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

D9.2

First 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: 30/05/2021

Actual submission date: 30/05/2021

30/5/2021

Version 1.0

Responsible partner: WIT

Editor: Ruisong Han

E-mail address: rhan@wit.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: Ruisong Han (WIT), Christine O'Meara (WIT), Stefano Sebastio (RTRC)
Roland Rieke (FhG), Christian Plappert (FhG), Sergi Paniagua (Pildo)
Hajer Saada (RTRC), Ilaria Matteucci (CNR), Fabio Martinelli (CNR)

Approved by:

Revision History

Version	Date	Name	Description
0.1	04/Feb/2021	Ruisong Han (WIT)	Table of Content (TOC)
0.2	02/Mar/2021	Ruisong Han (WIT)	Revised the TOC and added some general introduction to each section
0.3	07/Apr/2021	Ruisong (WIT), Stefano Sebastio (UTRC), Roland Rieke (FhG), Christian Plappert (FhG)	Merged the contribution from FhG and RTRC; added more content to the document
0.4	26/Apr/2021	Ruisong (WIT), Ilaria Matteucci (CNR), Fabio Martinelli (CNR)	Revised the content and include the contribution from CNR
0.5	05/May/2021	Christine O'Meara (WIT), Ruisong (WIT)	Merged the exploitation section and revised the document.
0.6	25/May/2021	Roland Rieke (FhG), Sergi Paniagua (Pildo), Hajer Saada (RTRC), Ruisong (WIT)	Roland revised Section 3 with more content added; Sergi, Hajer and Ruisong reviewed and revised the deliverable.
1.0	30/May/2021	Fabio Martinelli (CNR)	Final version

Executive Summary

This document reports the dissemination, communication, exploitation and standardisation activities of E-CORRIDOR in the first 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 dissemination, communication, exploitation and standardisation against the plan, and the rest of the report is organised as follows.

First, the dissemination and communication section briefly summarises the project's dissemination and communication targets and describes all the dissemination materials generated and all the communication activities in the first project year.

Then, the exploitation section recaps the business plan of the project, and reports the progress in identifying key assets, improving business plans, and establishing the Exploitation Board.

Last, the standardisation section describes the liaison with standardisation bodies and related contribution.

In all, this deliverable reviews the progress in dissemination, communication, exploitation and standardisation, and will help the project summarise the achievements and gaps in implementing the first Exploitation and Dissemination Plan. Results from this deliverable will be fed into further plans, to refine the project's communication and management work.

Table of Contents

List of Figures

List of Tables

1. Introduction

E-CORRIDOR values the dissemination, communication, exploitation and standardisation of the project results, which bring real innovation in cybersecurity and multi-modal transport domains and positively impact a number of stakeholders. The design of the E-CORRIDOR architecture and its key subsystems, namely Information Sharing Infrastructure (ISI), Information Analytics Infrastructure (IAI), DSA Lifecycle Infrastructure (DLI), Common Security Infrastructure (CSI), and Advanced Security Infrastructure (ASI) has been well documented in Deliverables 5.2, 6.1, 7.1 and 8.1. Besides, the three pilots, which are Airport and Train (AT) Pilot, Car Sharing Pilot (S2C), Information Sharing and Analytics Centre Pilot (ISAC) also design the architecture for their pilots, by customising the configurations of the E-CORRIDOR framework and adding local components. The design and architecture for these pilots have been reported in Deliverables 2.2, 3.2 and 4.2. With lots of new knowledge generated and new tools designed in these deliverables, E-CORRIDOR project members and relevant stakeholders have a wealth of assets to be promoted and exploited, to deliver solid innovation and impacts to the market, industry and academia.

To ensure the dissemination, communication, exploitation and standardisation will be performed in a consistent and high-quality manner, the project has presented its first exploitation and dissemination plan in Deliverable 9.1. This plan will form the basis for the successful execution of various exploitation and dissemination activities, to realise the ambitious goals set in its exploitation and dissemination strategies and enlarge the project impacts. Moreover, the plan was made by considering the key assets presented in the aforementioned deliverables and designing relevant communication and dissemination tactics strategically.

Deliverable 9.2 *First exploitation and dissemination repor*t presents the progress of the project in dissemination, communication, exploitation and standardisation during the first project year, to provide a reference point for checking against the plan made in Deliverable 9.1 and making strategical adjustments. The rest of the deliverable is organised as follows:

Section 2 *Dissemination and Communication* first briefly summarises the project's dissemination and communication targets and describes all the dissemination materials generated and all the communication activities in the first project year.

Section 3 *Exploitation* recaps the business plan of the project and reports the progress in identifying key assets, improving business plans, and establishing the Exploitation Board.

Section 4 *Standardisation* describes the liaison with standardisation bodies and related contribution.

Last, Section 5 concludes this deliverable.

The deliverable will help the project summarise the achievements and gaps in implementing the first Exploitation and Dissemination Plan. Results from this deliverable will be fed into further plans, to refine the project's communication and management work.

2. Dissemination and Communication

2.1 Objectives

The E-CORRIDOR project results are the tangible and intangible outputs of the research, development, and innovation actions within the project, such as data, knowledge and information. These results can be utilised by both the project partners and other relevant stakeholders outside the project, to enable further exploitation, research, development or innovations.

Focussed communication and dissemination actions surrounding E-CORRIDOR results, which are oriented towards clear objectives and strategies, are of utmost importance for maximising their potential impact. E-CORRIDOR's communication and dissemination objectives reflect the ultimate goal of the project, which is to contribute to a secure, resilient, and digital Europe by providing E-CORRIDOR solutions.

The overall communication and dissemination objectives of E-CORRIDOR defined in D9.1 are as follows:

- Promote awareness of the E-CORRIDOR project and the issues related to secure software engineering by industry, end-users, academia, and policymakers.
- Reach out to the broadest spectrum of stakeholders from the scientific and industrial communities, and the general audience with the main results from E-CORRIDOR to ensure the maximum impact during and after the project.
- Transfer E-CORRIDOR knowledge and results, to enable others to use and take up results, thus maximising the impact of E-CORRIDOR research and development.

2.2 Dissemination and Communication Progress

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.

2.2.1 Promotional Materials

The primary dissemination and communication channels used by E-CORRIDOR are the websites and social media, and the individual channels owned by partners (such as their own Twitter channels and newsletters) complement these channels.

To support the dissemination and communication activities and create an impressive visual identity, E-CORRIDOR has designed and used the following promotional materials to engage with our target audiences.

2.2.1.1 E-CORRIDOR Logo

As outlined in Figure 1, the E-CORRIDOR logo symbolises the project, and it unifies and reinforces the branding. It should be used in all project materials such as project website, document templates, presentations, social media accounts, newsletters, posters and other distributed materials to ensure consistency.

