CASTOR

Building Trust
in the Computing Continuum

D7.2
Dissemination, Communication, Standardization and Exploitation Activities – Initial Version

Project number:	101167904
Project acronym:	**CASTOR**
Project title:	Continuum of Trust: Increased Path Agility and Trustworthy Device and Service Provisioning
Project Start Date:	1st October, 2024
Duration:	36 months
Programme:	HORIZON-CL3-2023-CS-01
Deliverable Type:	Report
Reference Number:	HORIZON-CL3-2021-CS-01-101167904/ D7.2 / v1.0
Workpackage:	WP7
Due Date:	31st March, 2026
Actual Submission Date:	31st March, 2026
Responsible Organisation:	SUITE5
Editor:	Konstantinos Latanis(SUITE5)
Dissemination Level:	Public
Revision:	1.0
Abstract:	This deliverable presents the CASTOR dissemination, communication, clustering and standardization activities for the first reporting period (M1-M18) of the project. Moreover, it provides a market analysis, an open source development plan and an exploitation plan with KER evaluation and IPR analysis for the various components of the CASTOR Framework.
Keywords:	Communication, Dissemination, Clustering, Liaison, Standardization, Open Source, KER, Exploitation, Market Analysis, IPR

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.

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

Konstantinos Latanis(SUITE5)

Contributors (ordered according to beneficiary numbers)

Nikos Fotos, Sofianna Menesidou, Panagiotis Banavos, Thanassis Giannetsos (UBITECH)
Stylianos Kazazis, Iasonas Sakellariou, Symeon Tsintzos (QUBITECH)
Fabian Schwarz, Meni Orenbach (NVIDIA)
Yalan Wang, Liqun Chen (SURREY)
Alexandru Coleș, Ioan Constantin (ORO)
Vlad Chiriac, Ciprian-Romeo Comsa (TUIASI)
Riccardo Orizio, Michael McElligott, Stelios Basayiannis (COLLINS)
Vangelis Kosmatos, Panagiotis Pantazopoulos (ICCS)
Gkilpathi Evgenia (SUITE5)
Christos Dalamagkas, Ioannis Boukas, Evangelos Syrmos (K3Y)
Aristi Galani, Sokratis Barmpounakis (WINGS)
Pablo Martinez, Antonio Skarmeta (UMU)
Alexandros Fakis, Kostas Maliatsos (FERON)
Gergely Kovacs, Andras Edelmayer (COMMSIGNIA)
Jamie Pont, Budi Arief, Theo Dimitrakos (UKENT)
Siro Dell'Ambrogio, Olivia Ciubotariu, Daniel Onwude (D4P)

Disclaimer

Versioning and contribution history

Version	Date	Author	Notes
v0.1	19.12.2025	Konstantinos Latanis (SUITE5), Nikos Fotos (UBITECH), Stylianos Kazazis (QUBITECH)	Table of Contents creation, Chapter 1 provision, Contributions' allocation to partners
v0.2	07.01.2026	Siro Dell'Ambrogio, Olivia Ciubotariu, Daniel Onwude (D4P)	First draft of Dissemination and Communication activities chapter
v0.3	15.01.2026	Stylianos Kazazis, Iasonas Sakellariou, Symeon Tsintzos (QUBITECH)	Open-Source Roadmap (Chapter 6)
v0.4	29.01.2026	Konstantinos Latanis (SUITE5), Pablo Martinez, Antonio Skarmeta (UMU), Kostas Maliatsos (FERON), Olivia Ciubotariu, Daniel Onwude (D4P), Yalan Wang, Liqun Chen (SURREY)	Input on synergies (Chapter 4), Clustering and Standardization (Chapter 3), Draft input on RTL in Chapter 8
v0.5	03.02.2026	Iasonas Sakellariou, Symeon Tsintzos, Stylianos Kazazis (QUBITECH), Siro Dell'Ambrogio, Daniel Onwude (D4P), Kostas Maliatsos (FERON), Ciprian-Romeo Comsa (TUIASI), Fabian Schwarz (NVIDIA), Jamie Pont, Budi Arief (UKENT), Andras Edelmayer (COMMSIGNIA), Michael McElligott (COLLINS)	Contributions on Market Analysis per application domain (Section 5.1) and Definition of CASTOR's functional and business model (Section 5.2)
v0.6	14.02.2026	Siro Dell'Ambrogio, Olivia Ciubotariu, Daniel Onwude (D4P), Gkilpathi Evgenia, Konstantinos Latanis, Gkilpathi Evgenia (SUITE5), Sofianna Menesidou, Panagiotis Banavos (UBITECH)	KER Analysis and Contributions on Chapter 7, Provision of exploitation plans
v0.7	02.03.2026	Siro Dell'Ambrogio, Olivia Ciubotariu, Daniel Onwude (D4P), Stylianos Kazazis, Iasonas Sakellariou, Symeon Tsintzos (QUBITECH)	CASTOR IPR Management finalization (Chapter 8) and provision of Comparative analysis of CASTOR and SCION
v0.8	19.03.2026	Thanassis Giannetsos (UBITECH), Konstantinos Latanis (SUITE5), Stylianos Kazazis (QUBITECH)	Chapter 9 provision, Final updates throughout the document and release for internal review.
v0.9.0	23.03.2026	Sofianna Menesidou (UBITECH), Antonio Skarmeta (UMU)	Interal review and comments provision.
v0.9.1	30.03.2026	Konstantinos Latanis (SUITE5)	Addressing reviewer comments, submission ready version delivery
v1.0	31.03.2026	Daphne Galani (UBITECH)	Final Review & Submission

Executive Summary

Deliverable D7.2 documents the overall dissemination, communication, standardization and exploitation activities of the CASTOR project within the span of the 1st reporting period (M1-M18), based on the initial strategic plan that had been released through deliverable D7.1 in M6. This deliverable comprises a direct outcome of WP7 ”Dissemination, Standardization, Exploitation & Impact Creation” which has targeted during the first 18 months of the project to provide input and requirements related to market needs & trends, ensure proper communication and dissemination of CASTOR outputs, and contribute to relevant standardization activities on trustworthy networking and secure implementations focusing on the interplay between performance and assurance level.

Deliverable D7.2 reports the different communication and dissemination activities of the CASTOR project. A significant facilitator is the CASTOR website that contains all the necessary information to keep interested stakeholders aware of the CASTOR news and results. The social media of CASTOR, such as LinkedIn, also play an important role in the dissemination of CASTOR results. Several videos have been created by the CASTOR partners to showcase the project vision and progress, while blogs have described the different artefacts that are being developed in the project. CASTOR has already been very active with participation in numerous conferences and workshops towards showcasing project results, creating synergies with other projects and liaising with interested stakeholders. Moreover, the plan has been specified for the organization of workshops and participation in further events to demonstrate the advancements in CASTOR developments within the 2nd reporting period (M19-M36).

The current deliverable also presents the clustering and liaison activities, such as the participation in ECSCI and the collaboration with other sister projects in the cybersecurity domain. In addition, CASTOR has been engaged in several standardization activities, including involvement of CASTOR partners in ISO working groups, IETF and TCG.

During the 1st reporting period, a Market Analysis Questionnaire has been circulated among CASTOR partners. Based on the analysis of partners’ answers, the CASTOR consortium has conducted a Market Analysis identifying trends and opportunities that CASTOR cross-domain solutions may leverage, while defining the CASTOR functional and business model that extends SCION. Moreover, an initial evaluation of Key Exploitable Results (KERs) of the projects has been performed. Eventually, the individual exploitation plans of the different CASTOR partners have been described, and the value propositions introduced by the CASTOR use cases have been identified.

Deliverable D7.2 also provides the preliminary analysis on the IPR management for the different KERs of the project, identifying potential ownerships, access rights, risks and the overall IPR management process that will be followed in the next period of the CASTOR project. Furthermore, information about the External Advisory Board is provided.

This deliverable will provide input in the next deliverable D7.3, which will be the final deliverable of WP7 documenting all the dissemination, communication, standardization and exploitation activities of the CASTOR project within the 2nd reporting period (M19-M36) and encapsulating the techno-economic impact analysis of the CASTOR Framework integrated developments.

Contents

List of Figures

List of Tables

List of Abbreviations

Acronym	Description
ACC	Adaptive Cruise Control
ACM	Association for Computing Machinery
AD	Autonomous Driving
AEB	Automatic Emergency Braking
AI	Artificial Intelligence
AIOTI	Alliance for IoT and Edge Computing Innovation
AMD	Advanced Micro Devices
ARM	Advanced RISC Machines
ATL	Actual Trustworthiness Level
CAGR	Compound Annual Growth Rate
CAV	Connected Autonomous Vehicles
CCAM	Connected Cooperative and Automated Mobility
CD	Committee Draft
CEPS	Centre for European Policy Studies
CFA	Control Flow-Attestation
CIM	Cooperative Intersection Management
CIV	Configuration Integrity Verification
CO	Confidential
CPM	Collective Perception Message
CPS	Collection Perceptive Service
CPU	Central Processing Unit
D	Deliverable
DAA	Direct Anonymous Attestation
DENM	Decentralized Environmental Notification Message
DFG	Data Flow Graph
DNN	Deep Neural Network
DoA	Description of Action
DRL	Deep Reinforcement Learning
ECU	Electronic Control Units
EMDS	European Mobility Data Space
ENISA	European Agency for Cybersecurity
EPC	European Policy Centre
ETSI	European Telecommunications Standards Institute
EU	European Union
EUCAD	European Conference on Connected and Automated Driving
FIF	First-in-First
F2F	Face to Face
GDPR	General Data Protection Regulation

Continuation of List of Abbreviations

GPP	Generation Partnership Project
HARA	Hazard Analysis and Risk Assessments
HW	Hardware
IDSA	International Data Space Association
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMA	Intersection Movement Assistance
IoT	Internet of Things
IPR	Intellectual Property Rights
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
JTC	Joint Technical Committee
KER	Key Exploitable Result
KPI	Key Performance Indicator
MaaS	Mobility as a Service
MEC	Multi-access Edge Computing
ML	Machine Learning
MPC	Multi-party computation friendly
NIST	National Institute of Standards and Technology
OBU	On-Board Units
ODD	Operational Design Domain
OEM	Original Equipment Manufacturer
OS	Operating System
OSD	Open Source Development
PKI	Public Key Infrastructure
PWI	Preliminary Work Item
RAM	Reference Architecture Model
RDI	Research, Development and Innovation
RoT	Root of Trust
RTL	Required Trustworthiness Level
SAE	Society of Automotive Engineers
SDO	Standards Development Organisation
SME	Small Medium Enterprise
SoS	System of Systems
SRIA	Strategic Research and Innovation Agenda
STLA	Stellantis
SW	Software
SWOT	Strength Weakness Opportunities Threats
TAF	Trust Assessment Framework
TARA	Threat Analysis and Risk Assessment
TCB	Trusted Computing Base
TCG	Trusted Computing Group
TC204	Trust Computing 204
TEE	Trust Execution Environment
TPM	Trusted Platform Module
TR	Technical Report
TRL	Technical Readiness Level

Continuation of List of Abbreviations

UC	Use Case
USD	United Stated Dollar
VTC	Vehicular Technology Conference
VNC	Vehicular Networking Conference
VPE	Verifiable Policy Enforcement
VRU	Vulnerable Road Users
V2X	Vehicle-to-Everything
WG	Work Group
WP	Work Package
ZKP	Zero Knowledge Proof
5GAA	5G Automotive Association

Chapter 1

Introduction

1.1 CASTOR vision and concept

CASTOR envisions a new Internet architecture that places trust at the heart of routing decisions, rather than treating security as an afterthought. The traditional Traffic Engineering selects network paths based on criteria such as hop count, bandwidth, and latency, but security is not inherently factored only in the way data flows across the network. CASTOR changes this by introducing a quantified trust criterion into routing decisions, enabling the construction of trustful service-graph-chains over public networks.

Going beyond today's largely static trust properties, CASTOR aims to be a pioneer in ensuring continuous secure data transmission over dynamically trusted paths. It acknowledges that trust levels vary across heterogeneous infrastructures and different network operator domains, and addresses this through a "never trust, always verify" (below-zero-trust) philosophy, where every entity, physical or virtual, must continuously provide evidence of its trustworthiness regardless of its location in the system.

To achieve this, CASTOR combines trusted computing, trust assessment, and multipath optimization to deliver routing security that is non-intrusive, scalable, and globally applicable, even across heterogeneous trust domains.

1.2 Scope and Purpose of the Deliverable

Deliverable D7.2 presents the work that has been conducted within WP7 "Dissemination, Standardization, Exploitation & Impact Creation" during the first reporting period (M1-M18) of the CASTOR project, as a direct outcome of Task 7.1 "Dissemination and Communication Strategy", Task 7.2 "Contributions to Clusters & International Data Spaces and Marketplaces", Task 7.3 "Standardization & Regulation Activities", Task 7.4 "Open-Source Plan for CC Trust Reference Implementation" and Task 7.5 "Exploitation, IPR Handling & Business and Sustainability Planning".

It provides a detailed description of the dissemination, communication, clustering and standardization activities of the project within these first 18 months, while presenting the plan for the second reporting period where the advancements in the CASTOR Framework will be showcased in the various interested audiences. Moreover, this deliverable describes the Open Source Development Plan of the project regarding the different components that are developed in CASTOR. A meticulous Market Analysis is also presented based on the different application domains of CASTOR, along with the definition of the CASTOR business model and a preliminary evaluation of its Key Exploitable Results. The CASTOR value proposition for each different use case is specified and the individual exploitation plans for each partner of the CASTOR consortium are described. Moreover, an initial IPR management analysis regarding the Key Exploitable Results of CASTOR project is provided.

Deliverable D7.2 has received input from deliverable D7.1, which had been the basis for the planning of the communication, dissemination, standardization and exploitation activities at the early stages of CASTOR project in M6. An updated version of D7.2, the deliverable D7.3, will be delivered at the end of the project in M36, where all WP7 activities during the second reporting period (M19-M36) will be reported along with a techno-economic analysis of CASTOR benefits towards a modern compute continuum.

1.3 Relation to other WPs and Deliverables

Deliverable 7.2 has eventually received input from all the other Work Packages of the CASTOR project, since these are producing the technical material that is disseminated as the output of the project. These contributions have enabled the operation of the WP7 activities in terms of dissemination, communication, standardization, and exploitation aspects. Figure 1.1 depicts these interdependencies among the relevant work packages in CASTOR.

More specifically, deliverable 7.2 receives input from WP2 regarding the CASTOR Architecture that drives the design and development activities in the project. WP3 provides information about the set of CASTOR Trust Extensions that are deployed across the compute continuum to unlock the trust assessment capabilities. In addition, input for the design and implementation of the overall trust assessment framework is provided by WP4. Moreover, WP5 offers material for policy enforcement in the cross-domain continuum topologies throughout the service lifecycle, while WP6 provides input from the initial analysis of Use Cases and relevant proof-of-concepts in CASTOR.

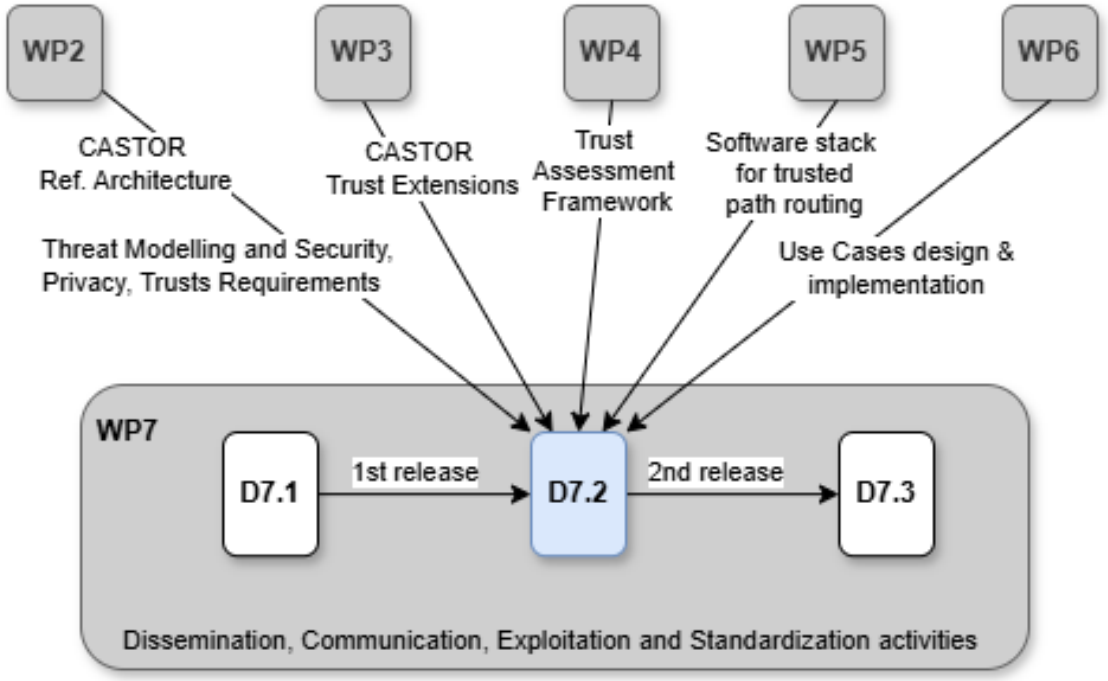

Figure 1.1: Relation of D7.2 with other WPs and Deliverables

1.4 Deliverable Structure

Deliverable D7.2 is structured as follows:

- Chapter 1 contains the introduction of the document.

- Chapter 2 presents the dissemination and communication activities of the project.
- Chapter 3 provides the clustering and standardization activities of the project.
- Chapter 4 describes the synergies of CASTOR with related projects.
- Chapter 5 provides a thorough Market Analysis through the prism of CASTOR.
- Chapter 6 presents the Open Source Development Plan of the project.
- Chapter 7 describes the overall exploitation plan of the project, along with the individual exploitation plans per partner.
- Chapter 8 describes the initial IPR management activities for the key exploitable results of the project.
- Chapter 9 presents the External Advisory Board of CASTOR.
- Chapter 10 contains the conclusions of the document.

Chapter 2

Dissemination and Communication Activities

In what follows, we offer a comprehensive updates on the first dissemination report (D7.1 [6]) of the CASTOR project. It explains the dissemination and communication initiatives undertaken during the project, while also providing a summary of forthcoming plans. Dissemination activities are considered key enablers for the success of the CASTOR project. The goal of dissemination is to make many stakeholders (network providers and operators, security OEMs, service and application providers) aware of the CASTOR approach and results. Wherever possible, research results will be used for the creation and support of CASTOR outcome and will substantially contribute to the benefit of the targeted constituents (Broad Public Society & Media (A), Policy Makers (B), Industry (C) and Research Community (D)).

2.1 Overview of CASTOR's Communication & Dissemination Approach

As it was presented under Deliverable D7.1, CASTOR's Communication and Dissemination strategy is structured around three distinct phases:

- **Awareness Creation** – This initial phase focused on establishing CASTOR's identity and visibility. It included the development of the project's visual branding and the dissemination of core project information through the official website and social media channels, laying the groundwork for broader recognition.
- **Scientific Stream** – The second phase emphasized the active dissemination of CASTOR's scientific outputs. Consortium partners engaged with external platforms by submitting research to conferences, journals, and workshops, enabling the presentation of results to both academic and industrial audiences. These engagements stimulated dialogue around project outcomes, generated feedback on progress, and supported future research directions. In parallel, project-owned communication channels (websites, blogs, and social media) were regularly updated to expand outreach and maintain stakeholder engagement.
- **Impact Spotlight** – This phase has not yet started. During this phase, Dissemination efforts will increasingly support Exploitation activities, including the use of project results for commercial applications and policy-related initiatives. Selected Dissemination actions will continue beyond the project's lifetime to ensure long-term visibility of outcomes. This includes maintaining the project website for an additional five years, sustaining social media and collaboration activities, participating in conferences, and supporting follow-up initiatives.

During the first 18 months of the project, Communication and Dissemination activities primarily concentrated on the **Awareness Creation** and **Scientific Stream** phases.

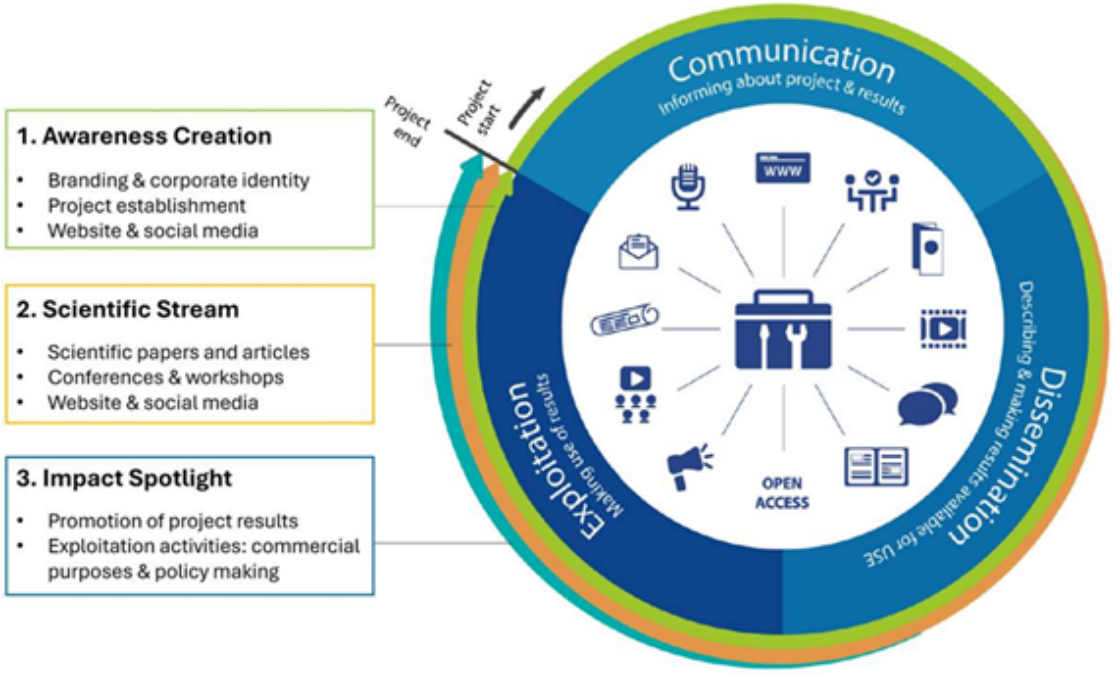

Figure 2.1: Dissemination & Communication Strategic Approach

2.2 CASTOR Objectives and Target Audiences

Guided by the project vision, CASTOR's Communication and Dissemination activities are designed to ensure broad visibility and meaningful engagement across scientific, industrial, and standardization ecosystems. These efforts are driven by four core objectives, to:

1. **Drive awareness among the targeted audiences** by clearly communicating the project's scope, goals, activities, and results.
2. **Disseminate CASTOR results with stakeholders** through a balanced mix of online and face-to-face channels that encourage knowledge exchange and collaboration.
3. **Establish liaisons with other projects, national and international cybersecurity agencies, standardization associations, and initiatives** to support cross-fertilisation of ideas and innovation transfer.
4. **Collect feedback from the targeted audiences** to validate the project's outputs, ensuring their relevance, practicality, and alignment with real-world needs through continuous stakeholder engagement.

The strategy addresses a diverse set of Target Audiences reflecting the project's interdisciplinary nature and broad application scope:

- Primary audiences include **Service Providers (SPs)**, to support adoption and alignment with end-user expectations, as well as **Dataspace Stakeholders** involved in exchanging trust-related information within traffic engineering processes and domain-level trust signalling.

- The project also targets stakeholders across the B5G/6G ecosystem, including **ISPs, infrastructure providers, routing vendors, and telecommunication operators**, alongside **Trusted Computing vendors and Network Hardware vendors** interested in CASTOR's cryptographic and trust mechanisms.
- Beyond industry, CASTOR actively engages **Academia and Research Institutions, related projects and initiatives, Standardization and Certification Bodies, and National and EU Public Authorities and Policy Makers**, supporting both technical advancement and policy alignment.
- Finally, CASTOR considers the **wider public** a key audience, recognising that long-term impact depends on strong user acceptance of the secure, trust-aware solutions introduced by the project.

2.3 Communication & Dissemination Activities

2.3.1 Internal Communication

Over the first 18 months, consortium coordination and day-to-day collaboration within CASTOR were carried out through a combination of **SharePoint, mailing lists, Slack, and regular meetings**. SharePoint served as the central workspace for document sharing and project tracking, while dedicated mailing lists supported structured communication across consortium, technical, and work-package levels. Slack was used as the secure messaging platform for ongoing discussions and quick exchanges.

In parallel, the consortium held 5 face-to-face meetings (Kick-Off Meeting in Athens, Plenary meetings in Limassol, Amsterdam, and Athens; and one technical workshop in Surrey), ensuring continuous alignment, progress monitoring, and effective decision-making throughout the project.

2.3.2 External Communication and Dissemination Activities

2.3.2.1 Project Identity

As a brand's visual presence plays a key role in how it is perceived and recognized, CASTOR established a strong and distinctive brand identity from the very beginning to create a unique and memorable image.

These brand guidelines and visual elements have been, and will continue to be, integrated into all Communication and Dissemination materials produced during the project and are intended for use by all project partners in their communication activities.

For more information on CASTOR's brand identity, including guidance on maintaining a consistent and recognizable visual style, you may refer to **Appendix B**.

2.3.2.2 Website

During the first 18 months, the CASTOR website operated according to the following 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)."

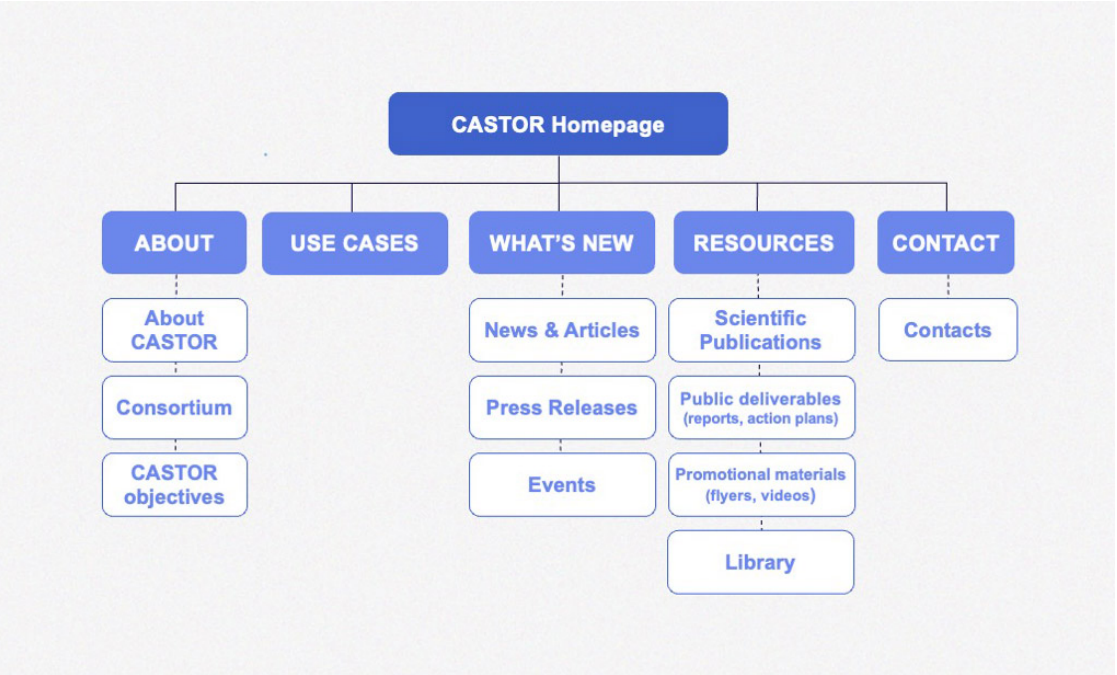

Figure 2.2: CASTOR Website Architecture

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.

From November 29th, 2024, the website launch date, until March 15th, 2026, the website has recorded 2510 visits, with over 4130 unique pageviews; and visitors engaged with the content for an average duration of one minute and 59 seconds. Of these visits, 1824 originated from direct entries, 417 from search engines, 151 from other websites, 114 from social networks, as shown in Figure 2.3.

2.3.2.3 Optimization and Traffic Strategies

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

- **Constant published content, SEO optimised**: The website's News section serves as an important source of traffic, with blog posts acting as a primary driver due to their scientific relevance and promotion across the project's social media channels. A comprehensive overview of the blog posts published to date, as well as those planned for the upcoming period, is provided later in this Section. Website visits are expected to grow steadily throughout the project, supported by targeted strategies designed to enhance organic traffic, with particular emphasis on the keywords identified for optimization.
- **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:
  1. All consortium partners' websites
  2. Partner projects' websites – as CASTOR established several liaisons with partner projects, these collaborations are further strengthened via official cross-promotion
  3. Social media - all project posts on LinkedIn and X include links to various sections of the website

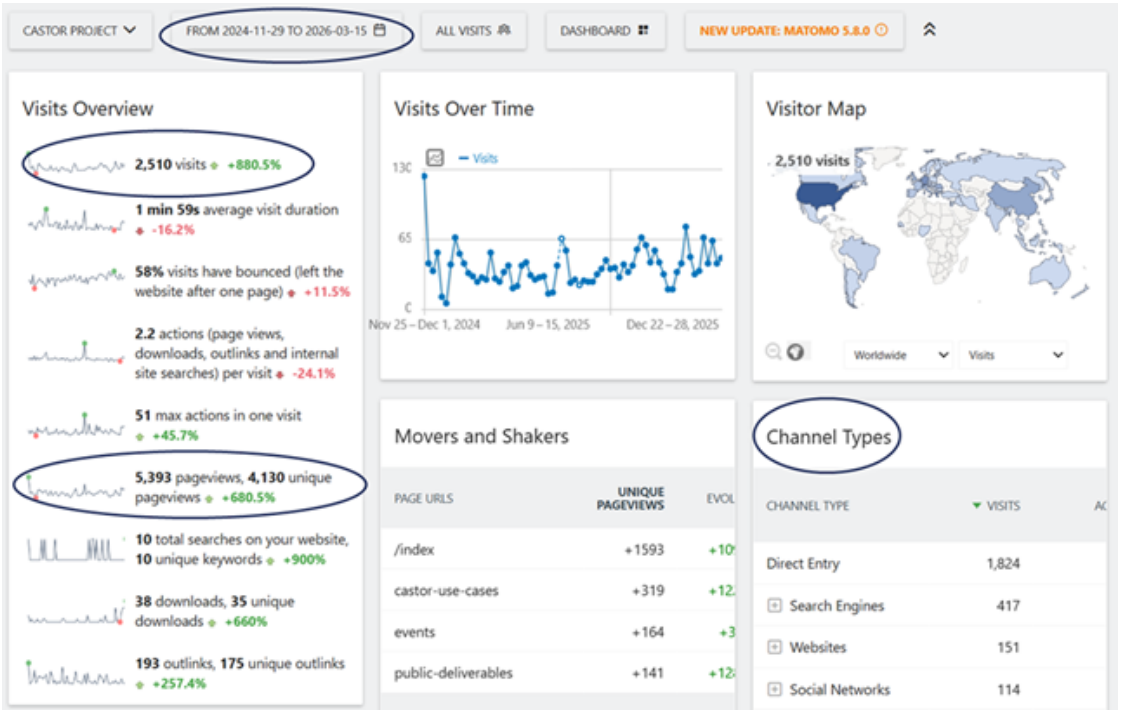

Figure 2.3: CASTOR Website Overview

4. Events websites (links will continue to increase upon participation in events)
5. EC websites
6. SERI

- **Tools used** (i.e. Matomo)

CASTOR website will be continuously maintained and updated throughout the project to ensure content remains current and relevant. It will highlight the latest project activities, results, and achievements, organized by topic and significance, using formats such as blog posts, videos, infographics, and other multimedia.

2.3.2.4 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 a **YouTube channel** (`https://www.youtube.com/@CASTORhorizon`).

