CASTOR

Building Trust
in the Computing Continuum

D7.1 Plan for Dissemination and Exploitation including Communication Activities

Project number	101167904
Project acronym	CASTOR
Project title	Continuum of Trust: Increased Path Agility and Trustworthy Device and Service Provisioning
Start date of the project	1st October 2024
Duration	36 months
Call	HORIZON-CL3-2023-CS-01

Deliverable type	Report
Deliverable reference number	HORIZON-CL3-2021-CS-01-101167904/ D7.1 / v1.0
Work package contributing to the deliverable	WP7
Due date	March 31st, 2025
Actual submission date	March 31st, 2025

Responsible organisation	D4P (Digital for Planet)
Editor	Olivia Ciubotariu
Dissemination level	PU
Reviewers	Thanassis Giannetsos (UBITECH), Konstantinos Latanis (SUITE5)

Abstract	This deliverable presents the CASTOR Communication and Dissemination strategy, highlighting the tactics and the assets to be leveraged throughout the project. A timeline of short- and long-term planned activities is presented. A detailed standardization plan is documented constituting a guideline for the liaison and further dissemination of the CASTOR project to external target groups and related standardization working groups. Furthermore, a full Exploitation strategy aiming to build a solid foundation for future commercial applications and market-oriented innovations is presented.
Keywords	Communication Strategy, Collaborative Tools, Infrastructure, Internal Communication, External Communication, Standardization, Liaisons, Stakeholders, Exploitation

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributors
V0.1	07.01.2025	Table of Contents created and discussed with the partners	Olivia Ciubotariu (D4P)
V0.2	20.01.2025	First draft of the Communication and Dissemination strategy focusing primarily on the activities done for establishing the “awareness” of the project.	Olivia Ciubotariu (D4P)
V0.3	17.02.2025	Initial draft on the standardization strategy of CASTOR listing those workings group of interest for which the project should aim to establish a liaison.	Olivia Ciubotariu (D4P), Nikos Fotos (UBITECH), Stelios Kazazis (QUBITECH), Fabian Schwarz (NVIDIA), Yalan Wang (SURREY), Ioan Constantin (ORO), Ciprian-Romeo Comsa (TUIASI), Michael McElligott (COLLINS), Panagiotis Pantazopoulos (ICCS), Teo Dimitrakos (KENT), Kostas Latanis (SUITE5), Vasiliki Lamprousi (WINGS), Antonio Skarmeta (UMU), Kostas Maliatsos (FERON), Andras Edelmayer (COMMSIGNIA), Anuj Pathania (UvA), Anastasia Kazakli (K3Y Ltd)
V0.4	24.02.2025	Final version of exploitation strategy with a detailed description of all envisioned Key Exploitable Results (KERs) as well as on the agreed Open-Source Development Plan (OSD) and strategy to be followed.	Olivia Ciubotariu, Daniel Onwude (D4P), Nikos Fotos, Thanassis Giannetsos (UBITECH), Stelios Basayiannis (COLLINS)
V0.5	03.03.2025	Final version of list of past and future dissemination activities of interest – capturing also a non-exhaustive list of events that the consortium will target.	Olivia Ciubotariu (D4P), Nikos Fotos (UBITECH), Stelios Kazazis (QUBITECH), Fabian Schwarz (NVIDIA), Yalan Wang (SURREY), Ioan Constantin (ORO), Ciprian-Romeo Comsa (TUIASI), Michael McElligott (COLLINS), Panagiotis Pantazopoulos (ICCS), Teo Dimitrakos (KENT), Kostas Latanis (SUITE5), Vasiliki

			Lamprousi (WINGS), Antonio Skarmeta (UMU), Kostas Maliatsos (FERON), Andras Edelmayer (COMMSIGNIA), Anuj Pathania (UvA), Anastasia Kazakli (K3Y Ltd)
V0.6	12.03.2025	Final version of the description of the standardization activities envisioned to be conducted. Particular emphasis was given to IETF related activities since they have the most overlaps with the core tasks of CASTOR.	Olivia Ciubotariu (D4P), Nikos Fotos (UBITECH), Stelios Kazazis (QUBITECH), Fabian Schwarz, Meni Orenbach (NVIDIA), Yalan Wang (SURREY), Ioan Constantin (ORO), Ciprian-Romeo Comsa (TUIASI), Michael McElligott (COLLINS), Panagiotis Pantazopoulos (ICCS), Teo Dimitrakos, Yannis Krontiris (KENT), Kostas Latanis (SUITE5), Vasiliki Lamprousi (WINGS), Antonio Skarmeta (UMU), Kostas Maliatsos (FERON), Andras Edelmayer (COMMSIGNIA), Anuj Pathania (UvA), Anastasia Kazakli (K3Y Ltd)
V0.7	17.03.2025	First internal reviews conducted	Thanassis Giannetsos (UBITECH), Kostas Latanis (SUITE5)
V0.8	25.03.2025	Revisions made and commencements of the second round of review	Olivia Ciubotariu, Daniel Onwude (D4P), Thanassis Giannetsos, Nikos Fotos (UBITECH)
V0.9	28.03.2025	Reviewed documents	Thanassis Giannetsos (UBITECH), Kostas Latanis (SUITE5)
V1.0	31.03.2025	Final version prepared for submission	Olivia Ciubotariu (D4P), Daphne Galani (UBITECH)

Funded by EU's **Horizon Europe** programme under Grant Agreement number **101167904** (*CASTOR*). Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

This work has received funding from the **Swiss State Secretariat for Education, Research and Innovation** (SERI).

Funded by **UK Research and Innovation** (UKRI) under the UK government's Horizon Europe funding guarantee 10139619.

COPYRIGHT NOTICE

Project funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	**R**	
Dissemination Level		
PU	Public, fully open, e.g. web (Deliverables flagged as public will be automatically published in CORDIS project's page)	**X**
SEN	Sensitive, limited under the conditions of the Grant Agreement	
Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No2015/ 444*	

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

DEM: Demonstrator, pilot, prototype, plan designs

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

DATA: Data sets, microdata, etc.

DMP: Data management plan

ETHICS: Deliverables related to ethics issues.

SECURITY: Deliverables related to security issues

OTHER: Software, technical diagram, algorithms, models, etc.

Editor

Olivia Ciubotariu (D4P)

Contributors (ordered according to beneficiary numbers)

Nikos Fotos, Thanassis Giannetsos (UBITECH)

Stelios Kazazis (QUBITECH)

Fabian Schwarz, Meni Orenbach (NVIDIA)

Yalan Wang (SURREY)

Ioan Constantin (ORO)

Ciprian-Romeo Comsa (TUIASI)

Michael McElligott, Stelios Basayiannis (COLLINS)

Panagiotis Pantazopoulos (ICCS)

Kostas Latanis (SUITE5)

Anastasia Kazakli (K3Y)

Vasiliki Lamprousi (WINGS)

Antonio Skarmeta (UMU)

Kostas Maliatsos (FERON)

Andras Edelmayer (COMMSIGNIA)

Anuj Pathania (UvA)

Olivia Ciubotariu, Daniel Onwude (D4P)

Teo Dimitrakos, Yannis Krontiris (KENT)

DISCLAIMER

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

EXECUTIVE SUMMARY

This Deliverable aims to provide a clear update on the **initial communication, dissemination and standardization plan**, of the CASTOR project. **Dissemination and communication activities that took place in the first six months of the project are explained and further plans are summarized**. Updates on the dissemination report will be provided in the upcoming periodic reports as well as in D7.2 “Dissemination, Communication, Clustering and Exploitation activities” in M18 and D7.3 “Dissemination, Communication, Clustering activities including concrete exploitation measures” in M36.

After the introductory **CHAPTER 1**, **CHAPTER 2** depicts the Vision and the Mission of CASTOR and the core technologies being investigated. The endmost goal is to set the scene of “*why, and which*” audience will be interested in the technical outcomes considering the multidisciplinary nature of the project: CASTOR envisions answering all questions related to the achievable assurances of Compute Continuum (CC) workloads operation over (end-to-end) communication paths, stressing the efficient (life-cycle) security management need under a zero-trust approach. **CHAPTER 3** then details the tactics and tools used to execute the converged Communications and Dissemination Strategy, including a status report on completed activities. This also includes the listing and description of the KPIs (metrics for the evaluation of the dissemination and communication activities) already defined for a successful dissemination plan to the defined target audiences (Section 3.3). Finally, it also puts forth detailed lists of already performed communication activities and a series of workshops and events that CASTOR is planning to attend and contribute in the near future (short-term activities). This list is a live document that will be updated throughout the lifecycle of the project.

CHAPTER 4 focuses on activities related the Collaboration with relevant initiatives and the Standardization plan. **CHAPTER 5** sets the baseline for the Exploitation plan that will be created later in the project by documenting the methodology to be followed (putting forth the envisioned Open-Source Development Plan to be employed) for the list of exploitable assets already identified. Finally, **CHAPTER 6** concludes the document.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1 INTRODUCTION

This Deliverable presents a strategic **Plan for Dissemination, Exploitation, and Communication Activities** as defined by **Work Package 7 (Dissemination, Standardization, Exploitation & Impact Creation)** within the **CASTOR** project. It outlines CASTOR's strategic framework and outreach approach, highlighting the activities conducted from M01 to M06, as well as detailing planned initiatives for **Dissemination**, **Communication**, **Standardization**, **Exploitation**, and **Impact Creation** to achieve project objectives and support partners' operational activities. Additionally, this document establishes a coordinated framework for collaboration with key stakeholders, including the European Commission and other Horizon Europe projects.

1.1 PURPOSE OF THE DOCUMENT

Apart from the overview of the **CASTOR Communication, Dissemination, Standardization, and Exploitation plan, this deliverable** provides also a first report on activities, which includes communication and dissemination materials that were created and used within the project up to this date. Regarding the latter, dissemination activities ensure the visibility and awareness of the project and support the wide adoption of its results among potential users**.** Our dissemination and communication plan prepares the way for a successful project from the beginning until its end – engaging continuously with both internal and external audiences. As thoroughly described in CHAPTER 3, our activities have been clustered into three main phases (illustrated in Figure 3) for reaching the widest possible audience, thus, increasing the impact of the overall project activities. These revolve around the following:

- Deliver a Robust Dissemination and Communication Strategy: **deploy a comprehensive set of tactics and tools aimed at increasing awareness of CASTOR's results among all target audiences.**
- **Highlight Strategic Partnerships:** underline current and future efforts concerning alliances with clusters, international data spaces, and marketplaces, engaging key players across domains such as cybersecurity, trustworthiness, sovereign identity, and data management/sharing.
- **Support Standardization and Legislation:** present research contributions to standardization and liaison processes, reinforcing alignment with industry standards and regulatory frameworks.
- **Outline Exploitation and Sustainability Plans:** Provide an overview of the Exploitation, IPR Handling, and Business & Sustainability Planning to capitalize on the project's technological artefacts and scientific outcomes, underpinned by an initial exploitation analysis.

In a nutshell, the first phase focuses on increasing awareness and consists of building up CASTOR's corporate identity, as well as establishing the CASTOR website and additional project information material for better conveying the core vision of the consortium (towards the establishment of a zero-trust compute continuum) even to a non-technical audience. In the second phase, the focus is shifted to the scientific and technical outcomes of the project consortium (aiming for both high-quality publications in top-tier conferences and journals, as well as initiating scientific debates in various workshops and organized webinars in relevant technologies – cf. CHAPTER 2) to bring information to the community. This will allow the consortium to make presentations at conferences and workshops to further raise awareness among the scientific and industrial stakeholders. This will facilitate lively discussions on the project's topics at these events by providing new insights and feedback on the project´s progress to project partners. This feedback will contribute to the project´s success and possibly also follow-up research activities. Furthermore, scientific publications and a selection of deliverables (those that are public) will be published on the project website to keep interested parties informed about the latest progress. Finally, in the third phase, all the above will culminate into further exploitation, which means using the results for commercial purposes or in public prototyping. There will still be some ongoing dissemination activities after the project has ended to promote the project results (e.g., the project website will be online for a further five years, and similarly, social media, and cooperation activities with other projects, talks at conferences and follow-up projects, will be kept alive), and the main focus will be to exploit them and attract the target audience group.

In this context, the **knowledge and outcomes generated by CASTOR will be systematically shared with target groups through dedicated tools and channels managed by WP7** (CHAPTER 3). Selected results will be curated to ensure clarity and accessibility for all audiences. This approach is vital for creating a sustainable impact and maximizing the exploitation potential of CASTOR's innovations.

Overall, this deliverable constitutes the first essential communication kit regarding the CASTOR project's activities, including a narrative text, photographs, slides, and any other suitable communication material, complemented with copyright licenses for the European Commission. This kit will be updated in (D7.2) "Dissemination, Communication, Standardization, and Exploitation Activities – Initial Version" and (D7.3) "Dissemination, Communication, Standardization, and Exploitation Activities – Final Version". The designed communication strategies constitute a guideline for presenting CASTOR to external target groups including conferences, dissemination, and communication channels. Furthermore, this deliverable constitutes the formal launch of the internal CASTOR communication infrastructure including the establishment of mailing lists, the repository, and the CASTOR website. Finally, it's important to note that as part of its communication efforts, CASTOR seeks to create and maintain a trusted knowledge suite designed to provide reliable, consistent, and well-organized information that will benefit both in-project collaborations and CASTOR's target audiences.

1.2 RELATION TO OTHER WORK PACKAGES

This Deliverable, and consequently the entire WP7 requires input from all core technical Work Packages (WPs) of the CASTOR project as these will provide the necessary technical material for disseminating the outputs of the project. These contributions will help boost the WP7 activities in terms of dissemination, communication, standardization, and exploitation aspects. **Figure 1** summarizes the interdependencies between the relevant work packages in CASTOR. Specifically, this deliverable takes input from WP2 concerning the overarching CASTOR reference architecture as well as the CASTOR Threat Modelling that is being targeted. Secondly, WP3 provides information about the set of CASTOR Trust Extensions that can be deployed across the Compute Continuum to unlock the trust assessment capabilities. Subsequently, input for the design and implementation of the overall trust assessment framework is provided by WP4. Finally, WP5 aims to accommodate the software stack realizing the trusted path routing across the Compute Continuum bridging the gap between requirements provision at a Service Level (Service Level Agreements (SLAs)) and their concrete enforcement of corresponding policies throughout the service lifecycle.

1.3 STRUCTURE OF THE DOCUMENT

After the introductory **CHAPTER 1**, **CHAPTER 2** depicts the vision and the mission of CASTOR and the core technologies being investigated. The endmost goal is to set the scene of "*why, and which*" audience will be interested in the technical outcomes considering the multidisciplinary nature of the project: CASTOR envisions answering all questions related to the achievable assurances of Compute Continuum (CC) workloads operation over (end-to-end) communication paths, stressing the efficient (life-cycle) security management need under a zero-trust approach. **CHAPTER 3** then details the tactics and tools used to execute the converged communications and dissemination strategy, including a status report on completed activities. This also includes the listing and description of the KPIs (metrics for the evaluation of the dissemination and communication activities) already defined for a successful dissemination plan to the defined target audiences (Section 3.3). Finally, it also puts forth detailed lists of already performed communication activities

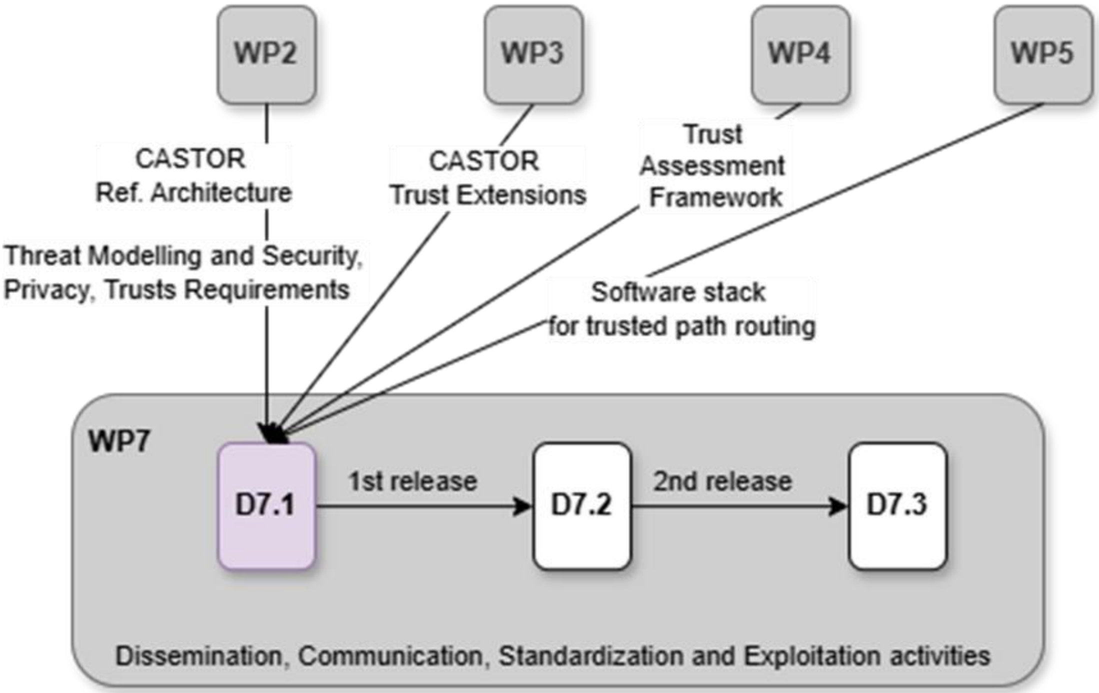


Figure 1: Relationship with other Work-Packages

and a series of workshops and events that CASTOR is planning to attend and contribute in the near future (short-term activities). This list is a live document that will be updated throughout the lifecycle of the project. **CHAPTER 4** focuses on activities related the collaboration with relevant initiatives and the standardization plan. **CHAPTER 5** sets the baseline for the exploitation plan that will be created later in the project by documenting the methodology to be followed (putting forth the envisioned Open-Source Development Plan to be employed) for the list of exploitable assets already identified. Finally, **CHAPTER 6** concludes the document.

CHAPTER 2 CASTOR VISION

Modern service provision in beyond-5G and emerging 6G infrastructure is witnessing a rapid shift from cloud environments to edge, and far-edge layers, shaping the notion of the compute continuum. Even though there has been great effort to the establishment of management and orchestration capabilities satisfying network- and performance-oriented requirements, there exists an ever-increasing need to server application service flows over secure and trustworthy routing channels. In this context, **CASTOR visions to engrain trust-aware decision making in the traffic engineering process as part the overall service provision.** This involves not only the deployment service but also the continuous monitoring of the routing path adhering to the agreed requirements.

Figure 2 captures the current landscape where CASTOR comes into play. At the top layer, diverse **customers and service providers want to deploy a multitude of services with diverse requirements and mixed criticality**. At the same time, **network operators and telecommunication vendors expose diverse capabilities to satisfy the network-based requirements** (e.g., jitter, throughput, hop count) introduced by service providers. Up to this point, there is extensive progress to achieving network consents between the service requirements and the offered resources. However, witnessing the emergence of security- and trust-related intents (e.g., sensitive workflows need to be served with guarantees on the trustworthiness of the carrier routing path), there is still work to be done to accommodate such scenarios. This situation is better illustrated in the hourglass-like diagram of Figure 2: **despite the abundance of vendors (bottom) and the level of complexity of modern provision (top) there is still a limited set of mechanisms (center; this showcases the confined space of available solutions) that provide the required security guarantees in the traffic engineering process**. One example is the definition of the IETF's Trusted Path Routing (CHAPTER 4) initiative that focuses on the integrity – one aspect of trust – of network devices equipped with TPM crypto processors. **To this extent, CASTOR provides the missing pieces to the entire puzzle of engraining trust throughout the CC enabling the introduction of trust-aware decision-making, bridging the gap between the high-level, abstract service intents to concrete deployment and continuous monitoring strategies**.

CASTOR aims to adopt and extend already established capabilities around management and orchestration practices and enrich the available traffic engineering processes with trust-related information for enabling both network- and trust-aware routing decisions. **The provision of novel and efficient trust extensions across the compute continuum lifts the heavy – and unrealistic – trust assumptions around the isolation of infrastructure segments and enables a dynamic, layered trust assessment framework**. This is achieved through the continuous monitoring of the network- and trust-related telemetry data that contributes to the trust characterization of the service and its underlying routing topology throughout its lifecycle. This information can be used for the provision of optimal path recommendations that accommodate both service requirements in terms of network and trust objectives.

Overall, before being able to materialize the service provision process, it is necessary to extract the (S)SLAs that capture all requirements which, in turn, enable the manifestation of enforceable routing contracts that can be pushed to the network plane. This transition highlights the multidisciplinary nature of CASTOR. To overcome all these challenges in each stage of this process, CASTOR enablers span across the layers of the compute continuum – from cloud to the far edge – and can be categorized into the following four pillars:

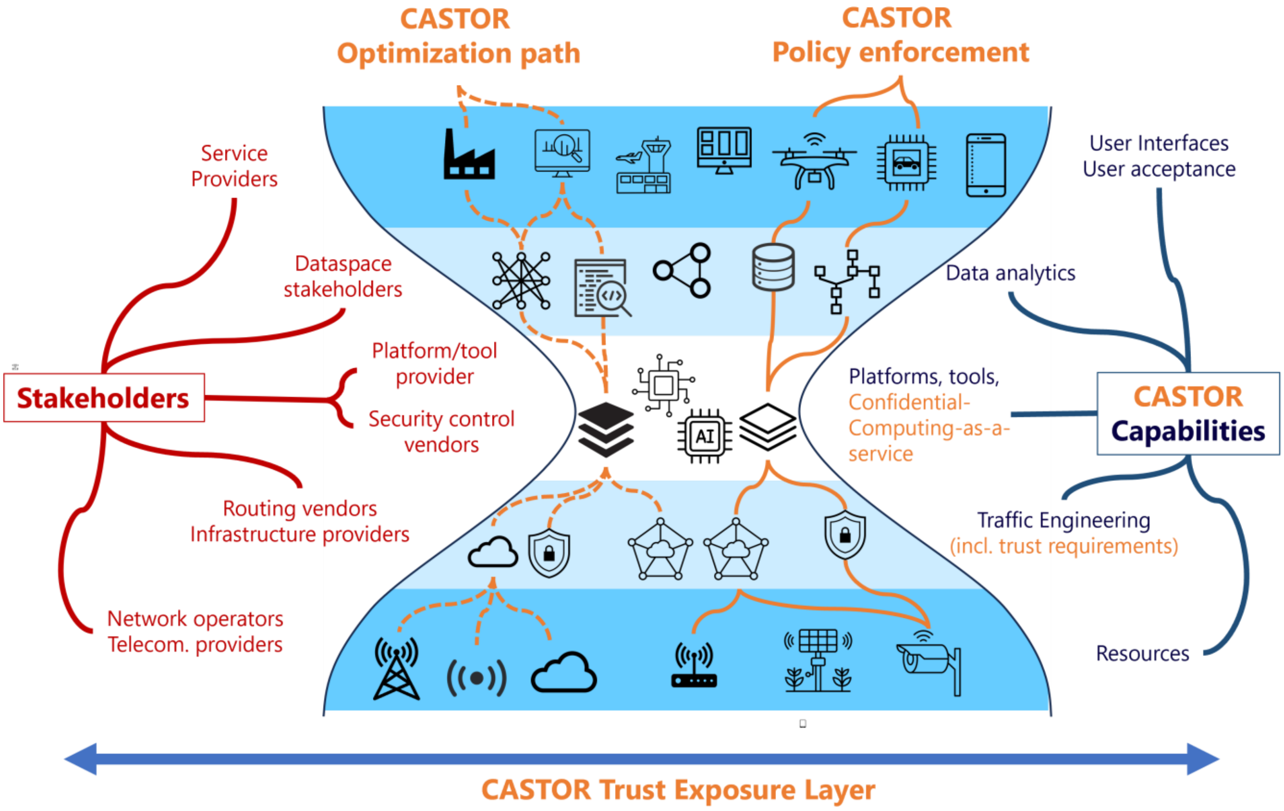


Figure 2: CASTOR Key Technological Capabilities & Vision for Securing the CC

- **Trust and Network-Aware Path Establishment**: Realization of continuum-wide path establishment, expanding across different administrative domains, by enabling path routing decisions for achieving both the strict trust and network resource requirements of mixed-criticality services.
- **Adaptive Trust Quantification**: Establishment and maintenance of an up-to-date view of the trust state of each CC device, enabling the routing of network workloads over the path that can exhibit the Required Trust Level.
- **“Chip-to-Cloud” Security Assurances**: Novel composable attestation mechanisms providing verifiable evidence on the configuration and behavioral integrity of CC devices. CASTOR is the first to account for a harmonized Trusted Computing Base, over decentralized Roots-of-Trust, in the context of trusted path routing.
- **Combinatorial Trust and Resource Optimization**: Intelligent and secure- and network-resources-aware traffic engineering process, identifying and recommending optimal routing paths over only trustworthy edge-core-cloud elements. CASTOR provides a future-ready post-quantum optimization solution to resolve the computationally hard (NP-hard) trusted path routing problem in a hyper-dimensional network search space by employing a meta-heuristic Quantum Annealing (QA) algorithm to determine multiple path segments adhering to varying network and trust requirements.

