D2.1
Multi-Modal Transport Ecosystem Use-Cases

Work Package	2
Task	Multi-Modal Transport Ecosystem Use-Cases
Authors	Andrew Roberts (TalTech), Liivar Luts (TALLIN), Raivo Sell (TalTech), Kostas Maliatsos (UPRC)
Dissemination Level	Public
Status	Final
Due Date	30/04/2021 (M8)
Document Date	30/04/2021 (initial) 31/05/2022 (revision)
Version Number	1.0

Quality Control

Role	Name	Organisation	Date
Editor	Liivar Luts	Tallinn	16/04/2021
Peer review 1	Alkiviadis Giannakoulias, Anastasia Garbi Paraskevi Plagaki	ED	23/04/2021
Peer review 2	Sammy Haddad	OPP	23/04/2021
Authorised by (Technical Coordinator)	Jason Sioutis	ICCS	29/04/2021 (initial) 26/05/2022 (review changes)

Authorised by (Quality Manager)	Panagiotis Lytrivis	ICCS	29/04/2021 (initial) 27/05/2022 (review changes)
Submitted by (Project Coordinator)	Angelos Amditis	ICCS	30/04/2021 (initial) 31/05/2022 (review changes)

Contributors

Name	Organisation
Andrew Roberts	TalTech
Raivo Sell	TalTech
Liivar Luts	Tallinn Transport
Konstantinos Maliatsos	University of Piraeus
Fabio Podda	AMT Genoa
Luca Bianconi	SIGLA
Alkiviadis Giannakoulias	European Dynamics

Document Revision History

Version	Date	Modification	Partner
0.1	16/04/2021	Draft Release	TalTech
0.2	26/04/2021	Review Feedback	TalTech & Genoa
0.3	28/04/2021	European Dynamics Review Updates	University of Piraeus and European Dynamics
0.4	29/04/2021	ICCS Updates	ICCS
1.0	30/04/2021	Tallinn final Version	TalTech, Tallinn
1.1	31/05/2022	Revision based on reviewer comments	AMT Genoa Tallinn, TalTech University of Piraeus.

Legal Disclaimer

CitySCAPE is an EU project funded by the Horizon 2020 research and innovation programme under grant agreement No. 883321. The information and views set out in this deliverable are those of the author(s) and do not necessarily reflect the official opinion of the European Union. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any specific purpose. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the

information contained therein. The CitySCAPE Consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

Table of Contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

Abbreviation	Meaning
4G	Fourth Generation Network
5G	Fifth Generation Network
AFC	Automated Fare Collection
AMT	Genova Public Transport Operator
APC	Passenger Counting System
API	Application Programming Interface
APP	Application Program
AV	Autonomous Vehicle
AV	Autonomous Vehicle
AVM	Automated Vehicle Monitoring
C&C	Command and Control
CAMS	Cooperative Awareness Message
CAN	Controller Area Network
CCTV	Closed-circuit television
CERT/CIRT	Computer Emergency Response Team/ Cyber Incident Response Team
COCO	Common Objects in Context
DBMS	Database Management Systems
DSRC	Dedicated Short-Range Communications
ECU	Engine Control Unit
EMV	Europay, MasterCard,Visa
FIDO	Fast ID Online Protocol
FTP	File Transfer Protocol
GNSS	Global Navigation Satellite System
GUI	Graphical User Interface
HSM	Hardware Security Module
HTML	Hypertext Markup Language
HW	Hardware
ISIC	International Student Identity Card
ITS	Information Technology Systems
ITS-G5	Intelligent Transport System G5 (Frequency Band 5.9 Ghz)
ITxPT	Information Technology for Public Transport
JASON	JavaScript Object Notation

MaaS	Mobility-as-a-Service
MaaS	Mobility-as-a-Service
MAP	Map topology
MDVR	Mobile Digital Video Recorders
MQTT	Message Queuing Telemetry Transport
N/A	Not Available
NETEX	Network Timetable Exchange
NFC	Near Field Communication
OBU	On-board unit
OJP	Open Journey Planning
OPINFO	Website where announcements about planned changes in public transport. https://opinfo.tallinn.ee/kaart
OS	Operating System
PC	Personal Computer
PIKAS	Tallinn Public Transport Scheduling Software
POS	Point of Sale
RAID1	Redundant Array of Independent Disks Mode 1
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RFID	Radio-Frequency Identification
ROS	Robot Operating System
RSU	Road Sign Unit
RSU	Road Side Unit
SFTP	Secure File Transfer Protocol
SIRI	The Standard Interface for Real-time Information
SPaT	Signal Phase and Timing
SQL	Structured Query Language
SSH	Secure Shell Protocol
SW	Software
TELNET	Network protocol for remote terminal
TIGR	Telediagnostic for Intelligent Garage in Real-time
TLS	Transport Layer Security
TLT	Tallinn Public Transport Operator
TTA	Tallinn Transport Department
TTP	Tactics, Techniques and Procedures

UDP	User Datagram Protocol
USB	Universal Serial Bus
V2V	Vehicle to vehicle
V2X	Vehicle-to-Everything
V2X	Vehicle to everything
VLAN	Virtual LAN
VPN	Virtual Private Network
vSwitches	Virtual Switch
WAVE	Wireless Access in Vehicular Environments
XML	Extensible Markup Language
YOLO	You Only Look Once

Executive Summary

Deliverable 2.1 details the multimodal transportation ecosystem use-cases defined by the cities of Genoa, Italy and Tallinn, Estonia. The major concepts of multimodal transport covered in the use-case definition include:

- Mobility-As-A-Service
- Adaptive Traffic Control
- Infomobility
- Electronic and mobile ticketing

These use-cases, whilst diverse, demonstrate a variety of multimodal transport scenarios which focus on the interaction of the passenger with the transportation platforms and supporting system assets. They present realistic scenarios which the cities have selected for their importance for protection against cyber threats. The transportation modes included in the use-cases are:

- Bus
- Tram
- Trolley
- Trains
- Autonomous vehicle shuttle.

These modes exhibit both conventional city transportation and new innovative platforms such as autonomous vehicle public transportation.

An initial cyber threat scenario analysis has been provided, which will be updated from the results of risk modelling and vulnerability-threat analysis, the adopted system architecture, the pilot design and objectives, the types and methods of attack that may be demonstrated. Goals for the CitySCAPE solution were identified as:

1. Improve confidence in efficient handling of 0-day and denial-of-service attacks.
2. Minimise security risks introduced by (less-security aware) external service providers.
3. Improve fraud protection.
4. Minimise risks to personal privacy related to fraud prevention and new ticketing services.

1 INTRODUCTION

1.1 Project Introduction

The traditional security controls and security assurance arguments are becoming increasingly inefficient in supporting the emerging needs and applications of the interconnecting transport systems, allowing threats and security incidents to disturb all dimensions of transportation. CitySCAPE is a project funded by the EU's Horizon 2020 research and innovation program, which consists of 15 partners from 6 European countries, united in their vision to cover the cybersecurity needs of multimodal transportation. More specifically, the CitySCAPE software toolkit will:

- Detect suspicious traffic-data values and identify persistent threats.
- Evaluate an attack's impact in both technical and financial terms.
- Combine external knowledge and internally-observed activities to enhance the predictability of zero-day attacks.
- Instantiate a networked overlay to circulate informative notifications to CERT/CSIRT authorities and support their interplay.

The project duration extends from September 2020 to August 2023.

WP2 unfolds activities related to the use-cases and the threats in the multimodal transport domain. Initial use-cases will be further detailed and updated, while an exhaustive threat analysis taking into high consideration GDPR will be developed. WP2 outcomes will set the basis for the articulation of the two CitySCAPE pilots planned.

1.2 Deliverable Purpose

The purpose of this document is to provide the initial specification of multi-modal transportation use-cases that are targeted at piloting in CYBERSCAPE. The final deliverable (D2.1) of task 2.1 will be a detailed description of the use cases. The document is provided in M08 of the project so that the cross-domain threat analysis (Task 2.2) and user/systems requirements and architecture (WP 3.3) can conduct their analysis based on the detail provided by Tallinn multi-modal transport use-cases.
The purpose is to also provide indicative use cases that will help identify systems and assets vulnerabilities, threats and attack vectors. This information will be used to design the technical use-cases that will be presented in WP3, including all required details in relation to the involved CitySCAPE components and the datasets used to identify and respond to cyber security incidents.

1.3 Intended Audience

Besides the project reviewers, this deliverable is addressed to any interested reader (i.e., Public dissemination level). This deliverable is intended for reading by all transport and cybersecurity experts in the field, especially those in the public sector and also for internal project reviewers.

The deliverables outcomes have direct relevance to the following CitySCAPE tasks:

Task	Relationship
Task 2.2: Cross-domain threat analysis	Transportation assets and cyber security threats identified in task 2.1 will aid the cross-domain threat analysis. Specifically, this will aid them in understanding how the multi-modal transportation environment is impacted by cyber threats against major Operators of Essential Services (OES) and Digital Service Providers (DSP).
Task 3.1: User requirements elicitation	The use-cases detailed in task 2.1 will assist task 3.1 in identifying and categorising the requirements the CitySCAPE solution must have from an end-user perspective.
Task 3.2: System requirement elicitation	The use-cases and the role of CitySCAPE envisaged by Tallinn and Genoa, as detailed in Task 2.1, will assist Task 3.2 and 3.3 in developing the requirements and the design of the overall CitySCAPE architecture.
Task 3.3: Secure multi-modal transport architectures	

Table 1: Tasks and their relationships

1.4 Outline of the Document

This document is structured as follows:

- Chapter 2: Description of Design Process for CitySCAPE Multi-Mode Use Cases
  - Use-Case Design Methodology
- Chapter 3: Tallinn Use-Cases:
  - Use-Case 1: Last-mile extension/Mobility-as-a-Service (MaaS).
  - Use-Case 2: Adaptive Traffic Management
  - Cyber Threat Assessment
  - CitySCAPE Solution Integration
- Chapter 4: Genoa Use-Cases
  - Use-Case 3: Infomobility
  - Use-Case 4: Ticketing
  - Cyber Threat Assessment
  - CitySCAPE Solution Integration
- Chapter 5 Conclusion and recommendations

2 DESCRIPTION OF DESIGN PROCESS FOR CITYSCAPE MULTI-MODE USE-CASES

This section details the methodology for the design of the multimodal transportation use-cases that this project will pilot. The CITYSCAPE project is focused on enhancing the cybersecurity of multimodal transportation platforms and addressing users and data privacy concerns. Therefore, the main criteria for the selection of the use-cases are listed as follows:

- Involvement of multimodal transportation platforms.
- Inclusion of stakeholders and assets involved in transportation user data such as payment systems, transportation security and live-tracking systems.
- Realistic to the journey and interactions of a transportation user in the Genoa and Tallinn transport environment.
- Realistic to the future architecture of the transportation environment. The use-case must enable solutions that have future applicability and are not just built for today.
- The use-cases detailed in this section will be used to develop cybersecurity technologies and methods.

Finally, it is worth mentioning that the set of selected use-cases will be studied with a primary focus on the so-far under-explored areas involved, such as identifying specific security- and privacy vulnerabilities and the requirements of the CPaaS.

2.1 Use-Case Definition Methodology

A nine-step procedure was defined and followed in order to structurally design the use cases for the two CitySCAPE pilot sites. In this section, a description and analysis of the process are defined.

Step 1:
Determination of users and stakeholders:
Identify users and stakeholders expected to participate in the operation/exploitation of the system services and resources. It is generally expected to identify persons, however, other authorities, service providers, and corporate entities may also be considered a "user" or a "stakeholder".
For example: User of bus/metro services, operators of transport services, system administrator, system developer, security engineer, transport authorities, etc.

Step 2:
Description of the typical-desired system/platform operation from the end-user perspective:
At this stage, the focus is given on the typical/expected operation of the platform - as experienced by the end-user. While avoiding many technical

details, a description of events - typically triggered by the end users and the resulted system response is presented. At this step, the trip narrative is introduced.
As an example:

- A citizen is entering into a metro station and uses/validates his/her city-pass to enter the station using a mobile phone app. He/she is informed about the estimated time of arrival of the train, while through a trip planner service finds the timetables for transfer buses, and so on.

A scenario may involve transport authority officials or anyone else according to the scope of the use case and the project objectives. A simplified sequence diagram may be used to describe the trip narrative.

Step 3:
Specification of the System Boundary.
The specific step is generally performed in conjunction with Step 4. The system boundary defines the system of interest in relation to its environment. In a way, it is an attempt to define the boundaries of the target of evaluation (in terms of a certification/assessment procedure). The system boundary contains all the system components (functional, data and security) that are required for the operation of the system and will be investigated in the project context. Entities and elements external to the system boundaries are considered non-accessible and non-trusted.

Step 4:
Elaboration on the operational view - the assets and the entities.
The end-user request or action triggers a series of events. During this step, a more technical view is adopted. The objective is to track the process from the event triggering to the system reaction (usually provision of a service) by following the procedure flowing through the various system components. The objective of this step is to identify the system components and their interconnections. For example:

- A citizen wants to buy a ticket through an app. Through credentials, the application verifies the user id and establishes a secure connection with the ticketing server, as well as a banking service, and so on.

As system **assets**, we define entities that play specific key roles in the implementation narrative of the use case; and essential elements that represent functions and information providing added value to the entities. The assets are the system elements that have value and have to be protected. Generally, the assets can be further "divided" in components (or sub-assets). The level of detail in the definition of assets depends on the depth of the analysis. At this step, the assets participating in the use case should be specified. At the first iteration of the methodology, high-level assets can be considered.

Step 5:
Categorize assets and describe their operation.
In a cyber-physical system, the assets have to be categorized as follows: data assets (databases, files, etc.); software assets; hardware assets; network assets/communication channels; virtual machines or virtual network

functions; information messages; keys, IDs and certificates. In most cases, the assets are hybrid, i.e. combinations of the basic asset types. At this step, it is required to specify the type of each asset - as a combination of the aforementioned generic categorization.
The elements to be investigated are:

a) The functionalities/services offered by the asset;
b) Resources that are used/consumed to provide the aforementioned functionalities/services.

As an example:

- An application server installed on a physical machine in the organization premises is:
    - A software asset.
    - Installed on hardware resources.
    - Using or producing data (from a database or log files).

In conjunction with Step 4, the next step is to provide a description of what exactly is offered by the asset as a functionality or service. For example:

- The application server hosts a website; it presents the bus schedule to the user, extracted from a database installed in the same machine; Software and data assets are installed on a Linux machine with RAID 1.

Step 6:
Specify interfaces and users
The assets can be accessed through exposed interfaces. Generally, these interfaces are also the entry points of the system. The interfaces can be:

- Input-Output user interfaces and terminals (either software or hardware).
- Application Programming Interfaces (APIs)
- Network services and ports
- They may take other forms depending on the actual application service.

The assets may also have ownership. For example,

- The files (or the more critical certificates) may be owned by a specific user.

Finally, the information messages can be considered "owned" by the sender and/or the recipient.
To sum up, the objectives of this step are:

- To define the interfaces of the asset.
- To identify ownership of assets, if any.
- To identify who is actually using the interfaces (and also possibly identify unused exposed interfaces)

The interfaces are used in order to exploit an asset service and/or functionality. Thus, it has to be specified who/which user/service uses what. An asset interface may be used by:

- User/stakeholder, or
- Another asset, or
- External system.

Step 7:
Use case definition process

Repeat Step 2 and Step 4, using all identified assets, interfaces, users and external actors in order to define the information flow/event sequence realistic to how they would operate during the use-case scenario.

Step 8:

Add a flavour in the use-case

Up to this step, the use case description does not include any threat, risk, or attack. It simply describes a scenario, a set of assets, and a flow. That's why this risk modelling step will focus on each asset and identify vulnerabilities and, as a next step, identify threats and attacks that can exploit the vulnerabilities. In fact, risk modelling and threat analysis processes are investigated thoroughly in Tasks 2.2 and T2.3. However, in the context of D2.1, a first attempt to propose specific threats and attacks that the users and stakeholders consider critical and related to the CitySCAPE, objectives and that could be possibly demonstrated in the final events, can be made.
Identify and describe elements of (for). Thus, we deem it also necessary to make the first list of interest for the use-cases further studied in other work packages of the project or during the project. The attack description should identify the compromised asset and the interface that is used to implement the attack. Whenever possible, the potential propagation of the attack into the system and its effect on the overall operation should be described.

Step 9:

Attempt to envision the CitySCAPE solution in the use case

At this point, the use case is completed. However, the purpose of the use case is to facilitate the description of the system architecture, the definition of provided services by the CitySCAPE solution and how the CitySCAPE solution will interact with the CPaaS platform, and thus, during this step, an initial analysis of the user requirements for the CitySCAPE solution and realistic suggestions on how the CitySCAPE platform can be integrated into the described solution is made.

The procedure is summarized in Figure 1

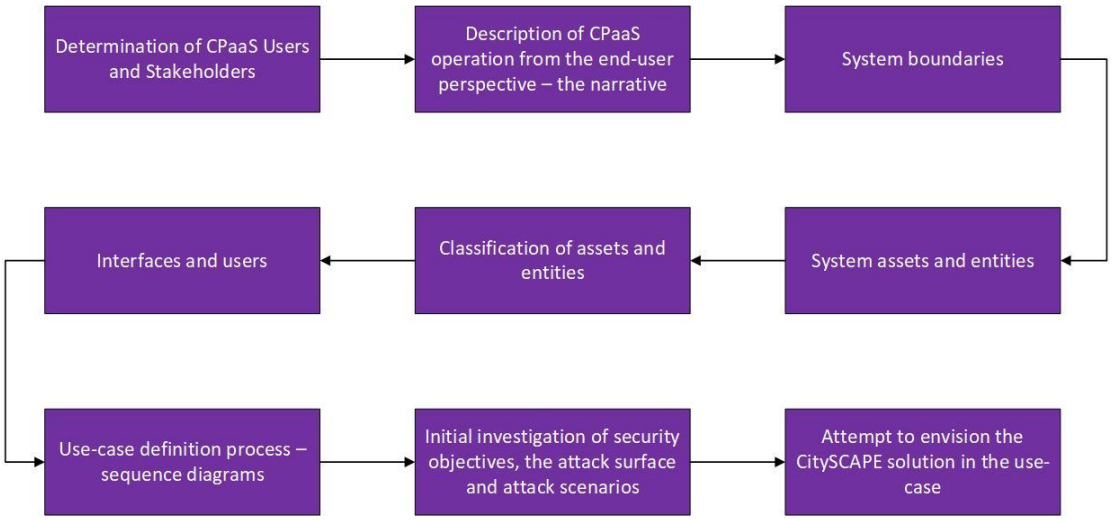

Figure 1: 9-step Use case definition methodology

3 TALLINN USE-CASE

The Tallinn Use Case will focus on two main smart city transportation ecosystem fields:

- Mobility-As-A-Service (MaaS)
- Adaptive Traffic Control

The macro scenario details the MaaS and Adaptive Traffic control concepts and the passenger, end-user, transportation journey and how the transport systems facilitate this. "Micro" scenarios focus on very specific situations. Each scenario will be detailed as follows:

- Definition of the "story" behind the scenario: actors, expected behaviour;
- Schematization of the process flow with the link between actors;
- Identification of the asset involved in the scenario;
- Sequence diagram to define the process;
- Identification of the possible attacks that could be made on the scenario;
- Identification of the blocks of the CitySCAPE platform that could help in mitigating the risk.

3.1 Mobility-as-a-Service Use Case

Last-Mile extension in the Tallinn Transport network refers to passenger transportation services that assist the Tallinn transport user in travelling from the end destination of their Tallinn city-transportation mode (bus, trolley, tram) their journey end destination. In the Tallinn Transport network, these last-mile extension services are provided by autonomous self-driving

shuttles (Figure 2).

Figure 2: Tallinn ISEAUTO Last-Mile Extension Service

Mobility-as-a-Service (MaaS) is a concept of integration of all urban mobility platforms: autonomous shuttles, e-scooters and e-bikes, city-transportation, and shared private transportation services. The enabler for MaaS is the real-time geo-location information of the transportation services. Real-Time geo-location allows the Tallinn transportation user to be informed, plan, and track the progress of their journey. Currently, the city-transport modes use a different real-time geo-location system to the last-mile extension. Figure 3 shows the live-tracking of the city-transport modes with the Tallinn Transport scheduling and live-tracking data. Figure 4 shows the web interface for the autonomous self-driving shuttle live geo-location.

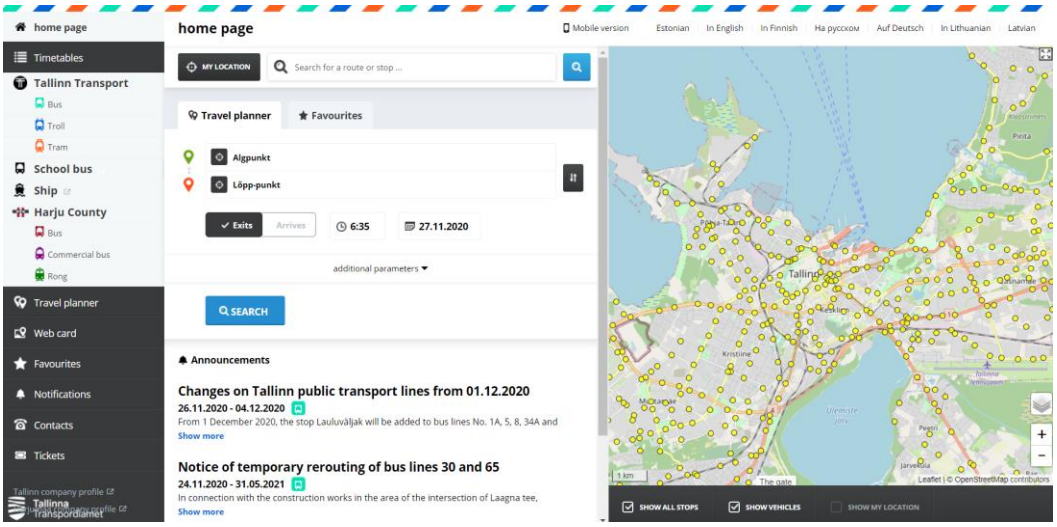

Figure 3 Mobility-as-a-Service of the city-transportation network.

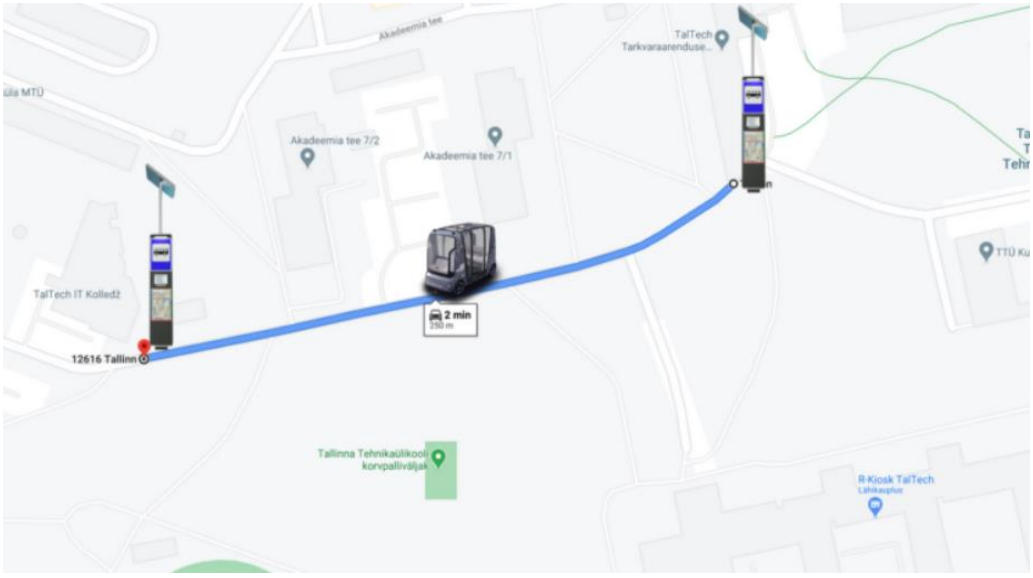

Figure 4: Mobility-as-a-Service of the Last-Mile Extension

The live-tracking is enabled by GPS, global positioning, location services. This is crucial for providing passengers information as to the progress of the transportation modes to the timetable. The original intent CitySCAPE was to assess the accuracy of the GPS unit in the payment validators, however, due to the addition of the AV shuttle to the scope, it is more relevant to

investigate the ability of the CitySCAPE platform to detect cyber-attacks or anomalies that could impact the accurate location of the AV Shuttle in the multi-modal transportation environment.

3.1.1 Users and Stakeholders

Users and stakeholders identified in the Tallinn Transport network for the MaaS use-case are depicted in figure 5. The users and stakeholders differ in each of the macro use-case scenarios as the systems involved in the MaaS are different to the Adaptive Traffic Control. Also, the Adaptive Traffic Control use-case is conducted in the traffic environment of Tallinn Smart Campus.

The users and stakeholders have been categorised as follows:

- A *user* is a primary user of transportation services. For example, a citizen of Tallinn uses the Tallinn bus service to journey from Estonia bus station to Keemia bus station.
- A *stakeholder* is an entity or individual involved in *operating, supporting* or *managing* the transportation service. For example, the private operator of the city bus services.
- An *external stakeholder* is an entity external to the management, operation, and support of the city-transportation environment that provides services essential to the city-transportation journey. For example: a company that provides the telematics units in the city busses for real-time information tracking and stores the information in their data centre.