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

- **Introductory themes**:
  1. **Meet the Consortium Members** – this theme was used at the beginning of the project, to introduce all the consortium partners;
  2. **Cybersecurity Glossary** – to introduce technical audiences to the specialized terminology relevant to CASTOR, while providing the general public with a clear understanding of fundamental cybersecurity concepts.
- **Technology-related themes** – as the project's technical work advanced, we feature/will continue to feature specific information concerning:

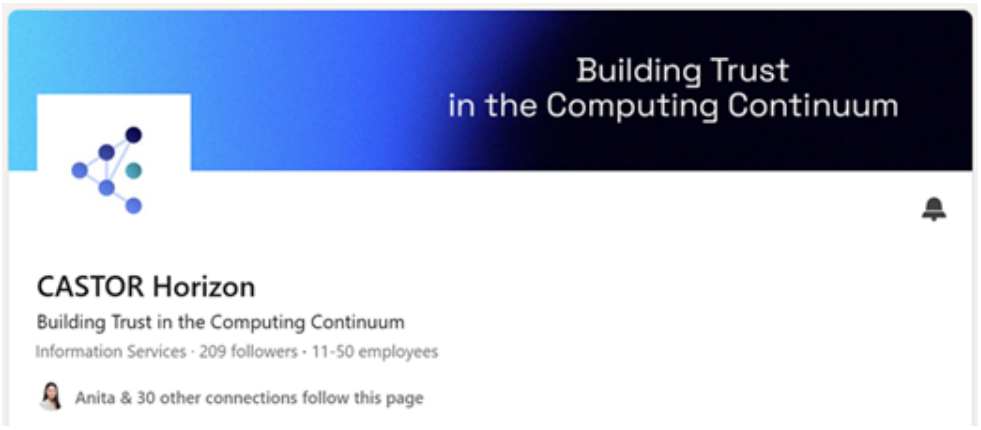

Figure 2.4: CASTOR's Linkedin Account

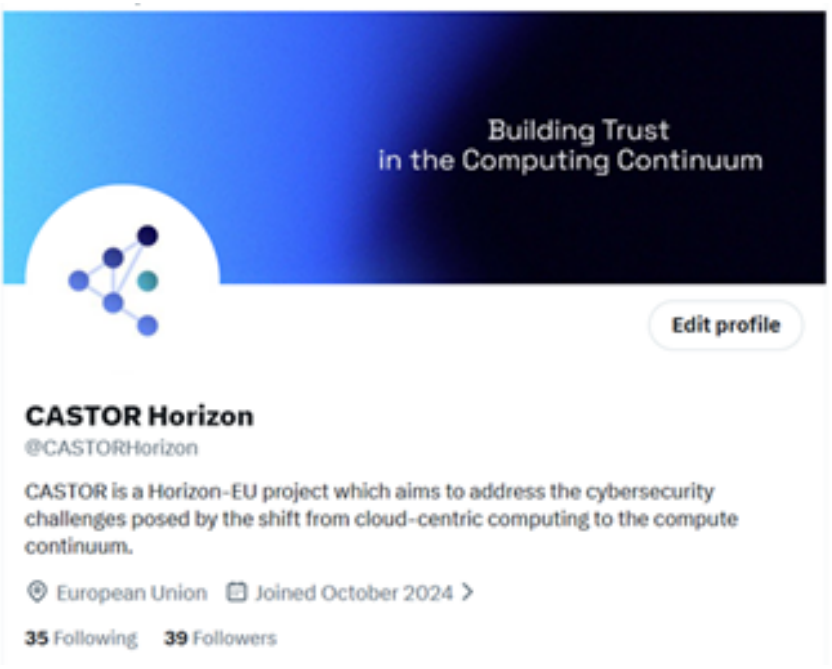

Figure 2.5: CASTOR's X Account

1. **The Language of Trust** – this is a series aiming to introduce key concepts used under CASTOR Trust Architecture, as defined in Deliverable 2.1
2. **Pilot use cases** - reports/videos;
3. **Contribution to Clusters and Marketplaces** – following events attended, collaboration with other projects, webinars/workshops organized by CASTOR;
4. **Standardization** – as per the opportunities reflected in Chapter 3;
5. **Exploitation** – as per the opportunities mentioned in Chapter 7;
6. **Other opportunities**: *Safer Internet Day* – February; *Cybersecurity Month* – October.

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

From October 1st 2024, to March 15th 2026, the LinkedIn page attracted 208 followers and generated over 47129 organic impressions and 2637 reactions. We will continue to grow the follower base and impressions, as per the above-mentioned posting topics and posting frequency.

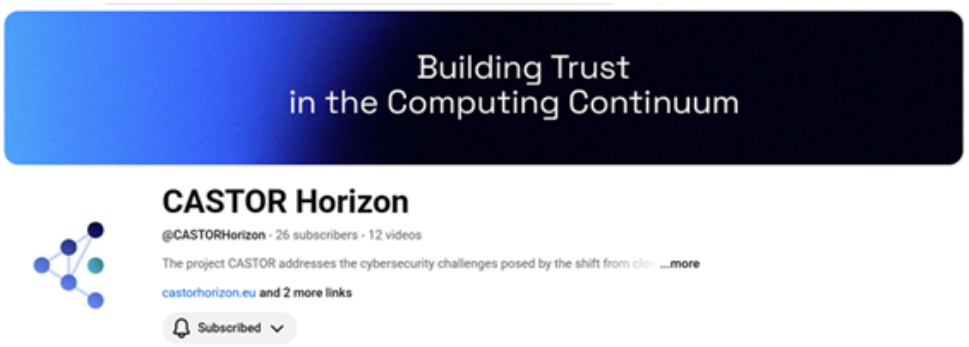

Figure 2.6: CASTOR's Youtube Account

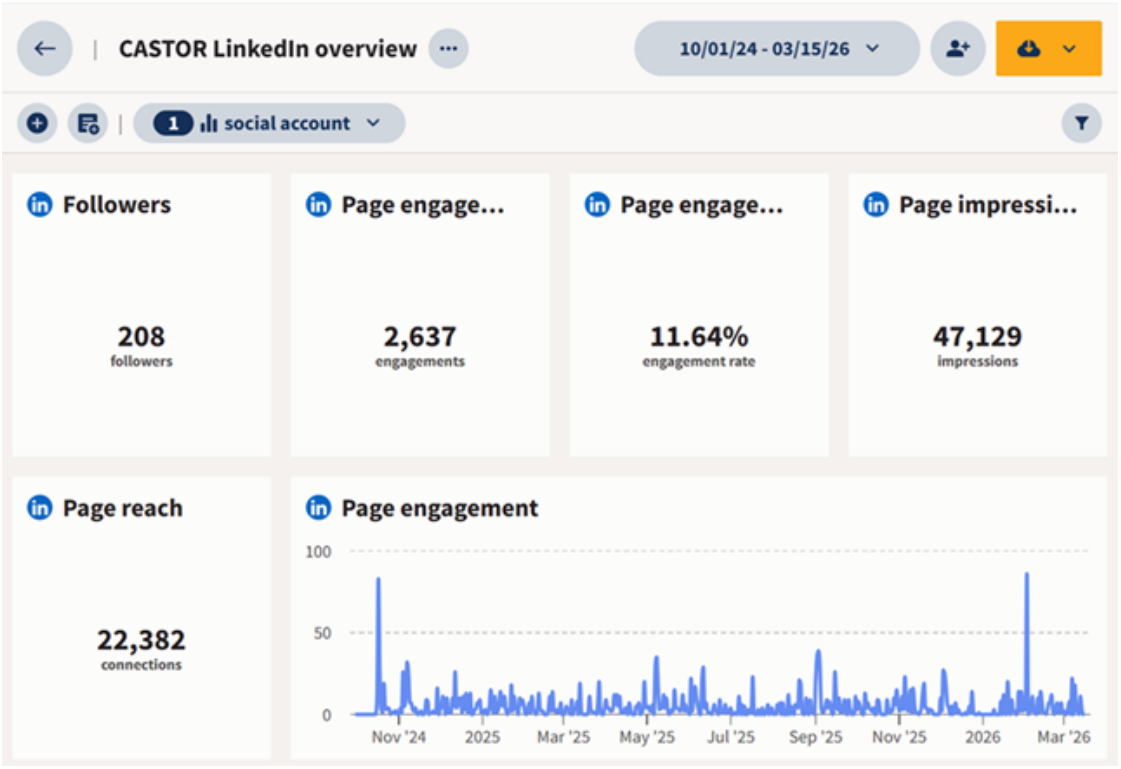

Figure 2.7: CASTOR LinkedIn's Analytics

Despite evolution over the past year, we decided to keep the X platform as a second source of information about CASTOR HORIZON. The posting strategy revolves around the same themes as the ones mentioned for LinkedIn, with a similar posting frequency of about 2 posts/week.

From October 1st, 2024 to March 15th, 2026, the X page built an audience of 39 followers and achieved more than 3858 organic impressions and 401 reactions. Moving forward, we will keep expanding both reach and community engagement in line with the planned topics and posting cadence.

2.3.2.5 Press Engagement

CASTOR's media outreach strategy acts as an additional channel to share key project results and milestones with journalists and the wider public. A press release to mark the launch of the project was issued on October 21st 2024, via Prowly.

A targeted database of 63 journalists specialising in cybersecurity and cloud computing across several European countries has been established. All contacts will receive broad project updates, while selected

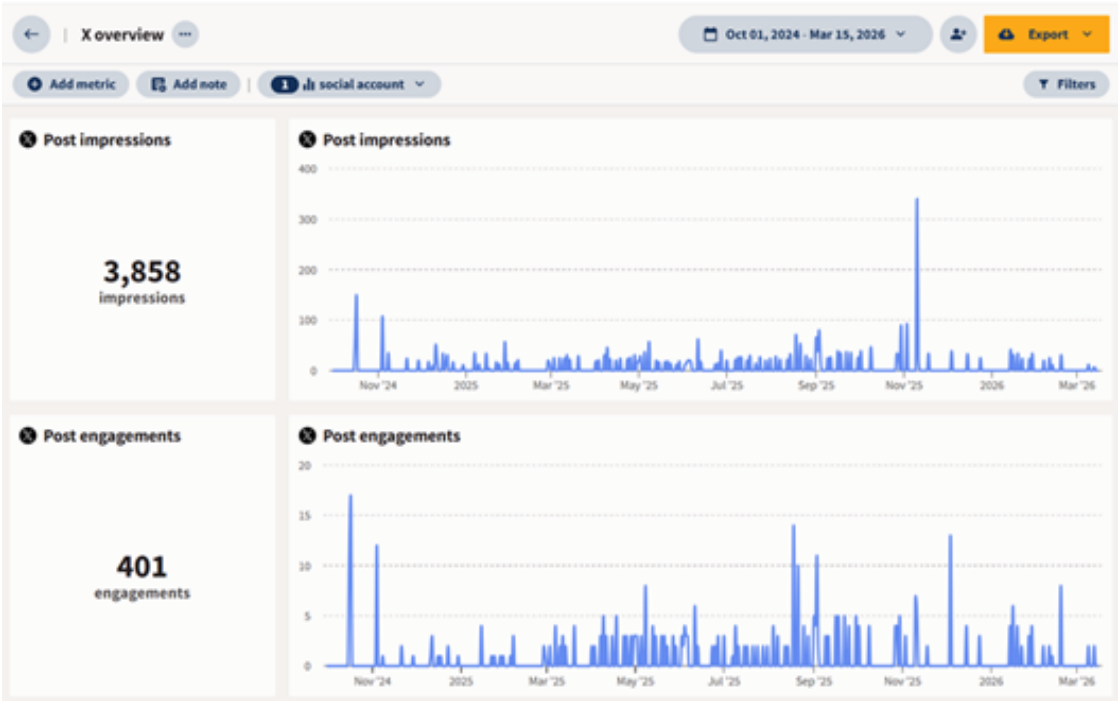

Figure 2.8: CASTOR X's Analytics

journalists will be approached individually with tailored story angles once the pilots are operational. Further press releases will be issued to highlight technical developments and showcase the results of the project's use cases.

2.3.2.6 Blog Posts, Articles & White Papers

To date, 10 blog articles have been published, either on the project website or by individual consortium partners, to raise visibility of the project's kick-off and each partner's role. The consortium has also defined a publications roadmap to accompany the evolution of technical work. Currently, emphasis is clearly on presenting the CASTOR Trust architecture, as outlined in Deliverable 2.1.

Table 2.1: List of Published and Planned Blog Posts

Partner	Topic	Timing	Blogpost title
D4P	Project launch	M1	Introducing the CASTOR project
UBI	Project launch	M1	Ubitech hosts kick-off meeting for the CASTOR innovation action pioneering the future of trustworthy computing continuum
K3Y	Project launch	M2	CASTOR kick-off meeting
QUBI	Trusted Path Routing Optimisation	M12	Quantum-inspired Optical Simulators for combinatorial optimization problems
UBI, D4P	Contribution to Standards	M13	New IETF Draft Advances Privacy-Preserving Attestation Standards
D4P	News on Clustering	M14	CASTOR Joins the European Cluster for Securing Critical Infrastructures (ECSCI)
UKENT	Trust Assesment	M15	Dynamic and federated trust assessment in the Traffic Engineering process
D4P, UBI	Trusted Path Routing	M17	The Core Problem Addressed by CASTOR: Finding a Path You Can Trust
D4P, UBI	Dynamic Trust Assessment	M17	Solving the Blind Spot: Why Dynamic Trust Assessment is Essential for the Computing Continuum
D4P, UBI	Network integrity	M17	Trust and Trustworthiness: Redefining Network Integrity with CASTOR

Partner	Topic	Timing	Links or estimated publishing date
D4P, UBI	Trust architecture	M19	The Dual Brain of Trust: Understanding CASTOR's Federated Assessment Model
UBI, SURREY	Attestation protocols	M19	Composability of Trustworthiness Evidence in Multiple Prover/Verifier Environment towards Trusted Path Routing
D4P, UBI	Trust architecture	M19	Open Questions Related to Trust Characterizations of Routers, Links, and Paths
NVIDIA	Dynamic tracing	M19	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

2.3.2.7 Videos

CASTOR has a dedicated YouTube channel: https://www.youtube.com/@CASTORhorizon. So far, 12 short video features have been released, and 3 more video vignettes are in work. The first released ones introduced the project's scope, goals, and use cases. As we approached M18, the latest released show project's progress by M18: work on the architecture and contribution to standards. All these videos were also shared via the project LinkedIn and X accounts. Additional videos will follow as the project advances, especially after the deployment of the use cases and during events, workshops, and the CASTOR Open Day. The consortium also plans to publish expert interviews on key technological areas, including risk assessment, trusted computing, cryptography, and optimisation.

Table 2.2: CASTOR Video Vignettes produced to date and their promotion

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# 3 (Video 1)	Link to post	Link to post
CASTOR USE CASE N# 3 (Video 2)	Link to post	Link to post
CASTOR USE CASE N# 3 (Video 3)	Link to post	Link to post
CASTOR USE CASE N# 3 (Video 4)	Link to post	Link to post
CASTOR USE CASE N# 4	Link to post	Link to post
CASTOR's Ultimate Goal	Link to post	Link to post
CASTOR's Core Innovations	Link to post	Link to post
CASTOR's Contribution to Standards	Link to post	Link to post

2.3.2.8 Promotional Materials

As part of CASTOR's project identity and promotional strategy, a project leaflet and roll-up templates were designed to visually communicate the project's key messages and branding. These materials were then physically produced and actively deployed at events, workshops, and public engagements, helping to raise awareness, attract interest, and provide stakeholders with concise, accessible information about CASTOR and its objectives.

Figure 2.9: CASTOR's Promotional Materials (1)

Figure 2.10: CASTOR's Promotional Materials (2)

Figure 2.11: CASTOR's Promotional Materials (3)

Figure 2.12: CASTOR's Promotional Materials (4)

Figure 2.13: CASTOR's Promotional Materials (5)

Figure 2.14: CASTOR's Promotional Materials (6)

2.3.2.9 Events & Workshops

The CASTOR Horizon consortium has participated, and will continue to participate, in a range of events to present the project's solutions and use cases to a wide audience. Key activities include conference presentations, workshops, webinars, and exhibitions, providing multiple opportunities to engage stakeholders and showcase project outcomes.

CASTOR Participation in Events: During the **1st reporting period (M1-M18) of the project**, the CASTOR consortium partners participated in 20 events relevant to the project's scope. All participations were promoted through the Events section of the CASTOR Horizon website and across the project's social media channels, as detailed in the table below.

Table 2.3: Participation in Events during the 1st Reporting Period of the CASTOR Horizon Project

Event Name	Event Topic	Partner	Link with CASTOR	Target Audience	Date
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 novel 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

Event Name	Event Topic	Partner	Link with CASTOR	Target Audience	Date
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 at NICT are involved.	Researchers	March 7th, 2025
CERTIFY Project First Infoday: Cybersecurity and IoT in Industry 5.0	Webinar	UMU, 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 core challenges that impact the wide-scale application of AI systems, with particular emphasis on fostering trustworthy and ethical use of AI in 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
Latest Research Results in IoT Supply Chain Security to Ensure Compliance with the CRA	IoT Day Online Webinar & Roundtable	UMU	UMU presented the concept of the Device Security Passport (DSP), relevant to CASTOR.	Researchers	April 9th, 2025
CompSys 2025	Dutch Computer Systems and Networks Research	UvA	UvA provided a research overview of ongoing research in the Parallel Computing Systems (PCS) group from University of Amsterdam, including the ongoing research in CASTOR.	Researchers, Educators	May 2025
Trusted Computing Group 2025	Event	UBITECH, SURREY	Presentation about Direct Anonymous Attestation and also on CASOR's novel work on memory introspection for enabling live migration of application states in a trustworthy manner.	Researchers, Engineers	June 2nd–5th, 2025

Event Name	Event Topic	Partner	Link with CASTOR	Target Audience	Date
EuCNC & 6G Summit 2025	Event	UBITECH	Presentation about "Network Softwarization Technology Enablers for Trust and Security in B5G and 6G Networks".	Researchers, Engineers, Industrial Stakeholders	June 3rd–6th, 2025
Technovers	Event	TUI	Project presentation at stand.	Academia, Engineers, Industrial Stakeholders, General Public	June 4th, 2025
Internet Engineering Task Force (IETF) Meeting	Meeting	UBITECH	CASTOR's unique runtime attestation functionalities were put forth for integration into the extended draft-rats-runtime-tpr-00.	Researchers, Engineers	July 19th–25th, 2025
IEEE NetSoft 2025 / SecSoft Workshop	IEEE International Conference on Network Softwarization	UMU	Connection to the orchestration aspects and the trust models for virtualization.	Researchers, Industrial Partners	July 2025
IEEE International Conference on Cyber Security and Resilience (IEEE CSR)	Event	UBITECH	Paper presentation: "Trust or Bust: Reinforcing Trust-Aware Path Establishment with Implicit Attestation Capabilities".	Researchers, Engineers	August 4th–6th, 2025
USENIX Security 2025	Systems research in all areas related to security and privacy.	NVIDIA	Related to the runtime monitoring of devices.	Academic and Industrial Researchers	August 13th–15th, 2025
ITSWC	Intelligent Transportation Systems	CMS	Discussion on CASTOR trust extensions and how they can be used for accommodating the establishment of secure and trustworthy CCAM environments.	Researchers, Engineers, Industrial Stakeholders, Policy Makers	August 24th–28th, 2025 (annual)
2025 International Conference on Information and Communication Security (ICICS 25)	Conference	UBITECH	Paper presentation: "Actions Speak Louder Than Words: Evidence-Based Trust Level Evaluation in Multi-Agent Systems" – CASTOR's deep dive into trust-aware network routing as part of traffic engineering efforts.	Researchers, Engineers	October 29th–30th, 2025

Event Name	Event Topic	Partner	Link with CASTOR	Target Audience	Date
Def.Camp 2025	Workshop	ORO	Orange has disseminated the overall architecture and use cases for CASTOR Horizon.	Researchers, Engineers	November 13th, 2025
TrustComm 2025	Conference	SURREY	Paper presentation: “An Improved Vector Commitment Construction with Applications to Signatures”.	Researchers, Engineers	November 14th–17th, 2025
HiPEAC Conference	RESCALE project workshop	SUITE5	Participation in RESCALE Workshop to present CASTOR project and its architecture.	Researchers, Engineers, Industrial Stakeholders	January 28th, 2026
IEEE CSR	Cyber Security/Resilience	QUBITECH	A PUF-Based Root-of-Trust for Resource-Constrained IoT Devices paper	Researchers, Engineers	Aug 4–6, 2025

During the **2nd reporting period (M19-M36) of the project**, the CASTOR partners look to actively participate in numerous evnts furthering the scientific dissemination to also industry-oriented events capturing also the results that will be extracted from the two-round experimentation phase. A non-exhaustive list can b found in the following table:

Table 2.4: Planned Participation in Events during the 2nd Reporting Period of the CASTOR Horizon Project

Event Name	Event Topic	Partner	Link with CASTOR	Target Audience	Date
32nd International Conference on Telecommunications (ICT)	Conference on network and telecommunications	FERON	Co-organizing Special Session: Mission Critical Services in 6G. Invited paper for CASTOR presentation.	Academic and Industrial Researchers	May 20th–22nd, 2026
IEEE International Conference on Communications (ICC)	Communications	ICCS	Participation in a panel session on secure orchestration capabilities.	Researchers, Engineers	May 2026

Event Name	Event Topic	Partner	Link with CASTOR	Target Audience	Date
EuCNC & 6G Summit	Networks & Communications	ICCS, ORO, Collins, UMU, UBITECH	Keynote talk on the trusted computing related activities of CASTOR and how these manifest the runtime monitoring of verifiable evidence based on which the trust assessment of the routing plane can be conducted.	Researchers, Engineers, Industrial Stakeholders, Policy Makers	June 2026
SecSoft 2026	Workshop	Several partners	Full-day workshop at IEEE NetSoft 2026, done by CASTOR together with several other projects from the Cybersecurity cluster.	Academic and Industrial Researchers	June 2026
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 CASTOR architecture with the TPM Automotive Working Group.	Researchers, Engineers, Industrial Stakeholders, Policy Makers	June 2026
The 22nd EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2026)	Conference	Surrey	A talk about the concept of attribute-based cryptography. These primitives can be used for CASTOR when integrity, confidentiality and authenticity are required.	Researchers	July 21st–24th, 2026
CSR 2026	Conference	UBITECH, QUBITECH	Papers regarding the post-quantum attestation schemes developed, as well as a novel Ising-PUF approach as an alternative Root of Trust.	Researchers	August 2026
35th USENIX Security Symposium	Systems research in all areas related to security and privacy	Surrey	Paper presentation: "FABS: Fast Attribute-Based Signatures".	Academic and Industrial Researchers	August 12th–14th, 2026

Event Name	Event Topic	Partner	Link with CASTOR	Target Audience	Date
ESORICS – European Symposium on Research in Computer Security	Computer and Network Security	FERON	Paper to be submitted: "Blockchain-based Trusted Routing for Multi-Operator 6G Networks" (working title).	Academic and Industrial Researchers	September 14th–18th, 2026
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
CASTOR's Research Workshop	Networking, Trusted Path Routing, Dynamic Trust Assessment	CASTOR Consortium	CASTOR's main scientific event, Advisory Board Meeting	Industry, SDOs, Researchers	2027
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.	Researchers, Engineers, Industrial Stakeholders, Policy Makers	Quarterly
RTX SEATN – Systems Engineering & Architecture Technology Network Symposium	Aerospace IT and Computing	Collins	CASTOR's aerospace use case.	Commercial aerospace engineers, designers, and decision-makers from one of the largest aerospace network providers in the world.	Annually
IEEE Vehicular Technology Conference	Automotive technologies for communications	FERON	Automotive use case results.	Academic and Industrial Researchers	Twice every year (Spring and Autumn)

CASTOR Scientific Workshops: CASTOR is planning to present its work and the resulting findings at a number of events. This will include the organization of CASTOR centred workshops for the dissemination of the CASTOR concepts and methodology with the practical demonstration of project results and the participation in international conferences with technical contributions and a project presence at the affiliated exhibitions. Furthermore, CASTOR consortium partners are participating in the organization of numerous workshops (under the umbrella of well-established scientific conferences) which will further trigger scintific debates over the main vision of the project towards establishing the next-generation secure Internet architecture. The present deliverable gives an overview of the present considerations, deliverable D7.3, due at the end of the project, will have the full report on CASTOR achieved organization/participation in conferences and workshops.

CASTOR plans to organize or to affiliate with several scientific workshops aimed at fostering dialogue between researchers, academia, and industry on building trust and resilience within the Compute Continuum.

Table 2.5: Scientific Workshops

CASTOR Scientific Workshops
CASTOR will be co-organizer of **SecSoft 2026**, together with the MIRANDA project, in the context of the 12th IEEE International Conference on Network Softwarization (NetSoft2026) that will be held from June 29 to July 3, 2026 in Berlin, Germany. The main purpose of the SecSoft workshop is to integrate the "Security, Safety, Trust and Privacy support in virtualized environments" conference topic. Beyond security mechanisms at the hypervisor or domain level, the softwarization of legacy security appliances, and federation schemes between multiple domains, this Workshop will look ahead to more dynamic, agile, and autonomic forms of detection and reaction of advanced threats, including the persistence ones. The specific focus will be on secure and trustworthy digital services, including pure virtual services as well as cyber-physical systems. The objective is to stimulate a constructive discussion on overall frameworks and specific aspects that are necessary to build wide situational awareness and to timely counter cyber-attacks: pervasive monitoring and deep inspection, cross-correlation in time and space dimensions and detection, automated control and management of complex orchestratable systems, forensics and legal investigation, trustworthiness and privacy. More information is available at: https://www.secsoft-workshop.org/.
CASTOR will be co-organizer of the **CyberShield Workshop**, in the context of the **2026 IEEE International Conference on Cyber Security and Resilience (IEEE CSR)**. The workshop focuses on cyber-resilience, secure systems, and trustworthy infrastructures, and is well aligned with CASTOR's objectives on trust-aware and secure networking across the compute continuum. More specifically, it constitutes a relevant scientific forum for addressing research challenges related to trustworthy service provisioning, dynamic trust assessment, runtime evidence collection, and secure orchestration across heterogeneous and multi-domain environments. It also provides an opportunity to discuss how resilience, assurance, and trustworthiness can be systematically integrated into the design and operation of next-generation networked systems. In this respect, the workshop offers an appropriate venue for disseminating and discussing CASTOR's research contributions on trusted path routing and continuum-wide trust engineering. More information is available at: https://www.ieee-csr.org/csr-cybershield/.
CASTOR will be leading the organization of a **Special Session on Mission Critical Services in 6G (SS6)** scheduled as part of the **International Conference on Telecommunications (ICT) 2026**, which will take place in Thessaloniki, Greece, from 20 to 22 May 2026. The coordination of this session will be undertaken by FERON Technologies and addresses research challenges that are highly relevant to CASTOR, including security, privacy, trust mechanisms, zero-trust architectures, dynamic trust management, and resilient communication systems for mission-critical environments. In this respect, the session provides a suitable scientific forum for discussing how trustworthy networking, service assurance, and resilience can be systematically incorporated into next-generation communication infrastructures. It also offers an appropriate venue for disseminating CASTOR's research perspective on trusted networking and secure service delivery in heterogeneous and mission-critical operational settings. More information is available at: https://ict2026thessaloniki.org/.
CASTOR will also be in the organization committee of a **Dagstuhl Seminar related to the emerging security needs in the CCAM domain** - titled *Trustworthy Generative AI for Connected and Automated Mobility*: As AI moves from pilots to operation in safety-critical domains, the limiting factor is no longer model accuracy alone but the ability to establish, carry, and act on trust throughout the lifecycle and across organisational and national boundaries. This is especially important in CCAM, where data and decisions are distributed among vehicles, infrastructure and services, and where safety and trustworthiness must be solved together. In CCAM, as the SRIA highlight, the end goal is not only trusted communication but trustworthy automated decision-making.

That creates a direct dependency between data-level trust assessments and model-level AI trustworthiness: if AI components cannot quantify and respect the varying trustworthiness of their inputs, even the most reliable V2X infrastructure can yield unsafe outcomes. CASTOR's dynamic trust characterization offers precisely these building blocks: evidence-based trust signals that can be propagated beyond per-message checks to inform how training datasets are curated and how models later adapt and behave. In this sense, CASTOR can also provide a CCAM-specific foundation that is compatible with broader trustworthy-AI practices now emerging in the CCAM community towards establishing trust functions for labelling the degree of belief on the data sources populating input and/or queries on the model itself. Within this context, the envisioned workshop will comprise researchers on all these overlapping technologies so as to identify a concrete roadmap for safet-critical trustworthy systems, grounded to policy-makers and industry practitioners.
As part of the dissemination activities of the 2nd reporting period, CASTOR envisions organizing a research workshop conceived as a scientific debate, revolving around the major research, engineering, and standardization challenges of trustworthy networking. The scope of the event extends beyond trusted path routing alone and covers broader questions related to trust-aware network control, secure service provisioning, resilience, runtime assurance, and trustworthy operation across heterogeneous and multi-domain infrastructures. The event will convene invited experts from academia, industry, and standardization bodies, including representatives from the IETF, the SCION association, and industrial actors active in secure and trustworthy networking. In this respect, the debate is intended to provide a structured forum for examining competing approaches, identifying unresolved bottlenecks, and discussing possible convergence paths for next-generation trustworthy networking frameworks. The main outcome shall be a consolidated roadmap capturing the main scientific and engineering showstoppers and outlining the directions required to advance trustworthy networking in zero-trust and below-zero-trust settings across the compute continuum.
CASTOR will host a **final event** alongside the project's concluding review in M36, with a focus on demonstrating the main technological achievements within the context of the planned use cases. Attendees will include engineers, researchers, policy experts, and members of the CASTOR external advisory board. The project will also invite representatives from standardization organizations to participate, aiming to present CASTOR's results and contribute to shaping future standardization efforts related to trusted path routing.

CASTOR Webinars and Technical Training Sessions: During the 2nd reporting period (M19–M36), CASTOR will organize a series of technical webinar and training activities targeting both internal and external audiences. These activities will be closely aligned with CASTOR's Open-Source Development strategy (Section 6) and will aim to support the dissemination, understanding, and potential uptake of the project's key exploitable results (KERs). The 1st integrated CASTOR framework is expected to become available around M21 of the project, whereas the final releases of the relevant CASTOR KERs are foreseen around M26. On this basis, a series of dedicated technical webinars will be organized for the individual KERs, presenting their architectural foundations, implementation aspects, and expected role within the overall CASTOR framework. The webinars will be complemented by technical sessions and hands-on demonstrations per KER, so as to provide a concrete view of the developed assets and enable more informed interaction with interested stakeholders from academia and industry.

2.3.3 CASTOR Publications:

Over the first reporting period, CASTOR has submitted and published more than (10) (peer-reviewed) papers in conferences and journals, contributing to the advancement of runtime security assurances in

the networking/telecommunications sector. Given the inherently multidisciplinary nature of the CASTOR framework, the project targets a wide range of scientific venues to share its research findings and engage into scientific debates with the broader academic and industry community. It is important to highlight CASTOR contributions into two main research avenues: First of all, in the context of accelerated and efficient monitoring of the runtime state of a VM or a container through only the VM introspection interface currently supported in all commodity operating systems. The developed ($BLUEGUARD$) framework [14] facilitates the runtime introspection of the CASTOR's TNDI [3] (containerized set of routing functions) based on which the trust characterization of the entire routing element is constructed. This novel set of VMI-based monitoring capabilities leverages the physically isolated Data Processing Unit (DPU) commonly found on data servers to efficiently run full system introspection by both host and guest introspection (HGI) without affecting the operational profile of the running applications. Secondly, as part of its crypto agility layer, CASTOR developed a new set of *attribute-based crypto constructions* to be tested for supporting the composite (path-level) attestation mechanism towards ensuing the correct node-level order in a constructed routing policy (enforced by the Path Computation Engine).

In addition to the already published scientific papers, CASTOR has already progressed with the submission of (3) additional manuscripts focusing on the integration of the CASTOR trust extensions into the B(5G) compute continnum. This acts as further evidence on the scientific impact of the ongoing research. This publication effort will continue and intensify throughout the second half of the project, where also the concrete outcomes of the evaluation and experimentation phase will become availble.

CASTOR's publications are openly accessible and hosted on Zenodo project account, ensuring broad dissemination and long-term availability within the research community.

