E-CORRIDOR
Edge Enabled Privacy & Security Platform For Multi Modal Transport

# D9.3

# Second Exploitation and Dissemination Report

## WP9 - Exploitation, Dissemination, Communication and Standardization

**E-CORRIDOR**

*Edge enabled Privacy and Security Platform for Multimodal Transport*

Due date of deliverable: 30 May 2021
Actual delivery date: 15 June 2022

Version 2.0

*Responsible partner: WIT*
*Editor: Christine* O'Meara
*E-mail address:*
*Christine.OMEARA@WaltonInstitute.ie*

| **Project co-funded by the European Union within the Horizon 2020 Framework Programme** | | |
|---|---|---|
| **Dissemination Level** | | |
| **PU** | Public | **X** |
| **PP** | Restricted to other programme participants (including the Commission Services) | |
| **RE** | Restricted to a group specified by the consortium (including the Commission Services) | |
| **CO** | Confidential, only for members of the consortium (including the Commission Services) | |

*The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883135.*

**Authors:** Christine O'Meara, Tom Walsh, Tommy McDonald (WIT)

**Approved by:** Fabio Martinelli (CNR)

**Revision History**

| Version | Date | Name | Description |
|---|---|---|---|
| 0.1 | 20/05 | Christine O'Meara (WIT) | Table of Content (TOC) |
| 0.2 | 01/06 | Christine O'Meara (WIT) | Dissemination activities, final phase, Exploitation update on key outputs and activities in phase 2 |
| 0.3 | 03/06 | Tommy McDonald (WIT) | Updated dissemination activities from current reporting period. |
| 0.4 | 08/06 | Tom Walsh (WIT)<br>Tommy McDonald (WIT) | Updated social media, events and publications from current reporting period |
| 0.5 | 09/06 | Christine O'Meara (WIT) | Further exploitation updates |
| 0.6 | 09/06 | Christine O'Meara (WIT) | Dissemination & exploitation updates |
| 0.7 | 09/06 | Tom Walsh (WIT) | DMP Update |
| 0.8 | 09/06 | Christine O'Meara (WIT) | Table of Tables, Table of Figures, Intro, Formatting |
| 1.0 | 12/06 | Christine O'Meara (WIT) | Address Stefano comments |
| 1.1 | 13/06 | Fabio Martinelli (CNR) | Review and additional CEA/ DIG contributions |
| 2.0 | 16/06 | Christine O'Meara (WIT) | Final edits |

# Executive Summary

This document reports the dissemination, communication, exploitation and standardisation activities of E-CORRIDOR in the second project year. The project has defined its first Exploitation and Dissemination Plan in D9.1, describing the set of strategies and approaches for enlarging E-CORRIDOR's impacts. This report will summarise the progress in Work Package 9, in particular focusing on dissemination, communication and exploitation aspects.

# Table of Contents

# 1. Introduction

This report documents progress on dissemination, communication and exploitation activities for the period since the first review, June 2022 until May 2022. From a dissemination and communication perspective, the emphasis has switched from project awareness to communicating specific learnings or knowledge. In particular, at this stage of the project, there was been some strong showcasing of research results and learnings from academic and technical partners. Conference presentations have highlighted key results in, for example, intrusion detection or advanced encryption techniques, with relevance to the transport domains at events that attract both academic and industrial participants. This deliverable summarises key dissemination activities for the period and recognises the importance of further engaging a wider audience the upcoming period. Specific plans for engaging the industry and commercial sector are included where the emphasis will be on demonstration and promotion of the project outputs and their application. The deliverable also summarises key exploitation related activities of the partners over the current period, as well as initiation of the next phase of exploitation work which focusses on a deeper elaboration of the commercial proposition of the E-CORRIDOR platform.

# 2. Dissemination and Communication

## *Promotional materials*

This section will report the dissemination and communication activities of the project in generating dissemination materials and conveying E-CORRIDOR messages to targeted audiences through different channels.

### Summary of Pre-Existing Collateral & Promotional Material

Pre-existing collateral are made available to the project partners on the E-CORRIDOR websites under 'Resources' which include all logos and brand guidelines to follow to keep consistent strong design representing the project throughout all areas for Partners to create themselves if they have internal design teams and resources.

All partners have been made aware WIT is available to design any and all promotional material for any events they wish to attend.

Current resources supplied are as follows:

- E-CORRIDOR brand guidelines documentation
- All logo types available to download in original design format .ai files for partners to use with their own internal design teams
- All logos created - Screen ready, Print Ready, with or without taglines and horizontal and vertical orientated and available in different file types .jpg, .png. These are ready to use with any document created by partners and available to download off Resource page on E-CORRIDOR website
- Project flyer and brochure
- E-CORRIDOR PowerPoint template
- E-CORRIODR PowerPoint project dissemination deck
- A template demo video for all Partners is also available on request to guide all WP on creating their own Demo videos

### New Promotional Materials

All Partners have been made aware that WIT is available to design any and all promotional material for any events they wish to attend.

- Full video creation is also available to any WP Partner on request.
- A Project overview E-CORRIDOR promotional video was created and is available by all partners for promotional material. It is also available on the E-CORRIDOR websites home page to view and YouTube.
- Animated E-CORRIDOR logo video intros and outros are readily available from WIT Creative Design Team for any demo or video content needed for promotion. Currently, WP lead partners are working on demonstration videos and collaborating with WIT to wrap the videos in the aforementioned intro/ outro.

- Upcoming events which will be attended by partners have been added the the E-CORRIDOR website events page
- Publications and Journals have been updated on the E-CORRIDOR website

A new Pull Up Banner has been developed as requested to support increased event attendance (see below)


Figure 1 Pull Up Banner

## *Dissemination & Communication Activities & Outcomes*

### Events, Conferences & Publications.

Table 1 summarises the most recent events attended by E-CORRIDOR partners. Links to publications are provided here on the E-CORRIDOR website and a list of most recent publications is in Table 2. The final phase of the project will work to enable green access for any publications that are not currently available on open access.

Table 1 - Events

| Event | Consortium Participant (s) | Presentation Topic (s) | Audience |
|---|---|---|---|
| PDP Conference 2022 – International Event on Parallel Distributed and Network-Based Processing with Special sessions including on 'Security in Parallel, Distributed and Network-Based Computing'<br><br>E-CORRIDOR presented 3 x papers illustrating key threat and privacy management technologies and approaches developed in the project with respect to the automotive domain. | CNR, FhG | Anomaly Detection-Decision Tree-Based Rule Derivation for Intrusion Detection I Safety-Critical Automotive Systems<br><br>Automotive Privacy – Towards a Privacy-Aware Electric Vehicle Architecture<br><br>Security Patters – SECPAT: Security Patterns for Resilient Automotive EE Architectures | RPOs/ Academic Enterprise including transport (e.g. Boeing), Computing (e.g. Intel), Cybersecurity CSPS |
| ARES 2021 – 16th International Conference on Availability, Reliability and Security with sessions of particular relevance including 'Threat Detection' and | CNR | Malware Analysis – SteælErgon: A Framework for Injecting Colluding Malicious Payload in Android Applications | RPOs & Industry Practitioners |
| SECRYPT 2021 – 18th International Conference on Security and Cryptography | FhG, CNR | Malware Analysis – Mobile family Detection through Audio Signals Classification | Academia Industry Government |

| | | | |
|---|---|---|---|
| RTX internal global event on aerospace, cyber analytics and intelligence service (Attendees - >1,100) | UTRC | Presentation of E-CORRIDOR platform within avionics security track, in particular the AT pilot activities. | Internal global corporate audience |
| Intl Conf on Parallel & Distributed Processing with Applications | CNR | Cybersecurity, Deep Learning, Obfuscation, Android | Academia, Industry |
| ACM International Symposium on Blockchain and Secure Critical Infrastructure | CNR | Security and privacy, Formal methods and theory of security, Networks security, security protocols | Scientific |
| European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning | CNR | Deep Learning, Cybersecurity, Call Graph, Machine Learning | Scientific, Industry |
| 2 x 2021 Virtual TCG VSWG Workshop on Securing the Charging Infrastructure of Electric Vehicles (Follow-Up) (Attendees – 80 per event) | FhG | Security enhancements to charging protocols | Scientific, Industry - Automotive, Public/ Gov |