This logo is based around a shield representing Security/Safe/Strong. The blue and green colours express a message of trust and security and correspond to the vision of the project to contribute to a secure, resilient and digital Europe by supplying E-CORRIDOR solutions. Also, the white dot in the centre is to also show the shield as a map marker/position, representing the transport domain. The blue line circling the shield with 3 lines through it is to represent an interconnected network. These

lines represent Communication/Connection. These lines are also to represent a character E and match the exact size and spacing as the E in the E-CORRIDOR.

The logo is available in JPEG, PNG, and AI (original design files) formats and shared in both the project SVN repository and the project website. When not using the logo, E-CORRIDOR should be referred to in capital letters, just as it is used in Figure 1. A detailed brand guideline has also been provided to project partners to regulate the usage of colours, logos, fonts and images in various dissemination scenarios.

Figure 1. E-CORRIDOR logo (Left: with tagline; Right: without tagline).

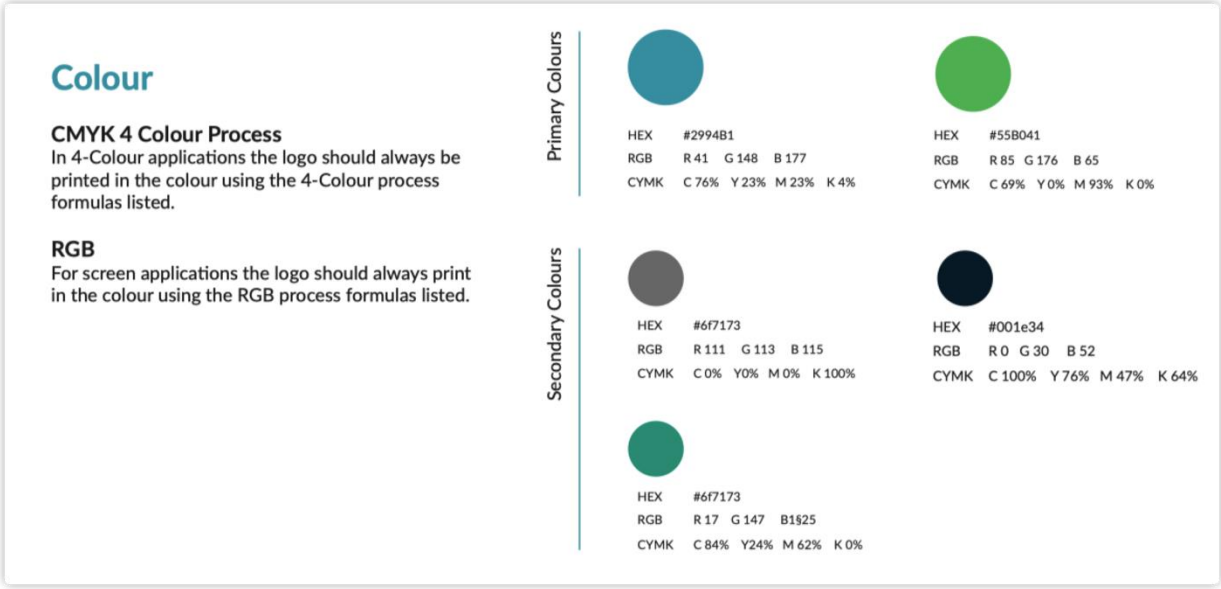

Figure 2. E-CORRIDOR colors in the project branding guideline.

2.2.1.2 Deliverables and Slides Templates

The templates for deliverables and slides have been provided in Section 8 *Templates* of D10.1 *Project Quality Handbook*, and they provide a unified format for the two most important documents within the project.

2.2.1.3 Videos

E-CORRIDOR has planned to create a series of promotional or interview videos to promote the concepts and innovation of the project. This work has been scheduled to start in Month 13 when a clearer technical roadmap is in place for each work package.

The length of each online interview will be around 10 mins, and the interview introduces the expertise of partners and their contributions to E-CORRIDOR project. Each partner should finish at least 1 video interview to achieve the set targets for WP9. However, if the outputs from partners such as pilots and deliverables need to be disseminated, more interviews/ news can be arranged. The WP9 leader will make a timetable for the interviews, record the videos interviews with partners, edit the videos, and publish them on our websites and social media.

Some example questions are as follows, but partners can also bring their own questions highlighting their originations and innovative work in E-CORRIDOR.

- Your organization and its involvement/expertise in the E-CORRIDOR project?
- Please introduce the project/work package/task achievement to date.
- What is the main challenge for the project or your work package? For instance, COVID-19 and travel restrictions around the world.
- What are the expected outcomes from your WP/tasks?
- How will the industry and academia benefit from the outputs of E-CORRIDOR?

2.2.1.4 Flyer and Leaflet

Flyers and leaflets act as important dissemination materials for the E-CORRIDOR project to support partners in attending events, presentations and workshops. These materials condense the project profile into a one- or two- page visually appealing document.

If roller banners or posters are needed for future events, their design will be based on the flyer shown below to ensure design consistency. The content on the roller banners or posters will be adjusted based on their applications.

Figure 3. E-CORRIDOR flyer.

Figure 4. E-CORRIDOR leaflet.

2.2.1.5 Slide Deck

In some cases, the target audience of E-CORRIDOR may want to learn more in-depth information about the project, where the flyer and poster could not meet the demand due to the limited space. Thus, E-CORRIDOR has created a 12-page slide deck with more project details provided. It is shared at the link https://e-corridor.eu/resources/ under the tab "BRANDING & LOGOS". The slide deck also functions as a project brochure, providing information on the project objectives, consortium, methodology, and pilots. Besides, the content of the slide deck will be regularly updated to reflect the latest information and outputs of the project.

