Project at a Glance

- **Call identifier**: H2020-SU-DS-2019
- **EC Funding**: 6 293 011,25 €
- **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

29/9/2022
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

CitySCAPE introduces innovative risk analysis techniques and orchestrates a number of software solutions to realize an interoperable toolkit that seamlessly integrates to any multimodal transport system.

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.
CitySCAPE Solution
Impact

CitySCAPE

✓ will offer the **concrete technical basis** for a unique opportunity of an efficient collaborative threat investigation among a broad set of CERTs/CSIRTs by introducing a **platform capable of sharing information coming from different sources** and therefore achieve the maximization of the CSIRT network added value.

✓ will allow an **accurate identification of so-far under-explored/hidden privacy risks** serving the in-depth application of privacy-by-default principle and GDPR regulation in all city-level transportation stakeholders.

✓ will **introduce and validate an agile concept of a standalone interoperable solution** to manage current cybersecurity/privacy risks across complex interconnected infrastructures.

✓ will **estimate the attack impact on both technology and financial terms** that will drive a cost-benefit analysis on potential further investments to cybersecurity and privacy countermeasures.

✓ will provide a scheme for **cybersecurity labelling** for City-level multimodal travel.
Impact

CitySCAPE

✓ will address related security issues of mobile devices, increasing passengers’ safety in city-level transport

✓ will identify and track the potential path of a cyber-attack across the whole multimodal transport chain showcasing how an attack may unexpectedly affect modules that are not directly connected to its entry point

✓ will immediately strengthen the CERTs/CSIRTs link to the transportation stakeholders

✓ will promote best practices in cybersecurity management solutions to the multimodal transport community and through training of security experts will seek to communicate their value and thus, increase their acceptance

✓ will fill the gap in security labelling showcasing the solid basis of a mature EU market and rendering the compliance to standards a clear path for commercial growth
Standardisation and security in multi-modal

Thierry Hénault
Project Manager
CS GROUP
Aix-en-Provence France
Multi Modal transport systems vs Cybersecurity

• ITS sector evolution, revolution
  • Societal
  • Technical
    • Accessibility
    • New modes
    • MaaS
  • Regulation

• CyberSecurity
  • From „Niche domain“ for experts
  • To Mainstream domain
2 worlds of Standardisation

• **ITS**
  - CEN
    - Transmodel
    - SIRI
    - NeTEx
    - ...
  - Private efforts
    - Mobility Data Suite
      - GTFS
      - GTFS/RT
      - GBFS

• **Cybersecurity**
  - ISO Efforts
    - ISO 27000 serie
    - Common Criteria
  - European Effort
    - ENISA
      - EUCS
  - National Efforts
Multi modal Transport Systems (MTPS) specificities

- Multiples types of interfaces
Multi modal Transport Systems specificities - Basic Assets

- MPTS system specificities analysis on a Cybersecurity perspective
Multi modal Transport Systems specificities:
Cybersecurity Analysis

“Market Survey”
- Labelling
- Public Transport Standards
- CyberSec Standards

MPTS Specificities
- Business / functions / Technical identification
- Vulnerabilities identification
- MTPS Specific requirements elicitation

Recommendations for labelling
- Considering Existing labelling process
- Specific MPTS requirements
- Dedicaded Security Assurance Methodology

Proposal for MPTS CyberSec Standard
- Addendum to existing Standards
- Based upon Specific MPTS requirements
Thank you!

Smart and Sustainable Mobility for all.

EUROPEAN CONGRESS
TOULOUSE
30 May - 1 June 2022
Any questions?

Thank you!

Thierry Hénault – CS GROUP

thierry.henault@csgroup.eu