Additionally, WIT is participating in IOT week on 20 to 23 June in Dublin. WIT will have a stand showcasing many of its key projects including E-CORRIDOR. There are several thematic areas of interest including 'IoT Markets and Applications in Industry, Agriculture & Smart Communities'. A large participation is expected for this in-person event with previous conferences attracting strong participation, particularly from Industry, but also Research and Government.

Table - Publications

| Title | Authers | Publication Details |
|---|---|---|
| A Semi-Automated Explainability-Driven Approach for Malware Analysis through Deep Learning | Iadarola, G., Casolare, R., Martinelli, F., Mercaldo, F., Peluso, C., & Santone, A. | Publication presented at 2021 International Joint Conference on Neural Networks (IJCNN) |
| Mobile Family Detection through Audio Signals Classification | Casolare, R., Iadarola, G., Martinelli, F., Mercaldo, F., & Santone, A. | Publication presented at SECRYPT 2021 |

| | | |
|---|---|---|
| Analyzing and Securing SOME/IP Automotive Services with Formal and Practical Methods | Zelle, Daniel (FhG) and Lauser, Timm and Kern, Dustin and Krauß, Christoph (FhG) | Publication presented at the 16th International Conference on Availability, Reliability and Security (ARES 2021) ***Best Paper Award Recipient*** |
| In-vehicle detection of targeted CAN bus attacks | Florian Fenzl, Roland Rieke (FhG), Andreas Dominik (THM) | Publication presented at the 16th International Conference on Availability, Reliability and Security (ARES 2021) |
| SteælErgon: A Framework for Injecting Colluding Malicious Payload in Android Applications | Casolare, R., Ciaramella. G., Martinelli, F., Mercaldo, F., & Santone, A. | Publication presented at the 16th International Conference on Availability, Reliability and Security (ARES 2021) |
| SECPAT: Security Patterns for Resilient Automotive EE Architectures | Christian Plappert, Florian Fenzl, Roland Rieke (Fraunhofer Institute for Secure Information Technology), Ilaria Matteucci, Gianpiero Costantino, Marco De Vincenzi (CNR) | Publication presented at the 30th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing |
| Towards a Privacy-Aware Electric Vehicle Architecture | Christian Plappert, Jonathan Stancke, Lukas Jäger | Publication presented at the 30th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing |
| Decision Tree-Based Rule Derivation for Intrusion | Lucas Buschlinger, Roland Rieke, Sanat Sarda, Christoph Krauß | Publication presented at the 30th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing |
| Analysis and Evaluation of Hardware Trust Anchors in the Automotive Domain | Christian Plappert, Andreas Fuchs (Fraunhofer Institute for Secure Information Technology), Ronald Heddergott (CARIAD) | Publication presented at the 30th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing |

| | | |
|---|---|---|
| Machine Learning Methods for In-Vehicle Intrusion Detection | Roland Rieke | Strive 2021 (Euro S&P) |
| Machine Learning based Security Analysis Capabilities for multi-modal transport applications (ML-SAC) | Roland Rieke | Seminar on cyber security and privacy for multimodal transport, 1st September 2021 |
| Cyberattack detection in vehicles using characteristic functions, artificial neural networks and visual analysis | Y. Chavalier, F. Fenzl, M. Kolomeets, R. Rieke, A. Chechulin, and C. Krauß | Journal of Informatics and Automation doi: 10.15622/ia.20.4.4 |
| Threatsurf: A method for automated Threat Surface assessment in automotive cybersecurity engineering | D. Zelle, C. Plappert, R. Rieke, D. Scheuermann, C. Krauß | Microprocessors and Microsystems doi: 10.1016/j.micpro.2022.104461 |
| Secure Role and Rights Management for Automotive Access and Feature Activation | C. Plappert, L. Jäger, and A. Fuchs | ASIA CCS '21 doi: 10.1145/3433210.3437521 |

**Online Channels**

Social Media

Twitter Analytics only holds 28 days of Data. In the last 28 days E-CORRIDOR has put out 12 tweets and made 935 impressions(views /interactions with said 12 tweets) as well as having over 1,50 profile visits in the 28th day period.


Figure 2 - Twitter Summary

E-CORRIDOR Website Analytics

The following stats are from the E-CORRIDOR Website for the past year from June 2021- June 2022.

In the 12 months there was a total of 1,816 users to the site with 1,735 being new users who had not visited the site previously. Total page views for the website for this time period was 4,975 through the site.

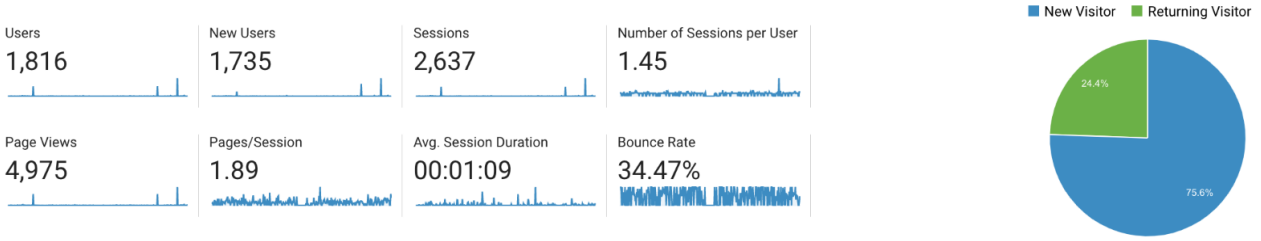


Figure 3 - Website Analytics

**Communication with Related Communities and Projects**

- FhG is actively involved in the Trusted Computing Group (TCG) in particular standardisation activity. Christian Plappert collaborates with TCG Vehicle Services Working Group (VSWG) and contributes to discussions. On topics related to the Trusted Service Manager developed in E-CORRIDOR with presentations at workshops including on securing the charging infrastructure of electric vehicles.
- FhG's Roland Rieke is workhop and programme chair for International Workshop on Privacy and Security of Multi-Modal Transport Systems (IWPSMTS 2022), a leading component of the ARES 2022 conference. Through this workshop and preparatory actions, scientific exchange is ongoing with other EU projects including;
    - Research area Secure Autonomous Driving (SAD) of the National Research Center for Applied Cybersecurity ATHENE which is funded by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts.
    - Project SecForCARS (security for connected automated cars) which is funded by the German Federal Ministry of Education and Research.
    - Project FINESSE (vehicle intrusion detection and prevention in a unified structure for road and rail) which is funded by the German Federal Ministry of Education and Research.
- E-CORRIDOR partners continue to liaise with related communities and projects referenced in D9.2
    - *H2020 Cyberwatching.eu – The European watch on cybersecurity & privacy (https://cyberwatching.eu/).*
    - *H2020 SPARTA (https://www.sparta.eu/)* - Cybersecurity Competence Network, supported by the EU, with the objective of developing and implementing top-tier research and innovation collaborative actions.
    - *CYRANO - CYbeR Awareness diploma (https://www.bologna-airport.it/en/the-company/business/european-projects/?idC=62586).* It is a co-funded EU project managed by the Bologna Airport, Italy (Aeroporto Guglielmo Marconi di Bologna S.p.A.) within the Connecting Europe Facility programme.
    - *H2020 CitySCAPE* (https://www.cityscape-project.eu/).