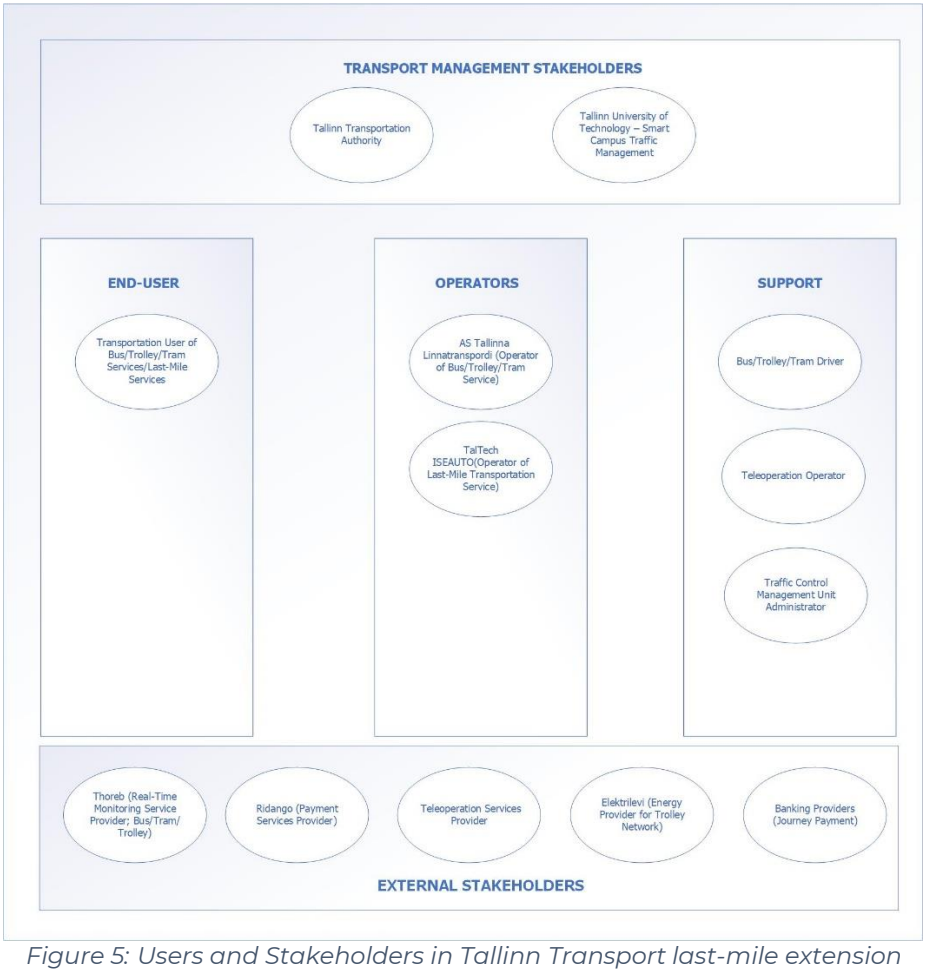

Figure 5: Users and Stakeholders in Tallinn Transport last-mile extension

Detailed Description of User and Stakeholders in Tallinn City Multi-Modal Transport Network
Actor: Transportation User of Bus/Trolley/Tram/Autonomous Vehicle Shuttle **Role:** User **Description:** Citizen or visitor to Tallinn that uses city-transportation services; Bus/Trolley/Tram and last-mile services; autonomous self-driving shuttles/e-scooters/e-bikes. To use the city-transportation network in Tallinn, the transportation user has the following options: • They can validate their journey on a Ridango ticket validation machine inside the transport mode using either their Tallinn Transport card or their credit card. • They can purchase a ticket online through (https://tallinn.pilet.ee/buy) and receive a QR code that can be used on the Ridango Payment validator. • The transport user can purchase a ticket from the driver of the transportation mode. Citizens of Tallinn can use the city transportation network for free. However, they still must validate their journey using the Ridango ticket validator. Paid city-transportation travel operates by purchasing and updating the balance of the Tallinn Transport Card, either at Kiosk shops or online (https://tallinn.pilet.ee/buy).
Actor: AS Talllinna Linnatransport (TLT) AS (Operator of Bus/Trolley/Tram Services) **Role:** Stakeholder **Description:** TLT are the operators of the Bus, Trolley, Tram services in Tallinn, Estonia.
Actor: TalTech ISEAUTO (Operator of Last-Mile Transportation Services) **Role:** Stakeholder **Description:** The TalTech ISEAUTO is an autonomous self-driving public transportation shuttle. It is designed and operated by the TalTech ISEAUTO team. Their responsibilities include system engineering, modifications/upgrades to the shuttle, as well as operation of the shuttle using the teleoperation station, normally located at TalTech campus, however, able to be located wherever.
Actor: Bus/Tram/Trolley Driver

Role: Stakeholder
Description: Responsible for driving the city-transportation mode.

Physical Location: Tallinn, Estonia

Actor: Teleoperation Operator
Role: Stakeholder
Description: The Teleoperation Operator is responsible for actively monitoring the journey of the autonomous self-driving public transport shuttle and taking driving actions if required. The operator is located in the teleoperation station at TalTech campus. The operator is a licenced driver, according to the Estonian Traffic Act. The ISEAUTO has the ability for the shuttle to be remotely operated from diverse geographic locations.

Actor: Traffic Control Management Unit Administrator
Role: Stakeholder
Description: The Traffic Control Management Unit Administrator is responsible for the administration of the Tallinn City traffic system. This involves activities such as monitoring traffic flows and programming and re-programming traffic lights.

Actor: Tallinn Transport Authority
Role: Stakeholder
Description: Authority responsible for Tallinn City-Transportation.

Actor: Tallinn University of Technology Smart Campus Traffic Management
Role: Stakeholder
Description: The Tallinn University of Technology Smart Campus Traffic Management is responsible for the administration of the smart campus private roads. This includes the last-mile extension from Keemia bus stop to the Mektory. The TalTech campus has interactive pedestrian crossings and will be responsible, in the pilot, for the adaptive traffic control.

Actor: Mobile Application Provider **Role:** Stakeholder **Description:** Provider of the passenger interface for Tallinn Transport scheduling and live-tracking.
Actor: Payment Service Provider **Role:** Stakeholder **Description:** Provides the ticket validation and payment infrastructure for the public transportation system. **Physical Location:** Tallinn, Estonia
Actor: Teleoperation/Remote Control Center Software Platform Provider **Role:** Stakeholder **Description:** The Teleoperation/Remote Control Center Software Platform Provider is a 3rd party provider of the teleoperation system for remote control of the autonomous self-driving shuttle. The teleoperation/remote control center software is a module on the Robot Operating System (ROS) middleware used by the autonomous vehicle shuttle.
Actor: Electrolevi **Role:** Stakeholder **Description:** Electrolevi is a 3rd party provider of electricity distribution services. The electricity network is relied on for the trolley and tram services.
Actor: Banking Providers **Role:** Stakeholder **Description:** Banking Providers are 3rd party providers of the payment services for the city transportation network.

Table 2: Users and Stakeholders in Tallinn City Multi-Modal Transport Network

From the description of users and stakeholders,

- The multi-modality of the Tallinn pilots can be verified since a) multiple transportation systems are involved (Buses, Trolleys, Trams, Autonomous vehicles) operated by different operators and stakeholders (TLT and TalTech ISEAUTO)

- The cross-domain character of the use case is supported by the fact that the overall platform relies on a) telecommunication services provided by operators, b) banking/payment services provided by the banking ecosystem, c) power grid services provided by electric distribution service providers, d) data analytics/digital services provided by third parties.

3.1.2 Macro Scenario: MaaS Use Case

This section focuses on the definition of scenarios that describe the real-life situation in the Tallinn multimodal transport ecosystem.

The desired behaviour of the passenger:

1. The transportation users plan their journey using the Tallinn Transport web application.
2. The transportation user enters the city bus/trolley and uses their Tallinn Transport card or credit card on the ticket validator inside the bus to validate their journey.
3. The transportation user is informed about the estimated time of arrival of the bus through a web interface presented on their mobile device; they can also see when the last-mile service will be available at their intended stop, Keemia or Ehitajate Tee bus stop.
4. The transportation user moves from the city bus/trolley onto the last-mile autonomous self-driving transport bus at their stop and is driven to their final destination, TalTech Mektory. (The user does not pay for the autonomous vehicle shuttle journey currently)

The desired behaviour of the transportation system:

1. The Tallinn Transport web application displays an accurate and real-time information of the Tallinn transportation timetables, routes, transportation modes, and transport journeys' progress.
2. The on-board systems of the transportation modes provide passenger information on external (outside screen display viewable to pedestrians) and internal (inside the bus/tram/trolley) displays.
3. The onboard systems of the transportation modes communicate with traffic infrastructure for effective traffic management.
4. The ticket validation systems allow passengers to validate their transportation journey.
5. The real-time tracking (geo-location) systems allow seamless transition of the passenger from city transportation to last-mile extension.

Figure 6 depicts a high-level Use-Case diagram of the Tallinn last-mile extension from the transport user perspective.

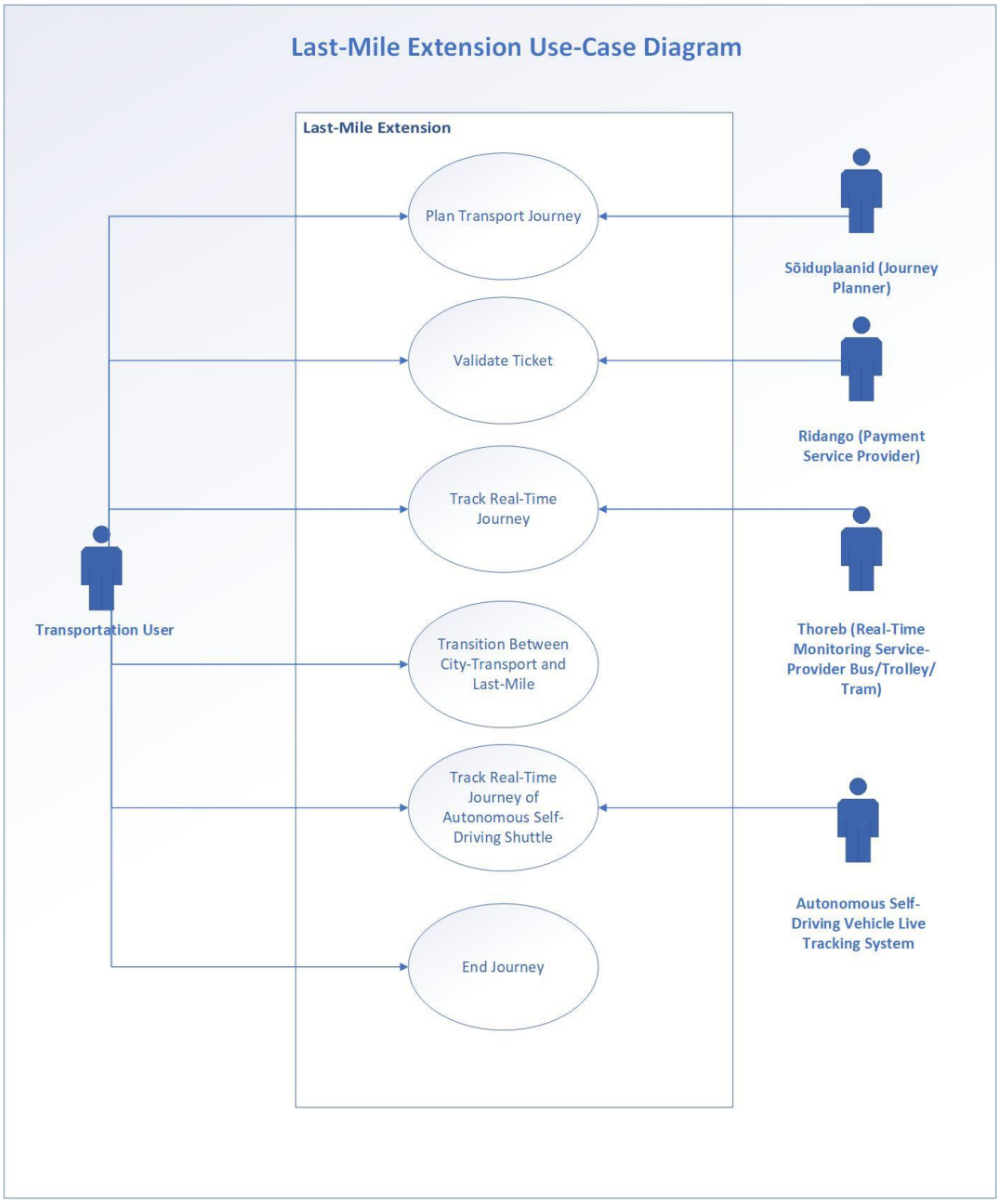

Figure 6: Last Mile Extension Use-Case Diagram

3.1.3 Macro Scenario: Description of typical-desired system/platform operation from the system-of-systems perspective

The multi-modal transportation systems perspective to enact the user journey involves complex system-of-systems interactions involving:

- **Transport platform** (bus/trolley/self-driving vehicle)
- **Road infrastructure**
- **Traffic management**

All of these elements rely on 3rd party providers managed by or on behalf of the city transportation authority, Tallinn Transport.
Multi-modal transportation platforms in the Tallinn use-case consist of the city-transportation modes and the TalTech iseAuto autonomous shuttle.
The Tallinn city transportation modes consist of bus, trolley and tram platforms.

Figure 7: Tallinn City Bus, Trolley, Tram

The trolleys and trams rely on the electricity network for power. If power is lost, then the trolley cannot operate.

The city-transportation network operates from 06:00 to 23:00 daily. The city-transportation network services extend to include important transit points such as Port of Tallinn, Lennart Meri Airport, Tallinn University, Tallinn University of Technology, Tallinn Hospitals and the Central Business District and Old Town.

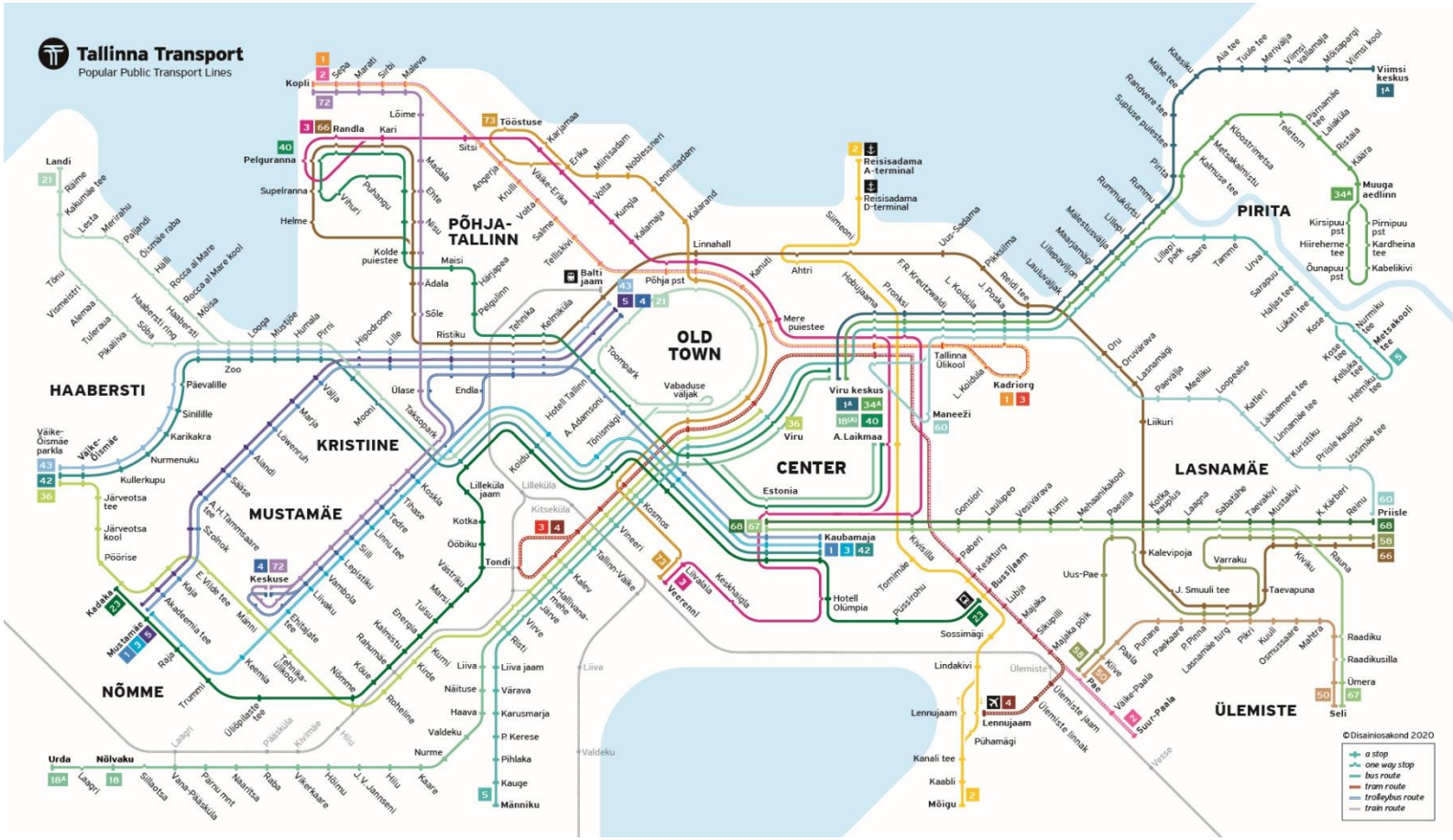

Figure 8: Tallinn City Transportation Network Map

The MaaS use-case will focus on the user journey from Keemia and/or Ehitajate Tee bus station to the Tallinn University of the Technology campus in the Mustamäe district. These bus stations are the intersection point between the city-transportation network and the iseAuto autonomous shuttle.

The **road infrastructure** in the MaaS use-case consists of a typical city. Traffic lights are preprogrammed to manage city traffic flows and traffic conditions are monitored by a centralised management team at Tallinn Transport.

Figure 9: Road Infrastructure of Tallinn

Real-time information is generated from the Tallinn public transport modes. This real-time information is comprised of the telemetry generated from the sensors on-board the vehicle. Such information includes GNSS positioning, passenger count etc. The real-time information is presented to the passengers via a mobile application. In this application they are able to schedule their transportation journey and track the progress of the Tallinn city transportation modes.

Payment and validation of the transportation journey uses a transportation payment validator. A passenger presses their transportation card (which uses the MiFARE classic protocol) against the validation machine to validate their journey. The Tallinn Transport system is a PCI-DSS compliant system. PCI-DSS is a set of standards for the security of payment card gateways and technologies which focus on the following areas:

1. Build and Maintain a Secure Network and Systems
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures

5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

CitySCAPE will emulate the commercial system used in Tallinn Transport. Therefore, this emulated system will not be accredited by a PCI-DSS Qualified Security Assessor (QSA), however, the emulated system will resemble, to a level of abstraction, many of the features of the commercial system, such as network protocols (Mifare classic), storage of cardholder data and access control measures. Ultimately, the emulated payment validation system in CitySCAPE will enable the defensive mechanisms developed to be tested against cyber-attacks against protection of cardholder data.

The **TalTech iseAuto autonomous vehicle shuttle** operates on the TalTech campus traffic network. It is primarily used by TalTech staff, students, and visitors as the last mile extension from their journey using the city-transportation network or as a quicker and more enjoyable means of travel around the university campus. The integration of the passenger journey between the city-transport modes and the autonomous vehicle shuttle is facilitated by the real-time tracking systems. The real-time information available to the transportation users allows them to transition from the city-transportation network effectively and efficiently to the autonomous vehicle shuttle with minimal time delay.

Figure 10: TalTech iseAuto autonomous vehicle & Remote-Control Operations Center

Safety of the transportation user is of paramount importance in the autonomous vehicle shuttle where there is no physically located driver. As depicted in figure 14, a remote-control operation centre with a driver, licenced for driving on Estonian roads, monitors the transportation user journey and can make driving decisions if there are any safety issues. Additionally, there are manual on-board mechanisms to stop the autonomous vehicle shuttle in the form of a "red stop button" located inside and outside the vehicle. The remote-control operation center can be configured anywhere. The TalTech iseAuto has successfully trialed cross-border teleoperation control with a vehicle in Tallinn, Estonia, being controlled by a remote driver in Munich, Germany.

The system boundary of the last-mile, MaaS use-case will encompass the Tallinn City-Transportation modes that utilise Keemia and Ehitajate Tee bus station (Bus, Trolley) and the autonomous self-driving shuttle. Exclusions (Outside the system boundary) are external systems that Tallinn Transport Authority and TalTech do not control. These systems includedata centers, information systems, services, software and hardware offered and operated by 3rd parties (e.g., Ridango payment system and Thoreb telematics).It is important to note that inclusive to the systems' scope is the transportation platforms and the associated traffic infrastructure controlled by Tallinn and TalTech. This includes the AV Shuttle remote control center and the Tallinn traffic management system.

3.1.4 Operational view of the Multimodal Transportation assets and the entities

The objective of detailing the operational view is to track the process from the event of the transportation user input to triggering of the system reaction (usually provision of a service). The operational view details how the process of the transportation end-user requesting a service initiates a procedure that flows through the various system components. The crucial activity of the objective is to identify the system components and their interconnections.

For transportation users to plan their journey on the city network, the mobile web application is used.

3.1.4.1 Mobile Web Application

The mobile web application allows the transportation user to plan their journey and observe the city-transportation modes' progress in real-time. The mobile application uses data collected from the Tallinn City, which originates from on-board units on the transportation modes (bus, tram, trolley) which collect information about journey progress, passenger count etc. Figure 15 shows a journey plan from Estonia to Ehitajate Tee stations.

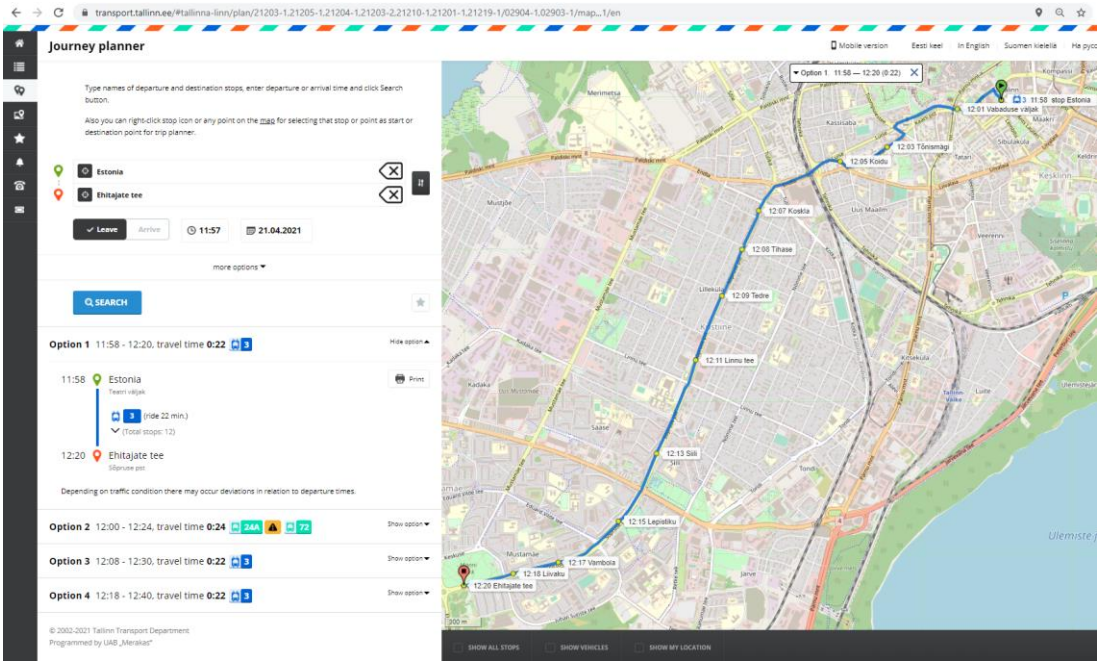

Figure 11: Sõiduplaanid Journey Planner

3.1.4.2 Thoreb Telematics System (Real-Time Geolocation and in-vehicle management)

The Thoreb solution connects within the in-vehicle networkand consists of the driver console system, which allows the driver to view telematics of the bus/tram/trolley, telematics hub which enables communication with the city traffic management and road infrastructure, and internal and external displays which are to inform city-transportation users. The solution is offered and controlled by a 3rd party; therefore, it is not actively used in the described use cases and it is only mentioned for functional completeness.

3.1.4.3 Payment System

The payment system implemented uses an account-based AFC system, in a semi-online mode and without any physical encoding of the travel cards in validators or POS locations. The Mifare-classic type smart cards are used. The system accepts different student and ISIC cards, stickers with chips, wristbands, etc. When the card is used, either through the vehicle system or another device, the token is captured and sent to the central server, where it is processed and stored in the central database. All the relevant ticket and travel card information would be duplicated in the online solution to the vehicle's local on-board database (accepted-list). Accepted-list includes all the information needed to validate the ticket in the particular area as well as the travel card information when there would be some personal discount group or monetary value (e-wallet) related to the card. The information exchange between the back-end and the vehicle' s system is done periodically (can be adjusted according to the actual situation with the connectivity, usually should be less than 1 min). Usually, all the ticket checks and validations are done offline (validation speed <300ms) against the vehicle database. The system makes online queries only if the information about a ticket is not found in the local database.

Due to the wide range of inbound and outbound data integration requirements, the solution is highly modular. It offers a variety of internal and external Application Programming Interfaces (API), starting from:

- transport line data import
- (national) disruption message services
- real-time and ticketing data push
- up to real-time integrations to external ticketing systems
- external Point of Sale (POS) systems
- integrations with a variety of payment processors etc.

On high-level, the system consists of a back-office system (containing ticketing functionalities), customer web front-end, a variety of API-s to interconnect back-end components, back-end and front-end components and the system to a variety of external systems. The highly modular and well interfaced approach provides the flexibility to accommodate to a variety of ticketing schemes and setups.

The payment services provided in Tallinn consist of:

- Transit ticketing system (account based) with mobility account provision and passenger identity
  - Transit hardware: smart controllers, validators with EMV contactless readiness, validators with 2D readers (QR / barcode)
  - Responsive web-based back-office
- Token provisioning via issuing NFC cards
- Revenue collection and clearing back-end (clearing of payments) and reporting to clear collections and payments between re-sellers, Mobility Service Operators and the Scheme Authority
- Handheld devices for ticket inspection, ticket sales and as a substitute for on-board ticketing device
- Large variety of API-s for account-based ticket sales (e.g., integrations to supermarket cash registers, to external ticketing systems).

Figure 16 shows the high-level system architecture offered by Ridango (3rd party) for contactless payments of the Tallinn Transport user.

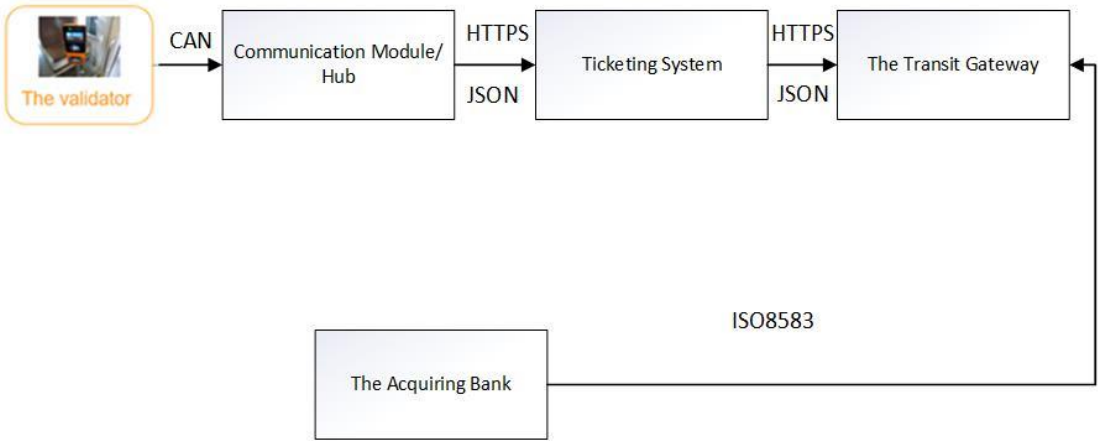

Figure 12: Tallinn Transport Payment System Architecture

Security

Data is transmitted between central server and devices in an optimal packaged format and is encrypted. Prior to the data transmission, a device authorization is required. Validators have tamper switches and their security keys will be lost if the enclosure is opened. Therefore, the ticket validators have to be authorised in the back-office every time they are changed and key management is handled (new keys added). Data is transmitted through Ridango communication module/ hub's mobile network (2G/3G/4G) (each service on the transport platform (bus/tram/trolley) has it's own communication network). To ensure the fastest possible data transmission, only the most necessary data is transmitted between different parts of the distributed system. All devices are also monitored and indication about their statuses is sent to the back-office system given. All activities/events are logged and reports can be triggered.

