set of wireless data requirements. – Test procedures. <p>CACC:</p> <ul style="list-style-type: none"> - Only longitudinal vehicle speed control. - Uses time gap control strategy similar to ACC. - Has similar engagement criteria as ACC. <p>Coordinated strategies to control group of vehicles, such as platooning, in which vehicles controllers base their control actions on how they affect other vehicles, and may have a very short following clearance gap are not within the scope of this of this standard. CACC system operates under driver responsibility and supervision.</p> <p>Motor vehicle including light vehicle and heavy vehicle are covered in the scope of this standard.</p>
Keyword	<ul style="list-style-type: none"> - Integration and interoperability - Devices and sensor technology - Applications - Communication and connectivity

Autopilot Area involved	Vehicle IoT Integration and platform
Use in the Project	This standard is used to manage test procedures and performance requirements related to C-ACC use cases. We reference it as a possible baseline for some of the functions of Pilot Sites which C-ACC is involved.
Author /Company	IDIADA

6.2.8 ISO TC 22 / SC 31

ISO 15118 - Data communication

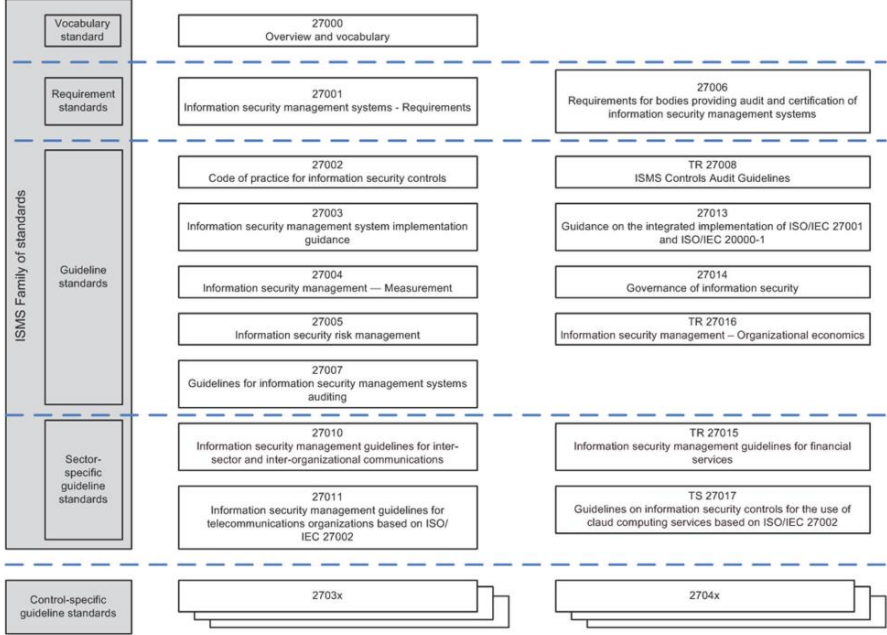
Standardization body	ISO (TC 22/SC 31)
Standard No.	ISO 15118-1:2013 - Road vehicles -- Vehicle to grid communication interface -- Part 1: General information and use-case definition. ISO 15118-2:2014 - Road vehicles -- Vehicle-to-Grid Communication Interface -- Part 2: Network and application protocol requirements. ISO 15118-3:2015 - Road vehicles -- Vehicle to grid communication interface -- Part 3: Physical and data link layer requirements.
Standard Title	ISO 15118 - Data communication
URL	https://www.iso.org/committee/5383568.html
Country	International
Status	ISO 15118-1: Published 2013. ISO 15118-2: Published 2014. ISO 15118-3: Published 2015.
Date	See above
Aim	Data communication for vehicle applications, including: Data buses and protocols (including dedicated sensor communication); V2X communication (including V2G); Diagnostics; Test protocols; Interfaces and gateways (including those for nomadic devices); Data formats; and Standardized data content.
Description	ISO 15118 specifies the communication between Electric Vehicles (EV), including Battery Electric Vehicles and Plug-In Hybrid Electric Vehicles (PEV), and the Electric Vehicle Supply Equipment (EVSE). As the communication parts of this generic equipment are the Electric Vehicle Communication Controller (EVCC) and the Supply Equipment Communication Controller (SECC), ISO 15118 describes the communication between these components. Although ISO 15118 is oriented to the charging of electric road vehicles, it is open for other vehicles as well.
Keyword	Charging, Communication, EV, PEV, V2G.

Autopilot involved	Area	Vehicle IoT Integration and platform. Communication network. IoT eco-system.
Use in the Project		Vehicle-to-Grid (V2G) communications for electric vehicles (EV) and Plug-In Hybrid Electric Vehicles primarily.
Author /Company		SINTEF

6.2.9 ISO/IEC JTC1/SC27

ISO/IEC 27000:2016 Information technology — Security techniques — Information security management systems — Overview and vocabulary

Standardization body	ISO/IEC - https://www.iso.org/standards-catalogue
Standard No.	ISO/IEC 27000:2016
Standard Title	Information technology — Security techniques — Information security management systems — Overview and vocabulary
URL	https://www.iso.org/standard/66435.html
Country	International
Status	Published
Date	2016
Aim	<p>Provide hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001</p> <p>Scope: This International Standard provides to organizations and individuals: a) an overview of the ISMS family of standards; b) an introduction to information security management systems (ISMS); and c) terms and definitions used throughout the ISMS family of standards.</p> <p>Purpose: ISO/IEC 27000 describes the fundamentals of information security management systems, which form the subject of the ISMS family of standards, and defines related terms.</p>

Description	<p>The standard "established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization". The actual controls listed in the standard are intended to address the specific requirements identified via a formal risk assessment. The standard is also intended to provide a guide for the development of "organizational security standards and effective security management practices and to help build confidence in inter-organizational activities".</p>  <p>The diagram illustrates the ISMS Family of Standards, categorized into four main groups on the left: Vocabulary standards, Requirement standards, Guideline standards, and Sector-specific guideline standards. The right side lists specific standards and technical reports, including 27000 (Overview and vocabulary), 27001 (Information security management systems - Requirements), 27002 (Code of practice for information security controls), 27003 (Information security management system implementation guidance), 27004 (Information security management — Measurement), 27005 (Information security risk management), 27007 (Guidelines for information security management systems auditing), 27010 (Information security management guidelines for inter-sector and inter-organizational communications), 27011 (Information security management guidelines for telecommunications organizations based on ISO/IEC 27002), 27006 (Requirements for bodies providing audit and certification of information security management systems), TR 27008 (ISMS Controls Audit Guidelines), 27013 (Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1), 27014 (Governance of information security), TR 27016 (Information security management – Organizational economics), TR 27015 (Information security management guidelines for financial services), and TS 27017 (Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002). At the bottom, there are boxes for 2703x and 2704x, representing control-specific guideline standards.</p>
Keyword	ISMS
Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform, Communication network, IoT eco-system.
Use in the Project	This standard is widely adopted by companies and organizations to manage security related aspects of information systems. We reference it as a possible baseline for overall IT security management by Autopilot service suppliers.
Author /Company	THALES

ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements

Standardization body	ISO/IEC - https://www.iso.org/standards-catalogue
Standard No.	27001
Standard Title	Information technology — Security techniques — Information security management systems — Requirements

URL	https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en
Country	International
Status	Published
Date	2013
Aim	Provide requirements for establishing, implementing, maintaining and continually improving an information security management system
Description	<p>This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.</p> <p>The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.</p> <p>It is important that the information security management system is part of an integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.</p> <p>This International Standard can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.</p> <p>The order in which requirements are presented in this International Standard does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.</p> <p>ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003[2], ISO/IEC 27004[3] and ISO/IEC 27005[4]), with related terms and definitions.</p>
Keyword	ISMS (Information Security Management System); Security, Application
Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform, Communication network, IoT eco-system
Use in the Project	This standard is widely adopted by companies and organizations to manage security related aspects of information systems. We reference it as a possible baseline for overall IT security management by Autopilot service suppliers.