CASTOR relies on these pillars to engrain trust in the traffic engineering process through a trust-aware decision-making process, distributed across the Compute Continuum (CC). Based on **Figure 2**, the multi-disciplinary nature of CASTOR, allows the expansion of the target audience across different domains in the CC: Both as it pertains to standardization bodies to be targeted (Section 4.2), but also for various industry stakeholders (Section 3.3). Overall, it is important to highlight that CASTOR is agnostic to the target application. As part of the project, the instantiation of CASTOR will take place in four distinct application environments, serving as a proof-of-concept deployment to showcase the CASTOR framework in scenarios with diverse and real requirements.

CHAPTER 3 COMMUNICATION AND DISSEMINATION STRATEGY

A clear communication and dissemination strategy is essential and a forerunner for the execution of a dissemination and communication plan. Therefore, the **CASTOR project has set out a clear Strategy for Dissemination and Communication (Figure 3).** The following sections detail **CASTOR's strategic approach, the communication and dissemination goals, the target audiences, as well as the phases, channels, and tactics that will direct the implementation of these efforts.**

The main Communication goal is to highlight the benefits of the CASTOR project for society, e.g., by showing the public society and media the impact of our project on everyday lives. The core Dissemination goal is to transfer knowledge and make project results available to the industry community, researchers, and policymakers.

Within the CASTOR project, three main audience groups can be defined (a more granular breakdown can be found in Section 3.3):

(A) Broad Public Society

(B) Policymakers

(C) Industry/Research

The channels used to target the above-mentioned audiences are presented in **Figure 3**. The tactics and assets are described in the following sections.

3.1 OVERVIEW OF THE STRATEGIC COMMUNICATION & DISSEMINATION APPROACH

The Communications and Dissemination Strategy for CASTOR plays a pivotal role in ensuring the project's immediate and long-term success.

The strategy is and will continue to be coordinated across the several work packages, with the support of various Communication and Dissemination tactics and tools, fostering a unified approach. This will involve a mix of digital and traditional communication activities, participation in relevant events, and contributions to standardization initiatives. Ultimately, the project's activities, including developed content, tools, services, and Pilot Use Cases (PUCs), will be designed to create significant socioeconomic value from a multi-disciplinary and multi-stakeholder viewpoint.

CASTOR's strategic approach considers **three main phases** for Communication and Dissemination:

- **Awareness Creation –** this first phase consists of building up CASTOR's visual identity, as well as establishing the project through generic information provided via its website and social media channels.

- **Scientific Stream** - In this second phase, the consortium partners will actively promote the project's scientific work. The focus will be on communication via third-party channels, like submissions to conferences and journals. This will enable them to present at conferences and workshops, increasing awareness among both scientific and industrial stakeholders. These events will foster dynamic discussions on project-related topics, offering valuable insights and feedback on the project's progress. This feedback will not only support the project's success but may also inspire future research initiatives. The project and the consortium partners owned channels/tools (websites, blogs, and social media accounts) will be constantly updated to reach a wider and more diverse audience and increase their interest.

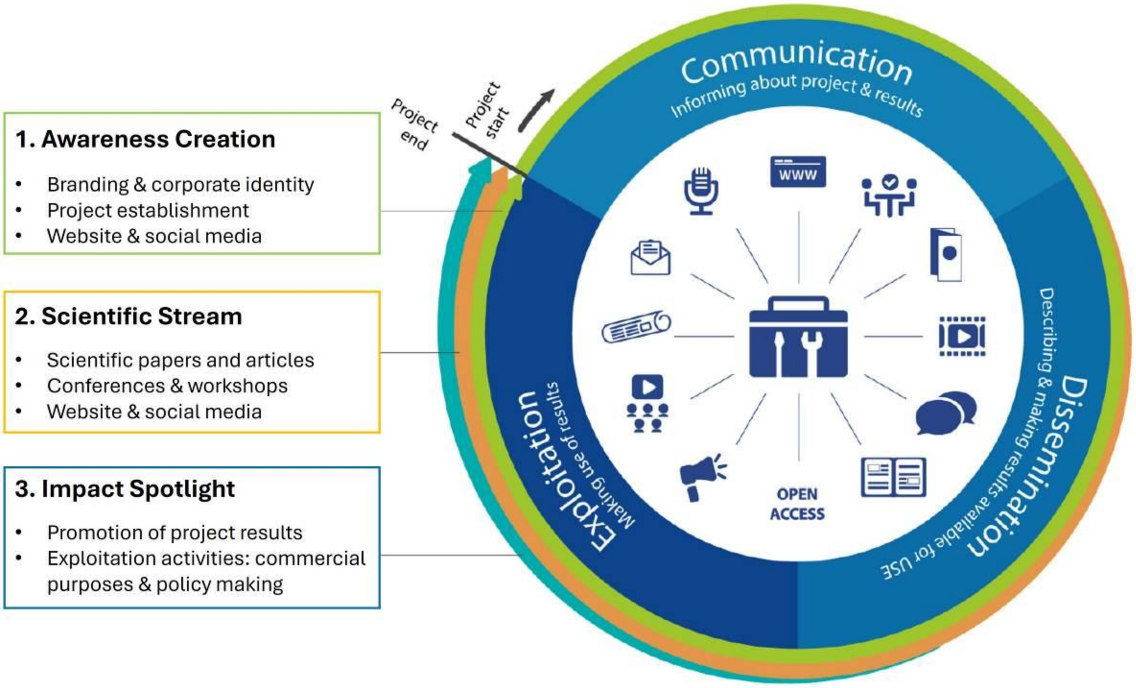


Figure 3: Dissemination & Communication Strategic Approach

- **Impact Spotlight** – during this phase, the Dissemination activities will feed into Exploitation, via using the results for commercial purposes or in public policymaking. There will still be some ongoing Dissemination activities after the project has ended to promote the project results (e.g., the project website will be online for a further five years, and similarly, social media, and cooperation activities with other projects, talks at conferences and follow-up projects, will be kept alive).

3.2 CASTOR OBJECTIVES

Based on the vision put forth in CHAPTER 2, CASTOR puts a lot of emphasis on reaching out both interested scientific, standardization, and industrial communities to have a wide-reaching impact and be effectively communicated to key stakeholders. To achieve this, several objectives will guide its dissemination and outreach efforts:

- **Drive awareness among the targeted audiences**, by ensuring that relevant groups are well-informed about the project's scope, objectives, activities, and outcomes.

- **Disseminate CASTOR results with stakeholders**, using a combination of digital and in-person methods to share project results, networking with stakeholders, and foster collaborative discussions across various platforms and events.

- **Establish liaisons** with other projects, national and international cybersecurity agencies, standardization associations, and initiatives for knowledge and innovation transfer.

- **Collect feedback** from the targeted audiences, validate the project’s results, and ensure their relevance and applicability, via actively seeking input from stakeholders to ensure the project's results meet their needs, validate the outcomes, and confirm their real-world applicability.

3.3 CASTOR TARGET AUDIENCES

The overall communication and dissemination strategy presented in this document aims at reaching out to multiple and diverse target audiences, or Target Groups (TG). As illustrated in Figure 3, the multifaceted characteristics of the CASTOR project allow its influence across a wide range of communities and stakeholders. Specifically, CASTOR's dissemination efforts target **Service Providers (SPs) as it is necessary to ensure that the offered solutions can be eventually reflected in the user experience and accepted by both the relevant SPs and their corresponding end users**. In addition, CASTOR targets to disseminate its findings to **Dataspace Stakeholders concerning the exchange of trust-related information both as part of already-existing traffic engineering protocols as well as in the context of advertising the trust-related capabilities of a domain**. Inherently, all the CASTOR's solutions and the relevant extensions to existing traffic engineering processes are of interest to multiple stakeholders in the **B5G/6G spectrum, including ISPs, infrastructure providers, routing vendors, and telecommunication operators**. Similarly, CASTOR's cryptographic mechanisms can be of interest both for **Trusted Computing vendors as well as for Network Hardware vendors**.

In addition, CASTOR aims to disseminate its work in both research (Section 3.4.2) and policy-making and (pre-) standardization communities (CHAPTER 4). Key stakeholders include **Academia, Research Institutions, and related projects and initiatives; Standardization and Certification Bodies, which ensure compliance with industry benchmarks; and National and EU Public Authorities and Policy Makers**, who influence regulatory frameworks and governance.

Finally, CASTOR targets to evaluate its impact on the wider public as it is critical to ensure the high (end) user acceptance of the solutions and mechanisms that are introduced in the context of the project.

3.4 COMMUNICATION & DISSEMINATION ACTIVITIES

3.4.1 Internal Communication

Effective internal communication and the smooth flow of information are critical to the success of any project. Recognizing this, CASTOR has implemented several tools to ensure seamless information exchange among partners:

- **SharePoin**t **–** To facilitate information sharing and encourage collaboration, a secure, password-protected repository has been set up. This central platform stores important documents; distribution lists; meeting agendas, presentations and summaries; and other project-related materials. It also provides an overview of project progress, displaying key management data such as manpower, finances, deliverables, and partner contacts. The repository is managed by the project coordinator, Ubitech, and it is available at **https://ubitecheu.sharepoint.com/sites/CASTOR/**

- **Mailing Lists** – Several mailing lists, outlined in Table 1, have been created to streamline communication within various project groups. A general mailing list includes all project participants for broad updates, while specialized lists (general, technical, and by work package) are designated for specific matters. Ubitech is responsible for managing and maintaining these lists, ensuring they are kept up to date.

- **Messaging Platform –** In line with its commitment to cybersecurity and privacy, CASTOR uses Slack as the secure messaging platform for communication within the consortium.

- **Consortium Meetings** – Ubitech, the Project Coordinator, organizes monthly meetings with Work Package Leaders and the Project Board to review the progress of all work packages, address any emerging issues, and develop strategies for resolving them. The meeting minutes or recordings, along with any action items, are shared on the repository after each session. Each WP leader holds weekly meetings with their team, providing an opportunity to monitor the project's progress, discuss and resolve open points, and plan the next steps. The outcome of each meeting, as well as the presentations, are captured within the CASTOR SharePoint. At the moment when this deliverable is developed, the main discussions of the weekly meetings revolve around the finalization of the overarching CASTOR architecture. Finally, in-person general assembly meetings are held every semester to ensure alignment and streamline pending discussions among partners at a consortium level.

Table 1: Mailing Lists Developed for Ease of Email Communication within the CASTOR Project

Email list	Description
general@castorhorizon.eu	Mailing list for the entire consortium
technical@castorhorizon.eu	Mailing list for the technical staff of all partners
wp2@castorhorizon.eu	All matters relating to Work Package 2
wp3@castorhorizon.eu	All matters relating to Work Package 3
wp4@castorhorizon.eu	All matters relating to Work Package 4
wp5@castorhorizon.eu	All matters relating to Work Package 5
wp6@castorhorizon.eu	All matters relating to Work Package 6
wp7@castorhorizon.eu	All matters relating to Work Package 7

3.4.2 External Communication and Dissemination Activities

3.4.2.1 Project Identity

As the recognition and perception of a brand are significantly shaped by its visual presentation, a strong and distinct brand identity for the project was established since its launch, to ensure to establish a unique image and distinctness.

The brand guidelines and specific elements were and will continue to be incorporated into all Communication and Dissemination materials produced throughout the project and will be used by all project partners in their Communication and Dissemination efforts.

Further details about CASTOR's brand identity, including guidelines for creating a distinctive and easily recognizable image, can be found in **APPENDIX A.**

3.4.2.2 Website

The CASTOR website is designed to serve as a centralized hub for showcasing and promoting the project's activities. In line with the GA, the website was launched as a Milestone at the end of November 2024, at: https://castorhorizon.eu/, and it was built on the following architecture:

- The **Home** page of the project website offers easy navigation and access to all key public information about the project: vision, mission, consortium, and links to social channels.
- The **About** tab provides further information about the project and detailed data about the consortium partners and each of the project's seven objectives.
- The **Use Cases** tab is an overview of the four Use Cases and individual scenarios. Specific information is to be provided once the use cases are implemented.
- The **What's New** tab will feature news, press releases, and articles about the project, as well as presentations of the events attended throughout the project duration.
- The **Resources** tab is/will be featuring scientific publications, public deliverables, and promotional materials.
- The **Contacts** section enables visitors to directly contact the project through a dedicated form and includes links to CASTOR's social media channels. Messages submitted via the contact form are forwarded to the email address contact@castorhorizon.eu, which is then sent to the relevant project partners, who will review and respond to the inquiry. It's important to note that all information and emails collected are protected under GDPR.

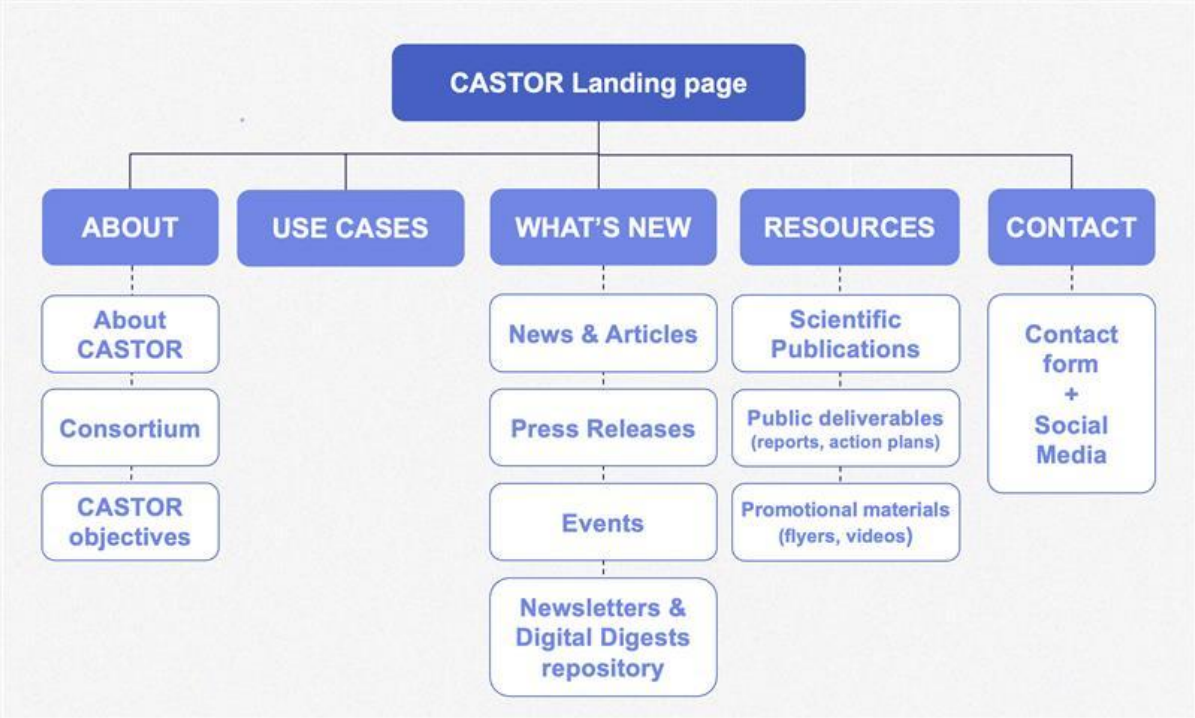


Figure 4: CASTOR Website Architecture

To acknowledge the **EU funding**, both the EU and SERI logos and the following disclaimers are displayed on the website: "Funded by EU's Horizon Europe program under Grant Agreement number 101167904 (CASTOR). Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI)."

The website provides details on the data it collects and how it is used in compliance with GDPR, which can be accessed through the Privacy Policy and Cookie Policy links in the page footer.

CASTOR’s website acts as a comprehensive tool to evaluate the effectiveness of the project Communication and Dissemination efforts, through detailed analysis of web analytics data. The consortium uses Matomo as a web analytics platform to generate in-depth reports on communication campaigns, website traffic, acquisitions, and overall performance. Notably, Matomo complies with European GDPR standards and ensures the protection of collected data ownership.

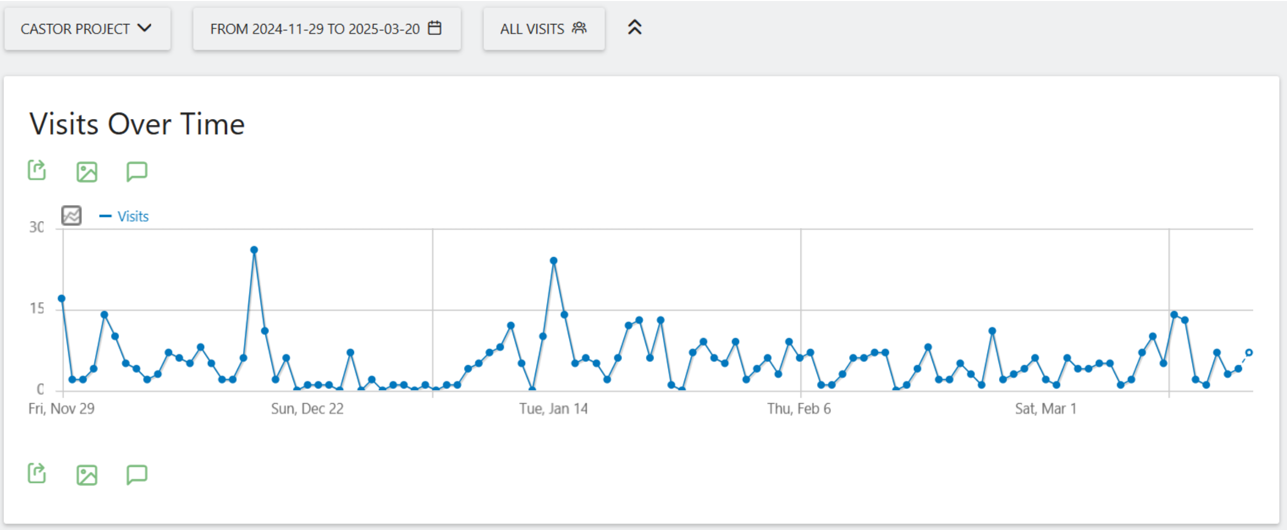
From November 29th, 2024, the website launch date, until March 20th, 2025, the website has recorded 583 visits, with over 1000 unique pageviews; and visitors engaged with the content for an average duration of 3 minutes and 11 seconds. Of these visits, 56% originated from direct entries, 24 % from other websites, 30% from search engines, and 22 % from social networks, as shown in **Figure 5.**

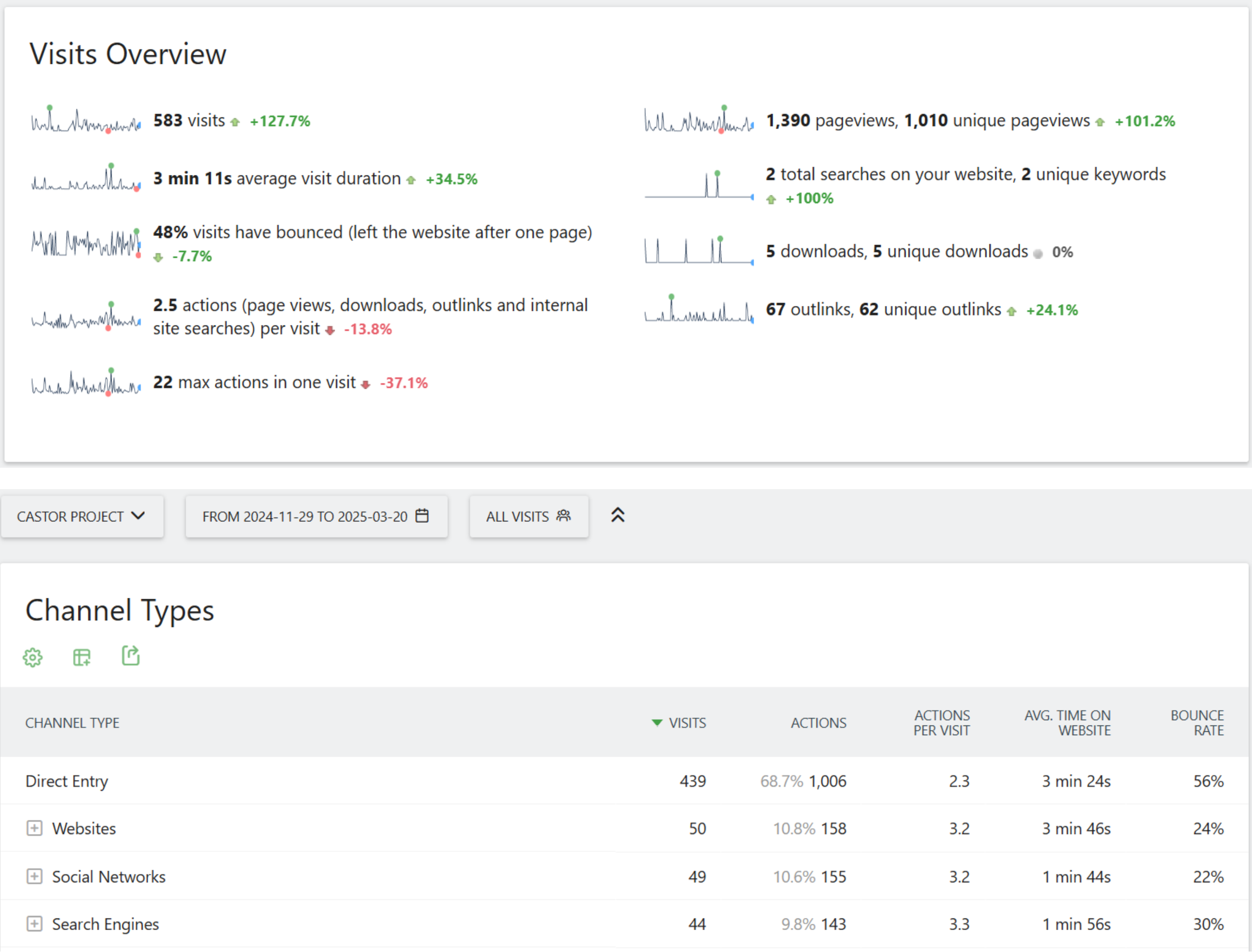
Since the launch of the CASTOR website, we have focused on increasing website traffic through the following strategies:

➲ **Search Engine Optimization (SEO)**: The number of visits to the project website will gradually increase over the course of the project, driven by the implementation of strategies aimed at boosting organic traffic, with a focus on the identified keywords.