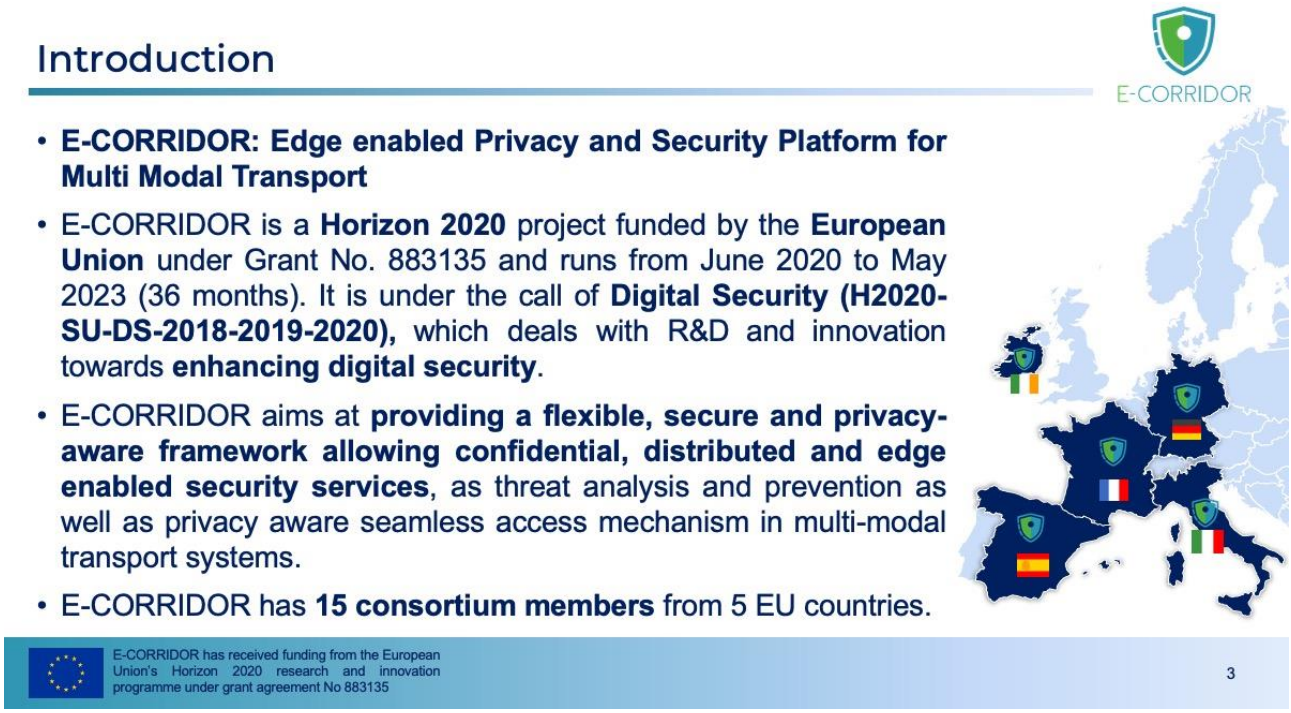

Figure 5. E-CORRIDOR slide deck.

2.2.2 Website

The E-CORRIDOR website (https://e-corridor.eu/) is the primary dissemination channel to share project information with the world. The website (shown in Figure 6) was designed and developed by the Creative Design Unit (CDU) at TSSG/WIT over the course of several months and has been online since November 2020.

A wealth of information to introduce the project and the project's progress has been provided across different sections of the website. Besides, it has been continuously monitored and updated to facilitate better dissemination, outreach and project operation.

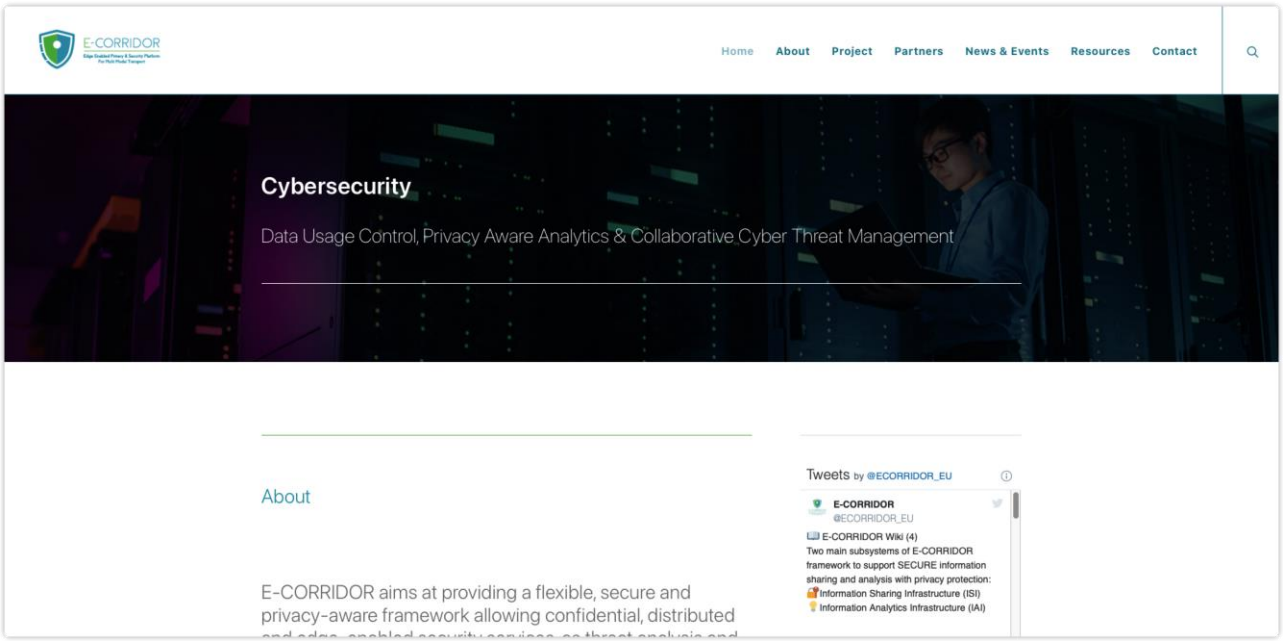

Figure 6. E-CORRIDOR website homepage.

Figure 7. E-CORRIDOR website - news page.