Author /Company	THALES
------------------------	--------

ISO/IEC: 27002 Information technology — Security techniques — Code of practice for information security controls

Standardization body	ISO/IEC - https://www.iso.org/standards-catalogue
Standard No.	27002
Standard Title	Information technology — Security techniques — Code of practice for information security controls
URL	https://www.iso.org/standard/54533.html
Country	International
Status	Published
Date	2013
Aim	Provide hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001
Description	The standard "established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization". The actual controls listed in the standard are intended to address the specific requirements identified via a formal risk assessment. The standard is also intended to provide a guide for the development of "organizational security standards and effective security management practices and to help build confidence in inter-organizational activities".
Keyword	ISMS (Information Security Management System); Security, Application
Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform, Communication network, IoT eco-system
Use in the Project	This standard is widely adopted by companies and organizations to manage security related aspects of information systems. We reference it as a possible baseline for overall IT security management by Autopilot service suppliers.
Author /Company	THALES

ISO/IEC 15408-1 - Evaluation criteria for IT security - Information and General Model

Standardization body	ISO/IEC – https://www.iso.org/standards-catalogue/browse-by-ics.html
-----------------------------	---

Standard No.	ISO/IEC 15408-1
Standard Title	Information Technology – Security Techniques – Evaluation criteria for IT security – Information and General Model
URL	http://standards.iso.org/ittf/PubliclyAvailableStandards/c050341_ISO_IEC_15408-1_2009.zip
Country	International
Status	Published
Date	2014 – 01 – 15
Aim	<p>This document is the Part 1 of the ISO/IEC 15408 that permits comparability between the results of independent security evaluations.</p> <p>This part of ISO/IEC 15408 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the standard which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.</p>
Description	<p>Part one provides an overview of all parts of ISO/IEC 15408 standard. It describes the various parts of the standard; defines the terms and abbreviations to be used in all parts of the standard; establishes the core concept of a Target of Evaluation (TOE); the evaluation context and describes the audience to which the evaluation criteria are addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given.</p> <p>It defines the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 may be tailored through the use of permitted operations.</p> <p>The key concepts of protection profiles (PP), packages of security requirements and the topic of conformance are specified and the consequences of evaluation, evaluation results are described. This part of ISO/IEC 15408 gives guidelines for the specification of Security Targets (ST) and provides a description of the organization of components throughout the model. General information about the evaluation methodology are given in ISO/IEC 18045 and the scope of evaluation schemes is provided.</p>
Keyword	Application Programming Interface (API), Configuration Management (CM), Information Technology (IT), Operating System (OS), Public Key Infrastructure (PKI), Adverse actions, Assignments, Authentication Data, Authorized User, Connectivity, Target of Evaluation (TOE)
Autopilot Area involved	ITS Security Functional Model, Security Management System Architecture, V2X Communications
Use in the Project	This standard shall be the guide for the AUTOPILOT architecture in particular for T1.5 “Security, Privacy and Data Specification” and for T1.2 “IoT Architecture and Specification”
Author /Company	THALES

ISO/IEC 15408-2 - Evaluation criteria for IT security – Security Functional Components

Standardization body	ISO/IEC – http://standards.iso.org/
Standard No.	ISO/IEC 15408-2
Standard Title	Information Technology – Security Techniques – Evaluation criteria for IT security – Security Functional Components
URL	http://standards.iso.org/ittf/PubliclyAvailableStandards/c046414_ISO_IEC_15408-2_2008.zip
Country	International
Status	Published
Date	2011 – 06 – 01
Aim	<p>This document is the Part 2 of the ISO/IEC 15408 that permits comparability between the results of independent security evaluations.</p> <p>This part of ISO/IEC 15408 defines the required structure and content of security functional components for the purpose of security evaluation. It includes a catalogue of functional components that will meet the common security functionality requirements of many IT products.</p>
Description	<p>This document is structured in clauses as following:</p> <ul style="list-style-type: none"> • Clause 5: describes the paradigm used in the security functional requirements • Clause 6: introduce the catalogue of this part of ISO/IEC 15408 functional components • Clause 7 to 17: functional classes
Keyword	Information technology (IT), Component, Component Identification, Dependencies, Functional Elements, Component Levelling, Management, Security Functional Components, Functional Requirements Paradigm, Security, Evaluation Criteria
Autopilot Area involved	ITS Security Functional Model, Security Management System Architecture, V2X Communications
Use in the Project	This standard shall be the guide for the AUTOPILOT architecture in particular for T1.5 “Security, Privacy and Data Specification” and for T1.2 “IoT Architecture and Specification”
Author /Company	THALES

ISO/IEC 15408-3 - Evaluation criteria for IT security T Security Assurance Components

Standardization body	ISO/IEC – http://standards.iso.org/
Standard No.	ISO/IEC 15408-3

Standard Title	Information Technology – Security Techniques – Evaluation criteria for IT security – Security Assurance Components
URL	http://standards.iso.org/ittf/PubliclyAvailableStandards/c046413_ISO_IEC_15408-3_2008.zip
Country	International
Status	Published
Date	2011 – 06 – 01
Aim	<p>This document is the Part 3 of the ISO/IEC 15408 that permits comparability between the results of independent security evaluations.</p> <p>This part of ISO/IEC 15408 defines the assurance requirements of ISO/IEC 15408. It includes the evaluation assurance levels (EALs) that define a scale for measuring assurance for component Targets of Evaluation (TOEs), the composed assurance packages (CAPs) that define a scale for measuring assurance for composed TOEs, the individual assurance components from which the assurance levels and packages are composed, and the criteria for evaluation of Protection Profiles (PPs) and Security Targets (STs).</p>
Description	<p>This document is structured in the following clauses:</p> <ol style="list-style-type: none"> 1. Clause 5: the paradigm used in the security assurance requirements 2. Clause 6: presentation structure of the assurance classes, families, components, evaluation assurance levels along with their relationships, and the structure of the composed assurance packages. It also characterized the assurance classes and families 3. Clause 7: detailed definitions of the EALs 4. Clause 8: detailed definitions of the CAPs 5. Clause 9 through 16: detailed definitions of assurance classes
Keyword	Information Technology (IT), Security Assurance Components, Assurance Class Structure, Class Name/Introduction, Protection Profile Evaluation
Autopilot Area involved	ITS Security Functional Model, Security Management System Architecture, IoT Architecture
Use in the Project	This standard shall be the guide for the AUTOPILOT architecture in particular for T1.5 “Security, Privacy and Data Specification” and for T1.2 “IoT Architecture and Specification”
Author /Company	THALES

6.2.10 oneM2M

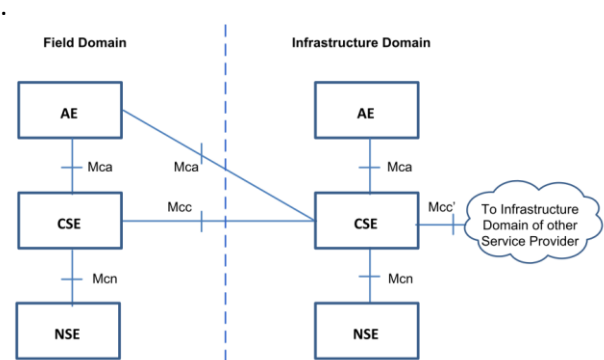
oneM2M: TS0001, TS0002, TS0004, TS-0012, TR-0033 - Semantics

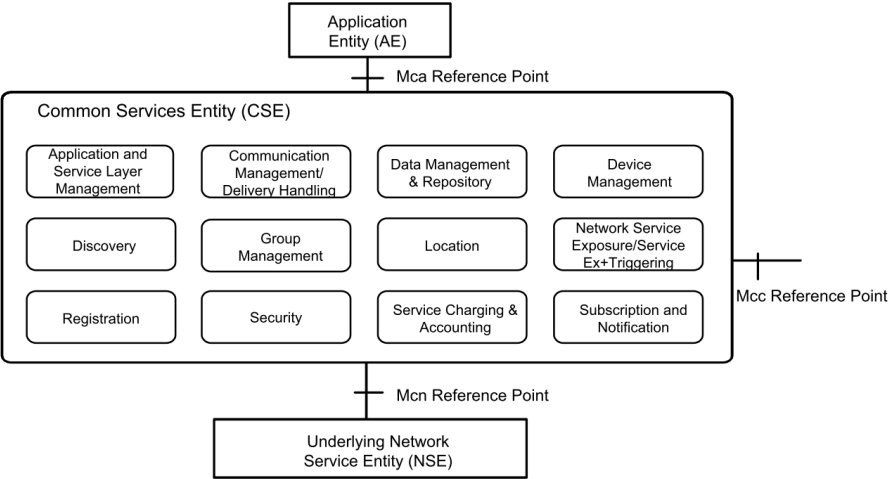
Standardization body	oneM2M
-----------------------------	--------