➲ **Link Building**: We are building a network of links on the project website, partner websites, and other relevant initiatives. The CASTOR website is/will continue to be cross-linked with the following websites:

- All consortium partners’ websites
- Social media - all project posts on LinkedIn and X include links to various sections of the website.
- Events websites (links will continue to increase upon participation in events)
- EC websites (https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en)
- SERI
- Tools used (i.e. Matomo)





Visits Overview

583 visits +127.7%

3 min 11s average visit duration +34.5%

48% visits have bounced (left the website after one page) -7.7%

2.5 actions (page views, downloads, outlinks and internal site searches) per visit -13.8%

22 max actions in one visit -37.1%

1,390 pageviews, 1,010 unique pageviews +101.2%

2 total searches on your website, 2 unique keywords +100%

5 downloads, 5 unique downloads 0%

67 outlinks, 62 unique outlinks +24.1%

Channel Types

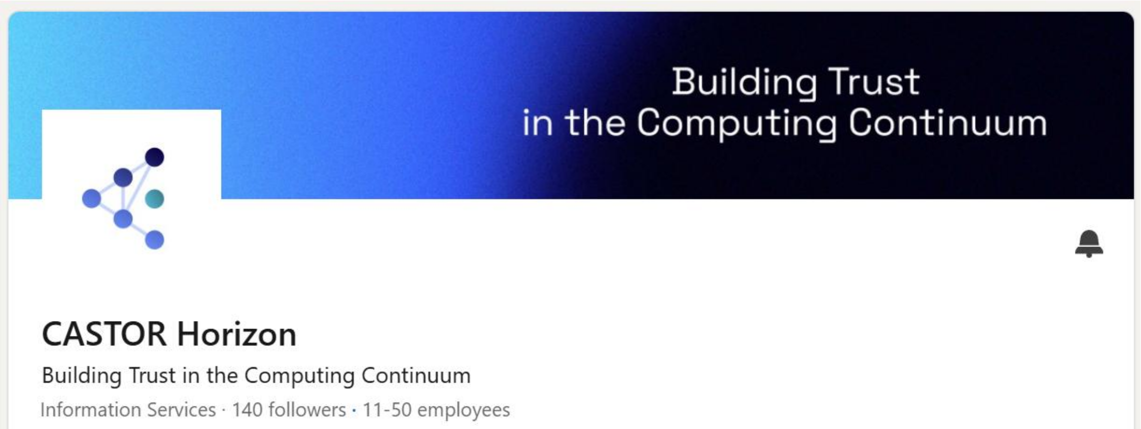
CHANNEL TYPE	VISITS	ACTIONS	ACTIONS PER VISIT	AVG. TIME ON WEBSITE	BOUNCE RATE
Direct Entry	439	68.7% 1,006	2.3	3 min 24s	56%
⊞ Websites	50	10.8% 158	3.2	3 min 46s	24%
⊞ Social Networks	49	10.6% 155	3.2	1 min 44s	22%
⊞ Search Engines	44	9.8% 143	3.3	1 min 56s	30%

Figure 5: CASTOR Website Visits Overview

As a primary dissemination tool, the CASTOR website is and will be regularly updated throughout the project’s duration to ensure it remains current and avoids becoming cluttered or outdated. The website will prominently showcase the latest activities, results, and achievements, organized by topic and relevance, through news posts, videos, infographics, and other formats. Special attention will be given to updating SEO keywords and cross-references to ensure consistent traffic flow to the website.

3.4.2.3 Social Media

The CASTOR social media strategy is built behind an active social media presence on LinkedIn (https://www.linkedin.com/company/castorhorizon-eu/), X (https://www.x.com/CASTORHorizon) and YouTube channel (https://www.youtube.com/@CASTORhorizon).



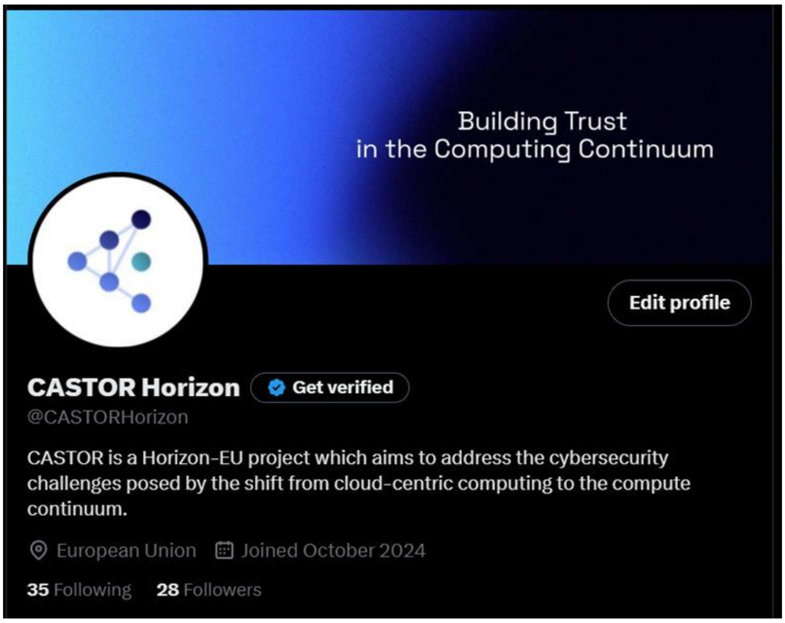
Building Trust
in the Computing Continuum

CASTOR Horizon

Building Trust in the Computing Continuum

Information Services · 140 followers · 11-50 employees

Figure 6: CASTOR LinkedIn Account



Building Trust
in the Computing Continuum

Edit profile

CASTOR Horizon Get verified

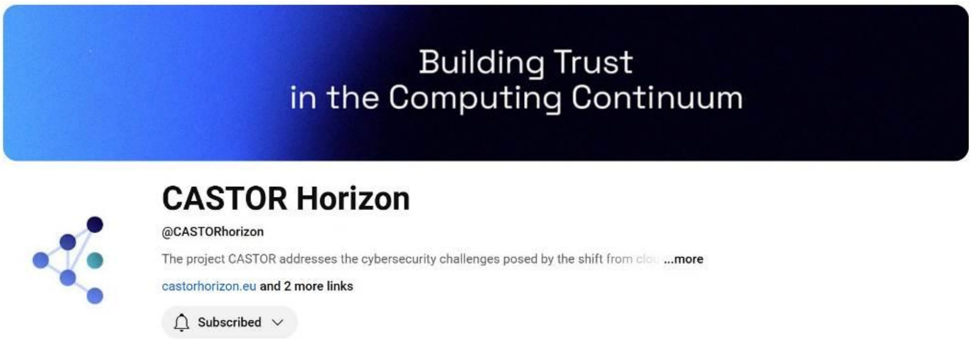
@CASTORHorizon

CASTOR is a Horizon-EU project which aims to address the cybersecurity challenges posed by the shift from cloud-centric computing to the compute continuum.

European Union Joined October 2024

35 Following 28 Followers

Figure 7: CASTOR X Account



Building Trust
in the Computing Continuum

CASTOR Horizon

@CASTORhorizon

The project CASTOR addresses the cybersecurity challenges posed by the shift from clo ...more

castorhorizon.eu and 2 more links

Subscribed

Figure 8: CASTOR YouTube Account

The social media strategy aims to regularly share updates and news about the project, on the following:

- **Introductory themes:**
  - **Meet the Consortium Members** – this theme was used at the beginning of the project, to introduce all the consortium partners;
  - **Cybersecurity Glossary** – to familiarize the technical audiences with specific terminology related to CASTOR scope, as well as the large public with the basic terminology related to cybersecurity.
- **Technology-related themes** – as the project's technical work advances, we will feature specific information concerning:
  - **Pilot use cases** - reports/videos;
  - **Technical aspects** – results of project activities and progress in the context of core trust extensions and the design of the overarching Trust Assessment Framework;
  - **Contribution to Clusters and Marketplaces** – following events attended, collaboration with other projects (Section 4.1), webinars/workshops organized by CASTOR (Section 3.4.2.8);
  - **Standardization** – see opportunities reflected in CHAPTER 4;
  - **Exploitation** – see opportunities mentioned in CHAPTER 5;
  - **Other opportunities**: *Safer Internet Day* – February; *Cybersecurity Month* – October.

The posting frequency has an average of two posts/week.

The two social media channels feature the following **hashtags**, as appropriate, to maximize reach: #CASTORHorizon, #HorizonEurope, #CyberSecurity, #Trusted_path_routing, #NetworkSecurity, #TrustedCommunications, #Blockchain, #ComputeContinuum, #EdgeComputing, #QuantumAnealing, #Innovation, #ResearchExcellence, #5G, #6G, #NetworkOrchestration.

The following **handles (Table 2)** of the consortium partners are available. They were and will continue to be leveraged as part of the project's posting strategy.

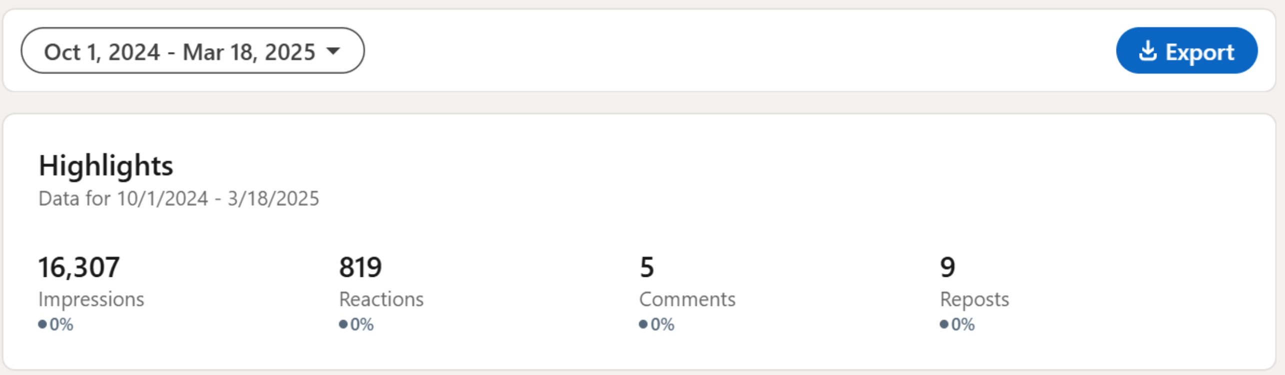
Table 2: Social Media Accounts of the Project Partners

Partner	LinkedIn Profile	X Profile
1. UBI	@UBITECH https://www.linkedin.com/company/ubitech/	@UBITECH_GR https://x.com/UBITECH_GR
1.1 QUBI	@QUBITECH - https://www.linkedin.com/company/q-ubitech	@Q_UBIT_TECH https://x.com/Q_Ubit_Tech
3. ORO	@Orange https://www.linkedin.com/company/orange/	NA

4. TUIASI	@Gheorghe Asachi Technical University of Iași https://www.linkedin.com/school/universitatea-tehnic%C4%83-%E2%80%9Egh.-asachi%E2%80%9D-din-ia%C8%99i/	NA
5. COLLINS	@Collins Aerospace https://www.linkedin.com/company/collins-aerospace	@CollinsAero https://x.com/collinsaero
6. ICCS	@I-SENSEGroup/ICCS https://www.linkedin.com/company/isensegroup/	@ISENSE_GROUP https://x.com/ISENSE_GROUP
7. SUITE5	@Suite5 Data Intelligence Solutions https://www.linkedin.com/company/suite5/	@suite5eu http://www.x.com/suite5eu
8. K3Y	@K3Y https://bg.linkedin.com/company/K3Y	@K3Y_BG http://www.x.com/K3Y_BG
9. WINGS	@WINGS ICT Solutions https://www.linkedin.com/company/wings-ict-solutions/	NA
10. UMU	@Universidad de Murcia https://www.linkedin.com/school/universidad-de-murcia/	@UMU https://x.com/UMU
11. FERON	@Feron Technologies P.C. https://gr.linkedin.com/company/feron-technologies	NA
12. CMS	@Commsignia https://www.linkedin.com/company/commsignia/	@Commsignia https://x.com/commsignia
13. UvA	@University of Amsterdam https://www.linkedin.com/school/university-of-amsterdam/	NA
14. D4P	@Digital for Planet https://www.linkedin.com/company/digitalforplanet/	NA

15. SURREY	@ University of Surrey https://www.linkedin.com/school/university-of-surrey/	NA
16. KENT	@ University of Kent https://www.linkedin.com/school/university-of-kent/ @ Institute of Cyber Security for Society at the University of Kent https://www.linkedin.com/company/icss-unikent/	NA

From October 2024 – March 2025, the LinkedIn page attracted 140 followers and generated over 16.300 organic impressions and 819 reactions. We will continue to grow the follower base and impressions, as per the above-mentioned posting topics and posting frequency.



Highlights

Data for 10/1/2024 - 3/18/2025

16,307	819	5	9
Impressions	Reactions	Comments	Reposts
●0%	●0%	●0%	●0%

Figure 9: LinkedIn Analytics

In light of recent developments surrounding the X platform and related actions across several EU countries and institutions, we are evaluating the potential closure of the CASTOR's X account and the establishment of a CASTOR presence on Mastodon. This matter has already been discussed with the Project Officer to ensure alignment, and we aim to reach a coordinated decision in the coming months.

3.4.2.4 Press Engagement

CASTOR's media relations strategy serves as another tool for communicating significant project achievements and milestones to media outlets and the broader public.

Each press release will include details about CASTOR's achievements, incorporating meaningful quotes from project partners, and will be distributed to a selected list of journalists from major media channels and relevant industry publications. A press release to mark the launch of the project was issued on October 21st 2024, via Prowly:

https://martel-innovate.prowly.com/358113-castor-project-launches-to-pave-the-way-for-trusted-communication-in-the-compute-continuum

A selected list of 63 journalists interested in cybersecurity and cloud computing, from several European countries, was created. While all are reached for general news, some of them will be contacted individually, to pitch stories related to the pilots, once these are implemented. More press releases are to be issued to drive awareness of the technical advancements of the project and the results of the Project Use Cases.

3.4.2.5 Blog Posts, Articles & White Papers

Several blog posts were published to date by the partners, to drive awareness about the launch of the project and the respective partner contribution. The Consortium developed the following publishing plan, to be implemented while the technical work behind the project progresses.

Table 3: List of Published and Planned Blog Posts

Partner	Topic	Timing	Links or estimated publishing date
D4P	Project launch	M1	https://digital4planet.org/introducing-the-castor-project/
UBI	Project launch	M1	https://ubitech.eu/ubitech-hosts-kick-off-meeting-for-the-castor-innovation-action-pioneering-the-future-of-trustworthy-computing-continuum/
K3Y	Project launch	M2	https://k3ylabs.com/blog/castor-kick-off-meeting/
UBI, SURREY	Attestation protocols	M9	Composability of Trustworthiness Evidence in Multiple Prover/Verifier Environment towards Trusted Path Routing
QUBI	Trusted Path Routing Optimisation	M12	Quantum-inspired Optical Simulators for combinatorial optimization problems
UKENT	Trust assessment	M15	Dynamic and federated trust assessment in the Traffic Engineering process
NVIDIA	Dynamic tracing	M18	Evidence Tracing of the Routing Infrastructure for Secure Runtime Attestation
COLLINS	Finite State Automation	M20	Finite State Machines for efficient trust analysis
COLLINS	Use case description	M23	Communicating data trustworthiness between disparate airspace surveillance domains
SUITE5	Blockchain technologies	M24	The CASTOR Blockchain Infrastructure

SURREY	Cryptographic primitives	M24	Trust Exposure Layer for privacy-preserving data sharing
ICCS, WINGS	Management and Orchestration	M24	Secure Orchestration using network- and trust-related metrics
TUIASI	Use case description	M25	Domain-to-domain trusted path routing for V2X applications
K3Y	Use case description	M26	Future-proof Next-Generation Unmanned Aerial Vehicles Communications Towards Critical Infrastructure Sustainability
UMU	Policy enforcement	M30	Secure intent-based networking focusing on policy enforcement
D4P	End of the project	M36	An overview article on the project development, outcomes, and exploitation opportunities

3.4.2.6 Videos

A YouTube channel dedicated to the project has been created to host all project-related videos: https://www.youtube.com/@CASTORhorizon

To date, CASTOR has produced five video vignettes, which have been promoted through social media channels to provide an overview of the project—its scope, objectives, and use cases. As the project progresses, more videos will be produced, particularly once the use cases are implemented, during participation in events, workshops, and the CASTOR Open Day. Furthermore, interviews will be conducted with our consortium experts working on the core technologies of risk assessment, trusted computing, crypto, and optimization.

Table 4: CASTOR Video Vignettes Produced to Date

Video vignette topic and YT link	LinkedIn post	X post
CASTOR Horizons's vision and mission	Link to post	Link to post
CASTOR Horizon's expected impact	Link to post	Link to post
CASTOR USE CASE N# 1	Link to post	Link to post
CASTOR USE CASE N# 2	Link to post	Link to post

CASTOR USE CASE N# 4	Link to post	Link to post

3.4.2.7 Promotional Materials

Upon participation to the previously mentioned events, will be promoted through leaflets, flyers, and/or brochures.

Figure 10 presents the CASTOR Horizon generic leaflet. Printable versions of these leaflets will be produced and shared with partners to distribute at the events they will attend.

The promotional materials will primarily be in English, with local language versions created if needed to ensure effective awareness among stakeholders and diverse relevant audiences.

The materials will combine clear text and visuals to convey essential project information. The design will be adaptable, allowing partners to tailor the materials if a more targeted version is required. All promotional materials will include the project logo, the EU flag, recognition of EC funding, and links to the CASTOR website and social media platforms.

Figure 10 CASTOR leaflet

3.4.2.8 Events & Workshops

CASTORS Horizon consortium attended and will continue to organize/attend a series of events to showcase the project's solutions and Use Cases to a broad audience. The project will focus on key activities such as workshops, open days, event presentations, and webinars.

3.4.2.8.1 Participation in External Events

During the first 6 months since the beginning of the project, the consortium partners participated in 5 events relevant to the scope of the project. All participations were and will continue to be promoted via the Events tab of the CASTOR Horizon website, as well as via the social media channels of the project.

Table 5: Participation in Events during the First 6 Months of the CASTOR Horizon Project

Name of event	Topic of the event	Consortium Member	Link with CASTOR	Target audience reached	Timing
Trusted Computing Group (TCG) Physical Meeting	Physical meeting of the TCG members discussing the progress of all open points in the various WGs, focusing on the implementation of the new specifications for decentralized Roots of Trust (such as TPM and DICE)	UBITECH	Presentation of the initial ideas towards the extension of the default remote attestation protocol to be able to cope with composite evidence originating from multiple devices.	Researchers, Engineers	October 2024, Athens, Greece
TPM.dev Online Webinar	TPM.dev is an open-source community aiming at the provision of novell designs and implementation for hardening CC applications workloads – with the support of underlying HW-based secure elements.	UBITECH	Presentation of the novel implicit attestation enablers implemented by UBITECH based on which the CASTOR trust extensions will be based.	Researchers, Engineers, Vendors, Policy Makers	January 2025[1]
UMU-NICT Workshop	1-day workshop meeting based on the MoU between UMU and National Institute of Information and Communications Technology (NICT)	UMU	Discussion carried on secure orchestration of service and the work ongoing in Internet Engineering Task Force (IETF) where researchers on	Researchers	March 7th 2025

[1] https://www.linkedin.com/posts/tpmdev_github-ubitechubitrust-activity-7272686000517115905-wUtE/

			NICT are involved		
CERTIFY Project First Infoday: Cybersecurity and IoT in Industry 5.0	Webinar	UMU and UBITECH	Attestation and secure management of devices as linked to the objectives of CASTOR activities	Industrial stakeholders	March 17th 2025
Workshop on Trustworthy AI	Workshop organized in the context of the CONNECT U project focusing on those core challenges that impact the wide-scale application of AI systems. Particular emphasis was given in the context of challenges towards fostering trustworthy and ethical use of AI in the context of 6g ecosystems	UBITECH	Thanassis Giannetsos (UBITECH) was invited into a panel talking on the use of AI towards secure orchestration of CC workloads. CASTOR was presented as one use case where AI can help towards the establishment of trusted path routes.	Researchers, Policy Makers, Engineers, Industrial Stakeholders	March 25th-26th, 2025

Participation in the following events is planned during the project:

Table 6: Planned Participation in Events Concerning CASTOR Horizon Project

Name of event	Topic of the event	Consortium Member	Link with CASTOR	Target audience reached	Timing
ITSWC	Intelligent Transportation Systems	CMS	Discussion on CASTOR trust extensions and how they can be used for accommodating the establishment of secure and	Researchers, Engineers, Industrial Stakeholders, Policy Makers	Annually (August 24-28, 2025)

			trustworthy CCAM environments		
5GAA	5G and Automotive	CMS, UBITECH	Participation in the TRUST4CAV discussions and panels on the finalization of the definition of the generic trust assessment methodology (Section 4.1.2)	Researchers, Engineers, Industrial Stakeholders, Policy Makers	Quarterly
ITS Europe/ ITS World / ITS Hellas	Intelligent Transportation Systems	ICCS	Participation in a roundtable discussion on privacy, trust and reputation management in Internet of Vehicles	Researchers, Engineers, Industrial Stakeholders, Policy Makers	October 2026
RTX SEATN - Systems Engineering & Architecture Technology Network symposium	Aerospace IT and Computing	Collins	CASTOR's aerospace use case	Commercial aerospace engineers, designers, decision-makers from one of the largest aerospace network providers in the world	Annually
EuCNC & 6G Summit	Networks & Communications	ICCS, ORO, Collins, UMU, UBITECH	Keynote talk on the trusted computing related activities of	Researchers, Engineers, Industrial Stakeholder	June 2026

