Grant Agreement No.: 952697
Call: H2020-SU-ICT-2018-2020
Topic: SU-ICT-02-2020
Type of action: RIA

D7.2 EXPLOITATION, STANDARDISATION, DISSEMINATION & COMMUNICATION ACTIVITIES REPORT

Revision: v.1.0

Work package	WP7
Task	Tasks 7.1 – 7.4
Due date	28/02/2022
Submission date	28/02/2022
Deliverable lead	TUDE
Version	1.0
Authors	Kaitai Liang (TUDE), Margherita Facca (MARTEL)
Reviewers	Thanassis Giannetsos (UBITECH), Klaudia dos Santos (MARTEL)
Abstract	This deliverable includes updates on exploitation, standardisation, dissemination, and communication plans and provides an initial report on executed activities.
Keywords	Dissemination, exploitation, communication, standardisation, website, leaflet, newsletter, social media, market expectations

Document Revision History

Version	Date	Description of change	List of contributors
V0.1	13/01/2021	Table of contents	Kaitai Liang (TUDE)
V0.2	06/02/2022	First draft	Margherita Facca (MARTEL), Thanassis Giannetsos (UBITECH)
V0.3	08/02/2022	Contribution from all ASSURED partners on their exploitation strategy, dissemination activities and performed standardisation actions	Richard Mitev, Phillip Rieger (TUDA) Liqun Chen, Nada El Kassem (SURREY) Meni Orenbach, Ahmad Atamli (MLNX/NVIDIA) Thanassis Giannetsos, Dimitrs Papamartzivanos (UBITECH), Stefanos Venios, Sotiris Koussouris (S5) Edlira Dushku, Nicola Dragoni (DTU) Kaitai Liang (TUDE) Riccardo Orizio, Stelios Basayiannis (UTRCI) Nikos Drossos (SPH) Karthik Shenoy Panambur, Shantanoo Desai (BIBA) Ilia Christantoni, Dimitra Tsakanika (DAEM) Ioannis Avramidis (INTRASOFT) Ilias Aliferis (UNISYSTEMS)
V0.4	14/02/2022	First draft	Margherita Facca (MARTEL), Thanassis Giannetsos (UBITECH)
V0.5	17/02/2022	Final review	Klaudia dos Santos (MARTEL)
V1.0	23/02/2022	Submission	Jean-Baptiste Milon (MARTEL)

Editors

Kaitai Liang (TUDE), Margherita Facca (MARTEL)

Contributors (ordered according to beneficiary numbers)

Edlira Dushku, Nicola Dragoni (DTU)

Richard Mitev, Phillip Rieger (TUDA)

Liqun Chen, Nada El Kassem (SURREY)

Kaitai Liang (TUDE)

Thanassis Giannetsos, Dimitris Papamartzivanos, Dimitris Karras (UBITECH)

Sotiris Koussouris, Stefanos Venios, Alexandros Tsaloukidis, Konstantinos Charalambous (SUITE5)

Ilias Aliferis, George Bekos, Thanassis Fameliaris (UNIS)

Sotiris Kousouris, Stefanos Venios (S5)

Ioannis Avramidis (INTRA)

Karthik Shenoy Panambur, Shantanoo Desai, Reyan Korel Erben (BIBA)

Nikos Drossos (SPH)

Ilia Christantoni, Dimitra Tsakanika (DAEM)

Riccardo Orizio, Stelios Basayiannis (UTRCI)

Funded by the Horizon 2020 Framework Programme of the European Union

DISCLAIMER

COPYRIGHT NOTICE

Project co-funded by the European Commission in the H2020 Programme		
Nature of the deliverable:	**R**	
Dissemination Level		
PU	Public, fully open, e.g., web	✓
CL	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to ASSURED project and Commission Services	

* R: Document, report (excluding the periodic and final reports)

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

OTHER: Software, technical diagram, etc.

Funded by the Horizon 2020 Framework Programme of the European Union

EXECUTIVE SUMMARY

This deliverable includes information on **dissemination, communication, and exploitation activities** as well as on **internal and external training and standardisation activities** of the ASSURED project. The document contains relevant information about executed activities in the first 18 months of the project and an updated plan for future activities.

The deliverable will be updated and finalized within “D7.3 Final plan and report on Exploitation, Standardisation, Dissemination & Communication activities” at the project end.

Information about the market, business opportunities, and market expectations form the industry partners will be documented in Deliverable D7.4 and D7.5 “Market Analysis, Business and Sustainability Plan”. Thus, in D7.2 an initial introduction of the market which ASSURED targets is put forth based on the list of exploitable assets that the consortium aims to produce by the end of the project.

Funded by the Horizon 2020 Framework Programme of the European Union

TABLE OF CONTENTS

1 INTRODUCTION 9
2 DISSEMINATION AND COMMUNICATION STRATEGY 11
2.1 Broad Public Society and Media 12
2.2 PolicyMakers 12
2.3 Industry 13
2.4 Research and Standardisation Communities 13
3 DISSEMINATION AND COMMUNICATION TARGETS 14
4 DISSEMINATION AND COMMUNICATION PLANS AND REPORT 15
4.1 Phase 1: Awareness Creation 15
4.1.1 Past Dissemination and Communication Activities – Phase 1 15
4.1.2 Highlights of Phase 1 19
4.1.2.1 Project Website 19
4.1.2.2 Interviews with Technical Experts 20
4.1.2.3 1st ASSURED Workshop 21
4.1.2.4 Newsletters 22
4.2 Phase 2: Continuity Of Information Flow 23
4.2.1 Past Communication Activities – Phase 2 23
4.2.2 Past Dissemination Activities – Phase 2 24
4.2.3 Highlights – Phase 2 31
4.2.3.1 Social Media 31
4.2.3.2 Twitter 31
4.2.3.3 LinkedIn 31
4.2.3.4 Open Access to Scientific Publications 33
4.2.3.5 Related Projects 36
4.2.4 Planned Activities – Phase 2 36
4.2.4.1 Scientific Events and Conferences 37
4.2.4.2 Social Media 37
4.2.4.3 Newsletters 37
4.2.5 Overview of Planned Presentations, Conferences, Exhibitions, Fairs, Workshops, etc. 38
4.3 Resume Dissemination and Communication Activities – Phase 1 & 2 40
4.4 Phase 3: Result Orientation 40
5 MARKET ANALYSIS AND EXPLOITATION 41
5.1 Market Analysis and Business Opportunities 41
5.1.1 Market Expectations 44
5.2 Exploitation Strategy and Commercialisation Roadmap 47
5.2.1 Updated Individual Exploitation Plans 47
5.3 ASSURED Exploitation Strategies (On Partner Level) 57

Funded by the Horizon 2020 Framework Programme of the European Union

5.3.1 Exploitation Strategy by UBITECH 57
5.3.2 Exploitation Strategy by BIBA 58
5.3.3 Exploitation Strategy by INTRASOFT 60
5.3.4 Exploitation Strategy by S5 60
5.3.5 Exploitation Strategy by UTRCI 61
5.3.6 Exploitation Strategy by SPH 62
5.3.7 Exploitation Strategy by DAEM 63
6 INTERNAL AND EXTERNAL TRAINING 66
7 STANDARDISATION 69
7.1 Contribution to Standards 69
7.2 Standardisation Activities 72
8 SUMMARY AND OUTLOOK 75

Funded by the Horizon 2020 Framework Programme of the European Union

LIST OF FIGURES

FIGURE 1: DISSEMINATION AND COMMUNICATION PHASES 9
FIGURE 2: COMMUNICATION, DISSEMINATION AND EXPLOITATION 10
FIGURE 3: DISSEMINATION AND COMMUNICATION PHASES 11
FIGURE 4: ASSURED TARGETED AUDIENCES AND MEASURES 12
FIGURE 5: ASSURED WEBSITE 19
FIGURE 6: ASSURED WEBSITE ANALYTICS 20
FIGURE 7: ASSURED EXPERT INTERVIEW SERIES 21
FIGURE 8: CYSARM 2021 - HOMEPAGE 21
FIGURE 9: ASSURED NEWSLETTER - SCREENSHOT 22
FIGURE 10: ASSURED TWITTER ACCOUNT 31
FIGURE 11: ASSURED LINKEDIN COMPANY PAGE 32
FIGURE 12: "FUTURE PROOFING AND CERTIFYING SUPPLY CHAINS" CLUSTERING WORKSHOP – SCREENSHOTS FROM THE ONLINE EVENT 36

Funded by the Horizon 2020 Framework Programme of the European Union

LIST OF TABLES

TABLE 1: KEY PERFORMANCE INDICATORS FOR DISSEMINATION AND COMMUNICATION ACTIVITIES 14
TABLE 2: PAST DISSEMINATION & COMMUNICATION ACTIVITIES – PHASE 1 15
TABLE 3: PAST COMMUNICATION ACTIVITIES 23
TABLE 4: PAST DISSEMINATION ACTIVITIES – PHASE 2 24
TABLE 5: SCIENTIFIC PUBLICATIONS 33
TABLE 6: PLANNED DISSEMINATION ACTIVITIES - PHASE 2 38
TABLE 7: INDUSTRIAL PARTNERS' MARKET EXPECTATIONS 44
TABLE 8: PARTNERS' UPDATED INDIVIDUAL EXPLOITATION PLANS 47
TABLE 9: INTERNAL AND EXTERNAL TRAINING BY ACADEMIC PARTNER 66
TABLE 10: TRUSTED COMPUTING GROUP (TCG) 70
TABLE 11: DECENTRALIZED IDENTITY FOUNDATION (DIF) & EUROPEAN SELF-SOVEREIGN IDENTITY LAB (SSI) 71
TABLE 12: RELEVANT BODY / STANDARD 71
TABLE 13: STANDARDISATION ACTIVITIES BY PARTNER 72

Funded by the Horizon 2020 Framework Programme of the European Union

1 INTRODUCTION

This deliverable provides an initial report and an updated plan of **exploitation**, **standardisation**, **dissemination,** and **communication** activities, as listed in Annex I. The activities will continue throughout the project while the report will be finalized by the project end in deliverable D7.3 “Final plan and report on Exploitation, Standardisation, Dissemination & Communication activities”.

Dissemination & communication activities ensure the visibility and awareness of the project and support the widest adoption of its results among potential users. The ASSURED dissemination & communication plan prepares the way for successful exploitation by facilitating internal communication within the project from the outset. Dissemination & communication activities are actively pursued from the beginning to the end of the project – engaging continuously with both internal and external audiences. The activities have been clustered into three main phases, as shown in Figure 1.

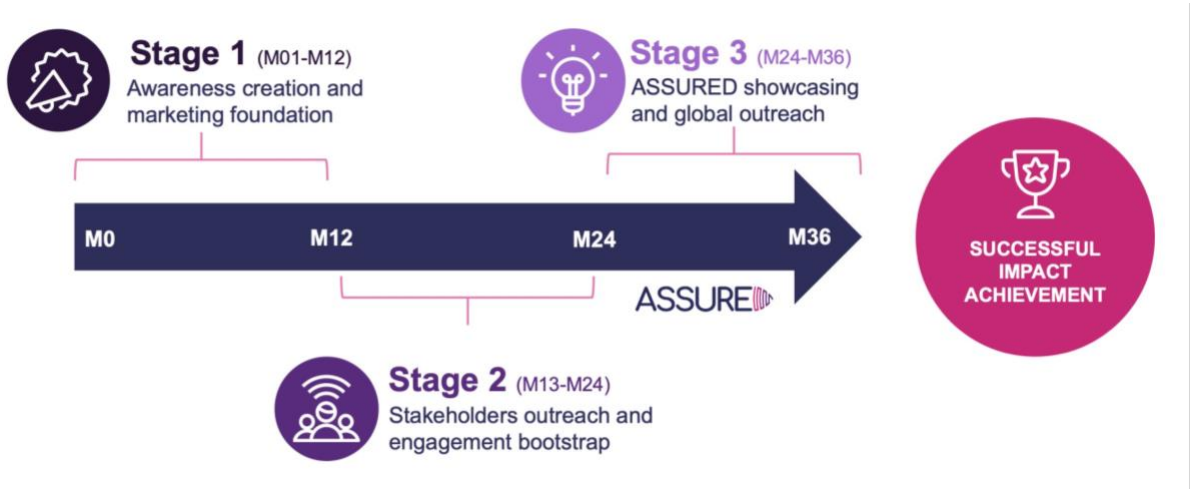

FIGURE 1: DISSEMINATION AND COMMUNICATION PHASES

The first phase, called ***“awareness creation and marketing foundation”*** consisted of building up the ASSURED branding and corporate identity, as well as establishing the ASSURED website and additional project information material, like templates for documents as well as presentations. The ASSURED project has successfully completed this first phase.

The project is not in the second phase, ***“stakeholders outreach and engagement bootstrap”*****,** in which scientific papers are written and submitted to conferences and journals as well as presentations at conferences and workshops are/will be given in order to further raise awareness among the scientific and industrial stakeholders. Furthermore, publications, whitepapers and certain deliverables will be published on the project website in order to keep interested parties informed about the latest progress. In addition, engaging posts on Twitter & LinkedIn and on the Blog constitute an important part of keeping the information flow upright and increase the interest of multiple audiences. Besides that, newsletters, press releases, poster, information about workshops and conferences, etc. are an integral part of this dissemination phase, allowing for more interactive communication within and outside the consortium. There will be additional press releases/newsletters when significant milestones are reached or for specific project events.

In the third phase, “***ASSURED showcasing and global outreach***”, dissemination will feed into **exploitation and standardisation**, which means using the results for commercial purposes or in public policymaking. There will be some ongoing dissemination activities after

Funded by the Horizon 2020 Framework Programme of the European Union

the project end in order to promote the project results (e.g., website will stay alive for 5 years, social media, cooperation activities with other projects, talks at conferences and follow-up projects). The main focus will be to exploit those project results and attract the target audience group.

At the beginning of the project, the consortium established an initial communication, dissemination and exploitation plan, which will be stated and explained in more detail in the following chapters, where we report on communication & dissemination activities as well as exploitation and standardisation activities.

FIGURE 2: COMMUNICATION, DISSEMINATION AND EXPLOITATION

Funded by the Horizon 2020 Framework Programme of the European Union

2 DISSEMINATION AND COMMUNICATION STRATEGY

A clear communication and dissemination strategy is essential and a forerunner for executing a dissemination and communication plan. Therefore, the assured project has set out a clear strategy for dissemination and communication (Figure 3). The strategy defines the audiences the project aims to target and determines why such audiences should be targeted and by which means.

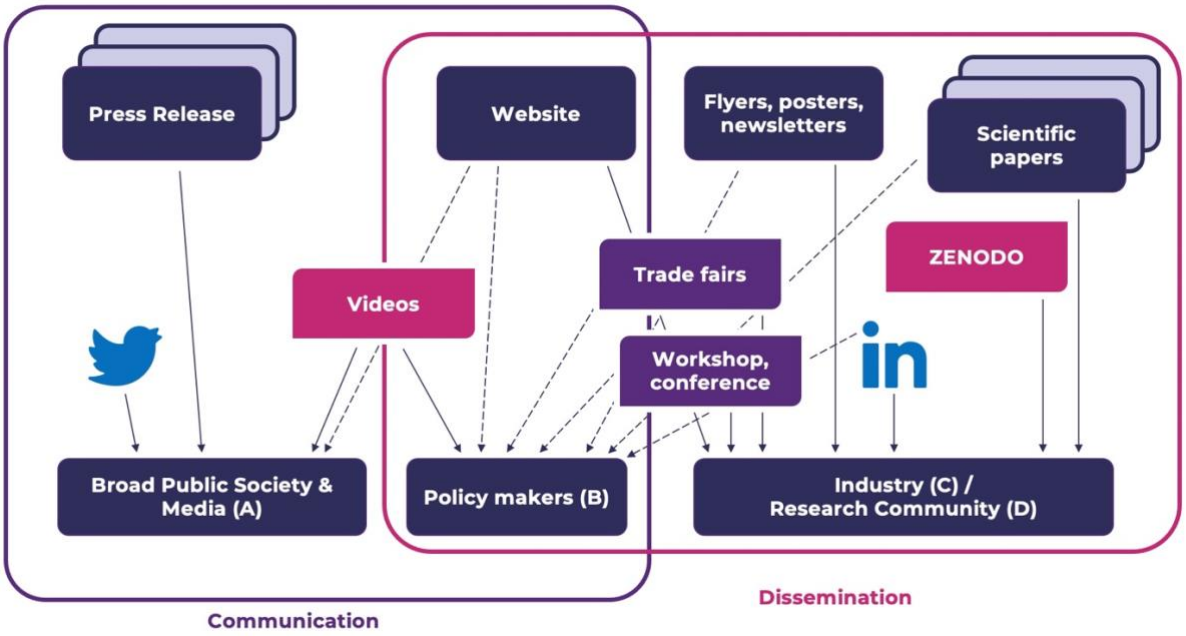

FIGURE 3: DISSEMINATION AND COMMUNICATION PHASES

Within the ASSURED project, four main audience groups can be defined:

For communication:

- **Broad Public Society & Media** (A)**,**
- **Policymakers** (B)**,**

For dissemination:

- **Policymakers** (B)**,**
- **Industry** (C)**,** and
- **Research Community** (D).

The project results can be explicitly used to reach different audiences using various channels from Figure 4. The channels and forms of their application are described in the following.

Funded by the Horizon 2020 Framework Programme of the European Union

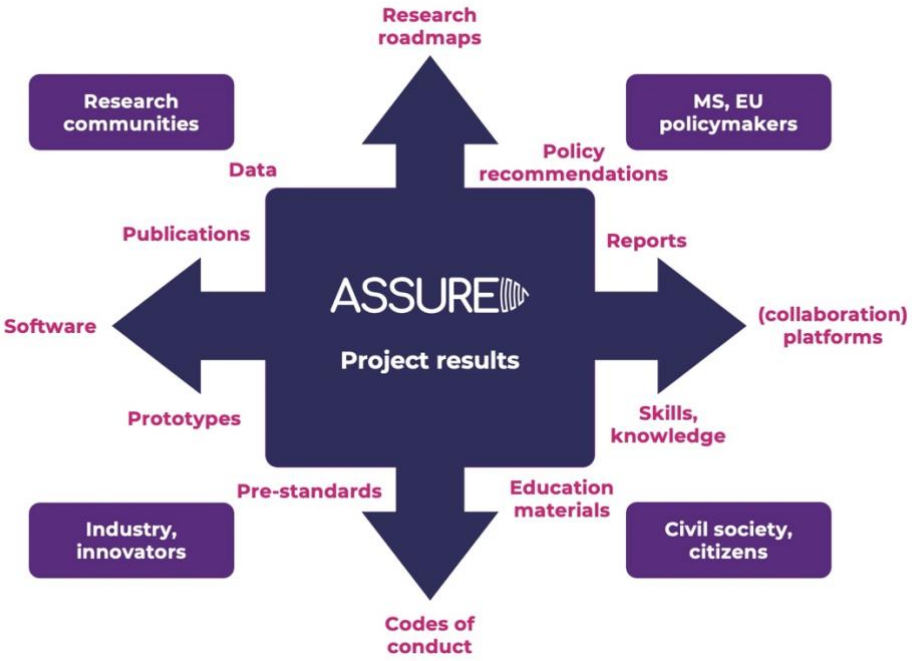

FIGURE 4: ASSURED TARGETED AUDIENCES AND MEASURES

2.1 BROAD PUBLIC SOCIETY AND MEDIA

Citizens are taxpayers and pay large amounts to the European Commission yearly. It is only fair that they expect to see that the resources they commit serve a meaningful purpose. Without funding from taxpayers, there would be no funding for H2020 projects. With different communication activities, we show to the society the impact and benefits of the ASSURED project and how they could profit from the project results in their everyday life.

Within the ASSURED project, many means are defined to reach the public. One of the main is the project website[1]: there it is possible to find an info postcard, a technical poster and, as well, a general presentation (under the "promo materials" area)[2]. Further channels that are emerging are introductory video interviews, which are available on the project website. Also, the ASSURED Twitter account [3]gives an overview of the EU funded R&I activities.

2.2 POLICYMAKERS

It is important to bring the research and its outcome to policymakers in order to support them while fostering collaboration and innovation. There are several benefits in presenting the work and the results of the ASSURED project to policymakers.