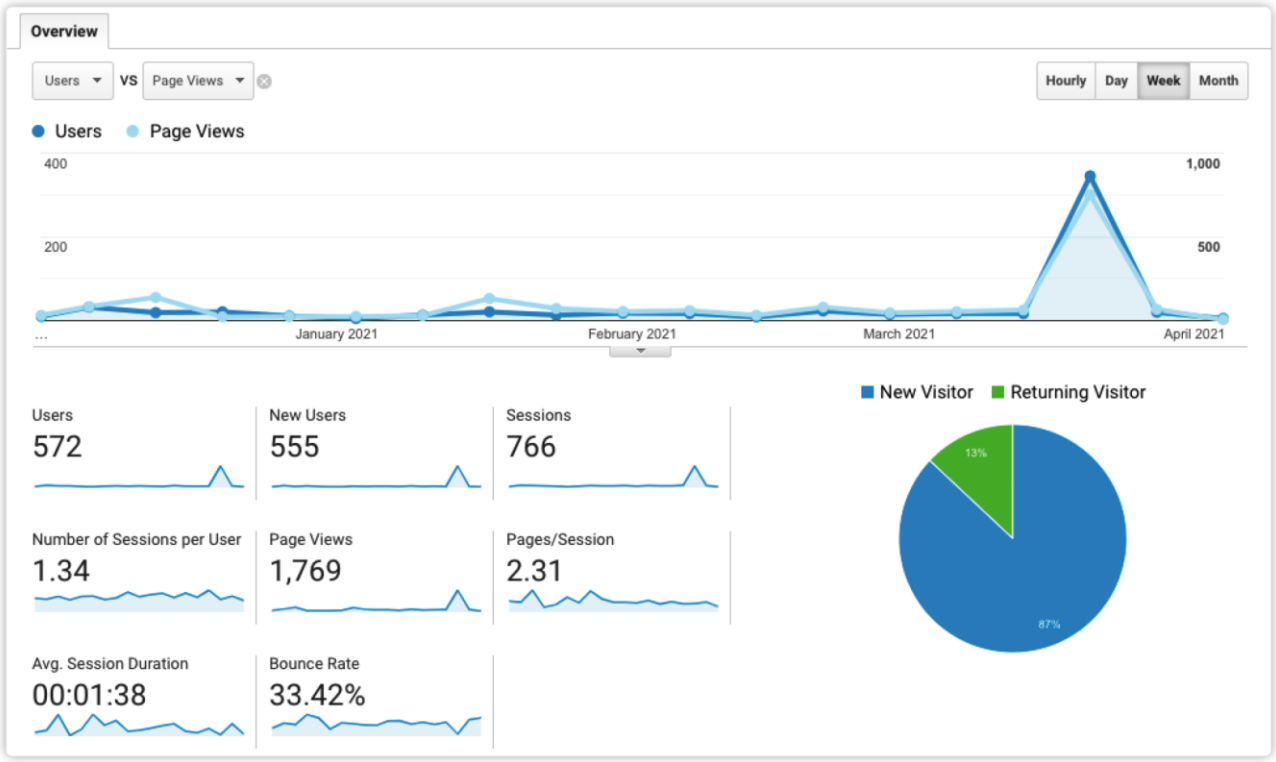

Figure 8. E-CORRIDOR website audience overview.

In this section, we will present the viewing trends of the E-CORRIDOR website (obtained through Google Analytics [1]), along with some relevant analysis in accordance with the presented data.

Figure 8 presents an overview of the E-CORRIDOR website audience and statistics between December 1st, 2020 and April 7th, 2021. The website has attracted 555 new (unique) users during this period and has a total of 1769 page views. For a project in its first year of operation and with a sparsity of concrete results due to development being in its early stages, we feel that this is a satisfactory outcome. Furthermore, we noticed that most of the views and new users are centred on March 2021. The reason is that E-CORRIDOR hosted its 3rd plenary meeting that month, and we generated lots of interesting content (such as news and tweets) from that. Thus, we can infer that the original content around E-CORRIDOR could attract more audience, and more efforts should be placed on generating E-CORRIDOR related content. As the project progresses with more concrete results available for public observation, we could expect a natural increase in audiences' interest and website visits.

Another two sets of data show the origin countries of our website users (Figure 9) and the top 10 pages viewed by users. Figure 9 indicates that E-CORRIDOR's audience has a great geographical coverage that is not limited to EU countries. E-CORRIDOR could attract the attention of international research powers and foster international communication.

Moreover, Figure 10 shows that most of the views of our website occur on our homepage, indicating that our target audience is still at the stage of learning about E-CORRIDOR, instead of focusing on a specific technical topic.

With a bunch of deliverables to be submitted in Month 12 and the concrete results derived from them, we can expect a better dissemination result in the following project year. We will keep monitoring the website's statistics and adjust our dissemination strategies accordingly to maintain a continuous and profound impact.

	Country	Users	% Users
1.	United States	59	10.30%
2.	Italy	46	8.03%
3.	(not set)	43	7.50%
4.	Ireland	41	7.16%
5.	France	35	6.11%
6.	China	29	5.06%
7.	Spain	22	3.84%
8.	Germany	20	3.49%
9.	Japan	20	3.49%
10.	India	18	3.14%

Figure 9. E-CORRIDOR website users by country.

	Page	Page Views ↓	Unique Page Views
1.	/	1,144 (64.67%)	683 (59.55%)
2.	/e-corridor-project/	100 (5.65%)	69 (6.02%)
3.	/our-partners/	98 (5.54%)	79 (6.89%)
4.	/about-ecorridor/	77 (4.35%)	59 (5.14%)
5.	/news/	61 (3.45%)	39 (3.40%)
6.	/resources/	57 (3.22%)	41 (3.57%)
7.	/contact-ecorridor/	44 (2.49%)	31 (2.70%)
8.	/cyrano/	24 (1.36%)	17 (1.48%)
9.	/event/	24 (1.36%)	17 (1.48%)
10.	/cve-for-kia-vulnerability/	22 (1.24%)	17 (1.48%)

Figure 10. E-CORRIDOR website page views.

2.2.3 Social Media

The primary goal of using social media for E-CORRIDOR is to spread the messages of E-CORRIDOR in a timely and lively way and promote the level of awareness regarding the project among key stakeholders. The table below lists all the social media channels of E-CORRIDOR, but the focus of this section is on Twitter.

Table 1. E-CORRIDOR social media channels.

Social Media Channel	Link
Twitter	https://twitter.com/ECORRIDOR_EU
LinkedIn	https://www.linkedin.com/in/ecorridor/
Facebook	https://www.facebook.com/ECORRIDOR.EU
YouTube	https://www.youtube.com/channel/UCKaYxHm9DTnhAtLMfM2AaGA

The E-CORRIDOR Twitter account (@ECORRIDOR_EU) has been the primary social media channel for the project to date. E-CORRIDOR started to manage its social media account since October 2020 and has published 28 tweets and received 9679 Tweet impressions (the number of times a tweet shows up in somebody's timeline), 796 profile visits and 45 new followers (at the time of

writing which is the end of March 2021). To date, the Twitter account has a total of 1,174 followers, among which are other H2020 projects and stakeholders in the cybersecurity and transport domains.

The dissemination effect through Twitter has also been analysed by using the data from Twitter Analytics [2]. The results have been shown in Figure 11, and we can see increasing efforts being put into this channel (more Tweets published) and wider impacts (more Tweet impressions and profile visits).

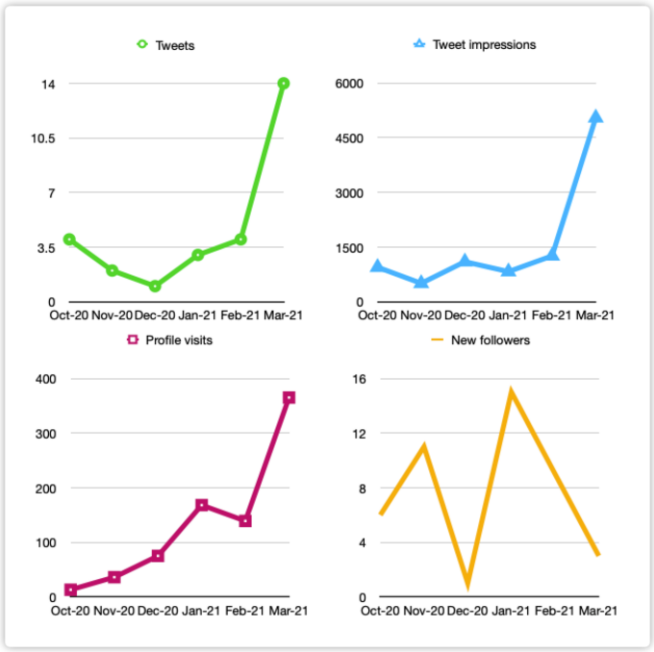

Figure 11. E-CORRIDOR Twitter Analytics statistical results.