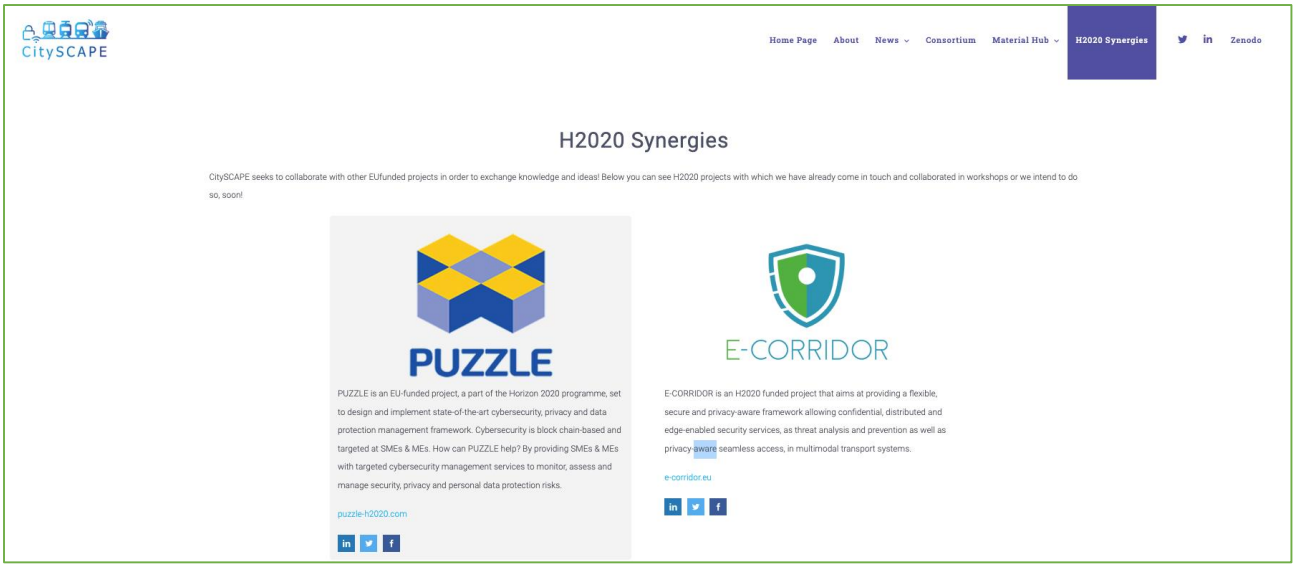


Figure 4 0 CityScape Synergy

## *Dissemination & Communication Plans – Final Phase*

As the project enters the final year, the dissemination and communication effort will switch the emphasis away from promoting project and research awareness to highlighting key project outputs. To date, the activities in this work package have leaned more heavily towards engaging with the research community through extensive publications, scientific exchange and participation at key events. concerted effort in this final phase will be made to engage all other stakeholders including Enterprise & SMEs, ISPs, CSPs, Mobility Service Providers, Mobility Consultancies, Public Sector including transport authorities and Standardization and policy making bodies. This effort will be reflected in the materials, the channels and the messaging. Activities for the final phase will include;

- A press release to mainstream and technical news outlets promoting the project and its key outputs.
- A blog series with at least 1 x contribution from all partners with a focus on industry relevant outputs, particularly related to key technologies and their outputs. The initial pipeline of blog posts is below;

Table 2 – Blog Schedule

| **Topic** | **Contributor** | **Est Publish Date** |
|---|---|---|
| Challenges and solutions for security and seamless authentication services in air-rail multimodal travels | UTRC | Jul 22 |

| | | |
|---|---|---|
| Fully homomorphic encryption and its application for use-cases related with transport context | CEA | Aug 22 |
| Security in Railways :what has been done so far and what remains to be tackled. | DITECFER | Sep 22 |
| Vulnerabilities, Threats and attacks in the mobile, automotive and transportation domain | CNR | Oct 22 |
| Micro incentives: a tool to nudging for sustainable mobility behaviour in multimodal trips | FACT | Nov 22 |

- A series of E-CORRIDOR demonstration videos (one per work package) showcasing technological outputs,
- Three case studies promoting the learnings from the 3 x pilot actions curated and templated by WIT,
- Targeted Industry & Scientific Events including;
    - E-CORRIDOR demonstration in STARS event. STARS [STrategic Alliances boosting Railway SMEs] is a EU COSME-funded project aimed at supporting SMEs from the Railway and Multimodality sectors to adopt Advanced Technologies. The event will take place in November 2022; European SMEs and other relevant stakeholders will be involved in a Hackathon, followed by Matchmaking with providers of solutions suitable to answer key needs. E-CORRIDOR solution will be used for both parts, as tool to address challenges and as commercial solution for the target market.
    - FhG, with CNR and UTRC has organized an International Workshop on Privacy and Security of Multi-Modal Transport Systems (IWPSMTS 2022) https:\www.ares-conference.eu\workshops-eu-symposium\iwpsmts-2022 held with ARES conference in Vienna, Austria. The workshop aims at providing a forum for researchers and engineers in academia and industry to foster an exchange of research results, experiences, and products in the domain of security and privacy for multi-modal transport systems. We will present the advancement on the state of art in these fields and the adoption of developed technologies in several scenarios involving pilots from the domain. Additionally, CEA has made three submissions for talks at the workshop IWPS HTS of this conference about solutions to address use-cases with FHE and ABE in transport related contexts. In total consortium partners will be involved in more than 10 talks and workshops,

  - Tech Connect Live, Dublin, 13 September – This event is targeted at SME and Enterprise level companies with over 5,000 business owners/ key decision-makers expected to be present. There is a substantial cybersecurity stream. WIT will promote E-CORRIDOR with collateral and demonstration videos form its stand at the event,
  - Futurescope, Dublin 21, October – This event is targeted at investors, innovation seekers and business leaders with a focus on identifying collaboration opportunities between start-ups, scale-ups, tech multinationals, innovative Irish tech enterprise and the research community. WIT will promote E-CORRIDOR with collateral and demonstration videos from its stand at the event.
- Additional conference papers in progress include;
  - Paper ('Hybrid approach for anticipating human activities in Ambient Intelligence environments') submitted to IEEE CASE by U-PEC,
  - Paper on Airport - Train pilot to be submitted by U-PEC to ACM Applied Computing (SAC) by Sept 2022.

# 3. Exploitation.

## *Exploitation Introduction*

The overall mission of E-CORRIDOR is to design and provide a flexible, secure and privacy aware framework allowing confidential, distributed and edge enabled security services, as threat analysis and prevention as well as privacy-aware seamless access mechanism in multi-modal transport systems. The E-CORRIDOR framework includes collaborative privacy-aware edge-enabled information sharing, analysis and protection as a service. The project plans to show the applicability of this framework in at least two domains: (i) collaborative and confidential cyber threat management and (ii) seamless access mechanism in multimodal transport systems.