			CASTOR and how these manifest the runtime monitoring of verifiable evidence based on which the trust assessment of the routing plane can be conducted	s, Policy Makers	
TCG Physical Members Meeting	Trusted Computing Extensions	UBITECH	Presentation of CASTOR's attestation enablers and primitives to the TPM Working Group. Discussion also on the overall CONNECT architecture with the TPM Automotive Working Group	Researchers, Engineers, Industrial Stakeholders, Policy Makers	June 2026
IEEE International Conference on Communications (ICC)	Communications	ICCS	Participation in a panel session on secure orchestration capabilities	Researchers, Engineers	May 2026
CompSys 2025	Dutch Computer Systems and Networks research	UvA	Participation in roundtable discussions on the SOTA on optimization techniques for	Researchers, Engineers, Industrial Stakeholders, Policy Makers	May 2025

			difficult to solve problems. CASTOR will be discussed as a use case due to the complexity of its design space of objectives and constraints that need to be met		
IEEE NetSoft 2025/Secsoft Workshop	IEEE International Conference on Network Softwarization	UMU	Connection to the orchestration aspects and the trust models for virtualization	Researchers and industrial partners	June 2025
USENIX Security	Systems research in all areas related to security and privacy	NVIDIA	Related to the runtime monitoring of devices	Academic and industrial researchers	August 2025
ESORICS European Symposium on Research in Computer Security	Computer and Network Security	FERON	Related to trust and risk assessment and cascading effects.	Academic and industrial researchers	Annually (every September)
ARES International Conference on Availability, Reliability and Security	Workshop on trust	FERON	Trust modelling, trust assessment, attestation.	Academic and industrial researchers	Annually (every August)

IEEE Vehicular Technologie Conference	Automotive technologies for communications	FERON	Automotive use case results	Academic and industrial researchers	Twice every year (Spring and Autumn)

3.4.2.8.2 *CASTOR Research Workshops*

Organization of numerous scientific workshops that will facilitate discussions between researchers, academia and industry on topics related to building trust and resilience in the Compute Continuum. CASTOR is envisioning to be affiliated with at least five (5) scientific workshops and has already taken the following actions towards the support of the following two workshops (further details on the outcomes will be documented in D7.2 [1]):

Table 7: CASTOR Envisioned Research Workshops

CASTOR Scientific Workshops
CASTOR aims to organize a scientific workshop in M18 as part of a well-established security conference. This affiliation will unlock great potential to the workshop's impact as it will be a great venue for CASTOR to disseminate and debate with the scientific communities around the key topics of the project. Specifically, the plan is to issue a call of papers around important CASTOR technologies (e.g., Trusted Path Routing, Trusted Computing, Remote Attestation and Multi-Objective Optimization) that will set the scene for fruitful discussions around these timely topics.
The CASTOR project aims to revamp the CYSARM Workshop (Workshop on Cyber-Security Arms Race), with the aim to organize it as a co-located event with the ESORICS 2026 conference. Given the complexity of the cybersecurity landscape, the goal of the 4th edition 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.
As part of its 2nd year dissemination activities, CASTOR envisions to organize a research workshop focusing on the advancements and challenges of trusted path routing concepts. The aim of this workshop is to assemble a small cohort of invited experts both from academia and industry organizations. The main outcome shall be the specification of a roadmap to address the major showstoppers and blocking points identified by the experts, enabling progress towards the establishment of zero-trust, and sub-zero trust across the compute continuum.
CASTOR will organize a final event along with the final review of the project in M36, where the focus will be placed on the demonstration of the key technology artifacts in the context of the envisioned use cases. The participants of this project will be a mix of engineers, researchers, policy experts, as well as members of the CASTOR external advisory board. In addition, CASTOR will encourage participation from standardization organizations as well, with the aim to showcase the CASTOR outcomes with the aim to impact and shape the future of new standardization activities around the topic of trusted path routing.

3.4.2.8.3 CASTOR Webinar and Trainings

Several training activities will be organized during the Y2 and Y3 of the project, addressing both internal and external audiences. These activities will be part of CASTOR's Open-Source Development (Section 5.2) strategy and will aim to provide all technical details behind the implementation of CASTOR key exploitable results. The endmost goal is to engage the scientific and industrial community to interact with CASTOR open-source solutions. Tailored webinars will be organized in the context of the key technological areas of CASTOR: **Trust Assessment, Trust Device Interfaces and Secure Communication Protocol, Optimization, Secure Traffic Engineering Process.**

3.4.2.8.4 CASTOR Target Venues for Scientific Publications

During the CASTOR project, the consortium aims to produce several scientific publications that contribute to the advancement of security assurance in the TELCO sector. As illustrated in **Figure 2**, it becomes obvious that CASTOR's framework is inherently multidisciplinary. Consequently, there are multiple and diverse scientific fora where CASTOR aims to share the research findings with the scientific community. These include high-impact **conferences** such as the **ESORICS (European Symposium on Research in Computer Security)**, **ARES (International Conference on Availability, Reliability, and Security)**, and **USENIX Security**. Additionally, events like **EuCNC & 6G Summit** and the **RAID (International Symposium on Research in Attacks, Intrusions, and Defences)** will provide opportunities for sharing findings related to network security, system reliability, and next-generation communication technologies. Finally, peer-reviewed **journals** such as **IEEE Internet of Things (IoT)** and **IEEE Transactions on Dependable and Secure Computing** will serve as venues for disseminating comprehensive, peer-reviewed publications that contribute to the ongoing open questions and academic dialogue in these domains. CASTOR's publications will be openly accessible and hosted on Zenodo, ensuring broad dissemination and long-term availability within the research community. To achieve this goal, the following Zenodo account has been opened: https://zenodo.org/communities/castorheu/

3.4.2.9 Dissemination & Communication Targets

During the proposal phase of CASTOR, an initial communication and dissemination and exploitation plan was already set up, stating different audiences (listed in Section 3.3), what the objective of reaching the audience would be and what the impact of reaching them will be. This plan is the basis for this deliverable and can be found in Section 2.2 of the DoA (Description of Action).

As can be seen, CASTOR's dissemination and communication activities are overarching throughout the whole duration of the project and aim to ensure a broad promotion and effective showcasing of the developed concepts, technologies, use cases, and results. In terms of communication and marketing, this ambition translates into the following main objectives:

- **Ensure broad visibility and raise awareness** about CASTOR, spreading knowledge about the project and its results, establishing a distinctive and recognizable identity that will support marketing efforts;
- **Reach, stimulate, and engage a critical mass of relevant stakeholders** to ensure that the results of the project are effectively showcased, leading to validation, improvement, and possibly further adoption of the developed technologies and concepts, especially toward the establishment of zero-trust architectures in the CC that can foster the deployment, operation, and lifecycle management of mixed-criticality services over trusted infrastructures;
- **Facilitate exploitation of project outcomes** and promote the development of innovative solutions based on the CASTOR technologies and architectures;
- **Foster impactful contribution** to relevant standardization bodies as appropriate and relevant to planned exploitation plans and the project's outcomes;
- **Ensure close coordination with relevant H2020 projects and EC bodies** while establishing liaisons with related initiatives in research and innovation domains such as IETF, ETSI, C2C-CC, TCG, AIOTI, etc. (more information can be found in CHAPTER 4).

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

Table 8: Communication and Dissemination KPIs

Activities/channels	KPIs
Project website	> 1000 unique visitors, > 200 registrants, > 350 blog interactions
Audio and Video Material	1 Promo + 1/Pilot + 1 Impact + 2-4 interviews or podcast episodes
Social Media (LinkedIn, X)	> 800 posts, > 1000 followers, > 5000 interactions
Press releases, blog posts, whitepapers	> 4/per year, > 1000 people
Publication of scientific/conference papers	> 4 Journal articles > 15 Conference papers
Interaction with policy makers	> 6 synergies established
Digital liaisons with related projects	Workshops organized (3) + attended (> 5), > 500 visitors, 10 speakers 5 posts in EC systems 10 project synergies
Non-scientific publications	> 5 Industry Magazines > 6 Conferences, 1 exhibition, 2 demos
Standardization associations	> 4 Networking, > 3 Standards Orgs
On-site pilot demos/ workshops	> 1 demo per pilot, > 1 workshop per pilot, > 20 attendees each
Online and/or F2F Training/Webinars	> 2 webinar/trainings, > 50 attendees

CASTOR Day	> 80-100 participants

We have to highlight that all listed KPIs will be monitored and adjusted throughout the duration of the project considering also the ongoing activities of the technical work packages that feed the dissemination material. Furthermore, these have also been associated with risks that have been identified and can potentially affect the achievement of the envisioned target values. For instance, at the time of writing the deliverable, the project partners are debating the possible discontinuation of CASTOR's presence on the X social media platform. This strategic move, while might hurt the KPI as it pertains to the number of followers and expected interactions (due to the popularity of the platform), is been proposed by many of the project partners that have expressed concerns about X’s alignment with fundamental EU principles on trust, security, and inclusion; and in particular, data privacy and user autonomy. In this case, CASTOR will redirect its focus towards other platforms and communication channels prioritizing user-centric designs of its material towards building a strong community that can interact with and ensure the wide outreach of the project results.

3.5 CASTOR ADVISORY BOARD

For the innovation developed within the CASTOR project to have any 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 CASTOR project foresees several ways to reach the industry and in particular, the target audience listed in Section 3.3. Whereas the main channel is the attendance of trade fairs (focusing on events related to the technological areas of CASTOR such as the EUCNC and 6G Summit[2] covering topics related to secure networking and/or the application areas of the envisioned use cases including the well-established EUCAD[3] and ESCAR[4] event focusing on Embedded Security in Connected Cars), the industry is also reached by attending conferences, and workshops and further by publishing newsletters and keeping the website up to date. In this context, the CASTOR consortium has also initiated the process for the establishment of an Advisory Board with outside experts in order to provide valuable feedback on the core research artifacts of the project from both an academic, scientific, and industrial standpoint.

The CASTOR Advisory Board is a group of experts who will meet periodically with the CASTOR consortium throughout the project. They will provide technical guidance, input, and feedback on the CASTOR technology roadmap, advise on links with relevant interest groups (outside CASTOR), propose and assist potential interactions of the project with other projects, initiatives, activities and standardization bodies. In addition, the Advisory Board will critically evaluate project proceedings and the technological and scientific outcomes, give feedback to the dissemination and clustering exercises, and thus provide an external review of project actions. The AB members will document their experiences when it comes to the developments of the project and their feedback will be fed into all modelling actions and into the improvement of the final outcomes and deliverables.

In this direction, the Advisory Board will consist of a partner-nominated group of external senior academic, business, industry and standards-associated advisors who will assist in reviewing the project’s development and progress from the very first steps of the project until its completion. During the construction of the AB, particular focus will be given on approaching **experts with exposure on the international cybersecurity regulations and standards covering both the core technology**

[2] https://www.eucnc.eu/

[3] https://www.smart-systems-integration.org/event/eucad-2025

[4] There are various events organized throughout Europe, USA and Asia. For more information please refer to https://www.escar.info/

of trusted path routing (working on other initiatives and protocols such as the SCION Protocol[5] (Scalability, Control and Isolation on Next-Generation Networks) that has already been started to be deployed in production network including the Swiss Secure Finance Networks) **but also on the other core dimensions of trusted computing and distributed orchestration and optimization**. This is of paramount importance so as to make sure that not only CASTOR is aligned with the latest security specifications but also participate (and possibly contributing) in the discussions towards the design of new cybersecurity management and traffic engineering processes enabling the long-term resilience of CC application workloads. Prominent regulatory and standards bodies include the ISO 26262 on functional safety [4]; ISO/SAE 21434 on cyber-security engineering [5]; and the UNECE (United Nations Regulation) that recently published the WP.29 Cybersecurity and Cybersecurity Management System (CSMS) detailing the deployment model of the Public Key Infrastructure (PKI) needed for supporting the security and privacy of the entire lifecycle of far-edge devices such as road vehicles [6]. In this direction, CASTOR has already established relationships with international experts and routing vendors dealing with the enrichment of path establishment with inherent trust and trustworthiness capabilities (as documented in Section 4.2 where CASTOR has already established a long liaison and participates in numerous IETF activities related to network attestation and trusted path routing, and Section 4.1.5 where the consortium has already sketches a detailed map of those ISO activities and working groups that focus on related activities in embodying trust and trustworthiness for the establishment of secure dataspaces) and will continue to try to liaise with organizations participating in the specification of such regulations to consolidate their findings and strengthen the international cooperation in trusted path routing.

Given the above, the consortium will liaise with numerous external, independent experts at different disciplines that will cover the following research/technology axes and impact categories of the CASTOR project:

- Routing Vendors and Telecommunication Network Providers in the overall supply chain;
- Cyber-Security and Risk Management in the target application domains (including automotive as one of the most safety-critical use cases);
- Mobile Edge Computing (MEC) Architecture;
- Trusted Computing Technologies and Hardware-Software Remote Attestation;
- Lightweight Cryptography;
- Security and Functional Safety of Vertical Application Domains;
- Certifiability of Automotive Security as required by regulatory organizations such as ISO, UNECE, ENISA, etc.

Currently, the CASTOR consortium has initiated the process of inviting experts, capturing the entire spectrum of the aforementioned capabilities and all the core technologies to be investigated:

International Expert Committee on Trusted Path Routing comprising Eric Voit & Chennakesava Reddy Gaddam (CISCO) and Prof. Adrian Perrig & Prof. David Basin (ETH). Mr. Voit and Mr. Gaddam are the two main contributors of the main IETF specification on trusted path routing and the designers of the current scheme mainly focus on intra-domain (static) TPE. Their consultation will prove valuable in both allowing CASTOR to push its findings as part of the next IETF specification and also on the standalone testing of CASTOR's novel TrustGrid extensions in CISCO-related network elements. Prof. Perrig and Prof. Basin are experts on the SCION path-aware routing architecture which defines the need for more path establishment based on the service trust and

[5] https://scion-architecture.net/

operational requirements. CASTOR's intra- and inter-domain secure path establishment extensions will be compared and also extended to support the SCION model.

International Expert Committee on Trusted Computing comprising Chris Fenner (Google) and Nick Grobelny (Dell). Both are members of the Trusted Computing Group (TCG) - Mr. Fenner been the Head of the TPM WG whereas Mr. Grobelny is the Head of the Cyber Resilience WG. Their engagement in the project's activities will allow for CASTOR's truste extensions, for enabling trusted I/O virtualization, to be considered as part of future releases of the standardized Trusted Software Stack (TSS) enabling the secure interaction with an underlying Trusted Platform Module (TPM) as the secure element.

International Expert Committee on Secure Networking comprising Diego Lopez (TELEFONICA) and Houda Labiod (HUAWEI). Dr. Lopez is one of the core participants in many of the IETF activities targeted by CASTOR and has been working for many years on secure networking with a particular emphasis on how to establish trustworthy service-graph chains. Dr. Labiod is a core member of the Network Attestation WG in IETF primarily driving the activities in the context of remote attestation when multiple provers and multiple verifiers are present.

Furthermore, an additional International Committee has been assembled with experts on the various application domains where CASTOR will be evaluated.

CHAPTER 4 RELEVANT INITIATIVES & STANDARDIZATION

4.1 LIAISON WITH RELEVANT INITIATIVES

An important part of the dissemination activities includes the build-up of liaison with other projects and initiatives relevant to the fields of CASTOR. Through this, CASTOR will promote stakeholder clustering, focus on targeted engagement, and perform cross-dissemination activities. The aim is to disseminate the project's outcomes, ensure the exchange of knowledge and best practices to the mutual benefit of all parties involved, and increase the visibility of CASTOR within the market and potential future clients for its solutions.

Under this approach, CASTOR will seek to develop liaison and collaborations with:

- Related projects and research initiatives.
- Industrial associations.
- Appropriate standardization bodies and Working groups.

An initial list of receivers is the already established and rich portfolio of connections with related projects and initiatives by the members of the consortium. The strong and multi-discipline partnership of CASTOR's consortium poses a wide network of synergies that will be exploited to engage with several market players and domain stakeholders. This list will further grow with the addition of relevant organizations and peers that will be identified during the project's lifetime. In this direction, CASTOR has already established liaisons with numerous ongoing activities that foster research on how to establish trust and trustworthiness in safety-critical applications but also with all recently started project initiatives fostering the deployment and operation of secure CC workloads (funded under the same call cluster as CASTOR project). A detailed list is put forth in Table 9.

It is worth highlighting the following activities: CASTOR has already established a liaison with the recently started MIRANDA EU project ("*An Adaptive Digital Twin for Agile Services over the Compute Continuum*") and INTACT EU project ("*Integrated Software Toolbox for Secure IoT-Cloud Computing*") focusing on the construction of a secure and agile Compute Continuum. Both initiatives foster the development of a Digital Twin that can be used for emulating the deployed topology of CC workloads, thus, allowing for the dynamic testing and validation of the functional correctness of application configurations and protocols prior to their actual deployment. This, in turn, allows for threat hunting and the identification of the optimal reaction strategies in case of risk indicators. CASTOR can greatly benefit from such initiatives towards further stipulating the dynamic trust assessment capabilities of the target CC through such DT deployments: Trust assessment of mirrored topologies can allow for the recommendation of optimal (network-aware and trust-aware) path decisions in anticipation to various service provider requests. Discussions on holding common events and webinars have already commenced and scheduled.

Continuing on the same path, CASTOR has also established a liaison with ongoing project activities that manifest the same type of trust assessment methodologies in safety-critical application domains. For instance, CASTOR is already collaborating with the numerous projects in the automotive domain, and in particular the PODIUM EU project ("*PDI Connectivity and Cooperation Enablers Building Trust and Sustainability in CCAM*") and CONNECT EU project ("*Continuous and Effective Trust Management in Next-Generation CCAM*") towards building trust and sustainability for CCAM. Both projects try to **address the challenge of trustworthy data sharing** in Vehicle-to-Everything infrastructures (linked also with low latency, cooperation, data management, security and resilience) leveraging the use of **Subjective Logic** as also foreseen in CASTOR. **The vision is that combining connectivity, cooperative systems and automation will enable automated and fully orchestrated vehicle manoeuvres, thus, bringing us closer to the overall CCAM vision**. CASTOR and CONNECT, PODIUM share a subset of use cases (especially in the context of **Slow Moving Traffic Detection**) and discussions are already ongoing to investigate possibilities for common activities on setting up and investigating shared experiments. While PODIUM, for instance, investigates the use of Subjective Logic (SL) for enabling vehicles to self-assess their internal perception system, CASTOR leverages SL to assist the establishment of secure data sharing/forwarding paths over infrastructure elements and neighbouring vehicles that can demonstrate the Required level of Trust. The endmost goal is to ensure that the complementary results of both projects can be implemented, capitalized and evaluated in large-scale proof of concept environments.

Table 9: CASTOR Liaison with other EU Horizon Projects

Partner project	Scope of the partner project	Synergies	Involved partners
INTACT	Cybersecurity across the compute continuum via Digital Twins	D4P is constantly driving synergies for Communication and Dissemination via sharing the opportunities across the social media platforms of the two projects – i.e. https://www.linkedin.com/feed/update/urn:li:activity:7287828625842708480	UBITECH D4P K3Y
MIRANDA	An Adaptive Digital Twin for Agile Services over the Compute Continuum	MIRANDA fosters the development of a Digital Twin that can be used for emulating the deployed topology of CC workloads, thus, allowing for the dynamic testing and validation of the functional correctness of application configurations and protocols prior to their actual deployment. CASTOR can greatly benefit from such initiatives towards further stipulating the dynamic trust assessment capabilities of the target CC through such DT deployments: **Trust assessment of mirrored topologies can allow for the recommendation of optimal (network-aware and trust-aware) path decisions in anticipation to various service provider requests**.	UBITECH
CONNECT	Continuous and Effective Trust Management in next-generation CCAM	UBITECH and ICCS participate in the design and development of a dynamic trust management framework centred on zero-trust. Part of the contributions involve the development of attestation enablers acting as trust sources for the assessment as well as the instantiation of the trust assessment framework in environments in edge-to-far-edge environments. CASTOR aims to advance the work provided in CONNECT, especially in the federation of trust assessment agents as part of the overall traffic engineering process both in intra-domain (device-level vs orchestration-level agents) and inter-domain (in the context of establishing a federation of orchestrators) settings.	ICCS UBITECH

REWIRE	Continuous security assessment of interconnected IoT devices under zero-trust architectures	Collins and UBITECH are contributing to formally verified attestation solutions in order to securely enable remote software updates of industrial use-case scenarios. Similar solutions can be used as part of CASTOR in order to authenticate users and increase trust score of interconnected CASTOR devices	COLLINS UBITECH
ENVELOPE	Tailored 5G interfaces and dynamic network (re-) configuration to enhance CCAM vertical services	The CASTOR trusted-path routing concept (with emphasis on the automotive use-case results) to be communicated with the ENVELOPE consortium exploring interest/opportunities to accommodate related data through the ENVELOPE interfaces. Expected to pursue liaison activities by the time some CASTOR (preliminary) results are available	ICCS CMS
CERTIFY	Management of the lifecycle of security of devices	CASTOR will take into account the solutions provided by CERTIFY on attestation and monitoring of devices and how they are CASTORed with the domain manager concepts for integration of status evidence	UBITECH COLLINS
ENTRUST	Dynamic and continuous security assessment of connected medical devices (CMDs) throughout their lifecycle	Both UMU and UBITECH contribute to the continuous trust assessment and certification assurances of interconnected medical devices throughout their lifecycle. CASTOR will take into account the solutions and frameworks that have been specified in ENTRUST for the dynamic trust assessment of rapidly evolving trust networks (like the one of the smart ambulance domain) while being able to cope with contradicting evidence and diverse trust requirements. In addition, CASTOR aims to advance the efforts on the harmonization of the attestation enablers that need to be deployed in a vendor-agnostic manner and, eventually, the certification of network elements in the context of trusted path routing establishment.	UMU UBITECH
HEISINGBERG	Realization of a Spatial Quantum Optical Annealer for Spin Hamiltonians	CASTOR will exploit the advancements of the HEISINGBERG project towards the development of a Spatial Photonic Ising Machine capable of addressing real-life optimization problems	UBITECH QUBITEC H

It becomes evident that the establishment of trustworthy CC workloads is a crucial factor that can unlock previously siloed application domains. This is further evident with the numerous industrial associations that also focus on the same set of questions and with whom CASTOR also foresees to establish strong partnerships (listed in Table 10). This list may further grow during the lifetime of the project depending on the involvement of CASTOR representatives. CASTOR will aim at participating in the associations with CASTOR partners that are members with the objective of contributing with project results and working on various specification activities related to the key objectives of the trusted path routing. This will make the project's work visible to the membership of the associations and make them part of the associations' publications which will further raise the awareness of the CASTOR work.