2.2.4 Publications

2.2.4.1 Press Release

The project has published several news on the website to disseminate the project messages to the public and media.

Table 2. E-CORRIDOR news on the project website.

Title	Date	Link
EU H2020 ICT Security project E-CORRIDOR successfully kicked off	2020-07-06	https://e-corridor.eu/ecorridor-kicked-off/
Open Research Europe, the EC scientific publishing service for H2020 and Horizon Europe	2020-11-24	https://e-corridor.eu/open-research-h2020/
CNR researchers successfully identified KIA Head Unit vulnerability and made it a CVE entry.	2020-12-02	https://e-corridor.eu/cve-for-kia-vulnerability/
Cyrano event to be held on Dec. 16th, 2020 to share the cybersecurity observatory	2020-12-08	https://e-corridor.eu/cyrano/

E-CORRIDOR 3rd virtual plenary meeting successfully held	2021-03-19	https://e-corridor.eu/plenary3/

2.2.4.2 Papers

Below are all publications submitted, accepted and presented at peer-reviewed international conferences with the contribution from E-CORRIDOR partners.

Table 3. Conference papers submitted/published by the E-CORRIDOR consortium

Conference	Date	Areas	Paper Title	Authors and Affiliation
ACM ASIACCS 2021 -16th ACM ASIA Conference on Computer and Communications Security	2021-06-07	Security	Secure Role and Rights Management for Automotive Access and Feature Activation	Christian Plappert, Lukas Jäger, Andreas Fuchs (FhG)
PDP 2021 - 29th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing	2021-03-10	Security	Attack Surface Assessment for Cybersecurity Engineering in the Automotive Domain	Christian Plappert, Daniel Zelle, Henry Gadacz, Roland Rieke, Dirk Scheuermann, Christoph Krauß (FhG)
ARES'20 - 15th International Conference on Availability, Reliability and Security	2020-08-25	Security	VisualDroid: automatic triage and detection of Android repackaged applications	Rosangela Casolare, Carlo De Dominicis, Fabio Martinelli (CNR), Francesco Mercaldo (CNR), Antonella Santone
WAINA-2020 - Workshops of the 34th International Conference on Advanced Information Networking and Applications	2020-04-15	Security	Colluding Android Apps Detection via Model Checking	Rosangela Casolare, Fabio Martinelli (CNR), Francesco Mercaldo (CNR), Vittoria Nardone, Antonella Santone
IJCNN 2020 - 2020 International Joint Conference on Neural Networks	2020-07-19	Security	Malicious Collusion Detection in Mobile Environment by means of Model Checking	Rosangela Casolare, Fabio Martinelli (CNR), Francesco Mercaldo (CNR), Antonella Santone

IJCNN 2020 - 2020 International Joint Conference on Neural Networks	2020-07-19	Security	Enhanced Privacy and Data Protection using Natural Language Processing and Artificial Intelligence	Rosangela Casolare, Fabio Martinelli (CNR), Francesco Mercaldo (CNR), Antonella Santone
IoTBDS 2020 – The 5th International Conference on Internet of Things, Big Data and Security	2020-05-07	Security; ML	Image-based Malware Family Detection: An Assessment between Feature Extraction and Classification Techniques.	Giacomo Iadarola (CNR), Fabio Martinelli (CNR), Francesco Mercaldo, Antonella Santone
KES 2020 - International Conference on Knowledge-Based and Intelligent Information & Engineering Systems	2020-09-16	Vehicular; ML	A Deep-Learning-Based Framework for Supporting Analysis and Detection of Attacks on CAN Buses	Alfredo Cuzzocrea, Francesco Mercaldo, Fabio Martinelli (CNR)
VTC2020-Spring - 2020 IEEE 91st Vehicular Technology Conference	2020-05-25	Vehicular; ML	Machine Learning for Driver Detection through CAN bus	Fabio Martinelli (CNR), Francesco Mercaldo, Antonella Santone

Below are all publications published at peer-reviewed journals which involve the contribution from E-CORRIDOR partners or acknowledge the project.

Table 4. Journal papers submitted/published by the E-CORRIDOR consortium

Paper Title	Journal Name	Authors	Link
Towards an Interpretable Deep Learning Model for Mobile Malware Detection and Family Identification	Computer & Security	Giacomo Iadarola (CNR), Fabio Martinelli (CNR), Francesco Mercaldo (CNR), Antonella Santone	https://www.sciencedirect.com/science/article/pii/S0167404821000225
Call Graph and Model Checking for Fine-Grained Android Malicious Behaviour Detection	Applied Sciences	Giacomo Iadarola (CNR), Fabio Martinelli (CNR), Francesco Mercaldo (CNR), Antonella Santone	https://www.mdpi.com/2076-3417/10/22/7975

Android Collusion: Detecting Malicious Applications Inter-Communication through SharedPreferences	Information	Rosangela Casolare, Fabio Martinelli (CNR), Francesco Mercaldo (CNR), Antonella Santone	https://www.mdpi.com/2078-2489/11/6/304
Humming Bad mobile malware detection and mitigation	Simulation Modelling Practice and Theory	Fabio Martinelli (CNR), Francesco Mercaldo (CNR), Vittoria Nardone, Antonella Santone, Gigliola Vaglini	https://www.semanticscholar.org/paper/Model-checking-and-machine-learning-techniques-for-Martinelli-Mercaldo/df1722134fa85ddf4b124cd034c69a001933dd28

2.2.5 Events

Table 5. Events attended by the E-CORRIDOR consortium.