Other important points to note are:

- The validator is EMV (e.g. Visa payWave, MasterCard PayPass) level 1 certified.
- Banks guarantee the money to the card owner and the merchant.
- Payments are only allowed on public transport. The internal camera's to the bus/ram/trolley capture passengers paying for services. CCTV must be present to monitor behaviour onboard of the public transport.
- Blocklists are used to keep known bad cards from purchasing tickets.

3.1.4.4 TalTech iseAuto Autonomous Shuttle

The main software framework is Autoware, an autonomous driving stack running on top of the Robot Operating System (ROS).

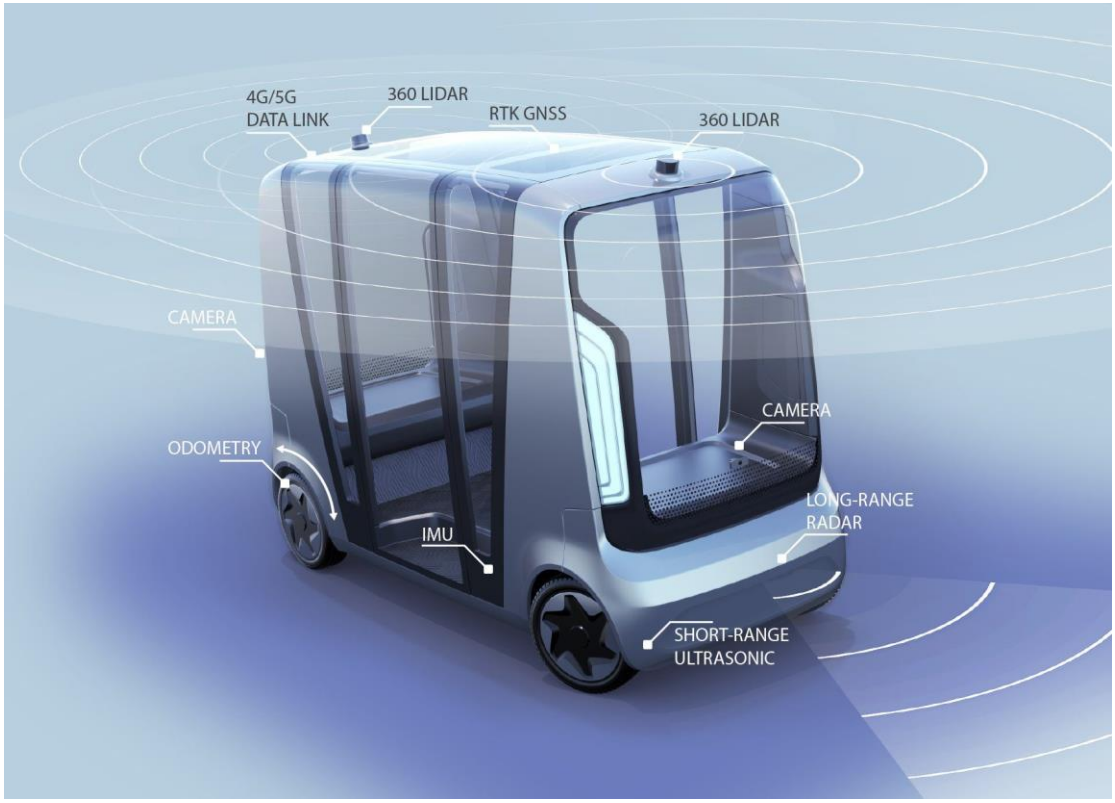

Figure 13: iseAuto sensors and communications

The platform takes inputs from the following types of sensors:
1) LiDAR, radar, and camera inputs are used for localization, obstacles detection, object classification and safety;
2) Global Navigation Satellite System (GNSS) is used for localization correction;
3) Ultrasonic sensors are used for maneuvering and second level obstacle detection;
4) Output commands are steering angle and linear velocity, sent to the low-level controllers over UDP messages.

The robot platform has four Basler Pylon cameras for object detection tasks. One in the front, one on the top and two on both sides. A ROS package for real-time object detection based on YOLO is applied for object detection. The pre-trained model of the convolutional neural network can detect pre-trained classes, including the dataset from Pascal Visual Object Classes (VOC) [1] and Common Objects in Context (COCO). This package publishes the number of detected objects and their position.

The operations and the workflow of the Macro scenario summary are described in the following sequence diagram:

Figure 14: Tallinn MaaS Macro Scenario

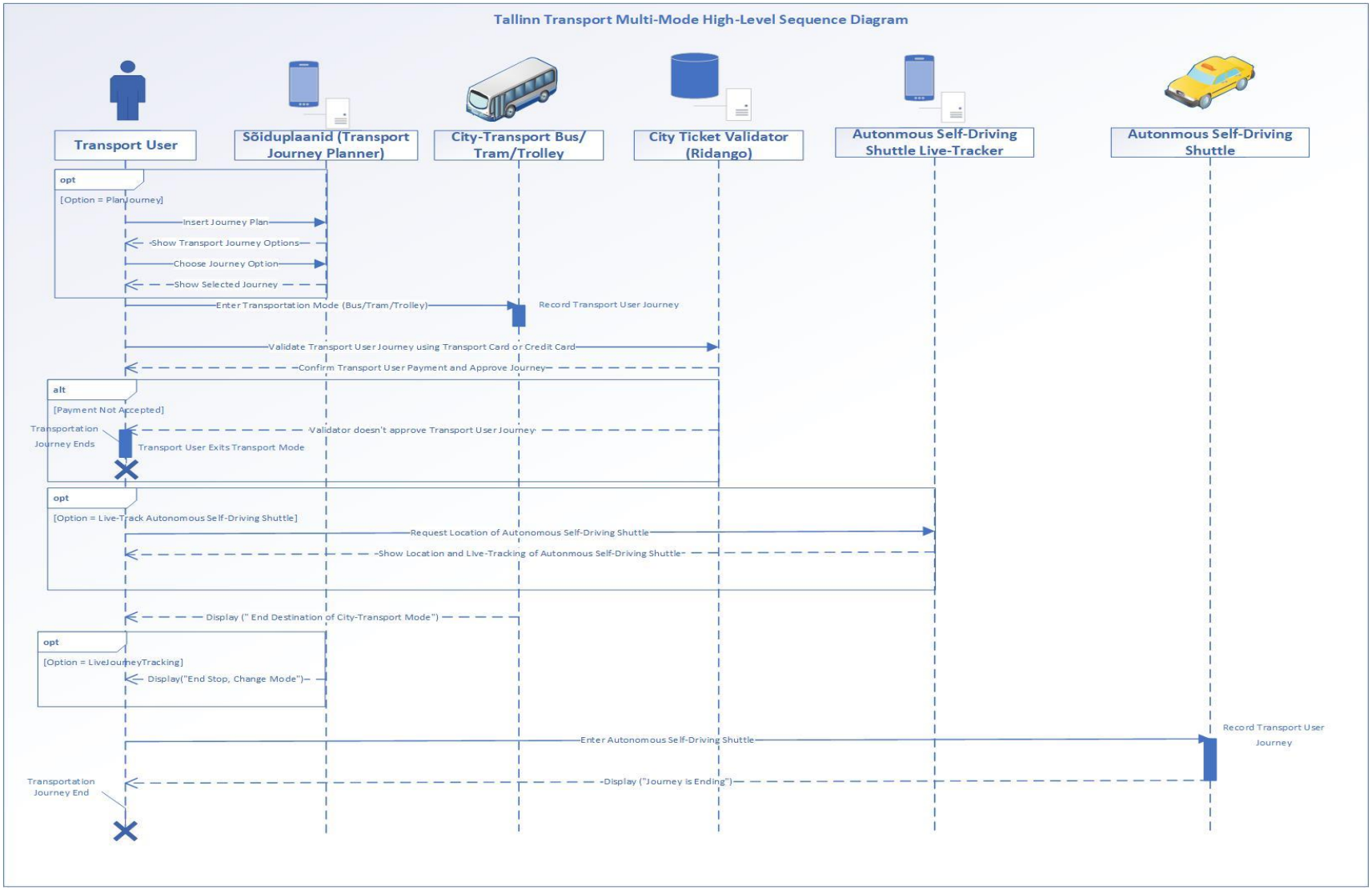

Figure 15: Tallinn Transport Multi-Mode High-Level Sequence Diagram

3.1.5 Mobility-as-a-Service Micro Scenario Definition

The micro scenarios presented constitute the elements of the MaaS macro scenario:

- Journey Planning
- Ticket Validation
- Real-Time Information
- Last-Mile Extension Transitioning

3.1.5.1 MaaS-1.1 - Journey Planning

In this scenario, a very typical situation is considered to be the following: a passenger wants to plan their transportation journey. The passenger could be at home, on the street, or directly at the desired bus stop. The passenger can only use the Tallinn mobile application on mobile device or computer (desktop/laptop).

The desired behaviour is as below:

1. The passenger opens the Tallinn mobile application.
2. The passenger can view more information about the transport routes on the Timetables tab.
3. The passenger can find their desired journey and then go to the journey planner tab and input:
    a. Desired start and end journey location.
    b. Time of travel (Date/Time)
4. The web interface displays a list of transport journey options to the passenger.
5. The passenger chooses the desired transport journey.
6. The web interface displays the selected journey information and a map of the journey with waypoints of the journey route.

The following table describes the assets involved in the scenario and the scope of each of them. It is noted that assets that are managed, owned, controlled by 3rd parties, where CitySCAPE may have limited, or no access are denoted with the use of a grey colour fill in the corresponding lines of the tables and they are only mentioned for functional completeness.

Name	Type	Managed by / Owned by	Basic Asset breakdown	Interfaces	Role
Servers – Information systems - Backends					
Real-time monitoring system	Hardware, Middleware, Software, Data, Redundancies	Thoreb (3rd Party)	Managed and owned by 3rd party – Out of CitySCAPE use cases scope – Registered for system functional completeness.		Provides schedules of service, holds the planned services and interacts with service schedules.
Journey Planning and Timetable Mobile Application	Software	Tallinn Transport Department/	Application, Log files, configuration data, Keys	Application interfaces – APIs to Web services GUI Integration with Tallinn Transport Data Integration with OPinfo (https://opinfo.tallinn.ee/kaart) File Transfer Services (e.g., FTP)	Allow transport users to plan journeys, track journey, plan timetable times, see departures etc.
Thoreb Real-Time Tracking System					
Thoreb On-Board Computer	Hardware, Middleware, Software	HW owned by operator SW owner is Thoreb. Provided under license	The asset is out of CitySCAPE use cases scope since it is used under license from a 3rd Party, and it can only be investigated as a black box. It is registered for functional completeness.		Interface connection between vehicle and back-end system. CAN connection, internal screens, connected with the counter Manages Thoreb system in vehicle. Collects and stores information on the vehicle. Sends

				information to back-end system. Handles internal and external voice announcements.
Thoreb Internal Driver Display Screen	Hardware, Middleware, Software	HW owned by operator	The asset is out of CitySCAPE use cases scope since it is used under license from a 3rd Party, and it can only be investigated as a black box. It is registered for functional completeness.	Driver interface (GUI) Sends real-time route, stop, and destination information to ticketing system. Driver Display for displaying real-time timetable keeping, vehicle position on a map from Thoreb on-board unit. In-Cooperation with the voice notification, internal screens, external display of the driver display screen.
Thoreb Communication Module	Hardware, Middleware, Software	SW owner is Thoreb. Provided under license	The asset is out of CitySCAPE use cases scope since it is used under license from a 3rd Party, and it can only be investigated as a black box. It is registered for functional completeness.	3G/4G, GPS modem Establishing internet connection.
Thoreb Internal Passenger Display Screen	Hardware, Middleware, Software	HW owned by operator	The asset is out of CitySCAPE use cases scope since it is used under license from a 3rd Party, and it can only be investigated as a black box. It is registered for functional completeness.	Controlled by on-board computer. Next stops real-time information, real time information about

				departures from next stops transport zone and media playlists (video/picture) for passengers.
Thoreb External Display Screens (LED)				
Switch	Hardware, Middleware	HW owned by operator SW owner is Thoreb. Provided under license	The asset is out of CitySCAPE use cases scope since it is used under license from a 3rd Party, and it can only be investigated as a black box. It is registered for functional completeness.	Network Hub
Video surveillance system	Hardware, Middleware, Software	HW owned by operator SW owner is Thoreb. Provided under license.\	The asset is out of CitySCAPE use cases scope since it is used under license from a 3rd Party, and it can only be investigated as a black box. It is registered for functional completeness.	Normal vehicle 8 cameras, Articulated vehicle 11 cameras, Mobile DVR.
Radio modem	Hardware, Middleware	HW owned by operator SW owner is Thoreb. Provided under license.	The asset is out of CitySCAPE use cases scope since it is used under license from a 3rd Party, and it can only be investigated as a black box. It is registered for functional completeness.	Traffic light priority.

Table 3: Journey Planning - assets involved in the scenario

The following figure shows how the main actors and assets of the scenarios are linked.

Figure 16: Tallinn MaaS Journey Planning Scenario

3.1.5.2 MaaS 1.2 - Ticket Validation

In this scenario, a passenger wants to validate their transportation journey. The passenger will be on-board the transportation mode. The passenger has multiple methods of validating their user journey:

1. The passenger taps their Tallinn Transport smart card on the Validator.

The desired behaviour of the system is as below:

1. The payment validator checks the passenger data against a database. If the smart card, ticket, or credit card are fraudulent/expired/not valid, the validation will be rejected. If the validation is genuine, then a sound from the validator will acknowledge the successful validation.

The following table describes the assets involved in the scenario and the scope of each of them:

Name	Type	Managed by / Owned by	Basic Asset breakdown	Interfaces	Role
Payment service system	Hardware, Middleware, Software, Data, Redundancies	TalTech	Physical or virtual computing units, Operating System, Application Server, Web services, Databases and DBMS, Log files, configuration data	Network interfaces (Ethernet, Wifi, 4G, Bluetooth) OS interfaces (SSH, Telnet, RDP, etc.) Docker Flask Web Server Application interfaces (APIs, REST, etc.) Database connectors File Transfer Services (e.g., SFTP) NFC interface/RFID interface	System that manages ticketing service, holds the information on the active subscriptions, allows new registrations and manages payments.
Ridango Payment System					
HMI Machine Validator	Hardware, Middleware, Software	TalTech	Hardware (network interfaces, sensors, credit card, micro-computer, touch display), Firmware, OS, Log and configuration files	Network interfaces - RFID, Ethernet, NFC, QR Code, Credit Card, User Interface	Selling/Ticket Validator.
Gateway	Hardware, Middleware, Software	TalTech	Physical computing units, Operating System, APIs, Application Server, Software	Standard computer hw interfaces Network interfaces (Ethernet) OS interfaces (SSH, Telnet, RDP, etc.)	Gateway between ticketing system and the acquiring bank.

		components, Local data assets (databases), Log files, configuration data	Application interfaces (APIs, REST, JSON etc.) Web services Database connectors Interfaces for ISO8583 (financial transactions)	
Communication Module	Hardware, Middleware	TalTech Modem, Firmware, Log and configuration files	CAN bus, 3G/4G	Used for communication of the Payment services with internal network and external network.

Table 4: Ticket Validation - assets involved in the scenario

The following figure shows how the main actors and assets of the scenarios are linked together:

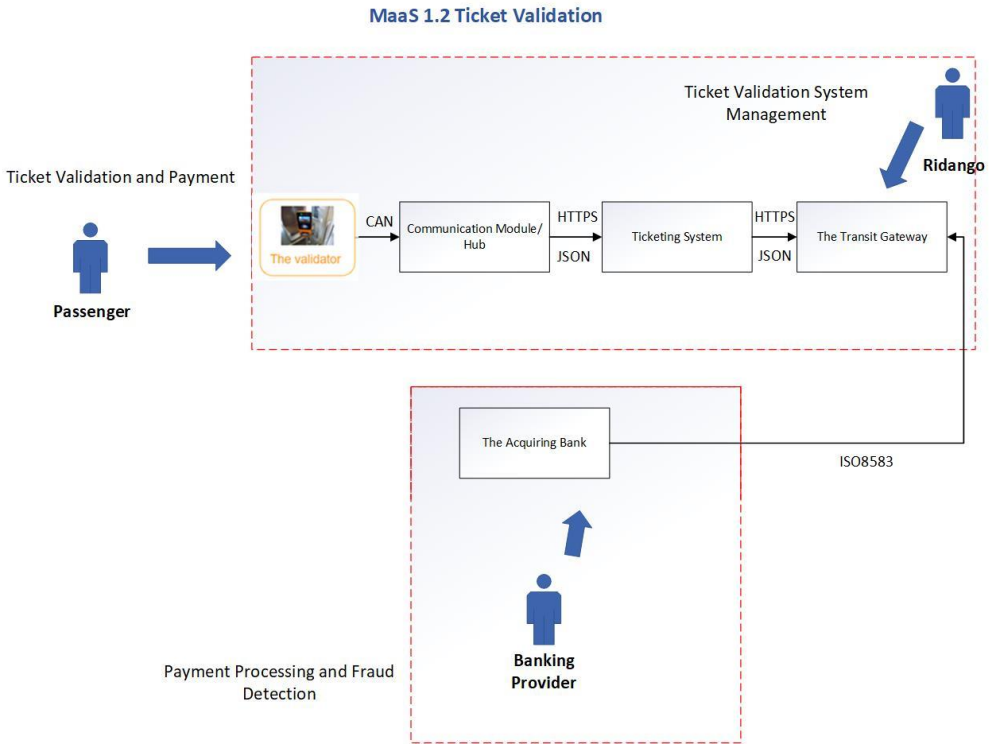

Figure 17: MaaS 1.2 Ticket Validation

3.1.5.3 MaaS 1.3 – Real-Time Information

In this scenario, the real-time information of the multimodal transportation helps the passenger guide their transportation journey. From the passenger perspective, real-time information assists their journey in the following way:

1. The passenger can view the current progress of the city transport on the Tallinn Transport journey planner web interface.
2. The passenger can view the journey information on the internal and external displays of the city transportation modes.
3. The passenger can view the location of the AV shuttle via the web interface.
4. The passengers can view the progress of their journey on the AV Shuttle.

The desired behaviour of the system is below:
The Tallinn Transport journey planner displays the accurate location of the city transportation modes.

1. The timetable information on the internal and external displays are accurate and help inform the passenger of their journey.

2. The information on the location and real-time positioning of the last-mile services is available to the passenger and the passenger can see when and where they can use the last-mile services.
3. The web interface of the last-mile services can display the progress of the passenger journey.

The following table describes the assets involved in the scenario and the scope of each of them:

Name	Type	Managed by / Owned by	Basic Asset breakdown	Interfaces	Role
Mobile Network (4G/5G/)	Network	TalTech	4G and 5G Router	Via network (DSRC, UDP, TLS1.3) to anyone having a valid subscription to the network (Access via 2F Authentication using FIDO tokens and VPN)	Communication between Remote Operations Center and AV Shuttle.
Adhoc vehicular network	Network	Taltech	-	Via ITS messages to anyone part of the ITS-V2X network OBU (CohDA Mk5) RSU (CohDA MKx) CAMS Messages (CohDA proprietary protocol (SPAT), ITS-G5 Application Compliant)	Direct adhoc communication between vehicles and roadside units.
			Servers – Information systems - Backends		
Real-time monitoring system	Hardware, Middleware, Software, Data, Redundancies	Thoreb (3rd Party)	Managed and owned by 3rd party – Out of CitySCAPE use cases scope – Registered for system functional completeness.		Provides schedules of service, holds the planned services and interacts with service schedules.
Journey Planning and Timetable Mobile Application	Software	Tallinn Transport Department/	Application, Log files, configuration data, Keys	Application interfaces – APIs to Web services GUI Integrations with Tallin Transport Data Integration with OPinfo (https://opinfo.tallinn.ee/kaart)	Allow transport users to plan journeys, track journey, plan timetable times, see departures etc.

			File Transfer Services (e.g., FTP)	
Thoreb Real-Time Tracking System				
Thoreb On-Board Computer	Hardware, Middleware, Software	HW owned by operator SW owner is Thoreb. Provided under license	The asset is out of CitySCAPE use cases scope since it is used under license from a 3rd Party, and it can only be investigated as a black box. It is registered for functional completeness.	Interface connection between vehicle and back-end system. CAN connection, internal screens, connected with the counter Manages Thoreb system in vehicle. Collects and stores information on the vehicle. Sends information to back-end system. Handles internal and external voice announcements.
Thoreb Internal Driver Display Screen	Hardware, Middleware, Software	HW owned by operator	The asset is out of CitySCAPE use cases scope since it is used under license from a 3rd Party, and it can only be investigated as a black box. It is registered for functional completeness.	Driver interface (GUI) Sends real-time route, stop, and destination information to ticketing system. Driver Display for displaying real-time timetable keeping, vehicle position on a map from Thoreb on-board unit.

				In-Cooperation with the voice notification, internal screens, external display of the driver display screen.
Thoreb Communication Module	Hardware, Middleware, Software	SW owner is Thoreb. Provided under license	The asset is out of CitySCAPE use cases scope since it is used under license from a 3rd Party, and it can only be investigated as a black box. It is registered for functional completeness.	3G/4G, GPS modem Establishing internet connection.
Thoreb Internal Passenger Display Screen	Hardware, Middleware, Software	HW owned by operator	The asset is out of CitySCAPE use cases scope since it is used under license from a 3rd Party, and it can only be investigated as a black box. It is registered for functional completeness.	Controlled by on-board computer. Next stops real-time information, real time information about departures from next stops transport zone and media playlists (video/picture) for passengers.
Thoreb External Display Screens (LED)				
Switch	Hardware, Middleware	HW owned by operator SW owner is Thoreb. Provided under license	The asset is out of CitySCAPE use cases scope since it is used under license from a 3rd Party, and it can only be investigated as a black box. It is registered for functional completeness.	Network Hub

Video surveillance system	Hardware, Middleware, Software	HW owned by operator SW owner is Thoreb. Provided under license	The asset is out of CitySCAPE use cases scope since it is used under license from a 3rd Party, and it can only be investigated as a black box. It is registered for functional completeness.		Normal vehicle 8 cameras, Articulated vehicle 11 cameras, Mobile DVR.
Radio modem	Hardware, Middleware	HW owned by operator SW owner is Thoreb. Provided under license	The asset is out of CitySCAPE use cases scope since it is used under license from a 3rd Party, and it can only be investigated as a black box. It is registered for functional completeness.		Traffic light priority.
Autonomous Self-Driving Shuttle					
Vehicle on-board Computer	Hardware	Taltech	Physical computing units, Operating System, APIs, Application Server, Software components, Local data assets (databases), Log files, configuration data	Network interfaces (Ethernet, CAN, Serial) OS (Ubuntu 16.01) Applications (ROS, Autoware.Auto, Skyhook)	The vehicle computer.
Camera Sensors	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP Connected to On-board Unit.	The vehicle on-board cameras.

Camera Data	Data asset	Taltech	Physical Unit, Log files, configuration data	Camera data is stored in the ROSBag logging system.	The video files from on-board camera.
GNSS	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected GNSS sensor using Skyhook GPS application.	The vehicle GNSS system. Used for geo-location/ SLAM.
IMU	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	CAN bus interface, integrated with GPS	Vehicle IMU for capturing of measurement data of AV (acceleration, orientation, heading).
Ultrasonic Sensors	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected to on-board L2 switch.	Used for short-range object detection.
Lidar	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected to on-board L2 switch.	LiDAR used for 3D point cloud mapping to build dynamic maps for SLAM.
Local Dynamic Map	Data asset	Taltech	configuration data	Application interfaces (APIs, REST, JSON etc.) Web services Database connectors	The vehicle complete database.
Communication modem	Hardware, Firmware, Software	Taltech	4G and 5G Router	Network interface (Ethernet, CAN) V2X 4G M2 Nighthawk Router 5G Router	The modem ensuring communication with other vehicles and infrastructure.
Switch	Hardware, Firmware, Software	Taltech	L2 Switch	Ethernet (Cat 6, 5E) L2 (VLAN segmentation)	Switch connects on-board unit, sensors and router. Manages access to the network and segments network in VLANs).

AV Shuttle Operating System	Middleware /Firmware OS	Taltech	-	OS interfaces (Proprietary port enabled, protected by access and authentication mechanisms)	ROS Melodic, Autoware 1.14
Self-driving application	Software	Taltech		Application interfaces (APIs, REST, JSON etc.) Messaging protocols Web services Database connectors	Autoware.ai Application framework for self-driving vehicles.
Teleoperation services	Hardware, Middleware, Software, Data, Redundancies	Teleoperation services provider	Physical or virtual computing units, Operating System, Application Server, Web services, Databases and DBMS, Log files, configuration data	Network interfaces (Ethernet, Wi-Fi, 4G, Bluetooth) OS interfaces (SSH, RDP, etc.) Application interfaces (APIs, REST, etc.) Database connectors File Transfer Services (e.g., SFTP)	Control PC communicating using the teleoperation software which is a module of the ROS.
Teleoperation Module	Software	Taltech	API	OS interfaces (SSH) – Access and Authentication using FIDO 2FA, TLSv1.3 and VPN	Module implemented in the ROS implementation.
CohDA OBU	Hardware, Firmware, Software	TalTech	Hardware – Network ports, Firmware/Router OS, web application	CAMS (SPAT, MAP) CohDA proprietary protocol (ITS-G5)	On-board unit for communication with CohDA MKx smart RSU.
AV Shuttle Journey Planning	Application, Log files, configurati	Application interfaces – APIs to	Application, Log files, configuration data, Keys	Application interfaces – APIs to Web services GUI	Uses the GNSS location data to present a web interface to track the AV shuttle.