First, it increases the visibility of our research and enhances the project partner's reputation. Further, it helps to gain understanding and support, also financially. Additionally, we attract potential end-users of the project results and by outlining the broader socio-economic and

[1] Project website: https://www.project-assured.eu/

[2] Promo materials: https://www.project-assured.eu/promo-materials/

[3] ASSURED Twitter account: https://twitter.com/Project_Assured

Funded by the Horizon 2020 Framework Programme of the European Union

policy context of our project. Future policymaking will be positively influenced. The scientific evidence of ASSURED additionally support the grounds for European policymaking.

2.3 INDUSTRY

In order for the innovation developed within the ASSURED project to have significant value, it is essential to show it and its applicability to industry needs. Within the industry, a large potential of stakeholders can be found which will eventually enhance the general exploitation of the innovation, thus also benefitting the global European economy.

The ASSURED project foresees several ways to reach the industry. Whereas the main channel is the attendance of trade fairs, the industry is also reached by attending conferences, workshops and further by publishing newsletters and keeping the website up to date. Furthermore, in the ASSURED Advisory Board two of its members work in the industry. (HP, Philips).

2.4 RESEARCH AND STANDARDISATION COMMUNITIES

Reaching the research and standardisation communities is crucial to innovation within the European Union: in order for the ASSURED project to have a real impact in further research, and to help the standardisation path, it is essential to reach and gain the interest of the said communities.

There are many channels through which the research community can be reached and results of the project can be made available. First, it is necessary to publish in open access. ASSURED provides open access to all published articles, on the ZENODO platform, a general-purpose open-access repository developed under the European OpenAIRE program and operated by CERN, where they are linked to their DOIs. ZENODO platform allows researchers to deposit research papers, data sets, research software, reports, and any other research-related digital artefacts. A persistent DOI (digital object identifier) is minted for each submission, which makes the stored items easily citable. So far on the ZENODO platform, we have published 17 papers and publications submitted and published (one is waiting to be published). They are also made accessible on the project website under the “scientific publications” area[4].

Standardisation is an utmost important aspect of the ASSURED project. A key strategic objective of ASSURED is to contribute to standardisation efforts at EU level. As described in Chapter 7, we anticipate that the work conducted in ASSURED will lead on standardisation proposals on **updated functional specifications and working version of the Trusted Software Stack (TSS)**, used for the interaction with the host TPM; on **privacy-preserving signature and authentication techniques** (on ISO/IEC JTC 1/SC 27) including also the newly developed (decentralized) Attribute-based Encryption scheme; on **device binding for wallet security** (through the Decentralized Identity Foundation (DIF) and Self-Sovereign Identity (SSI) working groups), and on **defining protection profiles including the definition of the type of (overarching) system properties and non-functional properties** that affect the level of trustworthiness of next-generation connected systems (ISO/IEC JTC1/WG13). Many of the ASSURED project partners are already members of the core standardisation working groups of interest (i.e., TCG, DIF, SSI, ISO/IEC, ETSI). In addition to that, ASSURED also plans to hold a scientific workshop in August 2022 where representatives from all relates standardisation initiatives will be invited.

[4] Scientific publications and papers: https://www.project-assured.eu/publications/

Funded by the Horizon 2020 Framework Programme of the European Union

3 DISSEMINATION AND COMMUNICATION TARGETS

During the proposal phase of the assured project, a detailed communication and dissemination plan was already set up, stating different audiences, the objective of reaching the audience, and the impact of reaching them. This plan is the basis for D7.2 and can be found in Section 2.2 of the DoA.

To assess the effect of the dissemination and communication activities on the target audience, several Key Performance Indicators (KPI) have been selected, allowing to measure progress towards fixed goals for dissemination activities. These KPIs are repeatedly referenced in the document. The following table collects the selected KPI:

TABLE 1: KEY PERFORMANCE INDICATORS FOR DISSEMINATION AND COMMUNICATION ACTIVITIES

Dissemination activity/channel	KPI	
Events participation	• Presentation/Talk at events	• 15 (5 x year)
Project flyer	• Number of flyer • Number of copies distributed (online/offline)	• 3 • 1500 (distributed online/offline)
Rollup / posters	• Number of rollups/posters	• 2
Press releases distributed to media	• Number of press releases	• 4
Videos	• Number of videos published • Number of total views	• 3 videos published • At least 300 total views
Scientific / conference publications	• Number of scientific publications submitted	• At least 15 scientific publications submitted
Newsletter	• Number of newsletter issued	• 12 newsletter issued
Website unique visitors	• Number of unique visitors	• At least 1500 unique visitor
Social media followers	• Number of followers on Twitter • Number of followers on LinkedIn	• 300 followers on Twitter • 100 followers on LinkedIn

Funded by the Horizon 2020 Framework Programme of the European Union

4 DISSEMINATION AND COMMUNICATION PLANS AND REPORT

4.1 PHASE 1: AWARENESS CREATION

The goal of the "awareness creation" phase was to build up the ASSURED branding and corporate identity, as well as to establish the website and other useful information material. The ASSURED consortium successfully finished this first phase. The planned activities for the first phase can be found in Section 2.2.1 of the DoA Part B document and the executed activities are described in the following sub-chapters.

4.1.1 Past Dissemination and Communication Activities – Phase 1

Dissemination & communication are ongoing tasks within ASSURED. Past activities which were already completed in the first awareness phase are summarised in Table 2. As most of the activities were needed for communication and dissemination, we have combined them in one table:

TABLE 2: PAST DISSEMINATION & COMMUNICATION ACTIVITIES – PHASE 1

Type of activities	Partner	Title	Date	Place	Audience[5]						Type and goal of the event / website
					A	B	C	D	O	Total	
Communication											
Press release	MAR	ASSURED announcement from Martel website	05/10/2020	Online	x	x	x	x	x	N/A	Martel Innovate announced the kickoff of the project on its own website. The announcement link is available also on the project website under the "press release" area. https://www.martel-innovate.com/news/2020/10/05/martel-launches-seven-new-h2020-projects/
Press release	ALL	ASSURED official announcement	09/10/2020	Online	x	x	x	x	x	N/A	The project published the official announcement of its kickoff through a blogpost on the website. The announcement link is available also on under the "press release" area. https://www.project-assured.eu/2020/10/09/assured-project-kicks-off/

[5] Broad Public Society & Media (A), Policymakers (B), Industry (C), and Research Community (D), Other (O)

Funded by the Horizon 2020 Framework Programme of the European Union

Type of activities	Partner	Title	Date	Place	Audience[5]						Type and goal of the event / website
					A	B	C	D	O	Total	
Press release	UBI	ASSURED announcement from UBITECH website	25/10/2020	Online	x	x	x	x	x	N/A	The announcement was published on UBITECH's website at first, and then later on the project website under the "press release" area. It was made available for all project partners in order to encourage partners to make their own internal announcements. https://ubitech.eu/ubitech-kicks-off-the-assured-research-and-innovation-action-on-sustainable-operational-assurance-and-verification-for-systems-of-systems-security-and-privacy/
Press release	MAR	ASSURED: state-of-the-art	20/02/2022	Online	x	x	x	x	x	N/A	More than 15 months of the ASSURED project have passed and we are almost at the middle of the project. Therefore, we are able to report you the project's progress. During this period, we have successfully completed the first work-package, which defines the security, privacy and trustworthiness requirements of the ASSURED framework and the envisioned use cases. All the technical tasks have been completed and the deliverables of this work package have been submitted to the EU and have been published on the project website. The announcement was publish as newsflash and is available as pdf under the "press release" area.
Video	MAR	Clustering workshop video	14/12/2021	Online	x	x	x	x	x	20	The Clustering Workshop co–organized by EU-funded projects ASSURED and CYRENE aims at bringing together projects that target Supply Chain Security, Resilience and Certification aspects, experts, members and consultants from standardisation and certification bodies for exploring synergies and identifying actions that can be pursued in common.
Video	MAR + UBI	ASSURED interview series: Thanassis Giannetsos (UBITECH)	09/02/2022	Online	x	x	x	x	x	48	ASSURED expert interview series: interview with Thanassis Giannetsos (UBITECH) technical coordnator of the ASSURED project, talking about the vision and mission of the project. https://www.youtube.com/watch?v=bxq4nKISjGQ

Funded by the Horizon 2020 Framework Programme of the European Union

Type of activities	Partner	Title	Date	Place	Audience[5]						Type and goal of the event / website
					A	B	C	D	O	Total	
Video	MAR + MLNX	ASSURED interview series: Ahmad Atamli (NVIDIA)	23/02/2022	Online	x	x	x	x	x	30	ASSURED expert interview series: interview with Ahmad Atamli (NVIDIA) talking about how Ahmad and his team are looking into one of the biggest challenges of building such mechanisms – the efficient monitoring of the behaviour of a system that ASSURED wants to attest and secure. https://www.youtube.com/watch?v=UGsc5ybZBwI
Other	MAR	Project branding	01/09/2020	Online	x	x	x	x		N/A	Project logo and a color scheme were agreed upon, which are used for all communication and dissemination activities in order to ensure a recognizable visual identity.
Website	MAR + ALL	ASSURED project website	01/09/2020	Online	x	x	x	x		2454[6]	To disseminate & communicate information on the project and its impact to interested parties worldwide (e.g., news such as conference visits, publications & deliverables, involved partners, links, etc.) the official project website https://www.project-assured.eu/ was.
Flyer	MAR + ALL	Project flyer	recurrent	Online + printed	x					N/A	The postcard addressed to the general audience. https://www.project-assured.eu/promo-materials/
Dissemination											
Newsletter		ASSURED Newsletter	Every quarter	Online		x	x	x		5	A newsletter templates and a newsletter mailing list as well as a subscription possibility via the project website were prepared. Within the first 18 month 5 ASSURED newsletters can be found on the project website: https://www.project-assured.eu/subscribe/
Poster	MAR + ALL	ASSURED technical poster	recurrent	Online + printed		x	x	x		N/A	The ASSURED technical poster gives an overview of the project and describes mission, motivation and concept of the project. The technical poster is one of our tailored dissemination materials capable of reaching a scientific audience (mainly used for fairs and project meetings). https://www.project-assured.eu/promo-materials/

[6] Website unique visitors from the beginning of the project (September 2020) till the end of February 2022

Funded by the Horizon 2020 Framework Programme of the European Union

Type of activities	Partner	Title	Date	Place	Audience[5]						Type and goal of the event / website
					A	B	C	D	O	Total	
Project slidedeck	MAR + ALL	ASSURED slidedeck	recurrent	Online	x	x	x	x		N/A	The ASSURED slidedeck gives a project overview and describes mission, motivation and concept of the project. The technical leaflet is one of our tailored dissemination materials capable of reaching a scientific audience (mainly used for fairs and project meetings). https://www.project-assured.eu/promo-materials/
Social Media	ALL	Twitter	recurrent	Online	x	x	x	x		185[7]	A Twitter account was set up for the project. On a continuous basis updates are posted. https://twitter.com/Project_Assured
Social Media	ALL	LinkedIn	recurrent	Online	x	x	x	x		78[8]	A LinkedIn account was set up for the project. On a continuous basis updates are posted. https://www.linkedin.com/company/assured-project/
Organisation of a Workshop	UBI + MAR	CYSARM '21	19/11/2021	Online		x	x	x		55	On the 19th of November 2021, the 3rd edition of the workshop on Cyber-Security Arms (CYSARM - co-located with the ACM CCS 2021) took place online. The goal of the CYSARM workshop is to foster collaboration and discussion among cyber-security researchers and practitioners to better understand the various facets and trade-offs of cybersecurity and how new security technologies and algorithms might impact the security of existing or future security models. https://www.project-assured.eu/event/cysarm-2021/ and https://www.cysarm.org/.
Organisation of a Workshop	UBI + MAR	Clustering workshop	14/12/2021	Online		x	x	x		63	"FUTURE PROOFING AND CERTIFYING SUPPLY CHAINS". On the 13th of December 2021, the Clustering Workshop, co-organized by EU-funded projects ASSURED and CYRENE, aimed at bringing together projects that target Supply Chain Security, Resilience and Certification aspects, experts, members and consultants from standardisation and certification bodies for exploring synergies and identifying actions that can be pursued in common. https://www.project-assured.eu/event/future-proofing-and-certifying-supply-chains/

[7] Twitter followers from the beginning of the project (September 2020) till the end of February 2022

[8] LinkedIn followers from the beginning of the project (September 2020) till the end of February 2022

Funded by the Horizon 2020 Framework Programme of the European Union

4.1.2 Highlights of Phase 1

As listed in the table above within the first phase of the project, several communication activities were planned. First, the project was announced by an official announcement published on the project website as a news. It was made available for all project partners, in order to encourage partners to make their own internal announcements. Other official announcements were made by UBITECH and Martel Innovate via their own website. All the announcements are available under the "press releases" area[9]. Further, the **project logo and a colour scheme** were agreed upon, which are used for all communication and dissemination activities in order to ensure a recognisable visual identity. Also, one technical poster, one flyer and one rollup have been produced to disseminate the project (available on the website under the "promo materials" area[10]) and the project website built-up, which is constantly updated.

Some of these communication and dissemination activities are already described in detail in D7.1 "Internal and external IT communication infrastructure and project website". Therefore, we here just briefly list these actions. For further details, please refer to D7.1 Internal and external IT communication infrastructure and project website.

4.1.2.1 Project Website

The ASSURED project website is available on the following link: **https://www.project-assured.eu/**.

The ASSURED project website (see Figure 5) is a fully functional and responsive web portal that contains comprehensive information on the ASSURED aims and objectives with easy access and a friendly interface to retrieve information and any public material generated within the project, as well as materials gathered via the various work packages activities about ongoing projects and relevant initiatives. The ASSURED web portal is the entrance point for all the cybersecurity community players/stakeholders (existing and newcomers) to the activities, services, material, and information that ASSURED is planning to create, collect and share. At each page of the ASSURED website the disclaimer, the cookie and privacy policy and the project info email are accessible (located at the bottom).

FIGURE 5: ASSURED WEBSITE

[9] Press releases: https://www.project-assured.eu/press-releases/

[10] Promo materials: https://www.project-assured.eu/promo-materials/

Funded by the Horizon 2020 Framework Programme of the European Union

The homepage provides an overview of the project, including information about the project's *mission and motivation*, about the planned *results*, the *technical approach* (work packages) and the *use cases* of ASSURED. Furthermore, the *consortium* is presented and each partner website is linked.

The website is kept up to date with latest information on past and upcoming events. Regular blog entries are also posted on the website, allowing to see work that has been performed by the different project partners. In addition to that submitted public deliverables are made available as well as publications related to the project.

To summarize, and according to Google Analytics, the ASSURED website was looked more than 4926 times (page views) from its launch until the end of February 2022 by approximately 2454 visitors. Most of the visitors come from Europe: Bulgaria, Croatia, Greece, Hungary, and Lithuania. We always refer back to the website (e.g., in social media and in dissemination material) and hope to boost the website analytics more in the upcoming months.

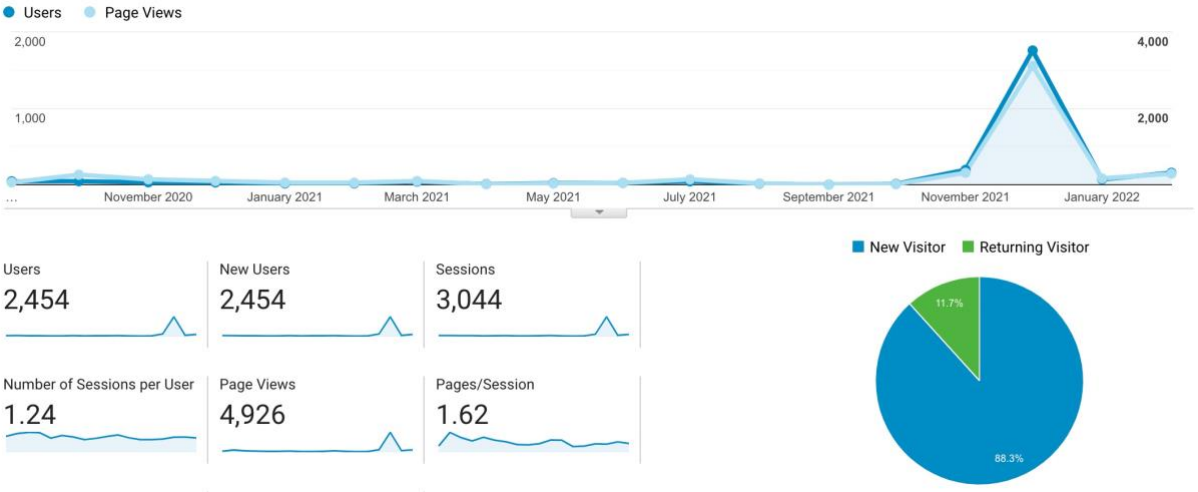

FIGURE 6: ASSURED WEBSITE ANALYTICS

4.1.2.2 Interviews with Technical Experts

Martel Innovate, with the collaboration of UBITECH, produced an interview series, in which we are talking about the future of security in next-generation smart connectivity systems comprising heterogeneous IoT and other types of cyber-physical systems. This is part of the vision of ASSURED towards creating some online webinars where experts are giving their insights on the core technical aspects that are been investigated in the context of the project. Besides this been an important dissemination avenue, it is also part of the project efforts towards creating additional training material as a medium for sharing knowledge on next-generation security protocol and defence mechanisms.

To date, two video interviews have been conducted with cybersecurity experts, explaining the project idea and challenges. One with Thanassis Giannetsos (UBITECH) and the second one with Ahmad Atamli (NVIDIA) who are both partners of the ASSURED project. The interviews are available on the project website and the project Youtube channel[11], and where circulated via social media channels (Twitter and LinkedIn). During the second half of the project further interviews with other experts will be conducted.

[11] Youtube channel: https://www.youtube.com/channel/UCSGTIRKPQAL91WPbJsV8Uwg

Funded by the Horizon 2020 Framework Programme of the European Union

FIGURE 7: ASSURED EXPERT INTERVIEW SERIES

4.1.2.3 1st ASSURED Workshop

FIGURE 8: CYSARM 2021 - HOMEPAGE

The ASSURED project was happy to announce the organisation of the third edition of the CYSARM workshop (3rd Workshop on Cyber-Security Arms Race - https://www.cysarm.org/) co-located with the 28th ACM Conference on Computer and Communications Security (CCS). The workshop was held remotely on November 19th, 2021, is a joint initiative of the most pertinent cyber-security and crypto-related EU H2020 projects: ASSURED, C4IIoT, PUZZLE, and RAINBOW.

Cybersecurity is a complex ecosystem that is based on several contradicting requirements. For this reason, it is often defined as an **arms race between attackers and defenders**: for example, when a new security model or algorithm is devised, it could act as a double-edged

Funded by the Horizon 2020 Framework Programme of the European Union

sword since it might both enhance the security posture of a system and introduce additional vulnerabilities. The goal of **CYSARM workshop** is to foster collaboration and discussion among cyber-security researchers and practitioners to discuss the various facets and trade-offs of cybersecurity and how new security technologies and algorithms might impact the security of existing or future security models.

4.1.2.4 Newsletters

Newsletters are efficient communication channel to provide news on the project progress and to discuss ongoing topics relevant to ASSURED for internal and external project partners, stakeholders and other interested bodies. Newsletters are amongst other tools part of the common dissemination strategy.

A newsletter will be produced by the ASSURED consortium on a quarterly basis and will provide regular updates on trends of cybersecurity innovation practices, project findings and results, news from industrial partners, among others.

The newsletters will also contain information regarding the upcoming tasks and events to inform the audience on how they can get in touch with the project and the connected initiatives. As such, a typical e-newsletter of the project will contain highlights (major outcomes, links, contacts, and dissemination activities), the most important news, announcements, and a schedule of the major upcoming events.

A mailing list has been created, based on subscription, giving the possibility to share the e-newsletter via mass mailing as well to inform interested users about project news, achievements and planning of events. A registration functionality allowing the interested visitors to subscribe to the newsletter is already available on the ASSURED website.

Through the Data Management Plan prepared by Martel Innovate (D8.2 at M06 and D8.3 at M24), it will be ensured that all these actions comply with the requirements of the General Data Protection Regulation (GDPR).