Event Name	Date	Location	Domain	Type	Attendees and Roles
CSET (Cyber Security for Energy & Transport infrastructure) International Conference 2020	2020-09-17	Genova, Italy	Security	Workshop	Fabio Martinelli (Speaker)
CYRANO	2020-12-16	Virtual	Security	Workshop	Fabio Martinelli (Speaker); Stefano Sebastio (Attendee)
EUROCONTROL: Introduction to Cyber Threat Intelligence	2021-01-28	Virtual	Security	Webinar	Riccardo Orizio (Attendee)
EUROCONTROL: Introduction to Cyber Threat Intelligence	2021-01-28	Virtual	Security	Webinar	Stefano Sebastio (Attendee)
SESAR-JU: ATM Cyber-security - The industry view	2021-02-05	Virtual	Security	Webinar	Stefano Sebastio (Attendee)
EUROCONTROL: Vulnerability management	2021-02-18	Virtual	Security	Webinar	Stefano Sebastio (Attendee)
ATHENE Secure Mobility Dialogue	2021-03-24	Virtual	Security	Workshop	Roland Rieke (speaker)
Automotive Security Research Group Waterford (ASRG-WAT)	2021-03-03	Virtual	Security; Automotive	Webinar	Ruisong Han (Attendee)
CCAM Association 1st General Assembly	2021-04-14	Virtual	Automotive	Event	Ruisong Han (Attendee)

2.2.6 Liaison with Related Communities and Projects

- *H2020 Cyberwatching.eu – The European watch on cybersecurity & privacy (https://cyberwatching.eu/).* It is the European observatory of research and innovation in the field of cybersecurity and privacy aiming at promoting the uptake and understanding of cutting-edge cybersecurity and privacy services emerging in Research and Innovation projects. By partnering with Cyberwatching.eu, the E-CORRIDOR project will enhance the visibility of its ICT products, services and software in particular towards SME and European citizens. Potentially proposing novel cybersecurity services in the European Digital Single Market. Ruisong (WIT) and Stefano Sebastio (RTRC) promoted E-CORRIDOR on cyberwatching.eu (EU observatory of research and innovation in the field of cybersecurity and privacy). (https://cyberwatching.eu/projects/2456/e-corridor-edge-enabled-privacy-and-security-platform-multi-modal-transport).
- *H2020 SPARTA (https://www.sparta.eu/).* It is a novel Cybersecurity Competence Network, supported by the EU, with the objective of developing and implementing top-tier research and innovation collaborative actions. Thanks to its mix of partners from the academia and industrial sectors, one of its main goals is the definition of an ambitious research and innovation roadmap in the cybersecurity strengthening the EU strategic autonomy in the field. E-CORRIDOR will be able to reach out to different stakeholders belonging to the SPARTA network (e.g., cybersecurity practitioners, service provides, and technology providers) and promote the novel results and products in the field of security and privacy.
- *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. It aims at increasing awareness of airport, critical infrastructures and essential services operators on cybersecurity aspects. The liaison of E-CORRIDOR and CYRANO will provide mutual benefits as both are oriented at improving the cybersecurity of the transportation domain with a special focus on the airways (see in particular the AT-pilot in E-CORRIDOR).
- *H2020 CitySCAPE* (https://www.cityscape-project.eu/). Fabio Martinelli (CNR) was a speaker for one cybersecurity workshop held by CitySCAPE. E-CORRIDOR also liaised with Cityscape and contributed to one interview for the Autobus and Trasporti Pubblici magazine on cybersecurity and privacy in their multimodal public transport and one event.

3. Exploitation

3.1 Exploitation Overview

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.

In the first period of the E-CORRIDOR project, some foundational work has been ongoing to support specific business modelling, development and exploitation activities in subsequent phases. A 4-step exploitation approach has been identified to coordinate the exploitation activities within the project:

1. **Discovery:** much of the effort to date has concentrated on activities in this phase. In tandem with user requirements elicitation which is happening through the course of pilot actions in WP2, WP3 and WP4, efforts in WP9 have focussed on market research, in particular, a comprehensive business environment analysis the outputs of which are documented in D9.1. In addition to a macro environmental analysis, several sectors of relevance in the cybersecurity and mobility technologies domains were identified and analysed. This research enabled the creation of an updated SWOT analysis, and insights will be used to inform business planning and exploitation activities. Furthermore, strategic tools, including Kotler's product levels [3] and Porter's competitive framework [4], have been used to describe E-CORRIDOR products and the marketplace. These tools will serve as a useful basis to further develop business and exploitation ideas and plans.
2. **Define**: this phase will be a collaborative exercise to define and refine the E-CORRIDOR value proposition and to advance business modelling activities. To date, a very high-level description of the business model for E-CORRIDOR exists and has been updated. Specific detail and hypotheses underpinning this business model need to be teased out, including identifying channel partners, pricing strategies etc. This work will be supported by Industry & SME partners 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.
3. **Validation**: this phase will involve testing the hypotheses, models and plans that have been developed. Activities will include pilot feedback, demonstrations and pitch presentations. Feedback from the Exploitation Board and business networks will also support this phase.
4. **Go-To-Market Plans** will be finalised closer to the end of the project. The plans will guide exploiting and commercialising E-CORRIDOR's outputs.

3.2 Overall Exploitation Progress

Table XXX below summaries the status of the exploitable assets identified through previous surveys with general good progress being made.

Table 6. Exploitable results definition/ description

Exploitation Asset	Category	Exploitation Type	Explanation

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.
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.
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
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. 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 transfer from research institutes to industry.
Machine Learning (ML) IDS techniques [FhG]	Knowledge	Lecture	Darmstadt University of Applied Sciences course
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.
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.

Contribution to Trusted Computing Group (TCG) [FhG]	Standards	Standard	Introduction of the solution to TCG, possibly resulting in a new standard.
Multi-modal transport security knowledge Transfer to SMEs [FhG]	Knowledge	Commercial	The E-CORRIDOR project will put Fraunhofer SIT in a leading position with respect to competence in multi modal transport security and will consequently open further possibilities in that domain.
Privacy-preserving analytics and security techniques [UTRC]	Knowledge Software Evaluation on the field (with ADP, and SNCF in the AT pilot) Patent applications	Research Commercial	Privacy-preserving techniques supporting enhanced passenger experience in multi-modal transportation
Advanced authentication techniques [UTRC]	Knowledge, Patent application	Research	Model-based approach for safety and security in airport authentication systems
Multi-modal Trip Planning Tool [WIT]	Software Knowledge Patent application	Research 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)

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.
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.

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 Technolgies is part of a leading global aerspace organisation. It has secured strong interest in its privacy-preserving analytics and security techniques in development in eCorrordor. In particular the Information Managemt Systems and Services groups are paying close attention to the citical information management anc connected ecosystem tools that enable contacltes passenge journeys within the aiprort, as well as the privacy-aware mobile-based enrolment solutions wwhich will be tested in the AT pilot. Furthermore, an invention disclosure related to the privacy-aware analysis of cmaeral feeds is in preparation. UTRC internal stakeholders are also very inteerested 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 initatives such as IATA OneID and IATA NEXTT.
- WIT is currently engaging with its Technology Transfer Officer to assess the merits of filing an IDF for the multi-modal trip planning tool being developed by its software team. Furthermore, WIT is involved in a collaboration with Waterford City County Council which is using cameras to monitor heavy traffic engerring 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 itenerary planning and carbon foodptint analysis – where for example, number and size of trucks and enviornmental footprint analytics could inform planning

- FhG, basedon its work with the ML test toolset, has secured an industrail funded project. At this point it is not possible to give details hbeduase of an NDA. Furthermore, FhG will soon participate in a new prject 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 Woring Group (VSWG) with presentations at workhsops on securing the charging infrastructure of electirc vehidlesand contributions to other topics related to the Trusted service Manager developed in E-CORRIDOR.
- CNR ……

3.2.1 Business Model

As previously mentioned, D9.1, which has been developed in the same timeframe as D9.2, contains updates to the original foreseen business model for the E-CORRIDOR solution.