Web Interface	on data, Keys	Web services GUI Integrations with sensor/telematics data		
HSM	Hardware, Firmware, Software	Taltech	Network interface (Ethernet) Physical access (USB, Serial) HSM interfaces (STM32)	Hardware security module for the certificates of the V2X/ITS PKI. HSMs are contained in the embedded STM controllers in the Autonomous Vehicle and embedded IoT devices such as OBU, RSU.
Actuators	Hardware, Firmware, Software	Taltech	Network interface (Ethernet, CAN)	Actuators

Table 5: Real Time Information - assets involved in the scenario

The following figure shows how the main actors and assets of the scenarios are linked together:

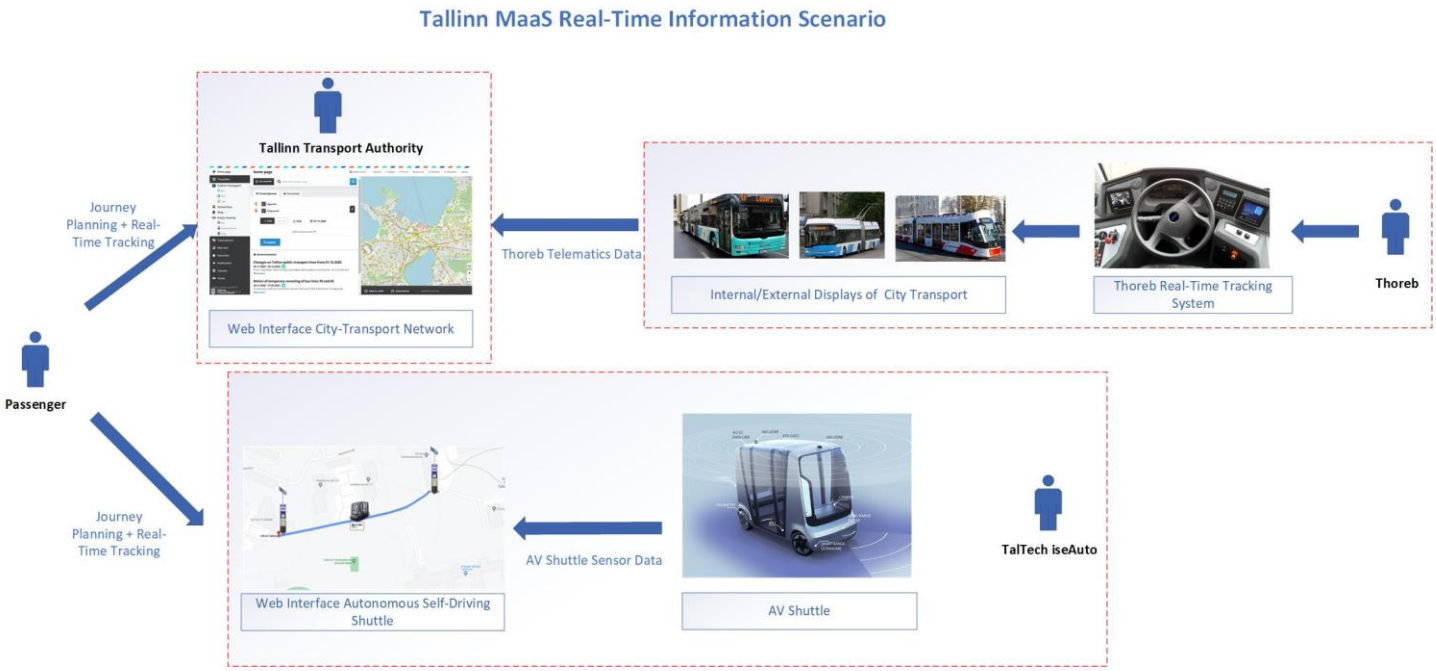

Figure 18: Tallinn MaaS Real-Time Information Scenario

3.1.5.4 MaaS 1.4 – Last-Mile Extension Transitioning

In this scenario the passenger is able to move between the city transportation mode onto the last-mile services (AV Shuttle, e-scooter) seamlessly. The passenger interactions to achieve this are below:

1. Passenger departs from the city-transport mode and is met by the AV Shuttle.
2. The AV Shuttle drives the passenger to the end destination.

The desired behaviour of the system is below:

1. The remote operations center of the AV Shuttle monitors the operation of the AV Shuttle.
2. The remote operations center monitors the passenger in the AV Shuttle.
3. If there are any safety events, the emergency stop can be used to stop the AV Shuttle, or the remote operator can make driving decisions.

The following table describes the assets involved in the scenario and the scope of each of them:

Name	Type	Managed by / Owned by	Basic Asset breakdown	Interfaces	Role
Mobile Network (4G/5G/)	Network	TalTech	4G and 5G Router	Via network (DSRC, UDP, TLS1.3) to anyone having a valid subscription to the network (Access via 2F Authentication using FIDO tokens and VPN)	Communication between Remote Operations Center and AV Shuttle.
Adhoc vehicular network	Network	Taltech	-	Via ITS messages to anyone part of the ITS-V2X network OBU (CohDA Mk5) RSU (CohDA MKx) CAMS Messages (CohDA proprietary protocol (MAP, SPAT etc.), ITS-G5 Application Compliant)	Direct adhoc communication between vehicles and roadside units.
Autonomous Self-Driving Shuttle					
Vehicle on-board Computer	Hardware	Taltech	Physical computing units, Operating System, APIs, Application Server, Software components, Local data assets (databases), Log files, configuration data	Network interfaces (Ethernet, CAN, Serial) OS (Ubuntu 16.01) Middleware (ROS Kinetic Kame) Applications (Autoware.Auto, Skyhook)	The vehicle computer.
Camera Sensors	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP Connected to On-board Unit.	The vehicle on-board cameras.

Camera Data	Data asset	Taltech	Physical Unit, Log files, configuration data	Camera data is stored in the ROSBag logging system.	The video files from on-board camera.
GNSS	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected GNSS sensor using Skyhook GPS application.	The vehicle GNSS system. Used for geo-location/ SLAM.
IMU	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	CAN bus interface, integrated with GPS	Vehicle IMU for capturing of measurement data of AV (acceleration, orientation, heading).
Ultrasonic Sensors	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected to on-board L2 switch.	Used for short-range object detection.
Lidar	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected to on-board L2 switch.	LiDAR used for 3D point cloud mapping to build dynamic maps for SLAM.
Local Dynamic Map	Data asset	Taltech	configuration data	Application interfaces (APIs, REST, JSON etc.) Web services Database connectors	The vehicle complete database.
Communication modem	Hardware, Firmware, Software	Taltech	4G and 5G Router	Network interface (Ethernet, CAN) V2X 4G M2 Nighthawk Router 5G Router	The modem ensuring communication with other vehicles and infrastructure.
Switch	Hardware, Firmware, Software	Taltech	L2 Switch	Ethernet (Cat 6, 5E) L2 (VLAN segmentation)	Switch connects on-board unit and sensors and router. Manages access to the network and segments network in VLANs).

AV Shuttle Operating System	Middleware /Firmware OS	Taltech	-	OS interfaces (Proprietary port enabled, protected by access and authentication mechanisms)	ROS Melodic, Autoware 1.14
Self-driving application	Software	Taltech		Application interfaces (APIs, REST, JSON etc.) Messaging protocols Web services Database connectors	Autoware.ai Application framework for self-driving vehicles.
Teleoperation services	Hardware, Middleware, Software, Data, Redundancies	Teleoperation Services Provider	Physical or virtual computing units, Operating System, Application Server, Web services, Databases and DBMS, Log files, configuration data	Network interfaces (Ethernet, Wi-Fi, 4G, Bluetooth) OS interfaces (SSH, RDP, etc.) Application interfaces (APIs, REST, etc.) Database connectors File Transfer Services (e.g., SFTP)	Control PC communicating using the teleoperation software which is a module of the ROS.
Teleoperation Module	Software	Taltech	API	OS interfaces (SSH) – Access and Authentication using FIDO 2FA, TLSv1.3 and VPN	Module implemented in the ROS implementation.
CohDA OBU	Hardware, Firmware, Software	TalTech	Hardware – Network ports, Firmware/Router OS, web application	CAMS (SPAT, MAP) CohDA proprietary protocol (ITS-G5)	On-board unit for communication with CohDA MKx smart RSU.
AV Shuttle Journey Planning	Application, Log files, configurati	Application interfaces – APIs to	Application, Log files, configuration data, Keys	Application interfaces – APIs to Web services GUI	Uses the GNSS location data to present a web interface to track the AV shuttle.

Web Interface	on data, Keys	Web services GUI Integrations with sensor/telematics data			
HSM	Hardware, Firmware, Software	Taltech		Network interface (Ethernet) Physical access (USB, Serial) HSM interfaces (STM32)	Hardware security module for the certificates of the V2X/ITS PKI. HSMs are contained in the embedded STM controllers in the Autonomous Vehicle and embedded IoT devices such as OBU, RSU.
Actuators	Hardware, Firmware, Software	Taltech		Network interface (Ethernet, CAN)	Actuators
Smart City Campus Infrastructure					
Smart RSU	Hardware Firmware, Software	TalTech	Hardware – Network ports, Firmware/Router OS, web application	CohDA proprietary protocol (ITS-G5)	Illuminated road side unit which contains the CohDA OBU.
Smart RSU Relay	Hardware	TalTech	Network-Arduino	CohDA proprietary protocol (ITS-G5)	Arduino relay device for traffic light.
Traffic Management Server	Hardware, Software	TalTech	Hardware – Network Ports, Physical Disk etc.	Intelligent Traffic Management Software.	Traffic management node for communication with RSUs.

	Software – Application, OS, firmware

Table 6: Last Mile Extension Transitioning - assets involved in the scenario

3.2 Adaptive Traffic Control Use Case

Adaptive traffic control is a concept of traffic management through automated, intelligent decision-making enabled through communication with an internet-connected roadside unit (RSU), vehicle on-board unit (OBUs) and traffic management control node. The vehicle communicates its telemetry (speed, steering angle, brake status, etc.), location and transit information (travel path intention, etc.) through messages from its on-board unit (OBU) to the RSU. The RSU then queries the traffic management node (remote server) and traffic control decisions are made. The connectivity from the vehicle is referred to as V2X communication.

3.2.1 Users and Stakeholders

Users and stakeholders identified in the Tallinn Transport network for the adaptive traffic control use case are depicted in figure 23. These users and stakeholders differ from the MaaS use-case as the focus is on the AV shuttle and the traffic environment is located in the TalTech smart campus.

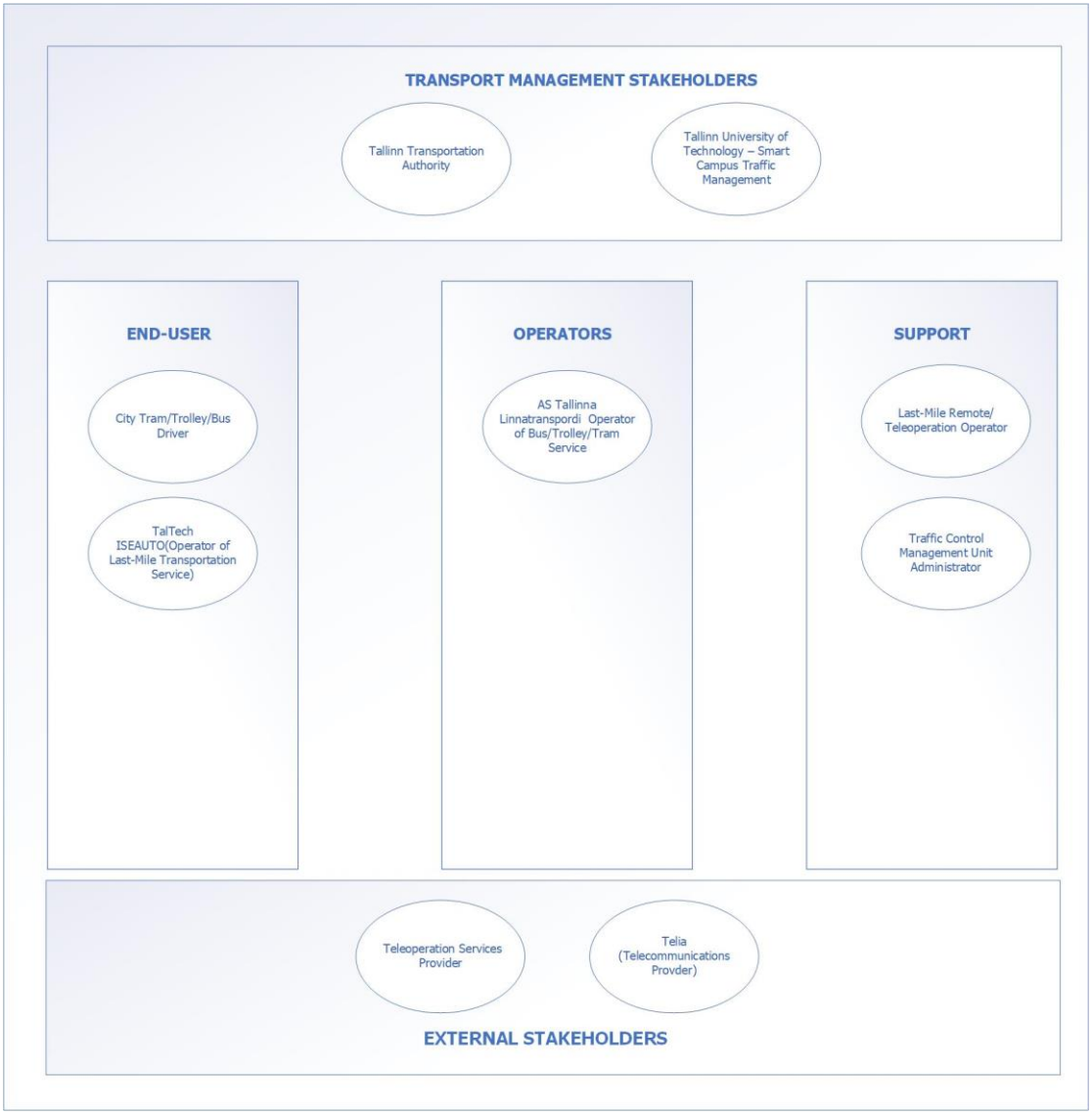

Figure 19: Tallinn Transport Management Stakeholders

Detailed Description of User and Stakeholders in Tallinn City Multi-Modal Transport Network
Actor: Bus/Tram/Trolley Driver **Role:** User **Description:** Responsible for driving the city-transportation modes.
Actor: TalTech ISEAUTO (Operator of Last-Mile Transportation Services) **Role:** User **Description:** The TalTech ISEAUTO is an autonomous self-driving public transportation shuttle. It is designed and operated by the TalTech ISEAUTO team. Their responsibilities include system engineering, modifications/upgrades to the shuttle as well as operation of the shuttle using the teleoperation station, normally located at TalTech campus, however, able to be located wherever.
Actor: AS Talllinna Linnatransport AS (Operator of Bus/Trolley/Tram Services) **Role:** Stakeholder **Description:** TLT are the operators of the Bus, Trolley, Tram services in Tallinn, Estonia.
Actor: Last-Mile/Remote Teleoperation Operator **Role:** Stakeholder **Description:** The Last-Mile/Remote Teleoperation Operator is responsible for actively monitoring the journey of the autonomous self-driving public transport shuttle and taking driving actions if required. The operator is located in the teleoperation station at TalTech campus. The operator is a licenced driver, according to the Estonian Traffic Act.
Actor: Traffic Control Management Unit Administrator **Role:** Stakeholder **Description:** The Traffic Control Management Unit Administrator is responsible for the administration of the Tallinn City traffic system. This involves activities such as monitoring traffic flows and programming and re-programming traffic lights.

Actor: Tallinn Transport Authority **Role:** Stakeholder **Description:** Authority responsible for Tallinn City-Transportation.
Actor: Tallinn University of Technology Smart Campus Traffic Management **Role:** Stakeholder **Description:** The Tallinn University of Technology Smart Campus Traffic Management is responsible for the administration of the smart campus private roads. This includes the last-mile extension from Keemia bus stop to the Mektory. The TalTech campus has interactive pedestrian crossings and will be responsible, in the pilot, for the adaptive traffic control.
Actor: Teleoperation Service Provider **Role:** Stakeholder **Description:** The Teleoperation Service Provider is a 3rd party provider of the teleoperation system for remote control of the autonomous self-driving shuttle. The software is a module on the ROS middleware used by the autonomous vehicle shuttle.
Actor: Telia **Role:** Stakeholder **Description:** Telia provides telecommunication services (4G/5G) for the iseAuto AV Shuttle and the smart campus traffic environment.

Table 7: User and Stakeholders in Tallinn City Multi-Modal Transport Network

The following picture shows how the main actors and assets of the scenarios are linked together:

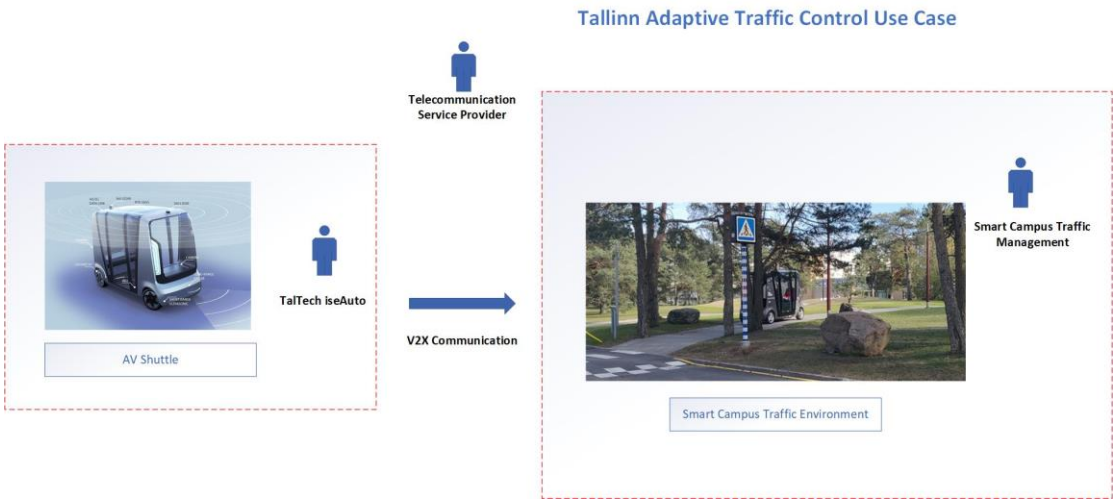

Figure 20:Tallinn adaptive Traffic Control Use Case

3.2.2 Adaptive Traffic Control Macro Use-Case

The desired scenario for the Tallinn Adaptive Traffic Control use-case is as follows:

1. A city bus/trolley and autonomous vehicle shuttle travel through the smart campus roadway of the TalTech Mektory.
2. The Autonomous vehicle shuttle reaches an intersection.
3. The Autonomous vehicle shuttle communicates with the smart city traffic management road sign unit.
4. The traffic management node then receives communication from the RSU and a traffic control decision is made. This is communicated back from the RSU and then from the RSU to the AV Shuttle.
5. The TalTech Smart Campus Traffic Management monitors the traffic environment and the teleoperation operator monitors the safety of passengers in the AV shuttle.

3.2.3 Macro Scenario: Description of typical-desired system/platform operation from the system-of-systems perspective

3.2.3.1 Cohda Wireless MKx V2X Devices

Cohda Wireless MKx devices consist of two units. The CohDa Mk5 OBU (On-Board Unit) and the CohDa mk6 RSU (Road Side Unit). The OBU should be reading the Autonomous Vehicle status and sharing it with the RSU. The RSU device is mostly responsible for broadcasting road-specific messages and alerts such as Basic Safety Messages, Red Light Warning, etc.

These devices are set to trans-receive messages based on the European and North American communication standards for V2X communication.

3.2.3.2 Traffic Management Node

The traffic management node is a server that functions to receive messages from RSUs and make intelligent traffic decisions.

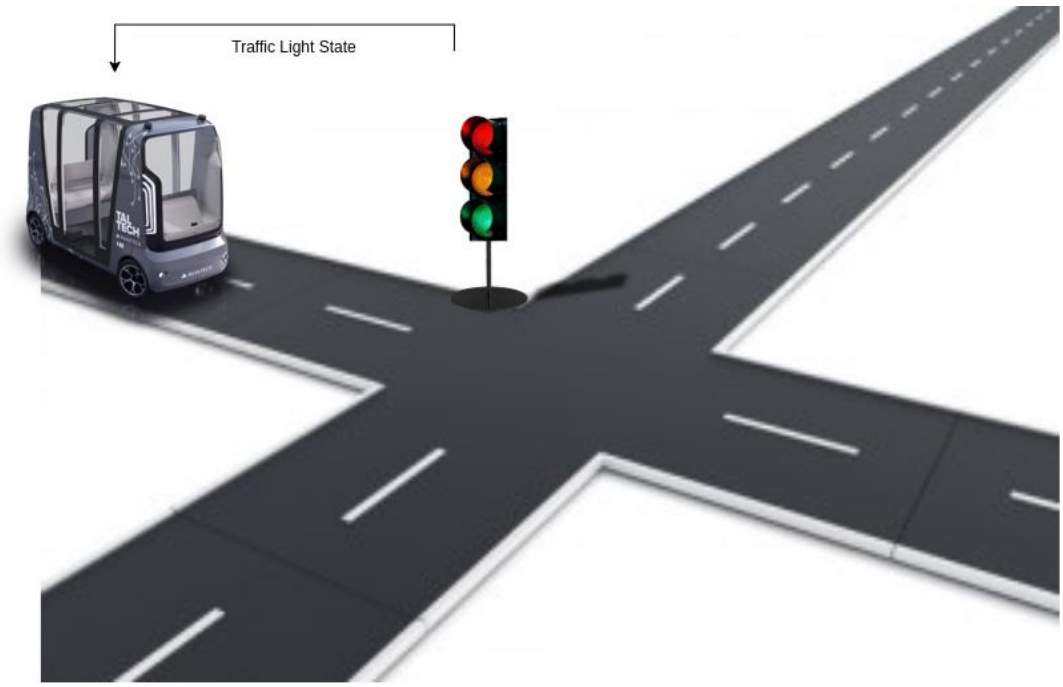

Figure 21: Traffic light integration with iseAuto

3.2.3.3 Connecting the MKx Devices

MKx devices, in this case, are set as gateways. This means that an onboard computer interacts exclusively with the OBU in the Autonomous Vehicle. The OBU then creates message packets and communicates these packets to the RSU, acting like a gateway. Similarly, the RSU is connected to a roadside controller. This controller then sends relevant information to the RSU only and RSU then broadcasts that information through WAVE (Wireless Access in Vehicular Environments) to the vehicles.

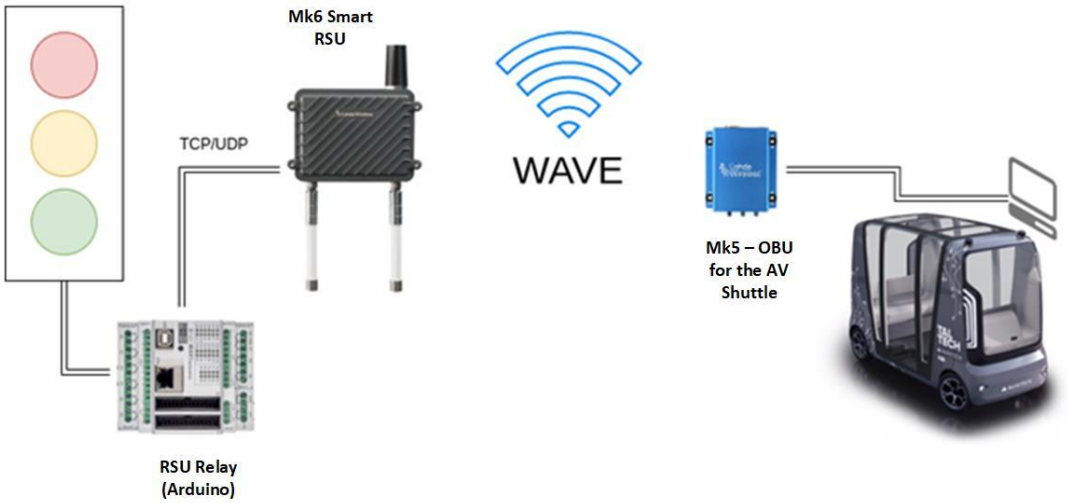

Figure 22: Connecting the MKx Devices

3.2.4 Micro Scenario Use Case Definition

3.2.4.1 AT1.1 – Intersection Pass-through

In this scenario, the AV Shuttle moves through the intersection of the smart campus traffic environment. As the passenger is driven by the AV Shuttle, only system behaviour is relevant. The desired behaviour of the system is as follows:

1. The OBU in the AV Shuttle sends a message using the DSRC communication (802.11p) containing control information as to the desired transit - proceed through the intersection.
2. The RSU receives the message and sends a communication to the traffic management node.
3. The traffic management node decides to allow the AV Shuttle passage through the intersection. That decision is communicated to the RSU.
4. The RSU communicates the traffic decision to the OBU on-board the AV Shuttle.
5. The AV Shuttle transits through the intersection.

3.2.4.2 AT1.2 – Intersection Stop

In this scenario, the AV shuttle moves through the intersection of the smart campus traffic and encounters other transportation modes transiting. The desired system behaviour is as follows:

1. The OBU in the AV Shuttle sends a message using the DSRC communication (802.11p) containing control information as to the desired transit.
2. The RSU receives the message and sends a communication to the traffic management node.

3. The traffic management node decides not to allow the AV Shuttle passage through the intersection as a passenger is walking across the pedestrian crossway. That decision is communicated to the RSU.
4. The RSU communicates the traffic decision to the OBU on-board the AV Shuttle.
5. The AV Shuttle transits through the intersection.

The following table describes the assets involved in both scenarios (AT1.1 and AT1.2) and the scope of each of them:

Name	Type	Managed by / Owned by	Basic Asset breakdown	Interfaces	Role
Mobile Network (4G/5G/)	Network	TalTech	4G and 5G Router	Via network (DSRC, UDP, TLS1.3) to anyone having a valid subscription to the network (Access via 2F Authentication using FIDO tokens and VPN).	Communication between Remote Operations Center and AV Shuttle.
Adhoc vehicular network	Network	Taltech	-	Via ITS messages to anyone part of the ITS-V2X network OBU (CohDA Mk5) RSU (CohDA MKx) CAMS Messages (CohDA proprietary protocol (MAP, SPAT, etc.), ITS-G5 Application Compliant).	Direct adhoc communication between vehicles and roadside units.
Autonomous Self-Driving Shuttle					
Vehicle on-board Computer	Hardware	Taltech	Physical computing units, Operating System, APIs, Application Server, Software components, Local data assets (databases), Log files, configuration data	Network interfaces (Ethernet, CAN, Serial) OS (Ubuntu 16.01) Applications (ROS, Autoware.Auto, Skyhook)	The vehicle computer.
Camera Sensors	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP Connected to On-board Unit.	The vehicle on-board cameras.