Standard No.	TS0001, TS0002, TS0004, TS-0012, TR-0033
Standard Title	TS0001 – Functional architecture, TS0002 - Requirements, TS0004 – Service layer core protocol, TS-0012 – Base Ontology, TR-0033 – Study on enhanced semantic enablement
URL	http://www.onem2m.org/technical/published-documents http://www.onem2m.org/technical/latest-drafts
Country	International
Status	Published in Release 2, but relevant enhancement are being made in Release 3
Date	2012 - ongoing
Aim	The goal is to provide semantic functionalities in the oneM2M platform. In Release 2, semantic annotation of oneM2M resources and the semantic resource discovery based on these annotations is supported. In Release 3 direct queries for semantic information and semantic mashups are under development.
Description	oneM2M enables the semantic annotation of resources of key resource types using semantic descriptor resources. The semantic annotation can be used to discover relevant resources by providing a detailed semantic filter in form of a SPARQL request. With the semantic annotation a detailed description of what is contained in the resource can be given, e.g. including the data type used, the unit provided, the quality of the information, or the real world entity that is being described
Keyword	Integration /Interoperability, IoT Architecture, Semantics
Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform, Communication network
Use in the Project	In order to provide basic information, e.g. coming from a sensor, that is stored in the oneM2M platform, to higher-level parts of the IoT platform, e.g. implemented by FIWARE GEs, the semantic information and related functionalities play an important part to facilitate this, as richer information is required, which may not directly be provided by low-level sources. Using semantic annotations, this can be added in the oneM2M platform. The existing semantic oneM2M functionality enables this, but the envisioned enhanced functionality will make this easier and more efficient.
Author /Company	Martin Bauer / NEC

oneM2M: TS-0001-V2.10.0 Functional Architecture

Standardization body	oneM2M http://www.onem2m.org/technical/published-documents
Standard No.	TS-0001-V2.10.0

Standard Title	Functional Architecture
URL	http://www.onem2m.org/images/files/deliverables/Release2/TS-0001-%20Functional_Architecture-V2_10_0.pdf
Country	International
Status	Draft
Date	2016-August-30
Aim	<p>The document describes the end-to-end oneM2M functional architecture, including the description of the functional entities and associated reference points.</p> <p>oneM2M functional architecture focuses on the Service Layer aspects and takes Underlying Network-independent view of the end-to-end services. The Underlying Network is used for the transport of data and potentially for other services.</p>
Description	<p>The oneM2M Layered Model for supporting end-to-end (E2E) M2M Services comprises three layers: Application Layer, Common Services Layer and the underlying Network Services Layer.</p> <p>Below the oneM2M functional architecture detailed in this technical specification.</p>  <p>The common service layer is composed of a set of common service functions providing services to the AEs via the Mca reference point and to other Common Services Entity (CSEs) via the Mcc reference point. CSEs interact with the Network Service Entity (NSE) via the Mcn reference point. An instantiation of a CSE in a Node comprises a subset of the CSFs from the CSFs described in the TS-001.</p>

	 <p>Those CSFs are listed in the graph above. Mca, Mcc, Mcn are the reference points, which provide the communication between two different entities. The CSFs contained inside the CSE can interact with each other.</p> <p>This Technical specification describes all the aspects related to the M2M-IoT functional architecture included features, interface and datagrams. Through its annex and references, it supplies a design environment to be used as reference.</p>
Keyword	application layer, common services layer, common services function (CSF), management proxy, reference points
Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform, Communication network, IoT eco-system
Use in the Project	The described security architecture should be used as guideline in the AUTOPILOT architecture design phase, whit particular reference to the WP1.2, IOT architecture and specification, and WP1.5 Security, Privacy and Data Specification.
Author /Company	THALES

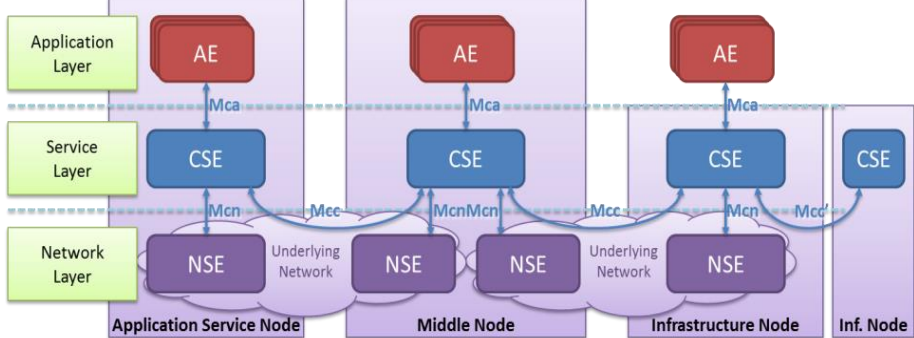
oneM2M: TS-0003-V2.4.1 Security solutions

Standardization body	oneM2M – http://www.onem2m.org/technical/published-documents
Standard No.	TS-0003-V2.4.1
Standard Title	Security solutions
URL	http://www.onem2m.org/images/files/deliverables/Release2/TS-0003_Security_Solutions-v2_4_1.pdf
Country	International
Status	Draft

Date	2016-August-30
Aim	The present document defines security solutions applicable within the M2M system. The security architecture and features described in this document shall be taken as guide for a M2M application.
Description	<p>This standard present a n High level overview of the Security architecture based on:</p> <ul style="list-style-type: none"> • Security Integration in oneM2M flow of events • Security Service Layer: <ul style="list-style-type: none"> ○ Access Management ○ Authorization Architecture ○ Security Administration ○ Identity Protection ○ Sensitive Data Handling ○ Trust Enabler security functions • Secure Environment Abstraction Layer Components • Authorization • Security Framework • Security Framework Procedures and Parameters • Protocol and Algorithm details • Privacy Protection Architecture using Privacy Policy Manager (PPM) • Security-Specific oneM2M Data Type Definitions <p>Security Layer is located between M2M applications and communication HW/SW that provides data transport. It provides functions that M2M applications across different industry segments commonly need. Those functions are exposed to Applications via APIs. It allows for distributed intelligence (device, gateway, cloud apps). It is based on RESTful APIs and resources</p>
Keyword	Security Functions layer; Security Environment Abstraction Layer; Secure Environment layer; Identification and Authentication; Authorization; Identity Management; Sensitive Data Handling; Security Association Establishment; Security Administration; Identity Protection; Remote Security Provisioning Frameworks (RSPF)
Autopilot Area involved	Security design and implementation analysis for: IoT Platform, Vehicle Integration and platform, Communication, IoT eco-system
Use in the Project	This standard shall be the guide for the AUTOPILOT architecture definition from a SECURITY prospective.
Author /Company	THALES

oneM2M TS-0010-V1.0.1 MQTT Protocol Binding

Standardization body	oneM2M - http://www.onem2m.org/technical/published-documents
Standard No.	TS-0010-V1.0.1

Standard Title	MQTT Protocol Binding
URL	http://www.onem2m.org/images/files/deliverables/Release2/TS-0010-MQTT%20Protocol%20Binding-V2_4_1.pdf
Country	International
Status	Draft
Date	2016-August-30
Aim	This document defines the binding of the oneM2M protocols to an MQTT transport layer.
Description	<p>The MQTT protocol binding specifies how the Mca or Mcc request and response messages are transported across the MQTT protocol. The binding is defined in terms of the MQTT protocol flows that take place between the client libraries and the MQTT server in order to affect the transport of an Mca or Mcc message.</p>  <p>This Technical specification map the primitive used by Reference Point of M2M architecture, on MQTT transport layer protocol. Other one is available like HTTP and CoAP. The primitives are independent from the transport Protocols. The protocol are the following:</p> <ul style="list-style-type: none"> • CoAP Protocol Binding TS - 008 • HTTP Protocol Binding TS - 009 • MQTT Protocol Binding TS - 010 <p>The MQTT binding makes use of one or more MQTT Servers to transport messages. The AE/CSEs both act as MQTT Clients of an MQTT Server that mediates delivery of messages between the two and the topic in the MQTT PUBLISH packet contains the originator credentials.</p> <p>In the chapter 7 the security issues are described with particular reference to the MQTT Server authentication and the access control policies.</p>
Keyword	Security, Binding, Request, Communication , CoAP, MQTT, HTTP, Authorization, Authentication
Autopilot Area involved	Security design and implementation analysis for: IoT Platform, Vehicle Integration and platform, Communication, IoT eco-system
Use in the Project	This standard, from the prospective of a specific messaging protocol like MQTT, should be a reference for the AUTOPILOT partners from an