Over the course of the project, exploitation of E-CORRIDOR is considered from the perspective of the framework as a whole as well as its constituent parts which include 3 x infrastructures (DSA, ISI, IAI), a range of tools including trip planners and ID verification, and finally advanced cybersecurity analytics. In this report, firstly an update will be provided on the general exploitation progress from the perspective of individual partners and the components and outputs they are developing. Secondly, an update will be given on the collaborative exploitation effort for the E-CORRIDOR proposition as a whole.

In the first period of the E-CORRIDOR project, some foundational work was carried out to support specific business modelling, development and exploitation activities in subsequent phases.

In D 9.2 4-step an exploitation approach, summarised in Fig 5 below, was identified to coordinate the exploitation activities within the project.

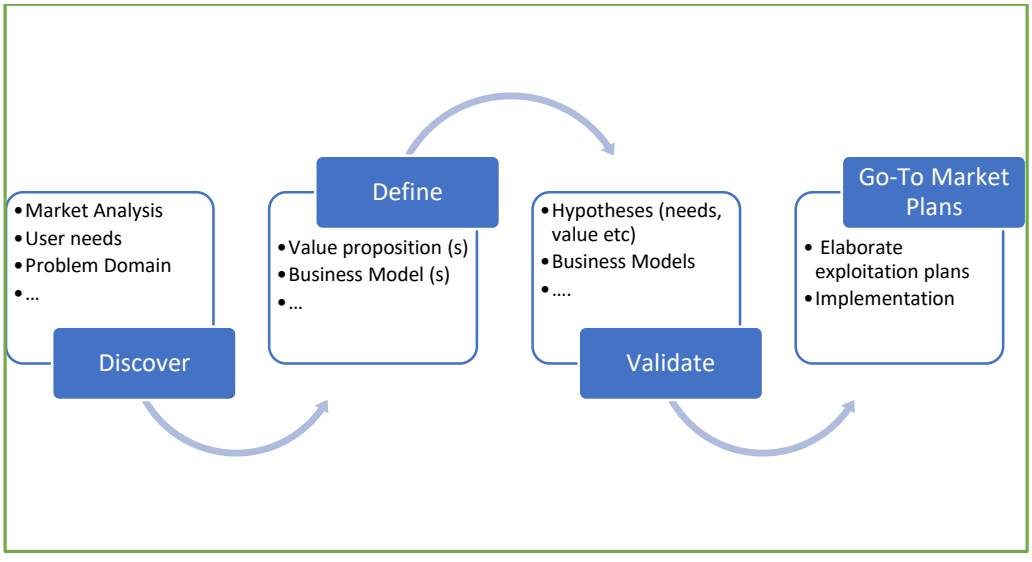


Figure 5 - Exploitation Approach

- **Discovery:** The results of the discovery phase was reported in D9.2 and include business environment analysis, opportunity analysis and a competitive review. In addition to the macro

environmental analysis, several sectors of relevance in the cybersecurity and mobility technologies domains were identified and researched. This research enabled the creation of an updated SWOT analysis and further strategic tools, including Kotler's product levels[1]and Porter's competitive framework[2].

- **Define**: In the most recent period of the project, the DEFINE phase has begun which consists of a series of collaborative exercises to define and refine the E-CORRIDOR value proposition and to advance business modelling activities and validation plans. To date, a very high-level description of the business model for E-CORRIDOR exists and has been updated. This deliverable will summarise the initial steps of this 'DEFINE' effort which is occurring with the involvement of all partners and importantly Industry & SME stakeholders as well as the Exploitation Board and business networks. Additionally, business models will need to be developed for alternative commercial propositions, e.g., subsets of E-CORRIDOR components.

- **Validation**: As part of the DEFINE stage, some validation plans are being developed to enable the testing of hypotheses, models and plans that are being elaborated. Those plans are likely to include pilot feedback, demonstrations and pitch presentations. Feedback from the Exploitation Board and business networks will also support this phase.

- **Go-To-Market / Exploitation Plans** will be elaborated in detail closer to the end of the project. The plans will guide exploiting and commercialising E-CORRIDOR's outputs.

## *Exploitation General Progress Update*

Prior to workshop initiation and following on from an initial exploitation survey in phase 1, a second survey was issued to partners in early 2022. This requested updates including;

- Status updates on work packages, tasks and pilots
- Key learnings/ challenges to date
- TRL at current stage and estimated to market readiness
- Primary users and secondary users of key outputs
- Identification of means to access / use outputs for both primary and secondary users

A direct, structured and intensive approach will be employed in the final phase of the projects as outputs are approaching readiness for validation and pilots are being realised with a view to delivering detailed exploitation pathways and plans

## *Status of Exploitable Results*

Table 4 below summaries the status of the exploitable assets with general good progress being made

[1] P. Kotler , Marketing Management (Fifteenth edition), PEARSON, 2016.

[2] M. Porter, Competitive Strategy: Techniques for Analyzing Industries and Competitors, Simon & Schuster, 1998

Table 3 - Exploitable Results Status

| Exploitation Asset | Category | Exploitation Type | Explanation | Status Update |
|---|---|---|---|---|
| Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) Technologies [CNR] | Knowledge Software | Research | The acquisition of new technologies within the E-CORRIDOR project will allow to compete in the national and international arena. | Prototype version developed and tested. CNR will promote it in the automotive domain – introduction of equivalent solutions recommended bd by UNECE regulations |
| Usage control methodologies and tools [CNR] | Knowledge Documents | Research | The methodologies considered in the E-CORRIDOR project will further enhance the research and development competence of the groups involved making even more competitive in the area. | Prototype developed in general format, adaptable to multiple scenarios |
| Privacy preserving analytics [CNR] | Software Documents | Research | The analytics developed within the E-CORRIDOR project will sprint up the competence of the group that has the possibility to enlarge its visibility in national and international venues | In progress |
| **Automotive security approaches (Trusted Platform Module - TPM / IDS) [FhG]** | Knowledge | Industrial Training Fraunhofer Academy Courses | The Fraunhofer Academy offers specialists and managers outstanding courses of study, certificate courses and seminars based on the research activities of the Fraunhofer institutes.<br>As the leading organisation of institutes of applied research and development in Germany, the primary objective of Fraunhofer-Gesellschaft is to improve information and technology | On hold – no onsite industrial training taking place due to pandemic |

| | | | | |
|---|---|---|---|---|
| | | | transfer from research institutes to industry. | |
| Machine Learning (ML) IDS techniques [FhG] | Knowledge | Lecture | Darmstadt University of Applied Sciences course | Pending subject to available resources |
| **ML test toolset [FhG]** | Software | Commercial | Machine learning modules for intrusion detection security analytics in the multi modal transport domain, e.g., in-vehicle IDS. | In progress with good outcomes |
| **Advancing the Open Source TPM Software [FhG]** | Software | Training Lectures | Advancing the development of the Open Source TPM software that can be integrated into trainings and lectures. | In progress with contributions ongoing to Open Source Software tack |
| **Contribution to Trusted Computing Group (TCG) [FhG]** | Standards | Standard | Introduction of the solution to TCG, possibly resulting in a new standard. | Actively involved in TCG standardisation activities |
| **Multi-modal transport security knowledge Transfer to SMEs DIG** | Knowledge | Industrial Training | Being a Railway Cluster, DIG operates as a driver to transfer E-CORRIDOR knowledge to SMEs operating in the Railway domain in Italy and as well as in other European countries both through the ERCI meta-cluster and relevant EU projects | E-CORRIDOR system and key knowledge are being tracked in the list of Tech-Savvy Solutions mapped by the STARS project (EU COSME programme) to promote connections and potential commercial partnerships with the SMEs operating in the Railway and Multimodality sector targeted by the project |