Camera Data	Data asset	Taltech	Physical Unit, Log files, configuration data	Camera data is part of ROSbag logging system.	The video files from on-board camera.
GNSS	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected GNSS sensor using Skyhook GPS application.	The vehicle GNSS system. Used for geo-location/ SLAM.
IMU	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	CAN bus interface, integrated with GPS.	Vehicle IMU for capturing of measurement data of AV (acceleration, orientation, heading).
Ultrasonic Sensors	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected to on-board L2 switch.	Used for short-range object detection.
Lidar	Hardware, Firmware	Taltech	Physical Unit, Log files, configuration data	IP connected to on-board L2 switch.	LiDAR used for 3D point cloud mapping to build dynamic maps for SLAM.
Local Dynamic Map	Data asset	Taltech	configuration data	Application interfaces (APIs, REST, JSON etc.) Web services Database connectors	The vehicle complete database.
Communication modem	Hardware, Firmware, Software	Taltech	4G and 5G Router	Network interface (Ethernet, CAN) V2X 4G M2 Nighthawk Router 5G Router	The modem ensuring communication with other vehicles and infrastructure.
Switch	Hardware, Firmware, Software	Taltech	L2 Switch	Ethernet (Cat 6, 5E) L2 (VLAN segmentation)	Switch connects on-board unit and sensors and router. Manages access to the network

					and segments network in VLANs).
AV Shuttle Operating System	Middleware /Firmware OS	Taltech	-	OS interfaces (Proprietary port enabled, protected by access and authentication mechanisms)	ROS Melodic, Autoware 1.14
Self-driving application	Software	Taltech		Application interfaces (APIs, REST, JSON etc.) Messaging protocols Web services Database connectors	Autoware.ai Application framework for self-driving vehicles.
Teleoperation services	Hardware, Middleware, Software, Data, Redundancies	Teleoperation Services Provider	Physical or virtual computing units, Operating System, Application Server, Web services, Databases and DBMS, Log files, configuration data	Network interfaces (Ethernet, Wi-Fi, 4G, Bluetooth) OS interfaces (SSH, RDP, etc.) Application interfaces (APIs, REST, etc.) Database connectors File Transfer Services (e.g., SFTP)	Control PC communicating using the teleoperation software which is a module of the ROS.
Teleoperation Module	Software	Taltech	API	OS interfaces (SSH) – Access and Authentication using FIDO 2FA, TLSv1.3 and VPN	Module implemented in the ROS implementation.
AV OBU	Hardware, Firmware, Software	TalTech	Hardware – Network ports, Firmware/Router OS, web application	CAMS (SPAT, MAP) CohDA proprietary protocol (ITS-G5)	On-board unit for communication with CohDA MKx smart RSU.

AV Shuttle Journey Planning Web Interface	Application, Log files, configuration data, Keys	Application interfaces – APIs to Web services GUI Integrations with sensor/telematics data	Application, Log files, configuration data, Keys	Application interfaces – APIs to Web services GUI	Uses the GNSS location data to present a web interface to track the AV shuttle .
HSM	Hardware, Firmware, Software	Taltech		Network interface (Ethernet) Physical access (USB, Serial) HSM interfaces (STM32)	Hardware security module for the certificates of the V2X/ITS PKI. HSMs are contained in the embedded STM controllers in the Autonomous Vehicle and embedded IoT devices such as OBU, RSU.
Actuators	Hardware, Firmware, Software	Taltech		Network interface (Ethernet, CAN)	Actuators
Smart City Campus Infrastructure					
Smart RSU	Hardware Firmware, Software	TalTech	Hardware – Network ports,	CohDA proprietary protocol (ITS-G5)	Illuminated road side unit which contains the CohDA OBU.

			Firmware/Router OS, web application		
Smart RSU Relay	Hardware	TalTech	Network-Arduino	CohDA proprietary protocol (ITS-G5)	Arduino relay device for traffic light.
Traffic Management Server	Hardware, Software	TalTech	Hardware – Network Ports, Physical Disk etc. Software – Application, OS, firmware	Intelligent Traffic Management Software.	Traffic management node for communication with RSUs.

Table 8: Intersection stop - assets involved in the scenario

3.3 Tallinn Use-Case Cyber Threat Scenarios

The following use cases are indicative as seen from a business point of view and focus on multimodal transportation that integrates the traditional city-transportation network with the autonomous vehicle shuttles. For a seamless multimodal journey for the transport user, the integrity of live journey/telematics data, the payment system and the remote control and monitoring of transport platforms and infrastructure are of primary concern. If these systems were exploited by a cyber attacker, they would have a cascading affect across the transportation modes and affect system-of-system operations.

These use cases will be used in forthcoming tasks and activities in order to identify vulnerabilities, threats and attack vectors that in turn will help design the technical use-cases that will be presented in WP3. These technical use-cases will provide the required details in relation to the involved CitySCAPE components and the datasets used to identify and respond to cyber security incidents.

The aim of the presented use-cases is to:

1. Improve confidence of the efficient handling of 0-zay and denial-of-service attacks.
2. Minimise security risks introduced by (less-security aware) external service providers.
3. Improve fraud protection.
4. Minimise risks to personal privacy related to fraud prevention and new ticketing services.

In the following tables, a first approach on risks and attack scenarios that may damage the operation of the CPaaS in the use cases described in the previous sections.
It should be noted that, these scenarios will be subjected to changes and modifications during the next development steps of the project, i.e., through the results of risk modeling and vulnerability-threat analysis, the adopted system architecture, the pilot design and objectives, the types and methods of attack that may be demonstrated, etc.

Attack Scenario Name	***3rd Party Data Manipulation***
Related Use Case	MaaS 1.1 Journey Planning
Brief Description	The 3rd Party data collection relies on generated reports and timetable information. This scenario will investigate manipulation of the 3rd party data and the follow-on effects for public transport.

Involved Actors	1. External Service Provider 2. Transport security administrators 3. A Cyber attacker In an initial approach, the malicious user may be an insider (authorized user) that tampers data through direct access or a remote (unauthorized) attacker that accesses the stored or transmitted data.
Involved and affected Asset(s)	1. Data assets 2. Real-Time Monitoring System 3. Journey Planning and Timetable web interface
Interfaces, Entry and high-level vulnerable points	The attack is performed on 3rd Party Data Storage (Supply Chain) and cascaded to the system. The impact of the attack may maximize due to the lack of data validation methods and blind trust to 3rd parties.

Generic Scenario Description	▪ An internal or external (authorized or unauthorized) cyber actor manipulates the data in the 3rd party data storage system (not controlled by Tallinn Transport Authority). Data tampering may be implemented with a variety of methods (e.g., SQL injection) or, in the case of an insider, through direct data manipulation.
	▪ The attacker's objective is to cause operational chaos at the public transport system.
	▪ The result of the attack is that the Journey planning and real time tracking functionalities supported by the CPaaS provide incorrect information on the city transport timetable and routes.
	▪ The attack affects:
	  ▪ The transport operators and administrators that attempt to manage the transport system.
	  ▪ Passengers that are unable to accurately plan transportation journey.
	▪ The challenge of the attack is that the manipulation originates on a "trusted" source that is not controlled by the transport authority.

Desired Response	The specific type of risks is proactively taken into account and anticipated through risk analysis and impact assessment.

	In case of an incident, the anomalies are captured in a timely fashion (through monitoring, data/logs analysis, etc.), allowing to the administrators to take appropriate remediation actions. In case the security breach at the 3rd party is detected externally, the platform is notified of the event.

Table 9: Tallinn Threat Analysis - 3rd Party Data Manipulation

Attack Scenario Name	***GNSS Spoofing***
Related Use Case	MaaS 1.3 Real-Time Information
Brief Description	An external attacker uses GNSS spoofing equipment to generate false GNSS locations which are received by the city transport mode and/or AV Shuttle.
Involved Actors	1. Bus/Tram/Trolley Driver 2. Teleoperation 3. Transport management authorities 4. Cyber attacker, with the capability to produce fake GNSS data, retransmit/tunnel GNSS data, fake/ground "satellites", or any other technique for GNSS spoofing.
Involved and affected Asset(s)	1. Thoreb Communication Module 2. GNSS Receiver (AV Shuttle) 3. Teleoperation systems, remote control and any other applications that exploit the GNSS information.
Interfaces, Entry and high-level vulnerable points	The attacker may exploit the lack of GNSS signal authentication, lack of GNSS receiver redundancy, or existence of misbehaviour/anomaly detection[1] controls.

[1] Misbehaviour in the V2X context is when a legitimate user (i.e., with valid credentials and lawful access to the service) is transmitting incorrect data intentionally or due to misconfiguration or malfunction. This misbehaviour should be identified through inference, so that it can be reported and trigger specific countermeasures. When using misbehaviour is detected in GNSS data, it concerns falsification of position or speed, which can be a cause of tragic incidents for autonomous driving. Some misbehaving use cases include: overlapping Position (a

Generic Scenario Description	▪ An attacker uses GNSS spoofing equipment to jam/overwhelm the real GNSS signal and fool the receivers on the city transport mode and AV shuttle into accepting the spoofed GNSS data stream. The attacker generates, replicates, replays etc. modified satellite signals and broadcasts it to specific targets. ▪ GNSS spoofing equipment is cheap and provides a low cost of entry for a high-profile attack. GNSS spoofing has already been reported in the Baltic sea region. ▪ GNSS spoofing may affect the operation of various involved systems like journey planning, real-time monitoring of transport systems, traffic management, remote control and autonomous driving in general. ▪ Consequently, it affects the passengers – from the provision of erroneous information on transport mode status to their physical safety (e.g., in autonomous vehicles. ▪ Such an attack may undermine the credibility of the transportation system by impacting the integrity of public transport geo-location services and reducing trust in the use of GNSS data for public transport information.
Desired Response	The risks are modelled and analysed and the operators are aware of consequences, impacts and possible security controls. An incident notification platform is available to assist in classification, management and responses and exchange information for such incidents. In case the GNSS data from a source can be made available to an anomaly detection scheme, GNSS spoofing may be detected in a timely fashion.

vehicle claims to occupy space shared with other vehicles), speed consistency (it is not possible to instantaneously accelerate or break above a threshold), distance move (it is not possible to change location with irrationally high speeds), sybil attacks, frequency of transmitted messages (DoS attack), sudden appearance to a location, etc.). In the CitySCAPE context, this type of anomalies may be detected by the correlation engines, SIEM or IDS – depending on the adopted architecture.

Table 10: Tallinn Threat Scenarios - GNSS Spoofing

Attack Scenario Name	***Data Leakage Smart Card***
Related Use Case	MaaS 1.2 Ticket Validation
Brief Description	HMI Validators are a key element of ticket validation/processing. The validator devices may be attacked and breached by an external attacker. As an indicative example, since the devices have limited memory resources, a side-channel attack against possible lack of memory protection of the HMI validators may cause significant issues.
Involved Actors	1. Ridango (External Service Provider) 2. Banking Provider (External Stakeholder) 3. Cyber attacker – external to the system or malicious insider.
Involved and affected Asset(s)	1. Payment System Service 2. HMI Validator 4. Transit Gateway 5. Communication Gateway
Interfaces, Entry and high-level vulnerable points	The attacker may exploit possible insufficient cryptography of smart cards, or insecure memory protection of smart cards.
Generic Scenario Description	▪ The cyber-attacker launches an attack on the HMI validator (possibly through the smart card). ▪ The attacker's objective is to gain access to the data in the validator's memory/ and or cryptographic keys. ▪ For example, the attacker may monitor the HMI validator and perform a side-channel attack to extract the keys from the memory. ▪ Through these keys, data from the public transport system users are exposed with possibly severe impact (e.g., leakage of personal, banking data, etc.)

Desired Response	The risks are modelled and analysed, and the operators are aware of consequences, impacts and possible security controls. While a security support system may not be able to prevent or detect low-level side-channel attacks, it should assist in incident notification, reporting, management and response. Notification after detection may be feasible through forensics, log analysis, or other means. Assistance to the security administrators for risk management in order to prevent escalation of the side-channel attack to, e.g., identity fraud or financial/banking fraud, etc.

Table 11: Tallinn Threat Scenarios - Data Leakage Smart Card

Attack Scenario Name	***Manipulated Smart Card***
Related Use Case	MaaS 1.2 Ticket Validation
Brief Description	HMI Validators are a key element of ticket validation/processing. The validator devices may be attacked and breached by an external attacker. In this scenario, the attacker exploits vulnerabilities in order to claim free travel. This may be implemented indicatively through a fraudulent/manipulated credit card or smart card.
Involved Actors	1. Ridango (External Service Provider) 2. Banking Provider (External Stakeholder) 3. Cyber attacker - external to the system.
Involved and affected Asset(s)	1. Payment System Service 2. HMI Validator 1. Transit Gateway 2. Communication Gateway
Interfaces, Entry and high-level vulnerable points	The attacker gains access to data or functions that should be isolated by exploiting possible insufficient cryptography of smart cards, insecure memory protection of smart cards, or other system vulnerabilities.
Generic Scenario Description	▪ The cyber-attacker tries to manipulate the payment processing and ticket validation system using possibly a fraudulent/manipulated credit card/smart card.

	▪ By accessing confidential data, the attacker may craft a fraudulent/manipulated credit card or transportation smart card. ▪ The malicious user accesses all transportation services for free by using the fraudulent card on NFC Ticket Validator. ▪ The attack may have a financial and operational impact on the transport management authority.
Desired Response	The risks are modelled and analysed and the operators are aware of consequences, impacts and possible security controls. The security support system should assist in incident notification, reporting, classification management and response. Assistance to the security administrators for risk management in order to prevent escalation fraud/criminal activities with incident notification, classification and response, etc., is desired.

Table 12: Tallinn Threat Scenarios - Manipulated Smart Card

Attack Scenario Name	***Last-Mile Extension DDoS and DoS***
Related Use Case	MaaS 1.4 Last Mile Extension
Brief Description	The communication link of the teleoperation, the remote-control station and the vehicle is a vital element for the safe operation of the AV Shuttle. In the public transport environment, an external attacker, motivated to damage the AV shuttle, uses a denial-of-service attack to cause the communication link with the AV shuttle and the teleoperation/remote-control station to become unavailable.
Involved Actors	1. Teleoperation/Remote Operator 2. TalTech Smart Campus Traffic Management 3. Cyber attacker - external to the system
Involved and affected Asset(s)	1. Mobile Network 2. (Cross-border) Teleoperation services 3. (Cross-border) Teleoperation Module 4. Communication Modem

Interfaces, Entry and high-level vulnerable points	The attacker performs DoS attack by using open/unfiltered communication ports, lack of network monitoring for non-volumetric DDoS attacks, or any other method that can exploit resource limitation of the mobile network and onboard AV Shuttle equipment.
Generic Scenario Description	▪ The cyber-attacker launches an attack against the network that supports the teleoperation/remote-control station. ▪ This attack has a low-cost of entry from the attacker and requires relatively low skills (kali linux, Hak5 pineapple, etc.)– thus it has high probability of occurrence. ▪ Implementation of DDoS attack on the network may be instantiated with various techniques and through various network layers - from radio access to TCP/IP – by monitor the network via scanning and reconnaissance and deploying malicious tools on attacker equipment. ▪ The main goal of the attack is the malicious destruction of the AV shuttle and undermining the credibility of the last-mile transportation services. ▪ Accidents may harm public trust in automated vehicles beyond repair.
Desired Response	The specific type of attacks is proactively taken into account and anticipated through risk analysis and impact assessment. A security support system shall detect anomalous network activity that allows it to automatically activate new firewall rules or other defensive mechanisms to block traffic and monitor malicious behaviour for reporting of adversary tactics, techniques, and procedures. Timely incident notification of the security teams, risk management support, and incident reporting and notification of 3rd parties and CERTs are desired.

Table 13: Tallinn Threat Scenarios - Last-Mile Extension DDoS and DoS

Attack Scenario Name	***Ransomware Last Mile Extension***
Related Use Case	MaaS 1.4 Last Mile Extension

Brief Description	In the public transport environment, an internal or external attacker, motivated to damage the AV shuttle, injects ransomware on the onboard computer of the AV shuttle and tampers and/or encrypts files required to operate the AV shuttle safely. The onboard computer encompasses the ROS software platform required for the operation of the AV Shuttle – thus AV functionalities are affected.
Involved Actors	1. Teleoperation/Remote Operator 2. Cyber attacker - the malicious user may be an insider that accesses and tampers the vehicle's computer functionalities or a remote (unauthorized) attacker that gains access to it.
Involved and affected Asset(s)	1. AV Shuttle on-board computer 2. Mobile Network
Interfaces, Entry and high-level vulnerable points	The attacker is able to inject malicious software by exploiting vulnerabilities, like (indicatively): lack of operating system hardening, open and unmonitored usb ports, manipulated firmware update (supply chain), and more.
Generic Scenario Description	▪ The cyber-attacker launches an attack against the network that supports the teleoperation/remote-control station. ▪ The attack may be implemented using similar means with the DDoS, i.e., enumeration of the network via scanning and reconnaissance, access to the AV Shuttle network through open ports or other vulnerabilities, and the use of malicious command and control tools on attacker equipment. ▪ As a result, ransomware can be injected on the onboard computer by deploying malicious files – or more elegantly – through a tampered/rogue software update procedure. ▪ Ransomware is executed to encrypt the onboard computer file system. ▪ Alternatively, ransomware malware is uploaded using the unmonitored USB port of the on-board computer on the AV Shuttle - or generally by a malicious insider with direct physical or remote access to the device.

	▪ The goal of the attack is to render the AV shuttle inoperable and demand a ransom from the AV shuttle operator to decrypt the file system. The AV shuttle would not be able to operate without the ransomware removed from the system.
Desired Response	The risks are modelled and analysed, and the operators are aware of consequences, impacts and possible security controls. Cyber threat intelligence can provide to the operator heads up information on ransomware campaigns and new malware aiming at their systems. New mechanisms to protect against advanced persistent threats and cyber-attacks commonly used by cyber-criminal groups shall be investigated.

Table 14: Tallinn Threat Scenarios - Ransomware Last-Mile Extension

Attack Scenario Name	***Man-in-the-Middle V2X Attack***
Related Use Case	AT1.1 – Intersection Pass-through
Brief Description	The OBUs are key devices for the adaptive traffic management system. Interception of the V2X communication and injection with malicious packets, sybil attacks, or replaying of packets by a cyber attacker can cause unexpected traffic events.
Involved Actors	1. Security administrator 2. TalTech Smart Campus Traffic Management 3. Teleoperation/Remote Control Operator 4. Cyber attacker - external to the system or a malicious insider that accesses and tampers the OBU functionalities
Involved and affected Asset(s)	1. Ad-hoc vehicular network 2. CohDA OBU 3. Smart RSU
Interfaces, Entry and high-level vulnerable points	The attack may be implemented by exploiting vulnerabilities as weak authentication mechanisms, leaked certificates, weak or no encryption, etc.

Generic Scenario Description	▪ Attacker deploys network sniffer to sniff V2X messages between onboard AV OBU and the Smart RSU OBU. ▪ Through capturing V2X messages, handshakes, etc., it is possible to analyse the traffic and devise an attack plan to replay malicious communication or inject malicious packets. ▪ The attack impacts the integrity of the V2X communication stream and disrupts the flow of the traffic.
Main Flow	▪ As a result, traffic in the specific intersection is disrupted. ▪ The malicious user controls the traffic, and directly impacts the experience of the transport users, endangers lives and can harm the public trust in smart and automated solutions in traffic management and control.
Desired Response	The risks are modelled and analysed, and the operators are aware of consequences, impacts and possible security controls. A security support system shall be able to detect the attack and notify the security administrators, allowing them to timely take appropriate remedial action. The automated triggering of defence mechanisms such as firewall rules and signatures is desired, while actions to remove the rogue device from the network are initiated. The platform shall assist in incident notification, reporting, classification management and response.

Table 15: Tallinn Threat Scenarios - Man-in-the-Middle V2X Attack

Attack Scenario Name	***Spoofed RSU***
Related Use Case	AT1.2 – Intersection Stop
Brief Description	An attacker uses a spoofed RSU to control the adaptive traffic management system. The RSUs are key devices for the adaptive traffic management system. Spoofing of the OBU could allow the attacker to control the traffic management environment.

Involved Actors	1. Security administrator 2. TalTech Smart Campus Traffic Management 3. Teleoperation/Remote Control Operator 4. Cyber attacker - the malicious user may be an insider that accesses and tampers the RSU functionalities or a remote (unauthorized) attacker that gains access to it.
Involved and affected Asset(s)	1. Ad-hoc vehicular network 2. CohDA OBU 3. Smart RSU 4. Consequently, applications services that participate in the traffic management (e.g., Journey planner, teleoperation services, etc.).
Interfaces, Entry and high-level vulnerable points	The attack may be implemented by exploiting vulnerabilities as weak authentication mechanisms, leaked certificates, weak or no encryption, etc. It is also possible to consider that a malicious insider may access through otherwise legitimate and protected interfaces in order to cause harm.
Generic Scenario Description	▪ The external attacker deploys spoofed OBU or cellular base station. ▪ All V2X communications traffic and data are directed through the spoofed device. ▪ The cyber-attacker controls the intersection and directs traffic management according to their will. ▪ The challenge of the specific scenario lies in the fact that it involved detecting rogue devices directly deployed in the traffic environment. ▪ As a result, traffic in the specific intersection is disrupted – from increased delays to the cause of accidents. ▪ This directly impacts the experience of the transport users, endangers lives and can harm the public trust on smart and automated solutions in traffic management and control.
Desired Response	The risks are modelled and analysed, and the operators are aware of consequences, impacts and possible security controls. A security support system shall be able to detect the attack and notify the security administrators, allowing them to take appropriate remedial action

	promptly. The automated triggering of defence mechanisms such as firewall rules and signatures is desired, while actions to remove the rogue device from the network are initiated. The platform shall assist in incident notification, reporting, classification management and response.

Table 16: Tallinn Threat Scenarios - Spoofed RSU

Attack Scenario Name	***Disruption to Essential Service Provider Networks***
Related Use Case	All Use-Cases
Brief Description	An attacker disrupts the electricity grid, such as that seen in Ukraine (Attack on the cyber-physical equipment of the electricity distribution provider and the OT networks). The cascading effect renders the back-end ticketing and real-time information systems unavailable. Also, other 3rd party services such as banking providers and telecommunications experience intermittent service disruption.
Involved Actors	1. All Transportation Actors 2. Cyber attacker - the malicious user may be an insider that accesses and tampers the RSU functionalities or a remote (unauthorized) attacker that gains access to it.
Involved and affected Asset(s)	1. All Transportation Assets
Interfaces, Entry and high-level vulnerable points	The attack on an essential service provider has cascading effects on other service providers leading to the supporting transport infrastructure and the multimodal transportation platforms themselves.
Generic Scenario Description	▪ An attacker with multiple means of entry into the network of an electricity distribution provider can mount an offensive cyber campaign to disrupt the distribution of electricity in the city network. ▪ The loss of electricity service delivery impacts the availability of back-end supporting transportation assets and other essential service providers (Banking, Telecommunications).

	▪ Operators must initiate disaster recovery and business continuity plans.
Desired Response	The risks are modelled and analysed and the operators are aware of consequences, impacts and possible security controls. A security support system shall be able to trigger a defensive response to attacks against essential service providers, which have cascading effects on the transportation ecosystem. CTI should be available that informs the transport operator of any malicious campaigns and activity that can have major impacts on the provision of essential services. The platform shall assist in incident notification, reporting, classification management and response.

Table 17: Tallinn Threat Scenarios – Disruption to Essential Service Provider Networks

4 GENOA USE-CASE

The Genova Use Case will focus on two main transport ecosystem operation aspects:

- Information to passengers;
- Electronic and mobile ticketing.

These two fields will be explored in several “micro” scenarios that focus on very specific situations. Each scenario will be detailed as follows:

- Definition of the “story” behind the scenario: actors, expected behaviour;
- Schematization of the process flow with the link between actors;
- Identification of the asset involved in the scenario;
- Sequence diagram to define the process;
- Identification of the possible attacks that could be made on the scenario;
- Identification of the blocks of the CitySCAPE platform that could help in mitigating the risk.

After the description of these scenarios, different “macro scenarios” will be defined. They summarize the scenarios by describing a more complex real-life situation where a set of “micro” scenarios are involved. In this way, we create a more challenging situation to study, also improving the narrative behind our use case.

4.1 Macro scenarios definition

This section focuses on the definition of scenarios that describe real-life situations and tries to summarize all the “micro” scenarios defined in the previous section.

4.1.1 Passenger trip

In this macro scenario, a real-life situation of a passenger who wants to travel from his home to a location is considered. For the description of this scenario, we consider a passenger, called Alice, that wants to visit the small town of Casella, in the metropolitan area of Genova, and she wants to use public transport to do that.

Since the best option is to use the “Genova-Casella” railway that runs from the Genova city centre to the town of Casella, Alice has different trips to organize:

- Going from her home (A) to the nearest bus stop and take a bus to the nearest metro station of “Brin” (B);
- Take the metro from “Brin” to the “Darsena” stop (C);
- Take a bus from “Darsena” to the “Genova-Casella” railway station (D);
- Take the “Genova-Casella” railway from D to Casella.

The image below tries to summarize these steps:

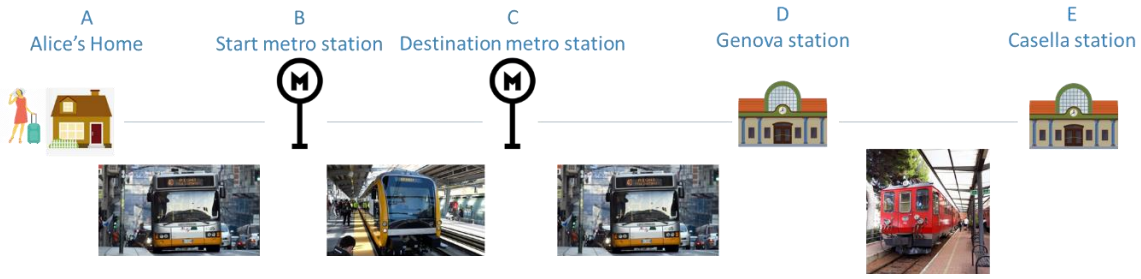

Figure 23: A schema of the "Passenger trip" macro scenario

Within all these steps, Alice encounters several of the scenarios defined in the previous section:

Going from her home (A) to the nearest bus stop and take a bus to the nearest metro station of "Brin" (B)

- She checks on the website for which lines that reach B are passing at a stop near her home (IS-2);
- At the stop, she opens the app to see the waiting times (IS-1);
- She purchases a ticket within the app when the bus is arriving (TS-1.1).