The 5 issues can be found on the project website: https://www.project-assured.eu/subscribe/

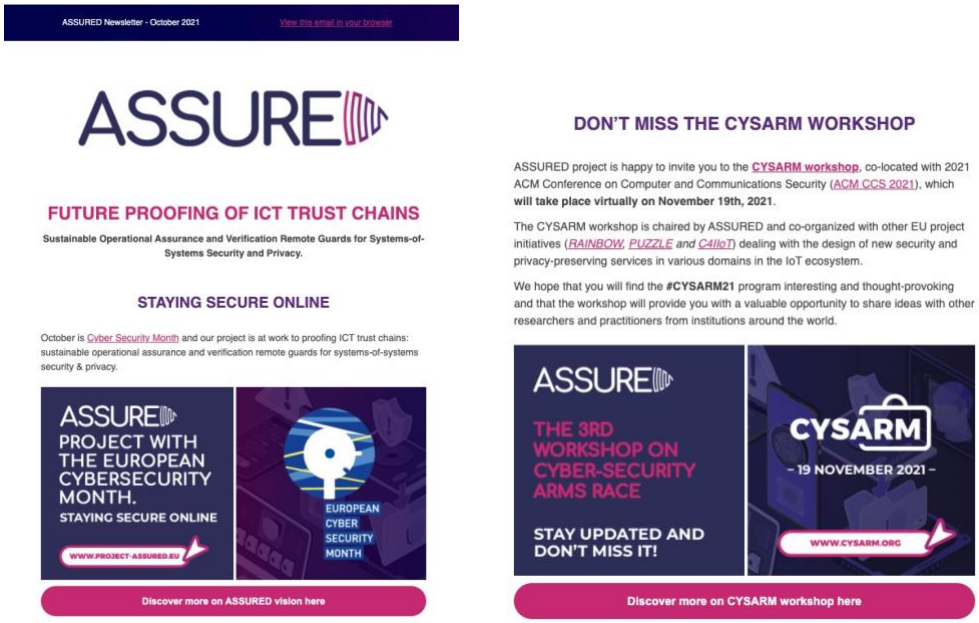

FIGURE 9: ASSURED NEWSLETTER - SCREENSHOT

Funded by the Horizon 2020 Framework Programme of the European Union

4.2 PHASE 2: CONTINUITY OF INFORMATION FLOW

The goal of the *Continuity of information flow* phase, which started approximately after the first year of the project, is to raise further awareness among our different target groups.

4.2.1 Past Communication Activities – Phase 2

The goal towards the *Broad Public Society & Media (A)* as well as towards the *Policymakers (B) and Industry (C)*, is to communicate the benefits of our ASSURED project for the society for example by explaining the impact of our project on everyday lives. Considering the penetration of complex "Systems-of-Systems" into all aspects of our lives, one can understand the importance of been able to dynamically assess the level of trustworthiness of each device and the entire system as a whole. An important message, e.g., to the Broad Public Society & Media, could be on the importance of designing new decentralized security solutions (avoiding current solutions that mainly rely on *isolation*) that can provide verifiable evidence on the security, assurance, and privacy of a service graph – an important aspect that will also allow the adoption and acceptance of such systems from the public. In addition to that, we can use our three use cases online banking, activity tracking and device management to communicate the benefits of a Trusted Platform Module to the society.

TABLE 3: PAST COMMUNICATION ACTIVITIES

Type of activities	Partner	Title	Date	Place	Audience[12]						Type and goal of the event / website
					A	B	C	D	O	Total	
Social Media	ALL	Twitter	recurrent	Online	x	x	x	x		185[13]	Regular tweets and re-tweets: https://twitter.com/Project_Assured
Social Media	ALL	LinkedIn	recurrent	Online	x	x	x	x		78[14]	Regular shares: https://www.linkedin.com/company/assured-project/

[12] Broad Public Society & Media (A), Policymakers (B), Industry (C), and Research Community (D), Other (O)

[13] Twitter followers from the beginning of the project (September 2020) till the end of February 2022

[14] LinkedIn followers from the beginning of the project (September 2020) till the end of February 2022

Funded by the Horizon 2020 Framework Programme of the European Union

Type of activities	Partner	Title	Date	Place	Audience[12]						Type and goal of the event / website
					A	B	C	D	O	Total	
Website	MAR + ALL	ASSURED project website	01/09/2020	Online	x	x	x	x	x	2454[15]	The project website was updated on a regular basis with interesting information on the project progress (blog entries, update on use cases, workshops, videos etc.) https://www.project-assured.eu/.

4.2.2 Past Dissemination Activities – Phase 2

Furthermore, we foster to disseminate knowledge and results with the Research Community (D) as well as with Policymakers (B) and the Industry (C). Therefore, scientific papers and articles are written and submitted to conferences and journals, presentations at workshops and conferences are given. Project partners were attending several conferences and workshops to spread information about the ASSURED project. Publications and certain public deliverables are published on the project website and on zenodo.org.

TABLE 4: PAST DISSEMINATION ACTIVITIES – PHASE 2

Type of activities	Partner	Title	Date	Place	Audience[16]						Type and goal of the event / website
					A	B	C	D	O	Total	
Participation to a conference	DTU	**TSN/A Conference 2020**	07-08 November 2020	Online	0	0	10	10	0	20	Security in Software Systems for the creation of secure service graph chains (considering also the transition to the 5G world). https://events.weka-fachmedien.de/tsna-conference/archive/
Participation to a conference	UBI	**ESCAR 2020**	11 November 2020	Online			200	120		320	Remote attestation in connected cars https://www.escar.info/history/escar-europe/escar-europe-2020-lectures-and-program-committee.html

[15] Website unique visitors from the beginning of the project (September 2020) till the end of February 2022

[16] Broad Public Society & Media (A), Policymakers (B), Industry (C), and Research Community (D), Other (O)

Funded by the Horizon 2020 Framework Programme of the European Union

Type of activities	Partner	Title	Date	Place	Audience[16]						Type and goal of the event / website
					A	B	C	D	O	Total	
Participation to a conference	UTRC	**HIPEAC Conference 2021**	18 January 2021	Online			10	50		60	ASSURED project dissemination via virtual booth. https://www.hipeac.net/2021/spring-virtual/#/
Participation to an internal conference	UTRC	**Collins Computing Conference**	02-04 March 2021	Online			75			75	Attestation and security
Participation to a webinar	DTU	**Security and Trust with TPMs**	22 March 2021	Online			20	20		40	Remote attestation https://english.ida.dk/event/security-and-trust-with-trusted-platform-modules-webinar-339057
Participation to other event	SUR	**ISO/IEC JTC 1/SC 27/WG 2 "Cryptography and security mechanisms"**	12-15 April 2021	Online		5		10	35	50	ISO meeting. Protocol standardisation. Ongoing discussions on key management and crypto primitives to be used in attestation schemes and for the management of Verifiable Credentials. Standardized Attestation schemes, Key management, encryption schemes etc.. that may be adopted for ASSURED. https://sd.iso.org/documents/open/de783177-bdd3-4bdf-a076-6805af0fb038
Participation to a conference	TUDE	**ICASSP 2021**	06-11 June 2021	Online				100		100	Data protection https://www.2021.ieeeicassp.org/2021.ieeeicassp.org/index.html
Participation to a conference	UBI	**EuCNC 2021**	07-10 June 2021	Online			25	55		80	Attestation in 5G https://www.eucnc.eu/

Funded by the Horizon 2020 Framework Programme of the European Union

Type of activities	Partner	Title	Date	Place	Audience[16]						Type and goal of the event / website
					A	B	C	D	O	Total	
Participation to a conference	DTU	**ACM WiSec 2021**	28 June - 2 July 2021	Online			50	60	40	150	Revocation https://sites.nyuad.nyu.edu/wisec21/
Participation to a workshop	SPH + UBI	**Securing Future Networks**	8 July 2021	Online				48		48	Enabling Security and Privacy in Next-Generation Smart Connectivity Systems. https://meditcom2021.ieee-meditcom.org/authors/call-for-special-sessions/
Participation to a conference	DTU	**International Conference on Distributed Computing**	14-16 July 2021	Online				60		60	Key exfiltration attack https://dcoss.org/dcoss21/
Participation to a conference	DTU	**IEEE CSR 2021**	26-28 July 2021	Online			15	45		60	Remote attestation https://www.ieee-csr.org/
Participation to a workshop	DTU	**Future-Proofing the Connected World**	31 July 2021	Jyderup, DK				10	50	60	Remote attestation https://thecamp.dk/
Participation to an internal conference	UTRC	**RTX Cyber Summit**	July-Sep/2021	Online	50	50	100	400		650	Attestation
Participation of other event	DTU	**IEEE P802.1DG Meeting**	10 August 2021	Online		4	50	5		59	Ongoing activities on the definition of protection profiles for heterogeneous systems in industrial automation.

Funded by the Horizon 2020 Framework Programme of the European Union

Type of activities	Partner	Title	Date	Place	Audience[16]						Type and goal of the event / website
					A	B	C	D	O	Total	
											https://listserv.ieee.org/cgi-bin/wa?A2=ind21&L=STDS-802-1-MINUTES&O=A&P=316563
Participation to a conference	TUDE	**USENIX SECURITY 2021**	11-13 August 2021	Online			10	127		227	Data protection https://www.usenix.org/conference/usenixsecurity21
Participation to a conference	UBI	**IEEE MeditCom 2021**	07-10 September 2021	Online			12	65		77	Tracing and attestation https://meditcom2021.ieee-meditcom.org/
Participation to a workshop	UBI	**International Workshop on Security and Trust Management**	08 October 2021	Online				43		43	Security analysis of remote attestation https://www.nics.uma.es/stm2021/
Participation to a workshop	SUR	**Cyber Security in a Post Quantum World**	13 October 2021	Online				30	35	65	Post Quantum Attestation schemes, Key management, encryption schemes etc.. that may be adopted for ASSURED in the Future. https://www.youtube.com/channel/UCUcogwm4HL0YejDuggiSA2w
Participation to other event	SUR	**ISO/IEC JTC 1/SC 27/WG 2 "Cryptography and security mechanisms"**	25-27 October 2021	Online		5		10	35	50	ISO meeting. Protocol standardisation. Discussion on Attribute-based Encryption, group and ring signatures. Standardized Attestation schemes, Key management, encryption schemes etc.. that may be adopted for ASSURED. https://sd.iso.org/documents/open/de783177-bdd3-4bdf-a076-6805af0fb038

Funded by the Horizon 2020 Framework Programme of the European Union

Type of activities	Partner	Title	Date	Place	Audience[16]						Type and goal of the event / website
					A	B	C	D	O	Total	
Participation to a conference	DTU	**Driving IT '21**	05 November 2021	Copenhagen			35	125		160	Remote attestation https://videos.ida.dk/category/Teknologi%3EIT_+tele+og+elektronik%3EIT%3EDriving+IT+K%C3%B8benhavn+2021/235923713
Participation to a conference	ALL	**ACM CCS 2021**	14-19 November 2021	Online			12	65		77	https://www.sigsac.org/ccs/CCS2021/
Participation to a conference	DAEM	**SCEW 2021**	16-18 November 2021	Barcelona			2000	6000		8000	Smart cities solutions https://www.smartcityexpo.com/
Participation to a workshop	ALL	**CYSARM '21**	19 November 2021	Online				55		55	CYSARM 2021: attestation, security, privacy. Standardized Attestation schemes, Key management, encryption schemes etc., that may be adopted for ASSURED. https://www.cysarm.org/
Participation to a workshop / roundtable	UBI	**Transnational Workshop on SEMS and Smart Grids**	1 December 2021	Online		5	25	40		70	Attestation as security enabler in the smart grid application domain. https://ithaca.ece.uowm.gr/jaunty_multiplier_event/
Participation to a webinar	TUDE	**Cybersecurity & Manufacturing webinar 2021**	07 December 2021	Online			20	30		50	Cybersecurity for manufacturing https://www.eitmanufacturing.eu/news-media/events/cybersecurity-manufacturing-webinar/

Funded by the Horizon 2020 Framework Programme of the European Union

Type of activities	Partner	Title	Date	Place	Audience[16]						Type and goal of the event / website
					A	B	C	D	O	Total	
Participation to a conference	TUDA	**Horizon Cloud Summit 2021**	8-9 December 2021	Frankfurt		20	60	160	60	300	https://www.h-cloud.eu/event/horizon-cloud-summit-2021/
Participation to a conference	DTU	**FPS 2021**	08-10 December 2021	Paris			40	60		100	Remote attestation http://www.fps-2021.com/
Organsation and participation to a workshop	UBI + MAR + ALL	**ASSURED 1st Clustering Workshop**	13 December 2021	Online		5		10	48	63	The Clustering Workshop aims at bringing together projects that target Supply Chain Security, Resilience and Certification aspects, experts, members and consultants from standardisation and certification bodies for exploring synergies and identifying actions that can be pursued in common. https://www.project-assured.eu/event/future-proofing-and-certifying-supply-chains/
Participation to a workshop	UBI	**Dagstuhl Seminar on Privacy Protection on Automated and Self-Driving Vehicles**	23 -28 January	Online			10	25		35	Revelance to ASSURED: Trust Modelling, Privacy and Direct Anonymout Attestation. Attendance and presentation https://www.dagstuhl.de/en/program/calendar/semhp/?semnr=22042
Participation to a webinar	S5	**How to start using Blockchain for innovation and**	15 February	Online			10	127		137	There is an ongoing and intensifying hype over crypto coins, the potential of Web 3.0 approaches and more recently about sales of NFTs. Last year record sums of VC investments went to companies in this field. But, how can

Funded by the Horizon 2020 Framework Programme of the European Union

Type of activities	Partner	Title	Date	Place	Audience[16]						Type and goal of the event / website
					A	B	C	D	O	Total	
		real-world projects									"normal" companies use blockchain? How can a start-up extend towards decentralisation concepts? https://www.ngi.eu/event/webinar-how-to-start-using-blockchain-for-innovation-and-real-world-projects/
Participation to a webinar	UBI	**GDPR Fundamentals: straight to the point!**	23 February	Online		5	15	40		60	How can this Regulation on data protection benefit my project? How to integrate the concept to ensure compliance? This webinar has been designed to help you practically manage the personal data principles through an understanding of its main concepts, how to integrate successfully the GDPR rules into your projects, and how to develop best practices. https://www.ngi.eu/event/webinar-gdpr-fundamentals-straight-to-the-point/

With all past dissemination activities carried out by ASSURED project partners in Phase 2 and listed in Table 4, we assume that we reached approximately 10000 people, mainly from the Research Community (D) and the Industry (C). The amount of person indicated in the table above is of course a best estimate, made by each project partner who attended an event and somehow disseminated our ASSURED project. The goal was to raise awareness and to make the ASSURED project more public. In some activities the project was explained in detail in a keynote/presentation, in other activities ASSURED was represented with a poster presentation or partners distributed leaflets, talked about the project, etc. The consortium is satisfied with the number of audiences reached until now and will do its best to reach further people in the the coming months.

Funded by the Horizon 2020 Framework Programme of the European Union

4.2.3 Highlights – Phase 2

4.2.3.1 Social Media

Social media is a very powerful tool to communicate and disseminate information and to effectively let people know about the activities we carry out in our ASSURED project, that's why we created, in September 2020, a ASSURED Twitter and as well as a LinkedIn account. Both accounts are updated on a regular basis, to schedule the postings and tweets, we have created a posting plan, which helps us to plan and organize upcoming content.

4.2.3.2 Twitter

Twitter is a microblogging and social networking service on which users post and interact with text-based messages of up to 280 characters, known as "tweets". Registered users can post, like, and retweet tweets, but unregistered users can only read those that are publicly available. The ASSURED project is available on https://twitter.com/Project_Assured.

Since the beginning of the project, ASSURED published 190 tweets and is mainly used for communication activities, including the announcement of the project website, news, press releases, newsletter publications and different meetings. The engagement rate (the number of engagements clicks, likes, retweets, replies) is around 3% and the account has 185 followers (status 27.02.2022).

At the moment we are satisfied with the number of followers. The goal is to reach 300 followers by the end of the project.

FIGURE 10: ASSURED TWITTER ACCOUNT

4.2.3.3 LinkedIn

LinkedIn is a social networking site for people in professional occupations or simply a social network for business. The ASSURED project has a public company page, which can be reached at https://www.linkedin.com/company/assured-project/. Until the end of February

Funded by the Horizon 2020 Framework Programme of the European Union

2022, the ASSURED team has established a good network on the social media platform and gathered 78 interesting and professional followers. Information (publications, deliverables, conferences, workshops) on the project is posted on a regular basis. We can report that the engagement rate (6,54%) on our LinkedIn page is quite good and that our followers are interested in the posted content. (Engagement measures the number of likes, shares, and comments our social updates receive. In our opinion a good engagement rate is more important than just the number of followers.)

We are satisfied with the number of followers attracted to date, also because they all are interesting contacts for the project and the work in related fields. The goal is to reach at least 100 followers by the end of the project and build a network interested in the results of ASSURED.

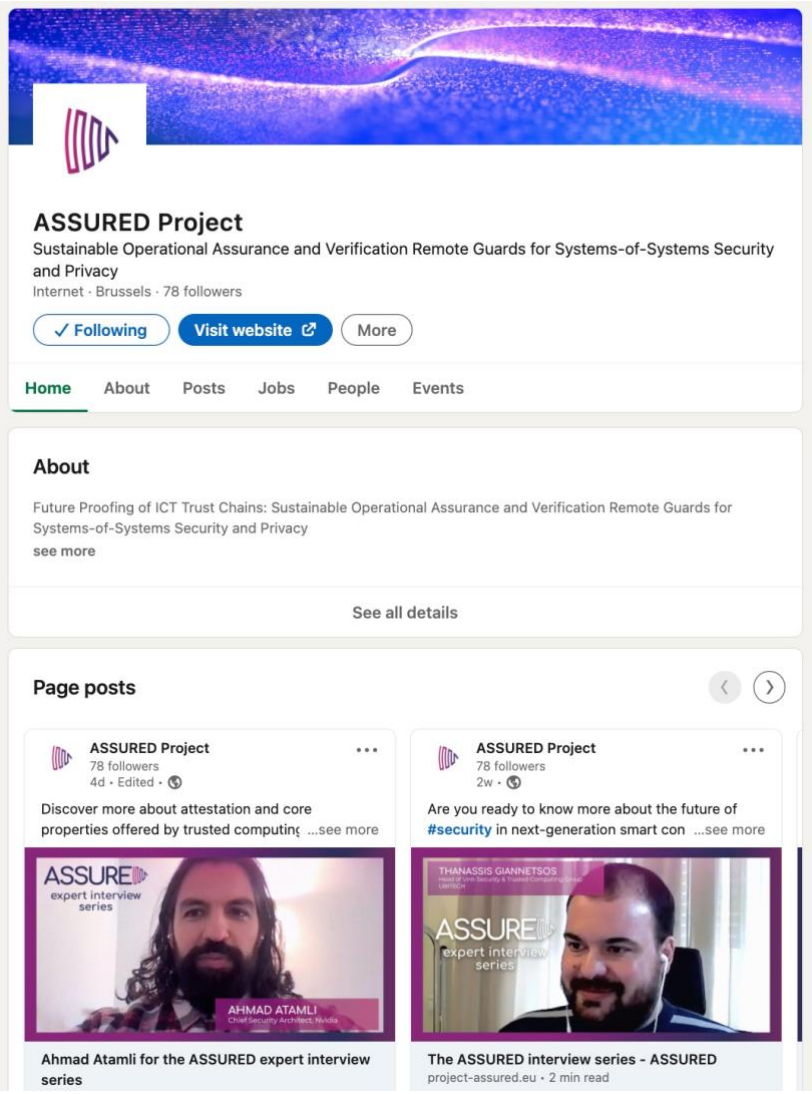

FIGURE 11: ASSURED LINKEDIN COMPANY PAGE

Funded by the Horizon 2020 Framework Programme of the European Union

4.2.3.4 Open Access to Scientific Publications

As soon as a paper has been published, the Consortium is committed to provide open access via the EU compliant repository ZENODO (https://zenodo.org/), where also an ASSURED community[17] has been established (not all the papers are already listed there, we are asking to the partners to updated the related info). ZENODO is convenient to access and also easy to use. This repository allows to easily share the long tail of small research results in a wide variety of formats including text, spreadsheets, audio, video, and images across all fields of science. Further, each uploaded publication and dataset receives a persistent identifier (DOI), which ensures long term preservation. If relevant, also underlying research data will be made publicly available and linked to the specific publication.