| | | | | |
|---|---|---|---|---|
| ASI infrastructure, FHE Component, IAI components - driving license checker, IP backlisting, Attribute based encryption protocol),<br><br>[CEA] | Software | Research, Licensing to commercial entities | | Developed and tested in standalone, Current status of components is at TRL5 and is expected to reach TRL 7 by end of project |
| Privacy-preserving analytics and security techniques [UTRC] | Knowledge<br>Software<br>Evaluation on the field (with ADP, and SNCF in the AT pilot)<br>Patent applications | Research<br>Commercial | Privacy-preserving techniques supporting enhanced passenger experience in multi-modal transportation | In advanced stages of development but tests yet to be done |
| Advanced authentication techniques [UTRC] | Knowledge, Patent application | Research | Model-based approach for safety and security in airport authentication systems | In Progress |
| Multi-modal Trip Planning Tool [WIT] | Software<br>Knowledge<br>Patent application | Research<br>Commercial | A multi-modal trip planning tool can predict the best multi-modal travel itineraries for end-users with users' interests and preferences, carbon footprint, price, time and number of connections considered. The software will be the trip planning tool; knowledge will be the routing algorithms and data analytics methods developed. Patent application concerns the commercial application of the asset such as trip planning tool and service for commercial vehicles (e.g., taxi and truck) | Multi-modal trip tool has been developed and includes micro subsidy data, CO2 calculator data and CLEM car hire information. Integration into E-CORRIDOR platform ongoing. |

| | | | | |
|---|---|---|---|---|
| Carbon Footprint Analytics [WIT] | Knowledge | Research | Carbon Footprint Analytics estimates the CO2 footprint in the multi-modal transport system, and is of great importance under the background of the European Green Deal. The research outputs here can be used to support other ITS applications and research. | Current version includes CO2 g/km for various car models and buses |
| Micro-subsidies platform [FACTUAL] | Software | Commercial | FACTUAL is developing a micro subsidies calculation engine which can be plugged on to any Mobility as a Service (MaaS) and Transport Service Provider platform to nudge certain type of travel behaviour, user segment or vehicle used. | Technology advanced and being piloted in multiple locations |

## *Partner Exploitation Updates*

Validation and feedback that can underpin exploitation beyond the lifetime of the project will intensify when pilots have taken place and demonstrations and proof points are available. However, the team is already seeking to leverage project outputs with a philosophy of seeking pre-prototype feedback where possible and monitoring industry/market trends for relevant opportunities or considerations. Some highlights of these efforts are noted below;

- UTRC, which is now merged with Raytheon Technologies is part of a leading global aerospace organisation. It has secured strong interest in its privacy-preserving analytics and security techniques in development in E-CORRIDOR. In particular the Information Management Systems and Services groups are paying close attention to the critical information management and connected ecosystem tools that enable contactless passenger journeys within the airport, as well as the privacy-aware mobile-based enrolment solutions which will be tested in the AT pilot. Furthermore, an invention disclosure related to the privacy-aware analysis of camera feeds is in preparation. UTRC internal stakeholders are also very interested in the token-based authentication mechanisms for safeguarding privacy. UTRC foresees that the E-CORRIDOR's outputs are key tools to deliver a seamless, secure BYOD experience to passengers as well as respond to industrial initiatives such as IATA OneID and IATA NEXTT

  .

- WIT is currently engaging with its Technology Transfer Officer (TTO) to explore exploitation opportunities. The TTO has recommended the filing of an IDF for the multi-modal trip planning tool that is being developed by its software team. The TTO is also supporting promotion of any IP through The EU Knowledge Valorisation Platform and the equivalent National Knowledge Transfer Ireland portal. In addition, exploitation through industry contacts will be explored. For example, mobility technology specialists, Routematch, has its European HQ on the Walton Campus. Walton has completed several commercial engagements with Routematch which itself has recently been acquired by UBER. Consortium partners will of course be able to secure access to the codebase under royalty free license. Furthermore, WIT is involved in a collaboration with Waterford City County Council which is using cameras to monitor heavy traffic entering the city. While the current implementation is focussed on basic monitoring, it is hoped to expand the initiative to equip city planners and administrators with key decision support tools. For example, privacy preserving itinerary planning and carbon footprint analysis – where for example, number and size of trucks and environmental footprint analytics could inform planning

- FhG, based on its work with the ML test toolset, has secured an industrial funded project. At this point it is not possible to give details because of an NDA. Furthermore, FhG will soon participate in a new project on vehicle intrusion detection and prevention in a uniform structure for road and rail where several SMEs are involved. On the standardisation side FhG is actively involved in the Trusted Computing Group, specifically the Vehicle Services Working Group (VSWG) with presentations at workshops on securing the charging infrastructure of electric vehicles and contributions to other topics related to the Trusted service Manager developed in E-CORRIDOR.

- FACTUAL Consulting is actively trying to exploit the microsubsidies platform with the brand Rideal. They have advanced their core engine prototype to a market ready product and the commercial presentation of this can be seen at www.rideal.mobi..Pilots of this technology is ongoing in multiple locations including;

    - Brussels – incentives for last mile micro-mobility
    - Vic, Spain – incentives for last mile logistics
    - Barcelona, Spain – incentives for car pooling to industrial areas

    .
- CNR intends to promote its IDS and IPS prototypes in the automotive domain. These technologies enable the introduction of equivalent solutions recommended by UNECE Regulations.

- CLEM views the homomorphic encryption techniques, when combined with the Data Sharing Agreements, as useful enablers to multi-modal service offerings. Data governance on distributed information system is challenging but with the E-CORRIDOR framework, DSAs are enforceable. With a TRL7 in this area, CLEM believes these technologies will be useful to all multimodal transportation providers, as well as EV charging companies and parking

service providers. In the last phase of the project, CLEM will seek validation and feedback from primary and secondary target users.

- PILDO Labs through its spinout company NEMI aims to exploit some of the E-CORRIDOR framework's capabilities to enhance its Demand Responsive Transit solutions. Nemi is currently supporting the operation of 9 services with a reach of 16,500 travellers.

- CEA has a strong interest in the new cryptographic technologies, especially in fully homomorphic encryption (FHE), and is an active actor in these domains, especially through regular publications. The current contribution to E-CORRIDOR is a real opportunity for CEA to work in this way in a concrete context. CEA has also made three submissions for talks at the workshop IWPS HTS 2022 of the ARES conference and they have all been accepted. These talks are in link with E-CORRIDOR activities on applying recent cryptographic technologies to address use-cases from multimodal transport contexts. In parallel, CEA is defining the role of a FHE-based server that provides a solution to compute on encrypted data for industrial people.

## *DEFINE Workshops*

The workshops have been designed to incorporate key principles of The Lean StartUp[3] movement and underlying methodologies developed by Steve Blank [Customer Discovery Model[4]] and creators of the Business Model Canvas Osterwalder &Pigneur[5]. Key guiding principles include;

a. In order to test and validate business model (s) the underlying hypotheses need to be sufficiently elaborated. Business model descriptions cannot be reduced to simple pricing strategies (e.g. freemium), service delivery models (e.g. SaaS) or customer targets (e.g. B2B).
b. The Business Model Canvas [BMC] offers a useful way of summarising the central value proposition , key inputs required to create the core product/ service and path to market which will realise the value and secure customers/ revenue.
c. Business models can be tested even in advance of a market ready products, by creating detailed hypotheses or specific statements related to product, customers, channels and other categories in the BMC and soliciting feedback from relevant stakeholders including target customers, industry advisors, government agencies or investors.

