Grant Agreement Number: 731993

Project acronym: AUTOPILOT

Project full title: AUTOmated driving Progressed by Internet Of Things

D. 1.10

Final Specification of Security and Privacy for IoT-enhanced AD

Due delivery date: M09 – June 2019

Actual delivery date: 02/10/2019

Organization name of lead participant for this deliverable: THALES

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

Project funded by the European Union's Horizon 2020 Research and Innovation Programme (2014 – 2020)

Document Control Sheet

Deliverable number:	D1.10
Deliverable responsible:	Thales Italia S.p.A.
Workpackage:	WP1
Editor:	Vincenzo Di Massa

Author(s) – in alphabetical order		
Name	**Organisation**	**E-mail**
Andrea BASTIANELLI	Thales Italia S.p.A.	andrea.bastianelli@thalesgroup.com
Arash KHABBZ SABERI	TNO	arash.khabbazsaberi@tno.nl
Bram VAN DEN ENDE	TNO	bram.vandenende@tno.nl
Bruno ROUCHOUZE	GEM (Gemalto)	Bruno.ROUCHOUZE@gemalto.com
Carlotta FIRMANI	Thales Italia S.p.A.	carlotta.firmani@thalesgroup.com
Cedric CHAPUIS	CONTI (Continental)	Cedric.Chapuis@continental-corporation.com
Daniele BREVI	ISMB	brevi@ismb.it
Enrico FERRARA	ISMB	ferrera@ismb.it
Guido GAVILANES	ISMB	gavilanes@ismb.it
Herve MARCASUZAA	VCDA (Valeo)	herve.marcasuzaa@valeo.com
Ilaria BOSI	ISMB	bosi@ismb.it
Jos DEN OUDEN	TU/e (Un. Eindh.)	j.h.v.d.ouden@tue.nl
Martin DAVID	GEM (Gemalto)	martin.david@gemalto.com
Petr STURC	GEM (Gemalto)	petr.sturc@gemalto.com
Sven JANSEN	TNO	sven.jansen@tno.nl
Vincenzo DI MASSA	Thales Italia S.p.A.	vincenzo.dimassa@thalesgroup.com

Document Revision History			
Version	**Date**	**Modifications Introduced**	
		Modification Reason	**Modified by**
V. 0.1.0	30/05/2019	First Draft of D1.10	Vincenzo Di Massa (THA)
V1.0	25/09/2019	Editorial check	Rita Bhandari (ERT)
V1.04	02/10/2019	Final for submission	Rita Bhandari (ERT)

Abstract

This document, 'Final Specification of Security and Privacy for IoT-enhanced AD', analyses the effect of risk identification related to the AUTOPILOT open IoT platform for autonomous driving. Following D1.9 it identifies and confirms the information assets of the system, the relevant stakeholders and the stakeholders' value for a given asset (Confidentiality, Integrity, Availability, Accountability and Authenticity).

It then identifies the system's vulnerabilities with regard to the system interfaces, the user interfaces (including management, administration and support interfaces), the physical location of the assets and the shared communications links with other services.

The identification of the system's assets and vulnerabilities is followed by establishing and quantifying security risks by assigning a probability value and listing the impact for each risk.

After the risk analysis, the document makes recommendations for security in Automated Driving.

The effect of the initial specification on AUTOPILOT development is then analysed and advice and considerations are given originating from experience.

Legal Disclaimer

Abbreviations and Acronyms

Acronym	Definition
EC	European Commission
PO	Project officer
GA	Grant Agreement
WP	Work Package
AA	Authorization Authority
AD	Autonomous Driving
AVP	Automated Valet Parking
BSA	Basic Set of Applications
CA	Co-operative Awareness
CAM	Cooperative Awareness Messages
CeH	Connected Electronic Horizon
C-ITS	Cooperative Intelligent Transport Systems
COTS	Commercial off-the-shelf
DENM	Decentralized Environmental Notification Message
DoS	Denial of Service
ETSI	European Telecommunications Standards Institute
FCA	Fiat Chrysler Automobiles
GDPR	General Data Protection Regulation
HMI	Human Machine Interface
IACS	Industrial Automation Control System
IoT	Internet of Things
IP	Internet Protocol
ISA	International Society of Automation
ISMS	International Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITS	Intelligent Transport Systems
LTE	Long Term Evolution
M2M	Machine – to – Machine
MPD	Massive Parallel Database
OBU	On-Board Unit
OSI	Open Systems Interconnection
PKI	Public Keying Infrastructure
PMI	Privilege Management Infrastructure
PoI	Point Of Interest
PS	Pilot Site
QoS	Quality of Service
RSU	Road Side Unit
SL	Security Level
TCC	Traffic Control Centre
TCP/IP	Transmission Control Protocol / Internet Protocol
TLC	Traffic Light Controller
ToE	Target of Evaluation
TVRA	Threat, Vulnerability and Risk Analysis
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle

V2X	Vehicle to Any
VRU	Vulnerable Road User (e.g. pedestrian, cyclist)
WSN	Wireless Sensor Network

Table of Contents

List of Figures

List of Tables

Executive Summary

With the increasing adoption of IoT, new security challenges need to be addressed as the threat of attacks is moving from the digital to the physical world, leading to even more severe safety implications.

Many operational systems are moving from closed, or not interoperable systems and protocols (e.g., SCADA, Modbus, CIP), to open networks of internet-connected devices that further expand the attack surface. Many of the vulnerabilities in IoT could be mitigated through a security–by-design approach. However, several IoT devices, today, do not incorporate even basic security measures.

Security is critical to the adoption of IoT, especially in AUTOPILOT, because we want to make sure we can "trust" data flowing between sensors, actuators, rules engines and other connected components of our architecture. Furthermore, when IoT devices are used for AD (Autonomous Driving) functionalities, as addressed by the AUTOPILOT project, security aspects must be stressed because matters of safety and national security may be at stake. Autonomous vehicles, if used as a weapon, would cause substantial harm to people and societies.

The analysis does not include different stakeholders that are responsible for these different objectives, such as safety, national security, ICT security.

Stakeholders can address these IoT security challenges around the following principles:

- Incorporate security at the design phase;
- Provide advanced security updates and vulnerability management;
- Build on proven security practices;
- Prioritize security measures according to potential impact;
- Promote transparency across IoT;
- Connect carefully and deliberately.

The existing security technologies and methodologies need to evolve from their current status to address all the new IoT an AD security issues. This document collects the state of the art information about AD in IoT, highlights the related threats and challenges, and provides guidance on how to address them with today's best practices.

As a takeaway from the AUTOPILOT project, we can highlight the importance to follow a security-by-design approach in order to achieve the project's security goals. The remarkable work conducted on AUTOPILOT has produced a clear understanding of the security needs for an IoT-enhanced AD infrastructure. Such information, distilled in particular into the risk analysis, was achieved during the initial project design Phase and gave inputs to the partners about the risks and security requirements involved. As a possible further improvement on this process the authors of this document suggest including a high level risk analysis during the initial project proposition, before the start of the project, so that more knowledge is available to allocate tasks that derive from the project risk analysis, and so that all partners are aware of the security needs of the project from their very first involvement.

1 Introduction

The scope of AUTOPILOT covers both autonomous driving (AD) and the Internet of Things (IoT) by leveraging the latter to provide better Intelligent Transport Systems (ITS) applications.

The hybrid nature of the project is reflected in this document: some use cases described in the project are heavily built on top of ETSI ITS-G5 standards [1] and enriched using IoT technologies and platforms.

The Security, Privacy and Data Models for this project can thus be seen as an evolution of ITS methodologies that integrate IoT measures. The AUTOPILOT risks, threats, assets and stakeholders are a superset of those of ITS and IoT.

In the AUTOPILOT context, the traditional confidentiality, integrity, non-repudiation, availability, authenticity and accountability security objectives must all come after safety and must help to ensure safety.

Safety, even though it is not strictly in the scope of this document, has major weight in deciding the risk ranking, the mitigations and the requirements for AUTOPILOT. For this reason it has been taken into account as a key aspect while performing the risk analysis.

As perfect security does not exist, the design of security features in a safety-critical environment always puts safety as the top priority. ETSI, as in the ETSI TR 102 893 [2], addresses the core threats, risks and vulnerabilities for ITS-G5.

In this document we present the AUTOPILOT open IoT platform for AD, which makes use of ITS-G5, and specify security and privacy approaches building on top of ETSI results. The document also provides references to several standards that cover security and privacy.

It is not in the scope of this document to analyse the low-level security details of the used communication technologies (e.g., LTE or Wi-Fi).

The purpose of the D1.9 deliverable, which was the result of work package 1, "Task 1.5, Security, privacy and data Specification", was to frame and guide the security and privacy developments for the AUTOPILOT project. This "Final Specification of Security and Privacy for IoT-enhanced AD", D1.10 document, is an updated version of the specification that has been written at the beginning of the AUTOPILOT project.

1.1 Purpose of the document

This document serves as the "Final Specification of Security and Privacy for IoT-enhanced AD: specification of security and privacy requirements". The requirements cover identified use cases, having as a reference the specified architecture and selected communication technologies.
This document is an update of D1.9 which was the overall guidance document for security and privacy in AUTOPILOT. The requirements identified are linked to relevant standards, so that engineers initially not fully familiar with security had links and entry points to guide their design choices. The document includes an analysis of the various security standards that are relevant to AUTOPILOT.

This document is organized in 6 sections.
Section 1 provides general introduction.
2 describes an overall view of the AUTOPILOT project and presents a summary of the use case and pilot site architectures and communication specifications based on deliverables D1.1 [4], D1.3 [5], and D1.7[6].

Section 3 defines the target of the evaluation and identifies key risks associated with the AUTOPILOT use cases in terms of security and privacy.
4 presents a critical assessment of the standards used in the project.
5 presents the state of the art in IoT security and privacy.
Section 6 defines the security and privacy requirements for AUTOPILOT taking into account and the risk analysis of 3 and referencing the architectures from T1.2 [7] and T1.3 [8] architectures and the communication specification from T1.4 [9].

1.2 Intended audience

This document is the final security and privacy specification of the AUTOPILOT project. As such, it contains a high-level set of controls used for designing and implementing security and privacy in the project.
D1.9 introduced the security and privacy standards, concepts and technologies relevant to the AUTOPILOT project.
The requirements in section 6.2 are derived by applying standard mitigations on top of risk analysis. The reader can use the same risk analysis to derive more or different requirements from other standards.

1.3 Terminology

End user: Functional agent directly representing the human user of the ITS or the ITS service provider [2].
ITS-G5: Access technology to be used in frequency bands dedicated to European Intelligent Transport System (ITS) [1].
Attack: Assault on a system that derives from an intelligent threat [10].
Availability: Property of ensuring timely and reliable access to, and use of, control system (as defined by the ISA IEC 62443 standard) information and functionality [10].
Incident: Event that is not part of the expected operation of a system or service that causes, or may cause, an interruption to, or a reduction in, the quality of the service provided by the control system [10].
Security level: Measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner [10].
Industrial automation and control system: Collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation [10].

2 AUTOPILOT Overall Architecture

2.1 AUTOPILOT Security and Privacy Architecture

The AUTOPILOT security and privacy architecture closely follows, uses and extends the ITS architecture.
A high-level view of the ITS architecture is shown in Figure 1, where a number of security interfaces allow security services to be provided at different levels. The diagram shows how the security component is connected to all the other components of the ITS architecture.

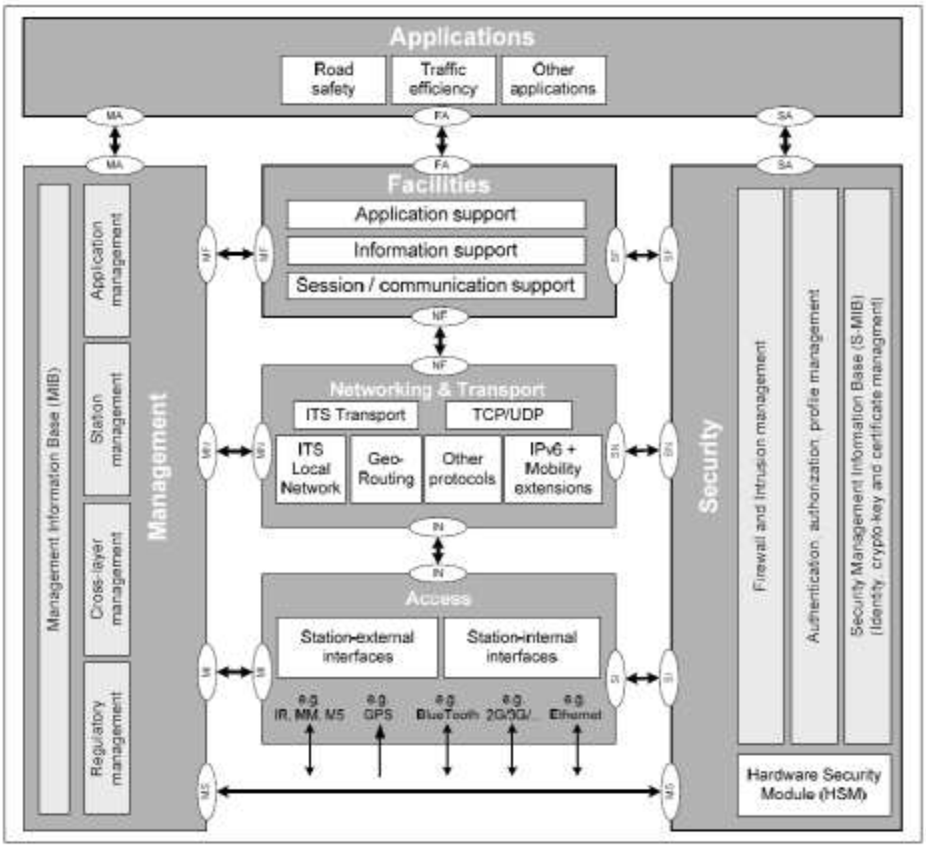


Figure 1 – Examples of possible elements in the ITS station reference architecture, taken from [11]

On top of the ITS architecture, AUTOPILOT introduces IoT functionalities which also must be secure and conform to privacy principles.
A simplified IoT security model is offered by ITU-T Recommendation Y.2060 [12] through the security capabilities layer reported in Figure 2. It includes generic security capabilities that are independent of applications.
ITU-T Y.2060, which provides an overview of the Internet of Things, clarifies the concept and scope of IoT, identifies the fundamental characteristics and high-level requirements of the IoT and describes the IoT reference model [12]. In addition, the Recommendation ITU-T Y.2060 [12] lists the following as examples of generic security capabilities, as illustrated in Figure 2:

- **Application Layer:** authorization, authentication, and application data confidentiality and integrity protection, privacy protection, security audit, and anti-virus;
- **Network Layer:** authorization, authentication, user data, and signalling data confidentiality, and signalling integrity protection;

- **Device Layer:** authentication, authorization, device-integrity validation, access control, data confidentiality, and integrity protection.

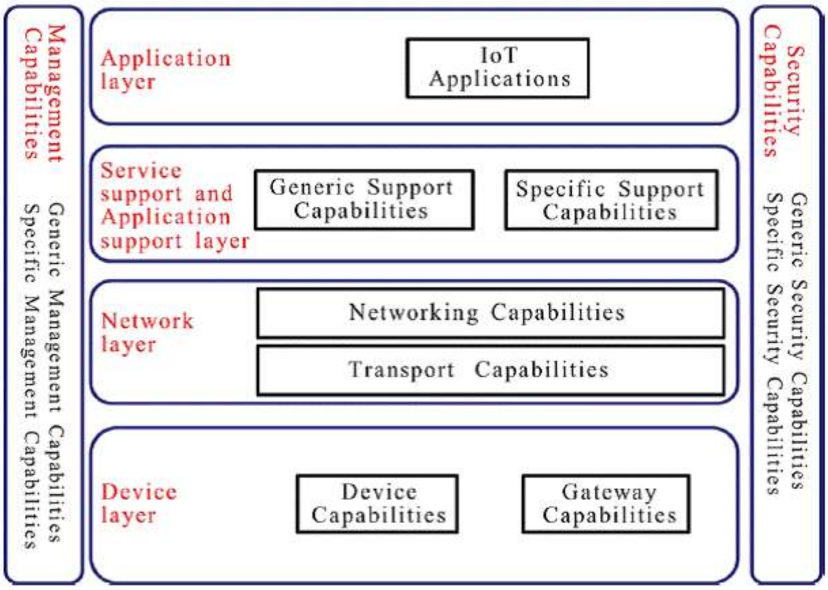


Figure 2 – ITU-T Recommendation Y.2060 IoT Reference Model, taken from [12]

As can be seen comparing Figure 1 and Figure 2, the IoT and ITS approaches are very similar in structure.
The differences are of course in the detailed specifications, but the overall approach can be shared. For this reason, this document will not address the ITS and IoT aspects separately, rather it will tackle the security and privacy requirements for both aspects at the same time.
As the ETSI and IoT architectures are similar in principle, in AUTOPILOT we choose to adhere to the ETSI architecture (Figure 1) [11].

