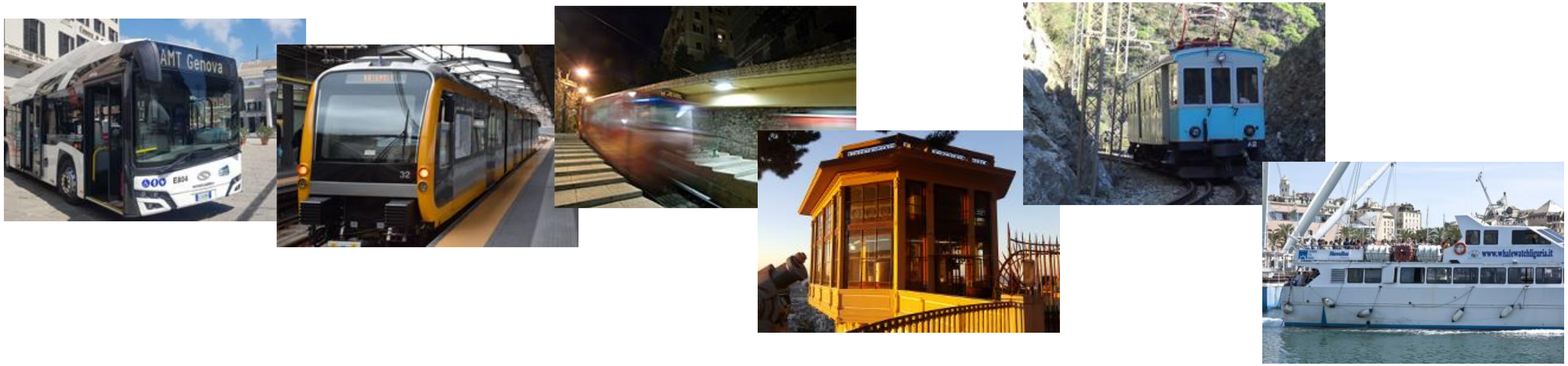
Protecting Data and Privacy in public transport sector: the CitySCAPE project

Fabio Podda – Project Manager AMT Genova SpA
Liivar Luts – Project Manager Tallin Transport Department

Who we are:
Azienda Mobilità e Trasporti S.p.A.

- Public transport company for the metropolitan area of Genoa
- Owned by Genoa Municipality (majority shareholder)
- Handling all the public transportation services of the Municipality of Genoa
  - ✓ **From 2021: handling the public transportation of the metropolitan area of Genova**



Who we are:
Tallinn Transport Department

- We direct the development of Tallinn city transport and mobility management and ensure smooth, fast, safe and environmentally friendly transport in the city.
- Main tasks: public transport, traffic management, parking, taxi service and shared mobility, strategic plans (SUMP).
- Subdepartment of City of Tallinn (operate within the City Border)

Tallinn
Transport Department

2/5/2023

Project at a Glance

- **Call identifier**: H2020-SU-DS-2019
- **Topic**: SU-DS05-2018-2019 - Digital security, privacy, data protection and accountability in critical sectors
- **EC Funding:** 4.998.057,88 €
- **Duration**: 36 months
- **Consortium**: 15 partners
- **Coordinator:** Institute of Communication and Computer Systems (ICSS), Greece – Dr. Angelos Amditis (a.amditis@iccs.gr)
- **Learn more**: www. cityscape-project.eu
- **Join us**: @EUCityscape CitySCAPE Project

Cybersecurity and multimodal transport: The Challenges

- Realization of ***truly*** interconnected transport systems
- Need for ***globally cyber-secure*** systems
- The mosaic of ICT services integrated over interconnected infrastructures makes it increasingly vulnerable to cyber-attacks
- Personal hand-held devices of users increase the system's attack surface
- Transport services relate to other NIS Directive areas that scale-up relevant cybersecurity and security-assurance challenges.
- Authorities' collaboration is needed