Table 2.6: CASTOR Scientific Publications

Title of the Paper	Conference or Publication	Topic / Relevance for CASTOR	Partner
Risk Analysis for V2X Scenarios	International Symposium on Signals, Circuits and Systems (ISSSCS) 2025	Work presenting a detailed analysis of the threat landscape in the automotive application domain. This listing sets the scene for the Required Trust Level (RTL) calculation for this safety-critical application domain extending it also to path-oriented attack vectors - how such device-specific risks affect the degree of belief of the overall path establishment considering also possible cascading effects.	TUI
Standardisation of and Migration to Post-Quantum Cryptography	International Conference on Research in Security Standardisation	Position paper on the confidentiality, integrity, and availability requirements for decentralized systems as we are migrating into the post-quantuam era. This helps with the identification of the of those security mechanisms and constructions that ned to be replaced with their PQ equivalent so s to ensure the seamless transition over such legacy infrastructures.	University of Surrey

Title of the Paper	Conference or Publication	Topic / Relevance for CASTOR	Partner
A PUF-based Root-of-Trust for Resource-Constrained IoT Devices	IEEE CSR 2025	This work presents the use of lightweight Physical Unclonable Functions (PUFs) as a secure element based on which secure identification and (swarm) attestation capabilities can be exposed. At a later stage, CASTOR will manifest a detailed benchmarking of the critical security functions operationa over varying types of Roots-of-Trust.	UBITECH
Trust or Bust: Reinforcing Trust-Aware Path Establishment with Implicit Attestation Capabilities	IEEE CSR 2025	Detiled presentation and formal verification of CASTOR's novel implicit attestation scheme that enables the zero-knowledge verification of a Prover's configuration state correctness. The concep of ky restriction usage policies was introduced.	UBITECH
Actions Speak Louder Than Words: Evidence-Based Trust Level Evaluation in Multi-Agent Systems	International Conference on Information and Communications Security (ICICS) 2025	Work presenting the details and inner working of CASTOR's Trust Assessment Framework based on the use of Subjective Logic (SL). Concrete definitions of trust and trustworthiness are provided and associated with the need to also consider trust models capable of adapting to uncertainties and environmental changes.	UBITECH
Comparative Performance Analysis of Lightweight Cryptographic Algorithms on Resource-Constrained IoT Platforms	Sensors 2025, 25(18), 5887	Work on documenting a baseline of performance results of the "AS-IS" operational scenario of CASTOR's automotive use case considering the (Vehicle-Network-Vehicle) system model.	TUI
Attribute-Based Key Exchange with Optimal Efficiency	International Conference on Cryptology and Network Security	Work on the novel crypto agility layer of CASTOR employing attribute-based signcryption for protecting the communication and sharing of extracted runtime evidence.	University of Surrey
An Improved Vector Commitment Construction with Applications to Signatures	22nd EAI International Conference on Security and Privacy in Communication Networks, 2026	Presentation of the novel signature scheme allowing for the multi-order signature construction enforcing the correct path-specific order of CASTOR's composite attestation scheme.	University of Surrey
FABS: Fast Attribute-Based Signatures	35th USENIX Security Symposium, 2026	Provision of new crypto constructions allowing for efficient attribute-based signatures featuring strong holder- and device-binding properties..	University of Surrey
BlueGuard: Accelerated Host and Guest Introspection Using DPUs	34th USENIX Security Symposium, 2025	Provision of a set of accelerated introspection capabilities setting the baseline for CASTOR's tracig units to enable the monitoring and observation of the runtime state of the target routing element	NVIDIA

Title of the Paper	Conference or Publication	Topic / Relevance for CASTOR	Partner
TALOS: Reinforcing Secure Live Migration through Verifiable State Management	Transactions on Dependable Computing, 2026 (UNDER SUBMISSION)	Novel methodology allowing for the live migration of the runtime state of an (enclavized) application in case of detecting an incident of risk. This work also contains the baseline of the *kernel extensions* that will be leveraged in CASTOR faciliating the monitoring of the system calls executed within a containerized vRouter.	UBITECH
Slice & Dice: Privacy-Preserving Layered Attestation via Active Memory Introspection	ACM SECRYPT Conference, 2026 (UNDER SUBMISSION)	This work presents the details of CASTOR's layered attestation scheme allowing for the efficient and scalable verification of onboarded routing functionalities operating under different trust assumptions.	UBITECH
Slice & Dice: Privacy-Preserving Layered Attestation via Active Memory Introspection	ACM SECRYPT Conference, 2026 (UNDER SUBMISSION)	This work presents the details of CASTOR's layered attestation scheme allowing for the efficient and scalable verification of onboarded routing functionalities operating under different trust assumptions.	UBITECH
NESTOR: A Wise Counsellor for Building the B5G Trust Plane	Transactions on Dependable Computing (TDSC), 2026 (UNDER SUBMISSION)	Documentation of the first archetype integrating CASTOR's trust assessment layer (*trust plane*) as well as the novel *composite attestation* capabilities for enhancing the operational assurance of 6G srvice-graph-chains.	UBITECH

Chapter 3

Clustering and Standardization Activities

In the following chapter, we document the project's active participation in activities organized by clusters/associations relevant to CASTOR results, especially as it pertains to **extending the trusted path routing mechanisms:** from static operational blocks (focusing on the establishment of trusted route configurations between routing elements verified only during the onboarding phase) to runtime, continuous trust assessment enablers. CASTOR partners managed to not only establish liaisons with the core community of IETF RATS and NASR but also participate as editors in many of the ongoing activities in the realted working groups. Highlight of these activities culminated in CASTOR's leading position in the IETF Trusted Path Routing series of drafts outlining architectural challenges and open issues in extending the Trusted Path Routing model to include runtime trust assessment and monitoring[1].

Furthermore, focus was also given to activities related to the core enabling technologies behind CASTOR's vision in trusted computing (Trusted Computing Group), agile crypto constructions for the novel composite attestation scheme (ISO) as well as 5GAA and CCAM communities (related to the safety-critical automotive domain) with the objective of testing the adoption of CASTOR by the industrial community. Activities at AIOTI, the CAR 2 CAR Communication Consortium and data spaces communities further strengthen the establishment of relationships with community stakeholders, such as cybersecurity and routing technology vendors who can benefit from CASTOR artefacts to address the existing challenge for further securing the Internet.

3.1 Clustering Activities

This section reports on CASTOR's participation in collaborative ecosystems, associations, and community-driven initiatives that are relevant to the project's technological scope and expected impact. Given that CASTOR operates at the intersection of trustworthy networking, trusted computing, secure orchestration, next-generation communications, and trust-aware service provisioning across the compute continuum, clustering is treated not merely as a dissemination instrument, but as a strategic mechanism for knowledge exchange, liaison building, validation of research directions, and preparation of longer-term uptake. Through its engagement with communities such as ECSCI, ETSI-related initiatives, 6G-IA, and 5GAA, CASTOR seeks to position its results within the broader European and international landscape and to establish meaningful synergies with initiatives addressing resilient, secure, and trustworthy digital infrastructures.

These interactions are expected to strengthen the visibility and relevance of CASTOR's technical outcomes, while also enabling dialogue with researchers, industry stakeholders, policy actors, and standardization oriented communities. In parallel, clustering activities provide an important channel for cross-fertilisation with adjacent projects and communities working on critical infrastructure protection, B5G/6G

[1] This work has been published as an ongoing draft that can be found online: draft-rats-runtime-tpr-00

systems, CCAM, and secure distributed service environments. In this respect, the clustering activities described in the following subsections support the progressive alignment of CASTOR's emerging artefacts with real-world requirements, adoption pathways, and the evolving European discourse on cybersecurity, trustworthiness, and resilient compute continuum architectures.

3.1.1 ECSCI

The European Cluster for Securing Critical Infrastructures (ECSCI) [10] is a cluster of EU-funded research and innovation projects in the field of cyber-physical protection of critical infrastructures (CIP). The main objective of the ECSCI cluster is to create synergies and foster emerging disruptive solutions to security issues via cross-projects collaboration and innovation. Research activities focus on how to protect critical infrastructures and services, highlighting the different approaches between the clustered projects and establishing tight and productive connections with closely related and complementary EU funded projects. To promote the activities of the cluster, ECSCI organizes international conferences, and national or international workshops, involving both policy makers, industry and academic, practitioners, and representatives from the European Commission.

ECSCI members share knowledge and best practices about CIP in different sectors. The cluster focuses on research and innovation outcomes on the protection and security of critical infrastructures and services, respecting the different approaches, CI sectors focusing, target audience, etc. between the projects, while establishing tight and productive connections with closely related or complementary ones.

ECSCI, as a collaborative ecosystem on critical infrastructures protection, collaborates on the following areas:

- Scientific collaboration in the form of joint workshops and conferences, and co-writing of scientific publications;
- Technical collaboration such as sharing approaches on cyber-physical security, risk assessment, and predictive analytics;
- Communication and dissemination of cluster's activities and outputs through a common web and social media presence, and organization of joint events;
- Building and fostering stakeholders' alliance (mobilisation of local ecosystems);
- Marketplace extension of members' products and services across various sectors and stakeholders.

As a result, collaboration and knowledge sharing among experts in the field is critical for ensuring the security and readiness of European critical infrastructures and services. In this direction, the ECSCI cluster tries to consolidate and reflect a European approach by engaging in various common activities:

- Contribution to standards and regulations on the protection of Critical Infrastructures;
- Joint scientific publications, including a broad spectrum of respective books;
- Workshops and events on critical infrastructure protection, with keynote speakers from policy making, academic and industrial sector;
- A platform for combined safety and security for European Critical Infrastructures.

CASTOR officially participates in ECSCI since November 2025 and actively targets at clustering activities in the following fields:

- **Scientific impact:** During the CASTOR project, the consortium aims to produce several scientific publications that contribute to the advancement of security assurance in the Telecommunications sector. CASTOR's framework is inherently multidisciplinary. Enabling compute continuum-wide trusted path establishment, building blocks and fundamental pillars for the dynamic detection of any indication of risk over critical infrastructures and based on them, representation of a network-centric trust model. CASTOR's publications are openly accessible and hosted on Zenodo, ensuring broad dissemination and long-term availability within the research community.
- **Contributions to Standards:** CASTOR envisions to actively contribute to the security and interoperability efforts regarding future-proofing safety-critical application workloads. 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.
- **Participation in Workshops:** 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. CASTOR consortium has already attended and will continue to organize/attend a series of events to showcase the project's solutions and Use Cases to a broad audience.

3.1.2 ETSI

ETSI (European Telecommunications Standards Institute) is the most important Standard Development Organization (SDO) on key global telecommunication, broadcasting, and information and communication technologies (ICT) in Europe providing thousands of standardisation deliverables every year. They take various forms, such as Technical Specifications (TS), Technical Reports (TR), European Standards (EN), Guides and Special Reports. The documents are drafted by Technical Committees (TCs) organized by technology specific Working Groups (WGs). Although ETSI's impact is essentially European, it has global technology development effects worldwide.

ETSI ITS (TC on Intelligent Transport Systems) is a fundamental standardisation pillar of ETSI and, from the point of view of the CASTOR use cases, it is one of the most important technical committees which develops standards for connected and automated mobility (CAM) and Automated Driving (AD). Within ETSI TC ITS, which is concerned with the creation of standards enabling the deployment of intelligent transportation systems, the activities of WG5 focus on the security and privacy aspects related to the exchange of information between entities.

ETSI TC ITS WG5 has published several technical specifications that collectively establish the current framework for secure and trustworthy communication among vehicles and infrastructure components. The technical specification ETSI TS 102 940 [2], in particular, specifies the ITS communications security architecture and management. In this context, Misbehaviour Detection is introduced as the functionality that performs checks on the incoming V2X messages; the Misbehaviour Authority is a remote entity able to process Misbehaviour Reports sent by the stations, with the aim of identifying stations that are sending incorrect data.

CASTOR's representation in ETSI: CASTOR takes an active role in the international standardization and standards making processes in Europe through its (CMS) partner. CMS is voting member of various ISO, SAE, IEEE, and more specifically ETSI ITS in the C-ITS and V2X/V2N related areas. It also contributes, in various forms, to the technical specification and policy making processes in 5GAA and Car2Car.

[2] ETSI, TS 102 940, "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2", 2021.

CMS is the rapporteur of standards in ETSI ITS and takes part in the technical specification of various work items, including work on ETSI TS 103 759 [3] focusing on the specification of dissemination protocols that can securely communicate messages outputted from integrated detection mechanisms such as Misbehaviour Service Reports. **CASTOR aims to present its use cases on the establishment of trustworthy paths that can accommodate the reliability and availability requirements of the transmission of such messages.** CMS is represented through its delegated in regular ETSI meetings where the CASTOR's project knowledge and experiences will be efficiently shared. The goal is for CASTOR to participate in the ETSI Security Conference (2027) for presenting its work on continuous and cooperative trust management of resilient CCAM listing all core principles that need to be adopted for adopting such dynamic trust extensions in such a safety-critical and well-regulated application domain.

Through their company delegates CMS will officially propose further development and/or extension of existing security and trust related standards in cases when missing features and/or functionalities are identified with regard to relevant standard documents. This also includes the systematic monitoring of ITS WG5 activity (security). In this respect the immediate feedback of validation results of experimental technical solutions of CASTOR to the standard development process is crucially important.

CASTOR's representation in ETSI SDG: In addition to the core TC activity, ETSI Software Development Groups (SDGs) are tailored for collaborative software development in support of the standardisation work done in the TC's. The Software Development Group OpenSlice (SDG OSL), *e.g.,* is developing an open-source, intelligent Operations Support System (OSS) to deliver Network-as-a-Service (NaaS), based on TM Forum's Open Digital Architecture (ODA) recommendation.

UBITECH and UMU, within ETSI OSL WG, are involved in the evolution of OpenSlice in order to support security requirement in the Application Onboarding taking into account TMF specifications. TMF921 intents allows specification of the requirements for the service provision, and in that sense the work focus on security intent processing workflows: registration, translation, refinement, prioritisation. At the end the main interest is on how to support the onboarding and deployment of the SSLA defined in the CASTOR architecture and how to integrate it in the orchestration of the service.

3.1.3 6G-IA

The 6G Smart Networks and Services Industry Association (6G-IA) [12] represents Europe's private sector in next-generation network research. It holds a central role in 6G innovations, their evolution as well as the promotion of EU-funded research under the Smart Network and Services (SNS) Joint Undertaking.

A dedicated Working Group of 6G-IA addresses innovation challenges at the intersection of Connected and Automated Mobility (CAM) with the 6G networking technology. It essentially acts as a knowledge hub for partners of the automotive and (6G) network connectivity expertise with participants representing entities that are typically active in Research and Innovation projects funded by the European Commission. The main focus of the WG lies on connected mobility use cases and their deployment.

CASTOR has established some communication links (through ICCS) with the aforementioned working group, informing (currently through unofficial discussions) the group about the automotive relevance of the CASTOR innovation (see the CASTOR CMS and TUIASI use-cases). A short presentation of the automotive CASTOR use cases and their findings in the WG will be conducted by the time a considerable body of CASTOR experimentation results will be formed.

CASTOR also has synergies with other 6G-IA projects related to security aspects. In that sense, UMU as chair of the Security WG is leading presentations of different projects in order to discuss enablers and approach for the orchestration of the security where CASTOR will contribute. Additionally, UMU has

[3] ETSI, TS 103 759, "Intelligent Transport Systems (ITS); Security; Misbehaviour Reporting service; Release 2", 2023.

promoted a workshop in the context of EuCNC2026 (pending approval) where CASTOR will be presented as part of the discussion between different projects,

3.1.4 5GAA

The 5G Automotive Association (5GAA) is a global, cross-industry organization 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, auto-motive players (like vehicle OEM manufacturers, OEM suppliers, system integrators, etc.) that work on vehicle platforms, hardware, and software solutions. 5GAA has more than 120 industry members, including automotive manufacturers, tier-1 suppliers, chipset/communication system providers, mobile operators, and infrastructure vendors. Several activities within 5GAA can be considered in synergy with the concept of trust:

The recent 5GAA study on Cybersecurity for Edge Computing [4] argues that at the moment is not possible to establish mutual trust between MEC applications and MEC platforms, and presents an analysis of the technological gap existing at the moment for achieving trust in such environments for the automotive domain. The problem of assessing the trustworthiness of geolocation information is specifically analysed in the recent report [5]. When OEMs receive V2X messages which include positioning information they do not know what level of trust they can associate to the received content and as such they do not know whether the car OEM can exploit the information.

- Another recent report [6] elaborates on mutual trust concept from the safety perspective, underlying security concepts (e.g., similar to the Protection Profile V2X Hardware Security Module currently under discussion in the C2C-CC).

CASTOR has established a liaison with 5GAA and regularly reports the project results to the 5GAA participants, arguing on the relevance to current activities in the association. In addition to that, CASTOR contributed to two white papers published from 5GAA:

- One [7] on defining the problem of trust establishment for connected and automated vehicles. This White Paper communicates the work on the definitions of trustworthiness, the need to have dynamic trust assessment based on verifiable evidence, and the need to build trust assessment framework that can reason with uncertainty. The document also defines a shared vocabulary and definitions relevant to trustworthiness and trust in mutli-agent environments, and develops a taxonomy of trust properties and trust sources and emphasises the importance of performing this assessment dynamically and in real time. It explicitly defines the CASTOR concepts of ATL and RTL and emphasizes that verifying evidence is a key part of the approach to trust assessment. **rust4CAV White Paper:** CASTOR joined the working item titled "*Trust4CAV*" that produced a white paper on "*A Framework for Dynamic Trustworthiness Assessment in Cooperative and Automated Vehicles" (5GAA, 2025)*". This work formally defines a structured, modular methodology for calculating both Actual Trustworthiness Level (ATL) and Required Trustworthiness Level (RTL), as originally introduced and defined within the CASTOR project (Deliverables D3.1 and D3.2). The methodology is defined in a generic way, in order to allow industry partners to adopt it and incorporated it in their own processes.

[4] 5GAA, "Cybersecurity for Edge Computing", 2023.
[5] 5GAA, "Trustable Position Metrics for V2X Applications", Sept. 2023.
[6] 5GAA, "Safety Treatment in Connected and Automated Driving Functions Report", Mar. 2021.
[7] 5G Automotive Association (5GAA). Creating Trust in Connected and Automated Vehicles. White Paper Trust4Auto, May 2024.

a new White Paper that is dedicated in defining the problem of trust establishment for connected and autorotated vehicles. This White Paper communicates the work from D3.1 ”Architectural Specification of CONNECT Trust Assessment Framework, Operation and Interaction” [2] and D2.1 ”Operational Landscape, Requirements and Reference Architecture – Initial Version” [1] on the definitions of trustworthiness, the need to have dynamic trust assessment based on verifiable evidence, and the need to build trust assessment framework that can reason with uncertainty. More specifically, the contribution of CONNECT to the 5GAA White Paper “Creating Trust in Connected and Automated Vehicles” is to explicitly describe how to address the challenge of dynamic trust assessment from the perspective of CONNECT and the work described in D3.1 [2] and D2.1 [1]:

3.2 Standardization Activities

The following section presents CASTOR’s standardization-oriented activities, which constitute an important component of the project’s effort to position its research outcomes within the broader technological and regulatory landscape of trustworthy networking. Given that CASTOR addresses challenges spanning trusted computing, attestation, cryptographic building blocks, trust-aware routing, and secure orchestration across heterogeneous compute continuum environments, engagement with standardization and pre-standardization processes is essential for ensuring relevance, interoperability, and longer-term uptake. To this end, CASTOR partners participate in and monitor activities in bodies such as the IETF, the Trusted Computing Group (TCG), and ISO/IEC, contributing expertise in areas that are directly connected to the project’s technical scope. The following subsections summarize these activities and highlight how CASTOR’s research directions interface with ongoing efforts in trusted computing, secure protocol design, and trustworthy networked infrastructures.

3.2.1 IETF

The Path Computation Element (PCE) is an IETF-defined network component responsible for calculating optimal routes across complex, multi-domain, or multi-layer networks by applying advanced algorithms and traffic engineering policies. It operates centrally and interacts with routers through the Path Computation Element Communication Protocol (PCEP), enabling dynamic and efficient path setup essential for MPLS-TE and GMPLS environments. A recent research extension introduces an *Enforcement Extension* module that bridges computation and configuration by directly applying path decisions on network devices. This innovation ensures that calculated paths are not only suggested but actively enforced, improving network reliability and consistency in path deployment.

Complementing this, the IETF’s Trusted Path Routing (TPR) framework integrates trust assessment into routing decisions via the Remote Attestation Procedures (RATS). In traditional models, device trust is verified at onboarding using boot-time evidence such as configuration measurements or hardware-based attestations (e.g., TPM, TEE), resulting in a binary and static trust posture. However, this approach is limited for dynamic or multi-tenant contexts where trust may shift over time. The proposed enhancement introduces continuous attestation, collecting real-time telemetry and integrity data to derive up-to-date trustworthiness scores. These scores are then integrated into control plane routing processes—like PCE or Segment Routing Traffic Engineering (SR-TE)—to prioritize routes formed exclusively of verified, trustworthy devices, ensuring adaptive and security-aligned network operation.

CASTOR has been involved in IETF and specifically became an editor on IETF RATS on Trusted Path Routing Working Item: There was a draft created on Extending Trusted Path Routing for ensuring the extension of the current scheme that only attested and trustworthy network devices are included in routing decisions. In this model, each forwarding element is evaluated by a Verifier prior to its inclusion in a trusted network domain. Evidence about the device’s integrity is assessed to determine its eligibility for

participation in the routing topology. While this enrollment-time verification establishes a baseline of trust, it does not account for the fact that a device's trustworthiness may change over time. If a device becomes misconfigured, compromised, or enters a degraded trust state after initial enrollment, this change should be reflected in the trusted path routing decisions. The TPR model, as currently defined, provides no mechanism to detect or respond to such changes. Extending it with a runtime trust assessment phase raises several open issues that we need to resolve. *CASTOR keeps on working in this item with the endmost goal to publish a new TPR draft merging together static- and runtime trust extensions based on the work demonstrated in Deliverables D3.2 and D3.3*.

Furthermore, CASTOR's work on advancing privacy-preserving attestation standards was endorsed by the IETF RATS Working Group. More specifically, IETF published a new Internet-Draft, Direct Anonymous Attestation for the Remote Attestation Procedures Architecture, which integrates the Direct Anonymous Attestation (DAA) implementation developed by CASTOR. This advancement consolidates privacy-preserving platform authentication and attestation, fully aligned with the IETF RATS standards,an important step toward more secure and trustworthy digital infrastructures. CASTOR leverages these same trusted computing principles to enable the establishment of secure and trusted "service segments" that operate on top of attested and verified routing elements across the continuum. The work presented in IETF sets the scene for CASTOR's novel composite attestation designs that are under construction and will be presented as part of IETF's Trusted Path Routing draft work.

3.2.2 TCG

Trusted Computing Group (TCG) is a not-for-profit global organization established for the development, definition and promotion of open and global industry standards, targeting to support a hardware-based root-of-trust, for interoperable trusted computing platforms. For this purpose, TCG aims to the enablement of secure computing, through the development of open standards and specification in the cybersecurity field. As far as the standardisation is concerned, TCG is widely recognised as an accepted standardisation group, at a global scale, setting standards in all relevant technologies and innovation on Trusted Computing (TC) and relevant assurance and attestation schemes.

CASTOR has a continuous participation in TCG members meeting: At the 2024 TCG meeting held in June in Athens, Greece, CASTOR presented extensions to the Trusted Computing Base (TCB) related to attestation, including mechanisms for configuration integrity verification, Verifiable Policy Enforcement (VPE), and other critical operations. Additionally, the live migration scheme was demonstrated. During the 2025 TCG meeting held in June in Amsterdam, Netherlands, CASTOR elaborated on the Threshold Direct Anonymous Attestation (DAA) protocol developed within the project. It is worth noting that the DAA implementation was endorsed by the trusted software stack, ensuring secure integration and compliance with TCG standards.

3.2.3 ISO

CASTOR, through SURREY, has been involved in ISO/IEC JTC1 SC27 WG2 – Cryptography and Security Mechanisms, contributing in the standardisation of cryptographic mechanisms. Currently, Professor Liqun Chen (Surrey) is serving as a co-editor for the following three projects:

- ISO/IEC 20008-3 Information technology – Security techniques – Anonymous digital signatures – Part 3: Mechanisms using multiple public keys.
- ISO/IEC 18014-1:2008 Information technology – Security techniques – Time-stamping services – Part 1: General – Amendment 1.

- ISO/IEC 18014-1:2008 Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens – Technical Corrigendum.

In addition, Prof. Liqun Chen also serves as the deputy chairman of Technical Subcommittee 2 of BSI IST/33, dealing with cryptographic mechanisms and providing input to ISO/IEC JTC1/SC27, on Information security, cybersecurity and privacy protection. In general, the BSI IST/33-2 IS responsible for representing the UK in ISO/IEC JTC 1/SC 27/WG 2, focusing on cryptographic techniques, including cryptographic key management and entity authentication protocols. At the same time, BSI IST/33 also provides input to CEN/CLC JTC 13/WG 10, which reviews national and international standards for adoption as European standards in the field of cryptography, including post-quantum cryptography. In CASTOR, we need to design an ordered multi-signature scheme for evaluating the number and order of routers in an enforced routing path. To achieve this, we may refer to building blocks used in anonymous digital signatures, such as PS signature, schnorr signature to design multi-signature with time-stamp style technique to prove order. Further, considering the transition to post-quantum cryptography, experience and activities in post-quantum cryptography, can help with coming up with post-quantum version of cryptographic primitives designed for CASTOR. This can help us be well-prepared for post-quantum era.

Moreover, CASTOR through QUBITECH contributes to the standardisation perspective of CASTOR through its work on the Optimization Engine, where trusted path routing is investigated using quantum and quantum-inspired optimisation methodologies, including QUBO/Ising-compatible formulations. At present, formal standardisation activity specifically targeting quantum annealing, quantum-inspired optimisation, simulated bifurcation, or QUBO/Ising-based optimisation appears to remain limited. However, closely related standardisation and pre-standardisation efforts do exist and are relevant to the framing of this work. In particular, QUBITECH follows ISO/IEC 4879:2024 on quantum computing vocabulary, which provides the emerging terminology baseline for concepts such as quantum annealing, as well as adjacent IEEE-oriented standardisation efforts identified in recent quantum-technology roadmaps, such as P3120 on quantum computing architecture and P3155 on programmable quantum simulators [13, 7, 11]. These activities do not directly standardise trusted path routing optimisation, nor do they yet define a dedicated framework for QUBO/Ising or simulated bifurcation methods. Nevertheless, they provide the closest current standardisation context for aligning CASTOR's optimisation research with the evolving conceptual, algorithmic, and architectural landscape of quantum and quantum-inspired computation [13, 7, 11].

3.2.3.1 JTC1 SC27 (Cybersecurity and Privacy)

ISO/IEC JTC1 SC27 on cybersecurity and privacy has several projects of interest in which CASTOR is involved:

- ISO/IEC 27115 (cybersecurity evaluation of complex system) [8]. The development of this standard started at the end of 2023. It takes an architecture approach to address the evaluation of complex system. It includes both complex systems and systems of systems. The project has studied the case of connected vehicles as a use case. As of today 27115 is going to get at CD stage, with probably two parts, one on the framework and one on cybersecurity architecture examples. We plan with the support of Ubitech to submit a CASTOR based consideration.
- ISO/IEC 27116 (customised and multipurpose evaluation) [9]. This preliminary work item was started in 2024. It is addressing the problem of multi-purpose evaluation either for multiple systems (e.g. data management system and IoT device) or for multiple regulations (e.g., AI compliance and cybersecurity compliance). The project has studied the case of connected vehicles with two compliance purpose: one on data management and one on the vehicle gateway. As of today 27116 is going

[8] WD TS 27115 ISO/IEC. Cybersecurity evaluation of complex systems introduction and framework overview, 2025.
[9] WD TS 27115 ISO/IEC. "customised and multipurpose evaluation", 2025.

to be a structured into two parts: one on the framework and one on practical examples. Again CASTOR can also be used as an example for the second part.

- ISO/IEC 27568 (security and privacy of digital twins) [10]. The development of this standard started in 2025 as the result of a preliminary work item (2023). CASTOR will provide the connected vehicle use case, and considerations on digital twin off- loading will be based on the results of the project. 27568 was approved in July 2025. CASTOR use case was submitted during the preliminary work item stage.
- ISO/IEC 27090 (Guidance for addressing security threats and failures in artificial intelligence systems) [11] and ISO/IEC 27091 (AI privacy protection) [12]. The development of those two standards started in 2022 and 2023 respectively. Since a CCAM infrastructure can contain AI capabilities, CASTOR is monitoring their development.

[10] TS 27568 ISO/IEC, 2023.

[11] DIS 27090 ISO/IEC. Cybersecurity — artificial intelligence — guidance for addressing security threats and failures in artificial intelligence systems, 2024.

[12] CD 27091 ISO/IEC. Cybersecurity and privacy — artificial intelligence — privacy protection, 2025.

Chapter 4

Synergies with Related Projects

Towards disseminating the work performed by the CASTOR consortium for ensuring secure path routing in the compute continuum, one of the main targets of the CASTOR project is to establish concrete liaisons with other EU-funded projects in the cybersecurity domain, and especially in the topic of secure edge-cloud continuum.

As such, within the first reporting period of the project (October 2024-March 2026), CASTOR has already created synergies with other EU-funded projects that have spread awareness about each project's objectives and leveraged knowledge among the consortia. These collaborations will drive further activities during the second reporting period (April 2026-September 2027) when CASTOR and the rest of the projects will exchange and disseminate their system development and validation results in various interested audiences to showcase the realization of trustworthiness establishment in the compute continuum. Especially regarding the cross-project leverage of development results, CASTOR envisages to collaborate with MIRANDA and INTACT projects towards using their Digital Twin initiatives for further strengthening the dynamic trust assessment capabilities of the compute continuum in CASTOR. Moreover, CASTOR will utilize ENTRUST project outcomes for the advancement of Secure Oracle developments in the underlying Blockchain Infrastructure, while cooperating with other projects, such as HEISINGBERG, in the enhancement of secure path routing optimization.

4.1 MIRANDA

Project Name	MIRANDA [21]
Project title	Monitoring, Investigation and Response to cyber-attacks with an Adaptive digital twiN moDel for Agile services over the computing continuum
Topic	HORIZON-CL3-2023-CS-01-01 - Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)

Project Name	MIRANDA [21]
Description	The growing level of interconnectedness of digital services and infrastructures creates tight and recursive security interdependencies between their providers, which are challenging to address due to the fragmentation of cybersecurity operations. This requires each provider to improve the security posture of its suppliers. However, existing practice, largely based on human interaction for disclosing vulnerabilities, reporting alerts, and suggesting remediations, demonstrates to be largely ineffective and risky. The MIRANDA project aims at operationalising awareness and remediation controls for service supply chains, by addressing feasibility, acceptance, and compliance issues. To this purpose, MIRANDA develops a Cybersecurity Digital Twin (CDT) to model and capture the security posture of such interconnected systems, which is used to detect, hunt, and remediate threats and attacks. The CDT will feature: i) functional and topological representation of digital services; ii) bidirectional control/monitoring data flow with real systems; iii) modelling and behavioural prediction of individual components and whole systems; iv) opaque representation of suppliers' assets based on confidentiality and privacy requirements. The framework also encompasses the necessary security controls to safely exchange data and controls between providers. On top of the CDT abstraction, MIRANDA builds adaptive and automated processes for threat hunting, detection of lateral movements, and eradication of the root causes of attacks. Validation of individual components and the overall MIRANDA platform will be conducted in three relevant Use Cases, covering different platforms for Smart City services. The purpose will be to demonstrate the adaptability to the evolving context and the effectiveness to stop latest-generation cyber kill-chains and lateral movements across digital chains. The Project will also consider the new business and operational models that are required to run the platform.
Liaison with CASTOR	Since its very early phase, the CASTOR project came in contact with the MIRANDA project as they both belong to the same call topic. The two projects established a robust liaison with dedicated calls and presented their collaboration through their project websites and corresponding social media posts. Moreover, CASTOR and MIRANDA promoted each other's material in social media and are both participating in the ECSCI cluster. In addition, CASTOR and MIRANDA have already started the organisation of the joint SecSoft2026 workshop that will take place in the context of the 12th IEEE International Conference on Network Softwarization (NetSoft2026) from June 29 to July 3, 2026 in Berlin, Germany. CASTOR and MIRANDA will also pursue further collaboration activities with the organisation of workshops and webinars within the 2nd reporting period, promoting their developed systems and evaluation results.