The ASSURED Consortium published 18 papers during the first 18 month of the project (for better monitoring of the project progress, we are also putting forth papers that have been accepted but are pending official publications in proceedings). Furthermore, out of these 18 scientific publications, more than 5 papers were the result of the strong collaboration between the consortium partners working on the core project artefacts in the fields of trusted computing, cryptology, formal modelling and remote attestation algorithms. The publications which are already on https://zenodo.org/ were viewed approximately 287 times and downloaded approximately 241 times from the ZENODO platform:

TABLE 5: SCIENTIFIC PUBLICATIONS

Title	Authors	Journal/ Conference	DOI (publisher)	Views[18] (Zenodo)	Downloads[19] (Zenodo)
RealSWATT: Remote Software-based Attestation for Embedded Devices under Real-time Constraints	C. Niesler, S. Surminski, F. Brasser, L. Davi, A.R. Sadeghi	CCS 2021	https://doi.org/10.1145/3460120.3484788	11	9
Incrementally Updateable Honey Password Vaults	H. Cheng, W. Li, P. Wang, C.H. Chu, K. Liang	USENIX Security 2021	https://doi.org/10.5281/zenodo.6036266	12	9
Practical Threshold Multi-Factor Authentication	W. Li, H. Cheng, P. Wang, K. Liang	IEEE TIFS 2021	https://doi.org/10.1109/TIFS.2021.3081263	8	8

[17] ASSURED Community on ZENODO: https://zenodo.org/communities/assured/

[18] Record date: 27/02/2022

[19] Record date: 27/02/2022

Funded by the Horizon 2020 Framework Programme of the European Union

Title	Authors	Journal/ Conference	DOI (publisher)	Views[18] (Zenodo)	Downloads[19] (Zenodo)
Direct Anonymous Attestation on the Road: Efficient and Privacy-Preserving Revocation in C-ITS	B. Larsen, T. Giannetsos, I. Krontiris, K. Goldman	WiSec 2021	https://doi.org/10.5281/zenodo.5084383	12	9
Root-of-Trust Abstractions for Symbolic Analysis: Application to Attestation Protocols	G. Fotiadis, J. Moreira, T. Giannetsos, L. Chen, P. B. Rønne, M. D. Ryan, P. Y. A. Ryan	STM 2021	https://doi.org/10.5281/zenodo.5546761	27	23
A Perfect Match: Converging and Automating Privacy and Security Impact Assessment On-the-Fly	D. Papamartzivanos, S.A. Menesidou, P. Gouvas, T. Giannetsos	MDPI Journal: Information and Future Internet Security, Trust and Privacy	https://doi.org/10.3390/fi13020030	43	41
Segregating Keys from noncense: Timely Exfil of Ephemeral Keys from Embedded Systems	H. Bergson Debes, T. Giannetsos	DCOSS 2021	https://doi.org/10.5281/zenodo.5084306	27	23
Towards Efficient Control-Flow Attestation with Software-Assisted Multi-level Execution Tracing	D. Papamartzivanos, S.A. Menesidou, P. Gouvas, T. Giannetsos	MeditCom 2021	https://doi.org/10.5281/zenodo.5546750	24	49
Towards 5G Embedded Trust: Integrating Attestation Extensions in Vertical Industries	T. Giannetsos, D. Papamartzivanos, S. A. Menesidou, S. Karagiorgou	EuCNC 2021	https://doi.org/10.5281/zenodo.5337038	14	14
Reviewing ISO/IEC Standard for Time-stamping Services	L. Meng, L. Chen	IEEE Communications Standards Magazine	https://doi.org/10.5281/zenodo.5546754	26	13
Analysis of Client-side Security for Long-term Time-stamping Services	L. Meng, L. Chen	ACNS 2021	https://doi.org/10.5281/zenodo.5546769	27	16
State-of-the-Art Software-Based Remote Attestation: Opportunities	S. F. J. J. Ankergård, E. Dushku, N. Dragoni	Sensors 2021	https://doi.org/10.3390/s21051598	13	8

Funded by the Horizon 2020 Framework Programme of the European Union

Title	Authors	Journal/ Conference	DOI (publisher)	Views[18] (Zenodo)	Downloads[19] (Zenodo)
and Open Issues for Internet of Things					
ERAMO: Effective Remote Attestation through Memory Offloading	J. Hagelskjær Østergaard, E. Dushku, N. Dragoni	IEEE CSR 2021	https://doi.org/10.1109/CSR51186.2021.9527978	6	5
RESERVE: Remote Attestation of Intermittent IoT devices	MD Masoom Rabbani, E. Dushku, J. Vliegen, A. Braeken, N. Dragoni, N. Mentens	ACM SenSys 2021	https://doi.org/10.5281/zenodo.6036103	12	7
ARCADIS: Asynchronous Remote Control-Flow Attestation of Distributed IoT Services	R. M. Halldórsson, E. Dushku, N. Dragoni	IEEE ACCESS	https://doi.org/10.1109/ACCESS.2021.3122391	9	7
Improved Probabilistic Context-Free Grammars for Passwords Using Word Extraction	H. Cheng, W. Li, P. Wang, K. Liang	ICASSP 2021	https://doi.org/10.1109/ICASSP39728.2021.9414886	6	5
BlindTrust: Oblivious Remote Attestation for Secure Service Function Chains	H. Bergsson Debes, T. Giannetsos, I. Krontiris	arXiv	https://doi.org/10.5281/zenodo.6036588	10	4
PERMANENT: Publicly Verifiable Remote Attestation for Internet of Things through Blockchain	S. F. J. J. Ankergård, E. Dushku, N. Dragoni (from Technical University of Denmark (DTU)	FPS 2021	Not available yet	Not on Zenodo yet	Not on Zenodo yet

Funded by the Horizon 2020 Framework Programme of the European Union

4.2.3.5 Related Projects

In order to create information flow with external parties, a "Related Project List" has been created. Those projects were integrated into the ASSURED website by following this link: https://www.project-assured.eu/links/. The coordinators of the projects which are still running have been contacted via email. We provided them with some basic information about the project, the link to the ASSURED flyer and poster and ask for permission to link their website to the ASSURED one.

ASSURED organized together with the H2020 C4IIOT, PUZZLE, and RAINBOW projects the *3rd Workshop on Cyber-Security Arms Race (CYSARM)* (https://www.cysarm.org/), co-located with the 29th ACM Conference on Computer and Communications Security (CCS).

In addition to that ASSURED organized and will organize together with the H2020 CYRENE project a series of clustering workshop with the goal of bringing together projects that target Supply Chain Security, Resilience and Certification aspects, experts, members and consultants from standardisation and certification bodies for exploring synergies and identifying actions that can be pursued in common. The first edition of the "**Future Proofing and Certifying Supply Chains**[20]" clustering workshop was held on the 13th of December 2021 and brought together the H2020 SANCUS, FISHY, MEDINA, BIECO, IoTAC, and SIFIS-Home projects.

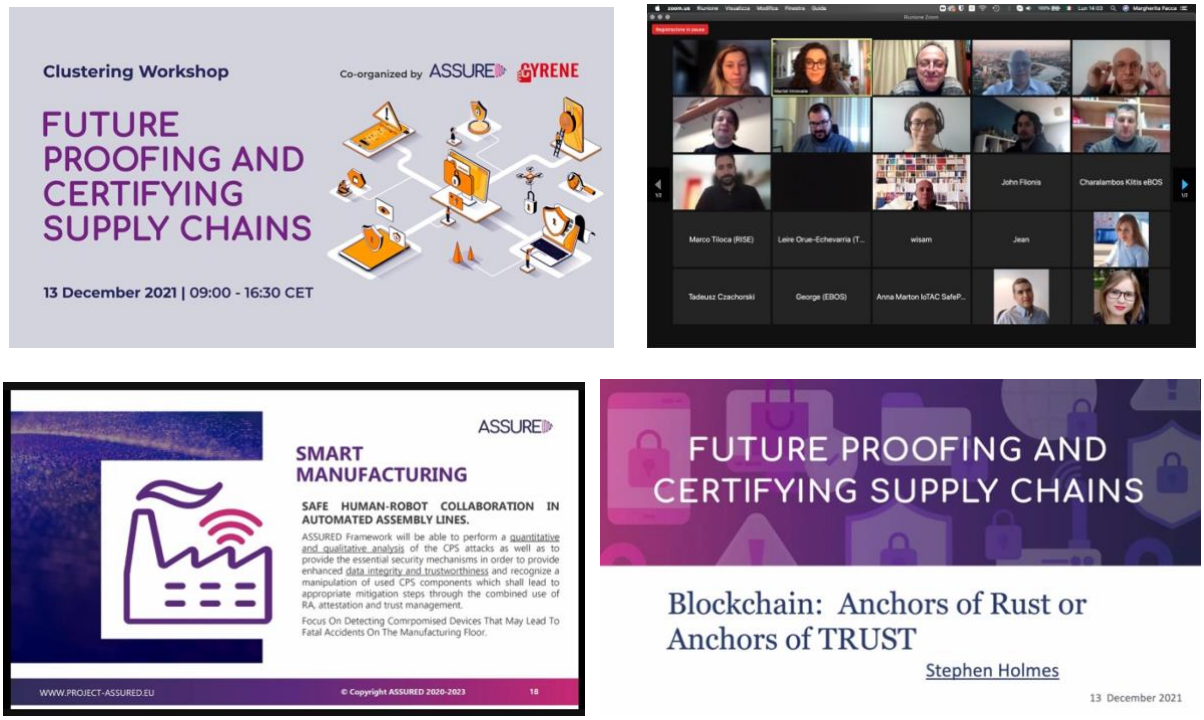

FIGURE 12: "FUTURE PROOFING AND CERTIFYING SUPPLY CHAINS" CLUSTERING WORKSHOP – SCREENSHOTS FROM THE ONLINE EVENT

4.2.4 Planned Activities – Phase 2

The following section presents the planned dissemination and communication activities planned (after M18) until the project end identified by the project partners. The lists are

[20] https://www.project-assured.eu/event/future-proofing-and-certifying-supply-chains/

Funded by the Horizon 2020 Framework Programme of the European Union

regularly monitored and updated, so all the partners are aware of possible opportunities to disseminate, and each activity is aligned with the others.

All consortium partners are involved in the planning of newsletters and press releases and participate in the creation and dissemination of these materials. The coordinator MARTEL manages and continuously updates the ASSURED LinkedIn and Twitter accounts to raise awareness about the ASSURED project among the general public and to its own stakeholders. Project partners are also encouraging external persons to follow the project on Twitter and LinkedIn, and those having a social media account also promote the project with frequent activities.

4.2.4.1 Scientific Events and Conferences

The ASSURED project will continue the CYSARM series by organizing the 4th edition of the CYSARM workshop together with the CCS conference in 2023. Furthermore, in August 2022, ASSURED will organize its second scientific workshop on *Security and Assurance Claims for Next-Generation Smart Systems* where the focus would be on disseminating the implemented ASSURED mechanisms (including also the results of the round of evaluation) to industrial partners, standardisation committees and research industry.

This workshop will aim at presenting a first set of preliminary results in researching assurance, attestation and cryptographic algorithms suitable for protecting the next-generation of complex systems by leveraging also the TPM as an underlying root-of-trust. A TPM is a security anchor, also known as root-of-trust, which is commonly used in domains with a strong requirement for security, privacy and trust, such as finance and banking (secure mobile payment), wearables (activity tracking) and device management.

4.2.4.2 Social Media

ASSURED Twitter and LinkedIn accounts will be frequently updated with news about the project. In addition to that the project website will be updated with all the relevant news and announcements, conferences, workshops, publications, meetings, etc.

4.2.4.3 Newsletters

Several further issues of the newsletter are planned until the project end. The newsletters will be created and published in correlation with the entire team after the achievement of certain results and milestones. At least three more issues are foreseen.

Funded by the Horizon 2020 Framework Programme of the European Union

4.2.5 Overview of Planned Presentations, Conferences, Exhibitions, Fairs, Workshops, etc.

In order to get a better overview of upcoming events, where participation is envisaged by one or more partners, the consortium established a dissemination plan for 2022 and 2023, a list for upcoming events and other dissemination activities (Table 6 – *it's a living document and will be updated on a quarterly basis*). This list complements the already existing list, where we collect past dissemination activities. Upcoming as well as past conferences are also listed on the project website.

TABLE 6: PLANNED DISSEMINATION ACTIVITIES - PHASE 2

Type of activities	Partner	Title	Date 2022	Place	Audience[21]						Description
					A	B	C	D	O	Total	
Participation to a conference	UBI	**Cybersecurity Standardisation Conference**	15 March	Online	30	50	150	150	20	400	Be aligned with the latest activities in the standardisation working groups for certification (CEN, CENELEC) and ETSI on securing technologies like digital wallets, infrastructure and supply chains, etc https://www.enisa.europa.eu/events/cybersecurity_standardisation_2022
Participation to a conference	S5	**European Cyber Security Conference 2022**	24 March	Brussels and Online						tbd	Gathering leading policymakers, industry players, high level cyber security and defence experts, this Forum Europe conference, organised in partnership with the European Cyber Security Organisation (ECSO), will explore Europe's response to cyber security issues in a dynamically evolving global risk landscape and what the next steps for all actors of the ecosystem should be to create a safe and secure environment allowing Europe to leverage the tremendous socio-economic benefits offered by digital technologies. https://eucybersecurity.com/

[21] Broad Public Society & Media (A), Policymakers (B), Industry (C), and Research Community (D), Other (O)

Funded by the Horizon 2020 Framework Programme of the European Union

Type of activities	Partner	Title	Date 2022	Place	Audience[21]						Description
					A	B	C	D	O	Total	
Participation to a workshop	UBI, TUDA, SURREY, TUDE	**Key challenges in global cybersecurity: Efforts and trends in EU**	28 March	Online		10	30	50		90	CYRENE, FISHY, and IoTAC, are organizing a joint workshop trying to track current research in cybersecurity, especially in the fields of IoT and supply chain but also open to other cybersecurity research areas and projects. The Workshop will be co-located with the DRCN2022 Conference. https://www.cyrene.eu/kcyeu-2022-workshop-call-for-papers/
Participation to a conference	DTU	**Privacy Symposium 2022**	5-7 April	Venice, Italy	10		20	60	10	100	The Privacy Symposium aims at promoting international dialogue, cooperation, and knowledge sharing on data protection regulations, compliance, and emerging technologies. https://privacysymposium.org/
Participation to other event	UBI + MAR	**Global IoT Day Roundtable**	8 April	Online		10	20	30		60	The need for IoT security standardisation and certification. (Link not available yet)
Participation to other event	MAR	**IoT Week 2022**	20-23 June	Dublin						tbd	The Internet of Things (IoT) technologies are heavily interwoven within every-day present life and tomorrow will impact even more. Predicting the next global tendency but need in society is key to IoT development. https://iotweek.org/

Funded by the Horizon 2020 Framework Programme of the European Union

4.3 RESUME DISSEMINATION AND COMMUNICATION ACTIVITIES – PHASE 1 & 2

Communication activities to promote the project itself and its success, as well as the dissemination of results are key areas of our H2020 ASSURED project. Our goal is, to bring research and its outcomes to the attention of non-scientific audiences, scientific community, potential business partners or policymakers. To achieve this, we have created our ASSURED dissemination and communication strategy described in Chapter 2

The ASSURED project has successfully passed the first phase “awareness creation and marketing foundation” and the project team has prepared the necessary communication and dissemination material (corporate design, leaflets, website social media channels, etc.) We would like to point out, that this work was carried out jointly and all project partners, especially the technical and the WP leaders were involved.

The project is now in the second phase called *“stakeholders outreach and engagement bootstrap”*. In the past months the partners submitted 18 papers to conferences and journals and presented the project at different conferences and workshops in order to further raise awareness among stakeholders. The project website and the social media channels (LinkedIn and Twitter) are updated on a regular basis with news from the project. At the moment the consortium is satisfied (compared to other projects) with the number of followers and visitors (compared to other projects), but we will work hard to boost the project in the upcoming months more.

4.4 PHASE 3: RESULT ORIENTATION

The ASSURED project will enter this third phase towards the end of the project. The result orientation phase consists of three main goals:

- Promotion of project results
- Exploitation activities (see exploitation strategies in Chapter 5)
- Attraction of the target group

The ASSURED consortium has currently the following plans for phase 3 (see table below).

Phase 3: Result orientation				
ASSURED Scientific Workshop	General public, scientific community, industry, policymakers, medias, investors, customers	End of the project	To disseminate and show case the results of the project to a larger audience from academia and industry. *KPI: 50/70 people are expected to attend this workshop.*	All

Funded by the Horizon 2020 Framework Programme of the European Union

5 MARKET ANALYSIS AND EXPLOITATION

This chapter presents an initial market analysis, including market expectations of the individual ASSURED industrial partners and the project's exploitation strategy, including partners' individual exploitation plans as well as joint strategies. As aforementioned, Information on the market, business opportunities and market expectations form the industry partners will be documented in Deliverable D7.4 and 7.5 on "Market Analysis, Business and Sustainability Plan". Thus, in D7.2 an initial introduction of the market which ASSURED targets is put forth based on the list of the exploitable assets that the consortium aims at producing at the end of the project.

5.1 MARKET ANALYSIS AND BUSINESS OPPORTUNITIES

The last couple of years saw a big shift in what is considered the protagonist in value generation. Today, all agree that it is not the services or infrastructures that should be the key focus of operations; the focus should be on data. Traditionally, data has not received the credits it deserved but the perception started changing in the recent years with the advent of methods that can analyse data, deliver insights, and generate knowledge, which ultimately is what is needed for every production system to operate.

One of the most valuable sectors of the data economy is that of personal data of any kind. Such type of data includes personal identifiable information, health data, activity and social life data, personal financial data, etc. Due to the fact that a person who possess data can gain huge economic benefits, the sector has been greatly exploited and abused in recent years. Apart from the economic benefits one could gain my manipulating personal data, there may be situations where critical conditions develop, especially when health and financial data are tampered with.

In the past decade, a new market was born thanks to innovations bought forward by small wearable devices, such as smartwatches offered by FitBit, Garmin, and other companies. Since its introduction to the market, the daily activity and health data tracking has seen a tremendous growth, especially when big players like Apple and Samsung, among others, entered the picture by offering devices and applications for everyday users, and not just those engaged in sports.

A recent report issued by Gallup says that as many as one in five adults in the U.S. track their activities using wearable trackers[22]. The report also points out that the global market of tracking devices is growing exponentially. As of November 2019, FitBit alone has 28 million active users across the globe, having sold more than 100 million devices.[23] According to another report[24], the market, that has been heavily impacted by the growing penetration of smartphones and the innovations in the healthcare sector is expected to reach $14.64 billion by 2027. Its popularity is starting to reach beyond healthcare, constantly attracting more and more industries, such as ICT industries, which help to transform healthcare into a digital industry. At the same time, the wearable devices are forecasted to grow with a CAGR of 23.2% over the same forecast period. A recent report by Statista[25] shows that in 2020 around 396 million wearable devices were shipped, which translates into an expected consumer spending of

[22] https://news.gallup.com/poll/269096/one-five-adults-health-apps-wearable-trackers.aspx

[23] https://www.transparencymarketresearch.com/health-tracking-apps-market.html

[24] https://www.globenewswire.com/news-release/2020/05/14/2033925/0/en/Fitness-App-Market-To-Reach-USD-14-64-Billion-By-2027-Reports-and-Data.html

[25] https://www.statista.com/topics/4393/fitness-and-activity-tracker/

Funded by the Horizon 2020 Framework Programme of the European Union

$62,96 billion in 2021, just for wearables. These numbers were also expected to be impacted by the COVID-19 pandemic, as people are becoming more eager to be able to monitor their health status.