	ARCHITECTURAL and SECURITY prospective, impacting WP1 and WP2 during the design and development phase.
Author /Company	THALES

oneM2M TS-0018, TS-0019, TS-0028, TS-0029 -Testing suite

Standardization body	oneM2M
Standard No.	TS-0018, TS-0019, TS-0028, TS-0029
Standard Title	<ul style="list-style-type: none"> • Test Suite Structure and Test Purposes, • Abstract Test Suite Implementation eXtra Information for Test • Security Test Suite Structure and Test Purposes • Abstract Security Test Suite Implementation eXtra Information for Test
URL	http://www.onem2m.org/technical/published-documents
Country	International
Status	Published
Date	
Aim	These specifications are the tests description for the various interfaces and protocols that are used to validate if the implementations correctly employ the described functionalities
Description	These specifications are the tests description for the various interfaces and protocols that are used to validate if the implementations correctly employ the described functionalities. TS-0018 and TS-0019 are for overall implementation TS-0028 and TS-0029 are for the security parts These tests will be used within the oneM2M certification activity
Keyword	Conformance, Testing, Interoperability,
Autopilot Area involved	IoT Platform, Vehicle IoT Integration and platform, Communication network, IoT eco-system
Use in the Project	<p>EGM actively participates in the oneM2M Security and Test Working Groups where contributes security Test Purposes under the Work Item “WI-0051 Security Functions Conformance Testing”, whose rapporteur is Dr. Franck Le Gall from EGM. The TST working group is responsible for this WI and there are joint TST and SEC working group meetings to discuss the details about security testing.</p> <p>EGM also participates in oneM2M Task Force 001 and ETSI STF 531. In these Task Forces, the goal is to write a TTCN-3 test cases for every Test Purpose contributed in the TS-0018 and TS-0028 documents of oneM2M. The oneM2M TF 001 was created in May 2016 and operates on a voluntary</p>

	<p>basis. Its members are TTCN-3 experts that work on the oneM2M standard. The STF 571 is funded by ETSI to speed up the TTCN-3 tests creation. The work of the Task Forces is overseen by the oneM2M TST working group and the produced TTCN-3 tests are contributed to the oneM2M standard in the document TS-0019 and TS-0029.</p> <p>These tests can be used in Autopilot to tests in particular the security aspects on the IoT/oneM2M part</p>
Author /Company	EGM

oneM2M TS 0006 2.0.1 Management Enablement (BBF)

Standardization body	OneM2M
Standard No.	TS 0006 2.0.1
Standard Title	Management Enablement (BBF)
URL	http://www.onem2m.org/technical/latest-drafts
Country	International
Status	Published
Date	2016-August-30
Aim	The document describes the protocol mappings between the management Resources for oneM2M and the BBF TR-181i2 Data Model
Description	<p>Specifies the usage of the BBF TR-069 protocol and the corresponding message flows including normal cases as well as error cases to fulfil the oneM2M management requirements.</p> <p>The mapping include:</p> <ul style="list-style-type: none"> - Device: all information on how to map management resources from TS-0004 [2] to managed objects and parameters as defined in the TR-181 [6] data model or the Remote Procedure Calls (RPCs) in TR-069 [4]] - Procedures for management (how to map oneM2M management resource primitives to BBF Remote Procedure Calls (RPCs)) [sul doc: This clause contains all information on how to map management resource primitives from TS-0004 [2] to the Remote Procedure Calls (RPCs) in TR-069 [4]] - Server Interaction (how the IN-CSE – Internal Common Service Entity - interacts with an ACS – Auto Configuration Server - in order to manage the Resources described). The interaction includes communication session, requests and notifications, discovery. [dal doc: This clause specifies how the IN-CSE interacts with an ACS in order to manage the Resources described in the present

	document.] Includes protocols for managing different devices. Although not so much a device but application that support devices this standards qualifies to be in this section because it is a device
Keyword	Devices and Sensor Technology
Autopilot Area involved	IoT eco-system
Use in the Project	WP1 and WP3
Author /Company	TIM

oneM2M-TR-0026 Vehicular Domain Enablement

Standardization body	OneM2M
Standard No.	oneM2M-TR-0026
Standard Title	Vehicular Domain Enablement
URL	http://www.onem2m.org/technical/latest-drafts
Country	International
Status	Draft
Date	17/10/2016
Aim	This Technical Report examines how the current oneM2M System can be used in the Vehicular Domain and includes a study of advanced features which the future oneM2M release(s) could support for this vertical domain.
Description	<p>The Technical Report begins describing technology trends in Vehicular Domain and lists organization and standards related to this field.</p> <p>Then it analyzes fifteen use cases:</p> <ul style="list-style-type: none"> - Vehicular Diagnostic & Maintenance Report - Use Case on Remote Maintenance Services - Traffic Accident Information Collection - Fleet Management Service using DTG (Digital Tachograph) - Use cases for Electronic Toll Collection (ETC) service - Use cases for Taxi Advertisement - Use Case on Vehicle Data Service - Smart Automatic Driving - Use Case on Vehicle Data Wipe Service - Vehicle Management based on Geo-Fence - Use Case on Secure Over-The-Air Firmware Update for Automotive ECUs - Car/Bicycle Sharing Services

	<ul style="list-style-type: none"> - Smart Parking - Vehicle Broadcasting without Registration - Vehicle location privacy protection <p>defining the potential requirements regarding this specific domain</p> <p>In the last section, three different type of high level oneM2M architectures are illustrated, mapping for these use cases.</p>
Keyword	IoT Architecture, Use cases, requirements , vehicular domain , vehicular domain architectures
Autopilot Area involved	Vehicle IoT Integration and platform
Use in the Project	WP1 and WP3
Author /Company	TIM

6.3 Annex C – ETSI TR 103 375 v1.1.1 (2016-10)

This section contains an excerpt from the Technical Report ETSI 103 375⁷. In particular are presented all the standards that are tagged useful for the Smart Mobility into the technical report.

SDO	Standards	Description/Analysis	Knowledge Areas
3GPP multi-purpose	ETSI TS 123 002 (network architecture) ETSI TS 123 401 (Packet Radio Service) ETSI TS 136 300 (Radio Access Overall description)	The 3GPP standards cover Radio, Core Network, and Service Architecture for cellular mobile networks. The different versions are named: GSM, GPRS (2G), EDGE, UMTS (3G), HSPA, LTE (or 4G), LTE-Advanced. The specifications cover all aspects of a radio telecommunication system. LTE is significantly more spectrally-efficient than 2G or 3G, hence transporting data over a 4G network can be done at a much lower cost per bit. The LTE-ADVANCED standard version is still evolving. New networks are being rolled out, and leading-edge features are being added to 4G to satisfy the market need for ever-increasing data rates. http://www.3gpp.org/specifications/specifications .	Communication and Connectivity
3GPP for MTC (Machine Type Communications)	LTE- (LTE for MTC) , EC-GSM, NB-IoT	LTE-(LTE for MTC): New categories of communications, complying with IoT requirements, are being launched in the 3GPP standards and they belong to LTEADVANCED and LTE-ADVANCED PRO (4.5G). They are evolving standards. EC-GSM (or EC-GPRS) provides an extended coverage capability, as a global connectivity solution for cellular IoT that leverage existing module ecosystem and allows for deep indoor coverage. It may also include eDRX, for extended battery life of the device (up to 15 years). NB-IoT is a new narrowband radio technology which will provide improved indoor coverage, support of massive number of low throughput devices, low delay sensitivity, ultra-low device cost, low device power consumption and optimized network architecture. NB-IoT standards are under progress.	Communication and Connectivity

⁷ http://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf

SDO	Standards	Description/Analysis	Knowledge Areas
3GPP V2X	TR 36.885 (RAN Study on LTEbased V2X Services)	The Radio Access Network (RAN) Group is working on TR 36.885, to evaluate performance of LTE for V2X communication and identify changes to LTE physical layer, RAN protocols, and interfaces to support V2X communications (started early 2016). ftp://ftp.3gpp.org/Specs/archive/36_series .	Communication and Connectivity
Bluetooth	Bluetooth BR/EDR (basic rate/enhanced data rate) Bluetooth Low Energy (BLE)	Bluetooth is a global wireless communication standard that connects devices. Communication between Bluetooth devices happens over short-range, ad hoc networks known as piconets. The network ranges from two to eight connected devices. When a network is established, one device takes the role of the master while all the other devices act as slaves. Piconets are established dynamically and automatically as Bluetooth devices enter and leave radio proximity. There are different versions of the core specification of Bluetooth. The most common are Bluetooth BR/EDR (basic rate/enhanced data rate) and Bluetooth with low energy functionality. http://www.bluetooth.com/what-is-bluetoothtechnology/bluetooth-technology-basics .	Communication and Connectivity
CEN/ISO	EN ISO 17575 Electronic fee collection - Application interface definition for autonomous systems EN ISO 12855 Electronic fee collection - Information exchange between service provision and toll charging ISO/TS 18750 Intelligent transport systems - Cooperative systems - Definition of a global concept for Local Dynamic Maps ISO 29281 Intelligent transport systems - Communications access for land mobiles (CALM) - Non-IP networking CEN/TS 16157 Intelligent	CEN TC 278 is responsible for standardization in the field of telematics for traffic and road transport. Through joint working groups, TC 278 is working closely with the ISO TC 204 committee, responsible for developing standards in the same field of action. CEN standards are also often ISO standards. A large set of standards is being produced, dealing specifically with issues relating to the identification of applications and services, C-ITS, embedded HMI, traffic management, tolling or eCall. http://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:6259&cs=1EA16FFFE1883E02CD366E9E7EADFA6F7 . http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=54706&published=on&wikipedi=true .	Communication and Connectivity