[3] E. Ries, The Lean StartUp, Penguin Books, 2011
[4] S. Blank, The Four Steps to the Epiphany: Successful Strategies for Products that Win, Wiley & Sons, 2020
[5] A. Osterwalder and Y. Pigneur, Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers, John Wiley & Sons, 2010.

Starting with consideration of the E-CORRIDOR platform as a whole, the workshops were designed with the following key objectives.

- Review & refine the E_CORRIDOR value proposition and elaborate the likely business model(s)
- Develop a set of specific hypotheses that can be used to test/validate both.

A review of the value proposition at this stage of the project benefits from continuous market discovery work, increased understanding of target users which has grown through pilot actions and a deeper appreciation of the technological and sectoral context achieved through scientific research. The workshops include all internal partners and also benefit from the involvement and expertise of key external stakeholders from Industry and public bodies.

Regarding the elaboration of hypotheses, the key to success will be to go beyond superficial statements, for example, 'Transport providers and users are exposed to increasing cybersecurity risks'. By contrast, a more descriptive statement of the problem would give context around potential users booking a multi-modal trip, no. of points of vulnerability or associated risks. Similarly, pricing statements should avoid generic labels such as mid-range, as this isn't testable.

**Workshop No 1**

The first workshop took place on 31 May, 2022 with 30 participants including consortium members and external Industry advisors. The event was promoted by social media, the ECORRIDOR website and via email networks.


Figure 6 - Workshop flyer

The session kicked off with 5 minute pitch presentations from WP leads summarising the key ECORRIDOR outputs to date, highlighting notable platform and solution features as well as status of testing and piloting. This was followed by presentations from the external Stakeholders;

- Dirk- Ulrich Krueger – European Rail Clusters Iniative
- Dora Ramazzotti – Bologna Airport
- Theo Dimitrakos – Huawei

At this point, some open floor discussions took place with Industry advisors offering some useful comments and perspectives on E-CORRIDOR. Some points of interest are summarised below;

- The importance of a seamless experience was repeatedly highlighted with Dirk noting that a seamless experience would help improve the green credentials of both passenger and freight transport with solutions such as E-CORRIDOR enabling passengers and logistics managers choose the greener options.
- The representative from Bologna Airport expressed the desire for airports to be more integrated in transport corridors in a bi-directional / multi directional manner and is open to further engagements.
- Dora Raamazzotti also recommended connecting with ITAIR ISAC of the Italian aviation sector.

- Security and privacy are big challenges that need to be resolved while balancing service delivery and customer experience against threat mitigation. Dora Ramazzotti remarked that there is a desire to access as much data as possible to improve services and manage risk. However, privacy, data sovereignty and access management must be considered. Intelligent data sharing agreements combined with privacy preserving technologies such as homomorphic encryption offer the possibility to address many of these pain points. Additionally, the opportunities in terms of the seamless services that can be enabled by these technologies are exciting, for example seamless reprotection or planning for freight or passengers in the event of service disruption.
- Continued collaboration with this Industry advisors will benefit the exploitation efforts of E-CORRIDOR in many ways including;

    - ERCI has a strong geographic spread and can help with networking including supporting customer, supplier and supply chain engagements
    - E-CORRIDOR will consider whether to make a submission the ERCI Innovation award.
    - E-CORRIDOR will engage with projects highlighted including CONNECT [Ref] and PRECINCT [ref].

The second part of the workshop included a presentation of key outputs from the market discovery phase followed by an elaboration of the process for the DEFINE phase. The key goal was identified as finding evidence that E-CORRIDORs value proposition and business model has found 'the sweet spot of innovation[6]' .

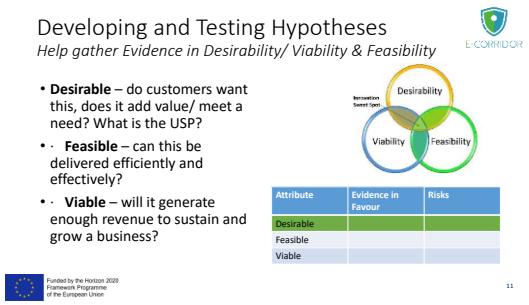


Figure 7 - Innovation Sweet Spot

Initially, the objective is to validate the desirability of E-CORRIDOR with target customers. To this end, the team has started teasing out assumptions related to the E-CORRIDOR product, customer and channels.

[6] https://www.ideou.com/blogs/inspiration/how-to-prototype-a-new-business

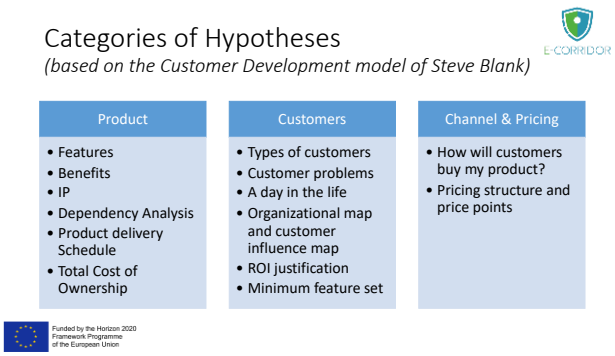


Figure 8 - Business Model Hypotheses

The starting point for these initial hypotheses was the relevant categories, highlighted in green, elaborated in the E-CORRIODOR BMC (see fig 9).

| Key Partners | Key Activities | Value Propositions | Customer Relationships | Customer Segments |
|---|---|---|---|---|
| - National CERTs.<br><br>- Law enforcement authorities.<br><br>- Large enterprise in multimodal transport<br><br>- Large enterprise as technology providers, Research and Technical Development (RTD)<br><br>- CASE mobility providers & supporting services<br><br>- Strong expertise and experiences in Cybersecurity domain<br><br>- Expert communication and dissemination at European level in Information and communications technology (ICT) domain<br><br>- Software houses. | - Security vulnerability information harvesting and propagation.<br><br>- Define of cust DSAs<br><br>- Data collection and privacy-aware data analysis via anonymization & Homomorphic Encryption.<br><br>- Data modelling, algo dev & refinement<br><br>- Alert incident notifications.<br><br>- Behavior-based seamless access continuous authentication and authorization<br><br>- Token-based Secure Identity Management<br><br>- IT infrastructure maintenance.<br><br>- Mutual information exchange with(CERT) partners and law enforcement.<br><br>- Software maintenance. | - Framework for automated collaborative analysis of security relevant information.<br><br>- Fast and accurate detection of cyberattacks and mitigation strategies.<br><br>- Data analysis compliant with customer policies, dictated by privacy or business needs.<br><br>- Traveller privacy offered cyber-aware interest cast-based itinerary<br><br>- Secure and Privacy Aware Multi-Modal Transport shared wallet.<br><br>- Seamless authentication<br><br>- Identity and Access Management (IAM) | - Customers are reached through key industry events, targeted advertisement, business development including direct selling, website and exploiting partnership with ISACs<br><br>- Account management & sales support function will ensure regular touchpoints with the customer delivering regular updates to alert/ prevent newly found threats. | - Large companies (Enterprise) offering consultant services and IT supports to other companies. For these customers the E-CORRIDOR be the core of the offered security services.<br><br>- Small and medium-sized enterprises (SMEs)<br><br>- Scheduled service transport provider<br><br>- Mobility technology providers |
| | **Key Resources**<br>- Know how on sticky policies & data usage control for preserving privacy.<br><br>- Know how -DSA tools formalisms, ontologies. Know how on collaborative data analysis<br><br>- Homomorphic encryption for privacy preserving collaborative data analysis<br><br>- Know how - behaviour based seamless authentication. | | **Channels**<br>- Email and web portal.<br><br>- B2B direct sales<br><br>- Integrators | |
| **Cost Structure**<br>- Cost of IT infrastructure, acquisition, maint<br><br>- Cost for software development, maintenance and update.<br><br>- Business dev, account mgmt, Marketing | | **Revenue Streams**<br>- Selling usage license of the E-CORRIDOR framework to large cos<br><br>- Fees for cloud accessible service for SMEs<br><br>- Consultancy & Research insights & reporting | | |