Take the metro from "Brin" to the "Darsena" stop (C)

- She checks the waiting time from the monitors outside the station (IS-3);
- She enters the station and waits for the train (IS-4);
- She shows the purchased ticket to an inspector when requested (TS-1.2).

Take a bus from "Darsena" to the "Genova-Casella" railway station (D)

- She watches from the app the waiting time of the bus to catch (IS-1);

Take the "Genova-Casella" railway from D to Casella

- She checks from the app the scheduled departure of the train (IS-2);
- She waits for the train departure at the station's platform (IS-1);
- She purchases a train ticket within the app (TS-1.1);
- When requested, she shows the purchased ticket to the inspector (TS-1.2).

4.1.2 Re-plan of trip

In this macro scenario, another real-life situation is taken into consideration. For the description of this scenario, we consider a passenger called Bob, who daily uses public transportation to reach his workplace. For these reasons, Bob is a CityPass subscription holder and he uses the mobile application both to handle his subscription and to stay updated on possible service interruption/change.

Bob uses to follow the same route every day, composed by bus and metro, to reach his office. Due to a technical problem, the metro service is stopped right before that Bob leaves his home. He receives an alert from the mobile application that informs him about the service interruption. So now, Bob has to re-plan his journey by using the urban train and a bus to reach its office approximately at the same time, not to be late at work.

In this situation, Bob can use the urban train since he has a valid CityPass subscription, so he can enter the train station where a Trenitalia inspector can verify the validity of his subscription (that has been registered inside the mobile application).

In this scenario, we take into consideration:

- The registration of the CityPass card within the mobile application (TS-2.1)
- The event of "technical problem" that led to the out of service, and hence the registration of that event in the "event database" (IS-5);
- Sending notification to the user on event registration (IS-5);
- Re-plan the trip by using the Trenitalia website/app and the AMT website/app to get the schedules (IS-2);
- Bob uses his CityPass to use the urban train services (TS-3).
- Bob uses his CityPass to use the urban bus services and, when requested, he shows the subscription to the inspector using his mobile app (TS-2.2).

4.2 Assets involved in the use-case

In this section, a brief description of each asset involved in the use-case scenarios is given.

4.2.1 AVM related assets

4.2.1.1 Smart Display

"Smart display" refers to the displays that show the real-time estimating arrival time on a bus stop or a train station. These displays are directly linked to the AVM system via a 2G connection in a segregated network.

Figure 24 - AVM Smart displays

4.2.1.2 System

The AVM (Automated Vehicle Monitoring) System is deployed to monitor the fleet of the public transport company (AMT). This system monitors all the buses and other transportation assets like the "Genova-Casella" railway. The System relies on three main items:

- The AVM System servers, deployed in the AMT premises, contain all the business logic, the databases and the applications.

- The on-board systems, deployed on the buses/trains to collect data about position and the event that happens on the site (e.g., arriving at a stop, open/close the doors, etc) that are connected via a 2G connection in a segregated network.
- The smart displays are defined in the previous section.

4.2.2 Application assets

4.2.2.1 Mobile application

The "AMT Genova" mobile application is the official app of the public transportation company of Genova. It offers several services to the citizens that want to use the public transportation system, such as:

- Get schedules for all the AMT services (bus, metro, suburban train, etc.).
- Get live transit data at bus stops.
- Get real-time updates to service modifications/interruptions.
- Purchase tickets for public transport.
- Register and renew subscriptions.

The application is linked to the AMT service backends and Google/Apple-specific services depending on the platform.

The application requests permission to access:

- The GPS position, to localize the user and propose to him/her the nearest stops.
- The Internet, for calling all the backend services.
- The smartphone camera to scan the CityPass barcode to verify its validity (this function is not used so frequently).
- The NFC reading for quickly registering the CityPass into the App.
- The microphone to perform a vocal search.

Note that the permissions are requested only when the functionality that requests a specific permission is used.

The application is available on Google Play Store, Apple App Store and the Huawei App Gallery.

4.2.2.2 Ticketing inspectors application

The so-called "ticket inspector application" is a mobile app that runs on specific devices and its main goal is to provide the inspectors with a tool to verify tickets and subscriptions and issue fines when necessary. The application is not publicly available, and it is installed only on the inspectors' devices (Android 7.0).
This application is linked with the AMT service backends and has internal storage to retain some off-line information, such as the validity of the subscriptions and some data about subscribers.

4.2.3 Backend assets

4.2.3.1 Infomobility System

The infomobility system is composed of a server that runs on AMT premises and that is exposed to the public. This server hosts all the services that offer information to passengers such as live transit and service schedules. It also supports the sending of real-time notifications to user through the mobile application and retrieves service interruption/deviation information. It is linked internally with the AVM System, the Service Management System and the Event Database to retrieve the information once requested by users. All these services are exposed as HTTPS web services (REST with JSON output or XML).

4.2.3.2 Event Database

The Event Database is a database that contains events that happen on the service execution that could be:

- Service interruptions
- Delay on certain services
- Deviation on bus routes

These events are not scheduled and are completely out of the control of the transport operator. When such an event happens, the transport operator fill this database with specific software and the event remains in the database to be used by infomobility services

4.2.3.3 Ticketing system

The ticketing system hosts all the services and the databases that allow passengers to purchase and inspectors to verify a ticket. This system is composed by:

- A database that hosts all the users and purchased tickets;
- A service to interact with the mobile app to present available ticketing options and functionalities in order to purchase them;
- A service to verify if a ticket is valid or not.

All the services and databases are handled as separated containers in a Docker environment installed on to virtual machines.
All the services are exposed as HTTPS REST web services with JSON as data format.

4.2.3.4 Subscription system

The Subscription system hosts all the services and data that allows passengers to register their CityPass subscription into the mobile application and the inspector to verify their validity. This system is composed of:

- A local database that hosts all the valid cards with associated user information;
- A service to register/unregister the card from the mobile app;
- A service to verify if a subscription is valid or not.

All the services and databases are handled as separated containers in a Docker environment
All the services are exposed as HTTPS REST web services with JSON as data format installed on to virtual machines.

4.2.3.5 Website

The website of AMT is the first and the most important communication channel of the company. It contains information about the company and all the services that AMT handles. On the website, a passenger can retrieve all the information they need to plan their public transport journey. Along with it, ticket purchase/subscription renewal services are also available.
The website is hosted in an apache webserver installed on to virtual machines and exposed via HTTPS .

4.2.4 Other assets

4.2.4.1 Service management system

The service management system is a software platform used to organize the entire fleet and schedule the service. In the context of CitySCAPE it will be used as a source element for the scheduled time of buses, metro, etc.

4.2.4.2 Smart Monitor

Smart monitors are installed at the metro station, and their main functionality is to give information to passengers. They are of two types:

- Monitor installed at the station entrance to give passenger information about train estimated arrival time.
- Monitor installed inside the station, at the platforms, with infotainment objectives.

4.2.4.3 Inspector's device

The Inspector's device is the device that the ticket inspector uses to verify passenger's tickets. They are Android devices that are capable of:

- Scanning NFC cards (i.e.. the CityPass card);
- Printing (i.e., for fines or payment receipt).
- Scanning barcodes/QR codes;
- Accepting payments - acting as an e-POS.

The device runs Android 7.0 with minimal vendors' customization.

4.2.4.4 CityPass card

CityPass card is an NFC tag that holds the subscriber's card number and is paired with a serial number. The passenger uses it to access and use the public transport network. Subscriptions are charged there and are always valid the day after the date they are purchased

4.3 Micro scenarios definition

4.3.1 Infomobility scenarios

4.3.1.1 IS-1: Waiting time at the stop

In this scenario, a very typical situation is taken into consideration: a passenger wants to know the waiting time for a bus at a certain stop. The passenger could be at home, on the street or directly at the desired bus stop. In this situation, the passenger has three ways to retrieve the information they want:

1. By using the AMT mobile application from their smartphone.
2. By browsing the AMT website from his PC or his smartphone.
3. By watching the smart display at the stop, if available (Note: not all the bus stops have a smart display installed on it).

The desired behaviour could be described, based on the different means of usage respectively, as follows:

1. The passenger opens the mobile application, then he selects the desired bus stop identified by a four-digit code and he eventually watches the live transits and waiting times.
2. The passenger opens a browser on its computer or smartphone, then he browses to the AMT website and selects the “live transit” section. Finally, he selects the desired bus stop identified by four-digit code and he eventually watches the live transits and waiting times.
3. The passenger arrives at the bus stop and watches the live transit and waiting times directly from the smart display.

This scenario's main actor is the passenger who uses different IT instruments (mobile application, website, smart display) to interact with the public transport infomobility system.

The following table describes the assets involved in the scenario and the scope of each of them.

Name	Type	Functions offered by the asset	Interfaces	Property, ownership
Smart display	HW	Displays information on transits at the stop and other general information	Linked to the AVM by segregated mobile network	AMT
AVM System	HW/SW	Gather events from buses; calculates the transit forecasts;	Linked with smart displays by segregated mobile network;	AMT

			Linked with internal servers via web services	
Bus (on-board embedded system)	HW	Periodically sends to the AVM bus events such as: GPS position, open/close doors, etc.	Linked with AVM System by segregated mobile network	AMT
Mobile application	SW	Displays information on transits at stops	Linked with Infomobility server via public HTTPS web service	AMT
Infomobility Server	HW/SW	Provides transits forecast on stops	Expose to public HTTPS web services	AMT
Website	HW/SW	Displays information on transits at stops	Exposed to the public via HTTPS; linked via infomobility server via internal HTTP call	AMT
Smartphone	HW	Runs the mobile application	Main interface to passenger	Passenger
PC	HW	Runs the web browser	Main interface to passenger	Passenger
Mobile network	HW	Provides the network infrastructure	N/A	Mobile op.

Table 18: Waiting time at stop - assets involved in the scenario

The following figures depicts how the main actors and assets of the scenarios are linked together.

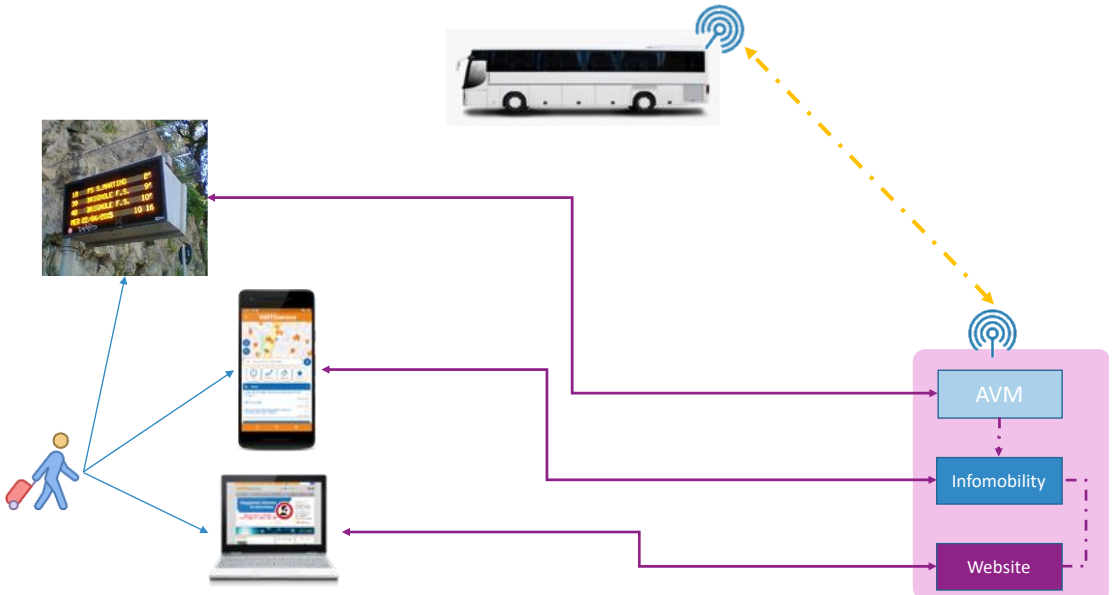

Figure 25: Waiting time at the stop - main actors and assets

The operations and the workflow of this scenario are described in the following sequence diagram.:

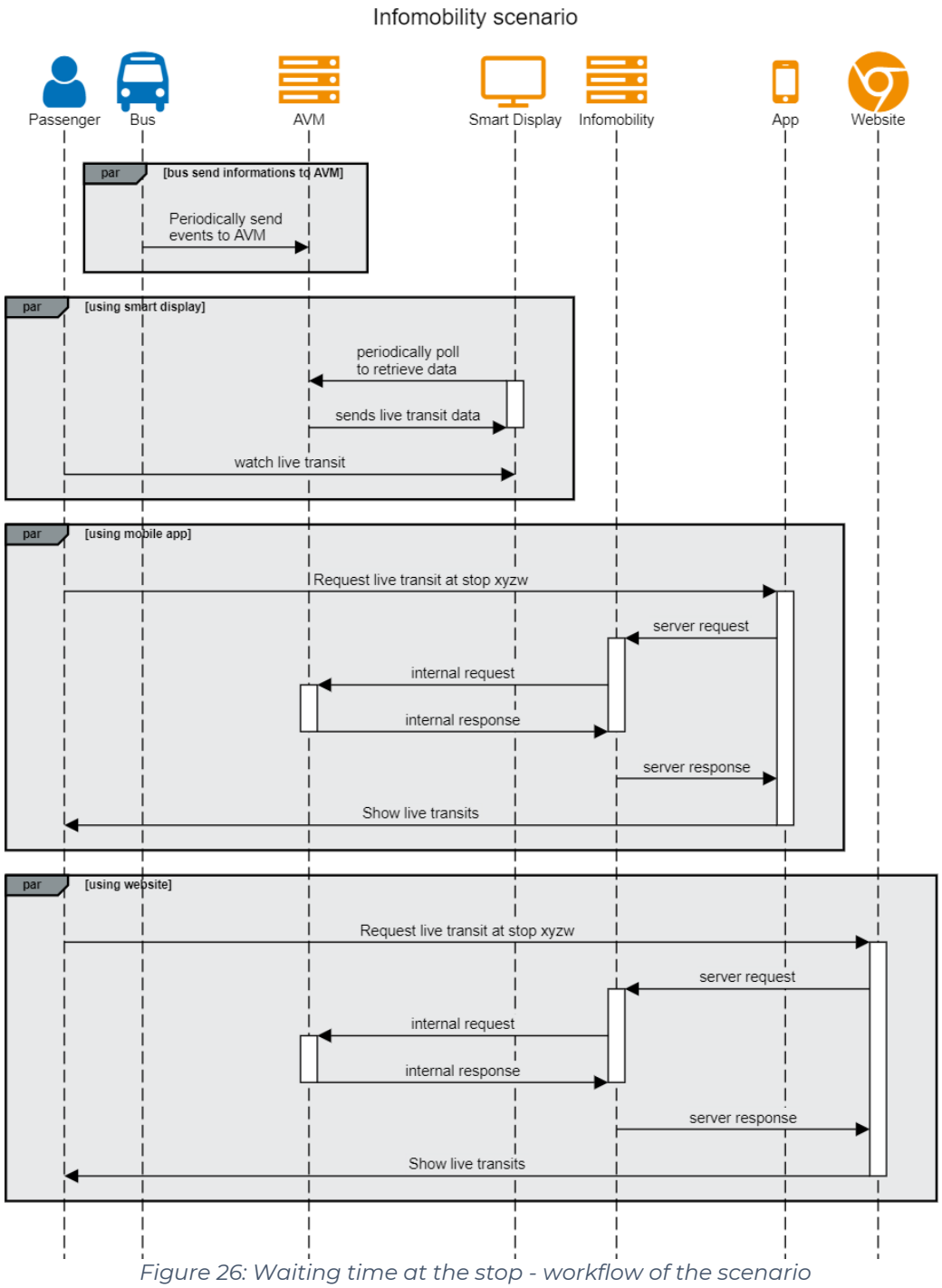

Figure 26: Waiting time at the stop - workflow of the scenario

In this kind of scenario several attacks are anticipated, with the objective mainly to compromise the information given to the passenger or to make the system unreachable. These could be made by several means or methods, for example:

- Manipulation of data: the passenger gets wrong data on arrival times. Passengers could also be alerted wrongly (e.g. fake bomb alarm, fake fire alarms, etc.). This also affects citizens that use the display for information (Smart display, App or Web Site).
- Resource made unavailable: the passenger cannot access and see the arrival times.
- Smart display made unavailable (sabotage).

- Valid information is purposely delayed in order to disrupt passenger commute.

4.3.1.2 IS-2: Service schedule

In this scenario, we present another very common situation: a passenger that wants to know the schedule of a public transport service such as bus, metro, etc.
In this case, the passenger can substantially retrieve this information in two ways:

- By using the AMT mobile application;
- By using the AMT website, from his/her smartphone or computer.

The desired behaviour could be described, based on the different means of usage respectively, as follows:

1. The passenger opens the mobile application, then he selects the desired bus line/service and eventually watches the schedule.
2. The user opens a browser on its computer/smartphone, then he browses to the schedule section, selects the desired bus line/service and eventually watches the schedule.

The main actor of this scenario is the passenger who uses different IT instruments (i.e. the mobile application and/or the website) to interact with the public transport infomobility system to retrieve service schedules.

The following table describes the assets involved in the scenario and the scope of each of them.

Name	Type	Functions offered by the asset	Interfaces	Property, ownership
Service Management System	HW/SW	A system that holds all the planned services and interacts with service schedules	Linked internally (no public) with the Infomobility System	AMT
Mobile application	SW	Displays information on schedules	Linked with Infomobility server via public HTTPS web service	AMT
Infomobility Server	HW/SW	Provides schedules of services	Linked with mobile app via public HTTPS web services	AMT

Website	HW/SW	Displays information on service schedules	Linked with clients via HTTPS; linked via infomobility server via internal HTTP call	AMT
Smartphone	HW	Runs the mobile application	Main interface to passenger	Passenger
PC	HW	Runs the web browser	Main interface to passenger	Passenger

Table 19: Service schedule - assets involved in the scenario

The following figure presents how the main actors and assets of the scenarios are linked.

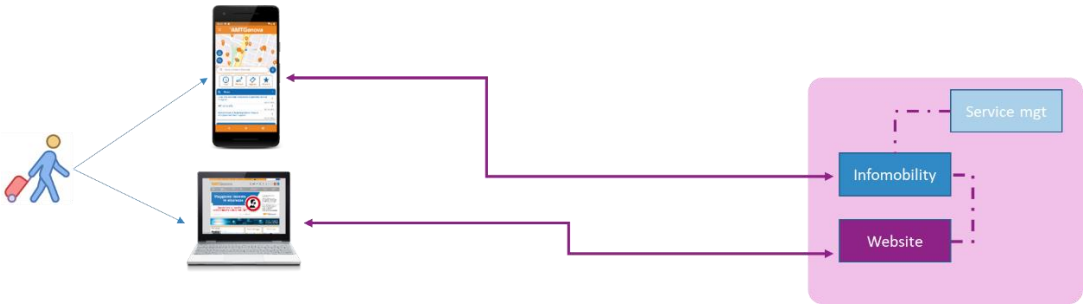

Figure 27: Service schedule - main actors and assets

The operations and the workflow of this scenario are described in the following sequence diagram.:

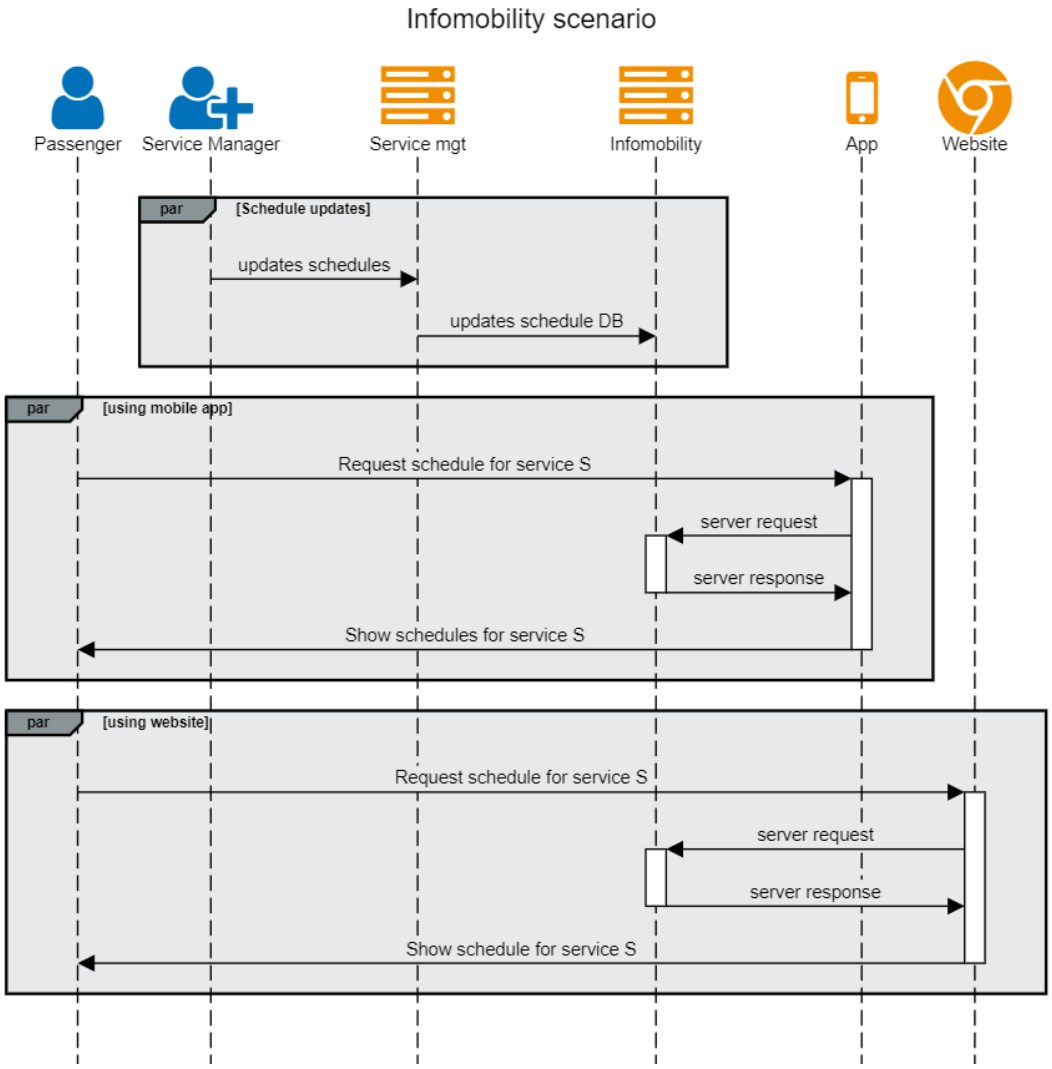

Figure 28: Service schedule - workflow of the scenario

In this kind of scenario, several attacks could be made, mainly to compromise the information given to the passenger or to make the system unreachable. These could be made by several means or in several ways, for example:

- Manipulation of data: the passenger gets wrong data on scheduled times.
- Resource made unavailable: the passenger cannot see schedules.

Valid information is purposely delayed in order to disrupt passenger commute.

4.3.1.3 IS-3: Waiting time to the next train

This scenario refers to a passenger that wants to know the arrival time of the next metro train before getting into the metro station: all the metro stations are equipped at their entrances (or very near to them) with displays that show the arrival time of the trains. In this scenario, a passenger approaching the station can see when the next train is expected to arrive at the station, allowing him to decide if he needs to hurry to catch up the train or go slower.

The main actor of this scenario is the passenger that interacts with the metro internal information system to retrieve arrival times.

The following table describes the assets involved in the scenario and the scope of each of them.

Name	Type	Functions offered by the asset	Interfaces	Property, ownership
Smart monitor	HW	Displays information on transits at the stop and other general information	Linked with the control centre by network connection	3rd party
3rd party system	HW/SW	Handles the smart display information visualization (arrival times, alerts, etc.)	Linked with smart display by network connection	3rd party
Metro train onboard system	HW/SW	Sends events to the control centre	Linked with metro control centre via segregated network and specific protocols	3rd party
Metro Control centre	HW/SW	Gathers events from metro trains and estimate waiting times	Linked with smart monitors via network connection; Linked with internal servers via web services (no public)	AMT

Table 20: Waiting time to the next train - assets involved in the scenario

The following figure depicts how the main actors and assets of the scenarios are linked.

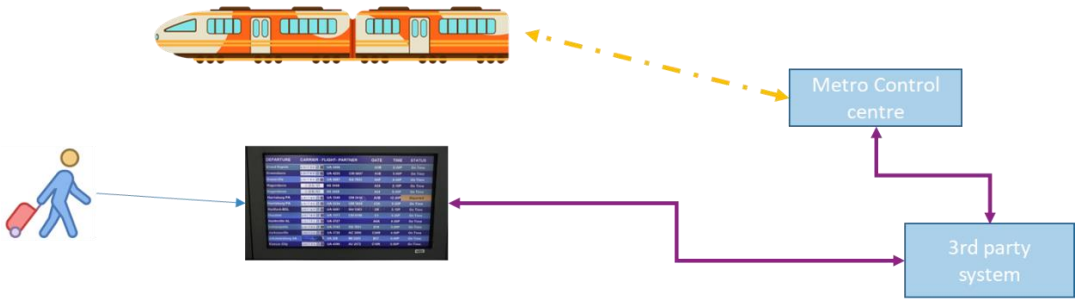

Figure 29: Waiting time to the next train - main actors and assets

In this scenario, attacks on the information showed on display are the most probable ones.

- The passenger could be misled due to data manipulation: the passenger gets wrong data on arrival times, or the display is made unavailable, for example.
- The passenger could also be wrongly alerted (e.g., fake bomb alarm, fake fire alarms, etc.) if someone takes control of the display to write a message into it. This problem could also affect citizens that see the display because they are near the station.
- Resource made unavailable: the passenger cannot see the arrival times.

4.3.1.4 IS-4: Metro station

This scenario explores what happens when a passenger is waiting for a train in the metro station, i.e., on the platform. In this situation, the passenger is typically not actively interacting with any part of the transport system, but he could be reached by different means of communications that are present in the metro station:

- Via the displays inside the platforms that show infotainment contents;
- Via the audio diffusion installed in the station;
- Via alarm systems, such as fire alarm.

In this situation, the passenger is a passive actor surrounded by different assets, described in the table below:

Name	Type	Functions offered by the asset	Interfaces	Property, ownership
Smart display	HW	Displays infotainment contents and general advices	Linked with the 3rd party system by network connection	3rd party

Display control system	HW/SW	Handles the smart display information visualization	Linked with smart display by network connection	3rd party
Metro station control system	HW/SW	Handles the station assets (electricity, audio diffusion, fire alarms, etc.)	Linked with station assets via dedicated link	AMT/3rd party

Table 21: Metro station - assets involved in the scenario

The figure below depicts how the actor and the asset are linked with each other.