SDO	Standards	Description/Analysis	Knowledge Areas
	transport systems - DATEX II data exchange specifications for traffic management and information		
CiA	ISO 11898 series	<p>CAN is a multi-master serial bus system with multi-drop capabilities. The CAN messages are broadcasted on the bus.</p> <p>Originally developed for use as an in-vehicle network in passenger cars (CAN bus), CAN is now used in many other industries.</p> <p>The original (or Classical CAN) data link layer protocol has been standardized in the ISO 11898 series. More recently, it has been improved as the CAN FD (Flexible Data Rate) protocol, defined in the same document (ISO 11898-1). The standards also describe several physical layer options. Most common is the high-speed transmission as standardized in ISO 11898-2.</p> <p>The other physical layer standard used in the automotive industry is ISO 11898-3, a so-called fault-tolerant, low-power transmission.</p>	Communication and Connectivity
ETSI	Terrestrial trunked Radio (TETRA); ETSI EN 300 392	<p>TETRA is a set of standards that describe a common mobile radio communications infrastructure throughout Europe. It is targeted primarily at the mobile radio needs of public safety groups (police, fire departments, etc.), utility companies and other companies that provide voice and data communications services at the scale of a metropolitan area (i.e. city) TETRA relies on digital trunking and TETRA products come with built-in encryption to ensure privacy and confidentiality.</p> <p>TETRA introduces various advantages when compared to other mobile technologies (e.g. GSM) such as long range communications, efficient mobility support, and direct communications in the absence of a network, one-to-many communications, etc. However, TETRA has the disadvantage of providing a slower data transfer rate.</p>	Communication and Connectivity

SDO	Standards	Description/Analysis	Knowledge Areas
ETSI ERM	<p>ETSI EN 302 571 (Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band)</p> <p>ETSI EN 300-674-2 (Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s/250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; [-1] Road Side Units (RSU)/[-2] On-Board Units (OBU)</p> <p>ETSI EN 302 858/ETSI EN 303 396/ETSI EN 301 091 (vehicular radars)</p> <p>ETSI EN 302 065/ETSI EN 303 883 (SRD Devices using UWB)</p>	<p>TG37 provides and manages ETSI deliverables for radiorelated ITS matters. TG SRR covers the field of automotive and surveillance radar applications.</p> <p>TGUWB (Ultra Wide Band) covers Short Range Devices (SRD) using broadband air interfaces and systems using Ultra Wide Band (UWB) technologies for communications purposes, sensor applications and networks.</p> <p>These European norms (EN) contain the Harmonised Standards covering the essential requirements of article 3.2 of the Directive 2014/53/EU (also called RE-D, Radio Equipment Directive)</p> <p>http://www.etsi.org.</p>	Communication and Connectivity
ETSI ITS	<p>ETSI TR 101 607 (Cooperative ITS (C-ITS); Release 1)</p> <p>ETSI EN 302 663 (Access layer specification for ITS operating in the 5 GHz frequency band)</p> <p>ETSI EN 302 636 Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking</p>	<p>ETSI TR 101 607 lists standards, specifications and other deliverables which have been developed to form a consistent set of standards as the basis for the Release 1 of ITS, including standards for interoperability developed in accordance with the work plan of the Mandate M/453.</p> <p>ETSI EN 302 663 defines the parameters and frequencies to be applied in Europe when using IEEE 802.11-2012/802.11p. The access technology defined is called ITS-G5.</p> <p>ETSI EN 302 636 is a series of European norms that specify the GeoNetworking protocols for dissemination of messages over geographical areas.</p> <p>http://www.etsi.org.</p>	Communication and Connectivity

SDO	Standards	Description/Analysis	Knowledge Areas
IEEE 802 LAN/MAN	IEEE 802.11 (WLAN) IEEE 802.15.4 (LR-WPAN)	The IEEE 802 LAN/MAN Standards Committee develops and maintains a set of wireless technology access standards for personal (802.15), local (802.11) and metropolitan (802.16) area networks. These standards cover wireless networks ranging from a few centimetres (WPAN) to thousands meters (WMAN). They specify the media access control (MAC) and physical layer for the implementation of wireless networks. IEEE 802.11 standard and its amendments cover Wireless local area networks, with a typical range up to 100m, using generally unlicensed spectrum. IEEE 802.15 focuses on Wireless Personal Area Network (WPAN). IEEE 802.15.4 standard and its amendments cover Low-Rate Wireless Personal Area Networks (LR-WPANs). http://standards.ieee.org/about/get/ .	Communication and Connectivity
IEEE 802 LAN/MAN	IEEE 802.11-2012 (WLAN, amendment 802.11p, integrated in 2012)	This amendment (well-known as 802.11p amendment), integrated in the main standard in 2012, contains an adaptation for V2V communications, i.e. communication outside the context of a BSS.	Communication and Connectivity
IEEE P1609	IEEE 1609.3: WAVE - Networking Services IEEE 1609.4: WAVE - Multi-channel Operation IEEE 1609.11: WAVE - Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS)	IEEE P1609 is a suite of "standards for Wireless Access in Vehicular Environments (WAVE)". They define architecture and a complementary, standardized set of services and interfaces that collectively enable secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications. https://standards.ieee.org/develop/wg/1609_WG.html .	Communication and Connectivity
IETF 6lo	Definition of Managed Objects for 6LoWPANs (IETF RFC 7388) 6LoWPAN-GHC (IETF RFC 7400) Transmission of IPv6 Packets over Recommendation ITU-T G.9959 Networks (IETF RFC 7428) Ipv6 over BLUETOOTH® Low Energy (IETF RFC 7668)	The IETF WG 6lo targets IPv6 over low power area networks, i.e. over networks of resource-constrained nodes in terms of memory, processing resources and bandwidth. It introduces mechanisms for packets fragmentation/assembling, headers encapsulation, compression, routing in mesh topologies, network selfconfiguration/ management, and interworking with full IPv6 networks. https://datatracker.ietf.org/wg/6lo/documents .	Communication and Connectivity

SDO	Standards	Description/Analysis	Knowledge Areas
IETF ITS	charter document for IETF95	The IETF ITS group is expected to meet for its first official meeting at IETF95 in April 2016. According to its draft charter, the goal of this group is to standardize IP protocols for establishing direct and secure connectivity between nearby moving networks. As many protocols are being developed at link layer level, the objective is to establish IP paths across them in an interoperable manner. The envisioned scenarios are C-ACC (Cooperative Adaptive Cruise Control) and platooning (or vehicle streams).	Communication and Connectivity
IETF XMPP	IETF RFC 6120 (Extensible Messaging and Presence Protocol (XMPP): Core) and IETF RFC 6121 (Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence) XMPP-IoT extensions in progress	The XMPP Standards Foundation (XSF) is an independent, non-profit SDO whose primary mission is to define open protocols for presence, instant messaging, and real-time communication and collaboration on top of the IETF's Extensible Messaging and Presence Protocol (XMPP). The XSF community has initiated a new interoperable extension series to enable sensors and actuators to communicate in the IoT world. http://www.xmpp-iot.org https://datatracker.ietf.org/wg/xmpp/documents/ .	Communication and Connectivity
ITU-R	Agenda Item (AI 1.12)	During the WRC15 the APT (Asian Pacific Telecommunity) has proposed a new Agenda Item (AI1.12) for the upcoming WRC-19 to investigate the potential of a harmonization of the ITS spectrum world-wide.	Communication and Connectivity
OASIS MQTT	Message Queuing Telemetry Transport (MQTT)	MQTT is an extremely lightweight and reliable (over TCP) connectivity protocol designed for M2M communications and the IoT. It is a client/server publish/subscribe messaging transport protocol designed to support messaging transport from remote locations/devices involving small code footprints (e.g. 8-bit, 256 KB ram controllers), low power, low bandwidth, high-cost connections, high latency, variable availability, and negotiated delivery guarantees. MQTT protocol offers mechanisms for resource discovery, bi-directional communication, QoS level specification, and scalability. http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqttv3.1.1-os.html .	Communication and Connectivity