4.2 ENTRUST

Project Name	ENTRUST [16]
Project title	ENsuring Secure and Safe CMD Design with Zero TRUST Principles

Project Name	ENTRUST [16]
Topic	HORIZON-HLTH-2022-IND-13-01 - Enhancing cybersecurity of connected medical devices
Description	Cyberattacks targeting healthcare networks could potentially compromise clinical data, personal health information and proprietary research initiatives. The EU-funded ENTRUST project will seek to tackle the lack of cybersecurity implementations in connected medical devices without limiting their wide applicability. The proposed trust management architecture will dynamically and holistically manage the life cycle of connected medical devices, strengthening trust and privacy in the entire medical ecosystem. This includes formally verified trust models, risk assessment processes, secure life cycle procedures, security policies, technical recommendations and real-time conformity certificates. The added value and effectiveness of the ENTRUST Trust Management Framework will be validated and evaluated in four real-world use cases ranging from wearable and medical devices used for remote patient monitoring to high-end stationery equipment used in hospitals and clinics. Aligned with the guidelines of the Cybersecurity Act and the existing guidance on cybersecurity for medical devices, ENTRUST envisions a Trust Management Architecture intended to dynamically and holistically manage the lifecycle of connected medical devices, strengthening trust and privacy in the entire medical ecosystem. Even from the proposal stage, ENTRUST has identified gaps and necessary revisions of the current guidance (e.g. absence of post-market conformity and certification, real-time surveillance and corrective mechanisms). Towards that ENTRUST will leverage a series of breakthrough solutions to enhance assurance without limiting the applicability of connected medical devices by enclosing to them cybersecurity features. The project will introduce a novel remote attestation mechanism to ensure the device's correct operation at runtime regardless of its computational power; will be efficient enough to run in also resource-constrained real-time systems such as the medical devices. This will be accompanied by dynamic trust assessment models capable of identifying the Required Level of Trustworthiness (RTL) per device and function (service) that will then be verified through a new breed of efficient, attestation mechanisms (to be deployed and executed during runtime). This will also enable us to be aligned with the existing standards on defining appropriate Protection profiles per device (especially considering the heterogeneous types of medical devices provided by different vendors with different requirements) including Targets of Validation Properties to be attested during runtime. The motivation behind ENTRUST is to ensure end-to-end trust management of medical devices including formally verified trust models, risk assessment process, secure lifecycle procedures, security policies, technical recommendations, and the first-ever real-time Conformity Certificates to safeguard connected medical devices.
Liaison with CASTOR	CASTOR established a constructive liaison with the ENTRUST project through dedicated calls, where the focus was given in the leverage of knowledge regarding the Trust Assessment Framework and specifically, how lessons learned in ENTRUST about trustworthiness establishment could be exploited in CASTOR design and development activities. The two projects presented their collaboration through their project websites and corresponding social media posts, while promoting each other's material in social media.

4.3 RESCALE

Project Name	RESCALE [22]
Project title	Revolutionised Enhanced Supply Chain Automation with Limited Threats Exposure
Topic	HORIZON-CL3-2022-CS-01-02 - Trustworthy methodologies, tools and data security “by design” for dynamic testing of potentially vulnerable, insecure hardware and software components
Description	In the digital age, the integrity of supply chains is under threat, with cyber threats looming large over software and hardware components. Vulnerabilities in third-party segments further exacerbate the risk, demanding a robust solution to ensure the security of our interconnected systems. In this context, the EU-backed RESCALE project aims to transform supply chain security. Specifically, the project will automate evaluations, fortify against vulnerabilities, and institute rigorous cybersecurity audits. This initiative represents a response to the critical need for a secure-by-design approach in our increasingly interconnected world. By automating software and hardware evaluations, ensuring vulnerability-free third-party segments, and implementing robust cybersecurity audit procedures, RESCALE is pioneering an approach that could redefine the future of digital supply chains. RESCALE aims at designing, building, and demonstrating secure-by-design supply chains. To this end, RESCALE will (i) automate the evaluation processes of both software and hardware components, (ii) ensure that third-party segments are free from vulnerabilities, (iii) offer effective audit procedures for cybersecurity testing, and (iv) enable the construction of secure systems with the strongest possible guarantees. Overall, RESCALE will systematically analyse and extend, as necessary, every hardware and software layer in a computing system and apply novel tools and methodologies at every step of the entire supply chain.
Liaison with CASTOR	CASTOR established a significant liaison with the RESCALE project through active collaboration of their consortia representatives in discussions on critical cybersecurity issues on software. This synergy resulted in the participation of the CASTOR project in the RESCALE workshop on 28/01/2026 within the HiPEAC Conference that took place in Krakow, Poland. CASTOR presented there its vision and system architecture and leveraged experiences on cybersecurity threats. Moreover, the two projects presented their collaboration through their project websites and corresponding social media posts, while promoting each other’s material in social media.

4.4 INTACT

Project Name	INTACT [19]
Project title	integrated software toolbox for secure IoT-to-Cloud computing
Topic	HORIZON-CL3-2023-CS-01-01 - Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)

Project Name	INTACT [19]
Description	As our world becomes increasingly connected, protecting data and infrastructure in the IoT-to-cloud continuum – infrastructure that links our smart devices with cloud services – is crucial. The EU-funded INTACT project plans to develop an integrated software toolbox to improve cybersecurity. This toolbox aims to maximise security and data privacy while keeping costs and computing resources low. By using virtual dataspaces, INTACT could help safely predict and prevent cyber threats without affecting real systems. AI automation and open standards should improve scalability and interoperability of services and data. Researchers will also focus on sustainability and reducing environmental impact, aiming to enhance EU data security and lower energy use across industries like telecom, healthcare, and smart cities. INTACT will develop an Integrated Software Toolbox that will offer predictive Cybersecurity sensing, optimization and management services for the distributed IoT-to-Cloud continuum. The scope is to continuously maximizing the continuum's infrastructure security and data privacy with minimal effect on its computing capacity, energy consumption, monetary costs, etc. that are necessary for the businesses to run. To do so, Twinning tools will be replicating the continuum as virtual (isolated) dataspaces, such that Threat Intelligence tools can stress-test the attack-surface of these dataspaces and predict optimal risk mitigation measures accurately and safely (i.e. pre-emptively protecting and without affecting the real system operation), subject to certain computing, energy, etc. thresholds set by the end-user. Scalability & Interoperability of services and data will be achieved via the use of open standards & APIs (including Eclipse Connector), while AI Automation will be embedded in all Toolbox processes. Identity & Access Management will be advanced over a zero-trust distributed computing pipeline covering all Hardware-, System-, and Application-level security. An initial Lab-testbed with matured DevSecOps & ML/Data-Ops stemming from previous EU Actions will lead developments roadmap to 4x + 1 final TRL7 operational deployments that will be validated over 1st & 2nd Stage Demos covering use cases related to Telcos, Health 4.0 Transportation, Safety-critical Nuclear Infrastructures, and Smart Cities (cross-vertical supply-chain assessments). The impact will not only safeguard EU position in data security, economy and applications verticals, but lower energy efficiency and CO2 footprint. Sustainability & Industry acceptance will be achieved via open source ecosystems, standardization involvement, and a dedicated Portal for linking INTACT dataspaces to EU Data Spaces and INTACT innovations to EU Bodies related to Cybersecurity, AI, IOT and Robotics.
Liaison with CASTOR	INTACT has been a key project for the liaison and clustering activities of CASTOR, as it has been the initial contact for the connection with and eventual participation in the European Cluster for Securing Critical Infrastructures (ECSCI). CASTOR and INTACT have participated in calls together with other cooperating projects towards investigating opportunities for further collaboration in the forthcoming period with participation in conferences and organization of workshops. As such, INTACT will participate in the joint SecSoft2026 workshop of MIRANDA-CASTOR that will take place in the context of the 12th IEEE International Conference on Network Softwarization (NetSoft2026) from June 29 to July 3, 2026 in Berlin. In addition, the two projects presented their collaboration through their project websites and corresponding social media posts, while promoting each other's material in social media.

4.5 HEISINGBERG

Project Name	HEISINGBERG [18]
Project title	Spatial Quantum Optical Annealer for Spin Hamiltonians
Topic	HORIZON-EIC-2022-PATHFINDERCHALLENGES-01-06 - EIC Pathfinder Challenge: Alternative approaches to Quantum Information Processing, Communication, and Sensing
Description	Optical simulators rank among the most promising candidates to power future technological breakthroughs in terms of speed, scalability, power-consumption and quantum advantage, serving a wide range of useful optimization problems. However, the operation of such simulators remains currently limited by noise, the extent of algorithmic problems they can embed and to the classical regime where they compete with supercomputers. HEISINGBERG aims to bring state-of-the-art spatial photonic spin simulator (an iterated cycle of all-optical processing through a spatial light modulator that couples 10,000 spins) into the quantum regime by upgrading its coherent drive to squeezed light, making it fully programmable through vector-matrix multiplication schemes, use of holography, ancillary spins & effective magnetic fields, and designing dedicated custom-tailored and purpose-built algorithms. The reduced fluctuations in one quadrature of the fields will allow us to scale up and optimize the performances of the existing machine to bring it beyond the capabilities of both classical supercomputers and competing spin-simulators. HEISINGBERG devices will operate 100,000 spins at room temperature and process new quantum annealing algorithms on an improved XY architecture. Besides, the nonclassical resources of squeezed states when modulated, admixed and phase-controlled through beam splitters, such as entanglement or superpositions of multiphoton states will be prospected to harness a quantum advantage and boost the machine into its quantum simulation regime. This development will stimulate the quantum information processing community by concretely articulating problems of algorithmic complexity and clarify the nature of the quantum advantage available in annealers and simulators. These advances will allow us to demonstrate, on a cloud platform, annealing and adiabatic algorithms that can efficiently solve NP-hard problems.
Liaison with CASTOR	CASTOR leverages the holistic approach and the innovative artifacts of HEISINGBERG project towards addressing the Trusted Path Routing optimization problem. Furthermore, CASTOR and HEISINGBERG presented their collaboration through their project websites and corresponding social media posts, while promoting each other's material in social media.

4.6 MEDIATE

Project Name	MEDIATE [20]
Project title	Multi facEteD ImplementAtion of a mixed sofTwarE/hardware-based zero-trust framework for the computing continuum
Topic	HORIZON-CL3-2023-CS-01-01 - Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)

Project Name	MEDIATE [20]
Description	Digital data spaces and collaboration rely on the integration of cloud, edge and internet of things (IoT) — the so-called computing continuum. The vast number of entities and devices involved in processing the huge volume of potentially sensitive information has created important security and privacy risks. The EU-funded MEDIATE project aims to develop a robust technology based on the concept of zero trust and using AI-based tools to address this. Its federated learning approach will perform security-based scrutinisation at all continuum levels using security models that can be updated, redistributed and reconfigured across it. It will enable cybersecurity resilience, mitigation of vulnerabilities, and heightened trust and security. Technological advances in Information communication Technologies (ICT) as well as the digital transformation of complex systems have led to the development of novel networks, platforms and systems, which have, in turn, kick-started the realisation process for multi-faceted technological collaborations and data-driven workflows on a scale never seen before. Consequently, an integration process among the different layers of complex systems and services has been unfolding raising significant issues and challenges in its wake. Hence, the digital data and collaboration spaces are all predicated upon the realisation of what is known as the computing continuum, which is based on the integration of cloud, edge and Internet of Things (IoT). Nevertheless, this has given rise to significant security and privacy risks especially since it is about systems that involve a high number of entities and devices with different profiles, processing a vast amount of potentially sensitive info MEDIATE's vision is to produce a robust technology, which will address the security and privacy attributes of the computing continuum. For this, it will put forth a complex architecture that is based on the concept of zero-trust and will assume a federated learning approach in order to perform security-based scrutinisation at all continuum levels. i.e. IoT, edge and cloud, using security models that can be updated, redistributed and reconfigured across it. The actual features of the MEDIATE framework will support major topic outcomes such as cybersecurity resilience through reconfiguration, vulnerabilities mitigation through cyber threat analysis, secure integration at the IoT level through software and hardware-based security sensors and trust and security for massive ecosystems through the use of federated learning-based orchestration. Moreover, it will feature AI-based tools for cyber threat intelligence that assist a decision support system and privacy policies for data and identity protection.
Liaison with CASTOR	As CASTOR and MEDIATE both belong to the same call topic, they have been engaged in liaison discussions among with other cooperating projects, seeking for future opportunities for collaboration. The two projects have already presented their collaboration through their project websites and corresponding social media posts, while promoting each other's material in social media.

4.7 CyberNEMO

Project Name	CyberNEMO [15]
Project title	End-to-end Cybersecurity to NEMO meta-OS

Project Name	CyberNEMO [15]
Topic	HORIZON-CL3-2023-CS-01-01 - Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)
Description	This project builds an IoT-Edge-Cloud continuum, in the form of an open-source, flexible, adaptable, and multi-technology meta-Operating System. NEMO aims to unleash the power of Artificial Intelligence IoT to increase European autonomy in data processing and lower CO2 footprint. Leveraging on consortium partners technological excellence, along with clear business and exploitation strategies, CyberNEMO builds on top of NEMO to add end-to-end cybersecurity and trust on IoT-Edge-Cloud-Data Computing Continuum. CyberNEMO will establish itself as a paradigm-shift to support resilience, risk preparedness, awareness, detection and mitigation within Critical Infrastructures deployments and across supply chains. To achieve technology maturity and massive adoption, CyberNEMO will not “reinvent the wheel”, but leverage on existing by-design, by-innovation, and by-collaboration zero-trust cybersecurity and privacy protection systems, and introduce novel concepts, methods, tools, testing facilities and engagement campaigns to go beyond today’s state of the art and create sustainable innovation, already evident within the project lifetime. CyberNEMO will offer end-to-end and full stack protection, ranging from a low level Zero-Trust Network Access layer up to a human AI explainable Situation Perception, Comprehension & Protection (SPCP) framework and tools, collaborative micro-cervices Auditing, Certification & Accreditation and a pan-European Knowledge Sharing, risk Assessment, threat Analysis and incidents Mitigation (SAAM) collaborative platform. Validation and penetration testing will take place in 6 pilots including OneLab for integration, various Critical Infrastructures (Energy, Water, Healthcare), media distribution, agrifood and fintech supply chain, along with their cross-domain, cross-border federation. Sustainability and adoption will be offered via the de-facto European Open source Eclipse Foundation ecosystem.
Liaison with CASTOR	As CASTOR and CyberNEMO both belong to the same call topic, they have been engaged in liaison discussions among with other cooperating projects, seeking for future opportunities for collaboration. As such, CyberNEMO will participate in the joint SecSoft2026 workshop of MIRANDA-CASTOR that will take place in the context of the 12th IEEE International Conference on Network Softwarization (NetSoft2026) from June 29 to July 3, 2026 in Berlin. The two projects have already presented their collaboration through their project websites and corresponding social media posts, while promoting each other’s material in social media.

4.8 GuardAI

Project Name	GuardAI [17]
Project title	Enhancing Robustness and Security of Edge AI Systems for Safety-Critical Applications
Topic	HORIZON-CL3-2023-CS-01-03 - Security of robust AI systems

Project Name	GuardAI [17]
Description	The GuardAI project seeks to enhance the security of edge AI systems, addressing their critical vulnerabilities. Emphasis is placed on high-stakes domains, as outlined in the EU's AI Act, where these systems, including drones, connected and autonomous vehicles, and network edge infrastructure, are becoming widespread and will play a pivotal role in making crucial decisions. These cutting-edge applications heavily rely on real-time decision-making and the processing of sensitive data, rendering them susceptible to various security threats and adversarial attacks. Therefore, the overarching objective of GuardAI is to develop the next generation of resilient AI algorithms tailored for edge applications. Leveraging cutting-edge technological advancements, the project will develop innovative solutions to ensure the integrity, security, and resilience of these systems, fostering trust, and accelerating the safe adoption of AI-driven technologies. A holistic contextual understanding will be integrated, enabling systems to adapt and make informed decisions in dynamic environments. Through a multi-disciplinary and multifaceted approach, by bringing together researchers, industry experts, government agencies, AI practitioners, and advanced threat analysis methods, and robust AI algorithms, GuardAI aspires to create a paradigm shift in AI security. The development of standardized evaluation criteria forges a path to certification frameworks, and real-world insights facilitate a systematic approach to ensuring security-by-design concepts. Embracing a holistic approach, GuardAI also examines ethical considerations in AI technology development to promote ethically sound digital landscapes. Overall, the project will strive to elevate the standards of secure AI systems through cutting-edge advancements and a comprehensive, collaborative approach.
Liaison with CASTOR	As CASTOR and GuardAI both belong to the same call, they have been engaged in liaison discussions among with other cooperating projects, seeking for future opportunities for collaboration. The two projects have already presented their collaboration through their project websites and corresponding social media posts, while promoting each other's material in social media.

Chapter 5

Market Analysis in CASTOR

This chapter provides an overview of the market context and exploitation potential of the CASTOR project. The analysis is primarily based on the responses collected through the specifically crafted Market Analysis Questionnaire (MAQ) (see Appendix A) from project partners, ensuring that the findings reflect first-hand insights from both technology providers and use case contributors involved in the development and validation of CASTOR solutions. Beyond capturing domain-specific observations, the MAQ also enabled the identification of cross-cutting patterns and recurring priorities across the analysed application domains. In particular, a notable convergence of interest emerged around two main areas: first, the role of the *network fabric*, and especially the effect of trust-related attributes on network performance, path selection, and service assurance; and second, the adoption of *zero-trust and below-zero-trust* approaches, including the use of trusted computing technologies to elevate routing and network elements into verifiable security anchors capable of producing trustworthy evidence.

Section 5.1 presents the market analysis structured by application and technology domain, identifying key trends, existing alternatives, adoption drivers, and barriers affecting the potential uptake of CASTOR capabilities. Section 5.2 complements this analysis by introducing the functional and business model perspective of the CASTOR framework, outlining how the project results may be positioned from a service and value creation standpoint. Finally, Section 5.3 provides an initial evaluation of the Key Exploitable Results (KERs) identified within the project, based on the MAQ responses provided by the technical partners.

Together, these sections offer a structured overview of the market environment addressed by CASTOR, the potential positioning of its technological outcomes, and the preliminary assessment of their exploitation potential. Some findings may appear across multiple sections or domains. This is intentional, as the deliverable is structured so that each section can be read independently without requiring sequential consultation of the entire chapter. At the same time, the analysis provided here establishes the foundation for the more detailed techno-economic assessment that will be delivered in M36 through D7.3, where the market, exploitation, and impact dimensions of CASTOR will be examined in a more mature form based on the final project results.

5.1 Market Analysis per application domain

This section presents the market analysis of CASTOR based on the responses collected through the Market Analysis Questionnaire (MAQ) from project partners. The objective of the analysis is to characterise the market and operational contexts in which the CASTOR framework and its Key Exploitable Results (KERs) may be adopted. Rather than conducting an external market study, the analysis consolidates first-hand insights provided by consortium partners, including both technology providers and use case partners involved in the development, integration, and validation of CASTOR solutions in specific

application environments. The responses therefore reflect both technical development perspectives and operational insights derived from the project use cases. To ensure traceability and avoid generalisation beyond the collected evidence, the analysis is structured directly around the relevant MAQ questions. In particular, Q6 (present market behaviour and domain trends) and Q7 (current competitors and alternative solutions) are used to identify domain-specific technological developments and currently adopted practices. Q8 (target customers and adoption drivers) and Q9 (barriers and limitations) provide insights into the conditions that may facilitate or hinder the adoption of CASTOR-like capabilities in the analysed sectors. Finally, the synthesis of domain trends (Q6), competing solutions (Q7), adoption drivers (Q8), and barriers and constraints (Q9) supports the formulation of a qualitative SWOT analysis for each domain. Additional contextual insights from Q10–Q13 (innovation potential, value proposition and exploitation perspectives) are considered where relevant to complement the interpretation of the results. The analysis is organised according to the technology and application domains represented in the MAQ responses. Based on the primary sectors indicated in MAQ question Q4, the responses were clustered into three main domains: **(i) Aerospace / UAV**, **(ii) Automotive and Cooperative Connected and Automated Mobility (CCAM)**, and **(iii) Telecommunications, Edge and Infrastructure platforms**. Each domain section follows a consistent analytical structure, describing the operational landscape, identifying key trends, analysing current alternatives, and assessing adoption drivers and barriers.

Table 5.1 summarises the distribution of MAQ responses across the identified domains.

Table 5.1: Distribution of MAQ responses across the identified technology domains.

Technology Domain	MAQ Responses (ID)	Number of Responses
Aerospace / UAV	#1, #2, #3, #6	4
Automotive / CCAM	#6, #8	2
Telecommunications / Edge / Infrastructure	#0, #2, #4, #5, #7	5

It should be noted that some MAQ responses relate to multiple technology domains, reflecting the cross-sector nature of several CASTOR technologies. In particular, certain respondents identified primary sectors that span telecommunications infrastructures and application domains such as aerospace or connected mobility. As a result, the corresponding responses contribute to the analysis of more than one domain. For example, response #2 refers to telecommunications infrastructures supporting aerospace and defence environments, while response #6 addresses telecommunications technologies applied to both aerospace and connected mobility contexts. In these cases, the same MAQ input is considered in multiple domain analyses when the responses contain information relevant to each domain. This approach ensures that the analysis reflects the actual scope of the partner inputs, while preserving traceability to the original questionnaire responses.

5.1.1 Aerospace / UAV Domain

5.1.1.1 Domain Context and Operational Landscape

Four MAQ responses refer to sectors related to aerospace and unmanned aerial systems (UAV) environments (responses #1, #2, #3 and #6). These responses describe application contexts involving

aerospace infrastructures, UAV communication systems, and telecommunications platforms supporting aerospace and defence environments. The operational landscape emerging from the responses is characterised by distributed communication infrastructures and multi-domain networking environments, where UAV systems and aerospace services rely on interconnected communication networks that may span multiple administrative or technological domains. In these contexts, communication infrastructures play a central role in enabling connectivity and coordination between distributed components and operational services. Some responses also reflect the integration between telecommunications infrastructures and aerospace applications. For example, telecommunications platforms supporting aerospace and defence environments are identified as part of the operational ecosystem, illustrating how communication infrastructures can support aerospace-related services and UAV communication environments. As a result, the aerospace domain considered in this analysis includes both domain-specific aerospace applications and telecommunications infrastructures that enable aerospace communication services.

5.1.1.2 Key Trends

The responses highlight several trends influencing communication infrastructures in aerospace and UAV-related environments (Q6 responses #1, #2, #3 and #6). Across these responses, a recurring theme is the growing attention to security and trust management in communication infrastructures supporting critical systems. Several respondents explicitly refer to the adoption of Zero Trust security architectures as an emerging trend in communication infrastructures (Q6 responses #1, #3 and #6). These responses indicate a shift toward security models in which trust is not implicitly assumed but must be continuously validated. This trend reflects broader efforts to strengthen the protection of infrastructures supporting critical operations. Another aspect mentioned in the responses concerns the increasing importance of secure communication infrastructures within telecommunications environments supporting aerospace and defence applications (Q6 response #2). In such contexts, communication networks are expected to provide secure and reliable connectivity across distributed infrastructures. Taken together, the responses indicate that trends in the aerospace and UAV domain are primarily associated with the evolution of security architectures and trust management approaches in communication infrastructures, with particular attention to Zero Trust security principles and the protection of critical networking environments.

5.1.1.3 Current Alternatives and Competing Solutions

The responses identify several existing approaches and solutions currently used in communication infrastructures relevant to aerospace and UAV environments (Q7 responses #1, #2 and #3). These alternatives include established security architectures, commercial networking platforms, and domain-specific communication approaches used in UAV networking environments.

Table 5.2 presents analytical groupings derived from the solutions mentioned in the MAQ responses.

Table 5.2: Categories of current alternatives and indicative solutions in the aerospace / UAV domain.

Category	Example Solutions / Actors
Security architectures	Defence-in-depth security architectures
Commercial networking platforms	Cisco ACI, Cisco SD-WAN

Category	Example Solutions / Actors
Domain-specific networking approaches	Distributed UAV networking approaches

These approaches illustrate the diversity of solutions currently used to manage and secure communication infrastructures in aerospace and UAV environments. The responses indicate that existing solutions primarily focus on network management, traffic control, and layered security mechanisms, rather than on integrated mechanisms that explicitly incorporate trust evaluation into communication infrastructure management.

5.1.1.4 Adoption Drivers

The responses highlight several factors that may encourage the adoption of trust-aware communication mechanisms in aerospace and UAV-related environments (Q8 responses #1, #2, #3 and #6). These drivers are mainly associated with security requirements in critical infrastructures, regulatory developments, and the growing operational relevance of UAV systems. One driver mentioned in the responses is the need to improve the resilience and survivability of communication infrastructures supporting aerospace-related operations (Q8 response #1). Ensuring reliable and trustworthy communication infrastructures is particularly relevant in environments where infrastructure disruptions may affect operational continuity. Another factor identified in the responses concerns regulatory pressure related to cybersecurity and infrastructure protection (Q8 response #2). Regulatory frameworks addressing the security of critical infrastructures and digital systems can encourage the adoption of stronger trust and verification mechanisms within communication infrastructures. The responses also indicate that the increasing use of UAV systems in critical operational environments creates additional requirements for secure and trustworthy communication infrastructures (Q8 response #3). As UAV systems are deployed in more demanding operational contexts, ensuring the reliability and integrity of communication infrastructures becomes increasingly important. Finally, some responses refer to ongoing Zero Trust security initiatives as a potential driver for adopting trust-aware communication mechanisms (Q8 response #6). These initiatives promote security models that emphasise continuous verification and stronger trust management mechanisms within digital infrastructures. Overall, the responses suggest that adoption drivers in the aerospace and UAV domain are primarily associated with infrastructure resilience requirements, regulatory developments, the increasing operational role of UAV systems, and the broader adoption of Zero Trust security principles.

5.1.1.5 Barriers and Constraints

The responses identify several factors that may limit or slow the adoption of trust-aware communication mechanisms in aerospace and UAV-related environments (Q9 responses #1, #2, #3 and #6). These constraints are mainly associated with certification requirements, integration challenges, and the characteristics of existing infrastructures in safety-critical sectors. One constraint highlighted in the responses concerns the certification and assurance requirements typical of aerospace environments (Q9 response #3). Aerospace systems are often subject to strict validation and certification procedures, which may increase the effort required to introduce new mechanisms or architectural changes within communication infrastructures. Another barrier relates to the conservative nature of infrastructures used in aerospace and defence contexts (Q9 response #2). In such environments, infrastructure components and operational procedures are typically stable and highly controlled, which may slow the adoption of new technologies or

architectural approaches. The responses also point to integration complexity with existing infrastructures as a potential challenge (Q9 response #1). Introducing additional trust mechanisms may require integration with existing networking components and operational systems. Finally, some responses note that many communication infrastructures still rely on implicit trust assumptions regarding device integrity or infrastructure components (Q9 response #6). In such contexts, introducing mechanisms that dynamically evaluate trust conditions may require changes to established operational models.

Table 5.3 summarises the main barriers identified in the MAQ responses for the aerospace and UAV domain.

Table 5.3: Main barriers identified for the aerospace / UAV domain.

Barrier Category	Description	MAQ Reference
Certification and assurance requirements	Introduction of new mechanisms may require compliance with aerospace certification and validation procedures	Q9 response #3
Conservative infrastructure environments	Established operational practices and stable infrastructures may slow technology adoption	Q9 response #2
Integration complexity	Additional mechanisms may require integration with existing communication infrastructures	Q9 response #1
Implicit trust assumptions	Existing infrastructures often rely on static trust assumptions regarding devices and infrastructure components	Q9 response #6

Overall, the responses indicate that barriers in the aerospace and UAV domain are mainly associated with certification processes, integration challenges, and the operational characteristics of established infrastructures, which may influence the pace at which new trust-aware mechanisms are adopted.

5.1.1.6 SWOT Analysis

The SWOT analysis summarises the main insights emerging from the responses related to the aerospace and UAV domain. The objective of this analysis is to consolidate the strengths, weaknesses, opportunities, and threats associated with the potential adoption of CASTOR-like capabilities in this sector, based on the trends, drivers, alternatives, and barriers identified in the previous sections. The analysis reflects the information provided by partners operating in aerospace and UAV-related environments (responses #1, #2, #3 and #6) and integrates insights from the questions addressing innovation potential, strengths, opportunities, and market conditions (Q10–Q13), together with the adoption drivers and barriers discussed in the corresponding subsections of the present domain analysis. From the perspective of strengths, the responses highlight the relevance of trust-aware mechanisms in communication infrastructures supporting aerospace and UAV applications. In particular, the increasing focus on secure communication infrastructures and the adoption of security frameworks such as Zero Trust architectures indicate that solutions capable of improving trust management in communication networks may provide operational value in these environments. Regarding weaknesses, the responses indicate that introducing new mechanisms into aerospace communication infrastructures may require significant integration

effort and alignment with existing infrastructures. In addition, the characteristics of safety-critical infrastructures may limit the speed at which new solutions can be introduced. In terms of opportunities, the responses suggest that regulatory developments, cybersecurity initiatives, and the increasing operational importance of UAV systems may create conditions that favour the adoption of stronger trust and verification mechanisms in communication infrastructures. Finally, the responses also indicate several potential threats, including the complexity of certification processes, the conservative nature of aerospace infrastructures, and the presence of established security and networking approaches already used in these environments.

Table 5.4: SWOT analysis for the aerospace / UAV domain.

Strengths • Alignment with emerging Zero Trust security architectures in communication infrastructures. • Relevance of stronger trust management mechanisms for communication infrastructures supporting critical operations. • Applicability to communication environments combining aerospace and telecommunications infrastructures.	**Weaknesses** • Integration complexity with existing communication infrastructures and networking platforms. • Dependence on infrastructure environments where security architectures are already established.
Opportunities • Increasing attention to cybersecurity and resilience in critical communication infrastructures. • Expansion of UAV deployments in operational environments. • Growing adoption of Zero Trust security principles across digital infrastructures.	**Threats** • Certification and validation requirements in aerospace systems. • Conservative infrastructure environments and slow technology adoption cycles. • Continued reliance on existing security architectures and networking solutions.

5.1.2 Automotive / CCAM Domain

5.1.2.1 Domain Context and Operational Landscape

Two MAQ responses refer to sectors related to automotive systems and Cooperative Connected and Automated Mobility (CCAM) environments (Q4 responses #6 and #8). These responses relate to application contexts involving connected mobility infrastructures and intelligent transportation systems, where communication networks support interactions between vehicles, infrastructure components, and backend platforms. The responses indicate that these environments rely on communication infrastructures enabling connected vehicle ecosystems, where vehicles exchange information with other vehicles, roadside infrastructure, and centralised services. Such environments are typically characterised by the integration of telecommunications technologies with transportation infrastructures to support connected mobility services. In addition, one of the responses reflects the role of telecommunications infrastructures supporting mobility-related communication environments (Q4 response #6). This illustrates the cross-sector nature of some connected mobility systems, where telecommunications technologies are used to enable communication between vehicles and supporting digital infrastructures. Overall, the responses indicate that the operational landscape in the automotive and CCAM domain involves communication infrastructures supporting connected mobility environments, where secure and reliable communication between distributed components is an important element of the overall system architecture.

5.1.2.2 Key Trends

The responses identify several developments influencing communication infrastructures in the automotive and CCAM domain (Q6 responses #6 and #8). These developments mainly relate to the evolution of connected mobility technologies and the increasing attention to security in communication infrastructures supporting connected vehicle ecosystems. One response highlights the relevance of Zero Trust security principles in communication infrastructures (Q6 response #6). This reflects broader developments in digital infrastructures where security models increasingly emphasise continuous verification mechanisms rather than relying on implicit trust assumptions. Another response refers to the expansion of Cellular Vehicle-to-Everything (C-V2X) communication technologies (Q6 response #8). C-V2X technologies enable communication between vehicles, infrastructure components, and other road users, supporting applications in connected mobility and intelligent transportation systems. Overall, the responses indicate that trends in the automotive and CCAM domain are associated with the expansion of connected vehicle communication technologies and increasing attention to security mechanisms within communication infrastructures supporting connected mobility environments.

5.1.2.3 Current Alternatives and Competing Solutions

The responses identify several existing actors and solutions currently involved in communication infrastructures supporting connected mobility environments (Q7 response #8). These alternatives mainly include telecommunications operators and technology providers offering connectivity and infrastructure solutions for connected vehicle ecosystems. In connected mobility environments, communication infrastructures are often supported by telecommunications platforms and intelligent transportation system (ITS) solutions enabling connectivity between vehicles, roadside infrastructure, and backend systems. The responses refer to several organisations active in this space, including telecommunications operators and mobility infrastructure providers.