2.2 Input from Other Tasks

2.2.1 Use cases

As reported in D1.1 and D1.2 we now provide here a brief description of the Use Cases for the AUTOPILOT project. For latest details, please see D1.2.

2.2.1.1 Automated Valet Parking

This use case is a driverless AD use case including on-street car drop-off, driving to and from a parking spot, forward and backward manoeuvring and on-street passenger pickup.
This use case has two main scenarios: namely autonomous parking of the vehicle and autonomous collection of the vehicle.
In the first scenario, the vehicle parks itself after the driver has left it at the drop-off point, while in the second scenario the driver will request the vehicle to drive itself to the pickup point.

2.2.1.2 Highway Pilot

In this use case the driver must deliberately activate the automated driving on motorways from entrance to exit, on all lanes, additionally he does not have to monitor the system constantly.
At the first stage of the project, vehicles can only rely on information collected within the range and capabilities of their own sensors.

The Highway Pilot provides road hazard warning and adaptations of the driving considering those hazards.

2.2.1.3 Platooning

This use case focuses on platoon scheduling and organization, from complex road networks towards motorway platooning.
There are various starting configurations of the platoon's assembly process and vehicle types, congestion levels of traffic, different penetration rates of legacy traffic connected to the platooning system, and specific (potential) interactions with legacy traffic, but the main two variants of platooning are:

- An urban variant to enable car rebalancing of a group of vehicles, involving one driver only;
- A highway variant at Brainport, exploring also the use of a dedicated lane (emergency lane).

2.2.1.4 Urban Driving

In the urban driving use case, a fully automated vehicle is able to handle all driving from point A to point B without the passenger's input, as described in the ERTRAC "Fully Automated Private Vehicle" [13] representing the SAE Level 5 "Full driving automation". The driver can override or switch-off the system at any time.
Two main situations are described in this use case: the road intersection equipped with traffic light and the VRUs detection and collaborative perception. In fact, the main research questions for urban driving are related to the interaction with traffic lights and legacy traffic, robustness and safety when dealing with vulnerable road users and positioning. In this context, the vehicle will become an IoT element, gathering relevant information and data from IoT connected elements, such as traffic lights, cameras or other connected vehicles.

2.2.2 Pilot Sites

As per the Grant Agreement, the AUTOPILOT project will develop new services on top of the IoT eco-system using five permanent large-scale pilot sites located in Europe, namely Finland, France, Netherland, Italy and Spain, plus one in Daejeon – South Korea.

In this section we briefly describe the main permanent pilot sites. For a more specific description of these different use cases see D1.1 [4].

- **FINLAND – Tampere:** The Tampere pilot site focuses on urban driving and automated valet parking. Users can access AD cars and use their smartphones or the vehicle's HMI (Human Machine Interface) to select a destination in which a parking-spot is automatically booked before leaving. During the trip, the car interacts with signalling devices like intelligent traffic lights that use cameras to detect non-AD road users. The car can autonomously reach (monitored by the control room) the parking after dropping off the user.
- **FRANCE – Versailles:** The Versailles pilot site focuses on tourist applications that enable users to share cars, offering a range of connected services and local business localization tools that drive them autonomously from sharing stations through the "Château de Versailles" (Level 4 AD) area and in the streets of Versailles. Fleet rebalancing and platooning are used to strengthen the business model. The autonomous small fleet will use a range of POI (Point Of Interest) detection technologies (satellite, pattern recognition, QR Codes, beams and RFIDS) and it uses VEDECOM vehicles equipped with IoT AD functions. Moreover, the system will provide a fleet manager HMI purposed at using platooning technology to rebalance the fleet.
- **NETHERLANDS – Brainport:** In the Netherlands pilot site, different use cases will be

implemented. First of all, there is the platooning of two or more vehicles from Helmond to Eindhoven using the motorway in which people can make themselves available as potential platoon leaders. The second use case, entitled “driverless car rebalancing”, pertains to the rebalancing of a number of shared driverless cars over a set of pickup locations, depending on user demands. In the third use case, entitled “automated valet parking”, an unmanned vehicle is driven automatically starting from a drop-off location to a parking spot. The procedure is assisted by some cameras, drones or other IoT-enabled vehicles, the vehicle has an obstacle-free route to a parking position.
Finally, in the highway pilot use case, a cloud service merges the sensor measurements from different IoT devices (in particular from vehicles and roadside cameras) in order to locate and characterize road hazards (potholes, bumps, fallen objects, etc.). The goal is then to provide incoming vehicles with meaningful warnings and adequate driving recommendations (taken into account by the autonomous/assisted driving functions) to manage the hazards in a safer or more pleasant way. Built upon collective learning of IoT, this 6th sense anticipation mechanism aims at replicating the human driving experience and road awareness in autonomous vehicles.

- **ITALY – Livorno:** The Italian pilot site implemented three main services related to:
    - Highway: with the road hazard on the roadway, roadway works with the traffic control centre (TCC) in the loop, surface road condition and in which the IoT enabled speed adaptation and lane change;
    - Urban: the VRU uses cameras in order to monitor and detect pedestrians, connected bicycles and road surface conditions, increasing road safety;
    - Highway and Urban: this use case mainly focuses on data crowdsourcing from IoT with pothole and surface road condition detection, Bluetooth and Wi-Fi MAC address detection and CAM-DENM detection from V2I.
- **SPAIN – Vigo:** The Spanish pilot site presents two different use cases: urban autopilot and automated parking. Urban autopilot is assisted by IoT and it foresees the adaptation of speed in urban roads in autonomous mode and early reaction to potential warnings. The innovation that the second use case brings to the project is the indoor positioning inside the parking lot. The vehicles using also data provided by the IoT platform, can park autonomously. Drivers are required to use a parking app in order to retrieve the car. The driver requests the car to exit the parking and waits for it to reach him. This last use case is called Automated Valet parking.
- **KOREA – Daejeon**: this pilot site is focusing on the Urban Driving use case, especially in the deployment of an Intersection Safety Information (ISI) System [D1.2]. This system is configured to warn vehicles about many obstacles like pedestrians and other vehicles crossing the road and traffic signal phases [D1.2]. A radar detects pedestrian and it send the information to the OBCU equipped in the vehicles. The OBCU receives the information and displays it in the User Interface

2.2.3 Architecture

The architecture adopted for each of the above use cases is described in the following subsections.

2.2.3.1 Automated Valet Parking

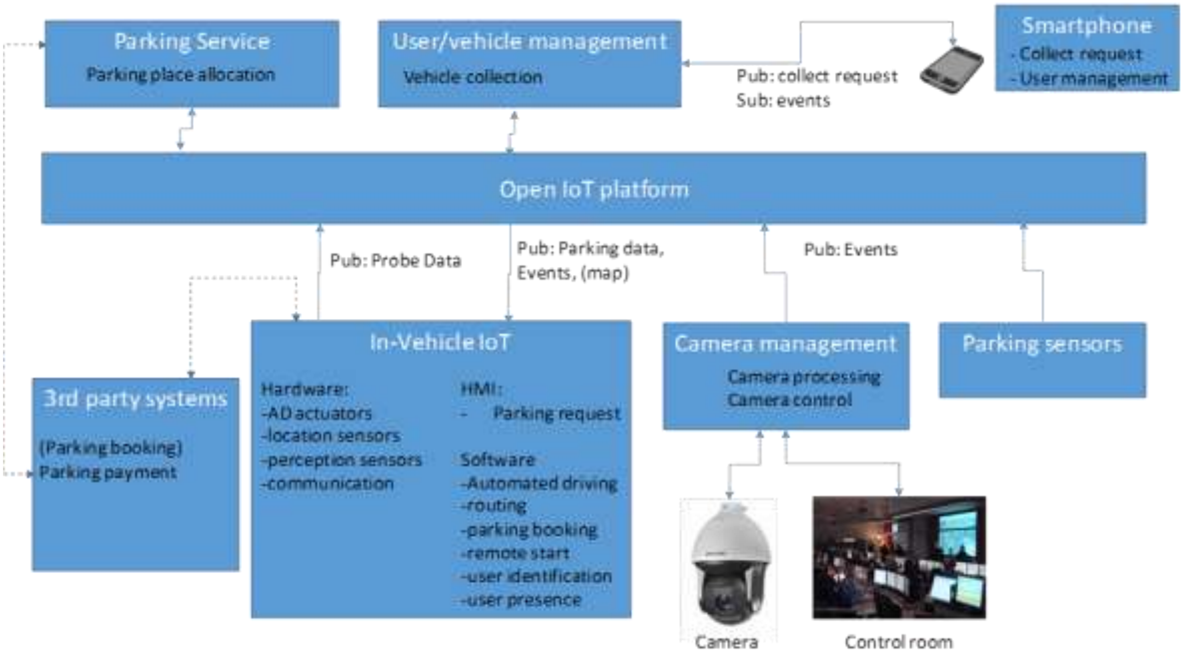


Figure 3 – Example of Automated Valet Parking Architecture, taken from D1.3 [5]

The components of the automated valet parking use case architecture (see Figure 3) are explained below.

- Autonomous Vehicle: equipped with in-vehicle sensors, this vehicle has functionalities for detecting that the driver has left the vehicle, for driving to the destination and for avoiding obstacles;
- Parking Camera Management: camera processing equipment sends events on detected objects and/or information on parking place availability to the IoT Platform. For monitoring and controlling the movement of unmanned vehicles, a control room may be needed;
- Smartphone: it contains the application for collecting the vehicle;
- User/Vehicle Management Service: it handles vehicle collection requests and submits validated collection requests to the vehicle;
- Parking Service: handles parking spot requests and allocates parking spots to vehicles;
- 3rd party systems: any external system that may be connected to the AVP system.

2.2.3.2 Highway Pilot

The main goal of this Use Case concerns the combined use of IoT and C-ITS. The IoT sensors send an alert to the road side unit (RSU) using IoT standard protocols. The RSU broadcasts the info to the vehicle (DENM) and the traffic control centre (TCC). The latter validates the alert and forwards the DENM message to remote RSUs. The TCC, at the same time, feeds the oneM2M platform with alert related data.

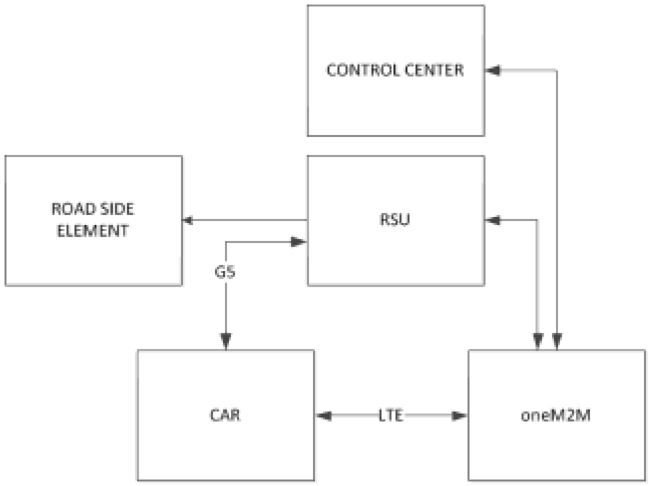


Figure 4 – Initial Highway Pilot Architecture

The combination of the "long range" information provided by IoT and the related cloud, and "short range" information provided by ITS-G5 notifications is expected to enhance the capability of an AD vehicle to perform manoeuvers with relaxed response time requirements. Figure 4 shows a possible architecture for this use case.

The Highway Pilot use case in Brainport will implement an overhead architecture where the car can upload its IoT sensor measurements, over LTE, through the IoT platform and up to a cloud platform On the cloud the regular process of immediate alerting as described above is enhanced by means of algorithms that can learn in real-time the changing road condition. Upon detection of a hazard in the analysed data, the cloud will trigger an alert that will propagate down following the architecture of Figure 4.

2.2.3.3 Platooning

Platooning is an AD application where fully automated driving or driverless vehicles will join and drive in a platoon with a leading vehicle in front. Driving in a platoon requires vehicles to use advanced V2V communications.

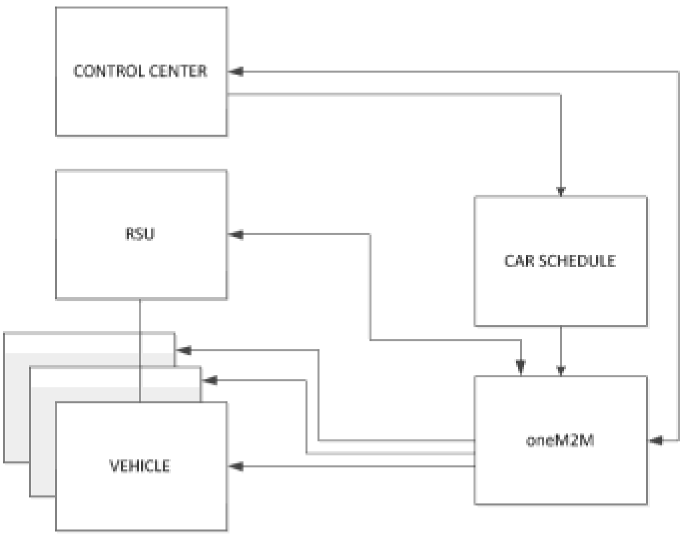


Figure 5 – Initial Platooning Architecture

Such communications use IoT, which makes the car an entity that can be controlled by the application and services.
Data at this level are standardized using common formats, structures and semantics.
Platooning requires low latency V2X communication (ITS-G5 or LTEV2X when available).

2.2.3.4 Urban Driving

The architecture proposed for the urban driving use case allows vehicles to obtain relevant information such as status and time to change traffic lights ahead, presence of pedestrians, or hazards ahead through the application layer.
Vehicles obtain relevant information such as status and time to change traffic lights ahead, presence of pedestrians, or hazards ahead through the application layer.
As can be seen in Figure 6, the main components of this architecture are:

- Vehicles: they connect through cellular communications, such as LTE/3G/4G or through ETSI ITS-G5, to interchange information with the infrastructure or with other connected vehicles;
- Traffic Lights: they provide information about light statuses and times to change;
- VRUs: they provide information about the presence of pedestrians;
- Road smart cameras: they provide information about the presence of pedestrians to the IoT Platform;
- Traffic sensors: they provide information about the traffic status;
- 3rd party services: additional services that can provide useful information about road work warnings, weather warnings, etc.;
- Urban driving services: they provide AD vehicles with the data and functionality required for urban driving, taking into consideration the data provided by the above components (things).

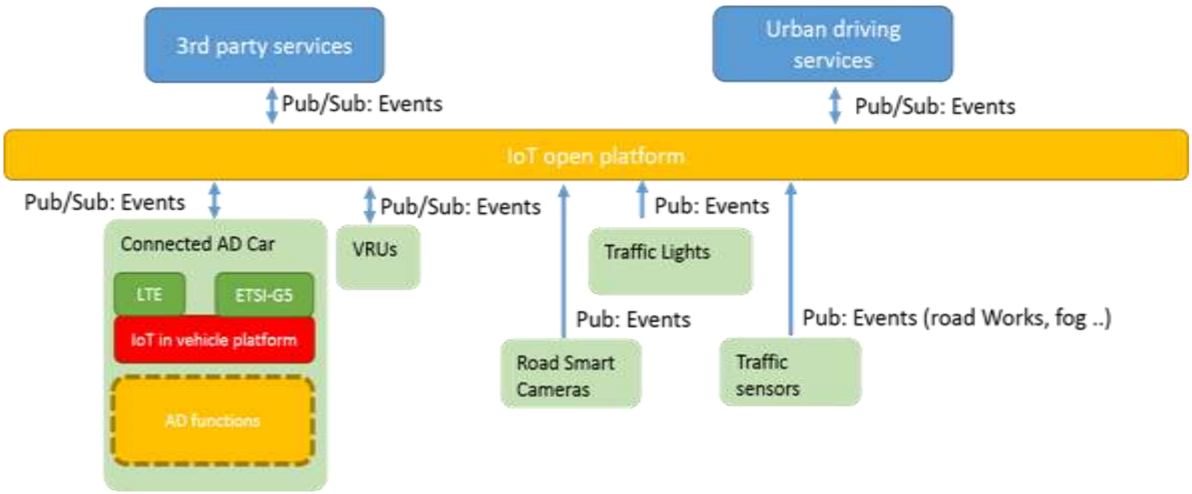


Figure 6 – Example Architecture for Urban Autopilot in Vigo, Taken from D1.3 [5]

2.2.3.5 Ride sharing

The architecture of Figure 7 illustrates the ride sharing use case.