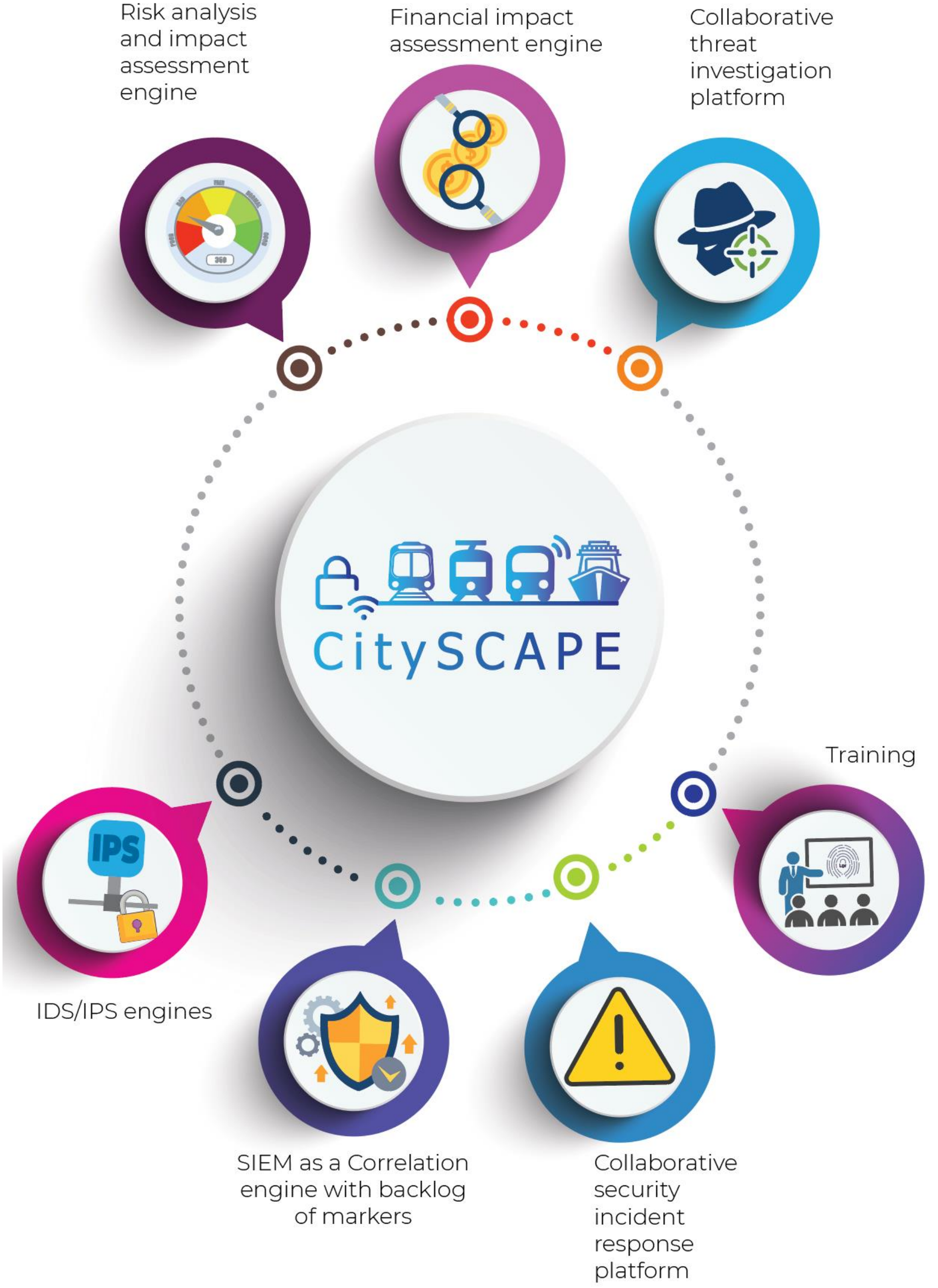
CitySCAPE Objectives

- **Enhance** cybersecurity technologies in the multimodal passenger transportation ecosystem at city-level addressing users and data privacy concerns
- **Introduce** risk analysis tools to identify threats and their propagation mechanism focusing on transport/ digital infrastructure but also relevant in other NIS Directive critical sectors and assess the impact of a potential attack
- **Improve** the proactive approach of handling cybersecurity challenges and actively contribute to the predictability of threats in (regional) multimodal transport systems
- **Enhance** end-user engagement towards the definition and provision of multimodal passenger transport requirements about digital security, privacy and personal data protection