Table 5.5 summarises the main categories of actors and example solutions mentioned in the responses.

Table 5.5: Categories of current alternatives and indicative solutions in the automotive / CCAM domain.

Category	Example Solutions / Actors
Telecommunications operators	Vodafone, Verizon
Mobility and ITS infrastructure providers	Kapsch, Yunex
Communication technology providers	Qualcomm

These actors illustrate the range of organisations currently involved in providing communication technologies and infrastructures supporting connected mobility environments. The responses indicate that existing solutions primarily focus on vehicle connectivity, infrastructure communication, and mobility service platforms, rather than mechanisms specifically designed to integrate trust-aware evaluation within communication infrastructures.

5.1.2.4 Adoption Drivers

The responses identify several factors that may encourage the adoption of stronger security and trust mechanisms in communication infrastructures supporting connected mobility environments (Q8 responses #6 and #8). These drivers are mainly associated with the growing importance of secure communication infrastructures for connected vehicle ecosystems and the evolution of connected mobility services. One response refers to ongoing Zero Trust security initiatives as a factor encouraging the adoption of stronger trust mechanisms in communication infrastructures (Q8 response #6). Such initiatives promote security models that emphasise continuous verification and stronger control of digital infrastructures. Another response highlights the need to ensure secure communication infrastructures supporting connected vehicle ecosystems (Q8 response #8). As connected mobility systems increasingly rely on communication between vehicles, infrastructure components, and backend services, ensuring secure and reliable communication becomes an important requirement. Overall, the responses indicate that adoption drivers in the automotive and CCAM domain are primarily associated with the expansion of connected vehicle ecosystems and the growing need for secure communication infrastructures supporting connected mobility environments.

5.1.2.5 Barriers and Constraints

The responses identify several factors that may limit or slow the adoption of stronger security and trust mechanisms in communication infrastructures supporting connected mobility environments (responses #6 and #8). These barriers mainly relate to performance and scalability constraints in large-scale deployments, as well as the technical maturity, standardisation, and interoperability of emerging mechanisms. One response highlights performance and scalability constraints as a potential limitation when deploying new mechanisms in large-scale environments (response #6). Communication infrastructures supporting connected mobility systems may involve large numbers of connected devices and distributed components, which can create challenges when introducing additional mechanisms that affect network performance or operational scalability. Another response refers to the technical maturity and standardisation of emerging mechanisms, noting the need to gain further experience with implementation and ensure interoperability across systems (response #8). In connected mobility environments, communication infrastructures often rely on multiple technologies and systems that must operate together, making interoperability and standards alignment important factors for adoption.

Table 5.6 summarises the main barriers identified in the responses for the automotive and CCAM domain.

Table 5.6: Main barriers identified in the automotive / CCAM domain.

Barrier Category	Description	MAQ Reference
Performance and scalability constraints	Deployment of new mechanisms may face performance and scalability limitations in large-scale environments	Q9 response #6
Technical maturity and standardisation	Adoption requires further experience, standards development and interoperability across systems	Q9 response #8

Overall, the responses indicate that barriers in the automotive and CCAM domain are mainly associated with integration challenges and the heterogeneous nature of connected mobility infrastructures,

which may influence the adoption of new mechanisms within communication environments supporting connected vehicles.

5.1.2.6 SWOT Analysis

The SWOT analysis summarises the main insights emerging from the responses related to the automotive and CCAM domain (responses #6 and #8). The analysis consolidates the strengths, weaknesses, opportunities, and threats associated with the potential adoption of stronger trust and security mechanisms in communication infrastructures supporting connected mobility environments. The elements of the SWOT analysis reflect the trends, alternatives, adoption drivers, and barriers identified in the previous sections. In particular, the responses highlight developments such as the adoption of Zero Trust security principles and the expansion of C-V2X communication technologies, while also indicating challenges related to performance and scalability constraints in large-scale deployments and the need for further technical maturity, standardisation, and interoperability across systems.

Table 5.7: SWOT analysis for the automotive / CCAM domain.

Strengths • Applicability to secure communication environments supporting connected vehicles. • Alignment with Zero Trust security initiatives in communication infrastructures. • Relevance for C-V2X communication ecosystems.	**Weaknesses** • Limited technical maturity of trust-aware mechanisms in connected mobility infrastructures. • Need for validation and testing in large-scale deployments.
Opportunities • Expansion of C-V2X communication technologies. • Increasing attention to secure communications in connected vehicle ecosystems.	**Threats** • Performance and scalability constraints in large-scale mobility deployments. • Standardisation and interoperability challenges across connected mobility infrastructures.

5.1.3 Telecommunications / Edge / Infrastructure Domain

5.1.3.1 Domain Context and Operational Landscape

Five responses refer to sectors related to telecommunications infrastructures, edge computing environments, and network service platforms (responses #0, #2, #4, #5 and #7). Several responses refer to telecommunications infrastructures that support multiple application sectors, including aerospace and mobility environments. These responses describe operational contexts involving network infrastructures and distributed computing environments supporting communication services and digital platforms. The environments represented in these responses typically involve telecommunications networks and cloud or edge infrastructures where communication services are deployed, managed, and orchestrated across multiple infrastructure components. These infrastructures support the operation of network services, applications, and digital platforms that rely on connectivity between distributed systems. Some responses also reflect the role of telecommunications infrastructures supporting other application domains, such as aerospace or connected mobility environments. In these cases, telecommunications platforms provide the underlying communication capabilities enabling services and applications operating across different sectors. Overall, the operational landscape represented in this domain involves telecommunications and

edge infrastructures supporting network services and distributed digital environments, where communication networks and computing platforms interact to provide connectivity and service delivery across multiple infrastructures.

5.1.3.2 Key Trends

The responses highlight several developments influencing telecommunications and edge infrastructures (responses #0, #2, #4, #5 and #7). These developments mainly relate to security approaches for network infrastructures, the automation of network management, and the evolution of distributed computing environments. Some responses highlight the increasing relevance of Zero Trust security principles in network infrastructures (responses #2 and #4). These approaches reflect a shift towards security models in which trust is not implicitly assumed and verification mechanisms are applied continuously across communication environments. Other responses refer to the automation and orchestration of network services and infrastructures, where automated mechanisms are used for network configuration, service deployment, and infrastructure management (responses #5 and #7). These approaches support the operation of complex network environments and enable more efficient management of telecommunications infrastructures. The responses also point to the growing importance of distributed computing environments such as edge infrastructures (response #0), where computing resources and communication capabilities are deployed closer to service environments. These developments influence how network services are deployed and managed across telecommunications infrastructures. Overall, the responses indicate that trends in this domain are associated with the evolution of security approaches for network infrastructures, the automation of network management, and the increasing role of distributed computing environments supporting communication services.

5.1.3.3 Current Alternatives and Competing Solutions

Several responses refer to existing platforms and solutions currently used to manage telecommunications infrastructures and network services (responses #2, #4, #5 and #7). These alternatives include network orchestration platforms, open-source network management frameworks, infrastructure automation tools, and security monitoring solutions used in telecommunications and distributed infrastructure environments. In these environments, network infrastructures are commonly managed through orchestration platforms and automation frameworks that support configuration, service deployment, and infrastructure management across multiple network components. Security monitoring and protection solutions are also used to support the protection and operational reliability of network infrastructures.

Table 5.8 summarises the main categories of alternatives and example solutions mentioned in the responses.

Table 5.8: Categories of current alternatives and indicative solutions in the telecommunications / edge / infrastructure domain.

Category	Example Solutions / Platforms
Commercial network orchestration platforms	Cisco NSO, Juniper NorthStar
Open-source network management frameworks	ONAP, OpenDaylight

Category	Example Solutions / Platforms
Infrastructure automation frameworks	Kubernetes, Ansible
Security monitoring and protection solutions	Imperva, Thales

These solutions illustrate the range of platforms currently used to manage telecommunications infrastructures and network services. The responses indicate that existing approaches mainly focus on network orchestration, infrastructure automation, and security monitoring, rather than mechanisms specifically designed to integrate dynamic trust evaluation within network management environments.

5.1.3.4 Adoption Drivers

Several responses identify factors that may encourage the adoption of stronger security and trust mechanisms in telecommunications and edge infrastructures (responses #0, #2, #4, #5 and #7). These drivers mainly relate to the need to strengthen security in network infrastructures, improve trust in distributed communication environments, and support the management of increasingly complex network services. Some responses highlight the growing importance of security and trust in telecommunications infrastructures, particularly in environments where network services support critical systems or distributed digital platforms (responses #2 and #4). In such contexts, mechanisms that enable stronger verification and trust management within network infrastructures may provide operational value. Other responses refer to the need for improved mechanisms to support the management and orchestration of complex network infrastructures, where services are deployed and managed across multiple network components and computing environments (responses #5 and #7). As telecommunications and edge infrastructures evolve, managing these environments efficiently becomes an increasingly important requirement. In addition, one response highlights the relevance of distributed computing environments such as edge infrastructures, where communication and computing resources are deployed closer to service environments (response #0). In such contexts, mechanisms that support secure and reliable communication across distributed infrastructures may become increasingly relevant. Overall, the responses indicate that adoption drivers in this domain are mainly associated with strengthening security in network infrastructures, improving trust in distributed communication environments, and supporting the management of increasingly complex telecommunications and edge infrastructures.

5.1.3.5 Barriers and Constraints

Several responses identify factors that may limit or slow the adoption of stronger trust and security mechanisms in telecommunications and edge infrastructures (responses #0, #2, #4, #5 and #7). These barriers mainly relate to performance and scalability constraints in large-scale network environments, as well as challenges related to interoperability and integration with existing infrastructures. One response highlights performance and scalability constraints as a potential limitation when introducing additional mechanisms in large-scale telecommunications environments (response #5). In such contexts, network infrastructures may involve large numbers of services, devices, and distributed components, making it important to ensure that new mechanisms do not negatively affect operational performance or scalability. Other responses refer to interoperability and integration challenges when introducing new mechanisms within existing network management and orchestration environments (responses #4 and #7). Telecommunications infrastructures often rely on established platforms and standards, and ensuring compatibility with

existing systems may require additional effort during deployment. Another response points to the need to consider operational complexity in distributed infrastructures, where services and network functions may be deployed across multiple environments and infrastructure components (response #0).

Table 5.9 summarises the main barriers identified in the responses for the telecommunications / edge domain.

Table 5.9: Main barriers identified in the telecommunications / edge / infrastructure domain.

Barrier Category	Description	Reference
Performance and scalability constraints	Deployment of additional mechanisms may affect performance or scalability in large-scale network environments	Response #5
Interoperability and integration challenges	Ensuring compatibility with existing network management platforms and infrastructures may require additional effort	Responses #4, #7
Operational complexity in distributed infrastructures	Managing services across multiple network and computing environments may increase deployment complexity	Response #0

Overall, the responses indicate that barriers in this domain are mainly associated with performance considerations, interoperability challenges, and the operational complexity of distributed telecommunications and edge infrastructures.

5.1.3.6 SWOT Analysis

The SWOT analysis summarises the main insights emerging from the responses related to the telecommunications, edge, and infrastructure domain (responses #0, #2, #4, #5 and #7). The analysis consolidates the strengths, weaknesses, opportunities, and threats associated with the potential adoption of stronger trust and security mechanisms in telecommunications and distributed network environments. The elements of the SWOT analysis reflect the trends, alternatives, adoption drivers, and barriers identified in the previous sections. In telecommunications and edge infrastructures, network services are increasingly deployed across distributed environments and managed through orchestration and automation platforms. At the same time, the responses highlight the growing importance of security approaches such as Zero Trust principles and the need to manage complex network infrastructures supporting distributed computing environments. These developments create opportunities for mechanisms capable of supporting trust and security management across network infrastructures while also highlighting challenges related to scalability, interoperability, and integration with existing platforms.

Table 5.10: SWOT analysis for the telecommunications / edge / infrastructure domain.

Strengths
- Alignment with security approaches such as Zero Trust principles in telecommunications infrastructures.
- Applicability to distributed network environments including edge infrastructures.
- Relevance for environments requiring improved management and security of complex network infrastructures.

Weaknesses
- Performance and scalability constraints when introducing additional mechanisms in large-scale network environments.
- Integration challenges with existing network orchestration and management platforms.
- Operational complexity in distributed telecommunications and edge infrastructures.

Opportunities
- Expansion of edge computing and distributed network infrastructures.
- Increasing attention to secure communications in connected vehicle ecosystems.
- Increasing need for security and trust management in telecommunications infrastructures.
- Growing reliance on automated network management and orchestration.

Threats
- Strong presence of established orchestration and network management platforms.
- Interoperability challenges across heterogeneous network infrastructures.
- Continued reliance on existing security monitoring and network management solutions.

5.1.4 Cross-Domain Synthesis

The analysis across the three domains — Aerospace / UAV, Automotive / CCAM, and Telecommunications / Edge / Infrastructure — reveals several common patterns in market developments, adoption drivers, and barriers affecting the potential adoption of stronger trust and security mechanisms in communication infrastructures. While the operational contexts differ across sectors, the responses indicate that many of the underlying technological and organisational challenges are shared across domains. This section synthesises the insights from the domain-specific analyses by identifying cross-domain trends, recurring drivers, shared barriers, and the overall competitive landscape. The objective is to highlight common dynamics across sectors while also identifying domain-specific characteristics that influence the potential positioning of CASTOR.

5.1.4.1 Cross-domain overview

The three analysed domains represent different application contexts in which communication infrastructures support distributed services and systems. Aerospace environments involve communication infrastructures supporting UAV systems and aerospace services. Automotive environments focus on communication technologies enabling connected mobility services, including V2N communication. Telecommunications and edge infrastructures provide the underlying communication and computing environments supporting network services and distributed digital platforms. Despite these differences, the responses indicate that communication infrastructures increasingly operate across distributed environments and interconnected systems, where security, trust management, and infrastructure orchestration play an important role in supporting reliable operations.

5.1.4.2 Common Market Trends

Several technological developments appear across multiple domains, as reflected in the MAQ responses (Q6 responses #0, #1, #3, #4, #5, #6 and #8). These developments particularly relate to security ap-

proaches, distributed infrastructures, and communication technologies.

Table 5.11: Cross-domain comparison of key market and technology trends.

Trend	Aerospace / UAV	Automotive / CCAM	Telecom / Edge
Adoption of Zero Trust security principles	✓	✓	✓
Distributed communication infrastructures	✓	-	✓
Edge and distributed computing environments	-	-	✓
C-V2X communication technologies	-	✓	-
Network automation and orchestration	-	-	✓

The responses highlight the increasing attention to Zero Trust security principles across multiple domains, reflecting a broader shift towards security models based on continuous verification. At the same time, the expansion of distributed computing environments and communication infrastructures influences how services and applications are deployed and managed across sectors.

5.1.4.3 Recurring Adoption Drivers

Across the analysed domains, several drivers support the adoption of stronger trust and security mechanisms in communication infrastructures.

Table 5.12: Cross-domain comparison of adoption drivers.

Adoption Driver	Aerospace / UAV	Automotive / CCAM	Telecom / Edge
Need for stronger security in communication infrastructures	✓	✓	✓
Increasing complexity of infrastructure management	✓	-	✓
Expansion of domain-specific communication ecosystems	-	✓	✓

Security requirements appear as a common driver across all domains. Some MAQ responses (notably responses #0 and #5) highlight the increasing complexity of managing distributed network infrastructures, which may create demand for mechanisms supporting infrastructure management and trust verification. The expansion of communication ecosystems, such as connected mobility services and distributed network platforms, further increases the importance of secure and reliable communication infrastructures. The MAQ responses indicate that the adoption of trust-aware networking capabilities is expected to follow gradual integration paths, influenced by factors such as infrastructure upgrade cycles, interoperability requirements, and the validation processes required in operational environments.

5.1.4.4 Shared Barriers and Constraints

While the responses highlight several drivers for adoption, they also identify common barriers affecting the introduction of new mechanisms across domains.

Table 5.13: Cross-domain comparison of barriers and constraints.

Barrier	Aerospace / UAV	Automotive / CCAM	Telecom / Edge
Certification and validation requirements	✓	-	-
Performance and scalability constraints	-	✓	✓
Technical maturity and interoperability	-	✓	✓
Integration with existing infrastructures	✓	-	✓

5.1.4.5 Competitive Landscape Across Domains

The competitive landscape identified in the responses reflects a variety of existing solutions used to manage communication infrastructures across the analysed sectors.

Table 5.14: Illustrative competitive landscape across the analysed domains.

Domain	Example Solutions
Aerospace / UAV	Defence-in-depth architectures, Cisco ACI, Cisco SD-WAN
Automotive / CCAM	Vodafone, Verizon, Kapsch, Yunex, Qualcomm
Telecom / Edge	Cisco NSO, Juniper NorthStar, ONAP, OpenDaylight, Imperva, Thales

Across domains, existing solutions primarily focus on network orchestration, infrastructure automation, connectivity services, and security monitoring. These solutions support the management and protection of communication infrastructures but do not necessarily address dynamic trust evaluation mechanisms integrated into infrastructure management processes.

5.1.4.6 Strategic Positioning of CASTOR

The cross-domain analysis highlights a common set of challenges across communication infrastructures, including the growing complexity of distributed environments, the need for stronger security mechanisms, and the expansion of communication ecosystems across sectors. While existing solutions provide capabilities for network orchestration, infrastructure automation, and security monitoring, the responses indicate limited focus on mechanisms that explicitly support trust evaluation within communication infrastructure management. In this context, the CASTOR framework may address an emerging need across

domains by exploring mechanisms capable of supporting trust-aware management of communication infrastructures, potentially complementing existing solutions used for orchestration, connectivity, and infrastructure protection.

5.1.4.7 Risk assessment

The purpose of this risk assessment is to identify the main factors that may affect the adoption and deployment of CASTOR capabilities across the analysed domains. The analysis is based on the barriers and constraints reported in the Market Analysis Questionnaire (MAQ) responses and complements the domain-level market analysis presented in the previous sections. The identified risks therefore represent technology adoption and deployment challenges, rather than risks related to project implementation. Based on the barriers and constraints reported by partners, several cross-domain risks affecting the potential adoption of trust-aware networking mechanisms were identified. To evaluate these risks, a qualitative likelihood–impact assessment was performed. In this framework, each risk is assessed along two dimensions: likelihood, representing the probability that the risk may occur in real deployment scenarios, and impact, representing the potential consequences for the adoption and large-scale deployment of the proposed mechanisms in operational communication infrastructures. The likelihood scale ranges from Remote to Certain, reflecting the estimated probability of occurrence based on the evidence provided in the MAQ responses and the cross-domain analysis presented in this section. The impact scale ranges from Insignificant to Critical, reflecting the potential effect of the identified risk on the feasibility of deploying trust-aware communication mechanisms in operational infrastructures. An initial risk assessment was first performed based on the current technological maturity of the mechanisms, the barriers reported by partners, and the operational characteristics of the infrastructures described in the MAQ responses. For each risk, potential preventive and corrective mitigation measures were then identified, reflecting actions that may reduce either the likelihood of occurrence or the potential impact of the risk. The residual risk level after mitigation was subsequently estimated by considering the expected effect of these measures. The resulting risk positions, both before and after mitigation, are visualised using the qualitative risk matrix presented later in this section. Table 5.15 summarises the main cross-domain risks emerging from the partner responses.

Table 5.15: Cross-domain adoption risks identified from MAQ responses.

Risk ID	Risk description	Evidence from MAQ responses
R1	Integration complexity when introducing trust-aware mechanisms into heterogeneous communication infrastructures and existing orchestration environments	#0, #4, #7
R2	Certification and regulatory constraints affecting the introduction of new networking mechanisms in safety-critical environments such as aerospace and automotive systems	#1, #3, #8
R3	Performance and scalability constraints when deploying trust-aware mechanisms in large-scale distributed network infrastructures	#5, #6

Risk ID	Risk description	Evidence from MAQ responses
R4	Interoperability and standardisation challenges when integrating new mechanisms with existing network platforms and technologies	#4, #7, #8
R5	Operational complexity in distributed infrastructures where services and communication paths span multiple domains and technological environments	#0, #5

The risks identified in Table 5.15 are further characterised below. For each risk, Tables 5.16, 5.17, 5.18, 5.19, and 5.20 provide a qualitative description, indicators of occurrence, mitigation measures, and the corresponding initial and residual risk assessment.

Table 5.16: Risk R1: integration complexity in heterogeneous infrastructures.

Element	Description
Category	Technical / Integration
Responsible	Consortium partners
Description	Integration of trust-aware mechanisms within heterogeneous communication infrastructures and existing orchestration environments may require significant adaptation efforts and interoperability with multiple network management platforms.
Indicators of occurrence	Difficulties integrating CASTOR mechanisms with existing orchestration platforms or vendor-specific networking infrastructures.
Initial assessment	Likelihood: Possible (3); Impact: Moderate (3); Risk score: 9
Preventive measures	Design of interoperable interfaces and compatibility with existing orchestration and networking frameworks.
Corrective measures	Collaboration with infrastructure operators and progressive integration through pilot environments.
Succes factors	Demonstration of interoperability with existing network management and orchestration solutions.
Residual assessment after measures	Likelihood: Unlikely (2); Impact: Moderate (3); Risk score: 6

Table 5.17: Risk R2: certification and regulatory constraints in safety-critical environments.

Element	Description
Category	Regulatory / Market
Responsible	Consortium partners and industry stakeholders
Description	In safety-critical environments such as aerospace or connected mobility systems, the introduction of new networking mechanisms may require compliance with certification procedures and regulatory frameworks governing communication infrastructures.
Indicators of occurrence	Requirements for certification, regulatory compliance processes, or additional validation procedures before operational deployment.
Initial assessment	Likelihood: Possible (3); Impact: Major (4); Risk score: 12
Preventive measures	Alignment of the proposed mechanisms with existing standards and regulatory frameworks relevant to the targeted application domains.
Corrective measures	Collaboration with certification authorities and integration of validation procedures within pilot environments.
Succes factors	Demonstration of compliance with relevant industry standards and security frameworks.
Residual assessment after measures	Likelihood: Unlikely (2); Impact: Major (4); Risk score: 8

Table 5.18: Risk R3: performance and scalability constraints.

Element	Description
Category	Technical
Responsible	Technical partners
Description	Trust-aware routing and orchestration mechanisms may introduce additional computational overhead or communication latency when deployed in large-scale distributed infrastructures.
Indicators of occurrence	Increased latency, higher computational load, or reduced performance in large-scale network environments.
Initial assessment	Likelihood: Possible (3); Impact: Major (4); Risk score: 12
Preventive measures	Optimisation of algorithms and validation of mechanisms in controlled experimental environments.
Corrective measures	Performance tuning and progressive deployment strategies within operational infrastructures

Element	Description
Succes factors	Demonstration of acceptable performance levels in pilot environments and large-scale scenarios.
Residual assessment after measures	Likelihood: Unlikely (2); Impact: Moderate (3); Risk score: 6

Table 5.19: Risk R4: interoperability and standardisation challenges.

Element	Description
Category	Technical / Ecosystem
Responsible	Consortium partners and industry stakeholders
Description	Adoption of trust-aware networking mechanisms may be affected by interoperability challenges with existing communication platforms and the absence of widely adopted standards supporting trust-aware infrastructure management.
Indicators of occurrence	Difficulties integrating CASTOR mechanisms with existing networking platforms or lack of standardised interfaces for trust exchange.
Initial assessment	Likelihood: Possible (3); Impact: Moderate (3); Risk score: 9
Preventive measures	Design of open interfaces and alignment with widely used networking and orchestration standards.
Corrective measures	Participation in standardisation initiatives and collaboration with ecosystem stakeholders.
Succes factors	Adoption of interoperable interfaces enabling integration with existing networking platforms.
Residual assessment after measures	Likelihood: Unlikely (2); Impact: Moderate (3); Risk score: 6

Table 5.20: Risk R5: operational complexity in distributed infrastructures.

Element	Description
Category	Operational
Responsible	Infrastructure operators and consortium partners

Element	Description
Description	Communication infrastructures supporting distributed services may involve complex operational environments where multiple domains, platforms, and infrastructure components interact, potentially increasing deployment complexity.
Indicators of occurrence	Operational challenges in managing communication paths across heterogeneous infrastructures and administrative domains.
Initial assessment	Likelihood: Possible (3); Impact: Moderate (3); Risk score: 9
Preventive measures	Design of management mechanisms compatible with existing orchestration platforms and operational procedures.
Corrective measures	Validation of deployment procedures through pilot implementations and operational testing.
Succes factors	Demonstration of operational feasibility and simplified deployment processes in real-world environments.
Residual assessment after measures	Likelihood: Unlikely (2); Impact: Moderate (3); Risk score: 6

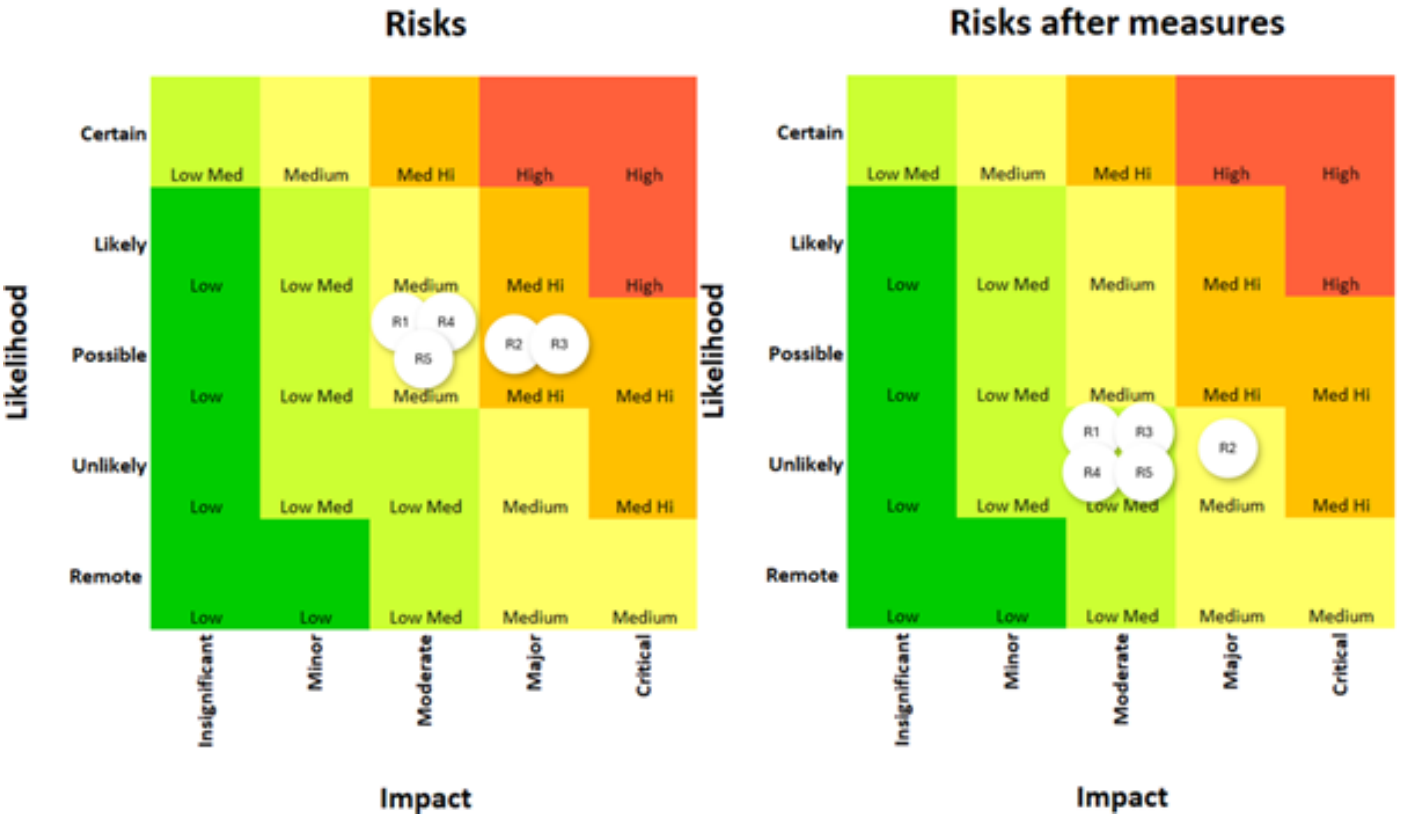

Figure 5.1: Qualitative risk matrix showing initial and residual risk levels after mitigation measures.

Figure 5.1 presents the qualitative risk matrix summarising the initial and residual risk levels of the identified risks. The matrix illustrates the position of each risk according to its likelihood and impact before mitigation measures and the expected residual position after the implementation of preventive and corrective actions.

5.2 Definition of CASTOR's functional and business model

This section complements the market analysis of Section 5.1 by introducing a functional and business-oriented interpretation of the CASTOR framework. The purpose is not to define CASTOR as a single product in a narrow commercial sense, but rather to explain how its architectural building blocks, technical capabilities, and key exploitable outcomes can be understood from the perspective of value creation, service delivery, and adoption in operational environments. In this respect, CASTOR is best interpreted as a modular framework for trust-/network-aware path establishment and orchestration, enabling communication services to be provisioned, monitored, and reconfigured according to both conventional network criteria and explicit trustworthiness requirements. This interpretation is consistent with the project's architectural framing, where the orchestration layer operationalises continuous trust evaluation and enables trust-informed decision-making in routing and traffic engineering processes, while remaining compatible with existing orchestrators rather than imposing a monolithic control stack.

5.2.1 Functional interpretation of CASTOR

From a functional perspective, CASTOR addresses a limitation of conventional communication and orchestration environments. Existing routing and orchestration mechanisms typically optimise for performance-related properties such as latency, bandwidth, availability, or resource utilisation, but they do not systematically treat trustworthiness as a first-class operational input for service provisioning and path selection. CASTOR extends this logic by enabling communication paths and service placement decisions to be influenced by trust-related knowledge derived from explicit trust assessment processes. In particular, trust is not assumed statically, nor inferred indirectly through coarse administrative boundaries, but rather evaluated continuously through trust sources, attestation evidence, runtime monitoring, and trust models that are interpreted by the Trust Assessment Framework (TAF).

This functional role is reflected in the project requirements and architecture. CASTOR's orchestration logic is designed to translate high-level intents and SSLA-derived trust and security requirements into concrete orchestration directives, so that services are placed and routed only through nodes and paths whose assessed trustworthiness satisfies the required trust level. In this sense, CASTOR extends traditional traffic engineering with a trust dimension: routing, placement, and lifecycle operations are expected to remain both network-efficient and trust-/policy-compliant, while also being capable of runtime adaptation when trust degradation or SSLA non-compliance is detected.

The CASTOR functional model can therefore be described through four interconnected capability layers. First, CASTOR provides a *trust evidence and assurance layer*, responsible for collecting, protecting, and conveying evidence related to the trust posture of routers, virtual routers, and associated network elements. This includes composable attestation and other trust sources capable of reporting both static and runtime trustworthiness properties. Second, CASTOR provides a *trust assessment and decision layer*, centred on the Local and Global TAF instances, where collected evidence is translated into operationally meaningful trust outputs such as Actual Trustworthiness Levels (ATLs), Required Trust Levels (RTLs), and ultimately trust decisions. Third, CASTOR provides an *optimization and orchestration layer*, where network and trust inputs are combined in order to derive candidate paths, placement recommendations, and traffic engineering policies. Fourth, CASTOR provides a *service assurance and trust exposure layer*, through which the resulting trust-aware behaviour of the network can support runtime assurance, policy enforcement, and controlled sharing of trust-related information across domains. These layers define CASTOR as a trust-aware service enablement framework rather than a single networking primitive.

A particularly important aspect of the functional model is that CASTOR does not require a full replacement of incumbent orchestration environments. On the contrary, the project explicitly adopts a modular approach, according to which the TAF and the Optimization Engine are designed so as to feed trust and optimization outputs into any compatible orchestration system. This means that CASTOR can be

interpreted either as a complete reference orchestration architecture or as a set of reusable trust-aware functions that enhance existing orchestration and traffic engineering environments. Functionally, this modularity is central to the project's value proposition because it allows CASTOR capabilities to be embedded incrementally into heterogeneous and legacy-prone operational settings.