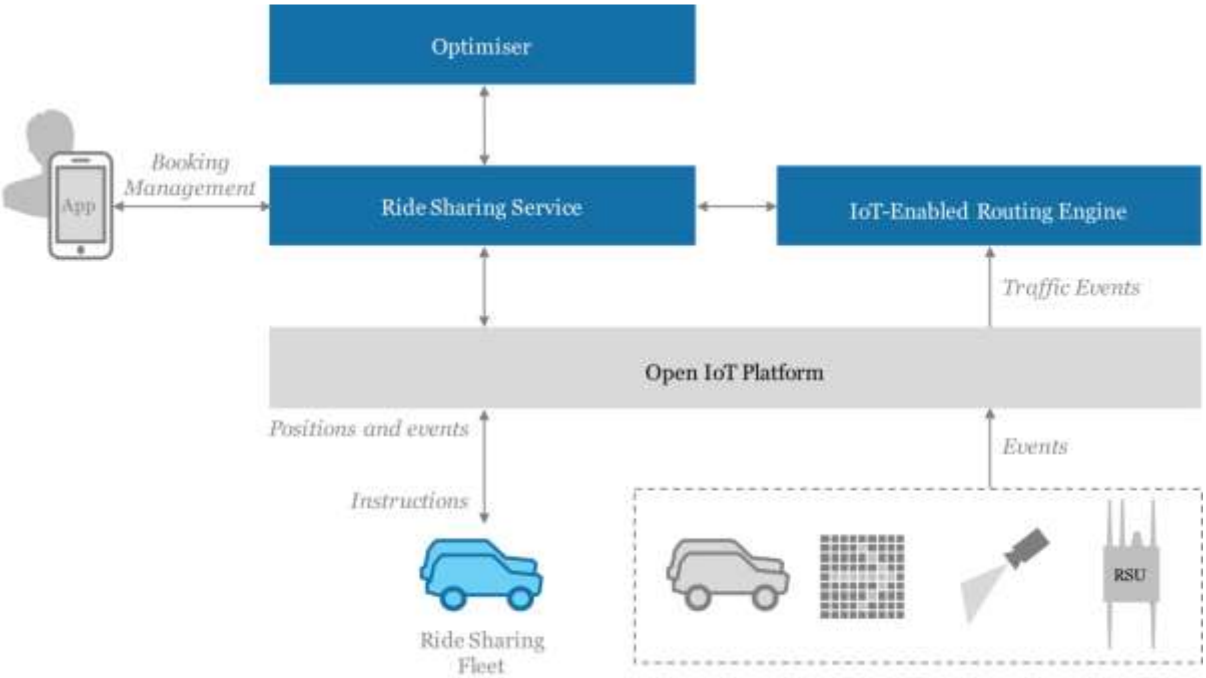


Figure 7 – Ride Sharing Use case Architecture, taken from D1.3 [5]

The open IoT platform allows the shared vehicles to communicate their probe data (GPS locations and speeds) to the car sharing service. It also allows infrastructure sensors and vehicle to publish and share traffic events and situations. The ride sharing service receives booking management requests from customers. It uses an IoT-enabled routing engine to compute potential optimum routes for the shared vehicles to cope with the customer requests. An optimisation module (optimiser) is used to select the optimum routes, pickup, and drop-off locations across all the customer requests.

2.2.4 Communication

The AUTOPILOT communication network is a heterogeneous distributed IoT, V2X and cloud instantiation.
From a security and privacy point of view, this network is mainly built by three building blocks:

- The Cloud IoT platform,
- The V2X and IoT network of connected devices,
- The in-vehicle network.

Therefore, three main network “zones” can be identified :

1. In car IoT network: this zone connects in car devices amongst themselves. As can be seen in Figure 8, various interfaces will be used to connect the on-board devices. This is the most safety critical zone of the system, requiring a high security level. Defining a security perimeter around the safety critical “sub zone” (the one that is connected to the AD decision taking devices) is foreseen. Outside this perimeter, this zone is quite open: potentially all the devices connected to the In-vehicle-IoT-Platform and to another network are potentially vulnerable. Confidential driver data and accounting information may be exchanged between this zone and the external cloud.
2. IoT & V2X networks: this zone covers the medium range communications between the vehicle and its close surroundings. For instance, car to car and car to RSU belong in this zone, which is characterized by short-lived and broadcast connections. Vehicles can send heartbeat-like localization signals using CAM and on-event-messages using DENM, both defined in C-ITS (G5). They will behave like IoT nodes themselves.
3. Cloud IoT platform: this zone collects and exploits data from IoT peripheral devices (e.g. ,

cars, smart cameras, etc.) and provides back control/navigation/optimization data to peripheral devices. Standard IT-security approaches can be recommended to make this zone secure, after covering the AUTOPILOT application specific risks and vulnerabilities.

All functions in one zone have similar requirements but they are not exactly the same.

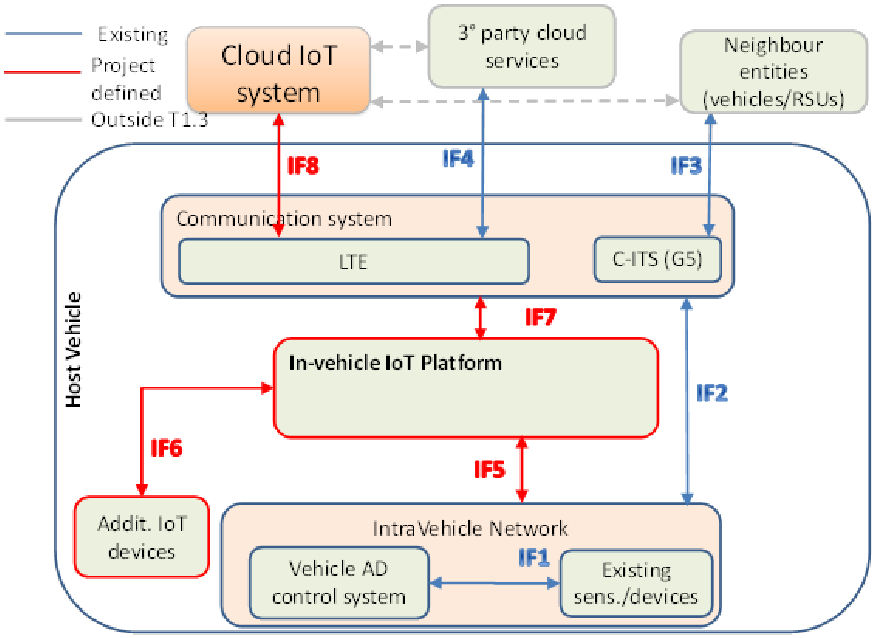


Figure 8 – In car network, taken from D1.5 [14]

All pilot sites share some common characteristics in terms of the network topology, but differ quite substantially in the employed network technologies and protocols: connected devices can be of different types ranging from IoT field devices to cloud infrastructure.
The information flowing through this network is heterogeneous, thus potentially different security and privacy requirements will be applicable.
The table in Figure 9 maps the suitable communication technologies to the various usages and architectural levels of the AUTOPILOT architecture.
Some technologies form heterogeneous stacks, such as IPv4 (yellow), are used as the transport and network component in oneM2M [15], Fiware [16], etc.
Similarly, the 802.15.4 (coloured in grey in Figure 9) is used for Zigbee [17].

2.3 IoT and V2X Security and Privacy Landscape

AUTOPILOT, from a security and privacy point of view, can be considered as a distributed, IoT-enabled, industrial control system [10].
This assumption was the basis of the analysis presented in Section 3, which introduces the most relevant standards for the AUTOPILOT project.
Similar to industrial control systems, AUTOPILOT security threats can compromise safety. But, in contrast with industrial control systems, autonomous cars and ITS infrastructures are very difficult to protect by means of physical measures because of the technologies used and their distributed nature.
The security and privacy standards landscape is rapidly evolving. Security and safety are still, for

historical reasons, described and approached independently even if it is now clear that they are going to become one unascendable topic in the coming years. Standardization bodies are already working towards security-and-safety standards.

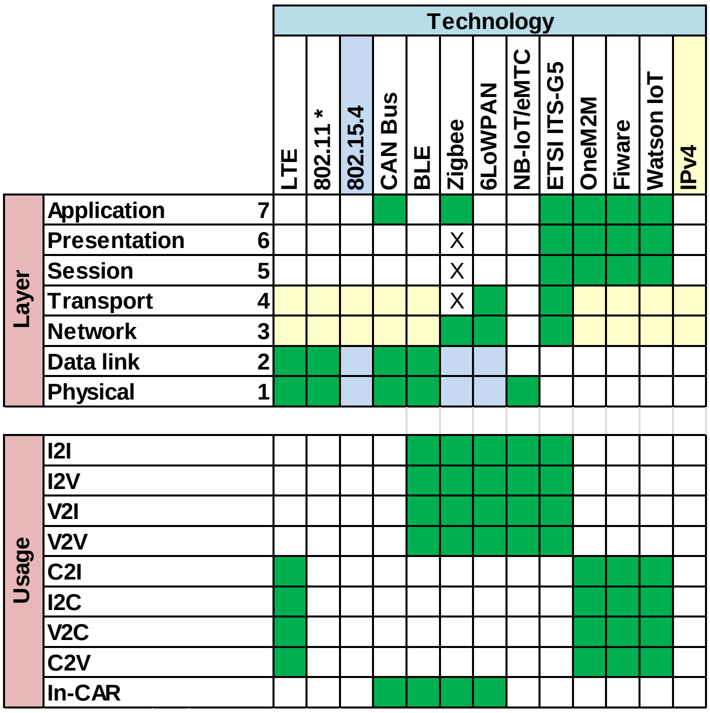


Figure 9 – Map of AUTOPILOT Network Technologies

The current situation is dominated by standards for systems that were traditionally isolated and segregated into air-gapped critical subsystems and non-critical systems. The wide concept of segregation is difficult to apply on wireless networks.

For this reason, this document will analyse several different security and privacy standards. It should be understood, though, that none of these standards can provide exhaustive guidance for the AUTOPILOT specifications.

Our objective is to specify and harmonize a combined set of requirements inspired by the recommendations from different standards.

The most relevant sets of standards for the AUTOPILOT project are the ETSI ITS-G5 [1] series and the ISA/IEC 62443 [10].

In this section, we introduce the relevant standardization bodies and standards.

2.3.1 Standards Organizations

The most relevant and useful standards for the security and privacy analysis are shown in the subsequent paragraphs.

2.3.1.1 International Society of Automation (ISA)

"ISA [18] is a non-profit professional association that sets the standards for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across the industry and critical infrastructures.

Founded in 1945, ISA develops widely used global standards; certifies industry professionals; provides education and training; publishes books and technical articles; hosts conferences and exhibits; and

provides networking and career development programs for its members and customers.
ISA is the developer and applications-focused thought leader behind the world's only consensus-based industrial cybersecurity standard, ISA/IEC 62443 [10]".

2.3.1.2 International Electrotechnical Commission (IEC)
"Founded in 1906, IEC [19] is the world's leading organization for the preparation and publication of International Standards for all electrical, electronic and related technologies. These are known collectively as "electro technology".
IEC publications serve as a basis for national standardization and as a reference when drafting international tenders and contracts [19]".

2.3.1.2.1 ISA/IEC 62443 Series – Industrial Automation and Control Systems Security.

"The ISA/IEC 62443 series of standards have been developed jointly by the ISA99 committee and the IEC Technical Committee to address the need to design cybersecurity robustness and resilience into industrial automation control systems (IACS)".
As reported in [20], the ISA99 committee's focus is to improve the confidentiality, integrity, and availability of components or systems used for manufacturing or control and to provide criteria for procuring and implement secure control systems.
The ISA/IEC 62443 standards define requirements and "procedures for implementing electronically secure automation and control systems and security practices, and assessing electronic security performance [10]".
"The 62443 series addresses the need to design cybersecurity robustness and resilience into IACS. It builds on established standards for the security of general purpose information technology systems (e.g., the ISO/IEC 27000 series [21]), identifying and addressing the important differences present in IACS. Many of these differences are based on the reality that cyber security risks with IACS may have Health, Safety or Environment (HSE) implications and the response should be integrated with other existing risk management practices addressing these risks.
The goal in applying the 62443 series, as reported in [10], is to improve safety, availability, integrity and confidentiality of components or systems used for industrial automation and control, and to provide criteria for procuring and implementing secure industrial automation and control systems.
Conformance with the requirements of the 62443 series is intended to improve electronic security and help identify and address vulnerabilities, reducing the risk of compromising confidential information".
ISA/IEC 62443 [10] defines security levels as a tool to describe the system's resistance level against different attackers ranging from unexperienced "script-kids" to government funded spy agencies.
The ISA/IEC 62443 [10] also defines 7 foundational requirements (FR) that will be used in Section 4:

- FR 1 – Identification & authentication control,
- FR 2 – Use control,
- FR 3 – System integrity,
- FR 4 – Data confidentiality,
- FR 5 – Restricted data flow,
- FR 6 – Timely response to events,
- FR 7 – Resource availability.

2.3.1.3 European Telecommunications Standards Institute (ETSI) (ITS & G5)
ETSI [23] produces globally-applicable standards for information and communication technologies (ICT), including fixed, mobile, radio, converged, broadcast, and Internet Technologies.

2.3.1.4 Automotive Intelligent Transport Systems (ITS)

ITS [24] add information and communications technology to transport infrastructures and vehicles in an attempt to improve their safety, reliability, efficiency and quality.
Intelligent Transport Systems include telematics and all types of communications in vehicles, between vehicles (e.g., car-to-car), and between vehicles and fixed locations (e.g., car-to-infrastructure) [25].
Over recent years, the emphasis in intelligent vehicle research has turned to Cooperative ITS (C-ITS) in which vehicles communicate with each other and/or with the infrastructure.
ITS embrace a wide variety of communication-related applications intended to increase travel safety, minimize environmental impact, improve traffic management and maximize the benefits of transportation to both commercial users and the general public.
As reported in [25], as individual vehicles continuously communicate with each other or with the road infrastructure, the benefit that comes from the stand-alone driver assistance will increase.
The goal is to address the life safety through the reduction of road fatalities and injuries, to address traffic efficiency with a reduction in transport time and the related economic consequences. There are some strong links with the European Commission whose related initiatives aim to stimulate the deployment of ITS [25].

2.3.1.5 oneM2M

oneM2M [26] was launched as a global initiative to ensure the most efficient deployment of Machine-to-Machine (M2M) communication systems and the Internet of Things (IoT).
The oneM2M initiative aims to develop technical specifications to address the need for a common M2M service layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide.

2.3.1.6 International Organization for Standardization (ISO)

ISO [27] is an independent, non-governmental, international organization with a membership of 163 national standards bodies. ISO creates documents that provide requirements, specifications, guidelines, or characteristics that can be consistently used to ensure that materials, products, processes and services are fit for their purpose [27].
The ISO/IEC 27000 [21] family of standards, Information security management systems, helps organizations keep information assets secure.
Also known as the ISO 27000 series, it is developed and published by ISO and the International Electrotechnical Commission to provide a globally recognized framework for best-practice information security management [21].

2.3.1.6.1 ISO/IEC 27000:2016 – Information Technology – Security techniques – Information security management system – Overview and vocabulary

This international standard [28] is applicable to all types and sizes of organizations and provides an overview of information security management systems and terms and definitions commonly used in the ISMS family of standards [28].
This Standard is applicable to all types and sizes of organizations, including commercial and not-for-profit organizations.
Organizations that align their information security practices with the ISO/IEC 27000 standards, citing the standards themselves, can:

- Secure their critical assets;
- Manage risks more effectively;
- Improve and maintain customer confidence;
- Demonstrate conformance to international best practice;
- Avoid brand damage, loss of earnings or potential regulatory fines;
- Evolve their information security posture alongside technological developments [27].

2.3.1.6.2 ISO/IEC 27001:2013 – Information Technology – Security techniques – Information Security Management Systems - Requirements

The ISO/IEC 27001 [29] is the best-known standard in the family providing requirements for an information security management system (ISMS): a systematic approach to managing sensitive company information so that it remains secure for people, processes and IT systems, by applying a risk management process [27].
This standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.
The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

2.3.1.6.3 The ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls

This standard [30] gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).
It is designed to be used by organizations that intend to select controls within the process of implementing and Information Security Management System based on ISO/IEC 27001; implement commonly accepted information security controls; develop their own information security management guidelines [27].