Countless Internet of Things (IoT) devices are connected to the internet every day while people need to gather and process massive amounts of information from the real world. The advent of 3GPP 5G, allowing for a massive information exchange, is a game changer in IoT. However, enhanced connectivity and IoT's low security have led to vast attacks, hindering a wide-spread adoption of IoT[26]. The Mirai IoT botnet is perhaps the most known example of IoT deficits[27]. Cyber-attacks get more sophisticated every day, affecting a large number of IoT-related infrastructures and raising serious security and privacy concerns among private consumers and businesses. It is estimated that the total cost of data breaches will increase by as much as 70%, from $3 trillion in 2019 to over $5 trillion in 2024. This highlights the importance of proper IoT security management and the need for further enhancements of IoT infrastructures with continuous security improvements integrated into the IoT lifecycle management. This is not a trivial task considering IoT device heterogeneity, dynamism of the security landscape, and the number of IoT stakeholders. Any security change caused by a new vulnerability or an insecure update (e.g., patch) on a single device can put the whole IoT system at risk. Security management of IoT infrastructures encompassing full lifecycle of products and continuous certification is a fundamental tool to guarantee a high-level of security, as emphasized by the European Union Agency for Cybersecurity (ENISA) Cybersecurity Act (CSA)[28]. Indeed, an effective security framework must stimulate collaboration among IoT stakeholders (e.g., auditors, manufacturers, users) as pointed out by the Network and Information Security (NIS) directive[29].

Furthermore, in recent years, there has been a shift in the type of security breaches that become the most prominent in the IoT systems (as indicated by OWASP[30]) where insecure design, security misconfiguration, and vulnerable and outdated components seem to be the highest exploitable vulnerabilities. Therefore, a holistic mechanism capable of protecting against a wide set of such vulnerabilities is of paramount importance.

ASSURED provides IoT stakeholders with mechanisms achieving high-level of security. ASSURED will detect and respond to a wide spectrum of attack, in a collaborative/decentralised fashion.

As described by ENISA (PROACTIVE DETECTION - GOOD PRACTICES GAP ANALYSIS RECOMMENDATIONS), "*proactive detection of incidents is defined as the process of discovering malicious activity*". ASSURED's attestation enablers comprise complete host- and network-based intrusion detection system for the IoT environment and the market of NIDS is

[26] https://www.gartner.com/smarterwithgartner/the-iot-effect-opportunities-and-challenges-2/

[27] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[28] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[29] https://digital-strategy.ec.europa.eu/en/policies/nis-directive

[30] https://owasp.org/Top10/

Funded by the Horizon 2020 Framework Programme of the European Union

growing. Markets and Markets have reported[31] that "the global cloud IDS IPS market is expected to grow from USD 600.9 Million in 2017 to USD 1,764.7 Million by 2022, at a Compound Annual Growth Rate (CAGR) of 24.04% during the forecast period". Big players involved are CISCO, Intel, Trend Micro, among others. Open-source products such as Suricata and Snort are also available and widely used but mainly in the U.S. and/or Asia (the EU market is almost non-existent). However, the same growth cannot be seen when it comes to host-based detection systems where there is a lack of well-established detection and assurance systems. This is where ASSURED comes to fill the gap.

Another important aspect that should be considered is that growth in connected devices, as part of future supply chains (in various application domains, such as the Industry 4.0, smart manufacturing, secure aerospace, automotive, etc.) furthers the need for strong authentication in the context of Self-Sovereign Identity (SSI). Connected IoT devices, for instance in the smart manufacturing domain, continue to improve outcomes and reduce operational and maintenance costs. 451 Research's Global IoT Market Monitor projects that the number of connected smart devices, such as assistive personnel monitoring devices, human-robot collaboration devices, and those found in smart manufacturing facilities, will grow from 39.5 million to 94.9 million between 2019 and 2024, representing a CAGR of 19%. It has been predicted that by 2024, such deployed devices will collectively make up 50% of total manufacturing floors. Unfortunately, as the number of devices continues to grow, so does the attack surface, which increases the already critical need for more robust device security, including strong authentication capabilities. This has been further evidenced by 451 Research's Voice of the Enterprise: Information Security, Organisational Dynamics 2019 survey, in which 15% of manufacturing respondents identified the poor authentication capabilities of IoT endpoints as the greatest security threat facing their organisations' IoT initiatives.

The safety risks of weak device authentication are real; the ability to remotely manipulate a device poses a direct threat to workers safety. For example, in a manufacturing environment, a ransomware attack, such as WannaCry could easily spread among robots that lack methods of validating data and device integrity. Various British working stations were among the organisations hit hardest by WannaCry, which took down instruments and other devices for extended periods, delaying the manufacturing process as part of the entire supply chain. The safety concern associated with such types of devices is so great that in 2017, Abbott Labs recalled nearly half a million of healthcare devices for an update after the discovery of a safety-critical vulnerability. In addition to the safety risks, stakeholders face extensive financial risk due to poorly secured devices – the impact of extended downtime on a factory's revenue and the impact of device recalls on that of an OEM. This risk is exacerbated by the fact that connected devices interoperate with a variety of resources on the network. Without a way to cryptographically authenticate a device's identity or the integrity of its communications – e.g., through secure decentralized methods – the devices provide potential attackers with a foothold in the network to exfiltrate sensitive data or conduct reconnaissance for more sophisticated attacks to steal financial and insurance information.

Despite these risks, devices are often manufactured without the specialized hardware necessary to perform essential functions, such as establishing root of trust, performing secure boot, validating updates, or authenticating commands. Part of the reason is that existing standards require manufacturers to submit any material device changes for regulatory review to ensure their continuous functionality, which is a long and expensive process. There are also no enforceable regulations in place that would require strong cryptographic authentication on IoT devices. For instance, in 2014, the FDA issued a premarket cybersecurity guidance for medical devices suggesting that manufacturers avoid the use of hard-coded passwords and authenticate firmware and software updates, however it did not specify acceptable

[31] https://www.marketsandmarkets.com/Market-Reports/cloud-ids-ips-market-158051963.html

Funded by the Horizon 2020 Framework Programme of the European Union

authentication methods. The FDA also issued post-market guidance on security management for medical devices in 2016, as well as a separate guidance in 2018 on securing devices with off-the-shelf software. However, no updates have been made that supersede the premarket guidance in terms of security controls recommended in manufacturing. While guidance is a step in the right direction, it lacks the enforceability necessary to strengthen the devices' authentication. GDPR, on the other hand, could have a material impact on manufacturers as weak authentication exposes private information. There are methods available to factories that recognize the need for stronger authentication on medical devices. Gateways deployed on the factory network can act as a trust broker between devices too constrained to store and exchange their own credentials, including certificates. However, a security vulnerability still exists - all devices need to first establish strong trust relationships for further communication.

5.1.1 Market Expectations

This subsection features market expectations of individual industrial project partners.

TABLE 7: INDUSTRIAL PARTNERS' MARKET EXPECTATIONS

UBITECH
One of the most challenging elements of cybersecurity is the continuously changing nature of security risks. The basic approach is to focus on the key system components and protect them against the leading known threats. Today, this basic approach seems unsatisfactory because the threats are getting more advanced and changes more often than anyone can keep up. Today, organisations are using an updated cybersecurity guideline in their risk assessment framework that suggests unremitting monitoring and real time assessments. According to Renub Research study Security and Vulnerability Assessment market will be more than USD 14.7 Billion by 2024. Security & Vulnerability Management (SVM) market can be bifurcated into two parts Security Management Market and Vulnerability Assessment Market. UBITECH aspires to include the proposed project' exploitable outcomes to the OLISTIC risk assessment platform, while acquired knowledge in the field of risk assessment is expected to influence this market since there is no other known existing framework that considers TPM itself and quantum resistance TPM.
S5
In the domain of services on activity tracking, the impact of the demonstrator is expected to introduce the need for building more secure and privacy preserving services. Despite the rise of the importance of personal data and of different regulations and considerations that surround such data from the viewpoint of privacy and security, the current solutions are more focused on increasing the number of data sources to be ingested and on user experience, as those factors generate a larger pool of users quickly. It is evident that existing implementations neglect security and privacy issues. Data veracity is also not tackled properly, which is crucial for services that rely on the authenticity of data. Therefore, it is believed that the proper communication of the demonstrator will push existing vendors to consider more secure and trustworthy implementations in the next deliveries of their services in this domain.
UTRCI
With Collins being a leading industrial vendor in the aerospace industry, ASSURED aims to evaluate its concepts and technologies in the challenging aircraft safety and security sector, where the execution of large data-based analytics and communication operation has to be carried out over certain time and computational power constraints, overcoming at the same time size, weight and power (SWaP) design hurdles. In addition to security assurance and verification requirements that, the slower-than-desirable sensor processing and lack of bandwidth in downlinks especially for small devices will challenge ASSURED technology to be adapted in the aerospace market.

Funded by the Horizon 2020 Framework Programme of the European Union

ASSURED is ideally suited to penetrate this application segment, as it has picked-up aerospace security use case that i) will enable secure remote attestation of security-critical devices ii) produce on average an amount of up to 844 TB during a single flight-time, iii) project a surge of global fleet generated data up to 98 Exabytes in 2026. The smarter the real-time secure decision making, the safer will be the end command and aircraft operability and control (e.g., fuel saving), safeguarding the whole system from possible failures and attacks. New security methods based on tracing and control flow attestation will enable aerospace vendors to gain leverage through innovative authentication and security analytics techniques, with solutions for malware and anomaly detection over internal or external network communication respectively. However, the avionics market is relatively small compared to consumer and industrial electronics markets to afford domain-specific processors. Consequently, many avionics systems repurpose the security of certain devices originally designed for non-avionics applications, despite the limited visibility of the device internals and worst-case behaviours. The associated risk is mitigated by only enabling an analysable subset of the device features – the so-called Platform Usage Domain (PUD) or Critical Configuration Settings (CCS). This restrictive subset may reduce available performance to less than 50% of the device performance benchmark. It is envisioned that in ASSURED Collins will benchmark and exploit the security and performance of the mechanisms offered, that will be acceptable by the market without jeopardizing expected device performance while securing its vital operations.

In the aviation industry, energy-efficient processing systems promote the reduction of environmental impact, fuel consumption and operational costs and represent a major challenge for future air transport systems, as, for example, in ACARE Flightpath 2050[32] goals for 75% reduction of CO2 emissions per passenger per km and 90% reduction of NOX[33], leading an equipment market of More Electric Aircraft (MEA) of $22.5B at a CAGR of 4.62% past 2020. At the same time though, secure and safe autonomous aviation, starting from safe UAVs up to pilot workload reduction systems in the cockpit foresee a 19.8% CAGR to reach $83.6 billion by 2027[34], while the fully autonomous aircraft market is expected to grow from USD 3.6 billion in 2018 to 23.7 billion by 2030 at 17.06% CAGR[35]. ASSURED addresses these markets by promoting innovative AI-inspired, security protection of basic data elements (aircraft intra-network) via its low-size, low-weight and low-power hardware or software technology, targeting on the fly real-time decision making and security maintenance.

Safeguarding all AI-driven operations through ASSURED, will not only accelerate the realisation of AI-aviation in the market (e.g., looking forward to cyber-pilots) but also will promote unbreakable standard security mechanisms for highly critical products of the aircraft ecosystem.

SPH

According to “The future of the European space sector” (EIB, 2018 https://www.eib.org/attachments/thematic/future_of_european_space_sector_en.pdf), space market presents positive prospects for future development and with growing investments from private sources.

According to Allied Market Research report ("Satellite Services Market by Type, and End-User Industry: Global Opportunity Analysis and Industry Forecast, 2019-2026,") the satellite services market accounted for revenue of $126.5 billion in 2018 and is anticipated to generate $144.5 billion by 2026. The market is projected to experience growth at a compound annual growth rate (CAGR) of 2.2% from 2019 to 2026. Especially for CubeSats, according to Allied Market Research (https://www.alliedmarketresearch.com/cubesat-market-A09399), the Global CubeSat market size was valued at 210.1$ million in 2019 and is projected to reach 491.3 $ million by 2027.

Another important aspect to be considered is the financial impact of cyber-attacks towards satellite systems. For example, according to C.V. Camp & W. Peeters[36] (2021), a set of cyber-attacks on

[32] Air Transportation Action Group. The right flight path to reduce aviation emissions. UNFCCC Climate Talks, 2010

[33] Cision PS Newswire. More Electric Aircraft MarketWorth $22548.59 Million by 2020. https://goo.gl/PtSPnn

[34] Unmanned Aerial Vehicle Market Worth $83.6 Billion by 2027- Exclusive Report by Meticulous Research, 2020

[35] Autonomous Aircraft Market worth $23.7 billion by 2030, MarketsandMarkets™ INC Report 2019

[36] Charlotte Van Camp, Walter Peeters (2021), A World without Satellite Data as a Result of a Global Cyber-Attack, Space Policy, https://www.sciencedirect.com/science/article/pii/S0265964621000503

Funded by the Horizon 2020 Framework Programme of the European Union

satellites have already taken place in the recent years, either via attacking the Ground Station or via other simpler means (e.g., jamming, spoofing, dazzling – blinding a satellite with a laser).

These kinds of attacks can create huge impact. Apart from service disruption and other types of impact, these attacks have caused huge financial impact. According to Cybersecurity Ventures, global cybercrime costs are expected to grow by 15% per year over the next years, and reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015[37] (Cybercrime magazine 11/2020). ASSURED outcomes can be applied and contribute to mitigate the risk from these cyber-threats in various sectors (including the Space one) and contribute to avoid this significant financial impact.

For example, in Greece, a Greek National development program was announced in June 2021 for microsatellites from Greek Ministry of Digitalisation (https://mindigital.gr/archives/2611). As the aim is this project of microsatellites to support critical applications (search and rescue, border control, national security) there is a need for increasing the availability, security, and authentication of communication networks. Towards addressing these needs for increased security, SPH can incorporate parts of technological know-how and outcomes from ASSURED which contribute to verify the integrity and the secure operation of system or systems of systems, to proposed solutions to be used.

DAEM

For DAEM, the addressable relevant market is the wider network of public administration and more specifically of municipalities in Greece. Recent study (2020, https://www.eetaa.gr/ekdoseis/pdf/169.pdf) regarding the landscape of the resources and investments in Greek municipalities has addressed the main axes of resources distribution including investment in technologies - and especially in security enhancement. The study highlights the lack of resources in investment - following the local financial and social crisis - since the majority of them are dedicated to personnel and mainly social services. However, the ASSURED technologies are innovating and inspiring products that can potentially have a field of application for Athens and other cities following the trends of the European cities overcoming the technological and financial barriers.

Therefore, the demonstration of the public safety use case is expected to influence the public administration but also the networking industry, both through an increase of availability of trusted computing and sovereign identity solutions in various municipalities, as well as through the crystallisation of trusted computing and operational assurance expectations in public administration operations.

While DAEM is not involved in market share analysis in the public administration industry, several agencies have been publishing whitepapers on the value of trusted computing and secure data sharing/trading in monitoring equipment. However, there is no unified approach across vendors and neither complete adoption across any given vendor's product catalogue. Some vendors support an end-to-end trusted computing solution, others are still building support for it starting from the hardware platform to the operating system. Cloud-based monitoring services largely support trusted computing at hardware platform and operating system level in use cases ranging from traditional server applications to cloud and network function virtualisation. While some cloud service providers are effectively leveraging trusted computing to support scenarios like data encryption and device attestation, in the public administration market there is little evidence on the complete adoption of trusted computing (besides on the research level).

There are several barriers to the adoption of trusted computing, such as added complexity, increased cost, performance impact, incomplete standardisation of trusted computing protocols and lack of customer requirements. In some countries trusted computing is allowed only for certain purposes (e.g., authentication, but not encryption), in others only national algorithms are allowed.

[37] Sausalito, Calif., Special Report: Cyberwarfare In The C-Suite., CyberCrime Magazine (Accessed 02/2022) https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Funded by the Horizon 2020 Framework Programme of the European Union

5.2 EXPLOITATION STRATEGY AND COMMERCIALISATION ROADMAP

The main objective of an efficient exploitation strategy is to ensure that the results and benefits of the developed project outputs are attractive and well-known in the industry. As such, the objectives of the ASSURED exploitation plan are to:

- Establish and maintain mechanisms for effective exploitation,
- Inform stakeholders of the project development and encourage interactions/networking,
- Coordinate all levels and types of exploitation of the knowledge produced by the project,
- Ensure that information is shared with appropriate audiences in a timely manner and by the most effective means and medium.

Alongside the dissemination of the project results, exploitation of the achievements of ASSURED is of crucial importance and is recognized as one of the key elements for the success of ASSURED as underpinned by its significant industrial participation. Our common goal is to create knowledge, research new solutions and pave the way for successful commercial product innovation. Individual exploitation plans, which define a preliminary strategy for the development and exploitation of the project results, are listed in the table below.

While the main goal of ASSURED is the specification and design of a dynamic trust assessment framework for complex SoS, through the design of a new breed of attestation enablers based on the of trusted computing technologies (based on the use of a TPM), the results of the project are valid beyond that and therefore can be exploited to a broader range of products. That is, there are other similar hardware and software platforms that have a similar goal as the TPM. These include the upcoming IBM Power chips, hardware security modules (HSM), Trusted Execution Environments as defined by the GlobalPlatform, the ARM TrustZone, Intel's SGX, to name but a few. All of these will need 1) new algorithms and protocols that can leverage them for producing strong security claims on the level of trustworthiness of a device, and 2) none of them have a comprehensive security model and analysis. Thus, the ASSURED aims to exploit its results also in the context of all of these stakeholders.

5.2.1 Updated Individual Exploitation Plans

The following table provides an overview of the partners' updated exploitation plans. The updates of the initial plans were performed in before the end of the first project period in M18.

TABLE 8: PARTNERS' UPDATED INDIVIDUAL EXPLOITATION PLANS

UBITECH
Exploitation Goals: UBITECH aspires to reinforce its solutions portfolio through the offering of innovative and specialised applications and services not yet present in the market or through the expansion and optimisation of its current services and prototypes (in particular, OLISTIC that constitutes the company's holistic risk assessment platform), exploiting the acquired know how and the technological results of the proposed project in order to proceed to the implementation of integrated vertical solution in the field of TPM security for IoT and CPS deployment. This vertical solution will include both the technological results from the expansion of the OLISTIC output to MPSL-based format but also the consideration of both privacy aspects but also the migration to the CVSS 3.1 version. This way it will increase its competitiveness, targeting in both the public and private sectors and especially the industry.

Funded by the Horizon 2020 Framework Programme of the European Union

Furthermore, UBITECH has a large number of open source projects, products, and services offering where security is very important and, in recognition of this, has formed a specific business unit for security; i.e., engaging into Secure VoIP services, identity management and authentication services for public administration services, etc. Having a large security research group, UBITECH is well positioned to bring the project results to UBITECH's security business unit for exploitation, in particular, for the secure hardware integration into mobile identity management wallets (for public administration services in collaboration with the Greek Ministry of Digitalisation - more particularly for the online transactions offered through the Gov.gr website) which will include trusted computing functionalities and, thus, are a premier exploitation opportunity. Further exploitation opportunities come from the Ubitech's cloud services and offerings, which already today make use of hardware security modules (HSM) to store keys and to run cryptographic primitives.

Overall, from a business perspective, UBITECH aspires to include the proposed project' exploitable outcomes to the overall corporate offerings and promote, exploit and commercialize the developed framework and mechanisms to its existing clients list as well as to the Spanish-speaking countries of Central and Latin America wherein UBITECH operates through its subsidiary in Buenos Aires (Argentina) and its business partner in Guayaquil (Ecuador).This will also increase the visibility of UBITECH as an established leader in security modelling, hardware-security and trusted computing.

Topics/Domain: Digital Security, TPM Security, IoT/CPS Security, Risk Assessment, Self-Sovereign Identity, Verifiable Credentials

Approach and Activities: On the one hand, UBITECH intends to play an active role in this process as a system integrator, so its target is to identify opportunities for technology transfer into industry, e.g., by transferring technological know-how and/or integrating the software components developed in the proposed project in future collaborations with industrial partners, e.g., software development SMEs, IT solutions and hardware vendors and consultants, in Balkans and East Europe. On the other hand, UBITECH intends to proceed with the direct exploitation of the project's results in Spanish-speaking countries of Latin America, though targeted, focused marketing activities and business partnerships.

In particular, at individual level, UBITECH envisages the following exploitation activities:

- enhancing and/or implementing a variation of its OLISTIC solution addressing specifically privacy requirements and TPM security requirements with regard to IoT and CPS deployments;
- utilizing its OLISTIC platform as a basis for the realisation of the supply chains risk assessment;
- introducing these new offerings in the existing corporate marketing and sales activities;
- providing professional and consultancy services to customers interested in deploying similar infrastructures and services;
- further technological exploitation of the innovative aspects of the developed technologies in new collaborative research projects and initiatives;
- Accompany TCG and SSI standardisation process and push the new attestation schemes in the Trusted Computing Group as well as the new crypto algorithms for the secure interaction with the Blockchain infrastructure.