Figure 9 - Business Model Canvas

However, a more detailed understand of market exploitation pathways was derived from the aforementioned exploitation survey where some partners identified primary and secondary users of the key technologies being developed, as well as pathways through which these target users might acquire or access the technologies. A summary of these responses is contained below;

Table 4 - Primary & Secondary Users

| **Primary Users** | **Access Pathways** |
|---|---|
| Mobility Operators – Car Sharing<br>Mobility Operators – Car Leasing<br>Automotive OEMs<br>Scheduled Transport Service Providers – Airport/ Railways<br>Car Owners/ Drivers<br>Airport Services<br>EV Charging Operators<br>Parking Service Providers<br>Security Operation Centers (SOCs) | Solution providers to transport sector (airport, fleet management, rail service providers, travel brokers)<br>Framework instantiated on edge device (mobile, kiosk, infotainment portal)<br><br>Direct Integration to Mobility Service Providers<br><br>Web API |
| **Secondary Users** | **Access Pathways** |
| Passengers for multimodal trip planning & execution | Accessible to passengers via BYOD<br>Register and Create an account just once |

From the earlier presentations it confirmed that the E-CORRIDOR proposition is sizeable with different infrastructures, an array of cybersecurity and identity management tools and advanced analytics. From a product perspective the features and benefits need to be specified and related to the actual pain points experienced by customers. During validation, it can frequently occur that an assumed benefit doesn't actually solve a pain point or that a critical 'dependency' hasn't been considered. As an example, Data Sharing Agreements can enable identity and access management, but the dependency is on key parties executing those agreements. Also, conversations with customers will often reveal benefits not previously considered.

In terms of format, Target customers have initially been grouped into three categories (with more to be added) with a view to mapping key hypotheses to these customer groups. Those groupings include mobility transport providers, mobility service providers and enterprise technology organisations. The workshop sought to complete the table below by identifying different segments within each user group, specify organisations within those segments and elaborate on the features, benefits and pain points relevant to same.

Table 5 - Workshop Categories

| | **Type** | **Like who (Specific Targets)** | **Features & Benefits of interest** | **Problems Solved** |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| **Mobility Transport Providers** | CASE<br>Scheduled Service Operators<br>…. | *For example,*<br><br>CLEM<br>UBER<br>LYFT | *Itemise the specific components relevant to target* | *Describe in detail the current scenario illustrating pain points* |
| **Mobility Service Providers** | EV Charging<br>Parking | *For Example*<br><br>PILDO<br>Aptiv<br>Vulog<br>Otonomo | *Itemise the specific components relevant to target* | *Describe in detail the current scenario illustrating pain points* |
| **Enterprise Technology** | Cybersecurity<br>IAM | *For example*<br><br>HPE<br>Thales<br>Microsoft<br>OAUTH | *Itemise the specific components relevant to target* | *Describe in detail the current scenario illustrating pain points* |

Three mural boards have been created to capture the related hypotheses. Much of the initial workshop was dedicated to getting feedback from external stakeholders and to establishing the framework to collect and organise the material which will form the basis for business validation. The allotted time was insufficient to complete this process and contributions are still being collected and insights tabulated.

Once complete, the next steps will be to have a follow-up workshop to discuss the findings and develop validation plan which will include

- Agreed list of standalone commercial propositions (platform, individual components, component bundles)
- Target list of contacts / channels to support validation
- Messaging & collateral needed to support validation engagements (.e.g. pitch decks, product sheets)
- Market engagement/ validation tracker file.

## *Next Steps & Continuation of Activities*

The validation activities will be monitored and will form the basis for the development of the 'Go-to-market plans' (Business plan light) highlighted in D9.1. In addition, ongoing dissemination and exploitation to non-commercial audiences (e.g. Research, Gov) of the broader project outputs such as knowledge will continue.

# 4. IPR Management and Protection.

Until now, no consortium partners have raised any IPR issue, and the key IPR principles within the Consortium Agreement will still be respected. Final exploitation plans will detail IPR agreements and technology transfer plans to govern exploitation of assets and sustainability of project outcomes beyond lifetime of project and in accordance with Consortium and grant agreement.

# 5. Data Management Plan

The existing DMP stands and some minor updates are stated below. Further updates will be delivered in D9.4

## *Data Summary*

E-CORRIDOR aims at developing a technological framework to unleash the power of information sharing coupled with edge-based collaborative analytics for cyber protection. The framework will be tailored for multimodal transport needs by developing a significant set of security and analytics services based on it. Also, the project is pilot-driven, and the pilots will integrate their own infrastructures, tools and applications within the E-CORRIDOR framework to exploit the framework services.

The actors within the E-CORRIDOR ecosystem are referred to as *prosumers*, which are information producers and consumers at the same time. Actually, the fundamental asset is the information, or data, that the framework allows sharing between a federation of different stakeholders or parties. Any prosumer involved in the E-CORRIDOR framework could be the origin of data, and it can range from normal passengers and mobility service providers, to national Information Sharing and Analysis Centres (ISACs). Thus, multiple datasets will be gathered from multiple sources and of varying sizes and characteristics.

In short, the purposes of collecting data in E-CORRIDOR are to support advanced data analytics and security services provided by the E-CORRIDOR framework, to verify the performance of pilots, and to foster research and business innovation.

As for data utility, prosumers can decide how the data generated by them is shared and processed within the E-CORRIDOR framework, through the usage of DSAs and associated policies. Thus, the data won't go beyond the boundary of the E-CORRIDOR framework. However, E-CORRIDOR emphasizes the importance of information sharing and will deliver mechanisms to ensure secure and privacy-preserving data exchange and analysis. Most of the data generated will be processed by the Information Sharing Infrastructure (ISI) and Information Analytics Infrastructure (IAI), and the generated results will be consumed by the prosumers defined in the DSAs attached to the data.

Deliverable 5.1 *Requirements for E-CORRIDOR Architecture* has specified the data types that need to be used by the pilots and the framework. Table 3 of Deliverable 5.1 summarised all the initial data classes and contains information such as Data Type Class, Data Format, Standard, Pilot Use Case ID, and usage purposes (for sharing, for analysis, for performing a Data Manipulation Operation).

**Update**

As is detailed in the pilot documents (up to date) progress is under way to implement the above data formats and sharing protocols

The following data will be collected for inclusion in the final report D9.4

- A separate entry for each data type used (will allow a blend of real and synthetic.)
- WP/Task Title:
- Type of Test Data: Real/ synthetic
- Purpose of Data: <provide a short summery>
- IF Real: Gathered specifically or from existing dataset <describe dataset>
- if Real: <minimization method>
- If Real: and Collected, <Were people informed of their GDPR rights>
- If Synthetic: <describe how generated>

**FAIR Data**

The management of research data from E-CORRIDOR will follow the 'FAIR' principles, which will make research data findable, accessible, interoperable and re-usable.