3 AUTOPILOT Risk Evaluation and Assessment

This part of the document presents the key elements used for the security risk assessment that are linked to each other by the following relations:

- **Owners** and other **stakeholders**:
    - Value the **information assets**;
    - Wish to minimize the **risk** to information assets;
    - Impose **countermeasures** to reduce risk to information assets and countermeasures that may pose **vulnerabilities** leading to risk to information assets;
    - May be aware of vulnerabilities leading to risk to information assets.
- Potential **attackers** (**Threat** agents):
    - Make attacks that give rise to threats that **exploit** vulnerabilities, that increase risk and to information assets;
    - Wish to abuse and/or may **damage** information assets.
- Vulnerabilities
    - may be reduced by countermeasures;
- Threats
    - Exploit vulnerabilities that may be reduced by countermeasures and that can lead to risk.

From the security analysis presented here, a few requirements are derived, specifically from privacy and Safety aspects.
See Annexes, in which the detailed risk analysis data is reported.

3.1 Stakeholders

The stakeholders of an operational AUTOPILOT system are listed below with their key interests in, and expectations from, the system.

- Passenger: user that cannot directly communicate with the autonomous driving system (end-user of the transport service but not necessary of the autonomous system):
    - Travel cost optimization,
    - Reduction of driving effort,
    - Travel reliability,
    - Travel availability,
    - Travel safety.
- Driver: end-user of the autonomous driving services that interacts directly with the autonomous driving system:
    - All passenger's interests,
    - Parking availability,
    - Reduction of driving effort,
    - Reduction of driving risk.
- Ride Sharing Driver: end-user of the ride sharing use case that interact directly with the autonomous driving system:
    - All driver's interests,
    - Reliability of passengers,
    - Availability of the ride sharing service,
    - Cost sharing with passengers,
    - Identification of passengers.
- Ride Sharing Passenger: customer of the ride sharing service that does not interact with the autonomous driving system:

  - All passenger's interests,
  - Driver reliability,
  - Availability of the ride sharing service,
  - Identification of the driver.
- Vehicle Owner: direct user of the AD system (driver) that bought the AD system (physical investment):
  - Vehicle availability,
  - Vehicle maintenance cost,
  - Vehicle integrity.
- Vehicle Manufacturer: Vehicle producer that implements and integrates the AD components inside the vehicle:
  - Vehicle safety,
  - Vehicle revenue.
- Pedestrian: part of the AUTOPILOT system who is not an AD user but directly involved in the scenarios:
  - Pedestrian safety,
  - Availability of crossing information,
  - Privacy.
- Other Road Users (Vehicles):
  - Privacy,
  - Traffic safety.
- AUTOPILOT Infrastructure Manufacturer: implements and integrates the AD infrastructure:
  - Infrastructure safety,
  - Infrastructure revenue.
- Infrastructure Operator: participant in charge of monitoring AD infrastructure:
  - Maintenance cost reduction,
  - Fault detection,
  - Traffic efficiency,
  - Infrastructure revenue.
- Police/Authority: force-keeping public order that interacts with the AD infrastructure but which can also be an end user of AD infrastructure:
  - Logging of driver behaviour,
  - Remotely alter traffic,
  - Identification of passengers/drivers.
- Citizen/Local Community: local authority that adopts, interacts, and maintains the AD infrastructure:
  - Pollution reduction,
  - Efficiency of local transport services,
  - Traffic reduction,
  - Traffic noise reduction,
  - Safer roads.
- Security Staff: security operators of AD infrastructure:
  - Confidentiality of design, including:
    - COTS version numbers and patch levels,
    - VLAN IP addresses, routing tables,
  - Confidentiality of user logons and passwords,
  - Availability of security log files,
  - Integrity of security log files.
- Ride sharing, Car parking, and Tourist Service Operator: end user of AD systems:
  - Service revenue,
  - Service availability,

    - Service safety,
    - Service accuracy.

3.2 Information Assets

In order to quantify the impact of cybersecurity threats, it is important to list the information assets that must be protected and to understand their importance to the various stakeholders.
Some information assets are also listed above as part of the stakeholders' interests:

- Communication with ITS infrastructure,
- Communication with IoT Cloud,
- Car location information,
- Communication with car sensors and actuators,
- V2V communication,
- Driver user interface information,
- Passenger's sensitive data,
- Road user and pedestrian sensitive data,
- Vehicle stored information,
- Infrastructure stored information,
- Cloud stored information.

3.3 Interface Types

In this section we define the main interface types used within the AUTOPILOT project.

- AD User Interface: interface that enables users to interact with the AD system. User interfaces include:
    - Smartphone: because it is one of the AUTOPILOT's HMIs,
    - Driver User Interface: driver's digital user interfaces,
    - Software: software running on the user interfaces.
- Vehicle Interface: interface inside the vehicle between the AD system and other infrastructure assets and car components:
    - Cloud Interface: cloud interface of the AD (e.g., oneM2M),
    - Hop-to-Hop interface: direct communication among infrastructure elements and vehicles (V2I, V2V, I2I),
    - In-car generic interface: Bluetooth, Wi-Fi and General Infotainment,
    - Sensor Interface: CAN bus sensor,
    - Actuator interface: CAN bus actuator.
- RSU Interface: interface between RSU and infrastructure assets:
    - Cloud interface: Cloud Interface of the RSU interface (e.g., oneM2M),
    - Hop-to-Hop interface: direct communication amongst infrastructure elements and vehicles (V2I, V2V, I2I).
- Traffic Light Interface: interface between the TLC node and the RSU
    - Hop-to-Hop interface: interface between the Traffic Light and the RSU.
- Camera Interface: interfaces of on-board traffic and pedestrian cameras
    - Cloud Interface: cloud interface between the camera and the infrastructure (e.g., oneM2M),
    - Hop-to-Hop Interface: direct communication between infrastructure elements and vehicles (V2I, V2V, I2I).
- Road Sign Interface: Intelligent road environment (e.g., speed road sign, etc.)
    - Hop-to-Hop interface: interface between component and RSU.
- Sensor interface: intelligent road sensor used for the detection of situations or events, e.g., puddle detection.

3.4 Components & Assets

The AUTOPILOT project involves multiple interconnected components and wireless communications to and from the vehicle. Below is a list of the required information assets, grouped by physical location.
The main physical components within the AUTOPILOT system are:

- In-car: Components inside the car:
  - Sensors and Information Sources,
  - GPS,
  - Long-Range Radio,
  - Hop-to-Hop Radio,
  - In-Car Communication,
  - Driver User Interface,
  - Actuators,
  - AD Engine.
- Infrastructure: components of the autonomous system infrastructure:
  - Traffic Lights: road environment,
  - Camera: road environment,
  - RSU: road environment,
  - Road Signs: road environment,
  - Sensors and Information Sources: road environment,
  - Hop-to-HOP Radio: physical radio component,
  - Long-Range Radio: physical radio component.
- Cloud: long-range interfaces (e.g., Internet):
  - Broker: Pub/Sub message-oriented middleware system,
  - oneM2M Adapter: any kind of adapter defined inside the OneM2M protocol standards.

3.5 Requirements on IoT data attributes

The requirements take into account the privacy and safety aspects of the functionalities described in the architecture chapter.

3.5.1 Privacy aspects

To ensure the privacy of pedestrians and road users, raw camera data from in-vehicle cameras should not be recorded or shared outside of the vehicle. Specifically, faces and licence plates can be the cause of violation of GDPR[1] regulations.

---

[1] General Data Protection Regulation (GDPR) is a new regulation to be enforced on May 2018 that will strengthen and unify data protection for all EU citizens. It will apply to all companies collecting data about EU citizens. In Autopilot scope, collecting data will play a key role for enabling AD and poses challenges as some of them are considered as personal data (see C-ITS platform final report).
'Personal data' encompasses many data types. The most important ones are:
•Identity
•Address
•Localization
•Online Identifier
•Health Information
•Income
•Social / cultural profile
Some guidelines (non-exhaustive)
•Communicate about who collect data and why
•Get consent of end-users
•Provide the 'right to be forgotten' (allow to erase data)

The possibility to track the position users is a privacy threat. Private information retention must be minimized and data should be collected only as obliged by Law enforcement authorities. This also considers the possibility to identify a person using a particular car. Even if the position of the car is a necessary feature for the platform tracking should be possible only for selected personnel with strong access control. The threat of tracking may be lowered by anonymization of the data or by periodically changing identifiers.

3.5.2 Safety aspects

All the information assets that are potentially used by the automated driving control system of the host vehicle (including world model and control) need to include information validation mechanisms. This would help to ensure traffic safety for the vehicle occupants, pedestrians, and other road users. These information assets include (but are not limited to) car location information, communication with car sensors and actuators, V2V communication, and data exchange through car interfaces (part of the AD system control). For all the identified information assets there is a security need to identify the integrity or trustworthiness of the received information. The host vehicle should be able to initiate proper safety measures to prevent any hazard and to set the vehicle to a defined safe state. The specifics of the information validation mechanism depend on the detailed design of a system and interface specification used for each of the information assets mentioned above. However, the validation mechanism should at least provide means to report:

- Known signal failure modes,
- The degree of confidence in the correctness of signal values,
- ASIL capability[2].

When cameras are used as environmental sensors in an automated driving vehicle, the complete sensor delay (from image to detection, tracking, classification) used is typically <50ms in order to guarantee complete closed loop control for automated driving at higher speeds. At low speeds, this delay is allowed to increase to up to 0.5 sec.

- •Let user access its data / move to another database
- •Safeguard the sensitive data
- •Privacy by design (integrate privacy mechanism when designing the application/system)
- •Hire a data protection officer
- •Keep records of all data / processing (data governance)
- •Anticipate with impact assessments

[2] Automotive Safety Integrity Level (ASIL) capability is an indication of integrity of an automotive system that depends on both technical aspect of the system, and the development process of it.

4 Critical Assessment of Standards

The AUTOPILOT project may benefit from the security and privacy standards of various fields.
In fact, AUTOPILOT builds on top of Intelligent Transport Systems, such as ETSI ITS, and, in addition, it aims to exploit IoT technologies in the context of ITS and autonomous driving cars.
From the use cases and safety requirements perspective, AUTOPILOT can also be seen as a distributed industrial control system.
This section will analyse the standards, from the different organizations described in Section 2.3.1 that are relevant to the security and privacy of AUTOPILOT.
It is possible to observe that, from an abstract point of view, all AUTOPILOT use cases are instantiations of ETSI Intelligent Transport Systems. Therefore, the standards that describe the ETSI ITS and G5 technologies can be the basis of the AUTOPILOT security and privacy specifications.
The ETSI ITS series of standards covers the details of security and privacy for the relevant use cases. What is not covered by ETSI ITS itself is related to AUTOPILOT IoT and IACS. Table 1 summarizes the various aspects of the AUTOPILOT project regarding security and the relevant standards.

Table 1 – AUTOPILOT Standards

AUTOPILOT is an	Covered in standards by
Intelligent Transport System	ETSI ITS
IoT Instance	ETSI IoT / oneM2M
Industrial Automation Control System	ISA / IEC 62443

In the remainder of this section, the relevant standards from the above-mentioned organizations will be analysed.
The goal of the evaluation is to define a set of requirements that originate from the standards and that AUTOPILOT can use as guidance for security and privacy.
The analysis starts from ETSI ITS, goes on adding the IoT specific information from oneM2M, and then it is integrated with the ISA/IEC 62443 approach.
This document considers what is most relevant and most characteristic from each of the above standards (e.g., it considers the IACS requirements from the ISA/IEC 62443 series).
At the same time D1.10 combines different and sometimes incompatible statements from different standards. When the incompatibilities are an obstacle, we try to generalise the concepts and to address an abstract and less specific case using generic IT standards (see Table 5).

4.1 V2X Standards

ETSI is the standards organization that best covers the AUTOPILOT ITS use cases and implementation scenarios.
ETSI develops a comprehensive set of standards covering many ITS topics (see e.g. Table 2), in particular the G5 protocols (CAM [31] and DENM [31]).
The use cases that are covered by the ETSI technologies [32] and standards are a subset of the AUTOPILOT ones.
For this reason the ETSI TR 102 893 [2] has been a starting point for the risk analysis in 3n 3.
The ITS system consists of ITS-S (ITS Stations) that can be either vehicles or infrastructure elements.
The ETSI ITS and G5 communication can use LTE or IEEE 802.11-OCB (also known as 802.11p) [33] similarly to the American WAVE (Standard for Wireless Access in Vehicular Environments) [34].
Even if WAVE and ETSI ITS have common roots they diverged and developed different stacks on top of IEEE 802.11-OCB. ETSI standards cover the security and privacy aspects of ITS use cases. For this reason the use of G5 is recommended by D1.9 for all the information assets that can make use of it

in AUTOPILOT: if car localization is to be broadcasted, the preferred AUTOPILOT approach is to use the G5 CAM protocol to broadcast it, because ITS-G5 already covers security and privacy and provides the required level of threat protection. Of course, other approaches can also be used to broadcast localization, but the implementer shall provide at least the same level of protection that G5 provides.

Table 2 – V2X Standard Table

Standardization Body /Source	Standard No	URL - Document should be publicly available	Title
ETSI	TR 102-893	http://www.etsi.org/deliver/etsi_tr/102800_102899/102893/01.01.01_60/tr_102893v010101p.pdf	Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)
ETSI	TS 102 940	http://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.02.01_60/ts_102940v010201p.pdf	Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management
ETSI	TS 102 723-8	http://www.etsi.org/deliver/etsi_ts/102700_102799/10272308/01.01.01_60/ts_10272308v010101p.pdf	Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 8: Interface between security entity and network and transport layer
IEEE	1609.2-2016	http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7544433&tag=1	Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages

4.2 IoT Standards

IoT is not a mainstream technology yet. As such, the IoT landscape is still scattered and no dominant organization has emerged so far as the main IoT standardization body. However, two of the most active organizations in this field are ETSI and oneM2M that publish related standards.
As reported in the related Section 2.3.1.4, oneM2M is a global organization that creates requirements, architectures, API specifications, security solutions, and interoperability for machine-to-machine and IoT technologies.
The oneM2M standards listed in Table 3 provide tools to secure different types of IoT applications with solutions that range from generic recommendations to specific countermeasures for IoT specific threats.
In AUTOPILOT, the oneM2M [35] approach for security procedures (see Figure 10 and Table 3) is used to provide mutual authentication and authorization to AUTOPILOT applications.

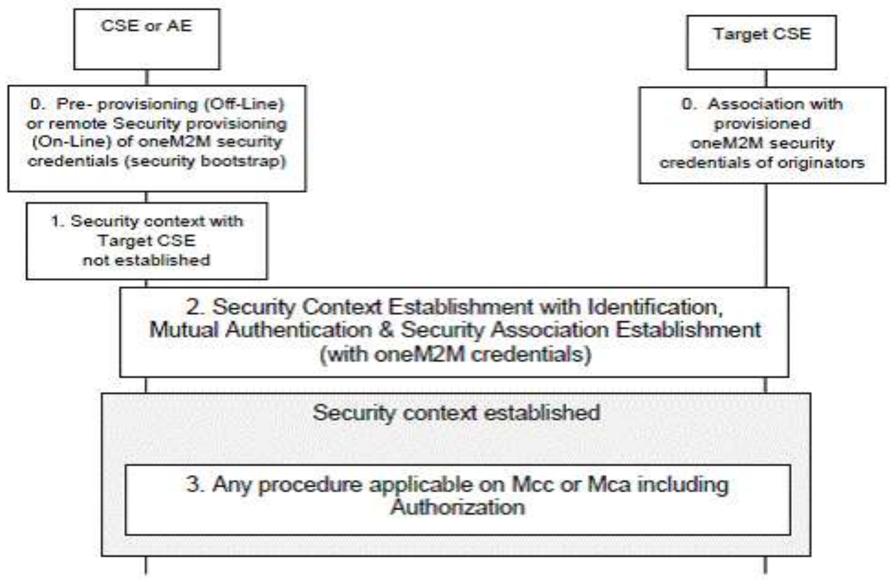


Figure 10 – oneM2M Security Procedures, taken from OneM2M TS-0008 [35]

Of course, AUTOPILOT IoT and V2X functions can use different security procedures as long as the overall requirements in Section 4 are met: if a device (for instance a vehicle) is already authenticated using ETSI G5, the implementer must decide whether to re-authenticate it with the oneM2M applications or just to use the G5 protocols.