Finally, at consortium level, UBITECH envisages the following exploitation activities:

- commercialisation of the project's exploitable assets that can be individually (having the permission of or being licensed by the partner owing the IP) or in collaboration with the other consortium partners, sold to interested customers;
- examining the potentials of jointly exploiting and offering micro-services trust validation and security assurance as a service in collaboration with the rest of the consortium partners (i.e., customisation, maintenance, installation, service provision, training).

Contribution to other related research projects: The initial findings of ASSURED have triggered UBITECH to interact with the eSSIF Framework Lab for further optimizing the implementation of a "DAA Bridge" as a middleware for protecting a Holder's Wallet when managing the issuance of

Funded by the Horizon 2020 Framework Programme of the European Union

verifiable credentials. This has led to the commencement of a small open-call project titled “DOOR: Hardware Roots of Trust as an Enabler of Trustworthiness in Digital Transactions”.

Furthermore, the trust attestation models already produced in ASSURED enabled UBITECH to participate in a Consortium for a Horizon Europe proposal on Automotive Security. In particular, UBITECH has introduced concepts of “chip-to-cloud assurance” that can be provided through the integration of trusted platform modules for the secure communication of an autonomous vehicle with the backend MEC infrastructure.

DTU

Exploitation Goals: Establishing connections to industrial partners to initiate common research projects and obtain third party funding. Foster collaborations between academic research institutes through demonstration of scientific excellence. Exploit outcomes of the project in shaping content of teaching curriculum.

Topics/Domain: Hardware and software solutions for assurance of security and privacy in cyber-physical systems and IoT.

Approach and Activities: The developed technologies in relation to ASSURED will provide DTU insight into real-world use cases of industry partners that will inspire future research within the institute. Publications generated during the project will strengthen DTU’s role as a leading research institute within the EU and worldwide and help establish collaborations with industrial players on real-world problems. Incorporation of selected project outcomes in teaching curriculum at DTU in the form of master and PhD theses, course material and seminar offering.

Contribution to other related research projects

N/A

TUDA

Exploitation Goals: Establishing connections to industrial partners to initiate common research projects and obtain third party funding. Foster collaborations between academic research institutes through demonstration of scientific excellence. Exploit outcomes of the project in shaping content of teaching curriculum.

Topics/Domain: Hardware and software solutions for assurance of security and privacy in cyber-physical systems and IoT.

Approach and Activities: The developed technologies in relation to ASSURED will provide TUD insight into real-world use cases of industry partners that will inspire future research within the institute.

Publications generated during the project will strengthen TUDA’s role as a leading research institute within the EU and worldwide and help establish collaborations with industrial players on real-world problems. Incorporation of selected project outcomes in teaching curriculum at TUDA in the form of master and PhD theses, course material and seminar offering.

Contribution to other related research projects: The exchange with the other partners allowed developing new ideas for attestation and anomaly detection in general, not only related to control flow attestation. One concrete outcome is more insight into context based anomaly detection, which was successfully applied for starting another project in another domain.

Funded by the Horizon 2020 Framework Programme of the European Union

We plan to extend on these initial results, build on top of the gained insights for publications on to top-tier conferences and follow-up projects improving the attestation schemes that were developed in ASSURED.

TUDE

Exploitation Goals: Establishing connections to industrial partners to initiate common research projects and obtain third party funding. Foster collaborations between academic research institutes through demonstration of scientific excellence. Exploit outcomes of the project in shaping content of teaching curriculum. Inspired by the ASSURED technical framework, TUDE aims to collaborate with company partners, e.g., Computest, FoxIT, to initiate data protection research and funding proposals, targeting to the Netherlands domestic funding agency, e.g., NWO, and EU funding agency, like Horizon Europe, EIT Manufacturing.

Via ASSURED, TUDE plans to complete sufficient numbers of research with specific consortium partners, including TUDA, SURREY, UBITECH and DTU, in the cryptography and blockchain fields, in particular data sharing on blockchain. And meanwhile, TUDE aims to organize international security conferences and workshops to provide platforms to enable international researchers to gather and discuss advanced technologies used in the project.

The outputs of ASSURED will be used to demonstrate successful cryptographic system and framework knowledge and showcases in cybersecurity specialisation programme MSc courses, in particular, blockchain engineering, security and cryptography, and privacy enhancing technologies. ASSURED WP4 cryptographic and blockchain related tasks will be converted into inspiring R&D topics for the CS undergraduate students' thesis projects.

Topics/Domain: Data encryption, user authentication, blockchain, privacy enhancing technologies for guaranteeing data security and user privacy.

Approach and Activities: TUDE explores activities to obtain the previously mentioned goals. TUDE is going to lead an international security conference - EAI SecureComm 2022 - 18th EAI International Conference on Security and Privacy in Communication Networks - so as to attract network security researchers to exchange research ideas and promote ASSURED blockchain based data sharing solutions. ASSURED WP4 data sharing, trusted hardware and Hyperledger Fabric combination tasks have been undertaken as bachelor students' thesis projects to redo and reproduce the results so as to provide cybersecurity training purpose. TUDE and UBITECH have written a few collaboration research papers, aiming to submit them to international cybersecurity conferences. Based on ASSURED technical inspiration, TUDE is working with a Dutch company called Computest on the blockchain-based data protection topic, and they aim to submit a funding proposal to EIT Manufacturing agency (call for 2023).

Contribution to other related research projects: ASSURED definitely delivers technical inspiration and useful tools to other R&D projects. The security and privacy requirements of the data sharing mode on ASSURED blockchain offers a guidance and sample for another H2020 project IRIS in its security data sharing concept; the combination of Hyperledger Fabric, smart contract and attribute-based encryption framework in ASSURED, directly provides a vision on how the encrypted data interacts with smart contract, which motivates the technical solutions to the IRIS project.

ASSURED project also provides a good technical sample on how to merge attribute, policy and identity control over the Hyperledger Fabric membership service provider mechanism. This benefits the development of access control blockchain protocols in TUDE's blockchain lab.

SURREY

Exploitation Goals: SURREY will target the exploitation of ASSURED in the topics of data encryption, trusted computing, use of the TPM for converting embedded systems to secure hardware tokens as well as techniques for ABE merging with Blockchain technologies developed in the project

Funded by the Horizon 2020 Framework Programme of the European Union

and explore their further development and deployment in commercial scenarios. To this end, SURREY's exploitation strategy can be split into three main tracks: (1) Continue to develop the ASSURED security concepts through internally funded projects and in collaboration with other strategic industrial partnerships based on its network of EPSRC/BIS/GCHQ-recognised Academic Centres of Excellence in Cyber Security Research; (2) Documentation and publication of research outcomes to allow the promotion and advertisement of key ideas and results. This will focus on the dissemination of results at targeted scientific and industrial communities and the liaison with interested stakeholders that can benefit and support the adoption of the novel ASSURED tools and concepts; (3) Education and training activities offered to students in all academic levels (BSc, MSc and PhD), post-docs and researchers and the possibility for external parties to participate in research exchanges, to visit project members' research labs, etc. Such visits are extremely beneficial to foster strong scientific collaboration and benefit from any external knowledge relevant to the project.

Topics/Domain: Exploitation activities will focus on the scientific and industrial communities specialising in trusted computing, embedded systems security, system-level software engineering, and trusted execution environments and more generally on trustworthy systems and applications for emerging markets in IoT, technologies.

Approach and Activities: Surrey Centre for Cyber Security will search for strategic industrial partnerships through its network of EPSRC/BIS/GCHQ-recognised Academic Centres of Excellence in Cyber Security Research and engage with IT companies specialising on trusted computing, penetration testing and software security to increase the technology readiness level of the developed components and explore their further applicability for commercialisation. Through its 5G Innovation Centre the University will approach telecommunication companies to identify use cases for the developed secure hardware technologies in relation to future 5G technologies and mobile applications. 5GIC is also a member of the ETSI community that produces applicable standards for Information & Communication Technologies – this will allow the further advertisement of the novel FutureTPM results to targeted stakeholders. The project team will review progress (every 6 months) with the University's Technology Transfer & Impact team to look for new commercial opportunities. The University is a founding member of SETsquared Partnership (along with four other UK universities) with links to over 100 small and medium-size companies and will seek for exploitation of technical project outcomes through this network. The transferrable background knowledge and technologies on trusted computing engineering and run-time security analysis gained from the project will be exploited by the Surrey Centre for Cyber Security in other R&D projects on the design and development of secure systems, in particular within the planned research projects on secure use of off-the-shelf commercial and open-source products in IoT, automotive and satellite technologies.

Contribution to other related research projects: The participation in ASSURED has triggered SURREY to participate in the following projects:

- "**Verifiably Correct Swarm Attestation**" which is and EPSRC project (https://gow.epsrc.ukri.org/NGBOViewGrant.aspx?GrantRef=EP/V038915/1) focusing on the formal analysis of remote attestation protocols using formal logic and mathematically rigorous statements.

BIBA

Exploitation Goals: As a highly networked academic partner, BIBA will exploit the achieved results on multiple levels. BIBA not only provides courses and workshops addressed to students of the domain of engineering and informatics, but also to regional and national industry. Those exploitation activities will take place e.g., in a form of:

- consulting for technology companies willing to integrate modules or methods into their product portfolio. A potential example would be the Secure Zero-Touch configuration on-boarding and TPM Wallet integration to generic IIoT Gateways for various companies, or introduction of securely scaling such IIoT Gateways within manufacturing processes through ASSURED's swarm attestation mechanisms.

Funded by the Horizon 2020 Framework Programme of the European Union

- industrial funded projects characterized by providing support for highly practice oriented challenges where ASSURED framework becomes the baseline security criteria for developing potential problem solving platforms for SMEs and drive potential Proof-of-Concept prototypical solutions to more concrete industrial solutions

Topics/Domain: Smart Life-Cycle Management, Cyber Physical Systems, Internet of Things, Interoperability, Security and Safety, Robotics, Human Computer Interaction

Approach and Activities: The developed technologies from ASSURED will be potentially applied for future project proposals within the national and international research frameworks to enhance BIBA's position in introducing secured technologies into Industrial Research and Development projects. ASSURED will also serve as a new horizon for BIBA in the cybersecurity space within our research for potential new ideas and innovations. Publications from BIBA and collaborative efforts with the ASSURED partners will strengthen BIBA and the collaboration stemming from the ASSURED project, to improve scientific contributions from a practical level, which in turn may serve the purpose of potentially introducing SMEs to cybersecurity solutions to their industrial spaces and manufacturing processes

Contribution to other related research projects: Potential introduction maybe possible to the ACROBA project (https://acrobaproject.eu/) and RAINBOW Project (https://rainbow-h2020.eu) where dynamic trust establishment is envisioned for different types of fog computing systems.

NVIDIA

Exploitation Goals: The security vision of NVIDIA, in the short-term, is to improve the resiliency of it's adapters and switches. Without the necessary component in place to assure the integrity of the component of the platform, it's not possible to establish trust with a remote node that may reside in a hostile environment such as IoT. The goal is to produce architecture specification and proof-of-concepts that would guide design robust and resilient adapters. The aforementioned would allow deploying embedded devices in edge devices. In addition, the goal is to produce good quality research in hardware security for embedded devices and contribute back to the academic community and portray leadership in hardware security.

Thus, in this context, NVIDIA intends to use the expertise and results gained from this project to enhance the trusted computing competence needed for NVIDIA's next generation products, ranging from traditional network devices to cloud-based telecommunication solutions such as Network Function Virtualisation (NFV).

Topics/Domain: The targets of exploitation are in the following areas and will be aligned with NVIDIA's business planning and customer requirements: secure telecommunication and enterprise network devices, trusted management of network infrastructures and trusted systems and applications.

Approach and Activities: NVIDIA envisions to consolidate the results of this project within its Cyber Security and Privacy Lab (CSPL) group and demonstrate the technologies to: NVIDIA product lines, for evaluation and integration; NVIDIA customers, to show leadership in trusted ITC solutions; industrial workshops such as the ones organised by TCG and DMTF.

The developed technologies in relation to ASSURED will provide NVIDIA insight into academic research being done in the field. Publications generated during the project will strengthen NVIDIA security research role as a leading organisation in the field of security within the EU and worldwide.

Contribution to other related research projects: The ASSURED project contributed to starting a new project in tracing in embedded devices, and this will allow NVIDIA to explore further collaboration with other partners in disseminate the knowledge and explore the opportunity to the fullest of this research in different settings and environments.

Funded by the Horizon 2020 Framework Programme of the European Union

SUITE5
Exploitation Goals: Suite5 expects to acquire further technological and innovation know-how related to advanced distributed analytics and real-time processing over secure infrastructures and large ICT systems, in order to complement its existing tools and services portfolio of data-driven intelligence, as well as gain competitive advantage when bidding for the design and delivery of related innovative, future cloud services related to network management. In this context, Suite5 aims to exploit the contributions it shall make to the development of the platform, to further improve the data sharing capabilities of the **S5 Enterprise Data Management and Analytics Platform** for evolving ICT systems that have strong security needs, allowing the interconnection with the platform of various trusted stakeholders, operating a similar concept as the blockchain architectural concept introduced in ASSURED. Last but not least, Suite5 will gain insights into emerging innovation areas and business models related to extreme scale analytics technologies, as well as envision future innovation and research projects based on the knowledge acquired during the implementation. Suite5 has successfully completed numerous digitisation projects in various industries by adopting a process-focused approach to solving supply chain challenges and leveraging our own industry expertise to industry associations and academia. We have proven capabilities for realizing solutions using the latest technologies on both hardware and software level. Thus, ASSURED will also allow Suite5 to verify new use-cases in the market.
Topics/Domain: Exploitation will be targeted towards: • Enterprises and Public Sector Organisations that need more flexible and trusted systems for data sharing and trading. • SMEs and NGOs providing consultancy services that would greatly benefit from a distributed data sharing architecture without compromising security. • Scientific Communities, Professional bodies, and Institutions working on big data technologies that need auditable and trusted systems for sharing data based on strong security guarantees.
Approach and Activities: The main approach for exploitation will focus on personal contacts with existing or potential clients through the participation in fairs, forums and workshops through online communication channels. Indicative activities that will be performed include: • Creation of dedicated videos and proof of concept implementations created during the project duration, to engage industrial players and SMEs. • Participation in online events using presentation slots in order to demonstrate the results and attract potential customers. • Introduction of new features to existing products and contacting the existing users base in order to inform them about the advancements. • Targeted marketing to organisations based in Cyprus, Greece, UK and abroad, dealing with cloud application development and deployment in their everyday operations. • Initiation of collaboration and business partnerships with research institutes and industry associations with direct interest on advanced distributed analytics and machine learning.
Contribution to other related research projects: The knowhow of the project relevant to the ASSURED blockchain architecture, has been introduced also in the DataVaults H2020 project, where a blockchain architecture is developed for trading data assets.
UTRCI
Exploitation Goals: Develop unique and certifiable aerospace products that will protect the aircraft from next-generation cyber-security attacks within the product, the network or the supply chain. Transition and evaluate ASSURED technology seamlessly to new products or services that in the future will be interconnected and, thus, securely integrated in their design and operation.

Funded by the Horizon 2020 Framework Programme of the European Union

Topics/Domain: Aerospace systems (hardware or software) that contribute to internal or external communications

Approach and Activities: As a series of activities and modules in ASSURED are related to the development and verification of several AI-driven automation procedures for security-critical operations, Collins aims to align all the ASSURED activities to the early directives of SAE G34 towards certification of security attestation mechanisms that will enable its usage in safety and security-critical systems that would need a high level of security assurance. It is of vital importance in order to transition the ASSURED technology to existing aerospace product lines that certain verification and validation processes are enabled towards the certification of the new solutions embedded into the device. Thus, methods, tools and processes as an outcome of ASSURED will be evaluated for their maturity level, executing a series of benchmark operations that will validate their efficacy and completeness.

Due to the complexity and nature of security requirements, certification streamlining will be defined as abstracting the certification process to allow alternative approaches that promote reusable and performance-based evaluation processes of the product while still retaining a guaranteed level of safety. The FAA streamlining workshops agreed on three “Overarching Properties” (OPs) a product should have to comply with regulations: Intent, Correctness, and Acceptability. As part of the ASSURED project, Collins will co-evaluate security requirements in the same manner, as a new OP, towards technology maturation and its final transition to the business unit. The goals of OPs are twofold; the first is to provide a development framework based on the fundamental properties that need to be demonstrated for certification, the second is to provide a certification framework that uses these fundamental properties for systems, hardware, and software certification. The European avionics industry contributed to FAA initiative on OPs with a research project named RESSAC (Re-Engineering and Streamlining the Standards for Avionics Certification). RESSAC resulted with a recommendation and accompanying examples for developing assurance case with structured arguments for documenting the rationale for the possession of OPs. ASSURED will explore new means of compliance at high level, particularly with the Security and correctness of the solutions but also with Acceptability and Intend for AI-based systems to enable, or at least contribute to their certification. All standardisation activities through Collins engineering departments in US (active participation in DO-326 for Aerospace systems Air-trustworthiness), Collins aims to communicate and validate all methods and technology developed in ASSURED to its peers. The main goal will be to extract certification credit for all the ASSURED technologies, impacting existing aerospace products (e.g., SSR7000/FOMAX) or new devices that will be interconnected in internal or external networks, raising the need for security assurance.

Contribution to other related research projects: Collins will leverage the results of ASSURED to accelerate the delivery of existing and new secure avionics products to the marketplace. Current solutions to increase dependability in avionics products are mostly enforced by over-dimensioned redundancies and functionality overhead to include many different operational modes. Being able to address certification of security functions using recognised techniques will allow our future systems to scale and evolve. These advances will enable more competitiveness when transferred to our Collins engineering departments, while additional transition opportunities may arise disseminating ASSURED results to Raytheon businesses around the world.

SPH

Exploitation Goals: SPH sees a dual exploitation potential on the project results: i) in a “horizontal” direction; SPH is looking forward to exploiting the entire ASSURED framework (acting as a prime contractor and liaising with the partners-technology providers) as a turn-key solution. SPH plans to offer the ASSURED framework either on-premises or in the cloud/as-a-Service, depending on the customers’ needs, perfectly complementing existing commercial security appliances and solutions offered by the company. ii) in a “vertical” direction, SPH aims to further penetrate the satellite services market by adapting its surveillance service to run securely onboard CubeSat constellations.

More specifically some components of ASSURED can be considered to be included in the envisioned technical solutions to cover emerging needs for CubeSats in the Greek Market (e.g., the National

Funded by the Horizon 2020 Framework Programme of the European Union

CubeSats program). ASSURED functionalities can contribute to enhance the security of the designed solutions and make them more resilient against a variety of attacks. In that way their use will be enabled to be expanded to critical sectors related with national security (e.g., border surveillance). Apart from direct related use of ASSURED outcomes to CubeSats communications, other members of SPH Group can evaluate them and take advantage of the provided services. More details are mentioned below.

Topics/Domain: Cybersecurity market, Satellite services market, CubeSats community

Approach and Activities: Leverage its connections in the Hellenic Space Technologies and Applications cluster (si-Cluster), of which SPH is a founding member, to liaise with the national and international cubesats community and promote the ASSURED solutions for securing onboard functions. Provide consulting services and support the integration of ASSURED to Satellites communications and CubeSats sector. Evaluate options for further exploitation of ASSURED outcomes through the members of SPH Group including companies active in IoT, Smart Cities and Agriculture sectors.

- SenseOne (https://www.senseone.io/) IoT, Smart meters
- SingularLogic (https://portal.singularlogic.eu/en) Smart Cities
- AgroApps (https://agroapps.gr/en/home/) Smart Agriculture and Remote Sensing

Contribution to other related research projects: N/A

DAEM

Exploitation Goals: Exploit the outcomes and results of the project at the relevant market sector that includes smart city systems locally. Include the services into DAEM's products portfolio for security enhancement of the services provisioned to citizens of Athens and potential diffusion to other cities, public authorities etc. Develop a best research practice for the City of Athens that could be a prototype for relevant products and initiatives focusing on: policymaking for city sustainability and city solutions provision. Finally, establish connections with research, industry and other partners to exploit the know-how gained from ASSURED and technological advancements for future research and funding. Furthermore, DAEM - through ASSURED - can integrate the first IoT security and certification platform which eases the frictions associated with certification of public monitoring systems and privacy. ASSURED's results will be used to extend and automate some features linked to security evaluations and thus improve the efficiency of the pre and post certification processes.