5.2.2 CASTOR as a service-enabling framework

When interpreted from a service viewpoint, CASTOR enables communication infrastructures to expose differentiated service behaviours not only according to performance but also according to trustworthiness. In practical terms, this means that a service provider or infrastructure operator can use CASTOR to establish and maintain service paths whose selection is informed by explicit trust properties such as integrity, availability, confidentiality, or robustness, as evaluated by the TAF and enforced by the orchestration logic. In contrast to best-effort or purely performance-oriented networking, CASTOR enables an environment in which trust becomes an operationally manageable service parameter.

This service orientation is particularly relevant in the types of environments considered in CASTOR, namely distributed and multi-domain networking infrastructures, cloud-to-edge service topologies, and communication settings in which critical workloads rely on trustworthy connectivity. In such environments, value is generated not only by maintaining throughput or latency targets, but by ensuring that the selected path or placement option remains aligned with the service's risk posture and assurance expectations throughout its lifecycle. CASTOR therefore supports the emergence of *trust-aware connectivity services*, in which the communication substrate is differentiated not only by efficiency but also by verifiable trust and assurance characteristics.

Another relevant aspect of this service interpretation concerns assurance transparency. CASTOR enables the creation, maintenance, and controlled handling of trust-related evidence over time, making it possible to support auditing, service assurance reporting, and runtime justification of trust-based decisions. The value of CASTOR is therefore not exhausted in the moment of path selection; it also extends to the ability to explain, verify, and maintain trusted service delivery over time. From an operational and business perspective, this creates value not only for infrastructure operators but also for service providers, integrators, and downstream stakeholders who depend on verifiable claims regarding the trust posture of the underlying communication environment.

5.2.3 Comparative analysis of CASTOR and SCION

The functional interpretation of CASTOR becomes clearer when it is positioned against adjacent approaches to secure and path-aware networking. In this respect, the comparison with SCION is especially useful, as SCION represents one of the most mature and operationally advanced architectures for path-aware inter-domain networking. CASTOR itself recognises the relevance of SCION as an established technology and explicitly identifies both conceptual overlap and technical divergence between the two approaches. SCION has already evolved into a production-grade operating technology, with real deployments in sensitive environments such as the Secure Swiss Finance Network, and its path-aware design provides strong capabilities for route control, isolation, and inter-domain service provisioning.

SCION (*Scalability, Control, and Isolation on Next-Generation Networks*) is a path-aware inter-domain communication architecture that has emerged as one of the most prominent alternatives to the conventional Internet routing model. Its design introduces explicit path selection, packet-carried forwarding information, multi-path resilience, and a trust-structured organization of administrative domains, thereby addressing long-standing limitations of inter-domain routing related to security, availability, and path transparency [8, 9, 1, 23]. Given that CASTOR also addresses the establishment of trustworthy paths across heterogeneous domains, a vis-à-vis comparison against SCION is both technically justified and strate-

gically relevant. Such a comparison is necessary not only because SCION represents the most mature and architecturally coherent reference point in the area of path-aware inter-domain networking, but also because it helps clarify CASTOR's distinct contribution beyond secure path establishment alone, namely the introduction of trust-plane mechanisms, runtime trust characterization, attestation-driven path qualification, and orchestration support across the compute continuum [2, 4, 5]. Therefore, the analysis that follows is intended to position CASTOR with respect to SCION in a precise and balanced manner, highlighting both their common concern with trustworthy path establishment and their fundamental differences in scope, trust semantics, and operational objectives.

A rigorous vis-à-vis analysis between CASTOR and SCION should begin from the observation that the two efforts address adjacent, but not identical, layers of the trustworthy networking problem. SCION is a path-aware inter-domain communication architecture that gives endpoints explicit control over path selection, while its control plane securely discovers and disseminates path segments that can be combined into end-to-end forwarding paths [8, 9, 1, 23]. By contrast, CASTOR addresses the broader challenge of trusted path routing across the compute continuum, where routing and service-placement decisions must account not only for connectivity and network performance, but also for the trustworthiness of devices, software, execution environments, and administrative domains [2, 4, 5]. Consequently, CASTOR and SCION should not be interpreted as directly competing solutions, but rather as complementary architectural approaches situated at different abstraction layers.

This interpretation is explicitly supported by CASTOR's own architectural baseline. D2.1 states that SCION is the only initiative that addresses the same general problem space as CASTOR, but at the same time clarifies that CASTOR is complementary to SCION by focusing on path-level trust and on the exchange of trust-related data between entities in intra- and inter-domain scenarios so as to facilitate the construction of a trust plane [2]. This is a particularly important point for the functional and business-model analysis of CASTOR. It indicates that the project's differentiating value does not lie in merely reproducing path-aware routing, but in augmenting path establishment with dynamic trust characterization, context-aware path qualification, and orchestration mechanisms spanning heterogeneous continuum environments.

A first key axis of comparison concerns *architectural scope*. SCION fundamentally redesigns inter-domain communication. The current control-plane Internet-Draft defines SCION as a path-aware inter-domain network architecture in which endpoints can choose between multiple path options, while the control plane discovers such paths via beaconing, registration, and lookup procedures [8]. The corresponding data-plane draft further specifies that SCION is path-aware because inter-domain forwarding directives are embedded directly in the packet header, thereby enabling routers to forward packets based on explicit path information rather than by relying on large inter-domain routing tables [9]. The CACM paper and the official SCION documentation frame the same design in terms of explicit path control, packet-carried forwarding state, multi-path resilience, and trust isolation through Isolation Domains (ISDs) and Trust Root Configurations (TRCs) [1, 23].

CASTOR, by contrast, does not merely seek to establish explicit paths. As evidenced in D2.1, D4.1, and D5.1, CASTOR aims to transform high-level service requirements into trust- and network-aware path decisions across the compute continuum [2, 4, 5]. This includes the consideration of trust properties at node, link, path, and domain levels, the maintenance of trusted topologies throughout runtime, and the continuous alignment of routing and orchestration decisions with required trust levels (RTL) and runtime-assessed actual trust levels (ATL) [4]. Hence, while SCION primarily secures and structures the inter-domain communication substrate, CASTOR addresses the richer problem of whether a path is *acceptable* for a specific service under evolving trust, risk, and resource conditions.

A second key axis concerns the *treatment of trust*. In SCION, trust is structured at the architectural level through ISDs and TRCs. The official documentation describes ISDs as groups of autonomous systems that operate as independent routing planes and share a set of trust roots, collectively governed by core ASes [23]. The CACM paper similarly emphasizes that SCION's isolation domains provide scoped trust,

Table 5.21: Compact comparison between SCION and CASTOR.

Dimension	SCION	CASTOR	Combined value
Primary scope	Path-aware inter-domain networking substrate [8, 9, 23]	Trusted communication and orchestration across the compute continuum [2, 4]	Trustworthy continuum-wide communication over a secure path-aware substrate [2, 5]
Core problem addressed	Secure, explicit, resilient inter-domain path selection and forwarding authorization [8, 9, 1]	Which path and service placement are acceptable under trust, security, and resource constraints [2, 4]	Policy-driven selection and maintenance of trustworthy end-to-end paths [2, 5]
Trust model	ISD/TRC-based inter-domain trust and path authorization [23, 9]	Federated trust quantification, attestation, runtime evidence, and path/domain trust synthesis [3, 4]	Path-aware routing enriched with runtime trust characterization [2, 5]
Path logic	Endpoints select from discovered path segments; forwarding directives embedded in packet headers [8, 9]	Optimization engine and policies compute trust-/network-aware path decisions [2, 4]	Trust-conditioned path selection and dynamic reconfiguration [2, 4, 5]
Architectural layer	Layer 3 inter-domain architecture [8, 9]	Layer 3 plus trust, attestation, and orchestration layers [3, 5]	Layered integration of secure transport substrate and trust plane [2, 5]
Operational focus	Network setup, path discovery, and forwarding authorization [8, 9]	Runtime trust monitoring, trust-policy enforcement, and service-aware assurance [4, 3]	End-to-end trustworthy service delivery under changing trust conditions [4, 5]
Relationship	Reference path-aware substrate	Trust-enabling orchestration and assurance framework	Complementary, tandem-capable architectures [2, 5]

control-plane isolation, and transparency for path selection, forwarding, and authentication [1]. In the data plane, the path authorization property ensures that packets traverse only path segments authorized in the control plane by all on-path ASes, while hop-by-hop forwarding authorization is enforced through authenticated Hop Fields [9]. This results in a powerful architecture for secure path-aware inter-domain transport.

However, CASTOR's trust model is substantially broader and more dynamic. D4.1 explicitly observes that, while SCION provides route control, failure isolation, and trust information for end-to-end service provisioning, it does not provide the means to systematically measure and evaluate trustworthiness [4]. CASTOR seeks to bridge this gap by enabling end-to-end trust characterization at the node, path, and domain levels through a Trust Assessment Framework, runtime evidence collection, and dynamic trust functions that evolve across the lifecycle of the topology [4]. Likewise, D2.1 frames CASTOR's contribution as the introduction of trust-plane mechanisms and dynamic trust governance in environments where most routing infrastructures still lack strong mechanisms for path-level trust [2].

This difference becomes even more pronounced when one considers CASTOR's device-side and topology-side trust enablers. D3.1 defines a CASTOR device-side Trusted Computing Base anchored in hardware

roots of trust and complemented by dedicated Trust Network Device Extensions (TNDE), Trace Units, and evidence-generation mechanisms [3]. The same deliverable stresses that CASTOR is not limited to implicitly trusted paths, but instead introduces key management and evidence-sharing mechanisms to support continuous trustworthiness appraisals both at the node level and at the topology level [3]. D3.1 further states that CASTOR supports both local and composite attestation, allowing trust assertions to be formed not only for individual devices, but also across links and end-to-end paths [3]. In this sense, SCION provides architectural trust for inter-domain communication, whereas CASTOR provides operational trust synthesis across network, compute, and device-integrity layers.

A third comparison axis concerns *path selection logic*. SCION's control plane discovers path segments through beaconing and makes them available for endpoint path construction [8]. The data plane then carries the inter-domain forwarding directives in the packet header, so that border routers validate the current Hop Field and forward packets accordingly [9]. In practical terms, this means that SCION gives users and services enhanced transparency and path control, allowing them to select from multiple available paths while benefiting from path authorization and failure isolation [1, 23]. D5.1 of CASTOR also recognizes this overlap explicitly, noting that both initiatives advocate networking technologies of transparency and path control, where the user or service provider retains visibility and selection capability over the employed path [5].

Nevertheless, D5.1 also clarifies the principal divergence: SCION essentially redesigns Layer 3, whereas CASTOR combines trust assessment with management and orchestration primitives [5]. In CASTOR, path construction is driven not only by topological availability but also by trust semantics, policy constraints, and optimization objectives. D2.1 formulates this in terms of multi-path control and agility for optimal $\{$network, trust$\}$-aware end-to-end path construction, where the objective is not merely to minimize traditional cost functions, but also to maximize the trust profile of the established path [2]. Therefore, SCION exposes candidate paths and secures their inter-domain use, while CASTOR contributes the higher-layer decision logic needed to evaluate which path should be selected for a given service under trust and resource constraints.

This observation is central to the complementarity argument. A SCION-enabled infrastructure can expose authenticated, resilient, and policy-constrained path alternatives, but it does not by itself determine whether the devices, routers, service nodes, or intermediate infrastructures involved in those paths satisfy runtime trust requirements. CASTOR introduces precisely these missing capabilities. D4.1 emphasizes continuous runtime trust evaluation, the maintenance of trusted topologies throughout operation, and the use of up-to-date trust policies to support accurate recommendations by the optimization engine [4]. D3.1 complements this with runtime tracing, introspection, and evidence handling tied to the operational behaviour of routing elements [3]. Accordingly, CASTOR may be understood as lifting path-aware routing into *trust-conditioned path-aware service orchestration*.

A fourth axis concerns *deployment orientation and maturity*. SCION is already a mature path-aware inter-domain technology with a clear protocol architecture and a growing ecosystem [23, 8, 9]. D5.1 acknowledges this maturity and contrasts it with CASTOR's current role as a research-driven proof of concept with a strong innovation and standardization footprint [5]. The same comparison table in D5.1 is especially helpful for this subsection, as it summarizes SCION as a *secure path-aware routing innovation*, whereas CASTOR is described as *trust and optimization driven path routing*. It further distinguishes the two across architectural layer, trust model, path computation, and handling of dependency scoping and sovereign operation challenges, noting that SCION primarily addresses such challenges during network setup while CASTOR addresses them during runtime operation [5].

This latter point is especially relevant from a business-model and functional-model perspective. D5.1 identifies a concrete *trust characterization gap* in SCION-style inter-domain scenarios. More specifically, it notes that peer ASes within an ISD do not have verifiable means to continuously measure the trustworthiness of other participants at runtime, nor do non-core ASes retain sovereignty over future trust-policy updates in the TRC [5]. It also highlights that flexible TRC semantics may complicate the management

of end-to-end service needs and that this creates a need for transparent trust-dependency scoping [5]. CASTOR's Trust Assessment Framework is then positioned as a way to realize context-dependent trust evaluations and inter-AS trust characterization under different trust properties and scopes [5]. This is one of the strongest arguments for tandem deployment: SCION structures and authenticates the inter-domain path substrate, whereas CASTOR contributes the runtime trust characterization needed to operate such paths under explicit sovereignty, trust, and service constraints.

From this perspective, the most accurate way to position CASTOR vis-à-vis SCION is neither as a replacement nor as a narrow overlay. Instead, CASTOR can be viewed as a trust-enabling and orchestration-oriented framework that can operate above, alongside, or in conjunction with SCION-like path-aware substrates. SCION offers explicit path control, multi-path operation, path authorization, and ISD/TRC-based trust partitioning [8, 9, 23]. CASTOR contributes device-side trusted computing bases, runtime evidence collection, local and composite attestation, path-level and domain-level trust synthesis, and optimization mechanisms that translate service intent into trustworthy path-establishment decisions [3, 4, 2]. In a tandem model, SCION can expose and secure candidate inter-domain paths, while CASTOR can evaluate whether these paths remain suitable for specific workloads in light of trust thresholds, runtime evidence, and evolving service requirements.

This tandem interpretation is not speculative; it is already embedded in CASTOR's own architectural narrative. D2.1 explicitly positions CASTOR as complementary to SCION [2], and D5.1 concludes that there is a clear path for conceptual synergy between the two in the context of inter-domain traffic engineering [5]. It further states that CASTOR's progression toward broader inter-domain evaluation aims to demonstrate how the framework can address sovereignty and dependency-scoping gaps within cross-domain trust relationships, particularly where trust semantics may differ between domains [5]. Therefore, the strongest and most defensible conclusion for the present subsection is that SCION and CASTOR occupy complementary positions in the emerging architecture of trustworthy continuum networking: SCION secures and exposes the path, while CASTOR determines whether that path is acceptable for a given service under given trust conditions.

Overall, the vis-à-vis analysis demonstrates that CASTOR extends beyond the state of the art represented by SCION in a semantically richer direction. SCION remains highly relevant as a secure, path-aware inter-domain networking substrate with explicit path control and strong forwarding authorization properties [8, 9, 1]. CASTOR, however, introduces the trust-plane, runtime evidence, and orchestration machinery necessary for continuously qualified path establishment across heterogeneous compute-continuum environments [2, 3, 4, 5]. This distinction is also important for the business model of CASTOR: its exploitable value lies not in re-implementing SCION's Layer 3 path-awareness, but in augmenting secure path-aware substrates with trust characterization, dynamic assurance, and policy-driven optimization. Such positioning provides a strong basis for presenting CASTOR as a complementary framework capable of operating in tandem with SCION to enable end-to-end trustworthy communications across heterogeneous infrastructures and administrative domains.

5.2.4 Business model interpretation

From a business model perspective, CASTOR is best interpreted as an enabling framework for differentiated trust-aware connectivity and orchestration services. This means that the value created by CASTOR does not derive from a single monolithic commercialization route. Instead, different parts of the framework can support different exploitation modalities, depending on the needs and maturity of the adopting organization.

A first business interpretation is *CASTOR as an orchestration enhancement layer*. Under this model, network operators, service providers, or infrastructure managers adopt CASTOR capabilities to improve the way services are placed, routed, and maintained in distributed or multi-domain environments. In this case, value is generated through better alignment between service requirements and the trust posture of

the underlying infrastructure, as well as through more defensible and auditable runtime decisions. This model is especially relevant for operators of critical communication infrastructures or distributed digital platforms where assurance requirements cannot be reduced to traditional performance metrics alone.

A second business interpretation is *CASTOR as a portfolio of technical enablers*. Because the project is modular by design, several of its core functions may have stand-alone exploitation value. These include trust assessment functions, attestation enablers, optimization modules, policy-driven orchestration interfaces, and controlled trust data handling capabilities. In such a model, CASTOR is not necessarily adopted in its entirety. Instead, selected artefacts can be embedded into existing vendor platforms, orchestration stacks, or domain-specific infrastructures. This modular exploitation route is commercially important because it reduces adoption barriers and supports incremental deployment strategies, which are generally more realistic in networking and critical infrastructure environments than wholesale architectural replacement.

A third business interpretation is *CASTOR as a foundation for high-assurance service differentiation*. In this model, infrastructure operators or service providers can use CASTOR to define and expose service classes or path profiles that differ not only in terms of bandwidth, latency, or availability, but also in terms of trustworthiness-related characteristics. This would enable offerings in which customers or dependent stakeholders select connectivity or service options on the basis of both performance and assurance expectations. In market terms, this shifts the proposition from generic connectivity toward trust-aware and policy-compliant service delivery. This interpretation is particularly coherent with the use case logic of CASTOR, where trusted path establishment is expected to support operationally sensitive scenarios such as connected mobility, airspace monitoring, and other communication environments where the consequences of path compromise or infrastructure degradation are not negligible.

Across these business interpretations, one common feature remains central: CASTOR transforms trust from an implicit background assumption into an explicit service and governance parameter. This has direct business implications. It enables not only better internal decision-making for operators, but also improved accountability, more structured assurance reporting, and stronger alignment with domain-specific security and compliance expectations. The resulting value proposition is therefore not limited to efficiency gains; it also includes transparency, resilience, policy compliance, and the potential for premium differentiated service offerings in environments where trust-aware operation has measurable operational relevance.

5.2.5 Concluding synthesis

Overall, the CASTOR functional and business model can be summarised as follows. Functionally, CASTOR is a modular framework for trust-/network-aware path establishment and assurance-driven orchestration, combining trust evidence collection, attestation, trust assessment, policy derivation, optimization, and runtime enforcement. It extends conventional networking and orchestration approaches by making trustworthiness an explicit, monitorable, and enforceable parameter of service delivery. Architecturally, CASTOR is intentionally modular and interoperable, which enables both full-framework adoption and selective integration of individual components into existing ecosystems.

From a business perspective, CASTOR is best viewed not as a single product template but as a flexible exploitation framework. It can support orchestration enhancement, stand-alone technical enablers, and differentiated high-assurance connectivity services, depending on the adoption context. Its comparison with SCION further clarifies this positioning: whereas SCION exemplifies a mature path-aware networking architecture, CASTOR's distinct contribution lies in embedding dynamic trust assessment, trust-context scoping, attestation-supported evidence generation, and runtime assurance logic into the operational processes of path establishment and service orchestration. In this sense, CASTOR defines a functional and business space centred on trustworthy connectivity, continuous assurance, and trust-informed service management across heterogeneous and potentially federated communication environments.

The functional and business interpretation presented in this section provides the conceptual basis for evaluating CASTOR's individual exploitable outcomes. Building on this perspective, the following section examines the identified KERs in terms of their role within the CASTOR framework, their expected exploitation route, and their preliminary potential for uptake beyond the project.

5.3 Initial KER Evaluation

5.3.1 Methodology

This section provides an initial evaluation of the exploitable results identified by the technical partners of the CASTOR project. The objective is to provide a structured overview of the Key Exploitable Results (KERs) emerging from the project, focusing on their technological maturity, observed strengths and limitations, and their preliminary relevance for potential market applications. The evaluation is based on the responses collected through the Market Analysis Questionnaire (MAQ) completed by project partners. Information provided in the questionnaire is mapped to specific evaluation elements to ensure traceability between the questionnaire responses and the KER assessment presented in this section.

Table 5.22 summarises how the relevant MAQ questions are used to derive the different elements of the initial KER evaluation.

Table 5.22: Mapping of MAQ questions to KER evaluation elements.

KER evaluation element	MAQ question
Identification of exploitable result	Q1
Responsible partner	Q2
Application domain	Q4
Observed limitations	Q9
Target users / adopters	Q8
Observed strengths	Q12
Current TRL	Q14
Expected TRL	Q15

The information collected from these responses is synthesised into a structured overview of the identified KERs, allowing a comparative assessment of their technological maturity, strengths, and limitations across the different application domains represented in the project. This initial evaluation does not constitute a full exploitation strategy. Instead, it provides a preliminary technical and market-oriented overview of the identified results, supporting the exploitation and business model development activities addressed in later work packages.

It should be noted that the MAQ responses initially described a broader set of exploitable artefacts, including both technology-core results and use-case-specific manifestations. For consistency with the consolidated KER structure and OSD classification adopted in Chapter 6 (Table 6.1), the present subsection organises the initial evaluation around the final five KER families retained at project level. As a result, some MAQ-derived entries previously presented separately are now grouped under broader consolidated KERs. In particular, orchestration-related artefacts are merged under *PCE-extension with trusted network orchestration*, while trusted device-, attestation-, and trust-evidence-related artefacts are grouped under *Trust Network Device Extensions (TNDE)*.

5.3.2 Initial KER Evaluation

Based on the MAQ responses and the final KER consolidation adopted by the project, five Key Exploitable Results (KERs) are retained for the initial evaluation: (i) Trust Assessment Framework (TAF), (ii) Trust Network Device Extensions (TNDE), (iii) Optimization Engine, (iv) Secure Oracle Layer, and (v) PCE-extension with trusted network orchestration. The following tables summarise the main characteristics of each KER, including the lead partner(s), application scope, indicative TRL progression, target users, and the main strengths and limitations derived from the partner inputs and the consolidated KER mapping.

Table 5.23: Initial evaluation of KER1 – Trust Assessment Framework (TAF).

Attribute	Description
Lead partner(s)	UKENT / UBITECH
Underlying MAQ basis	Primarily response #6; complemented by the consolidated project KER structure
Primary sector	Telecommunications, cybersecurity, and safety-critical network infrastructures
TRL progression	TRL 3 → TRL 6
Target customers / users	Enterprises, telecommunications operators, cloud and edge providers, public sector organisations, security administrators, network engineers, and infrastructure operators
Key strengths	Continuous trust evaluation based on verifiable evidence; dynamic trust propagation across network nodes and domains; support for trust-aware traffic engineering and policy-driven decision making in safety-critical and multi-domain environments
Observed limitations	Computational complexity of trust evaluation; scalability challenges in large network environments; limited standardisation for cross-domain trust exchange; dependence on reliable trust evidence collection and integration with orchestration logic
Indicative market signal	Growing demand for dynamic trust management and verifiable trust assessment in next-generation and critical communication infrastructures

Table 5.24: Initial evaluation of KER2 – Trust Network Device Extensions (TNDE).

Attribute	Description
Lead partner(s)	NVIDIA / UBITECH / SURREY
Underlying MAQ basis	Primarily response #4; complemented by the consolidated project KER structure and the grouping of trusted device interfaces, attestation enablers, cryptographic primitives, and dynamic tracing artefacts
Primary sector	Trusted network devices, data centre networking, device attestation, and trust-evidence generation across the compute continuum
TRL progression	Indicatively TRL 2 → TRL 5
Target customers / users	Enterprises, telecommunications operators, cloud providers, public sector organisations, infrastructure vendors, integrators of trusted networking environments, network equipment providers, infrastructure operators, and security administrators
Key strengths	Continuous device trust integration into routing and orchestration decisions; unified trust-evidence collection across heterogeneous network devices; support for attestation, monitoring, and secure evidence channels; consolidation of reusable trusted device-side enablers for continuum-wide trust management
Observed limitations	Immaturity of supporting technologies and standards; heterogeneous hardware and attestation mechanisms across vendors; operational complexity associated with continuous attestation and evidence collection; dependency on deployment-specific trusted hardware and protocol integration
Indicative market signal	Increasing interest in device attestation, confidential computing, trusted device interfaces, and Zero Trust networking for critical infrastructures and data centre environments

Table 5.25: Initial evaluation of KER3 – Optimization Engine.

Attribute	Description
Lead partner(s)	QUBITECH
Underlying MAQ basis	Response #2
Primary sector	Telecommunications and multi-domain network infrastructures
TRL progression	TRL 4 → TRL 7
Target customers / users	Telecommunications operators, cloud and edge providers, automotive OEMs, critical infrastructure operators, ISP backbone providers, government and defence networks, and operators of multi-domain communication infrastructures
Key strengths	Integration of formal trust modelling within a multi-objective path optimisation engine; ability to jointly optimise network performance and security/trust criteria; compatibility with existing SDN, PCE, and traffic engineering environments
Observed limitations	Increased computational complexity compared to traditional routing approaches; trade-offs between network performance and trust requirements; dependence on reliable telemetry, monitoring, and trust inputs
Indicative market signal	Increasing demand linked to secure multi-domain connectivity, traffic engineering, and trust-aware service optimisation under regulatory and resilience pressures

The updated KER structure presented above is aligned with the consolidated project view adopted in Chapter 7. Compared to the earlier MAQ-derived listing, this version provides a more coherent representation of the CASTOR exploitable portfolio by distinguishing between use-case-specific manifestations

Table 5.26: Initial evaluation of KER4 – Secure Oracle Layer.

Attribute	Description
Lead partner(s)	SUITE5 / UBITECH
Underlying MAQ basis	Primarily response #7; aligned with the project-level consolidation of the blockchain infrastructure and secure oracle functions
Primary sector	Secure data management, trusted data anchoring, and blockchain-supported trust evidence handling
TRL progression	TRL 5 $\rightarrow$ TRL 7
Target customers / users	Enterprises, SMEs, public sector organisations, service providers requiring secure and auditable trust evidence management, system administrators, security auditors, orchestration platforms, and entities consuming auditable trust-related data
Key strengths	Hardware-isolated validation of trust evidence; cryptographically verifiable storage and controlled anchoring of trust-related data; support for secure enclave-to-enclave communication and auditable trust data handling
Observed limitations	Dependence on specific hardware technologies and TEE implementations; potential latency and scalability constraints; operational dependencies related to integration with DLT, trust sources, and authorization mechanisms
Indicative market signal	Growing interest in secure evidence validation, trusted data exchange, and blockchain-supported auditability in critical and multi-stakeholder environments

Table 5.27: Initial evaluation of KER5 – PCE-extension with trusted network orchestration.

Attribute	Description
Lead partner(s)	UMU / WINGS
Underlying MAQ basis	Responses #0 and #5; consolidation of the earlier separate entries “PCE-extension with network orchestration” and “Trusted Path Orchestration framework”
Primary sector	Telecommunications, network orchestration, and edge-to-cloud service management
TRL progression	Indicatively TRL 2–4 $\rightarrow$ TRL 7
Target customers / users	Enterprises, telecommunications operators, cloud and edge providers, public sector organisations, network operations teams, telecom operators, industrial organisations, and public sector entities requiring trusted connectivity services
Key strengths	Policy-to-action automation for PCE/PCC operations; support for both reactive and proactive orchestration; SLA/SSLA-aware orchestration of network services; integration of trust telemetry and trust-aware decision logic into automated network and service management
Observed limitations	Integration complexity with heterogeneous network infrastructures and vendor-specific implementations; need for validation, rollback, and other operational safeguards; additional control-plane complexity and processing overhead due to continuous trust telemetry collection and evaluation
Indicative market signal	Increasing demand driven by network automation, intent-based networking, secure edge computing, and network-as-a-service models requiring stronger assurance and orchestration flexibility

and the cross-cutting technical KER families that form the basis of the project’s exploitation and open-source strategy. In particular, the final structure clarifies that CASTOR’s core exploitable outcomes are centred on trust assessment, trusted device-side evidence generation, trust-aware optimisation, secure trust-data handling, and orchestration enhancement.

This consolidated KER view also provides the basis for the Open-Source Development Plan presented in Chapter 6, where the retained KER families are further classified according to their proposed open-source, hybrid, or non-open-source exploitation route.

Chapter 6

Open Source Development Plan

Building on the market positioning, functional interpretation, and initial KER evaluation presented in Chapter 5, this chapter defines the Open-Source Development Plan for those CASTOR results whose exploitation potential is strengthened through openness, interoperability, external uptake, and ecosystem-oriented sustainability.

The Open-Source Development Plan (OSD Plan) constitutes a central pillar of CASTOR's overall exploitation strategy, not as a generic dissemination instrument, but as a structured mechanism for ensuring that selected project results achieve technical uptake, interoperability, long-term maintainability, and ecosystem relevance beyond the lifetime of the project. In the context of CASTOR, open-source is not treated as an objective in itself. Rather, it is considered a strategic exploitation modality for those KERs whose value is strengthened through openness, third-party reuse, validation by external communities, alignment with standardisation activities, and possible upstreaming into established open-source ecosystems. This positioning is already explicit in D7.1, where it is stated that some exploitable artefacts will be released as open source and where the Open-Source Development Plan is introduced as a dedicated activity aimed at identifying suitable artefacts and defining the corresponding development roadmap. In particular, D7.1 explicitly highlights Trust Assessment, Attestation Enablers, Crypto Primitives, and Misbehaviour Detection as the initial artefact families to be assessed in this direction [6].

D7.2 therefore represents the first operational step from vision to implementation. While D7.1 established the rationale, the links to OpenContinuum and Eclipse-related initiatives, and the structure of the OSD template, the present deliverable moves towards a more concrete identification of which CASTOR KERs are suitable for open-source release, under what conditions, and according to which release logic. This is fully aligned with the role assigned to D7.2 in D7.1, namely to provide a first detailed version of the exploitation strategy and to further specify those aspects of the roadmap that were intentionally left open at D7.1, including licensing, IPR handling, governance, and community-building arrangements.

From a strategic perspective, the role of open-source in CASTOR is tightly connected to the nature of the project itself. CASTOR develops modular trust and trustworthiness enablers for trusted path establishment across the compute continuum, bringing together trust assessment, attestation, hardware-based trust mechanisms, trusted-domain interaction, blockchain-supported auditability, orchestration, and risk-aware routing intelligence. D7.1 already describes these as modular exploitable assets that can be reused not only within the final integrated CASTOR framework, but also as standalone building blocks by network operators, routing vendors, hardware security providers, orchestration platforms, and service providers. This modularity is precisely what makes an OSD strategy relevant: selected artefacts can become reusable technical primitives, reference implementations, or integration enablers for a broader ecosystem, thereby increasing both the scientific and industrial impact of CASTOR.

In methodological terms, the present Open-Source Development Plan is based on two complementary sources of evidence. The first is the strategic and architectural groundwork already laid in D7.1, including the identification of the core exploitable assets, the project's stated intention to collaborate with Open-

Continuum and Eclipse-related ecosystems, and the OSD template dimensions covering business logic, licensing and IPR, community approach, governance, engagement, development environment, release approach, support, and sustainability. The second source is the partner questionnaire collected for the D7.2 exploitation work (see Chapter 7), which provides bottom-up partner insight on each KER's expected exploitation route, ownership assumptions, dependence on background IPR, anticipated new IPR, and post-project role. The value of combining these two inputs is that D7.1 captures the consortium-level ambition, whereas the questionnaire reflects the current partner-level exploitation preferences. The OSD Plan in D7.2 must therefore reconcile a top-down strategic direction with a bottom-up exploitation reality.