Table 3 – IoT Standards Table

Standardization Body /Source	Standard No	URL - Document should be publicly available	Title
oneM2M	TS-0001	http://www.onem2m.org/images/files/deliverables/Release2/TS-0001-%20Functional_Architecture-V2_10_0.pdf	Functional Architecture
oneM2M	TS-0003	http://www.onem2m.org/images/files/deliverables/Release2/TS-0003_Security_Solutions-v2_4_1.pdf	Security Solutions
oneM2M	TR-0008	http://www.onem2m.org/images/files/deliverables/Release2/TR-0008-Security-V2_0_0.pdf	Security
oneM2M	TR 0012	http://www.onem2m.org/images/files/deliverables/Release2/TR-0012-End-to-End-Security_and_Group_Authentication_V2_0_0.pdf	End-to-End Security and Group Authentication
oneM2M	TR 0016	http://www.onem2m.org/images/files/deliverables/Release2/TR-0016-Authorization_Architecture_and_Access_Control_Policy-V2_0_0.pdf	Authorization Architecture and Access Control Policy

Table 4 – IoT Standards Table

Standardization Body /Source	Standard No	URL - Document should be publicly available	Title
oneM2M	TS-0001	http://www.onem2m.org/images/files/deliverables/Release2/TS-0001-	Functional Architecture

		%20Functional_Architecture-V2_10_0.pdf	
oneM2M	TS-0003	http://www.onem2m.org/images/files/deliverables/Release2/TS-0003_Security_Solutions-v2_4_1.pdf	Security Solutions
oneM2M	TS-0008	http://www.onem2m.org/images/files/deliverables/Release2/TR-0008-Security-V2_0_0.pdf	Security
oneM2M	TR 0012	http://www.onem2m.org/images/files/deliverables/Release2/TR-0012-End-to-End-Security_and_Group_Authentication_V2_0_0.pdf	End-to-End Security and Group Authentication
oneM2M	TR 0016	http://www.onem2m.org/images/files/deliverables/Release2/TR-0016-Authorization_Architecture_and_Access_Control_Policy-V2_0_0.pdf	Authorization Architecture and Access Control Policy

Table 5 – IT Generic Standards

Standardization Body /Source	Standard No	URL - Document should be publicly available	Title
ISO/IEC	29100:2011	http://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip	Information technology - Security techniques - Privacy framework
ISO/IEC	27000 series	http://www.27000.org/	Information Security Management systems

4.2.1 Industrial Automation Control Systems Standards

Industrial Automation Control Systems (IACS) standards are already employed as guidance for the development of transportation systems like railways and tramways. A transportation system has many points in common with an IACS, but also some differences. Similarities include the required level of security and availability and the impact of the system on the local economy. Both transportation systems and IACS can be seen as critical infrastructures, most of the time being operated by a single company.

What makes them different is mainly the distributed and public nature of transportation systems. This difference has deep implications on security and privacy requirements: while it is often possible to physically protect an IACS from attackers, by means of physical access control and network segregation, providing the same level of physical protection to a transport system is a challenge.

Following this consideration, the IACS security standards, such as ISA/IES 62443, are useful to provide guidance for some parts of the systems, especially for control centres. Moreover, IACS offers a good approach in which security is analysed in a context where a failure can have very high costs both in terms of human lives and money.

Given that ISA/IEC 62443 is technology-independent, we have been able to use it when analysing requirements, even if we are not designing an IACS.

In fact, even if ETSI and oneM2M give a more detailed set of countermeasures/requirements, they both benefit the high-level approach of ISA/IEC 62443.

5 Review of Current Technology for Security and Privacy in IoT

5.1 IoT Security – State of the Art

Security plays an important role in participative approaches, as the system deeply depends on the collaboration between users. It heavily relies on vehicle position information since traffic information is meaningless without location information. However, malicious third parties may inject wrong data into the system, and masquerade the identity of innocent users. Consequences can be dramatic as a malicious node can lie about its position in order to compromise services provided by the system or perhaps even cause an accident. Therefore, communication needs to be secured in order to avoid any wrong or malicious usage of data collected by the system. Privacy needs also to be considered, as users may want to keep their personal information secret, such as location, speed, etc. For instance, a malicious party can track individual cars by eavesdropping the location information messages sent over the system or the responses destined for the cars. This obviously implies a threat to location privacy of both cars and car users. The system should be able to detect malicious or erroneous nodes. It should also be combined with privacy preserving mechanisms to avoid tracking.

User identity management consists of data belonging to a user. Such identity may encompass the current context. Therefore, the user identity shall not be considered as static information but, rather. as potentially dynamic information. In the electronic world, a user is represented by one or more digital identities. At any time, each user exposes one Digital Identity.

A digital Identity is provided by an Identity provider and consumed by one or more service providers also called identity consumer. To authenticate a user on a system, the user shall prove he owns an object or provides required credentials.

Many technologies are available and shall be compared regarding some criteria to be addressed by the application. The main criteria are defined in Table 6.

Table 6 – Identity Criteria

Criteria	Description
Selective Disclosure	The user can choose which attributes to disclose to the service providers
Un-traceability	Even if the credential issuer and service providers collude, they cannot track the use of a credential back to the user identity
Un-linkability	Service providers must not link different transactions by the same user even if the user uses the same credentials, unless he uses the same pseudonym
Predicate on Attributes	Ability to compute semantic data on attributes and to integrate it in the issued token

5.2 Analysis of Security Risks

In a wireless sensor network (WSN), when two new entities that do not know each other would like to securely communicate, they must mutually prove to each other their identity and their legitimacy. This stage is called “authentication” and consists of assuring the authenticity of each interlocutor involved in the wireless communication process. Many authentication schemes are available and all of them require an initial secure wireless channel.

So, the problems of the secure keys pre-distribution and of the node deployment are open and must be solved to enable the authentication through a secure channel.

Once the nodes are authenticated and supplied with their own secure communication channel, they can exchange confidential messages. Cipher techniques are used to encrypt the message and ensure

the confidentiality; their complexity and their size in the memory space may vary [36]. The sent messages may be signed in order to prove the identity of the sender.
Facing ever more inventive and powerful hackers, the security of wireless communication leading to the use of secret keys is not only acquired once. The time and the regular renewal of the secret keys are essential to the durability of the system security.

5.2.1 Security needs in a Wireless Sensor Network

A WSN may not rely on a fixed infrastructure: in a Mobile Ad-hoc Network (MANET), sensors depend on each other to keep the network connected, resulting in increased vulnerability to security attacks. The design of a security scheme to assure the safety of the network during the deployment of the nodes and during the lifespan of the network is essential and must take into account several network requirements:

- Availability: network services survival in case of service denial,
- Confidentiality: information is not disclosed to illegitimate entities,
- Integrity: integrity of the delivered message,
- Authentication: capability of each node to identify the others,
- Non-repudiation: message origins cannot be disclosed.

In a WSN, the security mechanisms must be scalable. The usual security techniques based on authentication protocols [37], digital signature and encryption are essential but they are not sufficient.
Additional practices should be applied: the path redundancy to handle messages from one node to another contributes to the network availability. The threshold cryptography, which consists of sharing the deep secret between several nodes of the network, should be another approach to reinforce security [37].

5.2.2 The main known attacks

Pointing out that threats and attacks are different, a hacker of a WSN will act to reach a given goal. To determine a hacker’s intention, we can observe his strategy. An attack sequence could be depicted in three phases:

- Collecting information,
- Exploiting the collected information,
- Causing damage.

Five main intentions could be retained:

- Eavesdropping,
- Breaking communication,
- Throughput or battery corruption,
- Authentication access to use network services,
- Authorization access to obtain resources or cipher keys.

Attacks can be classified according to their action levels inside the network [38].
Physical layer attacks:

- Jamming: It consists of jamming the wireless radio channel. The hacker sends a signal in the same radio frequency as the legitimate receiver to create fading. This can be achieved with a laptop (with high energy resources) or a simple malicious node, within the same network. Jamming attacks are a subset of denial of service (DoS) attacks in which malicious nodes block legitimate communication by causing international interference in networks. Many approaches exist to counter such attacks. One solution consists in changing the carrier frequency or the spread spectrum codes during the data transmission. As it is complex and costly to apply, it is only used for military applications. Lighter solutions are to slide from one channel to another by frequency hopping or to isolate the spectral channel perturbed by jamming.

- Tampering: It consists in taking the whole control of a node. This attack implies a physical access to the node and could be invasive (access to the node hardware) or non-invasive (electromagnetic listening). A hacker could take the control of a node via its JTAG port [39] or via the Bootstrap Loader (BSL) which allows the read-write in the internal node memory. There are no miraculous solutions to avoid these attacks. But it is easy to take precautions by deactivating the JTAG port at the node deployment or password-protecting the BSL.

Link layer attacks:

- Collision: It consists in sending signals to cause interference and discharge the node battery. In practice, changing of only one bit of the message is enough to corrupt the CRC (Cyclic Redundancy Check) and requires very little energy. Such an attack is very easy to realize and is very difficult to detect. Error correcting codes may be employed to correct the errors when few bits are corrupted. But this technique leads to additional computing costs and an overhead on the exchanged messages.
- Exhaustion: It consists in introducing a collision into the frame at the end of the communication in order to force the node to continuously reemit the same packet. In order to prevent these attacks, requests should be ignored when they are identical or become too numerous. Another solution is to attribute a time interval to the node to access the transmission channel.
- Link Layer jamming: It consists in finding a data packet to disrupt the communication. This attack is as efficient as jamming attacks at the physical layer, but it is more energy-efficient. It is based on the MAC protocol timings observation and statistical prediction to determine the time arrival of the data packets. Changing the time slots between two data groups at the MAC layer could be an efficient counter-measure.

Routing layer attacks:

- Selective forwarding: A malicious node cancels any messages in order to lose data. An example of such an attack, called the black hole, is when the hacker destroys all the messages. The nearer from the base station the node is, the more efficient the attack is. The weakness is increased if the messages are not ciphered and if the hacker can read their contents. A multi-path routing protocol can be useful to counter this attack. Any nodes could also supervise their neighbouring traffic.
- Sinkhole: A malicious node tries to identify all the possible paths in order to create a false topology. This attack could be realized when an intruder compromise a node inside the network and launches an attack. Then the compromised node try to attract all the traffic from neighbour nodes based on the routing metric that used in routing protocol. When it managed to achieve that, it will launch an attack. Due to communication pattern of wireless sensor network of many to one communication where each node send data to base station, makes this WSN vulnerable to sinkhole attack. Such an attack could be led from a PDA and exploits the non-authentication of the links or identities. To avoid the sinkhole attack, each node could verify that its neighbours communicate in two directions.
- Sybil: A node or a device takes many identities that may not necessarily be lawful. It does not impersonate any node, but fast it only assumes the identity of another among several nodes, causing redundancies in the routing protocol. The goal is to fill the neighbour memory with useless information. It exploits the weakness of non-authentication of the node identity. The Sybil node tries to communicate with neighbouring nodes by using the identity of the normal node and in the process a single node gives many identities in the area to other nodes in the network which is illegal. The use of identity authentication efficiently protects against the Sybil attack only in a centralized network. In a MANET, the Sybil attack remains possible.
- Hello flood: It consists in bombarding the network with “hello” messages to saturate the node resources. This attack needs power radio devices to broadcast in the whole network. Authentication assures a protection against this attack. It is also possible to check the bi-

directionality of the link with a neighbour node.

- Routing cycles: It consists in setting up a cyclic path between a source node and a destination node to make messages turn around in circles in an infinite loop. This attack is easy to detect by limiting the path length or by using a tree routing protocol.
- Wormhole: It consists in relaying a message on a long way to make the nodes believe that they have a lot of neighbours and to saturate their resources. This attack needs sophisticated radio devices to establish a communication channel on a long way. Any protocols, like MAD (Mutual Authentication with Distance-bounding) [40], are protected against the wormhole attack.

Application layer attacks:

- Flooding: It consists in creating a congestion in order to discharge the battery or to saturate a node's memory. The hacker sends successive requests to establish the connection with a node until its death. This attack could be led from a powerful laptop with high energy resources. It could be avoided by the node using a "client puzzle" challenge [41].
- De-synchronization: It consists in de-synchronizing the communication between two nodes in order to cut the established dialog. A simple method to avoid this attack is to use authentication and encryption.

5.3 V2X Security – State of the Art

The present section reflects the current state of the art of security issues for the radio communications based on the ETSI G5 sets of standards as described in [2].
The description considers vehicle-to-vehicle and vehicle-to-roadside network infrastructure communication services in the ITS Basic Set of Applications [32].

5.3.1 ITS Architecture

Intelligent Transport Systems comprise the following communication entities:

- Vehicles,
- Roadside units,
- Network infrastructure.

These entities are interconnected as shown in Figure 11:

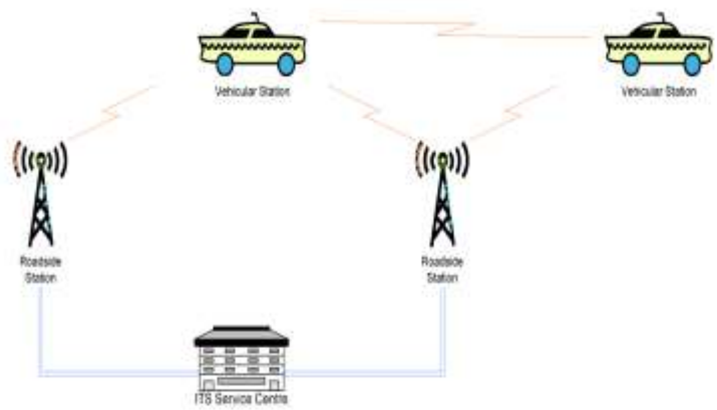


Figure 11 – Interconnection of ITS entities, taken from [17]

The entities are connected using the ETSI G5 channel at 5.9GHz. The network is composed of mobile

nodes. So the topology is continuously changing. A series of standardized messages are exchanged amongst vehicle and the infrastructure. These messages are used by services for safety, infotainment, etc.
In such a network, all the e-security threats that apply in a standard system are present and should be faced considering the type of exchanged data and the particularity of the network.
For example, if the content of the exchanged information is critical, it raises privacy and safety issues. An attacker can easily trace a vehicle thanks to the information present, i.e., in the CAM message [42]. Forged CAM or DENM [43] messages can be used to change the behaviour of the driver or even worst the behaviour of the vehicle autonomous function.

5.3.2 ITS threats and countermeasures analysis

In the literature, e-security threats are typically divided in the following categories: availability, integrity, authenticity, confidentiality and accountability.
In this section we introduce the main points addressed by the standard ETSI TR 102 893 V1.1.1. For each category, a brief description is provided to understand the potential vulnerabilities and which countermeasures are required to address these correctly.
Threats and countermeasures are directly taken from the standard and they will be used in the next paragraphs to better assess the security and privacy issues in AUTOPILOT.

5.3.2.1 Availability threats

Threats to the availability of ITS systems (Vehicle – RSU), including denial of service (DoS) attacks, mainly result from the introduction of malicious software (malware). Methods of attack include:

- Generating a high volume of false messages, such attacks may result in an ITS station failing to receive or send traffic safety messages,
- Formation of "black holes" (a number of adjacent ITS stations configured maliciously not to propagate messages).

DoS attacks can also be conducted using Radio jamming techniques.
Countermeasures include:

- Add source identification in V2V messages (saturation messages can be blocked before application level),
- Limit message traffic to V2I/I2V (use V2V only if infrastructure is not available),
- Implement station registration, each ITS-Station is required to register (and authenticate) to the ITS infrastructure before transmitting messages,
- Implement frequency agility within the 5.9 GHz band (communication frequency changes on pseudo-random basis in order to make more difficult to jam the signal),
- Implement ITS G5A [1] as a CDMA/spread-spectrum system [2] (more resistant to both jamming and eavesdropping),
- Integrate 3G into ITS G5A communications (alternative way for reporting jamming attacks, key/certificate exchanges),
- Implement a Privilege Management Infrastructure (a cryptographic-certificate-based approach to assert the rights of a user/application to access or modify data or executables within a system),
- Software authenticity and integrity verification before installation.

5.3.2.2 Integrity threats

Threats to the integrity of an ITS-S include:

- Unauthorized access to restricted information (associated with a particular ITS station or its end-users), gained by means of a masquerade attack or by the use of malware,
- Loss of information, as a consequence of unauthorized access to restricted information (malware that deletes service information, security parameters, local station data or information stored in the LDM),

- Manipulation/Corruption of information (malware may be used to change a message content before it is sent/received).

Countermeasures include:

- Digitally sign each message using a Kerberos/PKI-like token system [44] (messages must contain a digital signature or other cryptographic checksum),
- Non-cryptographic checksum of the message in each message sent (protection against accidental modification of the contents),
- Perform plausibility tests on incoming messages (rules and other ITS-S local mechanisms to determine the likelihood that a received piece of data has been maliciously modified in transit),
- Software authenticity and integrity verification before installation.