CitySCAPE Objectives

- Further **strengthen** the role of CERTs/CSIRTs by providing them with direct/real-time informative notifications about observed cybersecurity incidents and facilitate the collaborative investigation of incidents in line with the NIS Directive
- Significantly **contribute** to multimodal transport standards and gain experimental evidence on the feasibility of security labelling in city-level multimodal transport
- **Showcase** and **validate** the CitySCAPE solution efficiency in large scale pilot demonstrators involving all relevant entities and digital infrastructure of transport providers, under use cases of interest
- **Analyze** and **outreach** the multimodal transport security market to maximize the CitySCAPE footprint and exploitation.

CitySCAPE Solution


Risk analysis and impact assessment engine
Financial impact assessment engine
Collaborative threat investigation platform
CitySCAPE
Training
IDS/IPS engines
SIEM as a Correlation engine with backlog of markers
Collaborative security incident response platform

CitySCAPE Pilots

- Main goal: to test developed solutions in real context using real-life scenarios
- 2 pilot sites have been chosen to test the CitySCAPE tools developed throughout the Project

City of Tallinn (Estonia)

City of Genoa (Italy)

Tallinn Pilot

The Tallinn pilot focused on:

- Bringing an AV shuttle bus to the streets of Tallinn as a cyber-security exercise, where a set of simulated cyber threats towards the vehicle’s tele-operation and fleet management systems, as well as to their interface with the ticketing services will be pursued
- Setting-up simulation demo environment for testing and validation of services and network.
- Secure integration of last-mile AV shuttle bus to the public transport of Tallinn, including ticket validation, transport planning, etc. following demand-driven conce

- **Tallinn pilot is focusing** on future technology implementation for the city’s public transportation system as cybersecurity exercise and test case for the near future technology.

Tallinn Pilot

CitySCAPE

- **Main goal**: validate CitySCAPE tools in the Mobility-As-A-Service (MaaS) integration with Tallinn public transportation
  - Information to passengers
  - Ticketing
  - Running AV shuttle

- **Assets** to be involved
  - Mobile Application and back-end services
  - HMI Ticket validator
  - AV shuttle OBU
  - Network devices
  - Road Side Unit (RSU)

- **Different class of users** to take into consideration
  - AV system operaator
  - Real-time system operator
  - Passengers