#### 5.1.1.1 **Findable**

Research data used within E-CORRIDOR should be described with rich metadata and assigned a globally unique and persistent identifier to support the automatic discovery of datasets and services. Besides, metadata should clearly and explicitly include the identifier of the data they describe, and data should be registered or indexed in a searchable resource.
At this stage, E-CORRIDOR has identified the initial datasets to be communicated in Deliverable 5.1, but most of the data is privacy or business related and may not be suitable for being published online. Thus, E-CORRIDOR will regularly check the suitability of sharing their research data outside the project.
In the next stage, E-CORRIDOR will evaluate the suitability of publicising its datasets on a case-by-case basis. For a suitable dataset, the project will register or index it in a searchable resource (likely Zenodo) and provide its metadata in the suitable standardised formats requested by the searchable resource.

**Update**

In the final phase we will help to promote the research data that will be gathered by sharing it on community site such as Zenodo (https://zenodo.org), The data and papers shared will include white paper, academic paper, and other data as defined in article 29 of the grant agreement. Member of the Advisory board and the exploitation board will be invited to participate.

#### 5.1.1.2 **Accessible**

E-CORRIDOR supports open access where feasible and will follow the "green" open access for scientific publications. This means a published article, or the final peer-reviewed manuscript is archived (deposited) in an online repository before, alongside or after its publication. Repository software usually allows authors to delay access to the article ("embargo period"), and E-CORRIDOR partners will ensure open access to the publication within a maximum of six months.
On the other hand, E-CORRIDOR opted out "open access to research data" in the Grant Agreement due to confidentiality, privacy, and business consideration of its research data. However, E-CORRIDOR will keep evaluating the suitability of making its datasets openly available.

**Update:**

The Intent is to make 'GREEN' access to all papers and articles published and an investigation is under way as to how best to achieve this within the structures and funding provided by the project.

#### 5.1.1.3 **Interoperable**

E-CORRIDOR aims to collect and document its data in a standardised way to ensure that the datasets are easy to understand, reuse and interoperate among different parties who are interested in utilising them. Standard formats for knowledge representation and standard vocabularies will be used to facilitate inter-disciplinary interoperability.

#### 5.1.1.4 **Re-usable**

Data reusability means the easiness to re-use the data for further research or other purposes. In E-CORRIDOR, most of the datasets refer to sensitive data that can be linked with a person or a business, and the re-use of them should be restricted and limited to the consortium members. However, some tools and algorithms developed by E-CORRIDOR can be reusable for similar purposes during or after the project, and all the public deliverables are freely available on our website.

Regarding data quality, E-CORRIDOR will ensure the quality of its deliverables and research data. For deliverables, Section 5.2 *Quality Assurance* in D10.1 regulates the actions to ensure the highest quality of the deliverables. Additionally, quality assurance of research data at different stages from data collection, data entry or digitalization and data checking will be performed.

**Allocation of Resource**

Implementing the FAIR principle may incur costs. However, there are neither immediate costs anticipated for this stage nor a reasonable estimate of the protentional costs.
Project outputs and data are securely stored in an SVN repository (https://svn-security.iit.cnr.it/svn-multi/) hosted by CNR, and there is no extra cost incurred. For publicising the research data in an external data repository, the project will evaluate the suitability and risks around this plan and take prudent actions. When choosing external data repositories, free but secure options such as Zenodo [28] funded by the OpenAIRE project will be prioritised. Additional details will be provided, as needed, in future versions of the DMP. Any unforeseen costs related to open access to research data are eligible for reimbursement during the duration of the project under the conditions defined in Article 6.2.D.3 of the Grant Agreement.
Data management concerns the whole project and needs to be planned, coordinated, implemented, and monitored both at the project and work package level. The main actors involved here will be the project coordinator, work package leaders, and data providers in the pilots, and their roles and responsibilities will be refined in further DMPs.

**Ethical Policy**

Section 5 of the Grant Agreement details the Ethical Policy of E-CORRIDOR, and it specified the measures to manage personal and sensitive information while fully complying with relevant laws, regulations and principles. Besides, WP1 *Ethics requirements* is dedicated to ensuring compliance with the “ethics requirement”’ set out by the project, and D1.1 and D1.2 provide more detailed descriptions of our ethical policy.

**Update**
This should be handled by the D10 deliverable.

# 6. Conclusions.

The efforts of WP9 for the final phase of the E-CORRIDOR project will focus on disseminating the key project results to all relevant audiences with an emphasis on maximizing exploitation opportunities.

# 7. Appendix

## *Definitions and Abbreviations*

| Terms | Meaning |
|---|---|
| **API** | Application Programming Interface |
| **APT** | Advance Persistent Threat |
| **AT** | Airport-Train (E-CORRIDOR Work Package 2 Pilot) |
| **CAN** | Controller Area Network |
| **DoS** | Denial of Service |
| **DSA** | Data Sharing Agreement |
| **DKE** | German Commission for Electrotechnical, Electronic & Information Technologies of DIN and VDE (German: Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE) |
| **ITS** | Intelligent Transport Systems |
| **IP** | Intellectual Property |
| **ISO** | International Standard Organization |
| **IDS** | Intrusion Detection System |
| **IPS** | Intrusion Prevention System |
| **IPR** | Intellectual Property Rights |
| **VDE** | German: Verband der Elektrotechnik, Elektronik und Informationstechnik; one of the largest technical and scientific associations in Europe |
| **R&D** | Research and Development |
| **R&I** | Research and Innovation |
| **PKI** | Public Key Infrastructure |
| **ML** | Machine Learning |
| **MaaS** | Mobility as a Service |
| **TPM** | Trusted Platform Module |
| **TCG** | Trusted Computing Group |
| **V2X** | Vehicle-to-Everything Communication |
| **WP** | Work Package |
| **WG** | Working Group |

# 8. Bibliography

[1] “Google Analytics,” Google, [Online]. Available: https://analytics.google.com/analytics/web/.

[2] “Twitter Analytics,” Twitter, [Online]. Available: https://analytics.twitter.com/.

[3] P. Kotler, Marketing Management (Fifteenth edition), PEARSON, 2016.

[4] Institute for Manufacturing, University of Cambridge, “Porter's Generic Competitive Strategies (ways of competing),” [Online]. Available: https://www.ifm.eng.cam.ac.uk/research/dstools/porters-generic-competitive-strategies/.

[5] European Commission, “Network of Excellence on Engineering Secure Future Internet Software Services and Systems,” 1 August 2019. [Online]. Available: https://cordis.europa.eu/project/id/256980. [Accessed May 2021].

[6] European Commission, “European Network for Cyber-security,” 2 July 2020. [Online]. Available: https://cordis.europa.eu/project/id/675320. [Accessed May 2021].

[7] European Commission, “SoBigData Research Infrastructure,” 2 July 2020. [Online]. Available: https://cordis.europa.eu/project/id/654024. [Accessed May 2021].

[8] ERCIM, [Online]. Available: https://www.ercim.eu/.

[9] ERTRAC, “New CCAM Association started with 144 members,” April 2021. [Online]. Available: https://www.ertrac.org/index.php?mact=News,cntnt01,detail,0&cntnt01articleid=108&cntnt01origid=15&cntnt01pagelimit=3&cntnt01returnid=90. [Accessed May 2021].