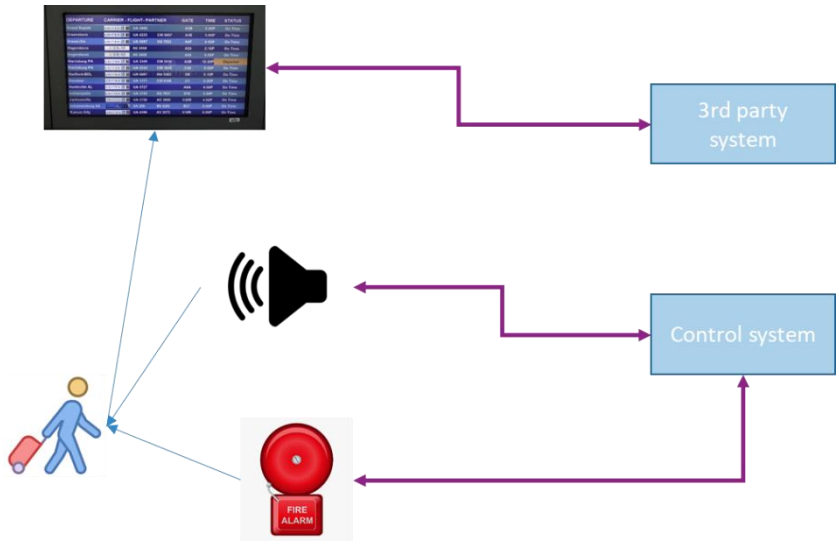

Figure 30: Metro Station - main actors and assets

Possible attacks that could be made on this scenario:

- Resource made unavailable: the passenger cannot see the monitors or listens to notice or alarm.
- Intrusion that shows offensive material on the monitors/audio diffusor.
- Audio is used maliciously to send fake alarms or messages, generating chaos in the station and alerting the operators.

4.3.1.5 IS-5: Notifications to passengers on service update

In this scenario, we analyse the active communications with passengers due to service outbreaks or modifications that are, in most cases, not scheduled but happen due to several special reasons such as road interruptions, technical problems and so on.
These messages reach the users by several means:

- Through SMS if subscribed to a specific alert service;

- Through the mobile app via the “service update section”;
- Through the mobile app via the notification system;
- Through the AMT Web site

The data about these events originate from an event manager system deployed on AMT premises and used by AMT personnel to introduce new events. When an event is imported, it is processed and specific business logic to decide the channels where to publish the communication is executed.

In this scenario, the main actors are the AMT operators that import events and the passengers that receive alerts or watch the corresponding information in one of the aforementioned channels through the infomobility system that interacts with the so-called “event database” that contains all the information about service interruption or deviation updated by the AMT personnel.

The following figure presents how the main actors and assets of the scenarios are linked.

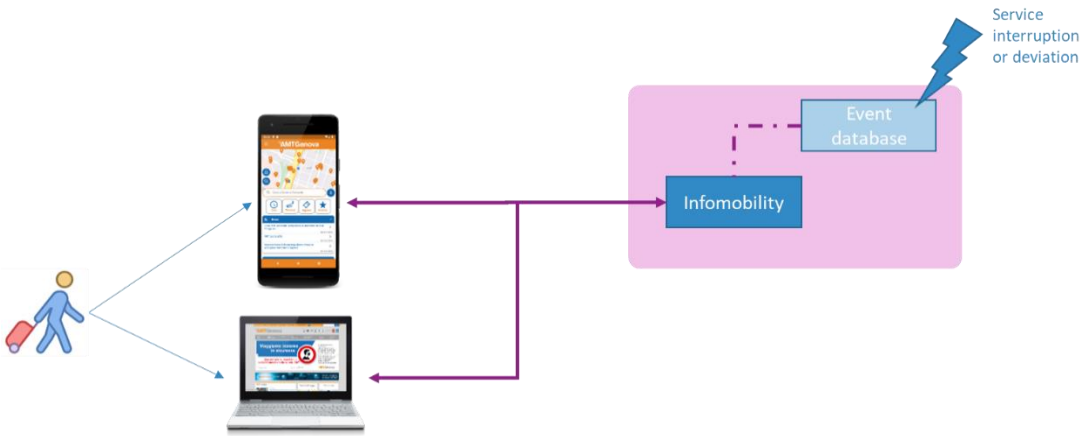

Figure 31: Notifications to passengers on service update - main actors and assets

In this scenario, several attacks could be made, mainly to compromise the information given to the passenger or to make the system unreachable. These could be made by several means or in several ways, for example:

- Manipulation of data: the passenger gets wrong alerts or fetches wrong service interruption data.
- Resource made unavailable: the passenger cannot see service changes or cannot receive notifications/alerts.

4.3.2 Ticketing scenarios

4.3.2.1 TS-1: Ticket from the mobile app

In this scenario, we analyse the case where a passenger wants to purchase a ticket for public transport. In the last decade, e-ticketing has become increasingly central in the ticketing process, especially in the last years with the explosion of smartphones and mobile payment systems that allows the purchase of a ticket with just a couple of taps without having to search for an open sale point or buy directly on board. As of today, there are different means of e-ticket in Genova. Still, the most significant (also for its relevance

in the mid-term development plan of the transport company) is purchasing a ticket via mobile application.

We analyse this scenarios from two different perspectives: the process of ticket purchase from the mobile application, that is called **TS-1.1**, and the verification process of the e-ticket purchased via the App, which is performed by transport company personnel by requesting the ticket and verifying it using a proper device. This latter is called **TS-1.2**.

The desired behaviour in this scenario is split into two parts: the purchase made by the passenger and the verification of the ticket made by an inspector.

TS-1.1 desired behaviour: passenger that buys a ticket from the mobile application

The passenger opens the mobile application, then he chooses the desired ticket, inserts the payment information (credit card detail, apple pay, or google pay credentials) and completes the purchase. The ticket is finally showed in the app and saved.
In the case of a verification request, the passenger shows the inspector the ticket's barcode to perform the verification process.

TS-1.2 desired behaviour: inspector that verifies ticket from its device (with its dedicated application)

The validator opens the application and then scans the ticket barcode presented by the passenger mobile app. Then, the inspector application shows if the ticket is valid or not, also displaying the ticket details so that the ticket inspector can double-check with the information provided by the passenger's smartphone.

The main actors of this scenario are the passenger that buys the ticket and the inspector that verifies it.

The following table shows the involved assets and their role in the scenario.

Name	Type	Functions offered by the asset	Interfaces	Property, ownership
Ticketing System	SW	System that holds all the planned services and interacts with service schedules	Linked with mobile app and ticket inspector app via HTTPS. Linked with the bank via HTTPS APIs (PUBLIC)	AMT
Mobile application	SW	Displays information on schedules	Linked with Ticketing system via public HTTPS web service	AMT

Ticket inspector's application	SW	Checks the validity of the tickets	Linked with Ticketing system via public HTTPS web services	AMT
Ticket inspector device	HW	Runs the ticket inspector app	Main interface to the ticket inspector	AMT
Smartphone	HW	Runs the mobile application	Main interface to passenger	Passenger
Mobile network	HW	Provides the network infrastructure	N/A	Mobile op.

Table 22: Ticket from the mobile app - assets involved in the scenario

The following figure depicts how the actors and the assets are linked to each other in the scope of this scenario.

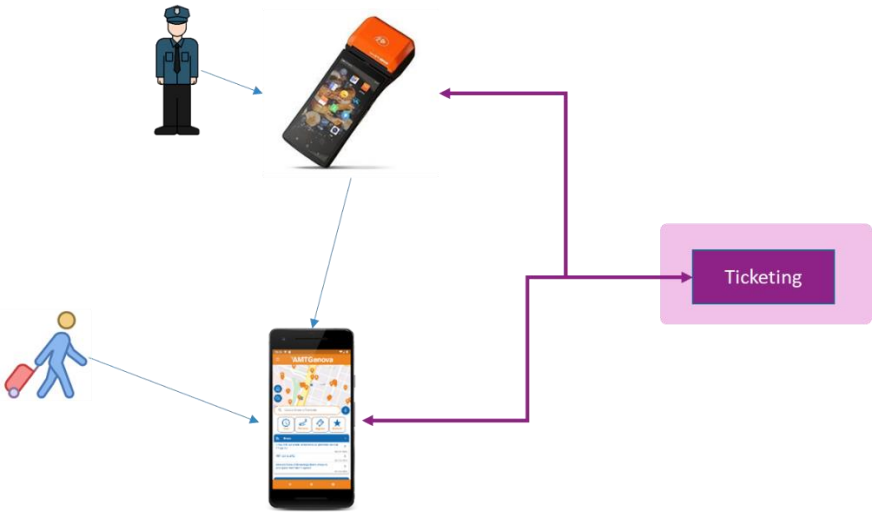

Figure 32: Ticket from the mobile app - main actors and assets

The operations and the workflow of this scenario are described in the sequence diagram below:

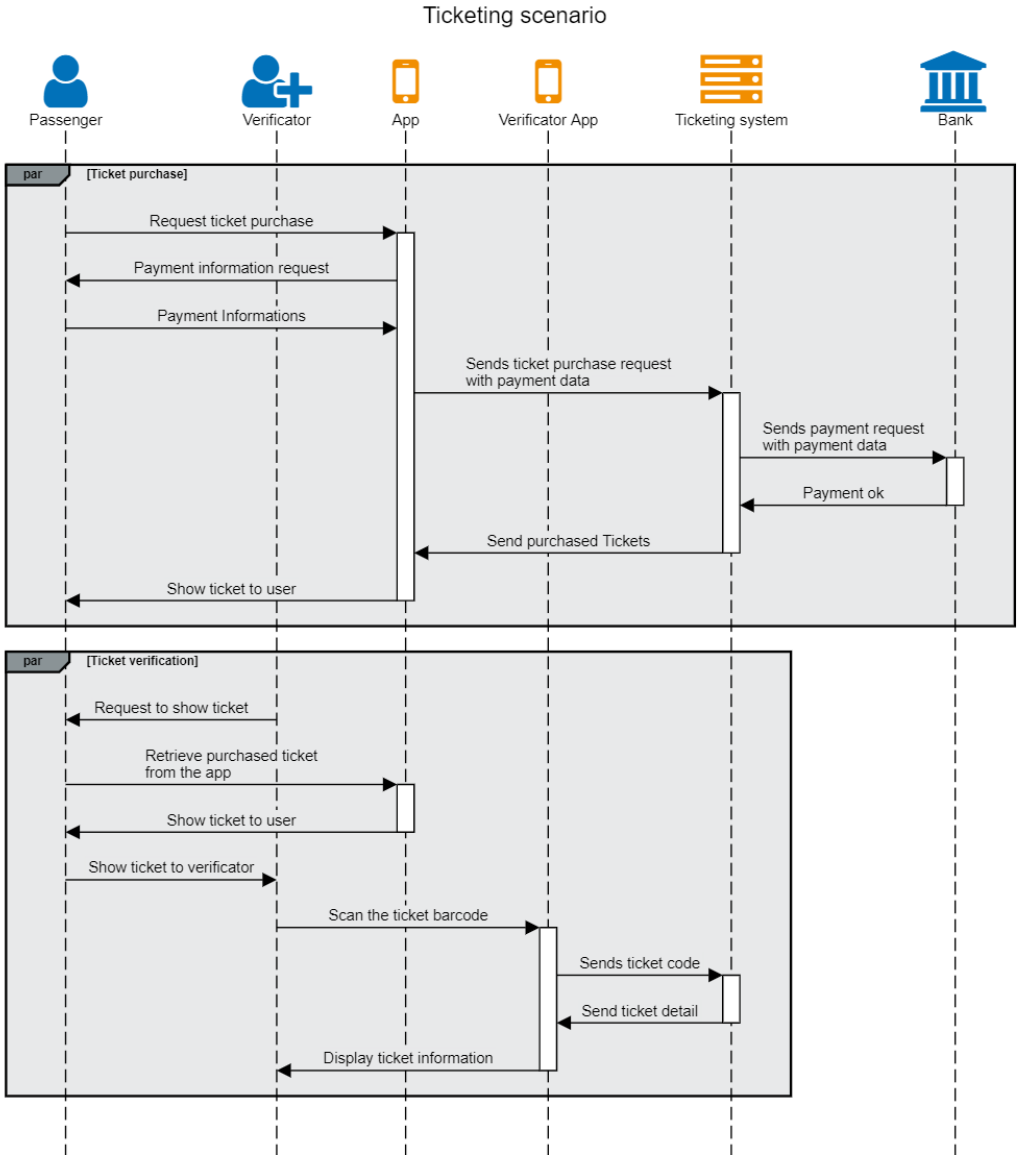

Figure 33: Ticket from the mobile app - workflow of the scenario

As shown in Figure 33, in TS-1.1 scenario we are dealing with a bank where sensitive information are present and are exchanged between involved parties. All these processes falls under the PCI-DSS directive that has to be considered with care when designing such scenario for the pilot. For the sake of completeness, it must be said that all the production process that are behind this kind of scenario are fully compliant with the aforementioned directive. However, in the scope of the Project pilot, all fake data will be used and the data exchange between the bank and the system under analysis will be emulated.

In this scenario, different attacks could be made, e.g.:

- Resource made unavailable: the passenger cannot purchase tickets and validator cannot verify them.
- Ticket forgery makes it possible to use transport services without pay or pay less (e.g., paying for one passenger or showing a ticket for two or more passengers).

- Ticket duplication makes it possible to use one valid ticket on multiple devices.
- Payment information theft when a passenger is inserting into the application.
- The integrity of the inspector app is compromised, and the validation results are erroneous.
- The inspector app does not perform cross-check but directly validates all tickets.
- Banking details from the mobile phone are leaked.

4.3.2.2 TS-2: CityPass subscription dematerialization

In this scenario, we analyse another e-ticket case that has been implemented in the last year and that is related to the public transport subscriptions. In detail, in Genova, all the subscriptions to the public transport system are registered into a card called "CityPass". With this card, a passenger can purchase its subscriptions (i.e., weekly, monthly and annual) and use the card to access all the subscribed services. In this way, the card is the ticket. In the last year, the possibility to register the CityPass card into the mobile application has been added to use the smartphone as the ticket and directly renew the subscription from the smartphone.

In this scenario we consider two main processes: the registration of the CityPass inside the app and its usage, called **TS-2.1**, and the verification made by the inspector, called **TS-2.2**. So, as in TS-1, the main actors are the passenger and the inspector.

The desired behaviour of this scenario is described below.

TS-2.1 desired behaviour: mobile application

The user opens the mobile application, then he first registers its subscription inside the application.
After that, he can show the mobile application to the ticket inspectors when requested.

TS-2.2 desired behaviour: ticket inspector application

The validator opens the application and then scans the CityPass barcode presented by the passenger. Then, the application crosschecks if the CityPass is valid or not, also by presenting the CityPass details so that the ticket inspectors can double-check with the information provided by the passenger's smartphone.

The assets involved in this scenario are listed in the following table.

Name	Type	Functions offered by the asset	Interfaces	Property, ownership
Subscriptions System	SW	System that holds the information on the active subscriptions and allows to register	Linked with mobile app and ticket inspector app via public HTTPS API	AMT

		them into the app, check the validity and renew		
Mobile application	SW	Holds the subscription's information after the user registers it	Linked with Subscription system via public HTTPS web service	AMT
Ticket inspector application	SW	Checks the validity of the subscription by reading the CityPass barcode/NFC	Linked with Subscription system via HTTPS web services	AMT
Ticket inspector device	HW	Runs the ticket inspector app	Main interface to ticket inspector	AMT
Smartphone	HW	Runs the mobile application	Main interface to passenger	Passenger
CityPass	HW	Subscription card	N/A	Passenger / AMT
Mobile network	HW	Provides the network infrastructure	N/A	Mobile op.

Table 23: CityPass subscription dematerialization - assets involved in the scenario

The figure below presents how the actors and assets are linked to each other in this scenario.

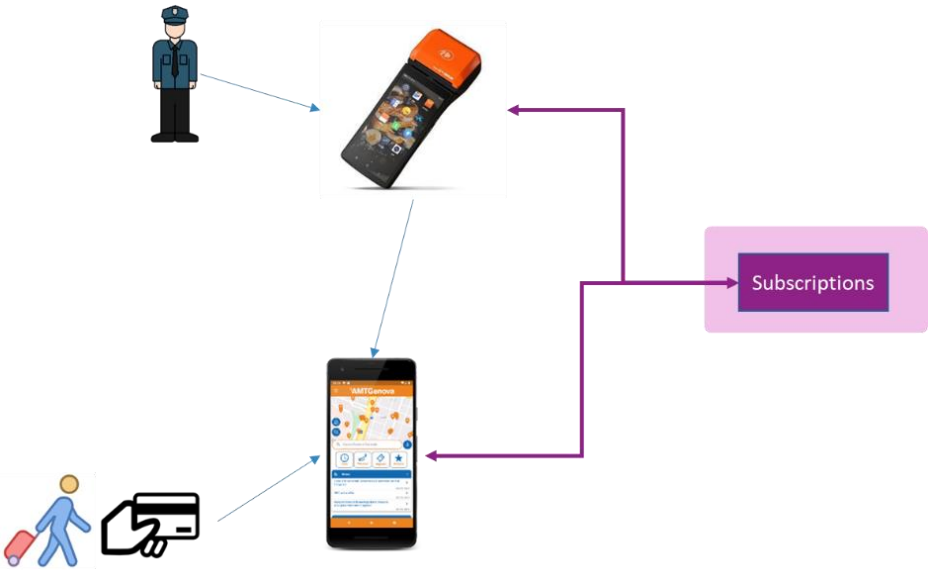

Figure 34: CityPass subscription dematerialization - main actors and assets

The operations and the process workflow are depicted in the following sequence diagram:

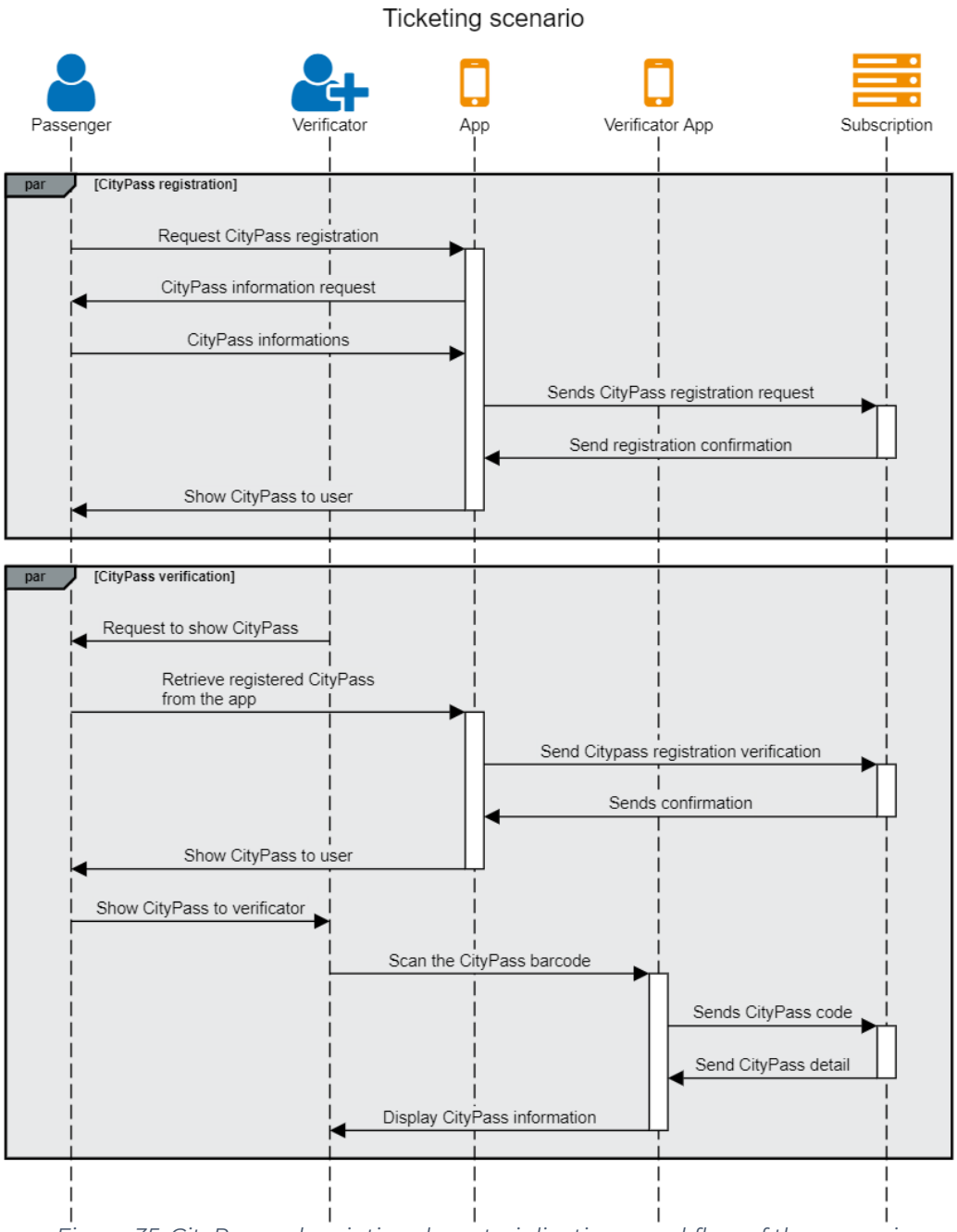

Figure 35: CityPass subscription dematerialization - workflow of the scenario

In this scenario, various attacks could be considered, e.g.:

- Resource made unavailable: the passenger cannot register its CityPass and the ticket inspector cannot verify it.
- CityPass falsification makes it possible to use transport services without paying.

- CityPass duplication makes it possible to use one valid CityPass on multiple devices.
- CityPass personal information of passenger may be stolen.

4.3.2.3 TS-3: Using urban train with CityPass subscription

In this scenario, we will analyse a multi-modal, multi-company scenario where a passenger wants to use the urban train transport with its CityPass subscription. When a passenger purchases a CityPass or renews its subscription, he can use all the urban services, including trains handled by the national train company (Trenitalia). Since the two companies handled the ticket control system independently, a data link between the two systems has to be provided.
In detail, since the CityPass subscription is handled directly by AMT, this latter provides the data about the validity or not of a CityPass to Trenitalia.

The data provided to Trenitalia are of two types:

- Data to be used at the station entrance: AMT provides data on the Valid CityPass daily; the reader on the gate reads the CityPass and then decides if it is valid or not and opens the entrance accordingly. These data are sent through secure communication links.
- Data to be provided to Trenitalia ticket inspectors so that they can verify if a passenger has a valid subscription when he is on board. These data are provided by means of a web service that is integrated into the subscription system.

The desired behaviour of this scenario is described below.
Desired behaviour: passenger
The passenger can seamlessly catch the urban train with his subscription. He can enter the train station by using his CityPass subscription when requested at the entrance gates or by the ticket inspector.

Desired behaviour: ticket inspector application
The ticket inspector can validate the CityPass of the passenger by getting information about its validity.

The assets involved in this scenario are listed in the following table.

Name	Type	Functions offered by the asset	Interfaces	Property, ownership
Subscriptions System	SW	System that holds the information on the active subscriptions and allows to register them into the app, check the validity and renew	Linked with mobile app and ticket inspector app via public HTTPS API. Linked to Trenitalia data asset via secure SFTP connection	AMT

Mobile application	SW	Holds the subscription's information after the user registers it	Linked with Subscription system via public HTTPS web service	AMT
Ticket inspector application	SW	Checks the validity of the subscription by reading the CityPass barcode/NFC	Linked with Subscription system via HTTPS web services	3rd paty (Trenitalia)
Ticket inspector device	HW	Runs the ticket inspector app	Main interface to ticket inspector	3rd paty (Trenitalia)
Smartphone	HW	Runs the mobile application	Main interface to passenger	Passenger
CityPass	HW	Subscription card	N/A	Passenger / AMT
Mobile network	HW	Provides the network infrastructure	N/A	Mobile op.

Table 24: Using urban train with CityPass subscription - assets involved in the scenario

The figure below depicts how the actors and assets are linked to each other in this scenario.