Standardisation organisations and involved CONNECT partners are listed in Table 12. The list is comprehensive and covers the technical areas in which CASTOR works comprehensively. CASTOR will adhere to existing standards and specifications; gaps and shortcomings may be found in the documents which will lead to feedback (e.g., change requests) to the SDOs that produced them. Furthermore, CASTOR will actively promote project results by participation of its partners in the SDO activities. This will include the presentation of the CASTOR work in standardisation workshops and by direct work in relevant working groups with the objective of contributing CASTOR results to existing and new standardisation working items (as the ones that are already ongoing with the IETF Working Groups (described in Table 12) and 5GAA Association as documented in Section 4.1.2). It should be noted that at the time of writing the present deliverable, CASTOR has already initiated the activities for establishing two new initiatives in the context of IETF (at the stage of BOF proposals on activities related to "*Remote Attestation Capabilities for Multiple Provers, Multiple Verifier Architectures*" as well as on "*Harmonized Policy Language for Dynamic Security Control Enforcement*"). Furthermore, it had already contributed with presenting CASTOR as a possible use case in the context of IETF Network Attestation (NASR) activities.

The 5G Infrastructure Public Private Partnership (5G PPP, https://5g-ppp.eu/) is a joint initiative between the European Commission and European ICT industry (ICT manufacturers, telecommunications operators, service providers, SMEs and researcher Institutions). The 6G Smart Networks and Services Industry Association (6G-IA, https://6g-ia.eu/) represents the private side where in 5G-PPP, the European Commission represents the public side. Partners in Horizon Europe projects are encouraged to join the working groups to feed in their project results which makes it an ideal forum to liaise with other projects also participating in the different WGs.

Overall, WGs should be followed by the CASTOR partners to identify partners for collaborations. UMU, for example, is member of the Pre-Standardisation WG which identifies standardisation and regulatory bodies to align with e.g. ETSI, 3GPP, IEEE and other relevant standards bodies; UMU will (and has already in Q4 2022) contribute with CASTOR standardisation results to the quarterly SDO impact reports.

4.1.1 Networking Domain Associations and Initiatives

CASTOR is in the position to contribute to various technical specifications and initiatives on cyber-security and trust in the traffic engineering process due to the novelty of its solution, as well as on the fact that it tackles a domain that is currently under investigation for overcoming the security hurdles that will enable higher levels of trust in the service deployment and operation. Its envisioned security architecture will provide a flexible trust model that is applicable in various networking domains. Apart from the envisioned participation and contribution to various standardization bodies (detailed in Table 12), CASTOR aspires to also contribute to a series of open-source communities, which are highlighted below:

Table 10: CASTOR Technology-Related Associations and Initiatives

Secure Networking Industry Associations

Global Semiconductor Alliance	GSA Trusted IoT Automotive Ecosystem Security (TIES) is a collaborative group of companies in the telecommunication value chain focusing on promoting use cases and end-to-end solutions that minimize risks. They have extended work on secure "Chip-to-Cloud" assurance solutions for enabling trustworthy and resilient safety-critical IoT-to-Cloud services such as autonomous driving, connected cars, shared mobility, intersection management, collision avoidance, etc. CASTOR envisions to contribute to the current specifications of how **trusted components can be deployed in far-edge devices acting as a Root-of-Trust for enabling the establishment of trust relationships and trust calculations in next-generation "Systems-of-Systems"**. *UBITECH is already a member of GSA TIES*.
Car-2-Car Consortium (C2C-CC)	C2C-CC is the influential decision support forum for the European C-ITS industry and standardization. It develops technical specifications for standards. CASTOR's V2X related activities, including the planning and implementation of V2X use cases follow C2C requirements and recommendations. CASTOR's use case validation results and experiences will be presented and discussed in the corresponding C2C working group (WG CG-SEC), occasionally. *COMSIGNIA and TUIASI are members of the C2C-CC*.
Open Networking Forum (ONF)	CASTOR can contribute to ONF by sharing its outputs in cybersecurity for Software-Defined Networking (SDN) and traffic engineering. CASTOR can assist in enhancing the security frameworks of SDN environments, by providing its flexible trust model and security architecture. Additionally, CASTOR's activities in threat intelligence and forecasting could contribute valuable insights to ONF's ongoing initiatives in improving network automation and resilience.
ETSI OSG Open Source MANO (OSM)	An open-source initiative whose objective is to create a production-quality NFV orchestrator based on open-source code that should become a reference implementation of the MANO stack. CASTOR aspires to closely monitor the developments of the OSM and contribute based upon the advancements of the development of the distributed attestation-enabled CPS orchestration for heterogeneous and high-density edge devices, leveraging the root of trust capabilities of the CASTOR composable (remote) attestation services and providing security and trust features at all levels of the VNF stack.
ETSI SDG-OSL (Open Slice)	The ETSI Software Development Group for OpenSlice (SDG OSL) is developing an open-source service-based Operations Support System (OSS) to deliver Network as a Service (NaaS). Either UMU and UBITECH are member of the OSL Working Group and they envision to present the results of CASTOR and how the provided trust path routing establishment mechanisms can enable the deployment of secure NaaS solutions. The endmost goal is to

	investigate whether these CASTOR trust extensions can be considered as part of the future item of the SDG-OSL. Furthermore, ETSI OSL is organizing every year “hackathons” as a means that allows the community to test the security of their solutions against pre-defined security test cases. CASTOR plans to participate in such events for stress-testing the resilience of its security controls and trust extensions.
IEEE SDN	Abroad-based collaborative project focused on Software Defined Networks and Network Function Virtualization (NFV). Providing contributions to IEEE NFV regarding the dynamic resource allocation mechanisms that are going to be applied, exploiting the CASTOR collective threat intelligence analysis and forecasting engine.
CYBER	The results of the CASTOR project can contribute to the standardization efforts of TC CYBER in a variety of cyber-security areas. These areas are Intrusion Detection Systems, Physically Unclonable Functions-based Authentication, Threat Modelling and Risk Assessment, Cyber Threat Intelligence sharing, DLT and Smart Contracts-based Trust Management, Self-Sovereign Identity-based Identity Management, Trusted Execution Environments. CASTOR will explore also the possibilities of collaboration presenting results on the periodic meeting of the TC-CYBER.
3GPP	3GPP has been working on the concept of trustworthiness as one of the key components of future mobile networks, particularly in the areas of network function virtualization (NFV), attestation, and slice isolation. Reports such as 3GPP TR 33.848 focus on establishing trust domains, enforcing continuous attestation, and securing NFV infrastructures against threats, while ongoing 6G studies in TR 22.870 explore broader trust and security requirements for next-generation networks. CASTOR is perfectly aligned with these developments by introducing dynamic trust quantification, policy-driven trust enforcement, and multi-domain trust interoperability. With continuous attestation, trust-based routing with versatility, and federated trust models, CASTOR can contribute to 3GPP SA1 and SA3 in the designing of a robust trust architecture for high-assurance and resilient 6G networks.
ECSO	The European Cyber Security Organization (ECSO) is a cross-sectoral organization that contributes to developing cybersecurity communities and building the European cybersecurity ecosystem. In that sense the work of CASTOR is related to the activities on WG6 related to the SRIA and Cyber Security Technologies, where CASTOR can contribute to promote the vision and impact of the solutions being designed for the improvement of the European cybersecurity market. UMU and other partners are members and are active on WG6.

4.1.2 5GAA

The 5G Automotive Association (5GAA, https://5gaa.org/) is a global, cross-industry organisation of companies from the automotive, technology, and telecommunications industries (ICT), working together to develop end-to-end solutions for future mobility and transportation services. The main essence of 5GAA work is to bring together two main categories of stakeholders: First, telecommunication companies (like operators, neutral hosts, network technology providers, chip makers, etc.) that are providing connectivity and networking systems, devices and technologies. Second, automotive players (like vehicle OEM manufacturers, OEM suppliers, system integrators, etc.) that work on vehicle platforms, hardware and software solutions. 5GAA has 119 industry members, including automotive manufacturers, tier-1 suppliers, chipset/communication system providers, mobile operators and infrastructure vendors.

5G Automotive Association (5GAA) has been working on defining trust assessment methodologies for the CCAM domain, partially based on the results of the EU Project CONNECT. Through its **Trust4AUTO and Trust4CAV Work Items** (UBITECH is a core member of these activities that have already culminated in white papers [9] on how trust in C-ITS becomes a crucial factor as we are moving towards more decentralized architectures and the integration of Multi-Access Edge Computing (MEC) capabilities), 5GAA has defined a structured process for evaluating trust in connected and automated vehicles (CAVs). This work is **currently being elevated to a generic trust assessment methodology, within Trust4CAV WI, defining how trust values are computed, dynamically updated and integrated in decision-making for multi-agent systems**. Trust4CAV is expected to officially publish its methodology by April 2025 based on CASTOR's harmonized trust assessment methodology leveraging evidence-based theory. In essence, CASTOR is working on the definition of a generic methodology that can allow for the calculation of ATL and RTL values considering the same dimensions, thus, allowing for their efficient, real-time comparison for accurate trust-aware decision making. CASTOR will further extend this methodology towards the Compute Continuum (CC) domain. The legacy from Trust4CAV in CCAM provides CASTOR with a validated and tested trust quantification model based on subjective logic, which will be further refined to handle the unique challenges of multi-domain, cross-administrative trust management in the CC. In this way CASTOR has the opportunity elevate trust assessment to a universal methodology, ensuring scalability, interoperability, and real-world applicability in highly dynamic and federated environments.

4.1.3 W3C: Work on Verifiable Credentials and Data Models v2.0

Work from UMU is aligned with the Verifiable Credentials Data Model v2.0 that was released in April 2024 towards the establishment of Self-Sovereign Identity Management ecosystems. CASTOR aims to leverage these type of credential encodings as assertions to the trustworthiness of a (routing) device state**,** maintaining interoperability with existing initiatives while extending the use of the W3C attribute structures for disclosing identity & device status attribute assertions. In these cases, **CASTOR aims to use advanced cryptographic techniques such as Attribute-Based (Signed) Encryption or Zero-Knowledge proofs**. To achieve transparent interoperability, new signature suites for treating the VC formats are created. The implementation of these suites has been carried out considering the JSON-LD syntax for the W3C VC data-model, although these could be based on JWTs.

However, the IETF work on Verifiable Credentials is being focused on JWTs as a syntax for the representation of the Verifiable Credential model, and particularly a specific realization that provides some privacy characteristics known as Selective-Disclosure JWTs (SD-JWT-based Verifiable Credentials (SD-JWT VC)). This document was published by the Verifiable Credentials WG as a Candidate Recommendation Draft using the Recommendation track. We remark that the use of SD-JWTs is conceptually complementary to the use of the advanced cryptographic solutions proposed in CASTOR, being alternatives to instantiating the W3C VC data model and its flows. The WG is actively seeking implementation feedback for this specification, to which CASTOR partners such as UMU may contribute. This work will be related to the privacy identity management and the integration on the verifiable credential's schemas, particularly providing an overview on how to achieve flexible solutions that cover different needs.

4.1.4 Open-Source Communities

The ECLIPSE foundation has transferred its headquarters to Europe in order to address the needs for open source in Europe. In particular, ECLIPSE is a partner of the OpenContinuum support action that will support the various European research projects in creating impactful open-source projects. To this end, ECLIPSE, with the help of UBITECH has defined an Open-Source Development plan guidance that is adapted to research project and that will be considered by CASTOR in its own open-source project.

A key project related to the Eclipse Foundation is CyberNEMO, CyberNEMO's approach to open-source development aligns with CASTOR's objectives in trusted path routing and secure data exchange within the Compute Continuum. By leveraging its integration with the Eclipse Foundation, CyberNEMO ensures that its cybersecurity and trust mechanisms are widely accessible and continuously maintained. This open-source framework incorporates secure and trustworthy communication and data transactions via inter-and multi-domain trusted path routing across the Compute Continuum in accordance with the SSLAs (intend/guarantee agreements). CASTOR can contribute by aligning with CyberNEMO to support the development of interoperable security architectures, fostering trust-aware communication and data transactions in Compute Continuum.

Further the outcome of CASTOR in terms of secure data exchange building block in the continuum could be of interest in future data space initiatives (GAIA-X, IDSA CASTORors) and coordination will be sought to identify synergies, with the support of UKENT. Project results will be in alignment with the IDSA and the secure extension of the currently standardized IDS Connector. Also, the project results will contribute to the GAIA-X Trust & Federated Identity initiative in order to foster the vision of a federated and trusted data space ecosystem by making sure that usage control policies can be bound to the trust characteristics of the requesting actors. Through the contribution and integrations to GAIA-X Framework and standardized IDS connectors, CASTOR will support a complete solution capable of establishing trusted communications among industry participants and supporting the creation of (secure-access) data management lakes.

4.1.5 Building Trust and Resilience in Next-Generation Networking & Dataspaces

The following activities in standardization will also be taken into consideration by CASTOR for **enabling trustworthiness capabilities to be engrained in the intra- and inter-domain communication; i.e., between dataspaces**. The consortium has already performed a rather detailed profiling of all ongoing **ISO activities (Figure 10) with which CASTOR will aim to establish a liaison**. The endmost goal is to align the trust architecture and model to be constructed in CASTOR with the latest activities and trust considerations towards the construction of secure and harmonized dataspaces: Dataspaces constitute a complex multi-vendor, multi-supplier, and multi-stakeholder ecosystem lacking a central entity that implemented system-wide security assurances or accepts full liability if things go wrong. As a result, this brings to the surface the issue of mutual trust between stakeholders meaning that we cannot make assumptions about the trustworthiness of participating entities and we have to move to the discussion of what is needed to prove that an actor is trusted or not. Several activities are currently ongoing in ISO towards the creation and adoption of a generic trust model defining the properties that need to be exhibited by the various actors for achieving specific Levels of Assurance.

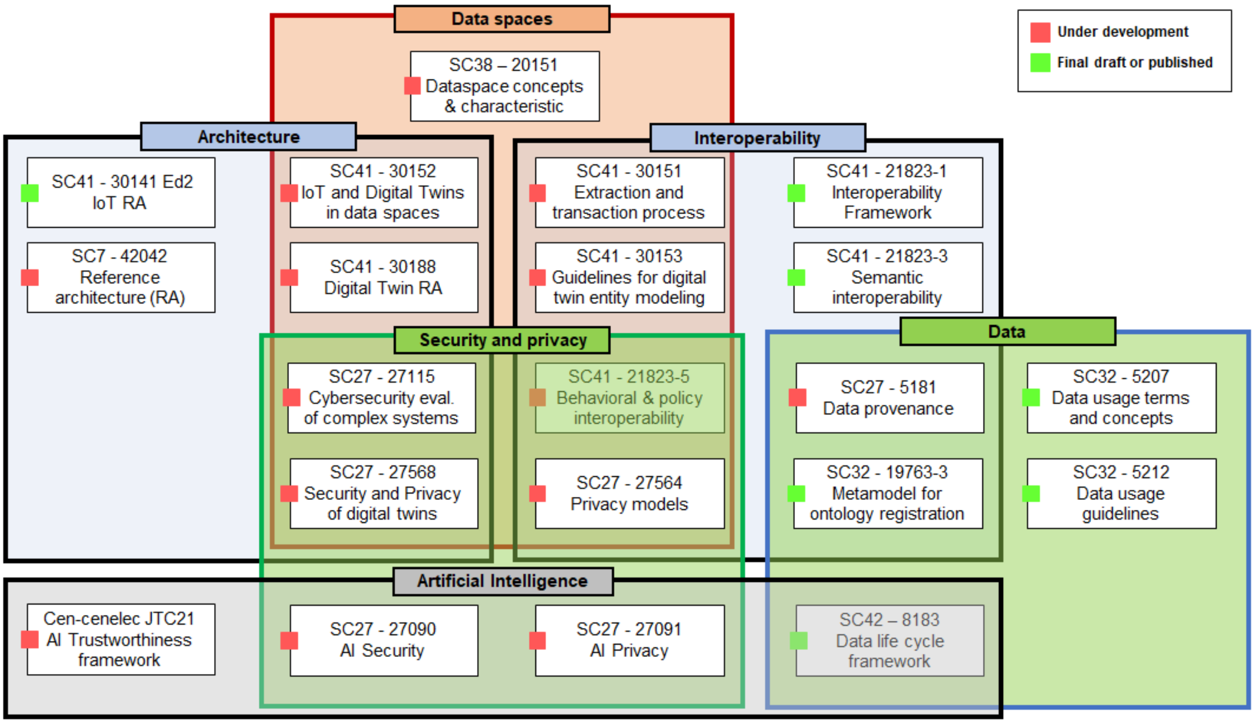

Data spaces
SC38 – 20151 Dataspace concepts & characteristic
Under development
Final draft or published
Architecture
Interoperability
SC41 - 30141 Ed2 IoT RA
SC7 - 42042 Reference architecture (RA)
SC41 - 30152 IoT and Digital Twins in data spaces
SC41 - 30188 Digital Twin RA
SC41 - 30151 Extraction and transaction process
SC41 - 30153 Guidelines for digital twin entity modeling
SC41 - 21823-1 Interoperability Framework
SC41 - 21823-3 Semantic interoperability
Security and privacy
Data
SC27 - 27115 Cybersecurity eval. of complex systems
SC41 - 21823-5 Behavioral & policy interoperability
SC27 - 5181 Data provenance
SC32 - 5207 Data usage terms and concepts
SC27 - 27568 Security and Privacy of digital twins
SC27 - 27564 Privacy models
SC32 - 19763-3 Metamodel for ontology registration
SC32 - 5212 Data usage guidelines
Artificial Intelligence
Cen-cenelec JTC21 AI Trustworthiness framework
SC27 - 27090 AI Security
SC27 - 27091 AI Privacy
SC42 – 8183 Data life cycle framework

Figure 10: ISO Standardization Activities on Secure Data Spaces

- Adopting the concept, framework and architecture being worked out by ISO/IEC JTC1/WG13 (trustworthiness)
- Adopting the trustworthiness principles and views of ISO/IEC JTC1 SC41 (IoT and digital twins).
- Integrating and contributing to various security and privacy standards (ISO/IEC 27564 Privacy models - in particular using ITS use cases, ISO/IEC 27568 security and privacy of digital twins)
- Monitoring, integrating and contributing CEN-CENELEC JTC21 (WG4 on AI trustworthiness characterization, WG2 on AI conformity assessment)

Below is a table summarizing those activities where members of the CASTOR consortium are been exposed:

Group	Description of involvement
ISO/IEC JTC1/AG8 Metareference architecture for system integration	Responsible for task force patterns, and contribution to guidelines standards development on reference architecture, based on ISO/IEC/IEEE 42010 architecture description. Connect will take into account those guidelines to facilitate contribution of standards
ISO/IEC JTC1/WG13 Trustworthiness	Contributions to 5957 (Trustworthiness reference architecture); 9814 (Trustworthiness concepts), 18149 (Trustworthiness ontology). Connect will take into account WG13
ISO/IEC JTC1/SC27 Information security,	Working Item 27563 (security and privacy in AI use cases – best practices), 27568 Security and privacy of digital twins, 5986

cybersecurity and privacy protection.	Cybersecurity assurance of systems and SoS, 27564 Privacy models, 27091 AI systems privacy protection (under ballot). Contribution to 5888 (Security requirements and evaluation activities for connected vehicle devices) Contributions from Connect are expected
ISO/IEC JTC1/SC41 IoT and digital twins	Contributor to 30141 (IoT reference architecture, PWI digital twin reference architecture. Editor of 30149 (IoT Trustworthiness principles), 21823-5 (Behavioral and policy interoperability). PWI Guidance on IoT and digital twin use cases. Chair of AG25 (use cases), AhG30 (CPS), AG31 (impact of other standards on SC41) Connect will take into account SC41
ISO/IEC JTC1/SC42 Artificial intelligence	Contributor to 5392 (Knowledge engineering reference architecture). Connect will take into account SC42
ISO PC317 Privacy-by-design for consumer goods and services	Contributor to 31700-1 (high-level requirements) Editor to 31700-2 (use cases)
ISO TC22/SC32/WG11 Road vehicles	Contributor to 8475 (Cybersecurity assurance level and Target attack feasibility), 8477 (Cybersecurity verification and validation),
CEN-CENELEC JTC21 Artificial intelligence	Contributor to WG2 AI conformity assessment (task force on automotive domain), to WG4 AI trustworthiness characterisation
ISO TC204	Active in WG17, 19 20

4.2 STANDARDIZATION ACTIVITY PLAN

4.2.1 Research & Standardization Communities

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

For the former, there are many channels through which the research community can be reached, and results of the project can be made available. First of all, it is necessary to publish in open access. CASTOR will provide open access to all published articles, on the ZENODO platform, and all publications will be made accessible on the project website, where they will be linked to their DOIs.

For the latter, standardisation is an utmost important aspect of the CASTOR project. CASTOR envisions to actively contribute to the security and interoperability efforts regarding futureproofing safety-critical application workloads, deployed over the CC, that the European Commission instruments, standardisation bodies and private organizations are pursuing. Towards this goal, the consortium will continuously analyse the standardisation potential of the project's key innovations and will map the key exploitable innovations to the standardisation objectives in order to

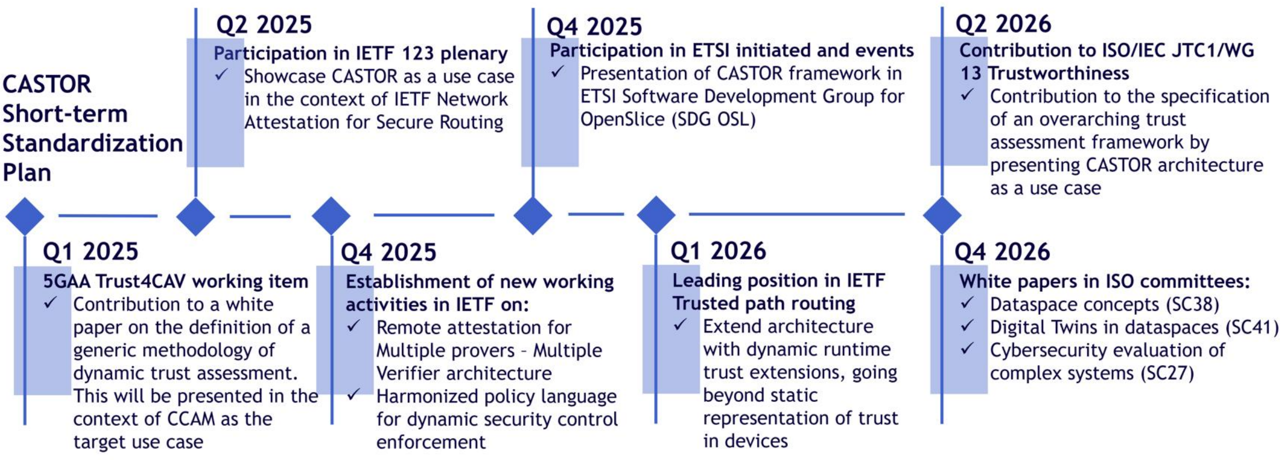

CASTOR Short-term Standardization Plan
Q2 2025
Participation in IETF 123 plenary
✓ Showcase CASTOR as a use case in the context of IETF Network Attestation for Secure Routing
Q4 2025
Participation in ETSI initiated and events
✓ Presentation of CASTOR framework in ETSI Software Development Group for OpenSlice (SDG OSL)
Q2 2026
Contribution to ISO/IEC JTC1/WG 13 Trustworthiness
✓ Contribution to the specification of an overarching trust assessment framework by presenting CASTOR architecture as a use case
Q1 2025
5GAA Trust4CAV working item
✓ Contribution to a white paper on the definition of a generic methodology of dynamic trust assessment. This will be presented in the context of CCAM as the target use case
Q4 2025
Establishment of new working activities in IETF on:
✓ Remote attestation for Multiple provers - Multiple Verifier architecture
✓ Harmonized policy language for dynamic security control enforcement
Q1 2026
Leading position in IETF Trusted path routing
✓ Extend architecture with dynamic runtime trust extensions, going beyond static representation of trust in devices
Q4 2026
White papers in ISO committees:
✓ Dataspace concepts (SC38)
✓ Digital Twins in dataspaces (SC41)
✓ Cybersecurity evaluation of complex systems (SC27)

Figure 11: CASTOR Short-Term Standardization Activities Plan

continuously update the concrete plan, already put forth in Section **Error! Reference source not found.**, towards submitting contributions to relevant standardisation bodies.