SDO	Standards	Description/Analysis	Knowledge Areas
OMG	DDS v1.4 - Data Distribution Service (DDS™); DDSI-RTPS v2.2 - The Real-time Publish-Subscribe Wire Protocol DDS™ Interoperability Wire Protocol (DDSIRTPS™)	The Data Distribution Service is a middleware protocol and API standard for distributed application communication and integration. http://portals.omg.org/dds/omg-dds-standard/ .	Communication and Connectivity
SAE	J2735_201601: DSRC (Dedicated Short Range Communications) Message Set Dictionary™	J2735 specifies a message set, and its data frames and data elements, specifically for use by applications intended to utilize the 5,9 GHz DSRC/WAVE (cf. IEEE P1609) communications systems.	Communication and Connectivity
ZigBee®	ZigBee® PRO ZigBee® RF4CE	ZigBee® technology uses the globally available, licensefree 2,4 GHz frequency band. It enables wireless applications using a standardized set of high level communication protocols sitting atop low-power digital radios based on the IEEE 802.15.4 standard for wireless personal area networks. ZigBee® PRO: wireless mesh, low-power networking capable of supporting more than 64 000 devices on a single network. ZigBee® RF4CE: two-way device-to-device control applications for low-power and low-latency control ZigBee® IP: open standard for an Ipv6-based wireless mesh networking solution with seamless Internet connections to control low-power, low-cost devices. http://www.zigbee.org/zigbee-for-developers/networkspecifications/ .	Communication and Connectivity
3GPP V2X	TR 22.885 (Study on LTE Support for Vehicle to Everything (V2X) Services); TS 22.185 (Service requirements for V2X services; Stage 1); TR 22.891 (3GPP; Technical Specification Group Services and System Aspects; Feasibility Study on New Services and Markets Technology Enablers; Stage 1) for Smarter.	3GPP has recently started working on C-ITS for LTE-Advanced and 5G (known as Smarter). These documents identify the main use cases where LTE could be used for V2X scenarios and the corresponding requirements. ftp://ftp.3gpp.org/Specs/archive/22_series .	Integration/ Interoperability
ACEA	Scientific Advisory Group reports	The Scientific Advisory Group reports are published regularly.	Integration/

SDO	Standards	Description/Analysis	Knowledge Areas
		They cover topics such as Driving Innovation, eCall, Electric Vehicles, Infrastructure, Intelligent Transport Systems, Urban Logistics, Urban Transport Policy, Weights and Dimensions. http://www.acea.be/publications	Interoperability
AVNU Alliance®	Profile for automotive use and certification tests from the automotive Certification Test Subgroup (CDS). Related standards: IEEE 802.1 Audio Video Bridging (AVB); IEEE 1722 AVB Transport Protocol (AVBTP); IEEE 1733 Layer 3 Transport Protocol for Time-Sensitive Applications in Local Area Networks	The AVNU Alliance is an industry forum dedicated to the advancement of professional-quality audio video transport by promoting the adoption of the IEEE 802.1 Audio Video Bridging (AVB), and the related IEEE 1722 and IEEE 1733, standards over various networking link-layers. The AVNU Alliance enables deterministic networking via certification of compliance and interoperability for devices using open IEEE standards. The AVNU certification program ensures interoperability of networked devices in a broad range of applications including professional AV, automotive, industrial control and consumer. A fully networked car according to AVNU alliance allows access to all sensors and cross-domain communication. http://avnu.org/automotive/	Integration/ Interoperability
C2C-CC	C2C Profile.	The C2C-CC plays an important role in the development of European standards for C-ITS and helps validate the systems by getting involved in FOTS and interoperability testing. The C2C-CC European profile specifies the standards profile that have to be used by C-ITS vehicles to enable interoperability. It contains a system specification complemented by a selection of standards and parameters. It allows to test the aspects that are going to be used by day 1 applications.	Integration/ Interoperability
CCC	MirrorLink® includes a certification process for - Devices communication protocol implementation, interoperability with complementary MirrorLink-enabled device or system. - Applications: Testing program to validate the API usage,	CCC member companies have created MirrorLink, a standard technology for drivers to connect their smartphones to their vehicles. CCC publishes specifications for exchange of data between car and smartphones and for applications certification. http://www.mirrorlink.com/	Integration/ Interoperability

SDO	Standards	Description/Analysis	Knowledge Areas
	industry guidelines for user interfaces.		
CEN/ISO	EN 16454 Intelligent transport systems - Esafety - Ecall end to end conformance testing CEN ISO/TS 14907 Electronic fee collection - Test procedures for user and fixed equipment EN 15509 Electronic fee collection - Interoperability application profile for DSRC.	A large set of standards is being produced. These standards focus on testing and interoperability. http://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:6259&cs=1EA16FFFE1883E02CD366E9E7EADFA6F7 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=54706&published=on&wikipedi=true .	Integration/ Interoperability
CLEPA	CLEPA position on Road Safety Automated Driving CLEPA Position Paper Open Telematics Platform.	CLEPA represents the automotive supply industry in Europe. CLEPA publishes regularly position papers on topics related to its members activities. http://clepa.eu/what-wedo/publications/ .	Integration/ Interoperability
ERTICO	Platforms coordination: <ul style="list-style-type: none"> • navigation/digital maps linked to Advanced Driver Assistance Systems (ADASIS) • eMobility ICT Interoperability Innovation (eMI3) • Traffic and Traveller Information (TISA) • Traffic Management 2.0 (TM 2.0) • Transport Network ITS Spatial Data (TN-ITS) 	ERTICO Platforms are focused on deployment of different services. http://ertico.com/projects/categories/platforms/ .	Integration/ Interoperability
ETSI ITS	ETSI EG 202 798 - Intelligent Transport Systems (ITS); Testing; Framework for conformance and interoperability testing".	ETSI EG 202 798 provides an ITS testing framework for conformance testing and an ITS testing framework for interoperability testing. This testing framework provides guidance for development of conformance and interoperability test strategies, test systems and the resulting test specifications for ITS.	Integration/ Interoperability

SDO	Standards	Description/Analysis	Knowledge Areas
IPSO Alliance	IPSO SmartObject Starter Pack IPSO SmartObject Expansion Pack	The availability of Internet Protocol (IP) on constrained devices with memory sizes of 16 kilobytes or less, including IPV6 and 6LowPAN, has made possible a new kind of interoperability for connected devices and Smart Objects. IPSO Smart Object Guidelines provide a common design pattern, an object model that can effectively use the IETF CoAP protocol to provide high level interoperability between Smart Object devices and connected software applications on other devices and services. http://www.ipso-alliance.org/so-starter-pack/ .	Integration/ Interoperability
IPv6 Forum	Ipv6 Ready Logo Phase-2: (Test Specifications and Test Tools)	The Ipv6 Forum "Ipv6 Ready Logo" Program is a conformance and interoperability testing program intended to demonstrate that Ipv6 is available and ready to be used. The Ipv6 Ready Logo Committee defines the test specifications for Ipv6 conformance and interoperability testing, to provide access to self-test tools and to deliver the Ipv6 Ready Logo. https://www.ipv6ready.org/?page=phase-2-tech-info .	Integration/ Interoperability
ITU-R	Recommendation ITU-R M.1890: "ITS - Guidelines & Objectives" Recommendation ITU-R M.2228: "Advanced ITS Radiocommunications" Recommendation ITU-R M.2084: "Radio interface standards of vehicle-to-vehicle and vehicle-to-infrastructure communications for intelligent transport systems applications".	Recommendation ITU-R M 1890 provide general guidelines for ITS communications. Recommendation ITU-R M.2228 is a technical describing ITS systems and applications Recommendation ITU-R M.2084 issued by Question ITU-R 205-5/5 identifies specific radio interface standards of vehicle-to-vehicle and vehicle-to-infrastructure communications for Intelligent Transport System applications.	Integration/ Interoperability
oneM2M	ETSI TS 118 101 Functional Architecture ETSI TS 118 104 Service Layer Core Protocol Specification Test and conformance specifications for interoperability (Rel 2):	An M2M services platform built upon devices, gateways, and servers. It allows end-to-end communication between data source and applications. oneM2M is network centric. It allows interoperability between devices and application through the use of uniform interfaces and APIs. oneM2M reaches to achieve interoperability through different standardization efforts. The different working groups produce specifications for a reference architecture (ARC WG), a messaging protocol (PRO WG), a data Management, Abstraction and Semantics	Integration/ Interoperability