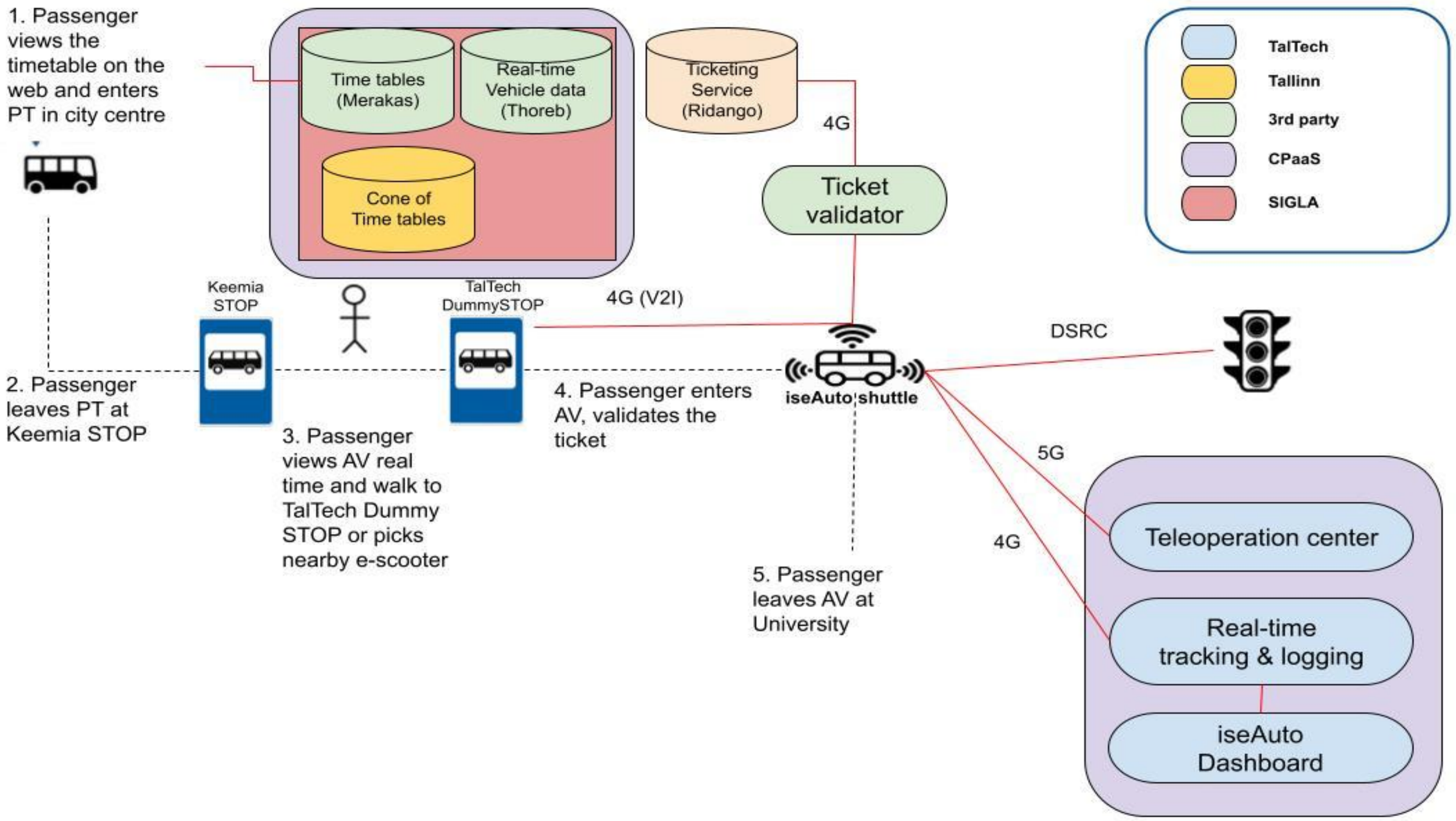
- Pilot has started on **july 2022** and has ended on **august 2022**

Tallinn Pilot

CitySCAPE

Tallinn pilot live demo:

- ○ Test-case 1: AV Shuttle Network Communication
- ○ Test-case 2: Integrity of RSU
- ○ Test-case 3: Ticketing system
- ○ Test-case 4: GNSS spoofing
- ○ Test-case 5: Transport Data Integration


1. Passenger views the timetable on the web and enters PT in city centre
Time tables (Merakas)
Real-time Vehicle data (Thoreb)
Cone of Time tables
Ticketing Service (Ridango)
4G
Ticket validator
TalTech
Tallinn
3rd party
CPaaS
SIGLA
Keemia STOP
TalTech DummySTOP
4G (V2I)
DSRC
2. Passenger leaves PT at Keemia STOP
3. Passenger views AV real time and walk to TalTech Dummy STOP or picks nearby e-scooter
4. Passenger enters AV, validates the ticket
iseAuto shuttle
5G
4G
5. Passenger leaves AV at University
Teleoperation center
Real-time tracking & logging
iseAuto Dashboard