CASTOR partners aspire to exceed instead of merely reaching the following list of Impact KPIs, concerning Standardization Activities in all parallel channels, as these are gathered from the relevant sections of the Grant Agreement and tracked through the plan presented in this deliverable.

Note: This list might be further enriched as the project progresses and the present plan is updated and refined accordingly (in M18 and M36 respectively).

Table 11: Research and Standardization Communities

Relevant Activities	Impact Metric – KPI	Target
Collaborations, Synergies, and Liaisons, with projects clusters and initiatives	Synergies with Projects	>=6
	Joint Activities, Joint Dissemination, Joint presence in Events	>=8
Standardization Bodies	Liaison with working groups	>=3
	Project presentation in standardization meetings	>=5
	Contributions to technical specifications related to remote attestation, use case specification (e.g., Misbehaviour Detection), trust management, etc.	>=2

	Participation in Committees (meetings)	>=3
	Synergies with Projects	>=6

4.2.2 Standardization Bodies & CASTOR Road-Map

As aforementioned, a key strategic objective of CASTOR is to contribute to standardization efforts at EU level with IETF, ISO/IEC, ETSI, 5GAA (among others) been at the forefront of the envisioned activities. Planned outcomes of the project include the development of standardization proposal that push the state of the art in core areas (targeted by CASTOR) of trusted path establishment, routing and management, remote attestation (and underlying trusted computing technologies), lightweight cryptography, and the secure and accountable exchange of collective perception data across all layers of the Compute Continuum.

Table 12: Standardization Bodies and CASTOR Road-Map

TCG
UBITECH and SURREY have already established an Academic Liaison relationship with the Trusted Computing Group (TCG) and are aiming to disseminate the work conducted in the context of CASTOR towards novel property-based attestation mechanisms to the TCG. They participate in the following working groups: Trusted Platform Module (TPM), TPM Software Stack (TSS), Trusted Network Communications (TNC), the Internet of Things (IoTs), and DICE. In addition, SURREY is working on a new breed of Direct Anonymous Attestation schemes which are targeted for inclusion in a future TPM. In this context, CASTOR aims to design a new palette of advanced composable attestation services, exposed through harmonized TEE Device Interfces, extending the already existing TC capabilities of the edge for providing a built-in trustworthy network-level functionality. • The CASTOR TrustGrid Extensions leverage a SW/HW co-design for materializing the concept of a Distributed RoT (or making use of swarm attestation), towards establishing a chain of trust for the entire continuum, anchored to the governance of the security elements instantiated in each node, including the integration of TEE that enable verifiable remote computing capabilities which can offer assurances on the “trust state” of a node through the required proofs. Such proofs provide evidence (encoded as **Verifiable Credentials (VC)** extending the use of the W3C attribute structures for disclosing identity & device status attribute assertions) of the device correctness and functional safety, from their trusted launch and configuration to the runtime attestation of both behavioural and low-level execution properties. • Secure lifecycle management capabilities will be supported through advanced crypto primitives, such as secure, zero-touch device on-boarding, which can be realized by **attribute-based signatures (ABS), attribute-based signcryption (ABSC) and zero-knowledge proofs.** • CASTOR ensures the correct ordering of all trustworthiness evidence and measurements collected, which can be realized by delegatable Order-Revealing Encryption or Order-Preserving Encryption to safeguard the robustness of the trust model against compromised information. TCG has formalized standards about attestation (standard attestation structure, privacy, qualifying data, anonymous signing, X.509 certificate signing), symmetric encryption, asymmetric encryption and signature operations, certification (credentials).
IETF Trusted Path Establishment Related Activities Trusted Path Routing

IETF is one of the main standardization bodies that is targeted by CASTOR due to its numerous activities and established working items related to CASTOR's core vision fostering trust and trustworthiness in the overarching traffic engineering process. Primary focus will be given on the following:

Trusted Path Routing[6] Working Group focusing on the provision of adequate protocols for safeguarding the integrity and trustworthiness of sensitive data flows as they transit a network. CASTOR, through UBITECH and UMU, have already established a liaison with the editing team of this WG in order to take the lead in drafting the new version of the protocol extending the (currently) static "device state evidence" (as presented during the onboarding of a device into the overall topology) into more dynamic evidence that can be presented, as assertions, during runtime. This essentially enables the continuous trust characterization of the overall topology, thus, guaranteeing that the Secure Service-Level Agreement is always achieved. CASTOR has already ensure the participation of core experts from the editing team of CISCO, FRAUNHOFER and HUAWEI to be part of the established Advisory Board (Section 3.5).

The Link-State Routing (LSR)[7] Working Group is chartered to document current protocol implementation practices and improvements, protocol usage scenarios, maintenance and extensions of the link-state interior gateway routing protocols (IGPs) - specifically IS-IS, OSPFv2, and OSPFv3. CASTOR envisions the possible integration of trust metric as part of the Flex-algorithm [RFC9350]. Hence, one area of work is to identify possible extension to the Flex Algorithm definition (FAD) in a similar way that some draft are doing like the one on Flexible Algorithms: Bandwidth, Delay, Metrics and Constraints.

Remote Attestation Procedures (RATS) working group developed procedures to establish a level of confidence in the trustworthiness of a device or a system. RATS provides the mechanisms for appraising evidence of a device's trust or security properties, and attesting to the verifiable integrity proof to the evidence (Attestation Result). CASTOR will contribute on providing attestation and evidence collection mechanism as well to the concept of the TAF for trust evaluation.

ACE and LAKE: Two working groups with the SEC area of IETF are Authentication and Authorization for Constrained Environments (ace) and Lightweight Authenticated Key Exchange (lake). Although they are more related to security on small devices, in the context of the continuum that covers far-edge and edge, these kinds of devices become more important. Compounding this issue, CASTOR work can be linked with the activities of attestation especially the use of efficient protocols for the transport of the evidence within networks. For example, some draft has been proposed for Remote attestation over EDHOC a protocol where the UMU team has been involved, EDHOC PSK authentication[8]. A similar situation happens with the possible connection in the work on ACE related to the integration of schemas provided by CASTOR for authentication and authorization in the different kind of network devices.

Interface to Network Security Functions (I2NSF): Another area of interest is the one related to definition of policies and capabilities of the networking entities. In that sense the objective will be to follow the possible continuation of the work of the WG Interface to Network Security Functions (I2NSF). **The goal of I2NSF was to define a set of software interfaces and data models for controlling and monitoring aspects of physical and virtual Network Service Functions NSFs, enabling clients to specify rulesets and provide enforcement mechanism.** A good example of the final results is the work led by one of the CASTOR consortium partners (UMU) on the use of a YANG Data Model (fully conformant with the IETF standards) for IPsec Flow Protection Based on Software-Defined Networking (SDN) RFC 9061. This work will be extended for capturing the runtime trustworthiness evidence extended in CASTOR (as part of the following NASR-related activities).

BOF Network Attestation for Secure Routing[9]**:** Following the same RATS philosophy and building on top of it, Network Attestation for Secure Routing （NASR) aims at a solution specifically designed for the routing use case. NASR aims to provide appraisable evidence of a routing path's trust or security properties; verifiable integrity proof in the path-level; and verifiable proof that certain packets/flows travelled such paths. CASTOR is clearly aligned with the work of the three main

[6] https://datatracker.ietf.org/doc/draft-voit-rats-trustworthy-path-routing/

[7] draft-ietf-lsr-flex-algo-bw-con-20

[8] draft-ietf-lake-edhoc-psk-02

[9] draft-liu-nasr-architecture-01 - Network Attestation for Secure Routing (NASR) Architecture

objectives of NASR related to how to use the evidence to calculate the path and integrate it in the secure routing concept that can be extended not only to security aspects but also trustworthiness. CASTOR has already secured a spot in IETF 123 Plenary Meeting that will take place in June 2025 for presenting CASTOR as a possible use case in the NASR WG (Figure 11).

BOF Harmonized Policy Language for Dynamic Security Control Enforcement: CASTOR aims to specify mechanisms for policy-based routing using a Trust Policy Language (TPL) based on ALFA policy language [10], enabling automated compliance with SSLAs in multi-domain environments. ALFA, a lightweight and structured policy language, allows for the precise expression of trust-based access control and routing policies, ensuring interoperability across domains. The project's objective is to drive the establishment of a new IETF Working Group (WG) initiative dedicated to trust-aware policy enforcement in networking. An initial engagement with IETF has led to a proposal for a BOF session, where the feasibility of a WG creation and the suitability of IETF for this standardization effort will be further evaluated. CASTOR's contributions will define how trust policies govern path selection and security enforcement, aligning with Trusted Path Routing (TPR) and Remote Attestation (RATS) initiatives.

IDSA and DataSpace

UMU has been working in the extension of the IDSA Connector components defined for integrating privacy-preserving technologies and their manifestation through the necessary policies for the data sharing and the link to the proposal protocols DSP. Additionally, the work includes the connection of the policies related to the privacy aspects to the enforcement of the policies by the PEP entities of the Connector. This work will have a direct link to CASTOR activities for policy enforcement as the Conenctor extended can be also integrated with CASTOR needs.

DMTF SPDM

DMTF's Security Protocols and Data Models (SPDM) [10]working group defines the SPDM standard. The SPDM protocol enables authentication, attestation, and key exchange capabilities, which are all relevant building blocks in the context of CASTOR's trust assessment of the network infrastructure. CASTOR will explore new protocols and mechanisms as part of the TrustGrid extension for the runtime monitoring and trust assessment of the network devices (especially routers), allowing for a runtime attestation of these devices. CASTOR will establish secure channels between the TrustGrid instances and the orchestrator/TAF for exchanging authenticated trustworthiness evidence, which will require key exchange and authentication protocols building on top of the attestation evidence. In this context, CASTOR's solution will be inspired by the SPDM protocol and we will look into extensions related to network infrastructure attestation. If applicable, these extensions will be presented in the SPDM DMTF working group.

ISO/IEC on Quantum Computing

At the start of 2024, an ISO standardization joint technical committee (ISO JTC 3) was formed for the generic quantum domain. The committee released an ISO/IEC 4879:2024 document titled "Information technology — Quantum computing — Vocabulary" last year, which standardizes the commonly used terminology in Quantum annealing. Currently, there is no active committee looking into the standardization of quantum computing-based next-gen design space exploration (optimization). D-Wave, a manufacturer of quantum annealers, provides an open-source suite of

[10] https://www.dmtf.org/standards/spdm

tools, *D-Wave Ocean SDK*, to work with its quantum annealers. D-Wave also provides an open-source hybrid quantum-classical solver called *qbsolv* which breaks large optimization problems into smaller ones solvable on its quantum annealers. Amazon's open-source *Braket SDK*provides tools to access various quantum computing backends, including quantum annealers from D-Wave. Orthogonally, PyQUBO is an open-source Python library for formulating Quadratic Unconstrained Binary Optimization (QUBO) models, which are the fundamental formulations to solve an optimization using quantum annealing. Furthermore, several classical open-source simulated annealing tools incorporate features from quantum annealing such as *neal* and *simanneal*, blurring the line between simulated and quantum annealing. Finally, since access to real-world quantum annealers is prohibitively expensive, open-source simulated quantum annealers running on classical machines provide flexibility. For example, *OpenJij* is an open-source, GPU-accelerated simulated quantum annealer for solving large-scale Ising and QUBO problems.

Cyber security standards for aerospace

Unmanned Airspace Management, and aerospace in general, has numerous safety standards. Security tends to be addressed through policy and procedure specifications, recommended practice, and certification processes which Collins monitor such as:

- National Aerospace Standard NAS9948, Unmanned Aircraft System Data Protection and Privacy – essentially best-practice checklist such as auditing and accountability, authentication and authorization, incident response, zero trust, encrypt at rest, idle session termination, etc.
- ED-201A - Aeronautical Information System Security Framework
- ED-205 – Process Standard for Security Certification and Declaration of ATM ANS Ground Systems
- ICAO Doc 9985 – Air Traffic Management Security Manual

Security of the IT infrastructure does not have aerospace-specific standards and relies on IT security best practices. The European UAS Standards Coordination Group (EUCSG) maintains a continuously updated rolling development plan tracking standards and certification processes across UAS. They publish quite a comprehensive list of activities, and these do not currently include any standards related to cyber security of the IT infrastructure. Collins monitor this RDP on an ongoing basis.

ISO Related Activities

CASTOR aims to establish a liaison with ISO TC204, namely in the working group WG20 on Big Data and Artificial Intelligence (supporting ITS) and WG17 on Nomadic Devices in ITS Systems. During ISO WG plenary meetings which are held twice a year in a rotating venue scheme (Europe, Americas, Asia-Pacific) special time slots are reserved for workshops. It is planned to present the CASTOR project, its methodology and results at those workshops which draw an international (worldwide) audience. This will be the perfect stage to disseminate knowledge of CASTOR beyond the European context.

SURREY have already been involved in ISO/IEC JTC1 SC27/WG2, which specify cryptographic mechanisms. SURREY attend this working group’s meetings regularly and have contributed to many existing standards, including entity authentication, digital signatures, anonymous digital signatures, direct anonymous attestation, hash functions etc. They are therefore in a good position to introduce any new requirements and the corresponding solutions from the CASTOR project to this working group.

UBITECH is involved in ISO/IEC JTC1/AG8 in a guidance document on future reference architecture standards. TRIALOG is also involved, in ISO/IEC JTC1/SC41 on IoT and digital twin on the future IoT reference architecture, on the future Digital Twin reference architecture, on the future standard on interoperability, on the future guidance on use case, and on the future standards for data spaces. UBITECH is involved in ISO PC317 and ISO/IEC JTC1 SC24 on standards related to cybersecurity assurance of systems of systems, security and privacy of digital twins, privacy models, data provenance, CPS, AI security and privacy.

CHAPTER 5 EXPLOITATION PLAN

Besides dissemination and standardization activities, another important aspect of CASTOR’s activities pertain to the exploitation opportunities of the various technical artefacts and trust-aware path routing enablers to be designed and implemented. Effective exploitation strategies play a crucial role in ensuring that the project's outcomes and associated benefits are well recognized, adequately disseminated, and attract considerable interest within industry sectors. Thus, *CASTOR project's exploitation strategy is crafted with clearly defined objectives, specifically targeting the maximization of the impact and practical usability of the project's outputs*. The objectives underpinning the exploitation strategy include:

- Establishing and maintaining mechanisms for effective exploitation, ensuring continuous engagement with stakeholders and seamless integration of project outcomes into commercial practices;
- Enhancing stakeholder awareness by systematically informing relevant industry and academic groups about CASTOR's developmental milestones, thereby fostering collaborative interactions, partnerships, and networking opportunities;
- Coordinating comprehensive exploitation activities across multiple layers and typologies, involving various stakeholders, to leverage the diverse knowledge generated;
- Coordinate all levels and types of exploitation of the knowledge produced by the project,
- Ensuring timely dissemination and sharing of relevant information with targeted audiences through strategically chosen communication channels and mediums.

Parallel to dissemination efforts, the exploitation of CASTOR's achievements represents a foundational element critical to the project's overarching success. This is further emphasized by significant participation from industry partners whose involvement underscores the project's practical relevance and commercial potential. **The shared objective of CASTOR’s consortium is therefore to stimulate knowledge generation, develop innovative security solutions, and set a solid foundation for future commercial applications and market-oriented innovations.** Detailed plans to achieve these aims include both individual exploitation strategies—where each partner identifies specific opportunities aligned with their expertise and market positioning (to be detailed in Deliverable D7.2 [1])—and a common exploitation roadmap guiding collective consortium efforts. Templates for these individual plans are provided in APPENDIX B to ensure structured and systematic tracking. The overall roadmap for exploitation will be initiated with an initial draft version of a common exploitation strategy for the CASTOR framework by Month 12 of the project where the overarching architecture will be finalized capturing all the detailed interactions between the core technical components and key exploitable artefacts (already listed in Table 13). A first detailed version of this exploitation strategy will subsequently be formalized and documented in deliverable D7.2 [1] focusing at the beginning on delineating the exploitation of the overall architecture (as a whole). Following this initial phase, and the ratification of this first established exploitation plan by external experts (cf. Section 5.2 and Figure 12 depicting CASTOR’s plan to hold workshops with the ECLIPSE foundation for stipulating a well-formed open-source development plan – one of the core goals of CASTOR towards the establishment of an open-source community that can facilitate the vision of zero-trust service graph chains equipped with the necessary security controls to withstand (zero-day) exploits) explicit, well-defined individual exploitation plans will be developed and documented post-month 24, coinciding with the anticipated release of the (first version of) integrated CASTOR framework. Both the individual exploitation plans and an updated version of the collective roadmap will be comprehensively described in deliverable D7.3 [2] at Month 36, marking the project's conclusion and the finalization of all technical artefacts.

As aforementioned, another crucial objective of CASTOR is its vision to **share most of its artefacts and components as open-source so as to better facilitate the endmost goal of embedding**

trustworthiness in the establishment of service-graph-chains over the CC: By allowing all stakeholders involved throughout the entire networking stack (cf. Figure 2 – from the Network Operators and Telecommunication Vendors to the (HW-based) Security Vendors and Service Providers in the analytics and orchestration supply chain), to be able to leverage CASTOR's security enablers and trust extensions as building blocks in their own deployments. Compounding this issue, CASTOR has already identified an open-source development plan (as specified in Section 5.2) with the vision to engage with the standardized ECLIPSE WG.

While the main goal of CASTOR is to embed the concept of trust and trustworthiness in the traffic engineering process and path establishment protocols, through the conversion of nodes in the routing infrastructure into security "hardened" tokens equipped with a new breed of trusted computing enablers, the results of the project are valid beyond and therefore can be exploited to a broader range of products. These include routing vendors (e.g., CISCO, ARIMA, etc.); Network Operators (e.g., Deutshe Telecom, NOKIA, COSMOTE GR, etc.); HW-based security providers including Hardware Security Modules (HSMs), Trusted Execution Environments as defined by the GlobalPlatform, the ARM TrustZone, Intel's SGX, to name but a few; Application Providers, etc. 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 an (infrastructure- and network-tailored) device, and 2) none of them have a comprehensive security model and analysis. **Thus, the CASTOR aims to exploit its results also in the context of all of these stakeholders, enabling the vision of Zero-Trust Compute Continuum**.

5.1 EXPLOITABLE ARTEFACTS

In the following, we aim to identify and present the **core technologies of CASTOR**, as well as the **exploitable assets**, which are essentially the innovations and **value propositions of CASTOR** in terms of marketability, and will set the scene for its market positioning taking into consideration the novel features it offers compared to its competitors, in terms of both the CASTOR framework as a whole, as well as its individual modules. In order to be able to later perform an analysis of the market trends and exploitation possibilities that covers the widest possible range of industry viewpoints (to be included as part of D7.2 [1] and D7.3 [2]), an extensive research framework will be employed. A mixture of different approaches will be followed in order to gain valuable knowledge and a complete understanding of the target markets. Specifically, five insight perspectives will be used in CASTOR:

- Market insights: Involves researching and studying publicly available industry and monetary reports in order to identify long term and emerging market trends, including estimates about market size evolution, challenges, and opportunities.

- Competition insights: Involves listing key competitors and their product offerings with emphasis on existing or planned features, their placement in the market, as well as their strengths and weaknesses. It should be noted that, due the nature of the market, a large volume of information about existing products and services is not available to the general public.

- Client insights: Involves identifying the key activities and main points of importance from the perspective of a potential customer. This includes the value proposition and its importance to the aforementioned customers, and aims to identify the customer base of CASTOR and assist in performing customer segmentation.

- Policy and Regulatory insights: To ensure alignment with evolving cybersecurity, privacy, and data protection standards.

- Technology integration insights: Even from the early stages of the overarching CASTOR architecture, efforts have been shifted towards maximizing alignment with existing standards from IETF, especially in the topics revolving around the concept of trusted path routing. In this context, interoperability aspects primarily refer to aligning - and extending where needed - a number of interfaces that are designed and exposed by legacy routing technologies.

Taking into consideration the above, the purpose and ultimate goal of the exploitation analysis and plan is to align and fine-tune the development of CASTOR with the expectations and needs of the market. Additionally, it seeks to determine the most effective exploitation tactics with an appropriate business model for the system. As previously mentioned, CASTOR is focused on enhancing the operational assurance and trust model of the entire automotive supply chain and service graph chain. In this context, several technological domains will be employed and integrated into the CASTOR framework, including **Trust Assessment, Trusted Computing**, **Attestation and Integrity Conformance, HW-based Trust Anchors, Blockchain technologies, and Risk Assessment.**

Each of the aforementioned technologies will be explored in CASTOR in a modular manner, and each one corresponds to a concrete **exploitable asset** that will be designed in. In what follows, we provide a high-level specification of the envisioned CASTOR assets that will be considered in the later exploitation planning and will be part of the overall open-source development roadmap. It must be noted that this is a live process that will go through several iterations in the life cycle of the project and will be updated dynamically. The final reporting of this process will be performed in D7.3 [2].