Topics/Domain: business market, citizens' service provision, safety and resilience policymaking, inclusion of new technologies, software and hardware developed for and by ASSURED for privacy and security of systems, IoT know-how.

Approach and Activities: DAEM, as a local government organisation, maintains strong interest in the project results. The results of the project will be exploited to leverage the company business opportunities to improve market positioning and to offer creditable services. DAEM will lead to a new set of services developed for ASSURED and technology outputs provided by ASSURED that can play the role of a credible best practice and evaluated by the Athens testbed. Innovative services may be conceived, through the proposed technology on emergency administration and the network with other authorities developed for the demonstration. This is the long term added value for DAEM as a service developer that foresees the potential of extending products and services portfolio. Respectively, the latter is expected to be an added value also for the City of Athens, as the overall responsible for smart services provision and public safety. Consequently, DAEM aims to exploit the gained knowledge, training, products as a whole, as well as sub-sets of features and tools to be exploited by the consortium.

Funded by the Horizon 2020 Framework Programme of the European Union

Contribution to other related research projects: DAEM following the involvement in ASSURED and in a past completed relevant project VisiOn, has progressed to participate also in another proposal targeting first response in city crisis management and potential attacks to public safety. However, the evaluation is still ongoing for this project, hence further information cannot be provided.

Funded by the Horizon 2020 Framework Programme of the European Union

5.3 ASSURED EXPLOITATION STRATEGIES (ON PARTNER LEVEL)

5.3.1 Exploitation Strategy by UBITECH

Key exploitable results	Exploitation Strategy	Target Sector	List potential competitors	Possible Market Barriers	Timetable of the exploitation	Impact	IPR Measures
Fully specified version of updated attestation schemes, through the close collaboration with the Trusted Computing Group and ISO bodies	N/A	All TPM relevant fields of applications with TPM: PCs &laptops, Industrial TPM, Automotive TPM.	N/A	N/A	N/A	Enable transition to dynamic trust modelling based on hw-based roots of trust	N/A
TPM-based Wallet for enhancing the level of assurance offered while managing Verifiable Credentials	Offer hw-based protection (through the DAA-protected Wallet) to companies requiring identity management for online transactions	All industries including online transactions, e.g., Banking, Public Administration, etc.	GATACA, GIMLY, SICPA, QUADIBLE	Not compliant interfaces in the mobile devices used, as Holders, for supporting the required TPM interfaces	Finalisation of the design of the TPM-based Wallet by the end of the project; commercialisation 1-2 years after the end of the project to be integrated within public administration services	General: Integrating TCG concepts into the SSI domain - "*bring the two worlds together*"; On your portfolio: DAA-Bridge implementation	IPR to be decided

Funded by the Horizon 2020 Framework Programme of the European Union

Concrete TPM-based solutions addressing commonly identified industry specific issues through the envisioned use cases	Obtain system know-how on uses of TPMs in industrial applications	All industries affects by zero-day exploits where different Levels of Assurance is required; e.g., Smart manufacturing, Banking and e-Commerce, eHelath	Thales, NXP, Intel, Nuvoton, etc.	Integration of TPMs, as the underlying hw-based root of trust, might be too costly to be adopted by OEMs; Attestation algorithms might be too expensive to run in heterogeneous resource-constrained devices	Development of demonstrator' s activities before the end of the project	Adaptation to further applications outside the identified set of use cases.	N/A
Framework for enhancing device security posture through holistic threat assessment against aspects of supply chain deployments, considering the entire TCG Software Stack	Existing OLISTIC risk assessment tool will be enhanced	All devices incorporating existing security protocols and cryptographic techniques vulnerable to various network- and host-based attacks.	exSILentia® Cyber, CIRMA, RBA's Risk Assessment Platform, etc.	Added complexity, increased cost, performance impact, incomplete standardisation of trusted computing protocols, lack of customer requirements.	Further prototyping in the four use cases till the end of the project	General: Generic exploitation including novel approaches to threat assessment entailing On your portfolio: likelihood and impact of sophisticated attacks.	Research publication (journal of conference) with the research results.

5.3.2 Exploitation Strategy by BIBA

Key exploitable results	Exploitation Strategy	Target Sector	List potential competitors	Possible Market Barriers	Timetable of the exploitation	Impact	IPR Measures
ASSURED Assurance and Safety Framework	Present ASSURED Project based Results during In-Person Events within BIBA's Demonstrator Hall	Industrial Research Communities, Potentials SMEs seeking advice on Digitisation	N/A	N/A	N/A	Illustrate Cybersecurity Solutions for Industrial Systems at application and device level	N/A

Funded by the Horizon 2020 Framework Programme of the European Union

ASSURED Runtime Monitoring/Tracing System	Integration with new software components to introduce security enhancements in Personnel Localisation Motion Capturing (PLMC) and Robot Motion Tracking (RMT) services	Industrial Research Communities	N/A	Potential Hardware Incompatibility Issues for Industrial Grade Machineries	N/A	Practical Familiarity regarding Software based Cybersecurity projects	N/A
ASSURED TPM based Wallet	Potential usage of TPMs within the BIBA Demonstrators for future Edge Computing Projects and Research	Presenting TPM based Edge Devices for Industrial Use Cases to potential SMEs, Industrial Research Communities	N/A	N/A	N/A	N/A	N/A
ASSURED Device Zero Touch Onboarding & Registration	Potential usage of Zero-Touch On-Boarding with TPM Wallets for the secure registration of additional robots in a smart manufacturing environments	Potential usage in Research Projects, Research Communities, Prototype projects	N/A	N/A	N/A	Prototyping Secure Edge Device Applications within Industrial Environments	N/A
ASSURED Swarm Attestation Algorithm	Potential usage of Secure Edge Devices within an Industrial Environment as a scalable prototype through Swarm Attestation	Research Communities, Prototype Projects	N/A	N/A	N/A	Prototyping Secure Edge Device Applications within Industrial Environments	N/A

Funded by the Horizon 2020 Framework Programme of the European Union

5.3.3 Exploitation Strategy by INTRASOFT

Key exploitable results	Exploitation Strategy	Target Sector	List potential competitors	Possible Market Barriers	Timetable of the exploitation	Impact	IPR Measures
Attack Validation Component, Policy Recommendation Engine	Since ASSURED most of results are Open Source INTRASOFT will integrate results linked to the ASSURED project and the know-how acquired during this project to already existing products or added value cyber security services like consulting and training to its established clientele.	Vulnerability Assessment Market	FireEye (US), Optiv Security (US), Qualys (US), Trustwave (US), Veracode (US), Check Point (Israel), Absolute Software (Canada), Rapid7 (US), CynergisTek (US), and Positive Technologies (UK)	Budget constraints Complexity of devices security	2 years after the project's end	Additional services, enhancement of clientele	Open Source

5.3.4 Exploitation Strategy by S5

Key exploitable results	Exploitation Strategy	Target Sector	List potential competitors	Possible Market Barriers	Timetable of the exploitation	Impact	IPR Measures
Blockchain Permission Management and Transaction Auditing & Assurance Services	Considering implementation of crypto micropayments for unlocking & acquiring data sharing capabilities of the S5 Enterprise Data Management and Analytics Platform for evolving ICT systems that have strong security needs	Enterprises Public Sector Organisations SMEs	N/A	N/A	N/A	N/A	N/A

Funded by the Horizon 2020 Framework Programme of the European Union

Smart Contract Definitions for Policy Enforcement and Security Data Management	Considering implementation of crypto micropayments for unlocking & acquiring data sharing capabilities of the S5 Enterprise Data Management and Analytics Platform for evolving ICT systems that have strong security needs	Enterprises Public Sector Organisations SMEs	N/A	N/A	N/A	N/A	N/A
TPM Wallet for Identity Management of customers registered to use the S5 Personal Activity Monitoring and Tracking Service	S5 also provides the ATracker Application for personal activity tracking and monitoring service. The integration of the ASSURED TPM Wallet for better Identity management (through the use of Verifiable Credentials) will be exploited internally, to renovate the existing service by integrating such security enhancement for online transactions	Healthcare and Insurance markets working with personal activity data	N/A	Constraints regarding flow of personal data, upfront investment in infrastructure too high for small clients	Prototype and testing till the end of the project (2023) and integration in the current service offering in 2025	On your portfolio: Improvement of the trust/security levels of the current S5 Personal Activity Tracker Infrastructure	IPRs of the current service will remain as is

5.3.5 Exploitation Strategy by UTRCI

Key exploitable results	Exploitation Strategy	Target Sector	List potential competitors	Possible Market Barriers	Timetable of the exploitation	Impact	IPR Measures
Security attestation	Embed specific mechanism into existing aerospace supply chain (e.g., SSR7000/FOMAX) and evaluate remote attestation completeness and performance	Transport sector with a focus on aerospace	N/A	Certification of solution could be expensive (time-consuming) based on avionics standards. Absence of expertise with respect to security	Prototype demonstration in 2022 and 2023; evaluation of Method Maturity Level (MML) in 2023 and transition of technology to	Potential usage of security attestation mechanism as part of Collins Interiors business for seamless passenger authentication (e.g., Collins Safepass solution)	Provided unique services are realized in the aerospace domain, Collins aims to file invention disclosures protecting certifiable

Funded by the Horizon 2020 Framework Programme of the European Union

				attestation execution	product line in 2024		security attestation mechanisms against DO software or hardware standards.
Smart contracts and blockchain technology	Incorporate blockchain technology and smart contract creation in existing aerospace supply chains	Transport sector with a focus on aerospace	Honeywell synergies with Aero blockchain technology	Legal barriers from involved parties (e.g., Collins, Airframer, Airline)	Prototype demonstration in 2023 and legal establishment-bylaws of technology for each involved partner	Potential technology usage in additional supply chains for safety-critical systems for new Collins business, Pratt and Whitney and Raythoen global divisions.	N/A

5.3.6 Exploitation Strategy by SPH

Key exploitable results	Exploitation Strategy	Target Sector	List potential competitors	Possible Market Barriers	Timetable of the exploitation	Impact	IPR Measures
Smart contract and Blockchain components.	Consider embedding Block chain-based functionalities to technical solutions provided to telecommunication sector including satellites.	Satellite communications and CubeSats	N/A	Increased complexity, lack of expertise.	Potentially after the end of the project.	Strengthen security with the utilisation and development of security enhanced functionalities. Increase resilience against attacks and safety (for critical mission applications).	N/A

Funded by the Horizon 2020 Framework Programme of the European Union

Integration of ASSURED security and attestation components to Smart Sattelites Sector.	Consider providing consulting services and support services on integration of ASSURED	Enterprises and SMEs active in sattelites sector.	N/A	Increased complexity. Lack of expertise to integrate with commercial vendor solutions.	Prototype Demonstration of integrated ASSURED functionalities by the end of the project (2023).	Enter new market s, develop new business activity	N/A
Framework for enhancing satellite device security posture through holistic threat assessment against aspects of new-generation communication deployments (e.g., Galileo)	N/A	All networked components used in the new type of satellite ecosystems	N/A	N/A	N/A	General: Generic exploitation including novel approaches to threat assessment including likelihood and impact of sophisticated attacks	N/A

5.3.7 Exploitation Strategy by DAEM

Key exploitable results	Exploitation Strategy	Target Sector	List potential competitors	Possible Market Barriers	Timetable of the exploitation	Impact	IPR Measures
Overall ASSURED framework and attestation mechanisms	Adoption from the City of Athens in case of a positive evaluation from the testbed	Greek Public sector, public administration	N/A	Lack of financial resources for the maintenance and costs for deployment Lack of knowledge on the field	Potentially after the end of the project	General impact on public safety and security cyber- city systems	N/A

Funded by the Horizon 2020 Framework Programme of the European Union

Sub-set of ASSURED features (Blockchain, policy recommendation, risk assessment on cyber-systems, attestation for edge devices, verification of users)	To other ICT companies providing city services	Private sector	N/A	Lack of knowledge on the field due to the innovative approach of ASSURED technologies for Greek cities and its providers	Potentially after the end of the project	General: Innovation in the security of provided city services	N/A
Research results and know-how for the deployment of cyber-security systems related to public safety	DAEM could exploit the result on consulting services for city systems	Greek Public sector, public administration	N/A	Lack of technological capacity in the Greek cities sector	Potentially after the end of the project	On your portfolio: DAEM as the main services provider for the largest municipality in Greece, Athens, has an impact on smaller cities as a best practise and provider of innovative tools/technologies	N/A
Adoption of ASSURED Risk Assessment for the identification/characterisation of the threat landscape applying to future end-to-end public safety and service systems and of the technologies and architecture to mitigate them	Adoption of DAEM to be integrated in their supply chain systems so as to have an up-to-date, dynamic risk assessment process	Public Safety and the deployed monitoring systems. Considering also the new concept of crowd-sensing where (video/image) input comes from user smart-phones, thus, introducing new risks	exSILentia® Cyber, CIRMA, RBA's Risk Assessment Platform, etc.	Added complexity, increased cost, performance impact, incomplete standardisation of trusted computing protocols, lack of customer requirements	Further prototyping during the duration of the project	General: Generic exploitation including the novel security and privacy risk assessment methodologies; On your portfolio: Additional dashboard for showcasing identified risks to users/customers	N/A

Funded by the Horizon 2020 Framework Programme of the European Union

TPM Wallet for Identity Management and Attribute-based Access Control of Different Roles accessing public safety data	Provision of the Wallet as an application for users wanting to access public administration services	Public Administration	AADE in Greece	Complexity, lack of alignment with the EU SSI ecosystem and especially eIDAS for the issuance of Verifiable Credentials, lack of data model alignment to W3C credentials	Long-term; after the end of the project depending on the adoption of SSI-based solution from the GR public administration authorities	General: Exploitation of the SSI capabilities for the better identity management of users and stakeholders accessing public administration data and services	Open sourcing most of the research results

Funded by the Horizon 2020 Framework Programme of the European Union

6 INTERNAL AND EXTERNAL TRAINING

The academic partners of the ASSURED project organized different training activities:

TABLE 9: INTERNAL AND EXTERNAL TRAINING BY ACADEMIC PARTNER

UBITECH
The expertise that UBITECH has created with its work in ASSURED, fuelled a number of guest lectures, in the context of trusted computing, that Dr. Thanassis Giannetsos presented in the context of the Master's Degree "*Digital Systems Security*" of University of Piraeus (UPRC) with which UBITECH has an established liaison and research collaboration. Furthermore, a number of Bachelor theses were offered, through this collaboration channel, that were undertaken by UPRC students based on the research done in ASSURED - especially related to the new type of attestation schemes provided. More specifically, the following two theses were supervised in collaboration with Prof. Xenakis of UPRC: • Evaluation and Implementation of Direct Anonymous Attestation (DAA) in the context of CCAM; • A Security Evaluation of TrustZone-based Trusted Execution Environments (TEEs). Finally, UBITECH and DTU through their continuous collaboration (Dr. Giannetsos holds also the title of Adjunct Associate Professor at DTU) provided a number of MSc theses in some of the core technologies of ASSURED including trusted computing and identity management: • Analysing TPM Communication for Fun and Profit: Is there anything to Gain; • Secure Boot: Bootstrapping Trust by Verifying TPM Validity through the UEFI Drivers.
DTU
Internal DTU training activities and events: • Supervision of several MSc students on ASSURED related topics: ▪ (Spring 2022) Remote Attestation Mechanisms for WebAssembly Enclaves in Widely-Distributed Systems, MSc. Thesis (ongoing), DTU Compute in collaboration with Aalto University, Finland; ▪ (Spring 2022) Fingerprinting schemes against Post Quantum Cryptography IPsec/IKEv2 encryption appliance, MSc. Thesis (ongoing), DTU compute in collaboration with Company SSH Communication Security, Finland and Aalto University, Finland; ▪ (Spring 2022) Distributed Remote Attestation Protocol through Smart Contracts Technology, MSc. Thesis (ongoing), DTU Compute, Denmark; ▪ (Spring 2022) Building a Common Framework for Efficient Remote Attestation Deployment in IoT Networks, MSc. Thesis (ongoing), DTU Compute, Denmark; ▪ (Spring 2022) Remote Attestation in Intermittent IoT Devices, MSc. Thesis (ongoing), DTU Compute, Denmark; ▪ (Fall 2021) Attestation of Distributed Services without Centralized Verification, MSc. Thesis (ongoing), DTU Compute, Denmark; ▪ (Spring 2021) Control-Flow Attestation of Asynchronous Distributed IoT Services, MSc. Thesis, DTU Compute, Denmark; ▪ (Spring 2021) Blockchain in Self Attestation for Making Trust Decisions in IoT Networks, MSc. Thesis, DTU Compute, Denmark; ▪ (Spring 2021) Scalable and Efficient Remote Attestation Protocol for Large Distributed Event-Based Systems, MSc. Thesis, DTU Compute, Denmark;

Funded by the Horizon 2020 Framework Programme of the European Union

- (Spring 2021) An IoT Security Framework Based on Modern IoT Security Standards, MSc. Thesis, DTU Compute (in collaboration with Develco Products), Denmark;
- (Fall 2020) Memory Offloading for Remote Attestation on IoT Devices, MSc. Thesis, DTU Compute, Denmark

- Supervision of several PhD students on attestation related topics:
  - "Trusted Computing Technologies for Operational Assurance", (PhD Student: Benjamin Larsen, DTU Compute);
  - "Security, Privacy and Trust Issues in Fog Computing", (PhD Student: Heini Bergsson Debes, DTU Compute).
- Internal departmental seminar for presenting the emerging trends in trusted computing technologies and also presenting the research avenues investigated within the ASSURED project (60 participants, other faculty members and MSc students).
- Supervision of 2 special project course on topics related to the use of trusted computing towards enhanced operational assurance in applications domains including V2X, crowdsensing and blockchains
- Teaching the TPM technology in the MSc information Security Programme;
- 2 invited talks on operational assurance through the use of TPMs and memory offloading approaches;
- 1 invited talk on Self-Sovereign Identity (SSI) and how to better increase the trustworthiness of all the SSI entities;
- Ethical Hacking Challenge: Christian Jensen was in the organisation committee of a challenge event on ethical hacking that was open to DTU students, security practitioners, etc. This event was also supported by the Municipality of Copenhagen and revolving around a series of small challenges that were handed out to the participants who tried to identify vulnerabilities in a number of real-world industrial systems.

TUDA

Due to the individual deliverables the understanding of attestation schemes and the interdependencies between different strategies was improved in our and/or Postdocs working on ASSURED group. To improve the general understanding of this, TUDA discussed the new schemes frequently in the weekly research seminar of our group.

Further, TUDA is currently considering including the gained knowledge into the curricula classes for MSc. students to give a basic understanding of the different attestation schemes and their targeted scenarios.

TUDE

TUDE has delivered ASSURED related cryptographic tools and knowledge to undergraduate, MSc courses and thesis projects. Inspired by the outputs of the ASSURED project, TUDE has been working with local companies on data protection research topics, and aims for the next level of funding proposal. TUDE has also worked with several consortium partners in research publications.

- International Network Security Conference - EAI SecureComm 2022 - 18th EAI International Conference on Security and Privacy in Communication Networks -, there will be around 80 - 100 attendances who are with the network security backgrounds.
- EIT Manufacturing Ideation session: AI and digital twins, with around 120 attendances who are with cybersecurity and manufacturing backgrounds.
- MSc thesis supervision related to ASSURED project: (i) searchable encryption: forward and backward security; (ii) exploring searchable encryption potential breaches; (iii) apply trusted hardware into Hyperledger Fabric.

Funded by the Horizon 2020 Framework Programme of the European Union

- Bachelor thesis supervision: (i) secure tools implemented into Hyperledger Fabric; (ii) leverage Intel SGX to protect Hyperledger Fabric smart contract
- Bachelor education - algebra and cryptography course, with around 209 students, who are with computer science backgrounds;
- Cybersecurity MSc programme course - security and cryptography, privacy enhancing technologies, and blockchain engineering, with around 80 students per course.