Tallinn Pilot

- Test Case 1: Availability of AV Shuttle Network Communication
  - An attacker external to the multi-modal autonomous transportation platforms, scans the AV Shuttle Network. The adversary then targets the network link between the autonomous transport and its remote control/teleoperation station (teleoperation network), with a DoS attack (Syn Packet flooding).
- Test Case 2: Integrity of Multi-Modal Intelligent Road Sign Infrastructure
  - 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.
- Test Case 3: Fraudulent manipulation of the Payment Validation System
  - 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.
- Test Case 4: Integrity of GNSS System
  - An external attacker uses GNSS spoofing equipment to generate false GNSS locations which are received by the city transport mode and/or AV Shuttle.
- Test Case 5: Transport Data Integration with Mobile Application (SIGLA Move)
  - A vulnerability in the application is able to manipulate the transportation data used for passenger services.

Tallinn Pilot results

- Tallinn pilot execution **was successful**
- **Testing scenarios** executed validating all the CitySCAPE tools initially foreseen
- **CitySCAPE toolkit** can produce the expected results for detection of cyber-attacks and enhanced incident response in the multi-modal transportation environment, involving collaboration with the CERT partner
- **Better understanding** about diferent cyber-security challenges and knowledge to require compliance with the terms, when allowing various MaaS service providers to join Tallinn Transport ecosystem.