Table 6.1: CASTOR KERs, declared exploitation route, and proposed OSD status

KER	Lead partner	Declared exploitation route	Proposed OSD status	Rationale for classification
Trust Assessment Framework (TAF)	UKENT / UBITECH	Open-source; Standardisation contribution; Training & research	Confirmed OSS	Explicitly positioned as an open-source-oriented KER and fully aligned with the CASTOR OSD direction set out in D7.1, where Trust Assessment is identified among the artefact families to be considered under the open-source roadmap.
Trust Network Device Extensions (TNDE)	NVIDIA / UBITECH / SURREY	Open-source; Standardisation contribution; Training & research	Confirmed OSS	TNDE consolidates Trusted Domain Interfaces, Attestation Enablers, Cryptographic Primitives, and Dynamic Tracing into a unified KER centered on the communication, collection, protection, and monitoring of trustworthiness evidence across the compute continuum. This grouping is fully aligned with D7.1, which explicitly identifies Attestation Enablers, Crypto Primitives, and Misbehaviour Detection as priority artefact families under the CASTOR Open-Source Development Plan, while Trusted Domain Interfaces constitute reusable interoperability enablers with strong open-source potential.
Optimization Engine	QUBITECH	Commercial product/service; Licensing; Standardisation contribution	Non-OSS	The declared route remains predominantly commercial and licensing-oriented. Although selective release of interfaces or supporting artefacts may be considered in the future, the core engine is better classified at this stage as non-open-source.
Secure Oracle Layer	SUITE5 / UBITECH	As-a-service	Non-OSS	The current exploitation path is service-based and likely depends on implementation-specific integration and controlled deployment conditions. For this reason, the Secure Oracle Layer is more appropriately classified as non-open-source at this stage.
PCE-extension with trusted network orchestration	UMU / WINGS	Internal use; As-a-service; Training & research	Hybrid	This KER consolidates the orchestration-oriented artefacts of CASTOR, including trusted path orchestration and the PCE-extension for network orchestration. Its technical role is highly relevant for interoperability and integration, and selected interfaces, protocol extensions, policy hooks, or reference implementations could later be released openly. At the same time, the full operational stack is currently better represented by a hybrid exploitation model due to service-oriented and deployment-specific aspects.

The classification presented in Table 6.1 is particularly important because it reflects the distinction between consortium-level strategic intent and KER-level exploitation positioning. At the consortium strategy level, CASTOR presents open-source as a major route for community creation, technical uptake, and contribution to the broader compute continuum ecosystem. At the individual KER level, however, partners do not necessarily converge on the same route. Some KERs are already explicitly positioned as open-source in the questionnaire, whereas others are described as commercial, service-oriented, or internally exploited. For this reason, D7.2 should not present the open-source mapping as fully finalised in absolute terms. A more rigorous approach is to classify KERs into three categories, namely confirmed open-source KERs, hybrid KERs, and non-open-source KERs whose main exploitation route is commercial, internal, or service-based. Such a classification reflects the current maturity of the exploitation analysis and is fully consistent with the iterative nature of the CASTOR exploitation process already introduced in D7.1.

On the basis of the currently available evidence, two KERs can already be considered *confirmed open-*

source results, namely the **Trust Assessment Framework (TAF)** and the **Trust Network Device Extensions (TNDE)**. The inclusion of these two artefacts is fully coherent with the OSD direction introduced in D7.1. The Trust Assessment Framework corresponds directly to one of the artefact families explicitly named in the D7.1 OSD section. TNDE, in turn, consolidates a set of closely related technical building blocks, namely Trusted Domain Interfaces, Attestation Enablers, Cryptographic Primitives, and Dynamic Tracing, which collectively support the communication, collection, protection, and monitoring of trustworthiness evidence across the compute continuum. This grouping remains fully aligned with the D7.1 baseline, where Attestation Enablers, Crypto Primitives, and Misbehaviour Detection are explicitly identified as artefact families to be assessed under the CASTOR open-source roadmap.

The case for these two KERs is strong not only because their declared exploitation routes are open-source-oriented, but also because their technical role inherently benefits from openness. The Trust Assessment Framework is a horizontal reasoning and decision-support asset whose value depends on whether it can be inspected, evaluated, adapted, and integrated by third parties. Making such a framework open source facilitates independent validation of trust logic, reproducible experimentation, alignment with ongoing trust-related standardisation activities, and adaptation to domains beyond the original CASTOR pilots. TNDE exhibits the same logic at the level of device- and network-facing trust extensions. By consolidating mechanisms for trustworthiness evidence exchange, attestation support, cryptographic protection, and runtime observability, TNDE can act as a reusable technical substrate for trusted interaction across the compute continuum. Its open-source release can therefore strengthen interoperability, encourage technical scrutiny, and foster wider reuse by actors developing trusted infrastructure components and trust-aware services.

The consolidation of these technical elements into TNDE is particularly meaningful from an exploitation perspective. While Trusted Domain Interfaces, Attestation Enablers, Cryptographic Primitives, and Dynamic Tracing each represent distinct technical capabilities, they collectively support a common operational objective, namely the establishment, protection, and monitoring of trust-related interactions at the network and device level. Presenting them as a unified KER provides a more coherent view of CASTOR's open-source-oriented technical offering and better reflects the integrated nature of the underlying trust-enabling mechanisms. This grouped representation also improves alignment between the KER mapping and the actual architectural logic of CASTOR, where these functions are not intended to operate in isolation but as mutually reinforcing extensions of trust-aware networking devices and associated control functions.

A second category includes those KERs whose current exploitation route is better represented through *hybrid* or *non-open-source* models. In the updated alignment with D7.1, this applies primarily to the **Optimization Engine**, the **Secure Oracle Layer**, and the **PCE-extension with trusted network orchestration**. This classification does not diminish their technical value. On the contrary, these KERs are highly relevant and potentially commercially significant. However, their exploitation logic differs from that of the artefacts forming the open-source-oriented core of CASTOR.

The **Optimization Engine** is currently associated with a predominantly commercial and licensing-oriented route. This is understandable given its role in CASTOR's trusted-path establishment logic and its likely reliance on advanced multi-objective optimisation capabilities that may constitute a source of competitive differentiation. In such a case, a more controlled exploitation model is justified, at least for the present stage of the project. The **Secure Oracle Layer** is similarly positioned under an as-a-service route. As a result, its implementation may depend on controlled deployment conditions, integration-specific design choices, or other constraints that do not naturally favour immediate full open-source release. In both cases, the non-open-source classification should therefore be interpreted as a reflection of the current exploitation model rather than as a statement about the importance of the corresponding artefacts.

By contrast, the **PCE-extension with trusted network orchestration** is more appropriately positioned under a hybrid model. Its technical role in enabling trusted orchestration, integration, and policy-aware routing makes it relevant from an interoperability standpoint, and therefore selected components may

eventually be opened without requiring the release of the full operational stack. Such components may include interfaces, orchestration hooks, policy schemas, protocol extensions, reference implementations, test artefacts, or integration adapters. A hybrid model is therefore methodologically sound for this KER, as it allows CASTOR to preserve the benefits of openness where these are most useful, while maintaining appropriate control over deployment-specific logic, service-oriented elements, or partner-specific know-how.

This type of selective openness is fully compatible with the needs of CASTOR. An effective Open-Source Development Plan does not require a binary distinction between artefacts that are entirely open and artefacts that are entirely closed. In practice, for complex trust and security architectures, a hybrid approach is often the most appropriate option. Under such an approach, selected layers of a KER may be openly released in order to promote interoperability, transparency, research reuse, and ecosystem uptake, while other layers may remain restricted due to commercial sensitivity, background IPR constraints, security considerations, or service-oriented exploitation models. For CASTOR, this is particularly relevant because several KERs combine reusable technical building blocks with deployment-specific logic, partner-specific know-how, or tightly integrated service components. As a result, openness may be applied at the level of interfaces, APIs, SDKs, policy schemas, adapters, reference implementations, or validation tools, without necessarily implying the unrestricted release of the entire operational stack. Such a differentiated model allows CASTOR to preserve the strategic benefits of openness where these are most valuable, while maintaining appropriate control over components whose exploitation logic, protection requirements, or integration context justify a more limited release model.

This observation also suggests that the OSD Plan in D7.2 should articulate not only *which* KERs are intended for open-source release, but also *what exactly* is intended to be open-sourced within each KER. In practice, this may include complete repositories for some artefacts and partial releases for others, such as SDKs, libraries, policy schemas, API specifications, reference datasets, emulation scripts, test harnesses, demonstrators, or connector modules. This level of precision would considerably strengthen the OSD Plan, because it would move the discussion away from abstract labels and toward concrete release units. It would also better reflect the modular reality of the CASTOR architecture, in which the openness decision may differ between a core mechanism, its supporting tooling, and the deployment artefacts required for production-grade operation.

A further aspect that D7.2 should address in a more explicit way is the licensing and IPR strategy. D7.1 clearly states that these aspects remained open at the time of its preparation and would be further elaborated in D7.2. The questionnaire responses confirm why this is necessary: several KERs depend on background IPR, some involve shared or yet-to-be-defined ownership, and some foresee new software copyright, methodological assets, or potentially protectable technical mechanisms. Accordingly, the OSD Plan should not yet commit to a single licence across all artefacts. Instead, it should define a decision framework. A reasonable position for D7.2 is that CASTOR will favour business-friendly and interoperability-oriented open-source licences for those KERs confirmed for open-source release, while ensuring compatibility with background dependencies and future industrial uptake.

For CASTOR, a prudent and academically defensible formulation is that licences should be selected per KER, or even per release unit, on the basis of four main criteria: compatibility with background code and third-party dependencies; consistency with the intended exploitation route; suitability for fostering industrial and research uptake; and acceptability for possible upstreaming into recognised foundations or community repositories. This approach avoids premature rigidity while demonstrating that the consortium is addressing the issue systematically and in a manner consistent with the heterogeneous nature of the CASTOR artefact portfolio.

Beyond licensing, the sustainability of the OSD Plan depends on governance and community structures. D7.1 already points to possible engagement with OpenContinuum, Eclipse-related initiatives, ETSI OSM, and related communities as future channels for uptake and upstreaming. This is an important strength of CASTOR's strategy and should be further developed in D7.2. A credible open-source roadmap re-

quires, at minimum, agreement on repository hosting, maintainership, contribution review, release approval, security handling, and post-project stewardship. During the project, repositories can remain under consortium-controlled infrastructure, with the KER owner and contributing technical partners acting as maintainers. At least for the confirmed open-source KERs, D7.2 should foresee the preparation of repository-level documentation, contribution rules, issue tracking, release tagging, and a lightweight review workflow.

Beyond the project lifetime, CASTOR can evaluate whether selected mature artefacts should remain under consortium stewardship, transition to partner-maintained repositories, or be proposed for onboarding into a more formal open-source ecosystem. In this respect, the OSD Plan should be understood as a roadmapping instrument rather than a static declaration. Its purpose is not only to identify open-source KERs, but also to define the conditions under which those KERs can evolve into sustainable community assets rather than one-off project releases.

Overall, the revised OSD Plan establishes a coherent and implementation-oriented classification of CASTOR's artefacts with respect to openness. It identifies the **Trust Assessment Framework (TAF)** and the **Trust Network Device Extensions (TNDE)** as the open-source-oriented core of the CASTOR roadmap. At the same time, it acknowledges that other KERs, including the **Optimization Engine**, the **Secure Oracle Layer**, and the **PCE-extension with trusted network orchestration**, currently follow controlled or hybrid exploitation paths. In this way, the chapter remains fully aligned with the terminology and KER mapping introduced in D7.1, while providing a more operational foundation for the subsequent elaboration of licensing, governance, repository strategy, and community-building actions in the remainder of D7.2.

Chapter 7

Exploitation and Integration of CASTOR

This chapter builds on the analytical basis established in Chapters 5 and 6 by addressing the exploitation and integration perspectives of the CASTOR project. While Chapter 5 examined the market context, the functional and business positioning of CASTOR, and the initial evaluation of the project Key Exploitable Results (KERs), and Chapter 6 defined the Open-Source Development Plan (OSD) and the corresponding openness classification of the consolidated KER portfolio, the present chapter focuses on how these results may translate into concrete value creation and exploitation pathways at use-case and partner level. The objective is therefore twofold. First, the chapter examines how the CASTOR framework may create value within the operational environments represented by the project use cases. Second, it outlines how individual partners may further develop, integrate, adopt, or exploit CASTOR results in line with their technological role, organisational priorities, and target application domains.

The chapter is structured accordingly. Section 7.1 analyses the value proposition of CASTOR in the context of the project use cases, highlighting the expected operational improvements and the conditions that may support uptake in the corresponding domains. Section 7.2 complements this view by presenting the individual exploitation perspectives of the consortium partners, thus connecting the consolidated CASTOR KER structure with partner-specific development, integration, research, service, and market uptake pathways. Taken together, these sections provide the first project-level view of how CASTOR results may move from technical development and validation toward post-project use, integration, and exploitation.

7.1 CASTOR Value Proposition per Use Case

This section analyses the value proposition of the CASTOR framework in relation to the project use cases. The objective is to describe how the capabilities developed in CASTOR may create value in the operational contexts addressed by the project, highlighting the potential improvements compared to existing practices and the conditions that may support their adoption. The analysis is based on the responses collected through the Market Analysis Questionnaire (MAQ) from project partners. In particular, the sections draw on partner inputs describing the innovation potential of the CASTOR results and their expected contribution to operational environments. The discussion therefore reflects the perspectives of partners involved in the development and validation of CASTOR technologies within the project use cases. For each use case, the analysis describes the operational context in which the CASTOR capabilities may be applied, the expected improvements enabled by the framework, and the factors that may influence the adoption of these capabilities. The information presented in this section primarily derives from the MAQ responses related to innovation potential and value creation (Q11–Q12), complemented by insights on adoption drivers and constraints (Q8–Q9). The following subsections analyse the four CASTOR use cases defined in the project: secure airspace monitoring in urban air mobility environments, trustworthy communications for first responder mobile units, priority-based trusted messaging for cooperative con-

nected and automated mobility applications, and next-generation UAV communications. Each subsection presents the operational context of the use case and summarises the value proposition of CASTOR in that specific application environment. Table 7.1 summarises the MAQ responses used to inform the analysis of each use case. As some partners operate across multiple application domains, certain responses contribute to more than one use case analysis.

Table 7.1: MAQ responses informing the use-case value proposition analysis.

Use Case	MAQ Responses	Lead Partner(s)
UC1 – Secure Airspace Monitoring in Urban Air Mobility (UAM)	#1	Collins Aerospace
UC2 – Trustworthy Communications of First Responder Mobile Units	#0, #2, #4, #5, #7	UMU, QUBITECH, NVIDIA, WINGS, SUITE5
UC3 – Priority-based Trusted Messaging for CCAM Applications	#8	Commsignia Ltd.
UC4 – Future-Proofing Next-Generation UAV Communications	#3, #6	K3Y, University of Kent (UKENT)

7.1.1 Use Case 1 – Secure Airspace Monitoring in Urban Air Mobility (UAM)

The operational context of this use case is derived from the MAQ response related to aerospace monitoring environments (MAQ Q11, response #1). According to the partner input, airspace monitoring infrastructures rely on distributed communication environments where multiple system components exchange operational data across communication networks supporting monitoring and coordination functions. In the current baseline configuration, monitoring infrastructures depend on established communication mechanisms and infrastructure-level security controls. The MAQ response indicates that trust validation mechanisms are not always explicitly incorporated into communication management processes, and infrastructures typically rely on predefined configurations and conventional security mechanisms to ensure the integrity and reliability of data exchanges.

The MAQ response highlights that CASTOR explores mechanisms aimed at strengthening trust verification within communication infrastructures supporting monitoring environments. In particular, the project investigates approaches that allow trust-related information to be incorporated into communication management processes. These mechanisms aim to enable infrastructures where trust conditions associated with infrastructure components or communication environments can be evaluated and considered in communication operations. Such capabilities may support environments where monitoring infrastructures can incorporate additional trust verification mechanisms within distributed communication infrastructures.

From the perspective of the partner response, the value of these capabilities lies in the potential to improve the resilience and trustworthiness of communication infrastructures supporting airspace monitoring environments. Strengthening trust verification mechanisms within communication infrastructures may support more reliable monitoring services in environments where multiple systems interact across distributed infrastructures. In addition, the partner response highlights that improvements in trust verification mechanisms may contribute to strengthening the protection of infrastructures supporting aerospace monitoring services. These factors indicate that trust-aware communication mechanisms may provide additional assurance in environments where reliable monitoring and coordination of airspace activities are required. To further illustrate the relationship between the operational needs of UAM airspace monitoring environments and the capabilities enabled by the CASTOR framework, the Value Proposition Canvas (VPC) is applied to this use case. The canvas maps the main operational challenges and expected

benefits identified in the partner response against the mechanisms explored in CASTOR, providing a structured representation of the potential value creation for stakeholders operating in UAM monitoring infrastructures. The resulting Value Proposition Canvas for this use case is presented in Figure 7.1.

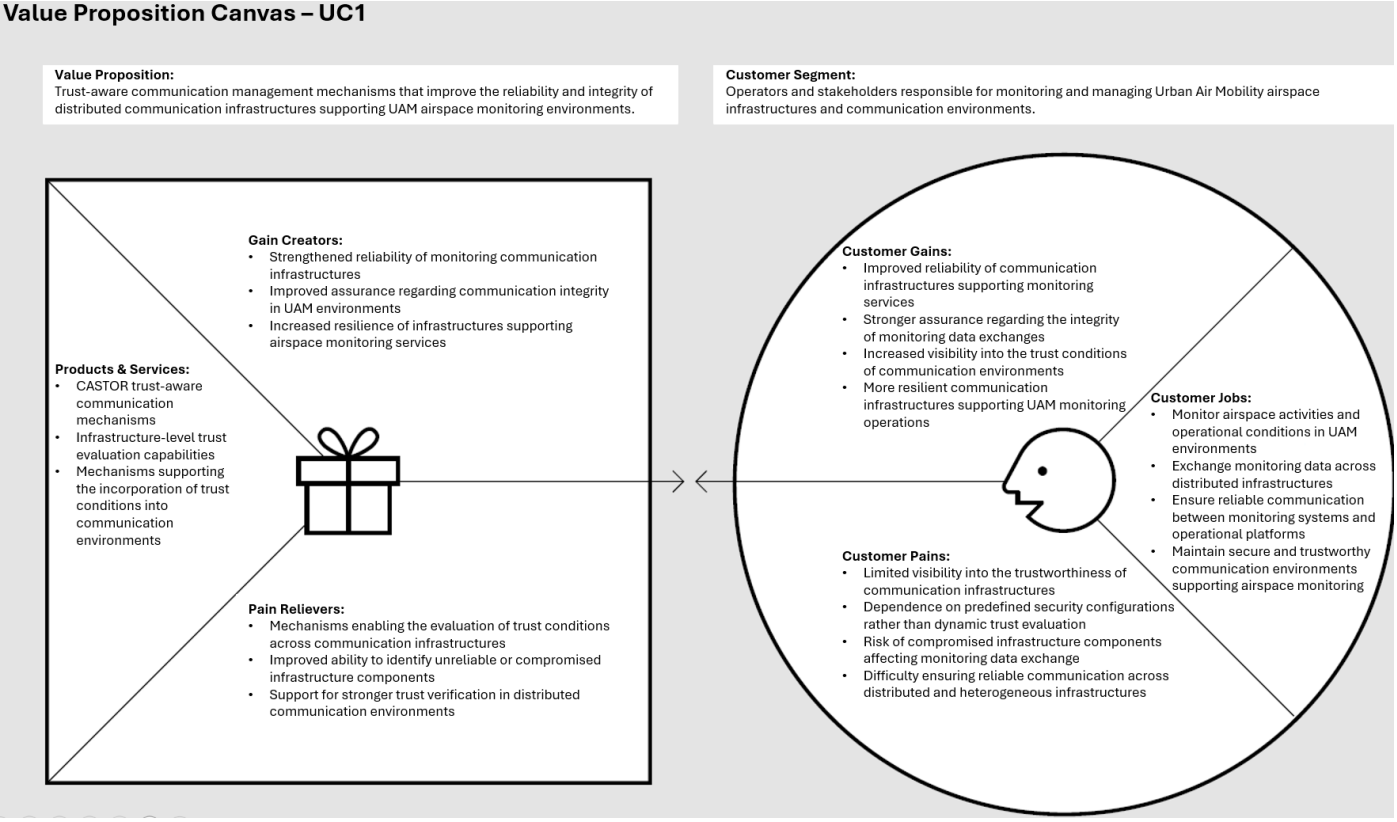

Figure 7.1: Value Proposition Canvas – UC1.

7.1.2 Use Case 2 – Trustworthy Communications of First Responder Mobile Units

The operational context of this use case is derived from MAQ responses related to communication infrastructures supporting mission-critical and distributed operational environments (MAQ Q11, responses #0, #2, #4, #5 and #7). These responses describe communication environments where mobile units interact with backend infrastructures and digital services through heterogeneous network infrastructures. According to the partner inputs, such environments rely on communication infrastructures that enable data exchange between mobile units, operational platforms, and supporting digital infrastructures. These infrastructures may involve multiple technological components and organisational domains, including communication networks, infrastructure services, and computing environments supporting operational coordination. The responses indicate that communication environments supporting distributed operational systems typically rely on established networking infrastructures and security mechanisms to ensure reliable data exchange. However, trust verification mechanisms across infrastructure components or communication environments may not always be explicitly integrated into communication management processes.

Within this context, the MAQ responses highlight the potential role of CASTOR in introducing mechanisms that support the evaluation and management of trust conditions within communication infrastructures. In particular, the responses refer to approaches that allow trust-related information associated with infrastructure components or communication environments to be considered in communication processes. These mechanisms aim to support communication infrastructures where trust conditions can be assessed across distributed environments and incorporated into communication management opera-

tions. According to the partner responses, such capabilities may strengthen the ability of infrastructures to manage communication environments involving multiple system components and infrastructure domains.

From the perspective of the MAQ responses, the expected value of these capabilities lies in improving the reliability and resilience of communication infrastructures supporting distributed operational environments. Strengthening the ability to evaluate trust conditions within communication infrastructures may support environments where communication services can operate with increased assurance regarding the integrity of infrastructure components and communication environments. In addition, the responses highlight that the adoption of stronger trust verification mechanisms in communication infrastructures may support environments where infrastructure protection and operational reliability are important considerations. These aspects indicate that mechanisms supporting trust-aware communication management may contribute to strengthening communication environments supporting distributed operational systems. To further illustrate the relationship between the operational needs of mission-critical mobile communication environments and the capabilities enabled by the CASTOR framework, the Value Proposition Canvas (VPC) is applied to this use case. The canvas maps the operational challenges and expected benefits identified in the partner responses against the mechanisms explored in CASTOR, providing a structured representation of the potential value creation for stakeholders responsible for managing communication infrastructures supporting mobile operational units. The resulting Value Proposition Canvas for this use case is presented in Figure 7.2.

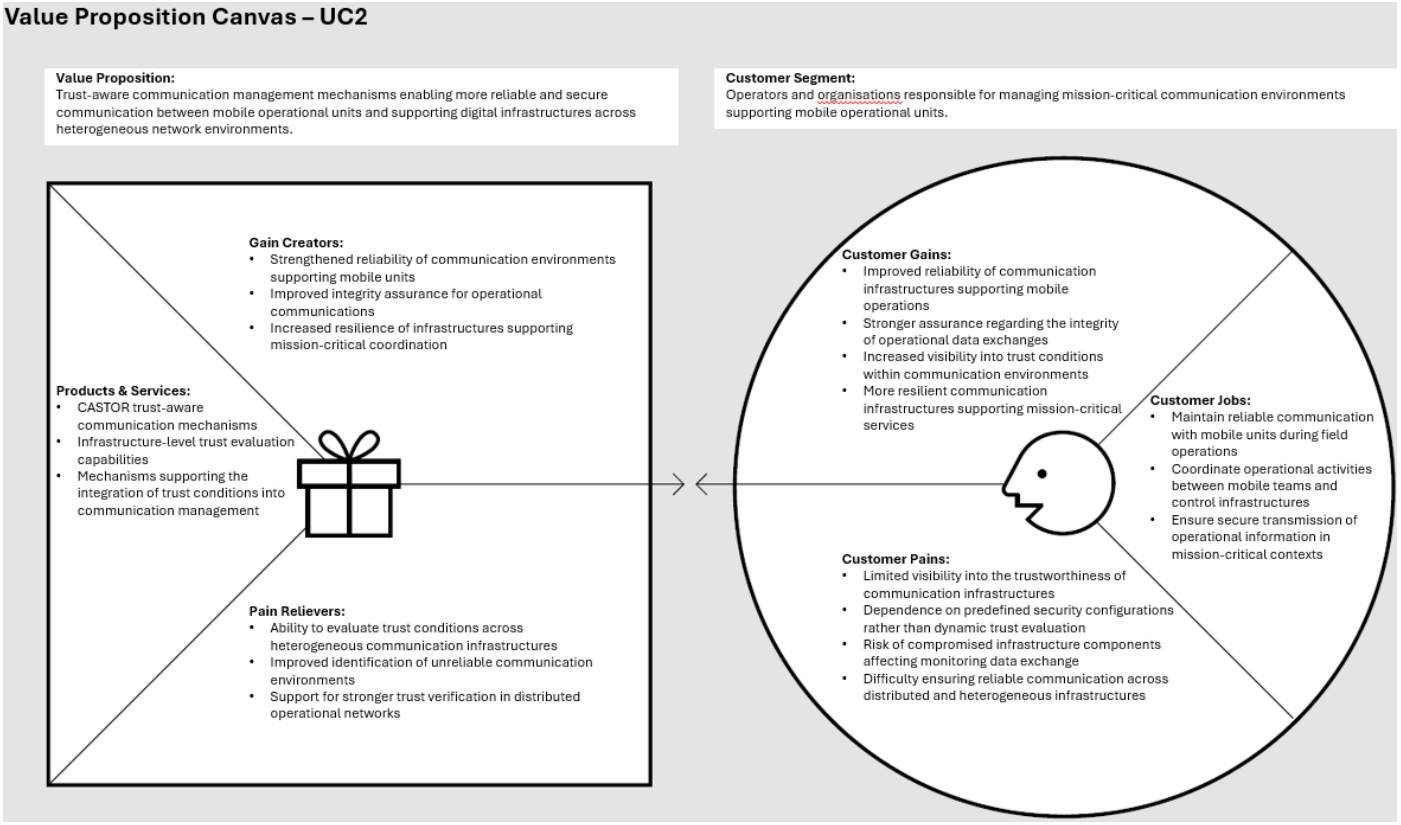

Figure 7.2: Value Proposition Canvas – UC2.

7.1.3 Use Case 3 – Priority-based Trusted Messaging for CCAM Applications

This use case focuses on communication environments supporting Cooperative, Connected and Automated Mobility (CCAM) applications, where vehicles exchange operational information with other vehicles, roadside infrastructure, and backend systems. The partner response related to this use case highlights communication environments where connected mobility services depend on the reliable exchange of data across distributed infrastructures (#8). In these environments, communication infrastruc-

tures support the exchange of messages used for coordination, situational awareness, and safety-related functions. Such systems typically rely on established communication technologies and networking infrastructures that enable interactions between vehicles and infrastructure components. In this baseline configuration, security mechanisms are generally implemented through established networking and authentication mechanisms, while trust verification across communication environments is not necessarily integrated into communication management processes.

The partner response highlights that CASTOR explores mechanisms aimed at improving trust verification within communication environments supporting connected mobility systems. In particular, the project investigates approaches that allow trust-related information associated with infrastructure components or communication environments to be incorporated into communication management processes. These capabilities may support environments where communication infrastructures can evaluate trust conditions associated with communication paths or infrastructure components. Such mechanisms may enable communication systems to incorporate trust-related considerations into the management of message exchanges across distributed infrastructures supporting CCAM services.

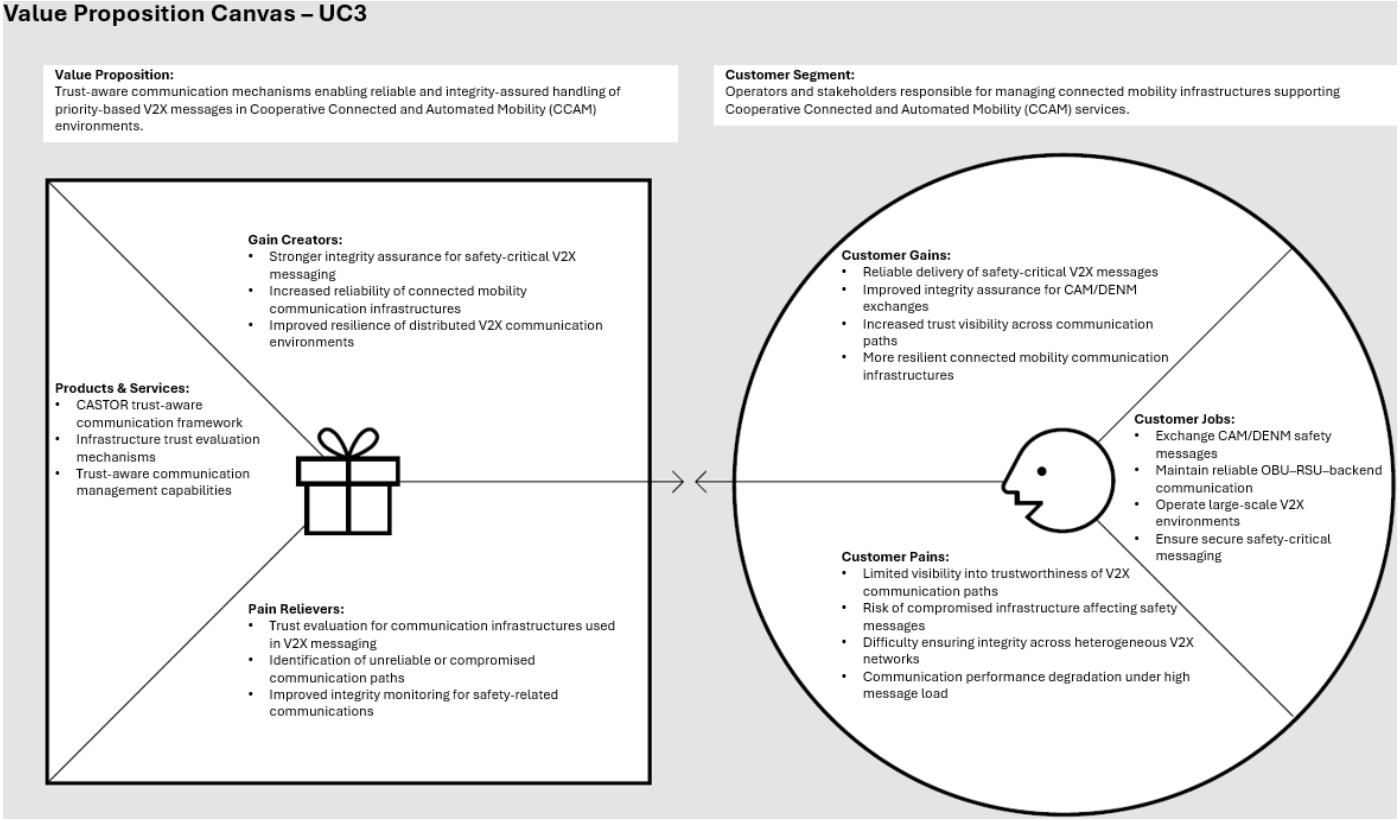

Figure 7.3: Value Proposition Canvas – UC3.

From the perspective of the partner response, the value of these capabilities lies in strengthening the reliability and integrity of communication infrastructures supporting connected mobility applications. By enabling mechanisms that support the evaluation of trust conditions within communication environments, CASTOR may contribute to improving the resilience of communication infrastructures used for message exchange in CCAM systems. In particular, the introduction of mechanisms supporting trust-aware communication management may provide additional assurance regarding the integrity of communication environments supporting connected mobility services, where reliable message exchange between vehicles and infrastructure components is essential for operational coordination. To further illustrate the relationship between the operational requirements of CCAM communication environments and the capabilities enabled by the CASTOR framework, the Value Proposition Canvas (VPC) is applied to this use case. The canvas maps the operational needs and constraints identified in the partner response against the trust-aware communication mechanisms explored in CASTOR, highlighting the potential value creation

for stakeholders involved in connected and automated mobility infrastructures. The resulting Value Proposition Canvas for this use case is presented in Figure 7.3.

7.1.4 Use Case 4 – Future-Proofing Next-Generation UAV Communications

This use case relates to communication environments supporting unmanned aerial vehicle (UAV) systems, where reliable connectivity is required to enable coordination between aerial platforms, ground infrastructures, and supporting digital services. The partner responses associated with this use case describe distributed communication environments where UAV operations depend on networking infrastructures enabling data exchange across multiple system components and communication domains (#3, #6). In such environments, communication infrastructures support interactions between aerial systems, infrastructure components, and operational platforms involved in UAV operations. These infrastructures typically rely on established networking technologies and security mechanisms to ensure reliable communication across distributed environments. According to the partner responses, trust verification across communication infrastructures is generally addressed through conventional security mechanisms, while explicit mechanisms for evaluating trust conditions across infrastructure components are not always integrated into communication management processes.