5.3.2.3 Authenticity threats

Authenticity is a major security challenge in ITS. Not ensuring the authenticity of information may cause serious security problems, such as:

- Masquerade attack, insertion of false messages into the network,
- Replay attacks, carried out by capturing and subsequently resending valid received messages at a different location or in a different time,
- Exposure of false GNSS signals, providing false location information to ITS (GNSS spoofing).

Countermeasures include:

- Digitally sign each message using a Kerberos/PKI-like token system (messages must contain a digital signature or other cryptographic checksum),
- Use broadcast time (Universal Coordinated Time – UTC – or GNSS) to timestamp all messages in order to reduce the likelihood of replay attacks,
- Include a sequence number in order to detect messages out of sequence,
- Implement differential monitoring [2] on the GNSS system to identify unusual changes in position.

5.3.2.4 Confidentiality threats

Threats to the confidentiality of information associated with ITS stations include the illicit collection of transaction data by eavesdropping and the collection of location information through the analysis of messages traffic.

As G5A is an open interface, messages transmitted over this interface may be intercepted and information may be extracted from them. An attacker may also construct a profile of a given ITS-S (Vehicle) or end-user by observing which services are used regularly, at what times and at which location.

Countermeasures include:

- Encrypt the transmission of personal and private data (location, requested ITS service, ITS-S id, etc.),
- Use a pseudonym that cannot be linked to the true identity of either the user or the user's vehicle.

5.3.2.5 Non-repudiation/Accountability threats

Law authorities must be able to prosecute ITS users for motoring offences or for mounting security attacks on other ITS users. Therefore, it is necessary to record all messages and service activities in ITS stations.

Countermeasures here include:

- Maintain an audit log of the type and content of each message sent to and from an ITS-S (available only to law enforcement authorities in the event of a dispute, users cannot access it),
- Implement a non-repudiation framework.

5.3.3 ITS Security reference model

This section describes the roles of various ITS entities for the ETSI ITS security reference model [45]. Particular attention has been given to trust management issues. Trust management requires secure distribution, maintenance and revocation of trust relationships. ITS communication systems rely on public key certificates and public key infrastructure in order to establish and maintain trust relationship between network nodes (ITS-S, authorities, etc.).

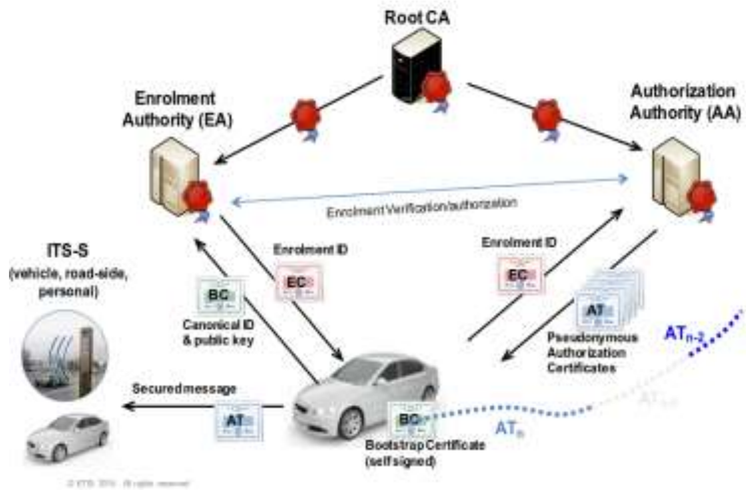


Figure 12 – ITS entities and their role in the security management system, taken from [45]

As depicted in Figure 12, in order to join the ITS network, an ITS-S shall contact different authorities to obtain public key certificates that act as proof of identity/authorization.
In particular, firstly it has to contact an enrolment authority in order to authenticate itself as a valid ITS-S and subsequently an authorization authority to obtain different authorization tickets. Basically, authorization tickets define which kind of message (basic CAM, emergency vehicle, public transport, valid geographic zones, period of time, etc.) the ITS-S can send to the other nodes of the vehicular networks.
In this section, enrolment and authorization processes are described considering all the entities involved. Particular emphasis will be given to ITS-S critical data (bootstrap certificate, canonical ITS-S identifier [46] and other information that shall be defined during the manufacturing process) and enrolment/authorization protocols.

5.3.3.1 ITS-Station

During the manufacturing process of the ITS-S, the following information elements shall be memorized within the ITS-S itself in order to enable it to start the authentication procedures with the ITS network authorities.

- A canonical identifier (globally unique).
- Network addresses and public key certificates of the set of current known trusted enrolment authorities and authorization authorities.
- A public and private cryptographic key pair for the ITS-S.
- A cryptographic certificate linking the ITS-S canonical identifier with the ITS-S public key.

Furthermore, ETSI TS 102 940 V1.1.1 [46] suggests the following guidelines:

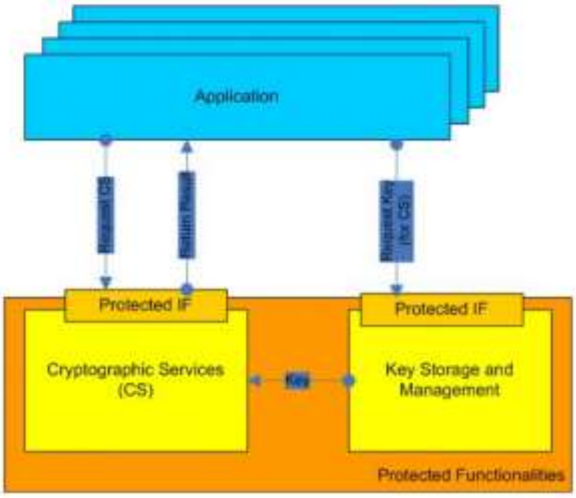


Figure 13 – Example of interaction with a secure module, taken from [46]

- Inside ITS-S, keys should only be communicated to a secure processing engine (referred to as a cryptographic module);
- Modules and applications other than the cryptographic module should have access only to key handles;
- Key storage and cryptographic functions should be integrated into a secure module, preferably in tamper resistant hardware, protecting the key material and offering cryptographic operations as services to all other applications (Figure 13).

Applications should be securely separated to avoid unsolicited interaction.

5.3.3.2 Enrolment Authority

An enrolment authority (EA) represents the access point to the ITS, which authenticates ITS-S (enrolment procedure) and grants access to ITS communications providing enrolment credentials.

5.3.3.2.1 Enrolment of ITS-S

The enrolment procedure succeeds if the following conditions are valid:

- ITS-S provides a valid canonical identifier;
- The enrolment authority validates that an ITS-S can be trusted to function correctly (the EA must be able to determine whether or not an ITS-S is in a compromised state).

5.3.3.2.2 Provision of enrolment credentials

Provision of proof of authentication of the ITS-S (enrolment credentials), in order to enable the ITS-S to pseudonymously [23] request authorization from the authorization authority. These credentials are valid only within the enrolment authority domain, if necessary ITS-S may enrol with multiple EA in order to act in different domains.

Enrolment credentials shall contain the following information:

- Enrolment Authority identifier;
- Pseudonym for the ITS-S (temporary identity).
- Cryptographic material allowing the ITS-S to demonstrate ownership of the credentials.

In addition, enrolment credentials may contain the following information:

- ITS-S attributes (protected in such a way to preserve privacy requirements).
- Credentials issue or/and expiry date.

Communications between ITS-S and Enrolment Authority shall be encrypted with EA asymmetric keys.

Note: An enrolment authority may require an already enrolled ITS-S to re-enrol periodically.
Note: An enrolment authority shall be able to determine the canonical identifier of an ITS-S from its enrolment credentials only if the ITS-S is in a compromised state.

5.3.3.2.3 Enrolment protocol

The ITS-S enrolment request message (Figure 14) mainly contains

- ITS- S certificate, including the ITS-S identifier and public key.
- Signature of the enrolment request.

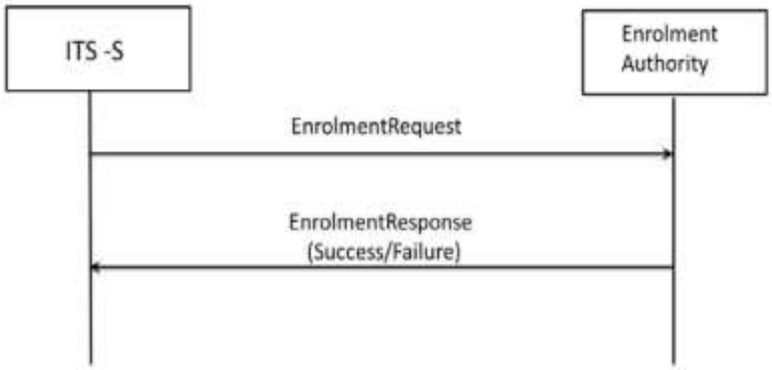


Figure 14 – Message sequence for enrolment request and response, taken from [47]

A successful enrolment response message (figure 14) mainly contains the enrolment certificate which includes the pseudonymous identifier (privacy) for the ITS-S, while an unsuccessful response contains information about the cause of failure.

5.3.3.3 Authorization Authority

The authorization authority provides enrolled ITS-S with authoritative proof that it may use specific ITS services. These privileges are granted by means of authorization tickets, each ticket specifies a particular authorization context.
Each AA is responsible for a particular set of contexts which may be specified by one or more of the following:

- Application (cooperative awareness applications, emergency service vehicles, etc.);
- Time period;
- Geographic region (nation, state, locality); or
- Other criteria.

An authorization authority shall accept credentials from one or more enrolment authorities.
When an ITS-S applies to that authorization authority for a set of authorization tickets, it shall present and demonstrate ownership of enrolment credentials from one or more of its enrolment authorities. If the authorization authority does not accept credentials from any of the enrolment authorities in the application, it shall reject the application.
Before issuing authorization tickets, an authorization authority may apply a policy to the presented enrolment credentials. For example: it may require that enrolment credentials are issued within a certain time period, in a specific geographic zone, etc. An authorization authority shall only issue an authorization ticket to an ITS-S that is valid within the combined enrolment domains of all the enrolment credentials presented to it by the ITS-S.
Note: An authorization authority shall be able to determine the enrolment credentials of an ITS-S from its set of authorization tickets only if the security of the ITS-S has been determined to be compromised.

5.3.3.3.1 Authorization tickets

Authorization tickets allow ITS-S to access a specific ITS capability. Tickets shall contain the following information:

- Authorization context
- Authorization authority identifier
- Cryptographic material allowing the ITS-S to demonstrate ownership of the ticket.

In addition, authorization tickets may contain additional information to support the use of authorization context.

5.3.3.3.2 Authority Hierarchy

The authorization system shall support the use of a hierarchy of authorization authorities, with lower-layer authorities authorizing vehicles and higher-layer authorities authorizing lower-level authorities.

Each CA hierarchy (for EA or AA) has at its summit a Root Certificate, which is the ultimate root of trust for all certificates within that hierarchy. An ITS-S must have access at least to the root certificate at the summit of the hierarchy for the authorization certificate attached to the message in order to trust an incoming message. ITS-S may obtain root certificates during the manufacture or maintenance lifecycle.

5.3.3.3.3 Authorization protocol

An authorization request message (figure 15) mainly contains:

- The enrolment certificate containing the pseudonymous identifier;
- Signature of the authorization request.

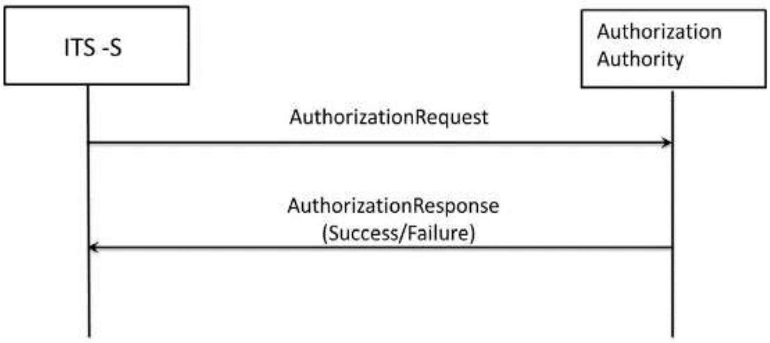


Figure 15 – Authorization protocol, taken from [47]

A successful authorization response message (figure 15) contains authorization tickets, while unsuccessful response contains information about the cause of failure.

5.3.3.4 Security profile for CAMs

This section defines at high level which information elements shall contain a secured CAM message. For more specific information please refer to [48].

Figure 16 – Signed Message with Certificate, taken from [45]

Figure 17 – Signed Message with Certificate digest, taken from [45]

CAM shall be wrapped inside a **SecuredMessage** [48] structure (Figure 16 and figure 17 graphically show two examples of its main sections):

```
struct {
uint8 protocol_version;
HeaderField header_fields<var>;
Payload payload_field;
TrailerField trailer_fields<var>;
}SecuredMessage
```

Figure 18 – *SecuredMessage* [48] structure

The structure *SecuredMessage* (Figure 18) defines how to encode a generic secured message:

- *protocol_version*: specifies the applied protocol version.
- *header_fields*: is a variable-length vector that contains multiple information fields of interest to the security layer.
- *payload_field*: contains the message payload.
- *trailer_fields*: contains information necessary to verify security property (authenticity, integrity, etc...) of the message.

5.3.3.4.1 Header fields

For CAM messages the following *HeaderField* element shall always be included:

- *signer_info* (mainly it contains an element of type certificate or certificate_digest)
- *generation_time*
- *its_aid* [49]

The *HeaderField* element *request_unrecognized_certificate* shall be included if an ITS-S received CAMs from other ITS-Ss that it had never encountered before and which included only a signer_info field of type *certificate_digest_with_sha256* instead of a *signer_info HeaderField* of type certificate. In this case, the signature of the received CAMs cannot be verified because the verification key is missing. The field digests<var> in the structure of *request_unrecognized_certificate* shall be filled with a list of HashedId3 elements of the missing ITS-S certificates.

5.3.3.4.2 Payload

A *Payload* element shall be included for all CAMs. This element shall be of type signed and contain the CAM payload.

5.3.3.4.3 TrailerField

The only *TrailerField* element that shall be included in all CAMs is the signature. The standard ETSI TS 103 097 v1.2.1 [48] defines which fields are covered by the signature.
CAM messages shall not be encrypted.

Element	Description
SecuredMessage	
uint8 protocol_version	Covered by the signature
HeaderField header_fields<var>	
...	
Payload payload_fields<var>	
...	
TrailerField trailer_fields<var>	
TrailerFieldType type	
PublicKeyAlgorithm algorithm	Not covered by the signature
EcdsaSignature ecdsa_signature	
EccPoint R	
EccPointType type	
opaque x[32]	ECDSA signature (r,s)
opaque s[32]	

Figure 19 – Example for ECDSA signature generation for SecuredMessage, taken from [48]

Figure 19 shows an example of CAM message wrapped inside a SecuredMessage structure. Furthermore, description column shows which data are covered by the signature.

5.3.3.5 Security profile for DENMs

This section defines which information element shall contain a secured DENM message [48]. For further details, please refer to [48].

Figure 20 – Signed Message with Certificate [45]

DENM shall be wrapped inside a *SecuredMessage* structure: (Figure 21 graphically shows its main sections)

```
struct {
    uint8 protocol_version;
    HeaderField header_fields<var>;
    Payload payload_field;
    TrailerField trailer_fields<var
}SecuredMessage
```

Figure 21 – Signed Message with Certificate [48]

5.3.3.5.1 Header fields

For DENM messages, the following *HeaderFields elements* shall always be included:

- *signer_info* (It contains an element of type certificate);
- *generation_time;*

- *generation_location;*
- *its_aid* [49].

5.3.3.5.2 Payload

A *Payload* element shall be included for all DENMs. This element shall be of type signed and contain the DENM payload.

5.3.3.5.3 TrailerField

The only *TrailerField* that shall be included in all CAMs is signature. The standard ETSI TS 103 907 v1.2.1 [48] provides more details about signature trailer content.
DENM messages shall not be encrypted.

6 Requirements for security and privacy in IoT [3]

6.1 General principles

6.1.1 Identification and authentication control

At the heart of the AUTOPILOT Cybersecurity framework is the authentication function used to provide and verify the identify information of an IoT entity.
When connected, IoT/M2M devices need access to the IoT infrastructure, the trust relationship is initiated based on the identity of the device, so IoT/M2M endpoints must be fingerprinted by means that do not require human interaction i.e. using radio-frequency identification (RFID), shared secret, X.509 certificates, the MAC address of the endpoint, or some type of immutable hardware based root of trust.

6.1.2 Use control

The second layer of the framework is the authorization function that controls a device's access throughout the network fabric. This layer builds upon the core authentication layer by leveraging the identity information of an entity. With authentication and authorization components, a trust relationship is established between IoT devices to exchange appropriate information.