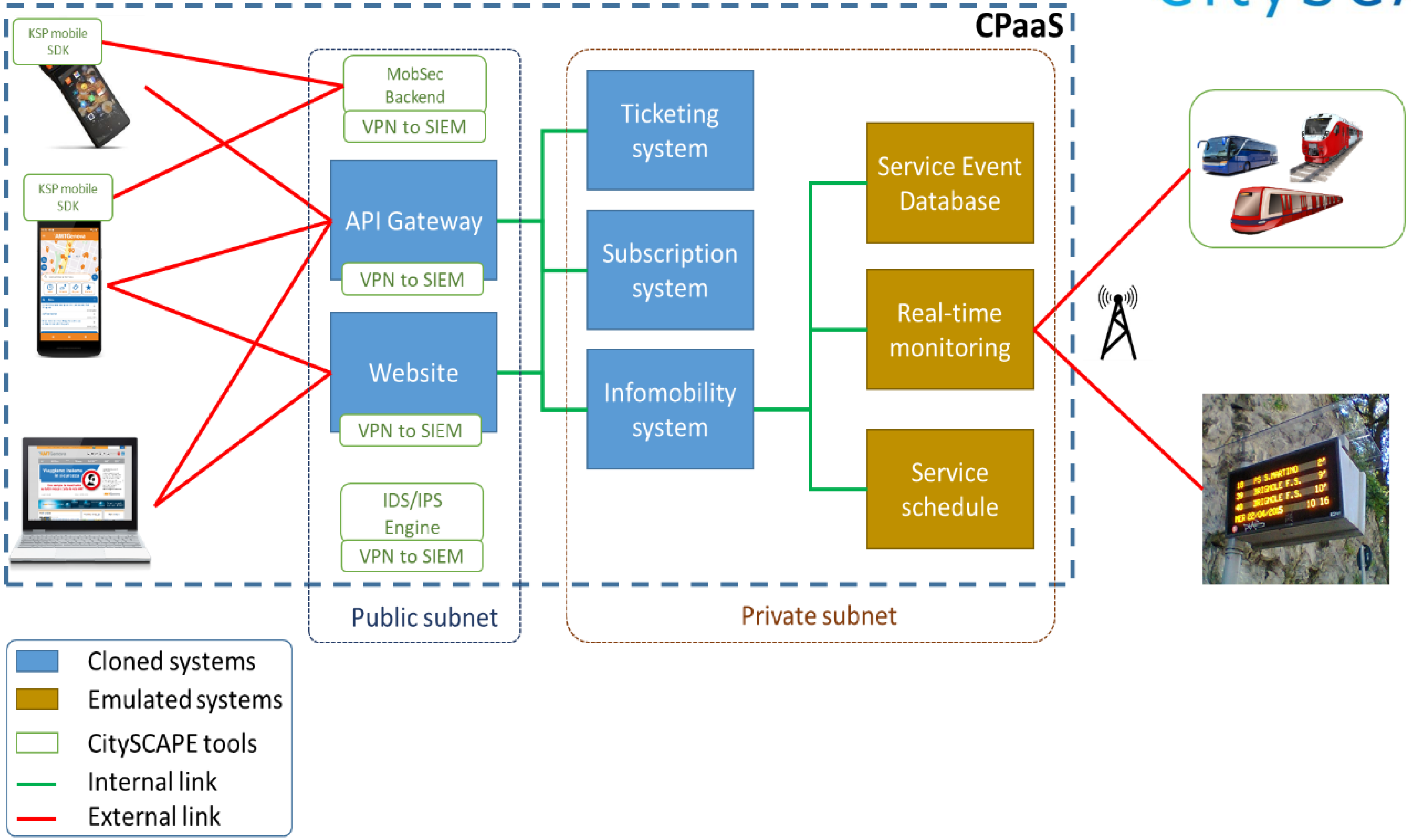
Genoa Pilot

CitySCAPE

- **Main goal**: validate CitySCAPE tools in the Genova public transportation context
  - Information to passengers
  - Digital ticketing
- **Two** main asset classes to be considered
  - **Mobile Application**, **website** and **back-end services**
  - **Informative panels**, **displays**, etc.
- **Two** different class of users to take into consideration
  - AMT personnel
  - Passengers

- Pilot has started on **november 2022** and has ended on **february 2023**

System under test



Genoa Pilot Activities

- 6 Public sessions for disseminating the project and conduct on-field tests with passengers
  - ✓ School students
  - ✓ University Students
  - ✓ Citizens
  - ✓ Stakeholders & local institutions

Genoa Pilot Activities

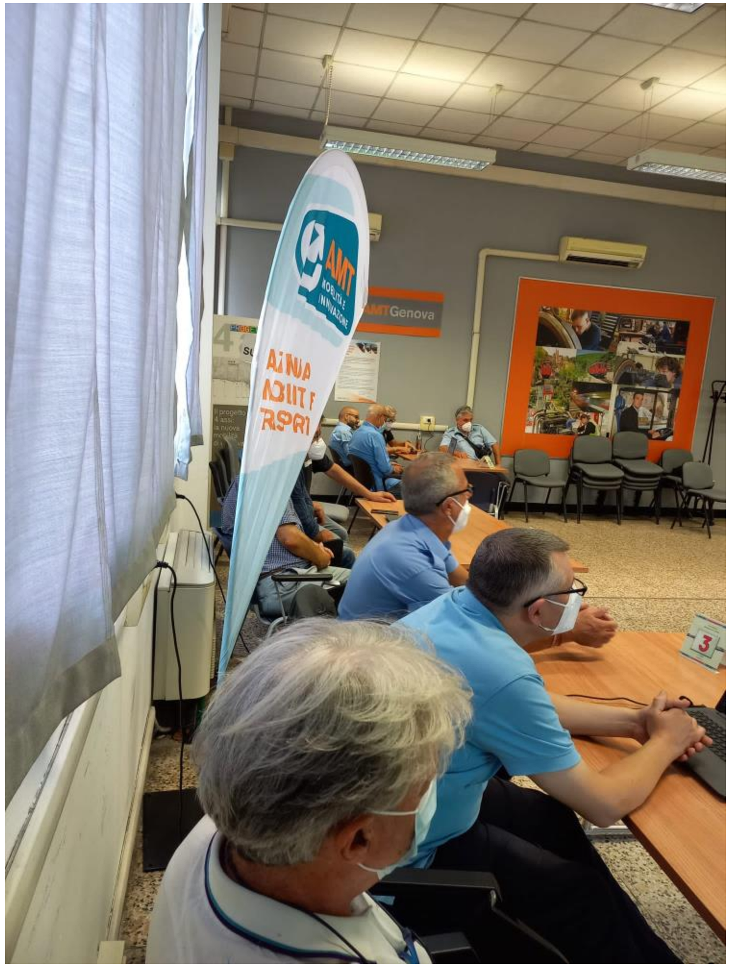
- 5 testing scenarios in order to cover all the pilot use cases
  - ✓ *Cyber threats on Mobile Application*
  - ✓ *Cyber threats on Ticket Inspector's Application*
  - ✓ *Attacks on the resources to make them unavailable*
  - ✓ *Attacks on the resources to manipulate them*
  - ✓ *Attacks on the resources to exploit known vulnerabilities*