Table 13: High-Level Listing of CASTOR Key Exploitable Artefacts

CASTOR Asset	Description
Trust Assessment Framework	CASTOR will define a trust architecture capturing the trust model and trust relationships among network elements in the process of the Traffic Engineering process across the computing continuum. This will enable network elements (e.g., routers) to **continuously assess the level of trust on target trust propositions based on fresh and observable evidence** collected from within the system. To address the dynamic nature of network protocols (e.g., IS-IS, BGP, OSPF), the optimal deployment of various services with mixed-criticality and the multitenancy aspects of service provision (i.e., multi MNO and multiple service providers), we place the Zero Trust concept at the base of CASTOR's trust architecture: trust on any entity is initially zero and needs to be established through suitable mechanisms. The Trust Assessment Framework aims to provide a reasoning mechanism to infer the actual trust level (ATL) while being able to cope with contradicting evidence and to operate under uncertainty. Trust assessments executed locally on a device/router level enable quick trust decisions and reactions in a time-constraint manner based on the local evidence. The secure collection and transmission of ATLs and trustworthiness evidence to the orchestration layer, allows for an enhanced global Trust Assessment Framework that has enhanced perception of the underlying network path and, thus, evaluate an aggregated ATL value characterizing an entire topology. *This CASTOR Asset will be led by the University of KENT and UBITECH.*
Optimization Engine	Identifying the optimal trusted path routing problem based on established service level agreements (SLAs) can be considered as an NP-hard problem. Extended on top of network-related requirements (e.g., latency, throughput) that needs to be attained, the challenge is aggravated by the introduction of trust-related properties that are required to be attained in the context of service provision over trust paths. To this end, CASTOR aims to tackle this optimization problem through **a future-ready post-quantum optimization solution**, reducing the solution space and identify a local optimum solution to accommodate service provision. On key aspect is that this problem involves not only the optimal path to serve a

	particular application based on the agreed requirements, but also the deployment of the necessary security controls to ensure that the agreed network- and trust-related properties are satisfied throughout the service lifecycle. Another important consideration is that the CASTOR Optimization Engine needs to translate the service provision problem into a multi-objective optimization problem ensuring the satisfaction of multiple application services with different requirements, though, sharing the same network infrastructure. *This CASTOR Asset will be led by the University of Amsterdam and QUBITECH.*
Attestation Enablers	The attestation enablers of CASTOR will provide enhanced mechanisms for providing assurances on the trustworthiness across the different levels of the compute continuum. Through the development of advanced **composable attestation services**, the CASTOR attestation enablers aim to provide trustworthiness evidence facilitating the conduction of trust assessment tasks that unlocks the establishment of trusted paths. To address scalability limitations and lift the assumption of trusted verifier entities, CASTOR aims to develop the attestation enablers following a **multi-verifier approach** that will unlock a robust mechanism for secure collection of trustworthiness evidence in the context of distributed trust assessment framework. *This CASTOR Asset will be led by UBITECH, NVIDIA and the University of SURREY.*
Dynamic Tracing	CASTOR envisions to design and develop dynamic tracing capabilities to **support core CASTOR technologies such as the overarching Trust Assessment Framework and the Device Finite State Machine abstractions**. Regarding the former, tracing capabilities provide the means to extract fresh and observable evidence from the target environment to the trust assessment agent so as to quantify trust, while the latter requires traces to be able to design and monitor the device state transitions. To this extent, **CASTOR will design implement novel tracing capabilities focusing on kernel extensions enabling the overall trust characterization across the Compute Continuum**. *This CASTOR Asset will be led by NVIDIA and UBITECH.*
Trusted Domain Interfaces	CASTOR aims to provide trusted domain interfaces for the communication of trustworthiness evidence across the computing continuum, starting from the far-edge devices, up to the global trust assessment framework running at the orchestration level. More specifically, CASTOR will **leverage the PCI-SIG TEE-Device Interface Secure Protocol (TDISP) and extend it to allow the secure and efficient transmission of trustworthiness evidence** from TSISP-Capable network elements up to the orchestration level. This includes the integration of TEE technologies that enable highly secure, trusted, and verifiable remote computing capabilities, which can offer guarantees and assurances for the establishment of trust through the required proofs/claims. Such proofs can provide verifiable evidence on their correctness and functional safety, from their trusted launch and configuration to the runtime attestation of both behavioural and low-level concrete execution properties. *This CASTOR Asset will be led by NVIDIA.*
Cryptographic Primitives	CASTOR aims to provide the mechanisms for provisioning a secure lifecycle management of network elements (and routing paths) from the early stages of the zero-touch on-boarding up to the continuous authentication and authorization

	necessary for application-, management- and trust-related data communication. To attain this goal, a set of advanced crypto primitives need to be designed and implemented. First, when it comes to the collection of attestation evidence within a path, the use of **Order-Revealing Encryption** will be evaluated so as to ensure the correct ordering of the relevant trustworthiness evidence. In addition, in the context of reacting to a decrease in the ATL value of a device (or sub-path), It might be critical to migrate network functions and services without compromising their operational behaviour. CASTOR aims to provide the cryptographic protocols to accommodate such **secure live migration schemes**. Finally, in the context of sovereign data sharing in a privacy-preserving manner, **the use of Verifiable Credentials and selective disclosure functionalities** will be adopted to ensure that only relevant attributes are disclosed to the intended recipients. *This CASTOR Asset will be led by the University of SURREY.*
Service Orchestration	CASTOR aims to provide an orchestration layer that provisions the establishment and configuration of routing paths as part of the traffic engineering process, including the deployment of trust paths when instructed by the corresponding intents. On top of the use of network-related properties and telemetry data, CASTOR **aims to extend this functionality by introducing trust-related aspects in the E2E service provision of the orchestrator**. To deploy and ensure the continuous monitoring of a trusted path topology, it is crucial that the orchestration engine accommodates also for the deployment and configuration of the necessary security mechanisms that enable the satisfaction of the relevant trust policies. Initially, the orchestration capabilities shall be evaluated in intra-domain settings where the orchestrator has complete visibility on the underlying network infrastructure. On top of that, CASTOR envisions to tackle the key challenges of **inter-domain environments as these introduce core challenges pertaining to the privacy-preserving exchange of (trust-related) information and claims as well as the provision of cross-domain services**. *This CASTOR Asset will be led by WINGS and ICCS.*
Routing Construction Engine	CASTOR envisions to bridge the gap between the intents coming from the service providers to service deployment. In the context of CASTOR, the intents are mapped to (S)SLAs between a service provider and an infrastructure provider. The (S)SLAs provide the necessary information to the Optimization Engine that expresses the network- and trust-related requirements as a multi-objective optimization problem for the selection of the optimal traffic engineering provision. Given the number of target objectives, the result can be a set of recommended optimal routing paths this can be extrapolated to the gap between the Optimization Engine and the Orchestration layer. To this extent, the Routing Construction Engine aims to **translate the recommended set of optimal paths coming from the Optimization Engine to an enforceable deployment strategy to be provided as input to the Orchestration layer.** *This CASTOR Asset will be led by WINGS and ICCS.*
Elevation to SLA	CASTOR aims to bridge the gap from the intents from the service providers towards the specification of concrete policies to be enforced in the traffic engineering process to ensure that the service level agreements (SLAs) are attained continuously. **In particular, CASTOR elevates the SLAs to secure SLAs (SSLAs) to express specific network- and trust-related objectives that need to be met through the development of an interoperable Trust Policy Language (TPL).** Part of the SSLAs include trust requirements that allow the trust

	assessment framework to derive trust decisions on the target trust propositions, as well as the necessary trust sources from which evidence need to be provided. The interpretation and the enforcement of the Trust Policies will be assigned to interoperable Data Connectors expanding the well-aligned notions of IDS Connectors. *This CASTOR Asset will be led by the University of Murcia, ICCS and the University of KENT.*
Device State Abstraction	CASTOR will employ finite state machines (FSM) to monitor the behaviour of network elements or specific functionalities of them. This **enables the identification of the ground truth of what constitutes a nominal behaviour in the routing plane**. Having an FSM per trust property would lead to a prohibitive explosion of resource and time requirements. To this extent CASTOR's State Learning & Merging Toolkit aims to **reduce the state-space that needs to be monitored by employing and advancing formal learning methodologies** so as to provide an abstract, fully representative device state abstraction. *This CASTOR Asset will be led by COLLINS.*
Secure Oracle Layer	**CASTOR envisions to provide an immutable repository to store trustworthiness evidence and trust decisions** for auditability purposes. Specifically, the use of Blockchain – particularly the recording of new data - is mediated **through Secure Oracle layers engrained across the Compute Continuum** to ensure the data veracity of what is stored on-chain. To ensure that only authenticated and authorized users can access the blockchain data, CASTOR employs secure and efficient cryptographic protocols to establish an SSI-based framework through the use of Verifiable Credentials. To this extent, the **CASTOR Secure Oracle Layer acts as a Verifiable Data Registry, ensuring the issuance and management of VCs** across the relevant stakeholders interacting with the blockchain. Finally, to facilitate the inter-domain exchange of trust-related information, CASTOR aims to provide **a decentralized Trust Exposure Layer design and implement a set of interoperable (north-bound) interfaces to expose a set of trust metrics of a domain to authenticated and authorized domains**. Similar to the ETSI Network Exposure Functions (NEFs), the CASTOR's Trust Exposure Layer provides verifiable information about the trust characterization of a domain without compromising sensitive data to external domains. *This CASTOR Asset will be led by SUITE5 and UBITECH.*

5.2 OPEN-SOURCE DEVELOPMENT PLAN

Some of the artefacts that CASTOR is considering for exploitation will be open-source. Since the practice of open-source requires a good understanding of the specific needs and a preparation, CASTOR will undertake work towards: (1) the identification of open-source exploitable artefacts (i.e., Trust Assessment, Attestation Enablers, Crypto Primitives and Misbehaviour Detection), and (2) the implementation of an open-source development plan.

Because open-source development plan requires experience and guidance, CASTOR will use an Open-source Development (OSD) plan template that is being developed in the frame of the OpenContinuum support action. TRIALOG is working on this template with ECLIPSE, so it will be able to provide support to CASTOR. The template (a version of which is put forth in Appendix B) includes:

- Information on stakeholders behind the plan.
- Context information describing the business intention.
- Strategy information (open-source business canvas, licensing, community approach, governance).
- Engagement information (stakeholders, in-bound and outbound activities).
- Project development (environment, development and release approach, support, evaluation).
- Approval and commitment.

The OSD plan is specific to collaborative projects as it makes the difference between activities carried out within the project and those carried out beyond the project (exploitation), currently one or two years after the project. Furthermore, it ensures interactions between partners on the preparation of the plan and its executions, through internal workshops.

The CASTOR OSD was constructed by UBITECH and then validated by ECLIPSE in the OpenContinuum project. It assumes a collaboration scheme with OpenContinuum which is described in the figure below (Figure 12), towards the identification the definition an appropriate OSD plan based on the nature of the technical activities of each project. For CASTOR, it is expected that the OpenContinuum project will be able to provide support in the definition of its open-source development plan, according to the timeline shown in Figure 12.

The support will consist of:

- Webinar explaining the questionnaire and the OSD plan template.
- An agreement for support provided by OpenContinuum.
- Up to four supporting sessions

The envisioned benefits of this collaboration are the following:

- CASTOR: Good practice and Awareness on potential collaboration with the continuum open-source initiatives (e.g., meta OS)
- OpenContinuum: Insight on an OSD plan template that can be used for future European projects and Insight on the CASTOR building block as a potential solution in the continuum.

The OSD template (see APPENDIX B) collects and reflects on the CASTOR's project (1) Open-source plan info; (2) Context; (3) Strategy including Business, Open-source licensing and IPR, Community approach and Governance; (4) Engagement of stakeholders and activities; (5) Project development encompassing environment, development and release approach, support, and evaluation. It is important to highlight that CASTOR has already planned the exploration of whether some of the produced artefacts can be upstreamed and shared through the ECLISPE OpenContinnum Project Foundation. UMU is already a member of this community, and with the support of all technical partners, will continuously monitor the CASTOR framework implementation and integration process trying to identify any opportunities for further contributing CASTOR insights for the establishment of a common architecture for the compute continuum. Target repositories include the OpenContinuum, ECLIPSE IoT (both focusing on the development of open-source

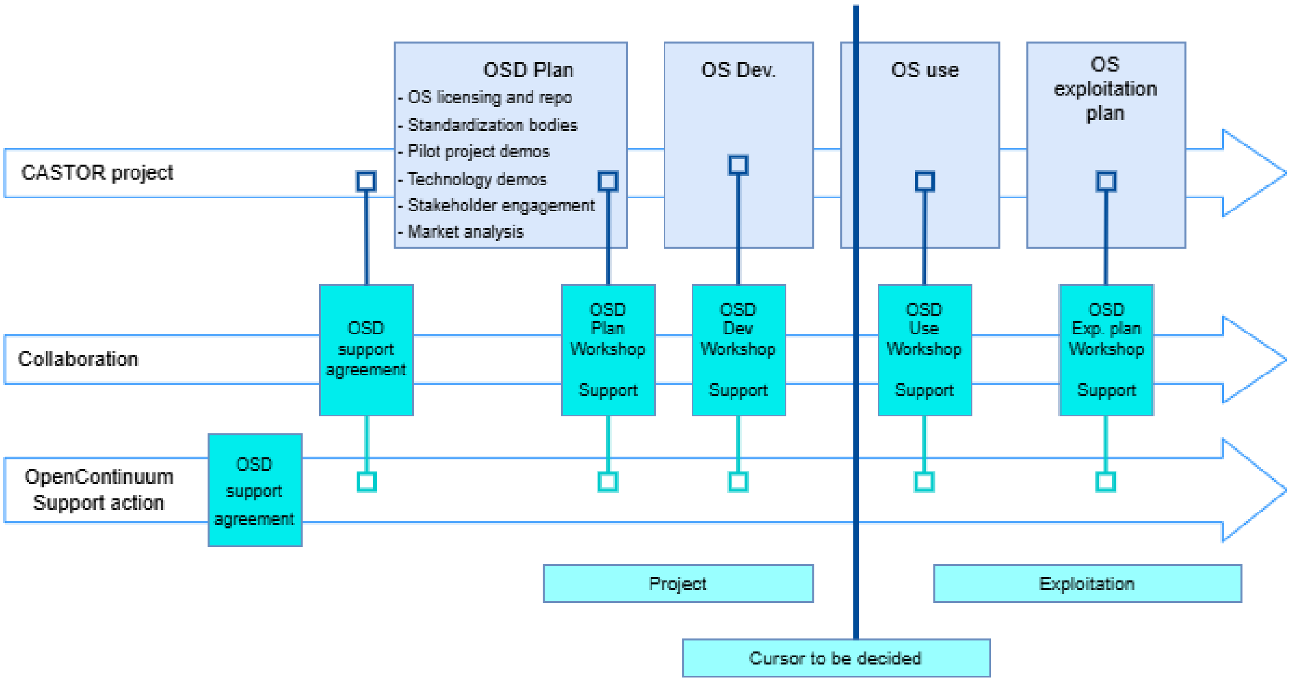


Figure 12: CASTOR Implementation of OSD Plan

implementations for IoT and cloud native protocols – candidate for CASTOR's TEE Device Interfaces and novel Trusted Computing Base), and the Oniro WG[11].

Overall, all the CASTOR core building blocks are planned to be publicly available as open-source repositories available at the project's Gitlab repository and maintained for at least two years by CASTOR's coordination aiming to enhance the CASTOR community. All relevant CASTOR repositories will be provided with the necessary documentation (i.e., README files) to facilitate understanding and adoption of the CASTOR artifacts by the community. Aspects related to IPR, and open-source licensing schemes are under discussion and will be fleshed out in D7.2. Throughout the lifespan of the project, CASTOR will organize and carry out webinar events, disseminating key technologies of the project to build and interact with the audience from the relevant stakeholders. Consequently, this community approach will empower the open-source CASTOR repositories to be widely adopted and lead the path for endorsement by well-established open-source communities. *Will it be feasible to upstream any CASTOR artefact to existing Eclipse projects or foundations? Will this be facilitated by the establishment of a steering committee or maintainers group?* Answers to these questions could signal long-term sustainability and boost community trust.

[11] https://www.eclipse.org/topics/edge-and-iot/

CHAPTER 6 SUMMARY AND CONCLUSION

This deliverable has been developed to provide a clear set of guidelines and a consistent framework for all project activities, ensuring broad visibility, effective promotion, collaboration with clusters, and contribution to standards, as well as putting forth a detailed and sustainable plan for ensuring the wide exploitation of CASTOR's innovative project results. Furthermore, D7.1 provides initial documentation of the CASTOR communication infrastructure as well as IT-related infrastructure.

First, a presentation of the visual identity of the CASTOR project, including the project logo and project templates, is given. A corporate visual identity expresses the values and ambitions of the CASTOR project and its characteristics. The visual identity of the project with visibility and "recognisability".

Then, this document goes into the details of the CASTOR Communication and Dissemination strategy, presenting the phases, the approach, as well as the tactics and tools planned to be used throughout the project. The agreed plan ensures that:

- All outreach activities are conducted in alignment with the guidelines and within the planned schedule;
- The messaging is consistent, high-quality, and impactful**;**
- All consortium members have an active contribution to promoting the project, open source, standards, and exploitation.

Deliverable D7.1 serves as a handbook for all project partners - it also identifies the partners who will play a key role in the successful execution of this plan. A monitoring and evaluation framework has been established to assess the progress and impact of the strategy.

Finally, this deliverable puts forth the details of the exploitation plan that will be further refined in the coming months. The identification of the core exploitable assets was performed, based on the technologies investigated in CASTOR (outlined as part of the CASTOR Vision – CHAPTER 2), to identify those mechanisms that can be further disseminated and advertised in the community. CASTOR envisions creating an open-source community, hence, most of these assets will be considered as part of the Open-Source Development (OSD) plan that has already been sketched and will further be detailed and validated with the support of ECLIPSE, as the most prominent standards on the creation of International Data Spaces.

The upcoming Deliverables 7.2 [1] and 7.3 [2] will provide updates on the progress of the strategy, the effectiveness of CASTOR's communication and dissemination activities, the collaboration within marketspaces and clusters, the contribution to standards, and the achievement of KPIs at M18 and M36, respectively.

CHAPTER 7 LIST OF ABBREVIATIONS

ABBREVIATION	TRANSLATION
3GPP	3rd Generation Partnership Project
5GAA	5G Automotive Association
API	Application Programming Interface
ATL	Actual Trust Level
BGP	Border Gateway Protocol
C2C-CC	Car-2-Car Consortium
CAV	Connected and Automated Vehicles
CC	Compute Continuum
CCAM	Connected, Cooperative, and Automated Mobility
CYBER	ETSI TC CYBER - The technical committee within ETSI dedicated to cybersecurity standardization, covering areas such as intrusion detection, authentication, and cyber threat intelligence sharing.
CyberNEMO	An open-source project under the Eclipse Foundation focused on trusted path routing and secure data exchange within the Compute Continuum.
ECLIPSE	Eclipse Foundation
ECSO	European Cyber Security Organization
ETSI	European Telecommunications Standards Institute
ETSI OSG OSM	ETSI Open Source MANO – An initiative under the European Telecommunications Standards Institute (ETSI) developing an open-

	source Management and Orchestration (MANO) stack for Network Function Virtualization (NFV).
ETSI SDG-OSL	Software Development Group for OpenSlice – A working group under ETSI developing an open-source Operations Support System (OSS) to enable Network as a Service (NaaS).
FSM	Finite State Machine
HSM	Hardware Security Module
IDS	International Data Spaces
IDSA	International Data Spaces Association
IEEE	Institute of Electrical and Electronics Engineers
IEEE SDN	A collaborative project under IEEE focusing on Software-Defined Networks (SDN) and Network Function Virtualization (NFV).
IETF	Internet Engineering Task Force
Intel SGX	Software Guard Extensions
Intel TDX	Trust Domain Extensions
IP	Internet Protocol
IPR	Intellectual Property Rights
IS-IS	Intermediate System to Intermediate System
JWT	JSON Web Token
MNO	Mobile Network Operator
NEF	Network Exposure Function
NaaS	Network as a Service

NFV	Network Function Virtualization
ONF	Open Networking Forum
OSD	Open-source Development
OSPF	Open Shortest Path First
PCI-SIG	Peripheral Component Interconnect Special Interest Group
PUCs	Pilot Use Cases
QA	Quantum Annealing
TCP	Transmission Control Protocol
Trust4CAV	A work item within 5GAA developing trust assessment methodologies for connected and automated vehicles.
SD-JWT	Selective-Disclosure JSON Web Token
SD-JWT VC	SD-JWT-based Verifiable Credentials
SDN	Software-Defined Networking
SLA	Service Level Agreement
SSLA	Secure Service Level Agreement
SSI	Self-Sovereign Identity
TDISP	TEE-Device Interface Secure Protocol
TEE	Trusted Execution Environment
TPL	Trust Policy Language

VC	Verifiable Credentials
WG	Working Group
WP	Work Package

CHAPTER 8 REFERENCES

[1] CASTOR Consortium, “Dissemination, Communication, Standardization and Exploitation Activities – Initial Version”, March 2026.

[2] CASTOR Consortium, “Dissemination, Communication, Standardization and Exploitation Activities – Final Version”, September 2027.

[3] 5GAA Automotive Associate, “MEC for Automotive in Multi-Operator Scenarios”, Technical Report, 2012, [Available Online: https://5gaa.org/mec-for-automotive-in-multi-operator-scenarios/] “D7.6: Project Impact Assessment.,” *The ASSURED Consortium,* July 2022.

[4] ISO 26262:2018, “Road Vehicles Functional Safety Standards”, 2018, [Available Online: https://blog.ansi.org/2019/02/iso-26262-2018-road-vehicle-functional-safety/].

[5] ISO/SAE 21434:2021, “Road Vehicles – Cyber-Security Engineering”, 2021, [Available Online: https://www.iso.org/standard/70918.html].

[6] WP.29 Cybersecurity and Cybersecurity Management System (CSMS), “UN Regulations on Uniform Provisions Concerning the Approval of Vehicles with regards to Cyber-Security and of their Cyber-Security Management Systems”, 2020, [Available Online: https://unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf]

[7] Car 2 Car Communication Consortium, “Guidance for Day 2 and Beyond Roadmap”, 2019, [Available Online: https://www.car-2car.org/fileadmin/documents/General_Documents/C2CCC_WP_2072_RoadmapDay2AndBeyond.pdf]

[8] CCAM Partnership, “CCAM Strategic Research and Innovation Agenda”, 2021, [Available Online: https://eraportal.sk/wp-content/uploads/2021/12/CCAM-Partnership-SRIA-FINAL-2021.pdf]

[9] 5GAA Automotive Association, “Working Item MEC4Auto – Technical Report on Use Cases and Initial Test Specifications Review”, 2020, [Available Online: https://5gaa.org/mec4auto-use-cases-and-initial-test-specifications-review/]

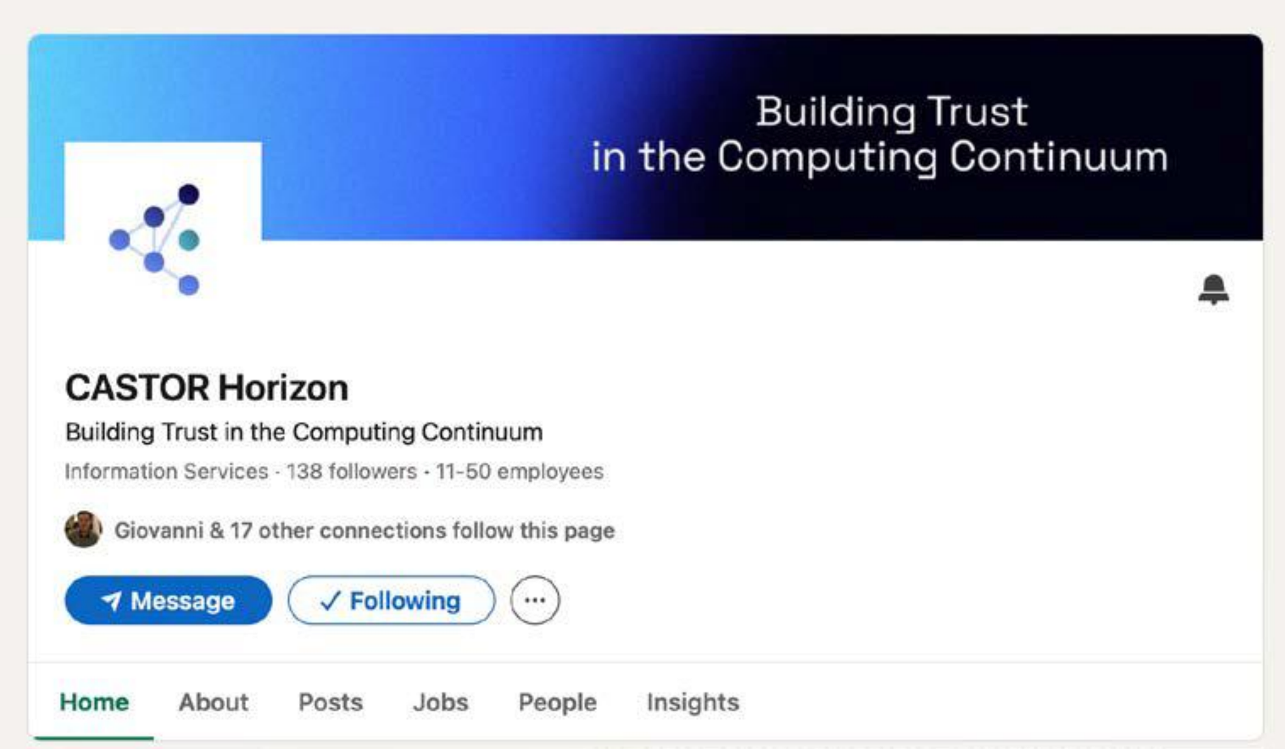
[10] H. Jurmaa, A. Hariri, A. Petrovska, O. Osliak, T. Dimitrakos, B. Crispo, ”Obligation Management Framework for usage Control”, In SACMAT 2024.