The details underpinning this business model and additional business models in the form of testable hypotheses such as value proposition, pricing strategies, channels and customer acquisition need to be teased out with the help of key structures (e.g., Exploitation board) and partners, and those hypotheses need to be validated.

3.2.2 Exploitation Board

The project has started the work to set up the Exploitation Board based on the plan in D9.1, and the current focus is finalising the board's constitution and selecting members.

The first exploitation Board meeting is planned for Q3 2021 since both the E-CORRIDOR framework (WP5-8) and the pilots (WP2-4) will have finished their work in defining the requirements and architecture of their solutions in Month 12. Then, project partners and the board will have clear clues of the critical assets and relevant business models. The coordinator will document the minutes of the Exploitation Board meetings, and the WP9 leader will take actions to coordinate the partners' efforts to implement the Exploitation suggestions from the meetings.

3.3 Individual Exploitation Progress

CNR (Consiglio Nazionale delle Ricerche), FhG (Fraunhofer-Gesellschaft), UTRC (United Technologies Research Centre Ireland), FACTUAL (Factual Consulting) and WIT (Waterford Institute of Technology) have revised their individual exploitation plans and reported their exploitation efforts within the first project year. Thus, this section will include the revised plans or reported efforts from these partners. As the project is finalising its requirements for the platform and pilots at the time of writing, the exploitation activities can be seen to stay more at the Discovery stage of the 4-stage exploitation plan. In this regard, not all partners have reported their progress here. However, exploitation activities will intensify as the project moves forward, and the exploitation plan defined in D9.1 will be respected to coordinate the exploitation activities.

3.3.1 CNR

CNR is the main public research organization in Italy. The results and the knowledge acquired in research projects have two major drivers for exploitation.

On the one hand, CNR is always interested in increasing its research capabilities (as well as the innovation ones). In particular, participating into E-CORRIDOR, it allows CNR to exploit the current technologies as well as to acquire new ones to compete in the national and international arena. Arguments like confederation, big data and security have been promoted by CNR in several formats,

including the communication and exploitation in EU projects such as Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSoS) [5] and the European Network for Cyber Security (NeCS) [6], the participation into the SoBigData Research Infrastructure [7] and the creation of several spinoff in the area, in particular of data analytics and business intelligence. The methodologies and tools developed in the E-CORRIDOR project will further enhance the research and development competence of the groups involved (security and data analytics) making even more competitive in the area. The CNR technicians are fully committed to increase their expertise on information sharing and analytics.

3.3.2 UTRC

UTRC is part of Collins Aerospace and Raytheon Technologies. With respect to the E-CORRIDOR project and use cases, UTRC is interested in passenger processing and facilitation solutions, creating a seamless, single-token, biometrically enabled journey for the passenger from home to the final destination. Collins airport operations solutions ensure that the right information is in the right place at the right time, throughout the terminal. A secure, efficient and privacy-preserving integration of all the airport operations brings a world-class architecture to accomplish the passenger seamless flow vision. Approaches and methodologies developed within the E-CORRIDOR framework about controlled data sharing, privacy-preserving analysis, cyber-physical security services and multi-biometric authentication in a multi-stakeholder domain could create a key product differentiation and increase market growth for Collins airport operation management. Therefore, towards the interactions with the Airport-Train pilot partners, UTRC is exploring the different use cases to identify areas of innovations with respect to the above-mentioned aspects.

3.3.3 FhG

FhG is the leading organisation of institutes of applied research and development in Germany. The primary objective of FhG is to improve information and technology transfer from research institutes to industry. So, in the Fraunhofer Institute for Secure Information Technology SIT (Fraunhofer SIT) as part of the FhG, the instruments and contacts to ensure professional exploitation of the research results are available. Fraunhofer SIT is focused on fortifying the foundations of the Internet, and on developing easy to deploy defences, ensuring security and availability of the Internet. To that end, the results of the E-CORRIDOR project will complement the already existing activities on: Defences against Denial of Service (DoS) attacks, Detection of malware and advanced persistent threats (APTs), Design and adoption of cryptographic schemes, and Privacy and anonymity. The E-CORRIDOR project will put Fraunhofer SIT in a leading position with respect to competence in multimodal transport security and will consequently open further possibilities in that domain. Additionally, FhG is a member of ERCIM (the European Research Consortium for Informatics and Mathematics [8]). ERCIM aims to foster collaborative work within the European research community and to increase co-operation with European industry.

3.3.4 WIT

WIT has defined its target assets in this period, which are Multi-modal Trip Planning Tool and Carbon Footprint Analytics coming from their research and development work in WP7. The state-of-the-art solutions in the market have been studied to identify the target features of our products. WIT will utilise the assets under development (Multi-modal Trip Planning Tool and Carbon Footprint Analytics within E-CORRIDOR) to further its Transport/Cybersecurity research and seek commercialisation opportunities. These assets can be integrated with the existing V2X communication system developed by WIT in the H2020 project TransSec, to foster innovative ITS applications and more comprehensive transport solutions.

With these creative know-hows and assets developed, WIT will seek to expand its Transport and Cybersecurity thematic research groups by attracting more research and business resources and

position itself as a transport/cybersecurity leader at the national level. WIT will endeavour to attract more research funding and bring in new students/researchers/developers for follow-on projects in this space. Besides, WIT also aims to become a go-to research organisation for companies in these domains to collaborate with. Furthermore, the research outputs can be fed into the WIT courses where applicable. WIT will prepare Invention Disclosure Forms ("IDFs") for the assets and link with Technology Transfer Offices (TTO) to identify commercial potential and patentability. WIT will contribute to EU initiatives/roadmaps/ working groups in the transport and cybersecurity domains. For instance, WIT joined the European Partnership on CCAM (Connected, Cooperative and Automated Mobility) [9] in March 2020 to advance its connected vehicle research and collaboration in Horizon Europe. Last, WIT will investigate the potential for investigating a spin-off company coming from the developed assets

3.4 IPR Management and Protection

IPR issues will be evaluated after the E-CORRIDOR framework and pilots have finished their design (due in Month 12) and reported in the following exploitation and dissemination reports. Till now, no consortium partners have raised any IPR issue, and the key IPR principles within the Consortium Agreement will still be respected.

4. Standardisation

4.1 Standardisation Overview

The E-CORRIDOR consortium aims at impacting international standardisation activities, as well as influencing domain specific initiatives on the topics relevant to E-CORRIDOR. Standardisation will facilitate technological cooperation, knowledge transfer and market take-ups of E-CORRIDOR results and innovation, therefore increasing the project impacts outside the consortium, in particular to the Industry and Society.