- Hands-on session with PTO's end-users in order to evaluate the tools
  - ✓ Getting feedbacks
  - ✓ Assess the adherence of the tools with the initial requirements

Genoa Pilot results

- Genoa pilot execution **was successful**
- **Testing scenarios** executed validating all the CitySCAPE tools initially foreseen
- **Public demonstration/dissemination sessions**
    - ✓ over **300** people involved in total
    - ✓ **70** complete questionnaires collected directly from passengers/citizens
- **Direct involvement of PTO** (i.e. AMT personnel) in the pilot validation process

Training for PTO internal Staff



- More than 200 people involved (more to come)
- About 2 hours sessions
- 3/4 people teams
- 5 teams per session

✓ Involve
✓ Have fun
✓ Reflect

➢ **Produce Awareness and training**

Serious Games for passengers

End Users

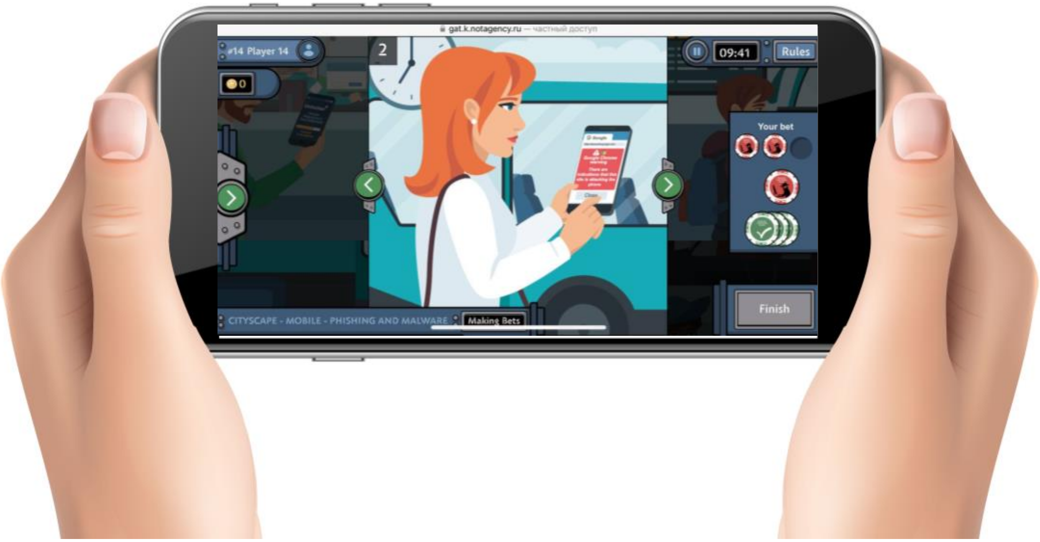
Passengers of multimodal local public transport.

Topics

- ✓ Confidential information.
- ✓ GDPR (data subject perspective).
- ✓ Phishing.
- ✓ Malware

Training Structure:

- ✓ 4 awareness campaigns, one for each topic.
- ✓ Each campaign will include 4 zones related to the topic
- ✓ Each campaign should take the individual passenger between 4 and 7 minutes approximately.



Any questions?

Thank you!

✉

fabio.podda@amt.genova.it

Liivar.Luts@tallinnlv.ee

This project has received funding from the EU's Research and Innovation programme Horizon 2020 under grant agreement No 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.