6.1.3 System Integrity

The system integrity layer implements an overall security policy with the goal of preventing data and processes from being modified by third parties. To achieve this, it has to operate at different levels in the systems:

- It grants protection to communications, so the sent data is received without any modification;
- It grants protection to devices, avoiding someone modifying files, configurations or executables;
- It grants protection to systems, avoiding the installation of any software from an unknown source.

6.1.4 Data Confidentiality and Privacy

From the privacy point of view the AUTOPILOT framework works with two types of data: direct user information, used for high level use cases, and machine information from automatic IoT/M2M devices.

6.1.4.1 User information and authentication

User privacy requirements are mandated by the GDPR regulation. It enforces the principle through which user data should be collected only at a minimum level and retained in the system for the minimum duration that is required for the system operation. Moreover, the user consent must be obtained for sharing any private or sensitive data.
User information is required for enrolment to the system, interaction with high level services such as car sharing, or direct authorization to use a car.
The system must provide enrolment of user data to ensure high assurance authentication supported by strong credentials. At the same time, the system should work in semi-anonymous or pseudonymous mode to provide levels of privacy that are in line with GDPR.
Even if pseudonyms are used and no private information is disclosed in the user identifier, the pseudonym may be used for tracking. If this information is submitted to the IoT cloud then potential

[3] Use cases identified in T1.1 referencing the T1.2 architecture and T1.4 communication means

attackers may be able to locate the user or reconstruct his past behaviour. This implies that information must be anonymized before it sent to the IoT cloud and must be anonymized before it is persisted.
Therefore, classical PKI schemes without additional measures cannot be used even if the certificate is anonymous. The certificate or public key fingerprint allows unique user identification. Usage of a scheme that preserves user privacy by design is mandatory for any user authentication and identification of the user in the cloud data. This level of privacy may be achieved by deployment of a polymorphic scheme [50], zero-knowledge-proof scheme such as IDEMIX [51][52] or U-prove [53] or at least by deployment of PKI with very short-lived anonymous certificates without linking possibility. It also implies that information must be anonymized before it is sent to the IoT cloud.
The system must also provide the possibility of inspection and investigation in case of security or traffic incidents with retrieval of the real user identity and identification of all actors.
User authentication must implement the following requirements:

- High level enrolment and strong link to real user identity,
- Semi-anonymous[4] user authentication to IoT cloud,
- Semi-anonymous identification without disclosure of private data for data stored in the cloud,
- Polymorphic scheme preventing user tracking for all data stored in IoT cloud,
- Possibility of investigation of incidents with recovery of real user identity by an authority.

6.1.4.2 Information from IoT/M2M devices
Devices connected to the IoT cloud do not contain any private data of users, but the devices may be used for user tracking.
Each device type must be reviewed and data coming from devices that may be used for tracking must be treated in the same way as personal data:

- Semi-anonymous identification without disclosure of private data for data stored in the cloud,
- Polymorphic scheme preventing user tracking for all data stored in IoT cloud,
- Possibility of investigation of incidents with recovery of real user identity by an authority.

6.1.5 Non-repudiation

In case of incident resolution, it may be crucial not only to identify all the actors (e.g., to find the source of the wrong information), but also to provide a proof of origin of the information. Non-repudiation must be taken into account during deployment of privacy-friendly solutions.

6.1.6 Restricted Data Flow

This security feature has to grant data separation and protection amongst different domains. It has to permit only the interaction between same domain agents. For example, car infotainment systems and a road signals have different scopes, the first have to inform the driver and passengers about the infrastructure status and driving enhanced data, while the second have to send some information to the autonomous infrastructure. These components must not communicate directly. Indeed, this layer provides network segmentation and application sandboxes.

6.1.7 Timely Response to Event

6.1.7.1 Secure Analytics: Visibility and Control
The secure analytics layer defines the services by which all elements, i.e. endpoints, network

[4] The user is granted access to the service, but his/her digital identity related data remains confidential even if valid credentials are used to authenticate.

infrastructure and data centres, may participate to provide telemetry for the purpose of gaining visibility and eventually controlling the IoT/M2M ecosystem.
By adopting big data architectures, we can deploy a massive parallel database platform that can process large amounts of data in real time. And by combining these with analytics, we can perform real statistical analysis on security data to detect security related anomalies. Further, this layer includes all elements that aggregate and correlate the pieces of information, including telemetry, to provide reconnaissance and threat detection. Threat mitigation could vary from automatically shutting down the attacker from accessing further resources to running specialized actions to initiate proper remediation.

6.1.8 Resource Availability

This security layer implements all countermeasures against denial of Service threats or any other problems that can interrupt any infrastructure services.

6.1.9 Network Enforced Policy

This layer involves all elements that route and transport endpoint traffic (control management or actual data) securely over the infrastructure, whether control, management or actual data traffic.
Like for the authorization function, there are already established protocols and mechanisms to secure the network infrastructure and also policies that are well suited to the IoT/M2M use cases.

6.2 AUTOPILOT Security and Privacy Requirements

The requirements aim to mitigate the six primary security requirements:

1. Authenticity: Ensures that unauthorized users cannot present themselves as authorized ones, that authorized assets cannot receive or process data from any unauthorized user, and that restricted ITS services can only be accessed by authorized users.
2. Integrity: This is related to the integrity of stored and transmitted information. It ensures that information is protected from unauthorized modification and deletion.
3. Confidentiality: This is related to the integrity of stored and transmitted information. It ensures that information is protected from unauthorized access.
4. Availability: This is related to service availability. It ensures that access to, and the operation of, services by authorized users and assets cannot be prevented by malicious activities.
5. Accountability: This is related to accountability of users. It ensures that every action that was taken and service usage can be audited.
6. Non-Repudiation: This is related to the non-repudiation of user actions. It ensures that a capability is provided to determine whether a given authorized or not authorized user took a particular action.

Every threat is analysed and mitigated for every interface in an ITS integrated system. The standard ISA/IEC 62443 – 3 – 3 [10] provides a map of all security requirements and recommends the requirement to be adopted for each security level. The ISA/IEC 62443 – 3 – 3 group security requirements into four security levels (SLs) associated to four attacker types. Each attacker type is described in terms of skill, motivation and resources. So, the risks we identified in automotive integrated systems have been analysed to produce a list of requirements linked to the 62443-3-3 standard. The adoption of this list and its security level is mandatory to mitigate the threat associated with the risk.
For example, risk number 41:

Table 7 – Risk n. 41

#	Interface	Vulnerability	Threat	Name	Description - Consequence	Information asset	Probability	Impact	62443- 3 - 3
41	Car Interface	Hop-to-Hop Interface	Accountability	Repudiation Driver	Messages ignored by driver who claims they have not been received	Communication with ITS infrastructure	Low	Impossible to prosecute a rogue driver	2-8(4),2-9(4), 2-10(4),2-11(4),2-12(4),3-9(3)

Risk 41 focuses on "in-car interfaces" (ITS-S Vehicle) and involves the network interface ETSI G5 for V2X communications. It is a threat for accountability. For example, a dishonest driver can ignore messages from the ITS infrastructure and, therefore, may not be prosecuted for a violation. To mitigate:

- The system shall audit events and shall be centrally managed (Security Requirement 2.8 with Security Level 4);
- The system shall have audit storage capabilities and shall issue a warning when a storage threshold is reached (Security Requirement 2.9 with Security Level 4);
- The system shall respond to audit processing failures (Security Requirement 2.10 with Security Level 4);
- The system shall memorize the audit timestamp, with time synchronization and protection of time source integrity (Security Requirement 2.11 with Security Level 4);
- The system shall adopt a non-repudiation function for all users (Security Requirement 2.12 with Security Level 4);
- The system shall adopt a protection to the audit information (Security Requirement 3.9 with Security Level 3).

Another example is risk n° 101:

Table 8 – Risk n. 101

#	Interface	Vulnerability	Threat	Name	Description - Consequence	Information asset	Probability	Impact	62443- 3 - 3
101	Road Sign Interface	Hop-to-Hop Interface	Availability	DoS	Jamming of Radio Interfaces	Communication with ITS Infrastructure	Low	AD System and users are not informed	7-1(4)

Risk 101 focuses on the RSU's hop-to-hop interfaces and it is about the risk of jamming attack aimed to turn off RSU communication in ITS infrastructure. The impact is that the RSU cannot communicate any kind of information and all assets and users in the infrastructure cannot receive any data about it.

To mitigate the risk, the system shall provide the capability to operate in a degraded mode during a DoS event and to restrict the ability of any malevolent user to disturb communication failures (Security Requirements 7.1 with Security Level 4). For example, it could adopt the LTE technology, which implements an anti-jamming technology.

Table 9 shows the various levels of skill, access and resources that identified attackers may have. Other levels and attackers are possible. For example: a terrorist organization could hire a rogue admin and a rogue engineer, thus ranking as a very serious threat. We consider that these kinds of attackers are beyond the scope of the AUTOPILOT project at this stage.

Table 9 – System access

Attackers	Level of System Access	Skills Level	Resources
Rogue driver	2	1	1
Rogue Maintainer	3	3	1
Rogue Operator	3	2	1
Rogue Administrator	4	4	1
Rogue Engineer	3	5	1
Anarchist / Vandal	1	1	1
Terrorist	1	1	5
Youth / Opportunity hacker	1	1	1
Industrial Spy	1	4	4

Table 10 – Level of Attacks

Legend	
Level of system access	1=External Access
	2=Normal System User
	3=System Operator Admin
	4=Insider
	5=Unlimited
Level skills	1=low
	5=high
Resources	1=low
	5=high

6.2.1 Unlimited Human User Authentication

The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces that provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.

6.2.2 Cloud data classification

All data submitted to the platform must be classified into one of the following categories:

- Public data that may be accessible by any entity (e.g., information from sensors such as temperature);
- Restricted data that require basic authorization to access (e.g., position of device owned by provider);
- Privacy sensitive data listed in GDPR that require detailed authorization access. In the case where data are disclosed to human users, information about which information was disclosed to which person must be stored in secure storage and must be available for future investigation and auditing.

6.2.3 Authorization of access to the IoT platform (FIWARE, Watson IoT)

Each platform must follow the above classification of data and enforce the following sets of credentials for communication with IoT services:

- Public access credentials to access public data;

- Restricted credentials to access restricted data;
- Credentials to access private data and services. Access to private data must be subject to an audit log, it must be possible to provide information about which user requested the information or service call. If possible, access should be provided only for certain actions, and not for a whole user session.

Each IoT service must be forced to use separate credentials.

6.2.4 Translation of user credentials into credentials for communication with the IoT platform

Each IoT defines a process by which the authorization data of end user services is translated into authorization data of the underlying IoT platform.

6.2.5 Logging of IoT service to IoT platform calls

Audit log information is provided for all calls to the IoT platform with following information:

- Type of transaction;
- End user or entity who initiated the call;
- Time of transaction;
- Which information was provided (in case of private information);
- Credential that was used for communication with the platform.

The audit log itself does not contain any privacy sensitive information.

6.2.6 Translation of authorization between IoT platform and oneM2M platform

Authorization of access to the oneM2M platform must follow [37] [38]. Each service must have at least the following sets of credentials:

- Public access credentials to access public data;
- Restricted credentials to access restricted data;
- Credentials to access private data and services. Access to private data must be subject to audit log. It is possible to provide historical information about which IoT service requested the information or service call.

Each oneM2M platform must define policies to follow data classification.

6.2.7 Logging of IoT platform to oneM2M calls

Audit log information is provided for all calls to IoT platform with the following information:

- Type of transaction;
- Credentials of the entity who initiated the call;
- Time of transaction;
- Which information was provided (in case of private information);
- Credentials used for communication with the platform.

The audit log itself does not contain any privacy sensitive information. In case of privacy sensitive calls the audit logprovide the means of investigation of the full communication chain starting with the user credentials.

7 Conclusion

We presented the security and privacy requirements of the autonomous driving systems and infrastructure. In particular, we highlighted that:

- Security at all layers should be implemented to mitigate all the risks identified.
- A process for measuring key performance indicators (KPIs) should be defined by the pilot sites so that it would be possible to evaluate the impact of the security mechanism proposed in this document on those KPIs.

8 Annexes

8.1 Annex A

Worksheet in
AUTOPILOT-D110-v1

8.2 Annex B: Feedback from the pilot sites

8.2.1 V2I secured Architecture from CEA

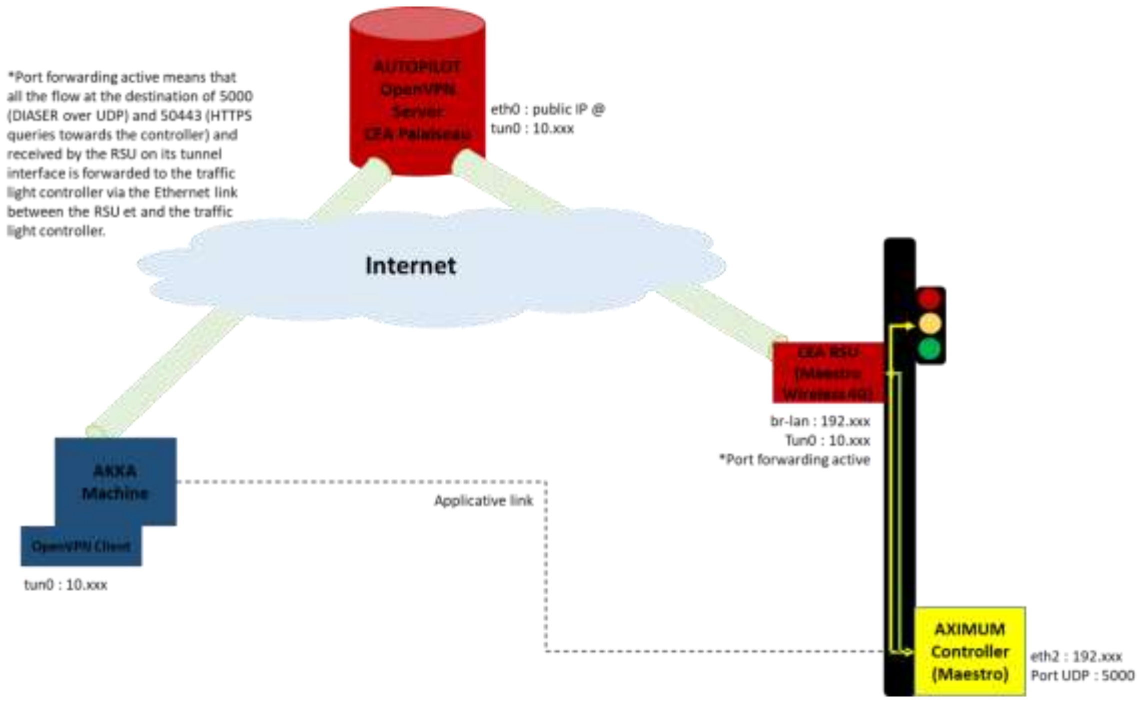
DIASER (Standard Dialog of Traffic Regulation Equipment): "DIAlogue Standard des Equipements de Régulation de trafic" (DIASER NF P 99-071-1 G3) [9] is a French closed standard which aims to normalize the exchanges of traffic light regulation equipment in a safe and secured manner. The major part of the TLC in France, in particular the ones on which we are working on in Versailles PS, implements the DIASER specifications.

TLC: Traffic Light Controller is a traffic regulation equipment that manages and controls semaphores and is able to provide traffic light status and traffic information.

TLCs are very critical equipment in a way that they manage road safety features like controlling traffic lights, managing traffic rules, configuring traffic lights depending on the characteristics and topologies of the road. Not everybody could have access to these equipment, because that can be a very important public security and safety issue; not only for cars, but also for all road users including the Vulnerable Road Users (VRU) such as pedestrians, bikes, etc. That is why it is essential to make sure that all exchanges that are made between any kind of host and one or several controller(s) are done in a secured way.

In Versailles Pilot Site (Versailles PS) the architecture of communication with TLC involves the use of a roadside unit (RSU) which will handle the IP and port forwarding to the TLC.

The architecture of communication is specific to each RSU provider in the Versailles PS. From CEA's point of view, we are considering the following architecture with the elements as shown:



- AKKA Machine which is a Linux host located in AKKA Technologies offices and which is in charge of sending DIASER requests to now the status and the remaining time of the traffic lights that are managed by a given TLC. This machine has an OpenVPN client installed to connect to an OpenVPN server. It has an OpenVPN certificate generated from the server side that allows it to connect to that one.
- AUTOPILOT OpenVPN Server which is located in CEA offices and which handles OpenVPN server role. All the client certificates are generated from this machine and given to the client hosts such as the AKKA Machine.
- CEA RSU (Maestro Wireless) is a cellular modem which handles IPv4 communication through Ethernet or WiFi. It is also called IP-RSU hereafter.
- AXIMUM Controller (Maestro) is a TLC which manages from 1 to 8 Carrefour(s) (semaphores area). This equipment is able to communicate only with DIASER protocol.
- Internet which is necessary to make this kind of communication work as the remote hosts need the Internet to be working to be able to activate the VPN client and to communicate securely.