SDO	Standards	Description/Analysis	Knowledge Areas
	ETSI TS 118 112 oneM2M Base Ontology ETSI TS 118 113 Interoperability Testing, ETSI TS 118 114 LWM2M Interworking; ETSI TS 118 115 Testing Framework, ETSI TS 118 118 Test Suite Structure & Test Purposes ETSI TS 118 121: oneM2M and AllJoyn® Interworking ETSI TS 118 123: Home Appliances Information Model and Mapping ETSI TS 118 124: oneM2M and OIC Interworking	(MAS WG), but also interoperability testing (TST WG). oneM2M ARC WG develops and specifies an architecture for an M2M system. oneM2M PRO WG develops and specifies APIs, protocols and message formats used across oneM2M interfaces, including mapping to commonly used M2M protocols (HTTP, CoAP, MQTT). oneM2M MAS deals with the technical aspects related to management of M2M entities and/or functions. It also deals with support for application specific abstraction and semantics. oneM2M TST WG identifies and defines test requirements for the oneM2M system and the services related to it. It also develops and maintains a set of specifications for conformance and interoperability testing. http://www.onem2m.org/technical/latest-drafts . oneM2M correspondent standard number: oneM2M TS 0001 2.10.0; oneM2M TS 0004 2.7.1; oneM2M TS 0012 2.0.0; oneM2M TS 0013 1.0.0; oneM2M TS 0014 2.0.0; oneM2M TS 0015 2.0.0; oneM2M-TS-0018-V-0.1.8 oneM2M TS 0121 2.0.0; oneM2M TS 0123 2.0.0; oneM2M TS 0124 2.0.0	
SAE	J2945: DSRC Minimum Performance Requirements (work in progress)	SAE J2945 specifies the minimum communication performance requirements of the DSRC Message sets, the associated data frames and data elements defined in SAE J2735 DSRC Message Set Dictionary. The document consists of multiple sections. Each section describes a specific message set's requirements. For example, J2945-1 represents Basic Safety Message communication minimum performance requirements.	Integration/ Interoperability
WiFi Alliance	Certification: Wi-Fi Test Suite	The Wi-Fi Test Suite is a software platform to support certification program development and device certification. http://www.wi-fi.org/certification/wi-fi-test-suite .	Integration/ Interoperability
CCC	MirrorLink	The MirrorLink specifications contain features for Device and App discovery, control and easy configuration by the user, Remote UI in the vehicles (smartphone screen replication, UPnP®, audio control). http://www.mirrorlink.com/ .	Application

SDO	Standards	Description/Analysis	Knowledge Areas
CEN/ISO	ISO 24102 Intelligent transport systems; Communications access for land mobiles (CALM); ITS station management ISO 24101 Intelligent transport systems - Communications access for land mobiles (CALM) - Application management	These standards specify the management of ITS-Stations and their applications.	Application
IEEE P1609	IEEE 1609.12: WAVE - PSID Identifier Allocations	IEEE 1609.12 defines the values allocated for WAVE application identifiers.	Application
OSGi	Part of OSGi Core Release 6 Specification	The OSGi technology also provides flexible remote management and interoperability for applications and services over a broad variety of devices and a variety of defined communication and messaging protocols, including UPnP, TR069, OMA DM, HTTP/REST, JSON-RPC. https://www.osgi.org/developer/downloads/release-6/release-6-download/ .	Application
3GPP	GSM, GPRS, EDGE, UMTS, HSPA, LTE, LTEAdvanced and LTE-ADVANCED PRO (4.5G)	Thanks to wide coverage, mobility support, and good data transfer, a cellular radio network is a proper communication infrastructure for the IoT. However, due to the shared radio resources, the great number of connected things, the communications characteristics (periodic, small data messages, etc.), rather than connecting all things, a cellular radio network is more likely to connect some devices (gateways, user devices, etc.) depending on the application scenario.	Infrastructure
CEN/ISO	EN 16072 Intelligent transport systems - Esafety -Pan-European eCall operating requirements EN 16062 Intelligent transport systems - Esafety - eCall high level application requirements (HLAP) using GSM/UMTS circuit switched networks.	These standards specify the infrastructure for the eCall functionality.	Infrastructure

SDO	Standards	Description/Analysis	Knowledge Areas
ETSI TC ITS	ETSI EN 302 636 .	<p>Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network architecture.</p> <p>This standard specifies the network architecture for communication-based Intelligent Transport Systems (ITS).</p> <p>The network architecture is focused on, but not limited to, vehicular communication. The architecture enables a wide range of ITS applications for road safety, traffic efficiency as well as for infotainment and business.</p>	Infrastructure
IEEE	802.11s (Public WiFi)	<p>The 802.11 standards specify a configuration where Wi-Fi devices connect through a mesh topology allowing the deployment of a Wi-Fi infrastructure. Public Wi-Fi networks can be a key technology for some Smart City applications. Indeed, a Wi-Fi-grade wireless network may enable various IoT applications through the provision of high data rate and low latency communication network; and can be very convenient for connecting mobile gateways.</p>	Infrastructure
IEC	IEC 61508	<p>IEC 61508 is an international standard published by the International Electrotechnical Commission of rules applied in industry. It is titled Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES).</p> <p>IEC 61508 is intended to be a basic functional safety standard applicable to all kinds of industry. It defines functional safety as: "part of the overall safety relating to the EUC (Equipment Under Control) and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities".</p> <p>The standard covers the complete safety life cycle, and may need interpretation to develop sector specific standards.</p>	Infrastructure

SDO	Standards	Description/Analysis	Knowledge Areas
ISO	ISO 26262 Road vehicles - Functional safety	<p>International standard for functional safety of electrical and/or electronic systems in production automobiles.</p> <p>The standard ISO 26262 is an adaptation of the Functional Safety standard IEC 61508 for Automotive Electric/Electronic Systems. ISO 26262 defines functional safety for automotive equipment applicable throughout the lifecycle of all automotive electronic and electrical safety related systems.</p> <p>ISO 26262 is a risk-based safety standard, where the risk of hazardous operational situations is qualitatively assessed and safety measures are defined to avoid or control systematic failures and to detect or control random hardware failures, or mitigate their effects.</p> <p>It is intended to be applied to electrical and/or electronic systems installed in "series production passenger cars" with a maximum gross weight of 3 500 kg. It aims to address possible hazards caused by the malfunctioning behaviour of electronic and electrical systems.</p>	Infrastructure
ITU-T	Recommendation ITU G.651, ITU G.652	<p>Optical access networks are supported by Fiber infrastructures.</p> <p>The fiber technology, when available, offers very high speed internet connection for end-users; and permits the implementation of very delay-sensitive applications but also QoS-based applications.</p>	Infrastructure
ITU-T		A VGP (Vehicle Gateway Platform) is being standardized by Question 27/16 in terms of telecommunications. It identifies global Vehicle Gateway standards needed to allow plug and- play of consumer devices working in vehicles and support ubiquitous connectivity in heterogeneous environments for global, seamless services/applications using Intelligent Transportation Systems.	Infrastructure
OAA	New features for Android to allow developers to add car modes to their apps.	<p>The OAA (Open Automotive Alliance) is a global alliance of technology and auto industry manufacturers whose objective is to bringing the Android platform to cars.</p> <p>With OAA enhancements, developers are able to take advantage of template based frameworks which provide app customization for the developer while also providing app familiarization for the driver to reduce distraction.</p> <p>http://www.openautoalliance.net</p>	Infrastructure
OSGi	OSGi Core Release 6 Specification	These specifications enable dynamic and modular end-to-end connectivity and facilitate the componentization of software and applications	Infrastructure

SDO	Standards	Description/Analysis	Knowledge Areas
	OSGi Compendium Release 6 Specification (services)		
3GPP V2X	TR 23.785 (Study on architecture enhancements for LTE support of V2X services) ETSI TS 123 246 (Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description).	The objective of TR 23.785 (under progress) is to study the required enhancements to existing 3GPP architecture and functionalities to support V2X. ETSI TS 123 246 specifies the 3GPP architecture for broadcasting. This is one of the main technologies to be used for Infrastructure-to-Vehicle (I2V) communications. ftp://ftp.3gpp.org/Specs/archive/23_series .	IoT Architecture
AIOTI	IoT high level architecture	AIOTI WG3 has developed a High Level Architecture (HLA) for IoT that should be applicable to AIOTI Large Scale Pilots. The HLA takes into account existing SDOs and alliances architecture specifications. AIOTI WG3 recommends that the HLA be the basis for further discussion with the Large Scale Pilot (LSP) WGs in order to promote architectural convergence among the WGs.	IoT Architecture
CEN/ISO	ISO 21217 Intelligent transport systems - Communications access for land mobiles (CALM) – Architecture	This standard specifies the architecture of the ITS Station. It has been harmonized with ETSI EN 302 665.	IoT Architecture
ETSI ITS	ETSI EN 302 665	ETSI EN 302 665 specifies the architecture of ITS stations in C-ITS supporting a variety of existing and new access technologies and ITS applications. This architecture considers a diverse set of terminals to accommodate the ITS-S: handheld devices, cars, trucks, public vehicles such as buses, but also the traffic lights, VMS or monitoring centers traffic. Mobile ITS-S are housed in mobile devices, typically smartphones or navigators, or in vehicles. The ITS-S infrastructure is divided between roadside ITS-S and central ITS-S, e.g. at traffic management locations. www.etsi.org .	IoT Architecture