SURREY

Internal SURREY training and activities include:

- Supervision of one PostDoc on Data Encryption, Trusted Computing as well as Attribute-based Access Control merging the use of a TPM with Blockchain techniques;
- Supervision of 1 PhD student on DAA schemes and their transition to the post-quantum era; Lattice-based Direct Anonymous Attestation;
- Supervision of several MSc students on secure data management topics (secure on-chain interactions);
- Invited talks in workshops for presenting ASSURED crypto primitives and what how they can leverage quantum-safe crypto algorithms
  - Oxford Post-Quantum Cryptography Workshop, March 2021.
- 2 invited speeches on TPM technology and future TPM consideration;
- 3 lectures on TPM and hardware security inside MSc and BSc courses (200 + 55 students);
- 2 lectures on Operating Systems, Virtualisation and Cloud security issues and countermeasures for MSc and BSc courses (200 students + 80 students);
- Surrey Open Day. Liqun Chen and Nada El Kaseem led the activities of the cyber Security Centre showroom at the Surrey Open Day. The showroom included a dedicated ASSURED presentation slot and dissemination desk, and there were plenty of opportunities to network and engage in discussions with visitors to disseminate the results of ASSURED. The event was very successful and was attended by around 200 participants.

SUITE5

Internal workshop on Blockchain & smart contracts with the participation of 2 software engineers and 1 data scientist.

UTRCI

Organize and execute internal engineering workshops within the product cyber and verification groups in Collins to disseminate and raise awareness of ASSURED technology. It is envisioned that more than 50 engineers from EU and US will be able to participate with a diverse level of experience and education (engineers, senior engineers, principal scientists, vice presidents).

Funded by the Horizon 2020 Framework Programme of the European Union

7 STANDARDISATION

A key strategic objective of ASSURED is to contribute to standardisation efforts at EU level targeting the main standardisation communities and working groups related to the core technologies investigated in ASSURED. As was described in D7.1, the core areas targeted in ASSURED revolve around **remote attestation (and underlying trusted computing technologies), lightweight cryptography, dynamic real-time risk assessment, enhanced and accountable knowledge sharing of operational threat intelligence data flows (through the use of Blockchains), and decentralized identity management through the use of verifiable credentials**. Towards this direction, ASSURED liaised with the technical committees of the relevant standardisation bodies, notable TCG, ISO, IEC and SSI.

In what follows, we first list the highlights of the main standardisation activities recorded by the project by providing details on those efforts that currently have led to some tangible outcomes (Section 7.1). Then, we proceed with summarizing additional standardisation activities performed by individual partners that are also ongoing and we are expecting to materialize in the near future (Section 7.2).

Contributions to standardisation is a continuous process, in the context of ASSURED, and is expected to intensify as we are moving to the second half of the project activities. Having finalized the design of all ASSURED novel schemes, algorithms and protocols (as part of the technical work-packages WP2, WP3, and WP4), the project is now focusing on the implementation and integration activities towards the release of the first integrated version of the ASSURED framework. This will also enable the evaluation of all ASSURED artefacts which, in turn, will allow the further dissemination in the respective working groups that may lead to the compilation of additional technical specification, white papers and/or position papers.

7.1 CONTRIBUTION TO STANDARDS

ASSURED efforts, during the first reporting period, focused on the collaboration with technical committees so as to create standardisation proposals that push the state-of-the-art in the areas of Operational Assurance (based on the employment of a new breed of attestation enablers), cryptography, Blockchain and Secure Distributed Ledger Technologies, Decentralized Identity Management (as part of the European Self-Sovereign Identity Lab) and the TPM itself, and involved the technical committees of the relevant standardisation bodies, notably ISO, IEC, TCG, DIF, and SSI. A particular focus was given on standardisation initiatives where partners are already actively engaged; we would anticipate the work leading to contributions on **updated functional specifications and working version of the Trusted Software Stack (TSS)**, used for the interaction with the host TPM; on **privacy-preserving signature and authentication techniques** (on ISO/IEC JTC 1/SC 27) including also the newly developed (decentralized) Attribute-based Encryption scheme; on **device binding for wallet security** (through the Decentralized Identity Foundation (DIF) and Self-Sovereign Identity (SSI) working groups), and on **defining protection profiles including the definition of the type of (overarching) system properties and non-functional properties** that affect the level of trustworthiness of next-generation connected systems (ISO/IEC JTC1/WG13).

Below, we proceed with a more detailed description of the activities that have been performed on the aforementioned working items:

Trusted Computing Group (TCG): The TCG is the internationally accepted standardisation group, which sets all relevant technologies and standards for Trusted Computing (TC) and relevant assurance and attestation schemes. The ASSURED project partners SURREY, DTU, and UBITECH are active members of the TCG and are participating in all TCG meetings for

Funded by the Horizon 2020 Framework Programme of the European Union

discussing the latest advancements in the areas of TPMs, TSS and remote attestation. ASSURED has already established a liaison with the appropriate working groups of TCG namely the TPM Working Group and Internet of Things Working Group, where one of the key points is how to better integrate decentralized roots-of-trust in complex system environments. Highlights can be

TABLE 10: TRUSTED COMPUTING GROUP (TCG)

Trusted Computing Group (TCG)
During the first project period, DTU and UBITECH, on behalf of the ASSURED project, participated in all TCG Meetings (the latest been held remotely on February 21st – 25th, 2022) as well as regularly participated in the biweekly meetings of the TPM Working Group where the ASSURED new attestation schemes were presented and discussed in the context of TCG's new specifications on integrity measurements and event log processing (https://bit.ly/3B6D6hP).
UBITECH and DTU actively contributed to TCG on the design and specification of the new revocation protocol for those devices and systems that have failed to prove their security through attestation (as described in Deliverable D3.2). This activity on the new revocation protocol also put forth a fix to a bug (**hash loop**) that was identified in the Trusted Software Stack (TSS). More precisely, UBITECH and DTU identified an issue with the current TPM specification that affected the ASSURED Configuration Integrity Verification (CIV) scheme implementation. The issue was about how to securely revoke the credentials of a possible compromised system after a failed attestation process. More specifically, the issue impacted the **policies- and sessions-related core TPM services** and was due to how these services were managed for enabling the communication with the attached host. This problem consisted of an **infinite hash loop** and was solved during the definition and development of the ASSURED Revocation protocol by updating the internal functionalities of some TPM commands and building blocks. **This elegant solution did not require any modifications or updates to the specification of the existing TPM commands, which would have limited the applicability of the new approach.** UBITECH and DTU worked together with TCG (more specifically TCG Chair of the TSS stack – Kenneth Goldman) to highlight the issue and propose its fix, which was included in the updated TSS Specification and Implementation as published in the core TCG Github ("Avoiding hash Loops when Making Policies for a TPM 2.0" - https://github.com/TrustedComputingGroup/TPM/wiki).
ASSURED also initiated collaboration activities for an optimized implementation of the Direct Anonymous Attestation (DAA) protocol to be possibly considered as a default command in the new TPM specification. While DAA has been proposed in the literature for many years, TCG was lacking adequate evidence on concrete use cases that may benefit from the integration of such an advanced security mechanism. ASSURED, through the use of DAA for achieving **device binding and enhanced level of trustworthiness and differential credential security** for a device towards the **self-issuance and management of their verifiable credentials (ASSURED TPM-based Wallet)**, was one of the first projects bringing together the TCG and SSI communities on how the **integration of hardware-based keys can enabled the vision of European Self-sovereign Identity**. ASSURED is currently under discussions and working together with the TPM working group on implementing and releasing a new optimized version of its Enhanced DAA protocol (updated also with revocation capabilities).
Finally, ASSURED is planning to setup a dedicated meeting with the TCG Board of Directors (as part of the next TCG Meeting scheduled to be held on June 2022) so as to present its latest advancement in the implementation of the newly developed attestation enablers.

Decentralized Identity Foundation (DIF) and European Self-Sovereign Identity Lab (SSI): DIF (https://identity.foundation/) and SSI (essif-lab.eu) are the two standardisation initiatives that work together to make existing (and new) SSI technology into a scalable and interoperable infrastructure so that all users and devices are able to securely manage their (decentralised) identities, thus, enabling them to perform secure online transactions. They focus on the design, implementation and operation of verifiable credentials for the secure identity management of entities in online transactions. So far, **SSI approaches do not explicitly contain trust management approaches**. The current focus is more on technical interoperability through standardisation of interfaces and protocols, but SSI is still missing an advanced trust

Funded by the Horizon 2020 Framework Programme of the European Union

management capable of dealing with different trust levels and roots of the participating entities as well as different trust domains. In this context, ASSURED has performed the following activities:

TABLE 11: DECENTRALIZED IDENTITY FOUNDATION (DIF) & EUROPEAN SELF-SOVEREIGN IDENTITY LAB (SSI)

Decentralized Identity Foundation (DIF) & European Self-Sovereign Identity Lab (SSI)
UBITECH has already established a liaison and is a member of both working groups. Thus, UBITECH (with the support of DTU and UNIS) **proposed the secure hardware integration into the SSI domain through the design of the ASSURED TPM-based Wallet.** This DAA-protected component can be integrated into the Holder side of the SSI ecosystem for protecting the issuance and use of both Verifiable Credentials and Verifiable Presentations. *This has already initiated a close collaboration with the community on integrating the use of DAA enhancing the level of assurance of such device wallets.* ASSURED is already working together with the eSSIF-Lab for releasing the implementation of the TPM-based Wallet to be considered as part of the SSI infrastructure.
ASSURED has also established a close collaboration with the DIF community and more specifically the Wallet Security Working Group. The focus here is on designing new security primitives for guiding and possibly defining a common and interoperable process for securing the identity management process. ASSURED is actively contributing to the Device Binding Working Item pushing the use of DAA as a building block for the wallet security that enables a high level in the differential credential security model by anchoring a hardware-generated public key to the credential. This specification will integrate the design of the current ASSURED TPM-based Wallet. The result of the design, implementation and evaluation will be packaged in the context of a specification document to be given as a guidance document to the SSI protocols.

ISO TC 307 (https://www.iso.org/committee/6266604.html): ISO TC 307 is working on standardisation of Blockchain technologies and distributed ledger technologies. ASSURED has already established a liaison with the respective working groups ISO/TC 307/JWG 4 and ISO/TC 307/WG 2 on Security, Privacy and Identity Management when interacting with the DLTs. ASSURED has already presented its newly designed cryptographic schemes (Attribute-based Encryption and Searchable Encryption) as part of the overall ASSURED Blockchain infrastructure where efficient and decentralized identity management (through the use of trust anchors) is of paramount importance towards downloading and executing the necessary attestation policies modelled as smart contracts. DTU and SURREY, as active members of these working groups, joined efforts in the “Overview of trust anchors for DLT-based identity management (TADIM)” (https://www.iso.org/standard/81773.html).

In addition to the collaboration with the aforementioned working groups, ASSURED has also identified the following initiatives with which it aims to establish a liaison for presenting the conducted work on putting forth a conceptual model capturing the different levels of trustworthiness for a “Systems-of-Systems” based on the safety-critical nature of the comprised services. This is part of the standardisation activities roadmap for the second half of the project and will be reported in D7.3.

TABLE 12: RELEVANT BODY / STANDARD

Relevant Body/Standard
ISO/IEC JTC1/AG8 – Meta Reference Architecture and Trust Reference Architecture Integration: ASSURED aims in contributing insights to: (i) Architecture Alignment – ASSURED trust management building blocks (through the designed attestation enablers) will be promoted to the EU trust reference architecture standards that are not currently well aligned for all actors in the IoT ecosystem since they still reflect a fragmented approach per actor/type.

Funded by the Horizon 2020 Framework Programme of the European Union

ISO/IEC JTC1/WG13 – Trustworthiness: ASSURED will contribute insights on the definition of the overarching system properties and non-functional properties that affect the level of trustworthiness of connected systems. This is essentially to push the identified type of system properties that need to be considered for continuous attestation to the various protection profiles for the different types of devices considered in the ASURED envisioned use cases.
ISO/IEC JTC1/SC27 – Information Security, Cyber-Security and Privacy Protection: ASSURED will work actively for pushing specifications on Data Spaces: There are currently no specific standards on a harmonized data model that can also capture the necessary security claims, as outputted by assurance mechanisms, and can be used by any received part for verifying the level of trustworthiness of the data origin.
ISO/IEC JTC1/WG11 – Smart Cities: ASSURED, based on one of its envisioned use cases on public safety will share insights on distributed trust assessment mechanisms for Smart Cities. ASSURED will try to push its trust management architecture as an open-source standard by promoting approaches such as the MIM (Minimum Interoperability Mechanism) of OASC.
ETSI MEC ISG, ETSI Zero Touch network and Service Management (ZSM) WG as well as to ETSI Experiential Networked Intelligence (ENI) ISG WG: ASSURED will share insights on activities related to TPM-based Zero Touch On-boarding of systems towards the creation of a secure service graph chain.

7.2 STANDARDISATION ACTIVITIES

TABLE 13: STANDARDISATION ACTIVITIES BY PARTNER

UBITECH
Besides the aforementioned activities of UBITECH as it pertains to its collaboration with TCG, DIF and SSI, UBITECH is also a member of the Trusted IoT Ecosystem, as part of the Global Semiconductor Alliance (https://www.gsaglobal.org/iot/ties/) where the focus is on proposing guidelines on the "end-to-end" security needs in today's supply chains. In this context, UBITECH is participating in the TIES/SWG-02 on "Secure Chip-to-Cloud Assurance Solutions for Enablement of Automotive IoT Services" where it pushes the developed TPM-based attestation extensions as a technical specification for **ensuring security together with a hw- or sw-based root-of-trust and secure safety island and showcase how to integrate them into automotive systems.**
DTU
DTU, besides the described activities that it contributed when it comes to trusted computing and its close collaboration with the TCG, it is also a member of the Danish standardisation committee on Blockchain infrastructures (Blockchain S-843) (https://www.ds.dk/da/udvalg/kategorier/it/blockchain). In this context, DTU has participated in all S-843 meetings and is also actively contributing to the specification documents of JWG4 on "Security, Privacy and Identity" presenting the new ASSURED solutions on secure on-chain interactions based on the use of a TPM as an underlying trust anchor. Furthermore, DTU attended the *TSN/A CONFERENCE TECHNOLOGY & APPLICATIONS*, which took place on 7 - 8 October 2020, as a virtual conference. DTU also participated in some of the meetings listed here, open to the public, where it interacted with people in the audience on the ASSURED vision: https://1.ieee802.org/tsn/tsn-tg-meetings/#Upcoming_Meetings. Furthermore, DTU participated and presented in this meeting: IEEE P802.1DG meeting, which took place on 10 August 2021 (here the agenda: https://listserv.ieee.org/cgi-bin/wa?A2=ind21&L=STDS-802-1-MINUTES&O=A&P=316563). The focus was on how ASSURED attestation enablers can also facilitate real-time systems as part of the Time Sensitive Networking (TSN) Group.

Funded by the Horizon 2020 Framework Programme of the European Union

TUDA
Due to the individual deliverables the understanding of attestation schemes and the interdependencies between different strategies was improved in our and/or Postdocs working on ASSURED group. To improve the general understanding of this, TUDA discussed the new schemes frequently in the weekly research seminar of our group. Further, TUDA is currently considering including the gained knowledge into the curricula classes for MSc. students to give a basic understanding of the different attestation schemes and their targeted scenarios.
TUDE
Dr. Kaitai Liang, from TUDE, has been participating in the Dutch NEN about the cybersecurity and privacy, and blockchain standardisation. He is participating into the quarterly meetings within NEN and the bi-yearly events of ISO/IEC JTC 1/SC 27/WG 2 to present and promote ASSURED technologies.
SURREY
Surrey has continued an Academic Liaison relationship with TCG to disseminate the work conducted in the context of ASSURED. Surrey participates in the following TCG working groups: Trusted Platform Module (TPM), TPM Software Stack (TSS), Trusted Network Communications (TNC), the Internet of Things (IoTs), Mobile, and Embedded Systems. In addition, Surrey is working on the Enhanced Direct Anonymous Attestation scheme which is targeted for inclusion in the next TPM specifications. Surrey has also been continuously involved in ISO/IEC JTC 1 SC 27 WG 2, to contribute to the development of several cryptographic standards, and to the study period of post-quantum cryptography. Prof. Liqun Chen designed some of the cryptographic algorithms used in the Trusted Platform Module (TPM). She has also developed several cryptographic schemes adopted by International Standards, such as ISO/IEC and IEEE. Prof. Liqun Chen has enjoyed her active roles as editor for six ISO/IEC standards, and as associate editor or member of the editorial board for four international journals. She also serves as the deputy chairman of Technical Subcommittee 2 of BSI IST/33, dealing with Security Mechanisms and providing input to ISO/IEC JTC1/SC27. Prof. Liqun has recently attended the two online ISO meetings on “ISO/IEC JTC 1/SC 27/WG 2 – Cryptography and Security Mechanisms”, held on April and November 2021, that discussed the Standardised attestation schemes, key management, encryption schemes etc. that are adopted in ASSURED. Surrey has reviewed and commented on the FIDO ECDAA protocol, which makes use of the TPM technology.
NVIDIA/MLNX
NVIDIA is involved in many standardisation bodies including but not limited to TCG, DMTF, and ISO. Nvidia shall propagate the research done in the context of assured and present the work done to these groups where it fits and can contribute to specifications being developed within the relevant groups.
UTRCI
Collins Aerospace (UTRC) is an active participant of SAE G34/EUROCAR WG114 international committee that prepares technical standards, guides and any other material required to support the development of systems and the certification of aeronautical systems implementing AI technologies. Collins engineers are also strongly involved in the avionics and autonomy working groups of several EU and US international standardisation committees related to DO-178C certification of GPUs, EASA-FAA multicore certification guidance (AMC20-193), and ESA’s ECSS revision. With well-established

Funded by the Horizon 2020 Framework Programme of the European Union

links with key avionics manufacturers and scientific networks, as well as specialist communications and exploitation professionals, Collins is ideally positioned to maximize dissemination and exploitation of its hardware/software architecture and research, while the international leadership of Collins industrial partners ensures efficient channels for exploitation.

Funded by the Horizon 2020
Framework Programme of the European Union

8 SUMMARY AND OUTLOOK

Beside the technical and R&D work, dissemination, communication, and exploitation are key areas of activity for the members of the consortium and for the success of the whole project.

This document provides an overview of dissemination and communication activities, both conducted and planned. As reported, several targeted dissemination activities have been performed both jointly and individually by project partners, including scientific publications which have been made available via the EU compliant repository ZENODO. To raise awareness of the project's goals and target project stakeholders, including the general public, the consortium's common dissemination strategy has been further developed and defined.

In addition to that, the deliverable includes an update on standardisation activities and a summary on internal and external training activities. A first few on the market as well as updated individual exploitation plans per partner were also included. The joint exploitation strategies will be discussed more precisely during the last year of the project, when the concrete project results will be available.

The individual exploitation plans, as well as the described market opportunities and the joint exploitation strategy confirm the effectiveness of the research results produced within the project, and the possibility to produce value by leveraging the project's activities.

In D7.3 "Final plan and report on Exploitation, Standardisation Dissemination and Communication activities", due in M36, the dissemination and communication activities undertaken during the second half of the project will be presented. Furthermore, the exploitation plans will be updated once again, and a rough insight on the target market opportunities and exploitation beyond the project will be presented.

Funded by the Horizon 2020 Framework Programme of the European Union

ABBREVIATIONS

IP	Internet Protocol
TCP	Transmission Control Protocol
AB	Advisory Board
CIV	Comprehensive Integrity Verification
CSPL	Cyber Security and Privacy Lab
DA	Dynamic Analysis
DoA	Description of Action
DOI	Digital Object Identifier
GA	Grant Agreement
HSM	Hardware Security Module
KPI	Key Performance Indicators
NFV	Network Function Virtualisation
Oss	Operating Systems
PSS	Privacy, Security, and Safety
R&D	Research and Development
S5	Suite5
SA	Static Analysis
SICORP	Strategic International Collaborative Research Program
SMEs	Small and Medium Enterprises
SVM	Security and Vulnerability Management
SVN	Subversion Server
TNC	Trusted Network Communications
TPM	Trusted Platform Module
WiTEC	Women in Science, Engineering, and Technology

Funded by the Horizon 2020 Framework Programme of the European Union