Specifically, the AKKA machine generates DIASER requests to ask for the traffic light status and the remaining time before switching to another status. These DIASER requests are transported through UDP and routed through an IP over 4G connection to the IP-RSU (Maestro Wireless provided by CEA). Then the IP-RSU forward (IP forwarding) the requests to the TLC.
The TLC generates corresponding DIASER responses to provide the cloud server with the traffic light status and the remaining time. These responses take the reverse path of the DIASER request.
The recipient decodes the response according to the DIASER specifications.
Then the cloud server sends the traffic light status and the remaining time to the VFLEX through a 4G connection.
Note that all the traffic through 4G connection is encapsulated into a VPN tunnel. It is important to secure communication between the remote host which is in this case a machine located somewhere in the cloud, but could also be a connected vehicle for the reason explained above.
Also, in this architecture, the remote host does not need to know the IP address of the TLC. It just needs to send the requests to the IP-RSU through the secured link, with a destination address which

is reachable only if the tunnel interface is up. In other words, without the OpenVPN connection between the remote host and the AUTOPILOT OpenVPN Server, there is no way to reach the RSU. That means that an eventual malicious user could not intercept the traffic if he does not have a certificate generated from our server.
To summarize, to access or take control of the communication between the remote host (whatever the host) and the TLC, there is a need for:

- Having a client certificate generated from the AUTOPILOT server;
- Establishing a OpenVPN communication based on that certificate;
- Knowing on which ports the RSU is listening to make the port forwarding to the TLC;
- Knowing on which ports the TLC is listening; which make this architecture very strong.

Additionally, OpenVPN is a powerful open source security software.

8.2.2 Pen-test on the Livorno Pilot Site

During the second iteration a Penetration Test has been conducted on the Italian pilot site by a Thales Red Team.

8.2.2.1 Red Team Testing

Our research goal within the first validation phase of the AUTOPILOT project has been focused mainly on the identification of the cyber risks that the ITS-G5 infrastructure could be exposed to. In order to thoroughly investigate this aspect we have chosen to analyze the standard from the point of view of a potential attacker, using tools easily available on the market, exploiting a laboratory environment offered by the project in which all the recommended cybersecurity policies had not yet been applied. In this way we have been able to demonstrate the maximum capabilities of the cyber-attacks that could be made against an open protocol managed ITS-G5 infrastructure. Once a good level of awareness in this topic has been obtained, the next phase of the project will have the objective of making use of all the technical details collected to achieve the effective securing of the ITS-G5 testing environment deployed within AUTOPILOT.
In order to carry out the survey from the point of view of an effective attacker, we have chosen to resort to the use of a red team-oriented analysis approach. Namely, a red team is an independent group of cybersecurity practitioners that performs cyber-attacks on an infrastructure with the aim to study its weaknesses and to improve its effectiveness, detecting and evaluating threats and vulnerabilities form an attacker-like perspective. What distinguishes a red team from a group of attackers are: customer consent and ethics. The advantage of using such strategy of test is to provide a more realistic picture of the security readiness than exercises, role playing, or standard assessments in general.
In this context, this line of attack has been used for technical research purposes. In red teaming approach, ethical hackers or white hats are responsible for system evaluation and penetration with limited (or without) any granted access to internal resources of an information security system or network.

8.2.2.2 The SDR: the tools of the trade

The ETSI ITS-G5 infrastructure is mainly based on the use of the IEEE 802.11p V2X communication standard, otherwise known as WAVE (Wireless Access Vehicle Environment), in the licensed band of 5.9 GHz (5.85-5.925 GHz). In addition, others two support interfaces are involved within the AUTOPILOT testbed deployed, such as: LTE, for communications with the command and control center, and the IEEE 802.15.4 standard, for the gathering of information from the scattered sensors on the roadside. In order to control all these interfaces, taking advantage of the maximum flexibility offered by a single hardware component, we decided to make use of Software-Defined Radios (SDR) which, moreover, are easily available on the market.

The advent of inexpensive SDRs has redefined the wireless hacking landscape. SDRs are systems where components that have been traditionally implemented in hardware (e.g. mixers, filters, amplifiers, modulators/demodulators, detectors, etc.) are instead implemented by means of software elements. At the moment there are several types of SDR devices to which we can refer to; in our case, we based our choice on the analysis of the following five features, finding the one that best suited into the AUTOPILOT operating context:

- Sample Rate/Bandwidth. The sample rate defines the maximum bandwidth that we are able to view simultaneously.
- Dynamic Range/ADC Resolution. Higher ADC resolutions let us view loud and quiet signals together and observe smaller differences in the signal. A typical resolution for most signals is done with the aid of 8 bits, but SDRs with 16 bits of resolution are still available on the market.
- Transmit Capability. Some SDRs allow us to transmit and receive simultaneously (full duplex), but others only allow half duplex transmit capabilities.
- Tuner Range. The tuner range determines what frequencies we are able to receive.
- Price. A too expensive SDR may not adequately represent the technology used by an effective attacker.

After these considerations, our choice fell on the HackRF One SDR, with the aid of a logarithmic antenna able to operate up to 6 GHz, in order to adequately overspread the operating frequencies of the IEEE 802.11p standard. To properly manage the software side we employed GNURadio, which is an open source development toolkit for programming SDRs. GNURadio Companion makes use of a graphical interface to develop the wanted behavior, generating a series of logic blocks connected to each other, called flowgraph. At the compilation time, these blocks are automatically converted into Python code and loaded within the HackRF One. Finally, the self-generated code was subsequently modified by hand in order to better fill our needs.

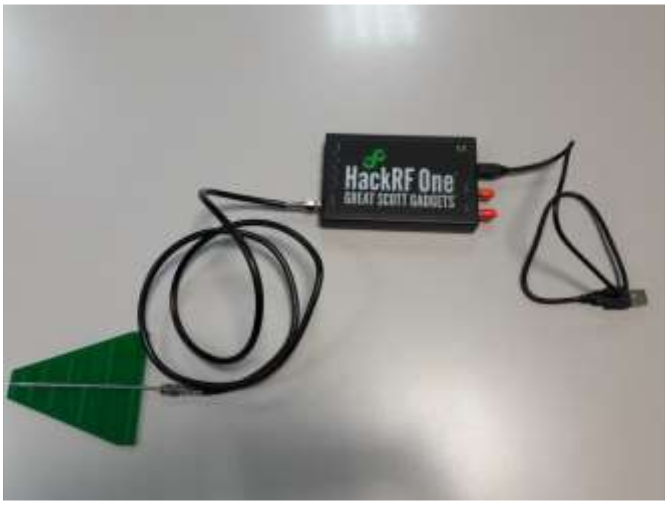


Figure 2: The HackRF One SDR with the logarithmic antenna used in this context

8.2.2.3 Attack perspective and work findings

On the prototypal environment of AUTOPILOT, not yet managed with all the appropriate cybersecurity policies, in order to follow a red team approach, we did the tests without being aware of the actual development of the infrastructure. The research work of the attack vectors on architecture has been structured into three main phases:

- Information Gathering.
- Reverse Engineering of the exchanged messages payloads.
- Exploiting ITS-G5 V2X communications.

8.2.2.4 Information Gathering

First of all, an inspection was carried out on the AUTOPILOT site, with the aim to attempt to understand what kind of technologies were actually in use, to locate the active Road Side Units (RSU) on the route, to map the pedestrian crossings and to mark the traffic light stations as points of interest. Subsequently, a huge amount of sniffing sessions were carried out, taking care to keep track of all the visual variations verifiable on the environment, such as: AD car passing, mapping of the active lights on the vehicles, recording of a braking event, proximity to a green/ yellow or red traffic light, etc.
The scanning for the IEEE 802.11p signals to be captured during the sniffing phase was made through the use of the open source tool Gqrx (GNU Radio and Qt graphical toolkit), which is an excellent framework for searching the analog signals within the frequency range covered by the SDRs, through a fairly intuitive graphical interface. Once the analog signals related to the exchange of IEEE 802.11p messages were identified, a module was developed by means of GNURadio for thei r reception and conversion into a digital layout. The code generated and executed on the HackRF One SDR allowed us to capture IEEE 802.11p frames and to collect them in various PCAP (packet capture format) files via Wireshark.

8.2.2.5 Reverse Engineering of the exchanged messages payloads

Secondly, once a massive and targeted collection of packet capture was obtained, a simplified reverse engineering operation of the protocol was made. In order to be able to extract the information that could allow us to understand the meaning of some bits of the gathered payloads, we used temporal and spatial correlation techniques between the available frames, aside from an in-depth analysis of the ASN.1 (Abstract Syntax Notation One) code of the ETSI ITS-G5 standard documentation, and above the receiving of some indirect advices through the use of simple social engineering operations.
At the end of the investigation, a Python script was created for the extraction and interpretation of the fields of interest from an IEEE 802.11p frame. At this stage we were able to correctly derive the message structure provided by the ITS-G5 standard: Simple GeoNetworking, CAM, DENM, SPATEM and MAPEM packets.

8.2.2.6 Exploiting ITS-G5 V2X communications

Finally, we moved on to the active phase, compiling a new Python script using the GNURadio tool (beside some additional handmade tips) to set up our HackRF One to transmit messages on the IEEE 802.11p channel. By simply changing the packet timestamps, the sender/receiver addresses and few other bits, we were able to emulate any type of message on the channel (e.g. Simple GeoNetworking, CAM, DENM, SPATEM and MAPEM) and to have them correctly interpreted by the RSU and the car On Board Units (OBU) devices.
Potentially, at this point, an attacker would be able to carry out AD cars flooding attacks, generate fictitious traffic light signals, report a false presence of pedestrians within the road, set unfit speed limits, realize OBU and/or RSU attacks spoofing, and so on.
Becoming aware of this result, we can move on to the introduction of the cybersecurity remediation to be applied to the ITS-G5 infrastructure, ensuring to make attacks of this type unfeasible in the next future.

8.2.2.7 Autopilot Risk Analysis Results

The autopilot risk analysis identified and predicted several risks and corresponding countermeasures. This has been done by dividing the System Under Consideration (SUC) in three main zones, as required by the risk analysis procedure described in ISA IEC 62443-2-3:

- The Cloud IoT platform,
- The V2X and IoT network of connected devices,
- The in-vehicle network.

The mitigations for the identified risks have then be mapped to system level requirements given in ISA IEC 62443-3-3 so that the security level capability (SL-C) of the overall system can be derived by following the requirements in that part of the standard.

The final requirements are collected in the annex of the D1.9 deliverable (and annex A of this Document).

As the previous sections shows, an initial pen-test, executed on the system before the full set of mitigations have been implemented, can demonstrate that the foreseen risks are effectively impacting the system negatively until mitigations are put in place.

The use of the ISA IEC 62443 has been beneficial in both providing grounded guidance to the risk analysis process and in deriving results and mitigations that can be easily tested, understood and compared.

9 Bibliography

[1] ETSI EN 302 663 V1.2.1 (2013 – 07) – Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band
[2] ETSI TR 102 893 V1.2.1 (2017-03) – Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)
[3] AUTOPILOT "D1.10 – Final specification of Security and Privacy for IoT-enhanced AD", 2019
[4] AUTOPILOT "D1.1 – Initial specification of IoT-enabled Autonomous Driving use cases", 2017
[5] AUTOPILOT "D1.3 – Initial IoT Self-organizing Platform for Self-driving Vehicles", 2017
[6] AUTOPILOT "D1.7 – Initial specification of Communication System for IoT-enhanced AD", 2017
[7] AUTOPILOT "T1.2 – IoT Architecture and Specification", 2017
[8] AUTOPILOT "T1.3 – Vehicle IoT Platform Specification", 2017
[9] AUTOPILOT "T1.4 – Communication Specification", 2017
[10] ANSI/ISA – 62443 – 3 – 3 – (99.03.03) – 2013 – Part 3 – 3: Security for industrial automation and control systems.
[11] ETSI EN 302 665 V1.1.1 (2010-09) – Intelligent Transport Systems (ITS); Communications Architecture.
[12] ITU – T – Y.2060 (06/2012) – Next Generation Networks – Frameworks and functional architecture models – Overview of the Internet of Things (https://www.itu.int/rec/T-REC-Y.2060-201206-I)
[13] ERTRAC – Automated Driving Roadmap – V6.0 – Draft for Public Consultation 03.04.2017
[14] AUTOPILOT "D1.5 – Initial open IoT Vehicle Platform Specification", 2017
[15] http://www.onem2m.org/
[16] https://www.fiware.org/
[17] http://www.zigbee.org/
[18] www.isa.org
[19] http://www.iec.ch/about/activities/?ref=menu
[20] https://www.isa.org/isa99/
[21] https://www.iso.org/isoiec-27001-information-security.html
[22] http://isa99.isa.org/Public/Information/The-62443-Series-Overview.pdf
[23] http://www.etsi.org/about
[24] http://www.etsi.org/technologies-clusters/technologies/automotive-intelligent-transport
[25] http://www.etsi.org/about/what-we-do/global-collaboration/onem2m
[26] http://www.onem2m.org/about-onem2m/why-onem2m
[27] https://www.iso.org/
[28] https://www.iso.org/standard/66435.html
[29] https://www.iso.org/standard/54534.html
[30] https://www.iso.org/standard/54533.html
[31] http://www.etsi.org/news-events/news/851-2014-12-press-etsi-publishes-european-standards-for-intelligent-transport-systems
[32] ETSI TR 102 638 V1.1.1 (2009-06) – Intelligent Transport Systems (ITS); Vehicular Communications; basic Set of Applications; Definitions
[33] IEEE 802.11-2016 – IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
[34] 1609.3-2016 – IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Networking Services
[35] http://www.onem2m.org/images/files/deliverables/Release2/TR-0008-Security-V2_0_0.pdf - oneM2M TR-0008-V.2.0.0 Security 2016 – August – 30
[36] Boyle, David, and Thomas Newe, "Securing Wireless Sensor Networks: Security

Architectures." JNW 3.1 (2008): 65-77.
[37] André Weimerskirch – « Authentication in Ad-hoc and Sensor Networks », Thesis Report, RuhrUniversity Bochum, Germany, 2004
[38] Wassim Znaidi, Marine Minier, Jean-Philippe Babau, "An ontology of attacks in Wireless Sensors Networks", INRIA Research Report n°6704, October 24th 2008, France
[39] https://www.xjtag.com/about-jtag/jtag-high-level-guide/]
[40] Pirzada, Asad Amir, and Chris McDonald. "Circumventing sinkholes and wormholes in wireless sensor networks." *IWWAN'05: Proceedings of International Workshop on Wireless Ad-hoc Networks*. Vol. 71. 2005.
[41] Juels, Ari, and John G. Brainard. "Client puzzles: A Cryptographic countermeasure against connection depletion attacks." *NDSS*. Vol. 99. 1999.
[42] ETSI EN 302 637-2 V1.3.1, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service
[43] ETSI EN 302 637-3 V1.2.1, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service
[44] KERBEROS RFC; https://tools.ietf.org/html/rfc1510
[45] ADVANCES IN ITS SECURITY STANDARDS, Public Workshop C2C-CC, ETSI and HTG#6, Stockholm, 17th June 2015 (https://www.preserve-project.eu/sites/preserve-project.eu/files/preserve-ws-etsi-status.pdf)
[46] ETSI TS 102 940 V1.1.1, Intelligent Transport Systems (ITS); Security; TS communications security architecture and security management (*schematic view of basic service protection for ITS-S station security*)
[47] ETSI TS 102 941 V1.1.1, Intelligent Transport Systems (ITS); Security; Trust and Privacy Management
[48] ETSI TS 103 097 V1.2.1, Intelligent Transport Systems (ITS); Security; Security header and certificate formats
[49] ETSI TS 102 965 Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration
[50] Hildebrandt, M., Jacobs, B., Meijer, C., Ruiter, J.D., & Verheul, E.R. – Polymorphic Encryption and Pseudonymisation for Personalised Healthcare. IACR Cryptology ePrint Archive, (2016)
[51] Camenisch, J., Van Herreweghen, E.: Design and implementation of the idemix anonymous credential system. In: Proceedings of the 9th ACMConference on Computer and Communications Security, CCS '02, pp. 21–30. ACM, New York, NY, USA (2002)
[52] IBM Research Zurich: Specification of the identity mixer cryptographic library. Tech. rep. (2013)
[53]Paquin, C., Zaverucha, G.: U-prove cryptographic specification v1. 1. Tech. rep., Microsoft (2011)