APPENDIX A CASTOR LOGOS

CASTOR VISUAL IDENTITY

A distinctive brand identity serves as a beacon, ensuring a unified presence across various platforms, be it digital or in print. It shapes the perception of those who engage with the brand, leaving a lasting impression and shaping their understanding of it.

Outlined herein are the guiding principles and visual elements that define the essence of the CASATOR project. These directions are designed to aid in the creation and curation of visual representations that embody its identity. Illustrations of the CASTOR brand identity can be witnessed across diverse channels such as LinkedIn and Twitter, showcasing its unique character and resonance.



Building Trust
in the Computing Continuum

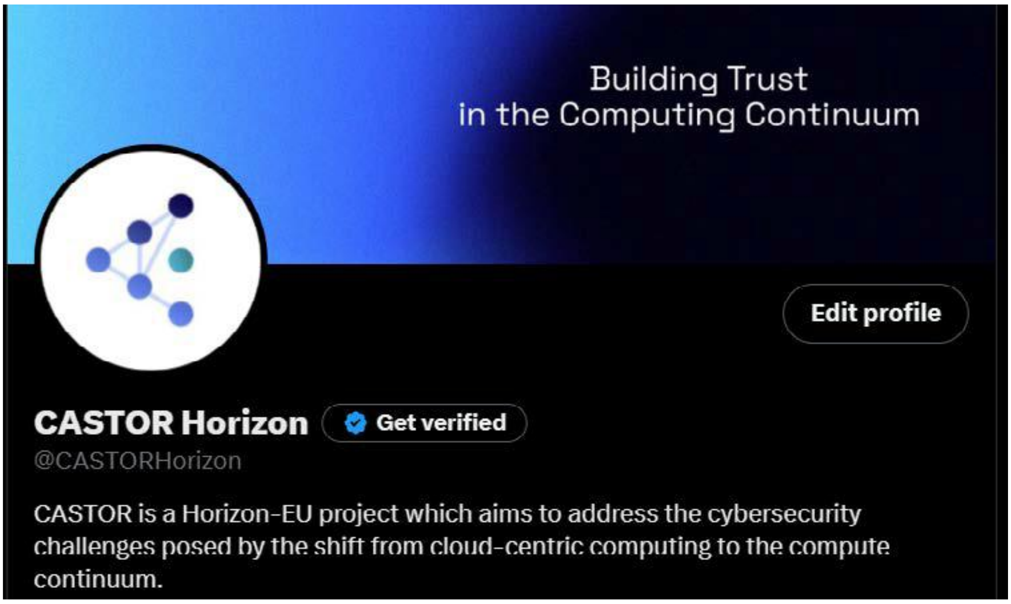
CASTOR Horizon

Building Trust in the Computing Continuum

Information Services · 138 followers · 11-50 employees

Giovanni & 17 other connections follow this page

Figure 13: CASTOR LinkedIn Account Logo



CASTOR Horizon

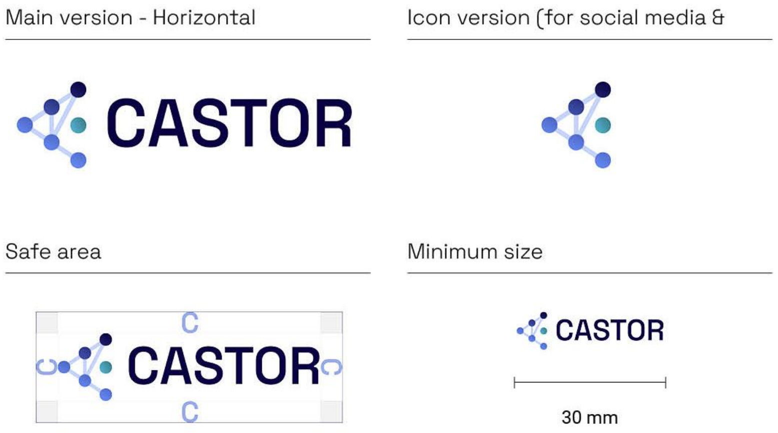
@CASTORHorizon

CASTOR is a Horizon-EU project which aims to address the cybersecurity challenges posed by the shift from cloud-centric computing to the compute continuum.

Figure 14: CASTOR LinkedIn Account Logo

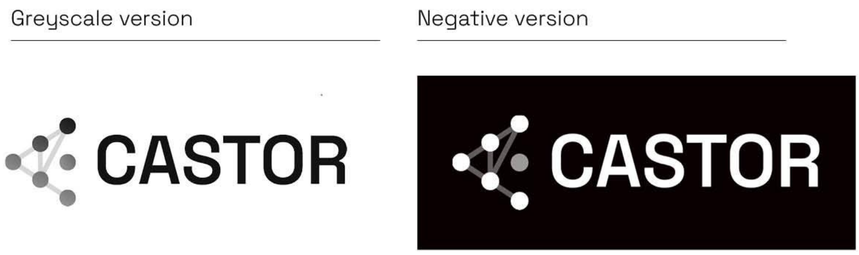
Logo

Main version of the CASTOR logo with technical specifications.



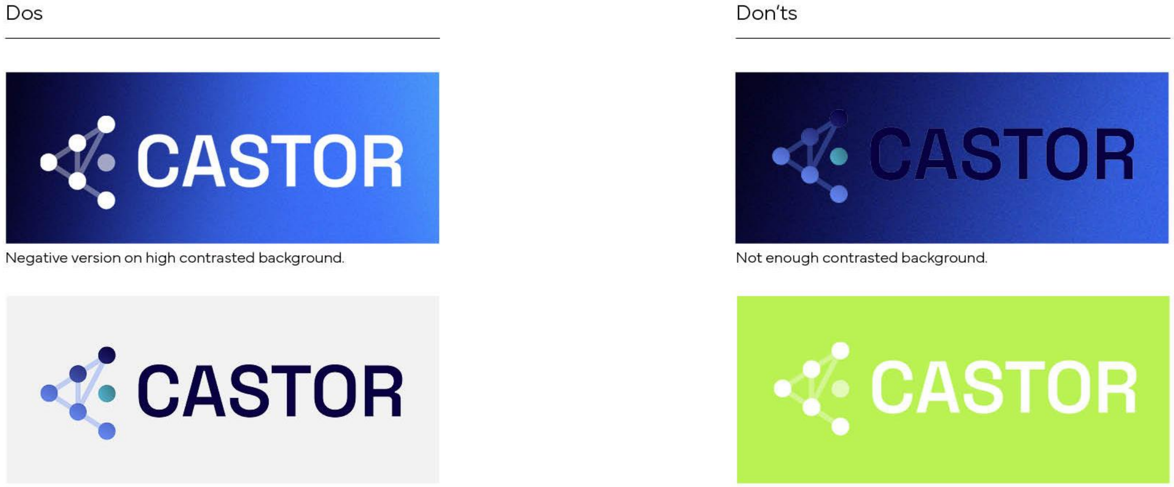
Logo variations

The main logo is also provided in the variations depicted here below, to allowreadability over dark backgrounds or for black and white printing purposes.



Do's and Don'ts

The Visual identity guide also provides instructions on how to use the main logo and its variation – over different types of backgrounds, with do's and don'ts.



Negative version on high contrasted background.

Not enough contrasted background.

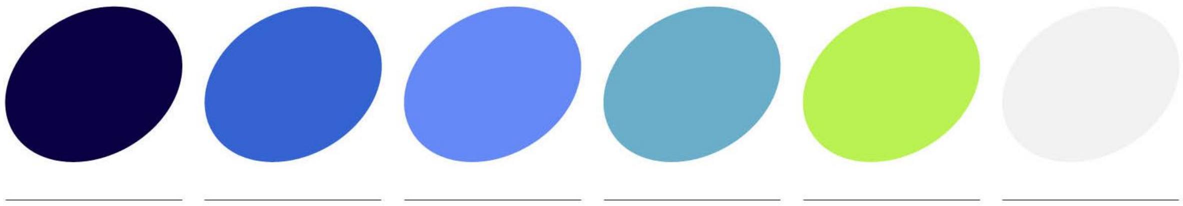
Main version on background assuring high contrast.

Not enough contrasted background.

Corporate Colours

CASTOR's corporate colours consist of a main palette of 6 colours, which are also reflected on the logo and the logo constituents.

Dos

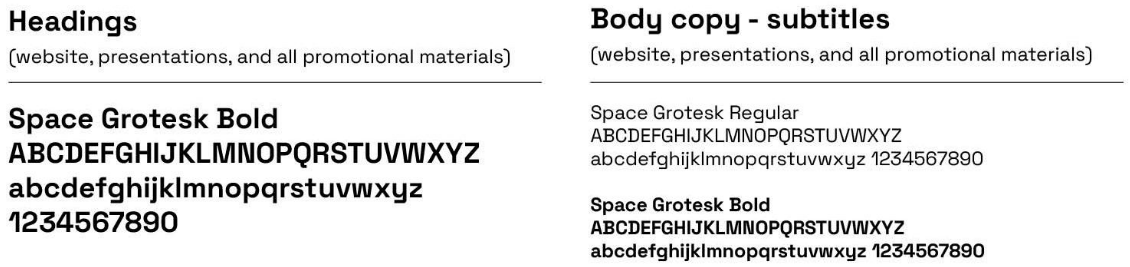


C100 M96 Y40 K53 R9 G0 B67 #1B2A30	C83 M62 Y0 K0 R53 G99 B210 #3563d2	C66 M47 Y0 K0 R101 G137 B245 #6589F5	C60 M17 Y16 K1 R106 G174 B202 #84AAC4	C36 M0 Y81 K0 R186 G241 B81 #BAF153	C0 M0 Y0 K5 R242 G242 B242 #F2F2F2

Font Types

CASTOR uses the open-source fonts from Google Fonts: Space Grotesk (Bold version) for headings and Space Grotesk (Regular and Bold versions) for body copy and subtitles. The usage of other versions of the fonts is allowed. This applies to the website, presentations, and all promotional materials.

For deliverables, the system font Arial (only Regular and Bold versions) should be used instead, to avoid missing font issues, as these documents are likely to be mainly edited outside Design departments. Arial could be also used for presentations in case Spece Grotesk fonts are missing.



Headings

(website, presentations, and all promotional materials)

Space Grotesk Bold
ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
1234567890

Body copy - subtitles

(website, presentations, and all promotional materials)

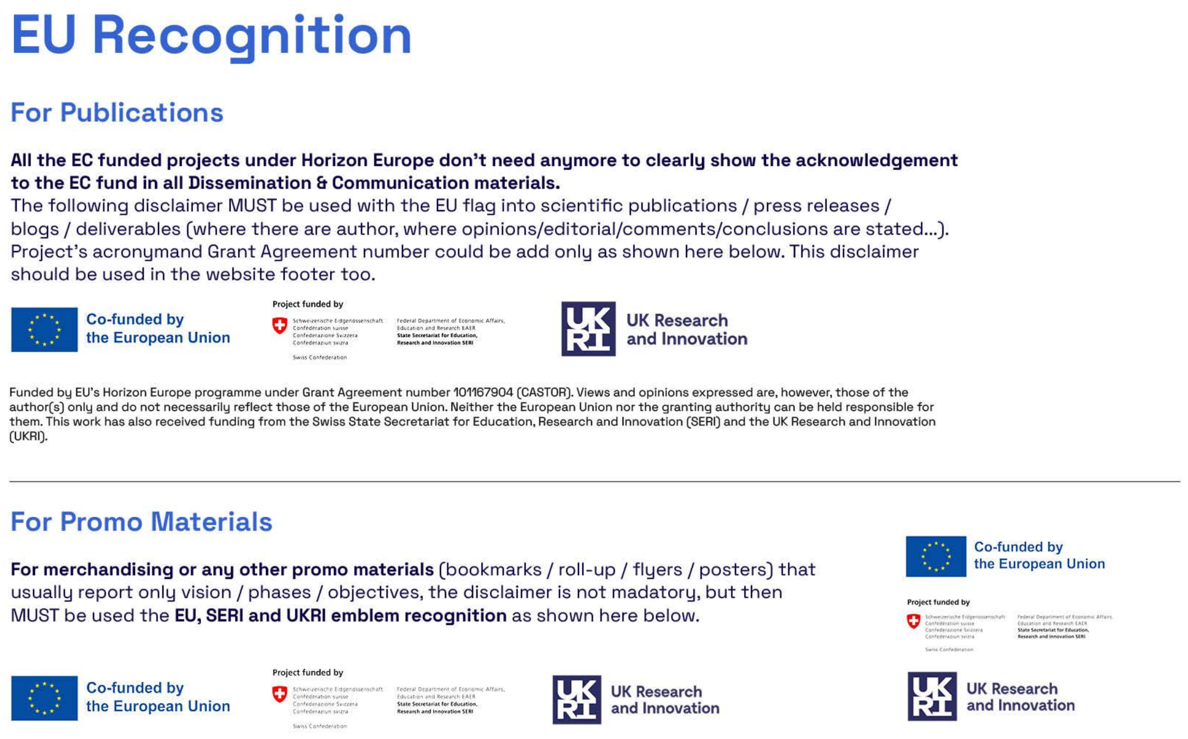
Space Grotesk Regular
ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz 1234567890

Space Grotesk Bold
ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz 1234567890

ADHERENCE TO THE EUROPEAN COMMISSION'S RULES OF COMMUNICATION OF RESULTS & ACKNOWLEDGMENT OF SOURCES OF FUNDING IN COMMUNICATIONS

All communications related to the project, including media relations, conference or seminar participation, and dissemination materials such as brochures, leaflets, posters, and presentations (whether in electronic formats, traditional media, or social media) recognize EU support. This includes prominently displaying the European flag (emblem) and the funding statement (Figure 15), translated into local languages where appropriate, as specified in the project's Grant Agreement, by Article 17.2.

Additionally, since three consortium partners (D4P, the University of Kent and the University of Surrey) are Associated Members and receive their portion of CASTOR resources from their respective national authorities, these organizations must also be acknowledged. This includes featuring their respective logos.



EU Recognition

For Publications

All the EC funded projects under Horizon Europe don't need anymore to clearly show the acknowledgement to the EC fund in all Dissemination & Communication materials.
The following disclaimer MUST be used with the EU flag into scientific publications / press releases / blogs / deliverables (where there are author, where opinions/editorial/comments/conclusions are stated...). Project's acronymand Grant Agreement number could be add only as shown here below. This disclaimer should be used in the website footer too.

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

UK Research and Innovation

Funded by EU's Horizon Europe programme under Grant Agreement number 101167904 (CASTOR). Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. This work has also received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI) and the UK Research and Innovation (UKRI).

For Promo Materials

For merchandising or any other promo materials (bookmarks / roll-up / flyers / posters) that usually report only vision / phases / objectives, the disclaimer is not madatory, but then MUST be used the **EU, SERI and UKRI emblem recognition** as shown here below.

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

UK Research and Innovation

Figure 15: The Acknowledgment of Funding by the EU, Swiss State Secretariat for Education, Research and Innovation (SERI), and UK Research and Innovation for the CASTOR Project All communications related to the project, including media relations, participation in conferences or seminars, and dissemination materials like brochures, leaflets, posters, and presentations - whether in digital formats, traditional media, or social media - also acknowledge the support of these organizations.

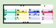
In addition, every communication or dissemination activity features/will feature the following disclaimer, translated into local languages where relevant:

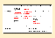
"*Funded by EU's **Horizon Europe** program under Grant Agreement number **101167904** (CASTOR). Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.*

*This work has received funding from the **Swiss State Secretariat for Education, Research and Innovation (SERI)**. Funded by **UK Research and Innovation** (**UKRI**) under the UK government's Horizon Europe funding guarantee 10139619."*

APPENDIX B OSD TEMPLATE

1	Open-source plan info	
Authors name and e-mail	*CASTOR persons in charge of providing and maintaining the plan. Can involve different partners.*	
History	*The open-source plan can be updated several times, depending on how the status of its execution. Examples are:* *- Change of strategy (e.g., modification of KER objective, merging with another KER)* *- Change in licencing approach* *- Change in community approach* *- Change in infrastructure use (e.g. Gitlab to Github)*	
	Date	
	Version	
	Description of modification	
Confidentiality	*You may wish to have up to three versions of the plan:* *- Confidential at partner level (not provided to consortium) – However experience shows that it does not run* *- Confidential at consortium and EC level (needed for deliverable)* *- Public (needed for engagement)*	

2	Context
Initial Key exploitation result name	*Mention if you have modified your plans with respect to the grant agreement.*
Initial description	*Mention if you have modified your plans with respect to the grant agreement*
Key exploitation result name	
Description	*Provide a rationale for the change if you have modified your plans*
Category of building block	 *How do you position your key exploitation results with respect to the 12 building blocks (OpenDei design principles for data spaces?)*

3	Strategy
3.1	Business
Open source canvas	*Option 1: Major open-source initiative* *Provide a first version of the open-source canvas.* *https://opensource.com/article/16/12/open-source-canvas* *The other options are identified by ECLIPSE* *Option 2: Leveraged service business model* *Option 3: Technology specialist*  *Option 4 Open source foundation* *Option 5 Co-creation of open-source extendible platforms* *Option 6 e-Pure service business model*
Assessment within project	*Describe tasks to be carried out on business within the project*
Assessment beyond project	*Describe tasks that will be carried out on business beyond the project, make recommendations for a roadmap*
3.2	Open-source licensing and IPR
Current licensing and IPR status	*Explain the current status (e.g., the selected licensing plan) and the dependencies. See https://opensource.org/licenses* *Describe decisions to be made on licensing and IPR within the project*
Analysis	*Provide an analysis of how you plan to enforce business-friendly licenses*
Decisions within project	*Describe decisions to be made on licensing and IPR within the project, justify when you do not select a well-accepted licensing scheme*
Decisions beyond project	*Describe decisions to be made on licensing and IPR beyond the project, justify when you do not select a well-accepted licensing scheme*
3.3	Community approach
Community	*Assess the intended community approach. Some references (https://opensource.org/community,*

	https://en.wikiversity.org/wiki/Open_community_approach, https://www.linuxfoundation.org/resources/open-source-guides/participating-in-open-source-communities, https://www.eclipse.org/collaborations/) *Example of community:* *- Governance: single organisation, Development: single organisation* *- Governance: single organisation, Development: community* *- Governance: open-source organisation, Development: community*		
	Current status of KER	TRL	
		Community	
	Intended status at the end of project	TRL	
		Community	
	Intended status beyond project	TRL	
		Community	
Decisions within project	*Describe decisions to be made on community approach within the project*		
Decisions beyond project	*Describe decisions to be made on community approach beyond the project*		
3.4	Governance		
Governance	*Select the agreed open-source governance approach (see* https://opensource.com/article/20/5/open-source-governance*)*		
Decisions within project	*Describe decisions to be made on community approach within the project*		
Decisions beyond project	*Describe decisions to be made on community approach beyond the project*		

4	Engagement
4.1	Stakeholders

Developers	Current team	*List developers and their roles . Is the team involving several partners?*
	Team evolution during project	*Explain if the team will evolve during project*
	Team evolution beyond project	*Explain if the team will expand externally beyond the project, and how engagement will take place*
Users	Intended users	List users (pilots) and their needs
	External users during project	*Explain if there will be external users during project, and how they will be engaged*
Other stakeholders	*List potential stakeholders that can have an interest to the project and need to be engaged* - *Other open-source communities* - *Platform / data space stakeholders* - *Domain specific stakeholders (Consumers, local communities, data energy cooperatives)* - *Energy and non-energy business stakeholders (finance, healthcare, water, mobility, etc.)* - *Regulated operators* - *Standardisation bodies* - *Academic Fora, Universities, Research Communities*	
4.2	Activities	
Activities within project	*Inbound activities: liaison with other projects (through Int-Net, DSCC, OpenContinuum, and other Horizon projects), presentation to data space events (IoT, BDVA, BRIDGE, …), conferences, blogs, …* *Outbound activities: if any*	
Activities beyond project	*Inbound activities* *Outbound activities*	

5	Project development

5.1	Environment
Platform	*List platforms and dependencies on other products or components*
Development environment	*Explain development environment used to develop open-source project (e.g. Yocto)*
Decisions during project	*Describe decisions to be made on environment during project*
Decisions beyond project	*Describe decisions to be made on environment beyond project*
5.2	Development and release approach – Associated with performance KPIs related to the CI-CD pipeline including: (i) Number of Github branches/contributions; (ii) Number of downloads; (iii) Number of users (community engagement); (iii) Laison and use of CASTOR technical artefacts in the use case evaluation of other EU project initiatives, etc.
Development lifecycle	*Explain lifecycle approach (development, verification et validation) and approach (e.g. DevOps) including tools to be used*
Development lifecycle security assurance	*Explain measures for development lifecycle security assurance*
Release building approach	*Explain approach including tools to be used*
Decisions during project	*Describe decisions to be made on development and release during project*
Decisions beyond project	*Describe decisions to be made on development and release beyond project*
5.3	Support
Pilots involved	
Contact points pilot	

Contact points KER	
Training material	
Training schedule	
5.4	Evaluation
Schedule	*Provide schedule for questionnaire to pilots, questionnaire to developers and evaluation report*
5.5	Sustainability Plan
Community	*Responsible partners or external organizations/foundations (e.g., Eclipse, Linux Foundation)*
Funding	*Funding strategy for continued maintenance (e.g., internal R&D, service-based model, grants)*
Sustainability mechanisms	*Planned community mechanisms to support evolution (e.g., external contributors, governance updates)*
Fallback strategy	*Exit or transition strategy, if no sustainability model is adopted*

6	Evaluation and approval of plan
Project manager name	
Approval date	

Exploitation manager name	
Approval date	