SDO	Standards	Description/Analysis	Knowledge Areas
Future Internet Public-Private Partnership (FIPPP)	Fiware	FIWARE or FI-WARE is a middleware platform, driven by the European Union, for the development and global deployment of applications for Future Internet. The API specification of FIWARE is open and royalty-free that facilitate creation and delivery of Future Internet applications and services in a variety of areas, including smart cities, sustainable transport, logistics, renewable energy, and environmental sustainability https://www.fiware.org/ .	IoT Architecture
IEEE P1609	IEEE 1609.0: WAVE -Architecture	IEEE 1609.0 defines the architecture of the WAVE protocol stack and its integration with other protocols from IEEE LAN/MAN and SAE.	IoT Architecture
ISO/IEC JTC1	Information technology - Internet of Things Reference Architecture (IoT RA) (under development)	The IoT RA will specify IoT Conceptual Model, conceptual reference model, and reference architecture from different architectural views, common entities, and interfaces between IoT domains. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=65695 .	IoT Architecture
oneM2M	ETSI TS 118 101 /oneM2M TS 0001 2.10.0 Functional_Architecture	Describes the end-to-end oneM2M functional architecture, including the description of the functional entities and associated reference points. oneM2M functional architecture focuses on the Service Layer aspects and takes Underlying Network-independent view of the end-to-end services.	IoT Architecture
oneM2M	ETSI TR 118 526 /oneM2M-TR-0026 (Vehicular Domain Enablement)	This Technical Report examines how the current oneM2M System can be used in the Vehicular Domain and includes a study of advanced features which the future oneM2M release(s) could support for this vertical domain	IoT Architecture
3GPP	GSM, GPRS, EDGE, UMTS, HSPA,	The 3GPP standards cover Radio, Core Network, and Service Architecture for cellular mobile networks. 3GPP mobile device standards is evolving with releases that are aimed at supporting IoT application	Devices and Sensor Technology

SDO	Standards	Description/Analysis	Knowledge Areas
ETSI TC SES	ETSI TS 103 246 - Satellite Earth Stations and Systems (SES) - GNSS based location systems.	ETSI TS 103 246 describes the functional requirements applicable to location systems, based on a synthesis of types of applications relying on locationrelated data. It provides a generic architecture for GNSS-based location systems (GBLS) that combine GNSS and other navigation technologies with telecommunication networks for delivery of location-based services. It covers the Performance Features for the data provided by the GBLS as well as location data exchange protocols and laboratory tests based on constellation simulators for assessing performances of GBLS. Positioning is an important topic for smart mobility. www.etsi.org .	Devices and Sensor Technology
IEC	IEC 62196: Plugs, socket-outlets, vehicle connectors and vehicle inlets - Conductive charging of electric vehicles	The objective of IEC TC 23 (Electrical accessories) SC 23H (Plugs, Socket-outlets and Couplers for industrial and similar applications, and for Electric Vehicles) is to prepare standards for connection products intended for the connection of electric vehicles to the supply network and/or to dedicated supply equipment. This family of standards specifies the plugs and sockets for the charging of electrical vehicles.	Devices and Sensor Technology
IETF CoRE	IETF RFC 7641 (Observing Resources in the Constrained Application Protocol (CoAP))	The state of a resource on a CoAP server can change over time. This document specifies a simple protocol extension for CoAP that enables CoAP clients to "observe" resources, i.e. to retrieve a representation of a resource and keep this representation updated by the server over a period of time. The protocol follows a besteffort approach for sending new representations to clients and provides eventual consistency between the state observed by each client and the actual resource state at the server. http://datatracker.ietf.org/wg/core/documents/ .	Devices and Sensor Technology

SDO	Standards	Description/Analysis	Knowledge Areas
ISO/IEC	ISO/IEC 29182	<p>The ISO/IEC 29182 series can be used by sensor network designers, software developers, and service providers to meet customer requirements including any applicable interoperability requirements. The ISO/IEC 29182 series are comprised of seven parts:</p> <ul style="list-style-type: none"> • Part 1: General overview and requirements • Part 2: Vocabulary and terminology • Part 3: Reference architecture views • Part 4: Entity models • Part 5: Interface definitions • Part 7: Interoperability guidelines <p>The purpose of the ISO/IEC 29182 series is to provide guidance to facilitate the design and development of sensor networks. Improve interoperability of sensor networks, and make sensor networks plug-and-play, so that it becomes fairly easy to add/remove sensor nodes to/from an existing sensor network.</p> <p>http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45261.</p>	Devices and Sensor Technology
oneM2M	ETSI TS 118 106 /oneM2M TS 0006 2.0.1 (Management enablement (BBF)	<p>Specifies the usage of the BBF TR-069 protocol and the corresponding message flows including normal cases as well as error cases to fulfil the oneM2M management requirements.</p> <p>Includes protocols for managing different devices. Although not so much a device but application that support devices this standards qualifies to be in this section because it is a device management application.</p>	Devices and Sensor Technology

SDO	Standards	Description/Analysis	Knowledge Areas
3GPP	ETSI TS 133 220 Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture Describes the security features and a mechanism to bootstrap authentication and key agreement for application security from the 3GPP AKA mechanism. ETSI TS 133 102 (Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 9)) ETSI TS 121 133 (Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements") ETSI TS 133 120 (Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives".)	3GPP can provide the "bootstrapping of application security" to authenticate the subscriber by defining a generic bootstrapping function based on AKA protocol. 3GPP has a series standards on security that address authentication, bootstrapping: Threats and Requirements" (ETSI TS 121 133) and implement the security objectives and principles described in ETSI TS 133 120. A security mechanism is an element that is used to realise a security feature. All security features and security mechanisms taken together form the security architecture http://www.3gpp.org/ftp/tsg_sa/wg3_security/_specs	Security and Privacy
3GPP V2X	TR 33.885	Study on Security Aspect for LTE support of V2X Services. 3GPP SA3 has identified three key issues to resolve and some resulting requirements for the security in 3GPP support of V2X: V2X communication security, Authorization for LTE-V2X radio resources, V2X Entities secure environment ftp://ftp.3gpp.org/Specs/archive/33_series .	Security and Privacy
CEN/ISO	ISO/TR 12859 ISO/TS 19299	ISO/TR 12859 Intelligent transport systems - System architecture - Privacy aspects in ITS standards and systems ISO/TS 19299 Electronic fee collection - Security framework. These standards tackle the security and privacy issues.	Security and Privacy

SDO	Standards	Description/Analysis	Knowledge Areas
ETSI ITS	ETSI TS 102 940	ETSI TS 102 940 specifies a security architecture for C-ITS communications. It identifies the functional entities required to support security in an ITS environment and the relationships that exist between the entities themselves and the elements of the ITS reference architecture defined in ETSI EN 302 665. It also identifies the roles and locations of a range of security services for the protection of transmitted information and the management of essential security parameters. These include identifier and certificate management, PKI processes and interfaces as well as basic policies and guidelines for trust establishment.	Security and Privacy
Hypercat	Hypercat 3 specification	Hypercat is an open, lightweight JSON-based hypermedia catalogue format for exposing collections of uniform resource identifiers (URLs) for exposing information about IoT assets over the web. Hypercat allows a server to provide a set of resources to a client, each with a set of semantic annotations. Implementers are free to choose or invent any set of annotations to suit their needs. A set of best practices and tools is currently being developed. Using HTTPS, REST and JSON, each Hypercat catalogue may expose any number of URIs, each with any number of resource description framework-like (RDF-like) triple statements about it. http://www.hypercat.io/standard.html	Security and Privacy
IEEE P1609	IEEE 1609.2-2013: WAVE - Security Services for Applications and Management Message.	IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages. This standard defines secure message formats and processing for use by Wireless Access in Vehicular Environments (WAVE) devices, including methods to secure WAVE management messages and methods to secure application messages. It also describes administrative functions necessary to support the core security functions	Security and Privacy
W3C		XML Key Management Specification (XKMS 2.0) Bindings. This is a two part standard. Part 1 of this specification covers the XKMS protocols and services. Part 2 of the W3C Recommendation for the XML Key Management Specification (XKMS Version 2.0) covers different protocol bindings with security characteristics for the XML Key Management Specification the XKMS Activity Statement.	Security and Privacy