The initial plan for advancing standardisation activities has been defined in Deliverable 9.1. Standardisation activities are tightly coupled with the research, development, and innovation efforts within the project.

The project has been in close cooperation with existing standardisation bodies related with the project topics. The relevant standardisation possibilities of E-CORRIDOR results have been continuously monitored and reported to make the project in sync with latest standardisation progress. To provide meaningful contributions to the international standardisation landscape, E-CORRIDOR keeps evaluating the potential of turning its research and development (R&D) outputs (such as deliverables and R&D experience) into a set of localised best practices.

4.2 Standardisation Activities

This section presents information on the main standardisation organizations and activities that project partners have participated in during the last reporting period. A list of the working group(s)/committee(s) in which a partner of the consortium is a member is provided, together with a brief explanation of the specific standard or area in which a partner of the consortium is involved and the current status in that activity.

Table 7. E-CORRIDOR standardisation activities.

Standardization Organization	Description of Contribution	Status	Members
ETSI - European Telecommunications Standards Institute	Design and Development of security and privacy preserving solution for V2X	Specification and Design	FhG; CNR
TCG - Trusted Computing Group	Implementation of Feature API (FAPI) in TSS and Tools WG Attestation (co-chair) https://trustedcomputinggroup.org/work-groups/attestation/ WG Dice https://trustedcomputinggroup.org/work-groups/dice-architectures/ WG Infrastructure https://trustedcomputinggroup.org/work-groups/infrastructure/ WG Network Equipment https://trustedcomputinggroup.org/work-groups/network-equipment/	Bugfixing FAPI Co-chair in WG Attestation; Actively working in several other WGs	FhG

	WG Trusted Network Communications (TNC) https://trustedcomputinggroup.org/work-groups/trusted-network-communications/		
IETF - Internet Engineering Task Force	Operations and Management Area Working Group (opsawg) (co-chair) https://datatracker.ietf.org/wg/opsawg/about/ IOT Operations (iotops) (co-chair) https://datatracker.ietf.org/wg/iotops/about/ Remote ATtestation ProcedureS (rats) https://datatracker.ietf.org/wg/rats/about/ Software Updates for Internet of Things (suit) https://datatracker.ietf.org/wg/suit/about/ Security Automation and Continuous Monitoring (sacm) https://datatracker.ietf.org/wg/sacm/about/ Concise Binary Object Representation Maintenance and Extensions (cbor) https://datatracker.ietf.org/wg/cbor/about/ Interface to Network Security Functions (i2nsf) https://datatracker.ietf.org/wg/i2nsf/about/ Drone Remote ID Protocol (drip) https://datatracker.ietf.org/wg/drip/about/ Network Modeling (netmod) https://datatracker.ietf.org/wg/netmod/about/	Co-chair in opsawg and iotops; actively working on several documents in all mentioned WGs	FhG
C2C-CC - Car-2-Car Communication Consortium	Work Group “Security” Security Task Force “C2X PKI”	Member of WG	FhG
DKE / VDE (Electromobility)	DKE AK 353.0.8 “User authorization for charging infrastructure” https://www.dke.de/de/ueber-uns/dke-organisation-auftrag/dke-fachbereiche/dke-gremium?id=3002826&type=dke%7Cgremium	Creation of application rule	FhG
ISO/TC 22/SC 31/JWG 1 “**Joint ISO/TC 22/SC 31 - IEC/TC 69** WG”	Working Group “Vehicle to grid communication interface (V2G CI)”: ISO 15118-20 https://www.iso.org/committee/5383568.html	Member of WG	FhG

5. Conclusions

This deliverable reports the dissemination, communication, exploitation and standardisation activities and progress of E-CORRIDOR in the first project year.

Within the deliverable, the dissemination and communication aspects have been described together, due to the blurry boundaries between the two and the similarity in their goals of showing project benefits and maximizing project impacts. Section 2 summarises the project's dissemination and communication targets and describes all the dissemination materials generated and all the communication activities in the first project year. Most of the dissemination and communication channels have been in place, and the project has seen positive progress in transferring knowledge and results and reaching out to society. However, the dissemination and communication will last for the whole lifecycle of the project (and even beyond), and the project still needs continuous efforts to communicate and disseminate its innovative results. Besides, the performance of dissemination and communication should be closely monitored using different metrics and mechanisms, to identify the gaps between the current status and targets.

Exploitation concerns the effective utilisation of project results in further research and business activities, aiming to turn R&I actions into concrete value and substantial impact for society. Section 3 recaps the business plan of the project, and reports the progress in identifying key assets, improving business plans, and establishing the Exploitation Board. The project has seen solid efforts from project members in identifying their key assets and initial exploitation plans, by participating in the exploitation survey and project deliverables.

Last, Section 4 describes the liaison with standardisation bodies and the related contribution from E-CORRIDOR partners. We notice that the participation in standardisation activities is relatively limited to the leading research originations in the project consortium. Therefore, the focus of the standardisation strategy for the next project year will be motivating more project members to get involved in relevant standardisation activities, while maintaining the current good momentum in standardisation.

In conclusion, this deliverable describes the project progress in dissemination, communication, exploitation and standardisation, and will help the project in summarising the achievements and gaps in implementing the first Exploitation and Dissemination Plan defined in D9.1. Results from this deliverable will be fed into further plans, to refine the project's communication and management work. Continuous efforts and improvements are needed to promote the four aspects above and be reflected in D9.3 *Second exploitation and dissemination report*, which is due at Project Month 24.

6. Appendix

6.1 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

6.2 E-CORRIDOR Preliminary Exploitation Survey

E-CORRIDOR

Preliminary Exploitation Survey

Partner Name:

Survey

1. Please list the exploitation assets that your organisation expects to develop during the course of its work on the E-CORRIDOR project.

Exploitable Results Definition/ Description			
Exploitation Asset	**Category**	**Exploitation Type**	**Definition**
1.			
2.			
3.			

Examples of category types:

Knowledge / Software / Hardware / Documents (concepts, guidelines, training material, strategies and plans, etc.) / Data (e.g., statistical evaluations of field trials) / Protected items (Patent applications, licenses, copyrighted/copylefted material, registered designs) / Standards/ Other

Examples of Exploitation Type
Commercial/ Research/ Training/ Other (please define)

2. Please describe any IPR that will be developed by your organisation.

Partner name (more than one if Joint Partnership)	**Description of foreground**	**Definition of specific limitations and/or conditions for exploitation**
ABC org		

3. For the assets developed by your organisation, please outline your organisation's exploitation plans in the immediate aftermath of the project.

4. For the E-CORRIDOR framework as a whole, please outline your organisations' exploitation plans in the immediate aftermath of the project.

7. 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].