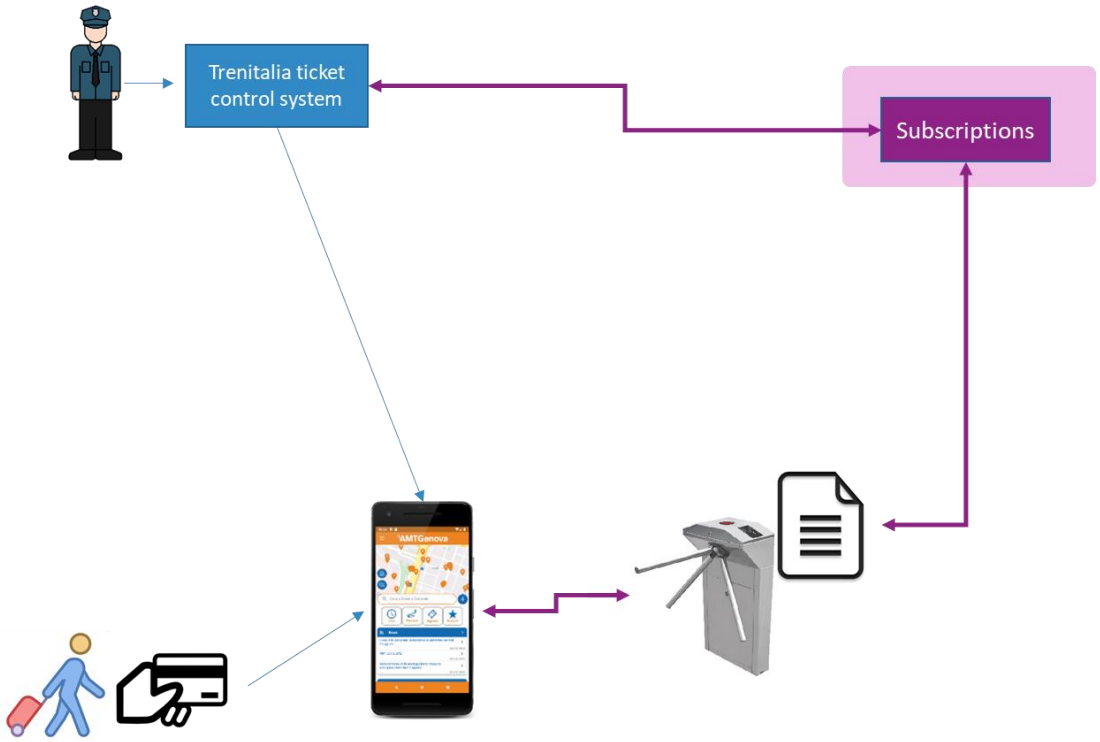

Figure 36: Using urban train with CityPass subscription - main actors and assets

4.4 Genova Use-Case asset table

In this section a table that contains all the asset used in the use case is presented. In this table we put details about each asset and the functions they offers

Name	Type	Managed by / Owned by	Basic Asset breakdown	Interfaces	Role
Mobile Network (2G / 4G)	Network	Third party (operator)	-	Via network To anyone having a valid subscription to the network	Communication with the mobile/remote system entities
Smart Display (bus stop)	Hardware, Firmware	AMT (Managed by 3rd party)	2G Modem, Microcontroller, Display, SIM card	To AVM through 2G modem. No other known interface	Displays information on transits at the stop and other general information
Control system (for metro station)	Hardware, Middleware, Software, Data	3rd party	Alarms, speakers, network interfaces (ethernet), Physical computing units, Operating System, Application Server, Databases and DBMS, Log files, configuration data	Network interfaces (Ethernet) OS interfaces (SSH , RDP, etc.) Application interfaces (APIs, REST, etc.)	Handles the station assets (electricity, audio diffusion, fire alarms, etc.) Linked with station assets via dedicated link.
Smart monitor (for metro station)	Hardware, Middleware, Software, Data	3rd party	Display, Network connection	To 3rd party control system via dedicated link	Handles messages displayed to passengers at the metro station
Smart Display	Hardware, Firmware	3rd party	Display, Network connection	To metro control system via dedicated link	Displays, outside the metro station,

(for metro station)					information on next train arrivals and other general information
AVM System	Hardware, Middleware, Software, Data, Redundancies	AMT (Managed by 3rd party)	Physical computing units, Operating System, Application Server, Web services, Databases and DBMS, Log files, configuration data	Server hosted on Virtual Machines (windows server) Network interfaces (Ethernet, 2G/4G) OS interfaces (RDP) Application interfaces (APIs, REST, etc.) Database connectors File Transfer Services (e.g., FTP)	Gather events from buses; calculates the transit forecasts; Communicates with Infomobility server and Smart Display
Infomobility Server	Hardware, Middleware, Software, Data, Redundancies	AMT	Computing units, Operating System, Application Server, Web services, Databases and DBMS, Log files, configuration data	Server hosted on Virtual Machines (Linux) Network interfaces (Ethernet) OS interfaces (SSH) Application interfaces (APIs, REST) Database connectors File Transfer Services (e.g., FTP)	Expose to public HTTPS web services. Provides schedules of services, real-time notification to mobile app, real-time transit data and service modifications
Event Database	Hardware, Software, Data, Redundancies	AMT	Computing units, Operating System, Application Server, Web services, Databases and DBMS, Log files, configuration data	Server hosted on Virtual Machines (Linux) Network interfaces (Ethernet) OS interfaces (SSH) Application interfaces (APIs, REST) Database connectors	Filled by specific software by transport operator. Contains all the events that happens on service execution. Provides interface to internal software components to gather the data aboiut events

					and their impact on the service
Service Management System	Hardware, Middleware, Software, Data, Redundancies	AMT	Computing units, Operating System, Application Server, Web services, Databases and DBMS, Log files, configuration data	Network interfaces (Ethernet) OS interfaces (SSH, RDP, etc.) Database connectors File Transfer Services (e.g., FTP)	System that holds all the planned services and interacts with service schedules. Linked internally with the Infomobility System
Ticketing System	Hardware, Middleware, Software, Data, Redundancies	AMT	Computing units, Operating System, Application Server, Web services, Databases and DBMS, Log files, configuration data	Server hosted on Virtual Machines (Linux) Network interfaces (Ethernet) OS interfaces (SSH) Application interfaces (APIs, REST) Web services Database connectors File Transfer Services (e.g., FTP)	Back-end for the ticketing system. Holds API to sell ticket via mobile app and verify ticket via the inspector app. Linked with mobile app and inspector app via HTTPS. Linked with the bank via HTTPS APIs
Subscriptions System	Hardware, Middleware, Software, Data, Redundancies	AMT	Computing units, Operating System, Application Server, Web services, Databases and DBMS, Log files, configuration data	Server hosted on Virtual Machines (Linux) Network interfaces (Ethernet) OS interfaces (SSH) Application interfaces (APIs, REST) Web services Database connectors File Transfer Services (e.g., FTP)	System that holds the information on the active subscriptions and allows to register them into the mobile app, check the validity and renew.

					Linked with mobile app and verificator app via public HTTPS API.
Website	Hardware, Middleware, Software, Data, Redundancies	AMT	Computing units, Operating System, Web Server, Content Management System, Web services, Databases and DBMS, Log files, configuration data	Server hosted on Virtual Machines (Linux) Network interfaces (Ethernet) OS interfaces (SSH) Application interfaces (APIs, REST) Web services Database connectors File Transfer Services (e.g., FTP) Administrator UI User UI	Displays information on service schedules, real-time transit and service modifications Exposed to public via HTTPS; linked via infomobility server via internal HTTP call
Bus-Train (onboard embedded system)	Hardware, Middleware, Software	3rd party	GNSS, sensors (stop - open doors), CAN bus, Microcontroller/Single Board Computer, Firmware/Middleware, Software components, SIM card, Log files, configuration data	Network interfaces (CAN, 2G/4G) Mobile network interface, Proprietary messaging protocols	Linked with AVM System by segregated mobile network
Metro Train (onboard system)	Hardware, Middleware, Software	3rd party	sensors (stop - open doors), Microcontroller/Single Board Computer - Firmware/Middleware, Software components,	Internal network interfaces Proprietary messaging protocols	Linked with Metro control system by segregated network

			Log files, configuration data		
Mobile Application	Software	Developed by AMT, owned by user	Application, Log files, configuration data, Keys	Application interfaces - APIs to Web services GUI Permissions to use from phone: Network, GNSS, Camera to scan Citypass barcode, Microphone (vocal search), NFC reading for quickly register Citypass	Linked with Infomobility server via public HTTPS web service. Linked with Ticketing system via HTTPS web service. Linked with Subscriptions server via public HTTPS web service. Displays information on schedules, real-time transits and real-time service deviations/interruptions. Allow users to purchase tickets and manage their subscriptions
Inspector' s application	Software	AMT / managed by inspector	Application, Log files, configuration data, Keys	Application interfaces - APIs to Web services GUI Permissions to use from device: Network, Camera, NFC reading	Checks the validity of the tickets and subscriptions. Linked with Ticketing system and Subscription service via HTTPS web services
Inspector device	Hardware, Middleware, Software	AMT / managed by inspector	Micro-controller, Camera, Firmware/Middleware, Software components,	Camera - QR reader, NFC, RFID, Mobile network interface (4G), debugging port, User Interface, Web services. Android OS	Runs the verificator app. Main interface to verificator

		Log files, configuration data		
Smartphone	Hardware, user Middleware, Software	Computing system, Smartphone OS, CityPass application, sensors	User Interfaces	Executes the mobile application and it is the main interface to passenger

Table 25: Genova Use-Case asset table

4.5 Genoa Use-Case Cyber Threat Scenarios

The following use cases are indicative as seen from a business point of view and aim to analyse and enforce the security of the mobile application provided to passengers.

These use cases will be used in forthcoming tasks and activities in order to identify vulnerabilities, threats and attack vectors that in turn will help design the technical use-cases that will be presented in WP3. These technical use-cases will provide the required details in relation to the involved CitySCAPE components and the datasets used to identify and respond to cybersecurity incidents.

The aim of the presented use-cases is to improve the confidence of efficient handling of attacks to the mobile application, focusing on the server-side that provides all functionalities. During the attack identification phase identified vulnerabilities, threats and attack vectors will be used to run a risk analysis. Risk analysis findings, together with the deployed CitySCAPE tools, will then be used to mitigate threats.

Attack Scenario Name	***Denial of Service attacks at infomobility Services*** • ***Waiting time at the stop*** • ***Service Schedule*** • ***Waiting time for next train*** • ***@Metro station***
Related Use Case	IS-1 IS-2 IS-3 IS-4
Brief Description	A malicious user (external attacker or malicious insider) performs denial of service attacks to infomobility services in order to prevent/damage the information exchange towards the passengers in the following operational use cases: IS-1: A potential passenger wants to know the waiting time of a bus at a certain stop IS-2: A potential passenger that wants to know the schedule of a public transports service such as bus, metro, etc. IS-3: A passenger approaching the station can see when the next train is expected to arrive at the station. In this way, he can decide if he needs to hurry to catch up the train or go slower. IS-4: A passenger can be reached by several different communications without the need of directly

	interacting with the systems delivering them (displays, audio diffusion, alarms). The denial-of-service attack causes the communication link or application resources to become unavailable – denying access to information through any of the above possible means.
Involved Actors	IS-1, IS-2, IS-3: 1. Passengers 2. Security Officers IS-4: 1. Passengers 2. Metro Station Operator For all cases: Cyber Attacker – external to the system or malicious insider
Involved and affected Asset(s)	IS-1, IS-2: 1. Mobile app 2. Website 3. Infomobility system IS-3, IS-4: 1. Infomobility displays / devices / actuators 2. 3rd party information system
Interfaces, Entry and high-level vulnerable points	For IS-1 and IS-2, the attacker performs DoS attack by using discovered vulnerabilities over three possible assets/entry points: • The Mobile app – i.e., the mobile app for one or many users is being attacked, making it impossible to obtain the requested information from the backend. • The WebSite (the web server hosting the website services) – i.e., network, application or data resources are being overwhelmed by the attacker, denying service to the incoming requests. • The Back-end - both mobile app and website request and get the necessary data from the backend. In this case, the attacker focuses on the backend in order to deny access to all information. For IS-3 and IS-4, the attacker performs DoS by identifying and exploiting vulnerabilities at the 3rd

	party information system – in a similar way with the attacks at the backend and the webserver. It is noted that the system is generally installed at the station (probability of physical access).
Generic Scenario Description	▪ The cyber-attacker launches an attack against network and application resources of either: the website server, the backend or the mobile application for a number of users. ▪ For IS-3 and IS-4, the attack is performed against the 3rd party information system providing data feeds to displays and controls located at a station (bus or metro) ▪ The DDoS attacks have generally a low-cost of entry from the attacker and requires relatively low skills – thus it has high probability of occurrence ▪ Implementation of DDoS attacks on the network may be instantiated with various techniques and through various network layers - from radio access to TCP/IP – by monitoring the network via scanning and reconnaissance and deploying malicious tools on attacker equipment. DDoS can also be performed at the application level, where continuous requests towards a service, a database, etc., can prevent the provision of services and functionalities ▪ The goal of the attack is to deny access to journey and schedule-related information for the passenger, harming the transport user experience and the reliability/trustworthiness of the operator.
Desired Response	Preventing the attack with the performance of complete risk analysis for threats, vulnerabilities and lack of security controls – as well as preparedness of new attack models. In case of an attack, a security support platform ideally detects the incident as soon as possible and warns the security team. This can be done by monitoring for anomalous network activity. Ideally, in case of an event, extra defensive mechanisms or countermeasures may be activated. Incident reporting and notification of 3rd parties and CERTs is desired.

Table 26: Genoa Threat Scenarios - Denial of Service attacks at infomobility Services

Attack Scenario Name	***Manipulation of data at infomobility Services*** • ***Waiting time at the stop*** • ***Service Schedule*** • ***Waiting time for next train*** • ***@Metro station***
Related Use Case	IS-1 IS-2 IS-3 IS-4
Brief Description	A malicious user (external or malicious insider) performs data manipulation attacks in order to harm/damage the journey experience of the passenger or trigger events and alarms to cause chaos at a station. Types of information that may be manipulated in this context – related to the aforementioned operational use cases are: IS-1: A potential passenger wants to know the waiting time of a bus at a certain stop IS-2: A potential passenger that wants to know the schedule of a public transports service such as bus, metro, etc IS-3: A passenger approaching the station can see when the next train is expected to arrive at the station. In this way, he can decide if he needs to hurry to catch up the train or go slower. IS-4: A passenger can be reached by several different communications without the need of directly interacting with the systems delivering them (displays, audio diffusion, alarms).
Involved Actors	IS-1, IS-2, IS-3: 1. Passengers 2. Security Officers IS-4: 1. Passengers 2. Metro Station Operator For all cases: Cyber Attacker – external to the system or malicious insider

Involved and affected Asset(s)	IS-1, IS-2: 1. Mobile app 2. Website 3. Infomobility system IS-3, IS-4: 1. Infomobility displays / devices / actuators 2. 3rd party information system
Interfaces, Entry and high-level vulnerable points	For IS-1 and IS-2, the attacker exploits vulnerabilities over three possible assets/entry points: • The Mobile app – i.e., the mobile app does not provide accurate data, e.g., due to an installed malware, a compromised update, etc. • The WebSite (the webserver hosting the website services) – i.e., the website is "hacked" and provides erroneous information to the users compromising either the integrity of stored or transmitted data. This kind of attack may include a persistent advance threat and may also lead to data leakage from data exchanged by users. • The Back-end with similar types of attacks with the web server, which consequently compromise the data exposed by the mobile app or the website. For IS-3 and IS-4, the attacker, the attacker gains access to the 3rd party information system. The attack may be implemented by exploiting vulnerabilities as weak authentication mechanisms, leaked certificates, weak or no encryption, etc. This scenario includes the possibility of a malicious insider that has access rights but intentionally or by mistake tampers the provided information.
Generic Scenario Description	▪ The cyber-attacker launches an attack against either the website server, the backend or the mobile application. ▪ For IS-3 and IS-4, the attack is performed against the 3rd party information system providing data feeds to displays and controls located at a station (bus or metro).

	▪ The attacker may use sniffers to monitor exchanged messages and analyze traffic or exploit open ports and unprotected interfaces (software or hardware) in order to manipulate data or inject malicious software with similar objectives. ▪ The attack impacts the integrity of the data exported by the backend or the data exposed at the frontends of the platform. The attacks may affect all media of communication with the passengers used by the transport system operator. ▪ A more immediate attack may be caused by a malicious insider that due to access rights has more opportunities to harm the system operation. ▪ The goal of the attack is to annoy/harm/interfere with the journey planning of passengers, and through that have negative impact on the reliability and trustworthiness of the operator.
Desired Response	Preventing the attack with the performance of complete risk analysis for threats, vulnerabilities and lack of security controls – as well as the preparedness of new attack models. In case of an attack, a security support platform ideally detects the incident as soon as possible and warns the security team. This can be done by monitoring for anomalous network activity. Ideally, in case of an event, extra defensive mechanisms or countermeasures may be activated. Incident reporting and notification of 3rd parties and CERTs is desired

Table 27: Genoa Threat Scenarios - Manipulation of data at infomobility Services

Attack Scenario Name	***3rd Party Data Manipulation***
Related Use Case	IS-3 IS-4

Brief Description	The range of provided services may extend through the use of 3rd party information systems and data sources. However, this means that the system operation relies on 3rd parties and the security controls imposed by the 3rd party policies. This scenario investigates a manipulation of the 3rd party information system and the follow-on effects for public transport. According to the operational descriptions, 3rd party information is used in the following use cases: IS-3: A passenger approaching the station can see when the next train is expected to arrive at the station. In this way, he can decide if he needs to hurry to catch up the train or go slower. IS-4: A passenger can be reached by several different communications without the need of directly interacting with the systems delivering them (displays, audio diffusion, alarms).
Involved Actors	IS-3: Security Officers IS-4: Metro Station Operator For all cases: Passengers Cyber Attacker – a malicious insider at the organization that provides 3rd party equipment, software, or data – or an external attacker gaining access to 3rd party resources.
Involved and affected Asset(s)	6. Infomobility displays / devices / actuators 7. 3rd party information system
Interfaces, Entry and high-level vulnerable points	The attack is performed on a 3rd Party information system and cascaded into the system operation. The attack may be a result of a malicious insider or an external attack on system vulnerabilities. The specific entry points are not controlled by the transport authority and cannot be protected. The attack may be possible due to the lack of data validation methods and blind trust in 3rd parties.
Generic Scenario Description	

	▪ An internal or external (authorized or unauthorized) cyber actor manipulates the data in the 3rd information system that may be owned – but not controlled by the transport authority. Data tampering may be implemented with a variety of methods (e.g., SQL injection) or, in the case of an insider, through direct data manipulation. ▪ Due to the fact that the information system is installed into the system – access through open hardware interfaces may also be possible. ▪ The attacker's objective is to provide fake information from the station displays and activate alarms, broadcast audio, etc. ▪ The result of the attack may be the cause of discomfort, confusion, and delays for passengers, which may escalate to something more severe (e.g., panic caused due to a false alarm). ▪ The challenge of the attack is that the manipulation originates on a "trusted" source that is not controlled by the transport authority.
Desired Response	The specific type of risks is proactively taken into account and anticipated through risk analysis and impact assessment. In case of an incident, if possible, the anomalies are captured (through monitoring, data/logs analysis, etc.), allowing the administrators to take appropriate remediation actions. If an external stakeholder detects the security breach at the 3rd party, the platform is notified for the event and takes appropriate action.

Table 28: Genoa Threat Scenarios - 3rd Party Data Manipulation

Attack Scenario Name	***Sends a notification to passengers on service update***
Related Use Case	IS-5
Brief Description	The specific scenario is similar to the aforementioned attacks during IS-1 and IS-2 use cases. Therefore, - Denial of Service Attacks may prevent the transmission of notifications to travelers. - Data manipulation attacks may modify information useful for the passenger.

	Nevertheless, this type of notification is not broadcasted to passengers through displays, or it does not include the information requested by passengers (through the website or the mobile app). Still, it is implemented through personal messages in a communication initiated by the infomobility system. This means that a possible attack may allow the transmission of malicious messages containing, e.g., disturbing messages, links to dangerous/compromised webpages and files, etc.
Involved Actors	1. Passengers 2. Communication Operator 3. Security Officers 4. Cyber Attacker – external to the system or malicious insider
Involved and affected Asset(s)	1. Mobile App 2. Infomobility System 3. Event Database
Interfaces/Entry and high-level vulnerable points	The attacker performs DoS, or data manipulation by using discovered vulnerabilities over three possible assets/entry points: • The Mobile app – i.e., the mobile app for one or many users is being attacked by preventing communication with the backend, or by directly tampering the data exposed by the app. • The Infomobility System - i.e., the server that hosts all the services and information to passengers may be isolated (no notifications sent), or attacked with data manipulation (erroneous notifications sent), or misused to disseminate irrelevant and possibly dangerous data. • The Event Database – i.e., the database where technical issues and service interruptions or deviations are reported, may be unavailable or provides erroneous data. Since the event database is populated with data from AMT personnel, it may be vulnerable due to weak access control or misused certificates.

Generic Scenario Description	▪ The cyber-attacker launches an attack against either the mobile app, the infomobility server and/or the event database. ▪ With an attack on the mobile app, fake notifications directly at the app may appear, real notifications may be denied. The attack may be implemented with the installation of malicious software or weak access and permission control. ▪ With an attack at the infomobility center, the attacker gains control of the notification messages and can drop them, change content or produce and transmit malicious messages. Attacks for data injection and manipulation may be able to exploit possible vulnerabilities at the server side. ▪ With an attack at the event database, fake/false events are imported and eventually transmitted to the passengers. This may be performed by exploiting vulnerabilities for data injection into a database – or by intentional or unintentional data entry from someone at the transport authority personnel. ▪ The goal of the attack is to deny access to the service, modify information useful for the passenger, exploit eventual weaknesses of services to get access to other systems, produce fake alerts, and more. ▪ The passenger journey may be affected and disturbed. Additionally, malicious messages/files may arrive at his/her smartphone with possible cascading effects (installation of virus, data leakage, software malfunctions, and more).
Desired Response	Preventing the attack with the performance of complete risk analysis for threats, vulnerabilities and lack of security controls – as well as the preparedness of new attack models. In case of an attack, a security support platform ideally detects the incident as soon as possible and warns the security team by monitoring the activities (logs, communication messages, etc.). End-user (passenger) report may be utilized, if possible. Assistance to the security administrators for risk management in order to prevent escalation of the

	event due to the nature of the contained malicious information is desired.

Table 29: Genoa Threat Scenarios - Sends a notification to passengers on service update

Attack Scenario Name	***Leakage of personal data*** • ***Ticket from the mobile app*** • ***CityPass subscription dematerialization***
Related Use Case	TS-1, TS-2
Brief Description	The specific scenario concerns attacks on the operational use cases TS-1 and TS-2, where: • (TS-1) A passenger wants to buy a ticket for public transport using the mobile application. The AMT inspectors may ask to verify/validate the ticket using the ticket validation devices and the corresponding applications throughout the trip. • (TS-2) A passenger wants to use his/her CityPass subscription through the mobile application. Throughout the trip, the AMT inspectors may ask to verify the validity of the subscription using the validation devices and the corresponding applications. A malicious user (external or malicious insider) may attack the processes in order to: • Extract personal information for the users/passengers. • Generate fake tickets and subscriptions. • Cancel/deny legitimate tickets and subscriptions. • Deny access in the ticket/subscription acquisition service. • Cause malfunctions in the validation process.
Involved Actors	1. AMT Staff 2. Passengers 3. Banking Services (external to the system) 4. Cyber Attacker – external to the system or malicious insider

Involved and affected Asset(s)	For both TS-1 and TS-2 1. Mobile App 2. Validator Mobile App For TS-1 3. Ticketing System For TS-2 4. Subscription System
Interfaces/Entry and high-level vulnerable points	For TS-1 and TS-2, the attacker exploits vulnerabilities over three possible assets/entry points: • The Mobile app – i.e., typically through installed malware, the mobile app may be used to leak personal user data, perform data manipulation and/or deny access to ticketing and subscription services. • The validator mobile app, where a similar set of attacks may be used in order to possibly leak data from the users (that were/are verified by the app), or cause malfunctions in the verification process (e.g., all tickets/subscriptions are considered valid or all tickets/subscriptions are considered invalid). • The Back-end: o (TS-1) Ticketing system server. o (TS-2) Subscription system server. By exploiting vulnerabilities like weak authentication mechanisms, leaked certificates, weak or no encryption, etc., the attacker is able to steal and/or manipulate data from the backend (generate fake tickets/subscriptions, cancel legitimate registrations, and more).
Generic Scenario Description	▪ The cyber-attacker launches an attack against network and application resources of either: the mobile applications (of passengers and/or AMT personnel) or the backend (ticketing system and/or subscription system). ▪ The attacker uses malicious software, scanners and sniffers to intercept data, detect unprotected entry points, identify usage of weak authentication and/or encryption schemes, perform DoS, and more. ▪ The goal of the attacker is to get access to personal user data (including identities,

	certificates, financial data, and more), produce fake tickets, deny access to the service, etc. ▪ Consequently, the attacks will have a huge negative impact on the reliability and trustworthiness of the operator and financial and legal consequences due to its liability for a possible data theft.
Desired Response	The risks are modelled and analysed and the operators are aware of consequences, impacts and possible security controls. An incident notification platform is available to assist in classification, management and responses and exchange information for such incidents. Prevention of the attack by the discovery of novel attack models or new system vulnerabilities is required. In case of attack, it is desired to detect it as soon as possible, blacklist malicious users, isolate/protect data, automatically activate extra controls, and warn the security team.

Table 30: Genoa Threat Scenarios - Leakage of personal data

Attack Scenario Name	***Using urban train with CityPass subscription***
Related Use Case	TS-3
Brief Description	The specific multi-modal, multi-company scenario concerns attacks on the operational use cases TS-3, where a passenger wants to commute between systems and use the urban train transport with his/her CityPass subscription. A malicious user (external or malicious insider) may attack the processes in order to: • Extract personal information for the users/passengers from either/both system backends. • Generate fake tickets and subscriptions to use the urban train service. • Cancel/deny legitimate tickets and subscriptions. • Deny access in the ticket/subscription acquisition service.

Involved Actors	1. Passengers 2. AMT Personnel 3. Urban train personnel 4. Cyber Attacker – external to the system or malicious insider
Involved and affected Asset(s)	1. Subscription System 2. Urban Train Validation System
Interfaces/Entry and high-level vulnerable points	For TS-3, the attacker exploits vulnerabilities to gain access to the back-end systems of the two organizations – or intercept the communication between them. By exploiting vulnerabilities like weak authentication mechanisms, leaked certificates, weak or no encryption, etc., the attacker is able to steal and/or manipulate data from the backend systems.
Generic Scenario Description	▪ The cyber-attacker launches an attack against network and application resources the backends of the two organizations. ▪ The attacker uses malicious software, scanners and sniffers to intercept data, detect unprotected entry points, identify usage of weak authentication and/or encryption schemes, perform denial of service attacks, and more. ▪ The goal of the attacker is to get access to personal user data (including identities, certificates, financial data, and more), produce fake tickets in order to use the urban train services, deny access to subscription systems, etc. ▪ Consequently, the attacks will have a huge negative impact on the liable party and may harm the relationship between the organizations.
Desired Response	The risks are modelled and analysed and the operators are aware of consequences, impacts and possible security controls.

	An incident notification platform is available to assist in classification, management and responses and exchange information for such incidents. Incident exchange between 3rt parties, cooperative peers and CERTs is desired. In case of attack, it is desired to detect it as soon as possible, blacklist malicious users, isolate/protect data, automatically activate extra controls, and warn the security team.

Table 31 Genoa Threat Scenarios - Using urban train with CityPass subscription

5 CONCLUSION

Deliverable 2.1 has identified the use-cases in the Genoa and Tallinn multimodal transportation ecosystem. The use-cases and the cybersecurity threat scenario analysis will serve as important inputs to the dependent CitySCAPE deliverables identified in the introduction. The use-cases exhibit multimodal transport with the interconnection of traditional public transport with autonomous vehicle shuttles in the Tallinn use-case. Also, the system-of-system interaction to support electronic ticketing and digital information services across multimodal public transportation in the Genoa use-case. The cyber threat scenarios identified threats against communication and application interfaces and against essential service providers, which have cascading impacts in the transportation ecosystem.

6 REFERENCES

1. Wang, R .; Sell, R .; Rassõlkin, A .; Otto, T .; Malayjerdi, E. (2020). Intelligent Functions Development is an Autonomous Electric Vehicle Platform. Journal of the Machine Engineering, 20 (2), 114–125. 10.36897 / jme / 117787 .
2. Merekas 2021, Public Transport Planning Solutions, accessed 10 February 2021, https://www.merakas.lt/
3. Ridango 2021, Ridango Mobility Solutions, accessed 10 February 2021, https://ridango.com/
4. Abasi-amefon O. Affia 2019, *Assessing the NFC Unlock Mechanism of the Tartu Smart Bike Share System*, Tartu University, accessed 20 February 2021, https://kodu.ut.ee/~arnis/bikeshare_nfc.pdf