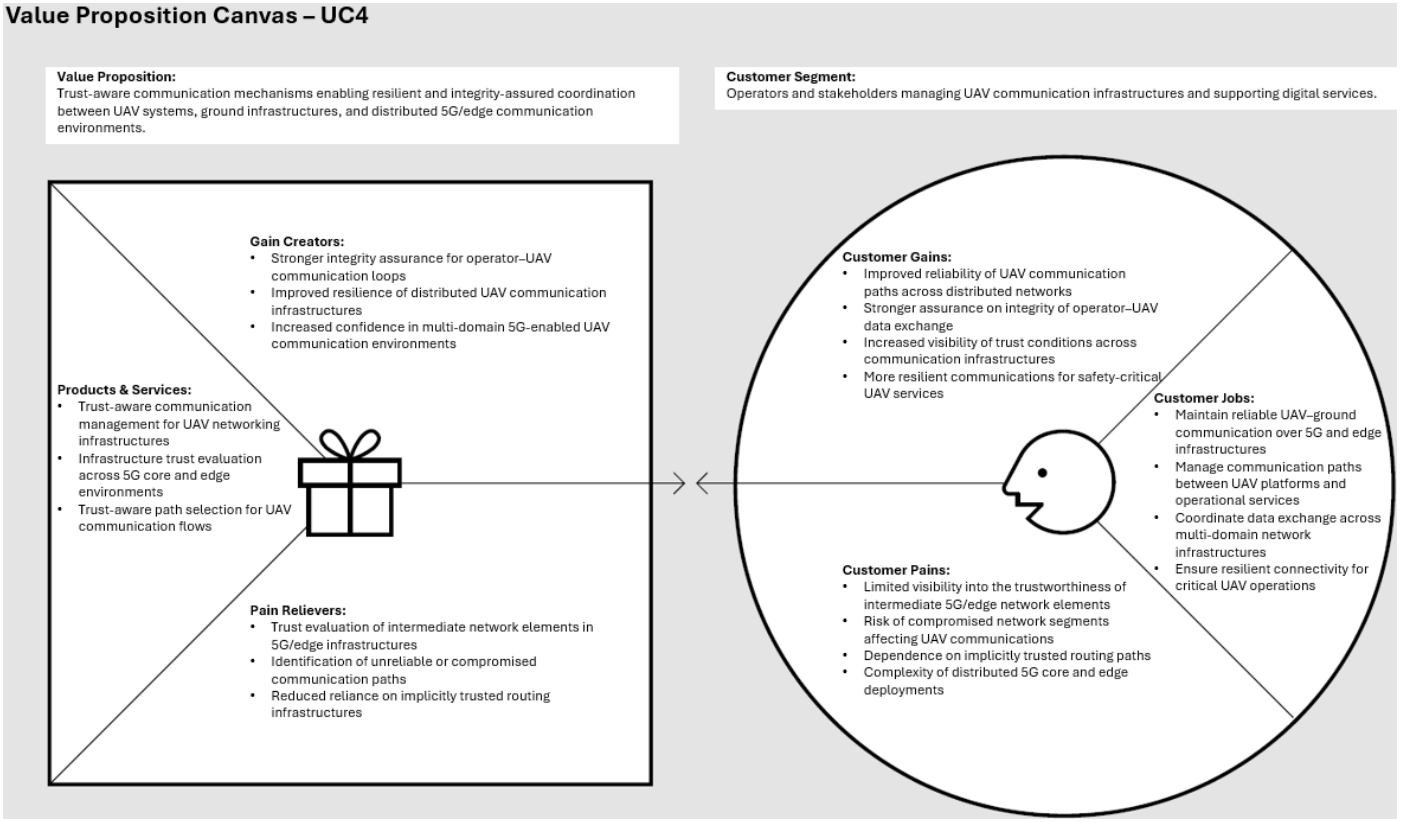

Figure 7.4: Value Proposition Canvas – UC4.

The partner responses highlight that CASTOR investigates mechanisms aimed at improving trust management within communication infrastructures supporting UAV communication environments (#3, #6). In particular, the project explores approaches that allow trust-related information associated with infrastructure components and communication environments to be incorporated into communication management processes. These mechanisms may enable communication environments where trust conditions can be evaluated across distributed infrastructures supporting UAV operations. By enabling infrastructures to consider trust-related information when managing communication environments, CASTOR aims to support more robust communication environments capable of operating across heterogeneous infrastructures and multiple operational domains.

From the perspective of the partner responses, the expected value of these capabilities lies in strengthening the reliability and resilience of communication infrastructures supporting UAV operations (#3, #6). By introducing mechanisms that support the evaluation of trust conditions within communication environments, CASTOR may contribute to improving the integrity and robustness of infrastructures used to support UAV communication services. Such capabilities may support stakeholders involved in UAV operations by providing improved assurance regarding the reliability of communication infrastructures and the integrity of data exchanges across distributed infrastructures supporting aerial systems. To further illustrate the relationship between the communication requirements of next-generation UAV environments and the capabilities enabled by the CASTOR framework, the Value Proposition Canvas (VPC) is applied to this use case. The canvas maps the operational needs and constraints identified in the partner responses against the trust-aware communication mechanisms explored in CASTOR, highlighting the potential value creation for stakeholders responsible for managing UAV communication infrastructures. The resulting Value Proposition Canvas for this use case is presented in Figure 7.4.

7.2 Partners' Individual Exploitation Plans

This section outlines the preliminary exploitation perspectives of the CASTOR partners based on the responses collected through the Market Analysis Questionnaire (MAQ). The objective is to provide an overview of how individual partners envisage the potential use and development of the results emerging from the project, considering their technological contributions, application domains, and organisational objectives. While the previous sections analysed the market environment, the technological results of the project, and the value proposition across the use cases, this section focuses on the partner-level perspective on exploitation. The analysis highlights how the participating organisations foresee integrating or developing the project results within their technological portfolios, research activities, or operational environments. The information presented in this section is derived directly from the MAQ responses provided by the partners. In particular, the analysis draws on responses describing innovation potential, strengths and opportunities associated with the project results, intended usage scenarios, and potential constraints or dependencies affecting future exploitation activities.

Table 7.2 summarises how the relevant MAQ questions are used to derive the different elements of the partner exploitation analysis.

Table 7.2: Mapping of MAQ responses to partner exploitation analysis elements.

Exploitation analysis element	MAQ question
Innovation potential of the developed solution	Q11
Observed strengths and value of the results	Q12
Opportunities for further development or application	Q13
Intended exploitation or usage scenarios	Q16
Dependencies or conditions affecting exploitation	Q17
Collaboration requirements and ecosystem aspects	Q18
IPR considerations	Q19

To provide an overview of the exploitation perspectives across the consortium, Table 7.3 summarises the partners, their primary exploitation role, and the consolidated KERs to which their expected post-project activities are most closely related.

The following subsections describe the individual exploitation perspectives of each partner, summarising the intended usage of the project results, the expected application contexts, and the main conditions

Table 7.3: Partners with explicit linkage to the consolidated CASTOR KERs.

Partner	Basis	Associated consolidated KER(s)	Primary application / exploitation context
UMU	MAQ #0	PCE-extension with trusted network orchestration	Telecommunications, network automation and orchestration
Collins Aerospace	MAQ #1	PCE-extension with trusted network orchestration (use-case integration context)	Aerospace / UAM communication infrastructures
QUBITECH	MAQ #2	Optimization Engine	Telecommunications and multi-domain network infrastructures
K3Y	MAQ #3	PCE-extension with trusted network orchestration (use-case integration context)	Drone communication and UAV networking systems
NVIDIA	MAQ #4	Trust Network Device Extensions (TNDE)	Data centre networking and trusted network device functions
WINGS ICT Solutions	MAQ #5	PCE-extension with trusted network orchestration	Network orchestration and edge-to-cloud service management
University of Kent (UKENT)	MAQ #6	Trust Assessment Framework (TAF)	Telecommunications, cybersecurity, and trust management in network infrastructures
SUITE5	MAQ #7	Secure Oracle Layer	Secure data handling and blockchain-supported trust evidence management
Commsignia Ltd.	MAQ #8	PCE-extension with trusted network orchestration (use-case integration context)	Automotive / V2X communication environments
University of Surrey	MAQ #9	Trust Network Device Extensions (TNDE)	Cryptographic support for trusted routing path proof and attestation-related mechanisms
UBITECH	MAQ #10	Trust Assessment Framework (TAF); Trust Network Device Extensions (TNDE); Secure Oracle Layer	Cross-cutting trust integration, secure evidence handling, and orchestration support across CASTOR domains

that may influence their future development and adoption. Several partners also highlight that the exploitation of CASTOR results depends on ecosystem-level factors, including interoperability with existing networking platforms, collaboration with infrastructure operators, and alignment with evolving standards and regulatory frameworks.

7.2.1 UMU

UMU contributes to CASTOR through research activities related to network orchestration and trust-aware management of communication infrastructures, associated with the PCE-extension and orchestration capabilities now consolidated under the PCE-extension with trusted network orchestration KER family. From the perspective of exploitation, the partner indicates that the results may support future research and technology development activities in network orchestration environments, particularly in contexts where distributed communication infrastructures require flexible and policy-driven management. The responses indicate that the potential application context includes telecommunications infrastructures and distributed network environments, where orchestration mechanisms can support the coordination of network services across multiple domains. The expected value of the developed capabilities lies in supporting more adaptive management of network services and infrastructures, particularly in environments where automation and policy-based control mechanisms are increasingly relevant. At the same time, the responses highlight that future exploitation may depend on integration with existing network orchestration frameworks and management platforms, as well as further development and validation activities required to transition research prototypes into operational environments.

7.2.2 Collins Aerospace

Collins Aerospace contributes to CASTOR through activities related to secure communication infrastructures for aerospace environments, particularly in contexts where communication networks support UAV operations and safety-critical aerospace services. Within the project, the partner's contribution is associated with the exploration of security architectures and trust mechanisms applicable to aerospace commu-

nication infrastructures. From an exploitation perspective, the partner responses indicate that the results may support future developments in secure networking solutions for aerospace systems, where communication infrastructures must satisfy strict requirements related to reliability, resilience, and cybersecurity. Potential application contexts include UAV communication environments and aerospace infrastructures supporting distributed operational systems, where secure coordination between multiple infrastructure components is required. The responses also indicate that the exploitation of these results may depend on alignment with certification procedures and regulatory frameworks typical of aerospace environments, as well as on the integration of the developed mechanisms within existing aerospace communication infrastructures.

7.2.3 QUBITECH

QUBITECH contributes to CASTOR through the development of mechanisms related to network optimisation and routing management in distributed communication infrastructures, associated with the Optimization Engine identified among the project Key Exploitable Results. Within the project, the partner explores approaches that support the optimisation of network operations across infrastructures involving multiple domains and communication environments. From an exploitation perspective, the partner responses indicate that the developed capabilities may support future technology development activities related to network optimisation and routing management in telecommunications infrastructures. The potential application contexts include operator-managed communication environments, distributed network infrastructures, and service environments where routing decisions must be adapted to complex operational conditions. The expected value lies in supporting more informed and adaptive optimisation of network services across infrastructures characterised by multiple communication paths and heterogeneous operational constraints. At the same time, future exploitation is expected to depend on compatibility with existing routing, traffic engineering, and network management environments, as well as on further validation in realistic operational contexts.

7.2.4 K3Y

K3Y contributes to CASTOR through activities related to communication infrastructures supporting UAV systems, particularly in environments where coordination between multiple aerial platforms and ground infrastructures is required. From an exploitation perspective, the partner is expected to build on the project results to support future trust-aware communication solutions for UAV platforms, particularly in operational settings involving drone swarms or distributed aerial coordination. In such contexts, communication infrastructures must support reliable and secure information exchange between aerial systems and supporting ground or edge infrastructures. The exploitation value of the CASTOR contribution lies in the possibility of strengthening communication robustness and trust-awareness in UAV networking environments. At the same time, post-project exploitation is expected to depend on integration with UAV communication platforms and supporting infrastructures, as well as on the broader evolution of communication technologies and governance requirements relevant to UAV networking environments.

7.2.5 NVIDIA

NVIDIA contributes to CASTOR through trusted communication mechanisms for networked infrastructures, associated in particular with trusted network device interfaces and the wider trusted device-side evidence handling functions now consolidated under the Trust Network Device Extensions (TNDE) KER family. From an exploitation perspective, the developed capabilities may support future networking environments in which trust verification mechanisms are integrated directly into communication infrastructures, especially in data centre networking and distributed computing environments. The expected value

lies in enabling trust-related information to be associated with network devices and infrastructure components in a systematic and reusable way, thereby supporting stronger assurance in infrastructure management and orchestration processes. Future exploitation is likely to depend on compatibility with existing hardware and software ecosystems supporting large-scale computing infrastructures, as well as on interoperability with trusted hardware, attestation mechanisms, and networking technologies used in high-performance or cloud-scale environments.

7.2.6 WINGS ICT Solutions

WINGS contributes to CASTOR through activities related to trusted path orchestration across distributed communication infrastructures, now consolidated under the PCE-extension with trusted network orchestration KER family. From an exploitation perspective, the partner is expected to use the results as a basis for future orchestration platforms and service-management solutions targeting distributed infrastructures, particularly in edge-to-cloud environments where communication services and workloads must be coordinated across heterogeneous infrastructures. The expected value of these results lies in supporting service-aware and trust-aware orchestration logic capable of coordinating communication paths and service deployment decisions across multiple infrastructure components. Future exploitation is likely to depend on interoperability with orchestration frameworks and cloud/edge platforms, as well as on further integration work required to embed the proposed mechanisms into operational service environments and platform offerings.

7.2.7 University of Kent (UKENT)

The University of Kent contributes to CASTOR through activities related to trust evaluation and trust propagation in communication infrastructures, associated with the Trust Assessment Framework (TAF). From an exploitation perspective, the partner is expected to use these results primarily as a basis for future research, technology development, and advanced trust assessment capabilities in network environments operating across multiple administrative or technological domains. Potential application contexts include network security analytics, trust monitoring, and environments where communication infrastructures require more explicit and evidence-based trust evaluation. The exploitation value of the result lies in improving visibility, decision support, and runtime understanding of trust conditions across distributed communication infrastructures. Future uptake is likely to depend on integration with monitoring and analytics platforms, as well as on the availability and quality of operational data required to support meaningful trust evaluation processes.

7.2.8 SUITE5

SUITE5 contributes to CASTOR through activities related to secure data management and trusted data exchange, associated with the Secure Oracle Layer and the project's secure blockchain-supported trust evidence handling functions. From an exploitation perspective, these results may support future data-sharing platforms and distributed services requiring secure, auditable, and verifiable handling of trust-related information. Potential application contexts include infrastructures involving multiple stakeholders that exchange operational or trust-related information across interconnected systems. The expected value lies in providing secure data anchoring, auditable evidence handling, and stronger support for verifiable trust management across organisational boundaries. The exploitation of these results is likely to depend on integration with enterprise platforms and distributed service infrastructures, as well as on the adoption of technologies supporting secure and verifiable data exchange in multi-stakeholder service ecosystems.

7.2.9 Commsignia Ltd.

Commsignia (CMS), being a key supplier of automotive V2X solutions for OEM trials and road and smart city deployment projects worldwide will embed newly developed CASTOR results into its platform solutions offered to the market. These will be emphasized as key, enabling features for road infrastructure operators. CMS focuses on stakeholders in the automotive and industrial sectors, emphasizing the importance of the global application and adoption of safety and trust considerations in cooperative intelligent transportation systems, using V2X/V2N technology, to promote the safety of automated transportation systems.

CMS contributes to CASTOR through activities related to secure communication mechanisms for connected vehicle environments, particularly with respect to trusted OTA firmware update processes and secure messaging functions in V2X communication systems. CMS's experiences with CASTOR will help to explore methods how the usage of standard C-ITS communication technologies can be augmented with additional trust increasing methods without adversely affecting the operation, security and performance of existing systems and technologies.

From an exploitation perspective, CMS is expected to use the project results as a basis for future connected vehicle platforms and V2X communication infrastructures, especially in contexts where secure communication is required to support operational services, software lifecycle management, and system maintenance. CMS developed specific communication scenarios to demonstrate CASTOR's concept of operations, including system requirements (technology and architecture) for the effective safety enhancement of vehicle traffic. The scenarios provide basis to further development of the safety applications which can be integrated in the C-ITS ecosystem and more specifically in the general V2N service architecture CMS has to offer the market.

CMS will implement selected elements of the various enhancement technologies validated by CASTOR that will be part of the company's standard product offerings. Demonstrative examples and tools will be provided to help third parties and other users to understand and utilize the subjected new features. The value of the result lies in strengthening the integrity and authenticity of communication exchanges and update processes in connected mobility ecosystems.

Future exploitation will depend on alignment with automotive related communication standards, integration with existing V2X/V2N infrastructures, and collaboration with stakeholders operating in the automotive field and in the C-ITS ecosystem.

7.2.10 University of Surrey

The University of Surrey contributes to CASTOR through the development and use of cryptographic mechanisms that support trusted routing path proofs, including path-oriented composite attestation and privacy-preserving trust-level comparison. From an exploitation perspective, these results may support future trusted routing environments in which the integrity, order, and authenticity of trusted network device interfaces along a path must be proved without disclosing unnecessary sensitive information. Potential application contexts include cross-domain routing environments in which path validation, privacy preservation, and trust-level comparison must coexist. The expected value lies in enabling stronger cryptographic assurance for trusted path establishment and verification, particularly in settings where the number and order of trusted elements along a route are operationally relevant. Future exploitation is likely to depend on the availability of suitable cryptographic building blocks, the concrete functional requirements of the target application environment, and the performance trade-offs inherent in the selected privacy- and proof-oriented cryptographic mechanisms.

7.2.11 UBITECH

UBITECH contributes to CASTOR across multiple cross-cutting technical and integration activities, with a particularly visible role in the consolidation of trust-related capabilities spanning the Trust Assessment Framework (TAF), the Secure Oracle Layer, and the Trust Network Device Extensions (TNDE). From an exploitation perspective, UBITECH is expected to position the relevant CASTOR results as reusable trust-enabling building blocks that can support future research, innovation, and solution development activities in trusted communication infrastructures, orchestration environments, and secure digital services. The main exploitation value lies in the ability to combine trust assessment, secure evidence handling, and orchestration-oriented support functions into interoperable assets applicable to multiple sectors. Future exploitation is likely to depend on the integration of these results within broader digital infrastructure portfolios, alignment with open-source and standardisation pathways where appropriate, and collaboration with industrial and infrastructure stakeholders requiring trusted networking and secure service management capabilities.

7.2.12 ORO

ORO is expected to contribute to the exploitation of CASTOR primarily through the validation, integration, or application of trusted communication and orchestration concepts in domain-relevant operational environments. From an exploitation perspective, the partner may use CASTOR results to support future service or platform environments where trust-aware connectivity, secure communication paths, or evidence-based network management can provide additional value. The expected exploitation pathway is therefore likely to focus on the integration and adoption of selected CASTOR capabilities rather than on the stand-alone commercialisation of a separate technology component. Future uptake is expected to depend on how well the relevant CASTOR functions can interoperate with incumbent infrastructures, operational workflows, and service requirements in the partner's target environment.

7.2.13 TUIASI

TUIASI is expected to exploit CASTOR primarily through research, education, and further technical development activities related to trusted communication infrastructures, orchestration, and cybersecurity-oriented networking. From an exploitation perspective, the project results may support follow-up research, academic dissemination, advanced experimentation, and contribution to future research and innovation initiatives involving trusted routing, secure orchestration, and trust-aware networking. The value of CASTOR for TUIASI lies in the possibility of reusing project results as a basis for continued scientific development, prototype extension, and knowledge transfer. Future exploitation is therefore likely to be strongest in research-driven and educational contexts, while also supporting participation in future collaborative projects where CASTOR-derived capabilities can be refined further.

7.2.14 ICCS

ICCS is expected to exploit CASTOR through the integration and further development of project results relevant to advanced communication infrastructures, service management, and secure distributed computing environments. From an exploitation perspective, the project may provide ICCS with reusable technical knowledge and modular enablers that can support future work in orchestration, network intelligence, and trust-aware service delivery. The main exploitation value lies in the potential to embed CASTOR-derived capabilities into broader research, innovation, or platform-oriented activities addressing network automation, secure service coordination, and multi-domain communication infrastructures. Future uptake

will likely depend on the compatibility of the relevant results with existing platforms, research priorities, and collaborative ecosystem opportunities.

7.2.15 FERON

FERON is expected to exploit CASTOR primarily through the adoption and integration of selected project outcomes within application-driven or infrastructure-oriented environments where trusted communications and secure service coordination are relevant. From an exploitation perspective, the project results may support future operational or pre-operational environments in which assurance, trusted connectivity, and more transparent communication management provide measurable value. The exploitation route is therefore likely to focus on uptake and integration of selected CASTOR capabilities rather than on the independent commercialization of a stand-alone KER. Future exploitation is expected to depend on demonstrable interoperability, operational relevance, and alignment with the requirements of the specific domain environments in which FERON operates.

7.2.16 UvA

UvA is expected to exploit CASTOR mainly through research, advanced experimentation, and continued scientific development in fields related to trustworthy networking, distributed infrastructures, and security-aware communication management. From an exploitation perspective, CASTOR offers a basis for follow-up academic work, contribution to scientific knowledge, and further refinement of methods related to trust-aware communications and secure orchestration. The main value for UvA lies in the possibility of using the project results as a platform for future research proposals, scientific dissemination, and collaborative innovation activities. Future exploitation is therefore likely to take the form of continued research use, conceptual refinement, and integration of CASTOR-derived insights into subsequent research and education activities.

7.2.17 D4P

D4P is expected to exploit CASTOR primarily through the integration, dissemination, and application of project results in environments where trusted communications, digital innovation, and operational uptake of emerging networking capabilities are relevant. From an exploitation perspective, the project may provide D4P with access to a portfolio of reusable concepts and enablers that can support future solution development, service integration, or ecosystem-facing innovation activities. The exploitation value lies in the ability to draw on CASTOR as a source of modular capabilities rather than as a single monolithic technology. Future uptake is expected to depend on the maturity, interoperability, and practical applicability of the selected CASTOR results in the partner's target environments and service contexts.

The partner-level exploitation perspectives presented above illustrate the heterogeneous but complementary ways in which CASTOR results may evolve beyond the project. For some partners, the most relevant route concerns further research, standardisation, and advanced prototype development. For others, the emphasis lies on system integration, service enablement, operational uptake, or the reuse of CASTOR functions as modular technical enablers. This diversity is consistent with the consolidated KER structure and with the business and OSD interpretations developed in the preceding chapters. Taken together, these perspectives indicate that the post-project impact of CASTOR is likely to emerge not through a single uniform exploitation pathway, but through the gradual uptake of its trust-aware communication, orchestration, and assurance mechanisms across a range of technical, operational, and sector-specific contexts.

Chapter 8

CASTOR IPR Management

This chapter defines the Intellectual Property Rights (IPR) management approach of the CASTOR project. Its objective is to provide a structured framework for identifying, handling, protecting, and exploiting the intellectual assets generated, consolidated, or further developed within the project, while ensuring consistency with the consolidated Key Exploitable Results (KERs), the Open-Source Development Plan (OSD), and the partner-level exploitation perspectives presented in the previous chapters. In the context of CASTOR, IPR management is not treated as a purely legal or administrative task. Rather, it is considered a strategic project function that supports exploitation, safeguards partner interests, enables collaboration, and ensures that different forms of dissemination and uptake, including open-source release, standardisation contribution, licensing, internal uptake, and commercial deployment, can be pursued in a coherent and controlled manner.

The need for an explicit IPR management approach is already embedded in CASTOR's exploitation planning. D7.1 states that D7.2 is expected to define the project's exploitation and IPR pathways, while also highlighting that a substantial part of the CASTOR artefact portfolio is expected to be shared through openness-oriented routes where appropriate. At the same time, the planning logic of the project makes clear that CASTOR's results may be relevant to a broad stakeholder base, including routing and orchestration technology providers, hardware-based security providers, network operators, application providers, and other actors that may integrate selected CASTOR capabilities into their own environments. This combination of broad exploitation potential and differentiated openness routes makes a structured IPR chapter particularly necessary.

Methodologically, the present chapter is informed not only by the consolidated KER structure and the OSD classification, but also by the dedicated IPR-related responses collected through the Market Analysis Questionnaire (MAQ). These responses provide partner-level indications regarding ownership status, dependence on background IPR, generation of new foreground IPR, intended protection measures, and perceived IPR-related risks or constraints. The resulting chapter therefore combines a governance-oriented IPR framework with an evidence-based baseline derived from the current exploitation expectations of the consortium.

It should be noted that the current IPR baseline is heterogeneous across the consortium. For some results, ownership orientation, background dependence, and protection logic are already relatively clear, whereas for others the appropriate IPR route remains to be defined and may depend on further technical maturation, contribution clarification, or alignment with the final exploitation pathway. Accordingly, the present chapter should be understood as a structured project-level IPR management framework based on the current state of partner declarations, rather than as a final legal allocation instrument.

8.1 IPR baseline derived from the MAQ responses

The MAQ responses confirm that IPR in CASTOR must be managed across a heterogeneous portfolio of technical artefacts, ranging from software-intensive frameworks and orchestration functions to trusted device-side mechanisms, secure oracle components, cryptographic methods, and domain-specific use-case integrations. At the same time, the project has already consolidated its exploitation logic around the five final KER families presented in the previous chapters. For this reason, the project-level IPR baseline is more appropriately analysed at the level of the consolidated KERs rather than at the level of the original MAQ entries. Table 8.1 therefore provides an indicative KER-aligned IPR baseline derived from the partner MAQ responses and the consolidated KER structure. Where a KER involves more than one lead partner, the ownership shares shown are indicative working assumptions intended to support internal IPR management discussions and do not constitute a final legal allocation of rights.

Table 8.1: Indicative KER-aligned IPR baseline derived from partner MAQ responses.

Consolidated KER	Lead / owning partner(s)	Indicative ownership share	Background IPR	New IPR	IPR status	Indicative IPR form / protection logic
Trust Assessment Framework (TAF)	UKENT / UBITECH	UKENT 50% / UBITECH 50%	Yes	Yes	To be defined	Methodology / framework; software-related foreground; likely combination of copyright, know-how, and controlled/open release decisions depending on final exploitation route
Trust Network Device Extensions (TNDE)	NVIDIA / UBITECH / SURREY	NVIDIA 34% / UBITECH 33% / SURREY 33%	Mixed	Yes	Following consortium agreement / to be refined	Methodology / framework; trusted device-side software and attestation-related know-how; likely combination of software copyright, contributor traceability, and selective modular release
Optimization Engine	QUBITECH	QUBITECH 100%	Not explicitly declared	Not explicitly declared	To be defined	Software-intensive optimisation logic; protection route to be refined in line with commercial/licensing-oriented exploitation pathway
Secure Oracle Layer	SUITE5 / UBITECH	SUITE5 50% / UBITECH 50%	No significant dependency declared at KER core level	Yes	Single partner / co-development logic to be clarified at consolidated KER level	Software copyright; secure data handling and implementation know-how; likely controlled access and service-oriented exploitation, with selective disclosure where appropriate
PCE-extension with trusted network orchestration	UMU / WINGS	UMU 50% / WINGS 50%	Yes	Yes	Single partner / access right / to be defined depending on component	Methodology / framework plus software copyright; orchestration logic and integration know-how; likely hybrid treatment with open interfaces and controlled implementation-specific assets

Several project-level observations can be derived from Table 8.1. First, background IPR is clearly relevant for a number of CASTOR KERs, especially for orchestration-related mechanisms, trust assessment functions, and some domain-specific integrations contributing to the consolidated KER structure. Second, newly generated IPR is explicitly associated with several software- and framework-oriented KERs, including the TAF, TNDE, Secure Oracle Layer, and orchestration-related artefacts. Third, the dominant forms of declared IPR are software copyright and methodology/framework know-how, whereas explicit patent-oriented routes appear only selectively. Fourth, the current status remains uneven across the KER portfolio: some KERs already suggest a relatively clear protection logic, while others still require further clarification in relation to ownership allocation, background dependencies, and final exploitation route.

8.2 Objectives and guiding principles of CASTOR IPR management

The overall objective of CASTOR IPR management is to ensure that project results can be exploited effectively while preserving legal clarity, partner interests, and compatibility with the project's dissemination, standardisation, and open-source ambitions. More specifically, the CASTOR IPR management framework aims to: (i) identify the intellectual assets associated with the project's consolidated KERs and supporting artefacts, (ii) clarify ownership and contribution patterns, (iii) distinguish between background and foreground knowledge, (iv) support appropriate protection and disclosure decisions, (v) manage risks related to joint ownership, access rights, or incompatible licensing dependencies, and (vi) enable exploitation pathways that remain consistent with the strategic choices documented in Chapters 6 and 7.

The management of IPR in CASTOR follows five guiding principles. First, *traceability*: each exploitable artefact or component should be associated, to the extent possible, with a clear record of contributors, ownership status, dependencies, and intended exploitation route. Second, *proportionality*: protection and disclosure decisions should be appropriate to the nature, maturity, and expected exploitation route of the result, rather than being driven by a one-size-fits-all logic. Third, *compatibility*: IPR management must remain compatible with CASTOR's mixed exploitation model, which includes confirmed open-source, hybrid, and non-open-source KERs. Fourth, *exploitation-orientation*: legal and organisational measures should support, rather than obstruct, the post-project uptake of the results. Fifth, *consortium coordination*: IPR-related decisions must be transparent and coordinated among the relevant partners, particularly in cases involving joint contribution, shared background, or interoperability dependencies.

8.3 Scope of intellectual assets in CASTOR

The intellectual assets relevant to CASTOR are broader than the final KER list alone. They include not only the consolidated KER families identified in Chapters 6 and 7, but also the supporting technical artefacts, enabling software components, architectural specifications, methods, policy models, protocol extensions, integration logic, experimental implementations, and documentation assets that contribute to the realization or exploitation of those KERs. Consequently, IPR management in CASTOR must be understood at two levels: the level of *consolidated exploitable results* and the level of *supporting intellectual components*.

At the first level, the primary objects of IPR relevance are the consolidated KERs retained by the project, namely: the Trust Assessment Framework (TAF), the Trust Network Device Extensions (TNDE), the Optimization Engine, the Secure Oracle Layer, and the PCE-extension with trusted network orchestration. These KERs form the backbone of the project's exploitation logic and therefore represent the main units around which ownership, openness, protection, and post-project use must be clarified. At the second level, each of these KERs may rely on a set of supporting components, such as attestation mechanisms, cryptographic constructions, protocol interfaces, policy logic, monitoring and evidence-handling functions, orchestration hooks, implementation scripts, testing artefacts, or domain-integration adaptations. From an IPR perspective, these lower-level components are important because they may carry different ownership status, dependence on background know-how, or different suitability for open release.

Accordingly, CASTOR IPR management should avoid conflating the KER label with a single uniform legal object. A given KER may contain components that are better suited for open release, components that depend on pre-existing partner know-how, and components whose protection or disclosure must be decided only after considering technical maturity, exploitation route, and external dependencies. This layered understanding of intellectual assets is especially important in a project such as CASTOR, where several consolidated KERs are composites built from multiple underlying technical artefacts and where the OSD classification already distinguishes between confirmed OSS, hybrid, and non-OSS results.

8.4 Ownership, access rights, and contribution patterns

A central task of IPR management is to clarify ownership of results and the associated contribution patterns. The MAQ responses show that ownership patterns in CASTOR are not uniform. Some results are already described as belonging to a single partner or as being managed under a single-partner plus access-right logic, while others remain explicitly marked as “to be defined”. In one case, the result is declared as being handled according to the consortium agreement rather than through an immediately specified single-owner model. This confirms that CASTOR requires a flexible but structured ownership management approach.

In CASTOR, ownership may arise in several forms. Some results may be predominantly developed by a single technical partner and therefore more naturally fall under single-partner foreground ownership. Other results may involve technically meaningful contributions from multiple partners, in which case joint ownership or a more granular component-level ownership model may be more appropriate. A third class of cases concerns use-case integrations or partner-specific adoptions of CASTOR functions, where the operational use of a result may rely on access rights or on integration with pre-existing systems rather than on foreground ownership of the underlying technical artefact itself. These distinctions are important because the appropriate exploitation pathway and protection model may differ significantly between a single-owner software component, a jointly developed framework, and a use-case deployment that mainly consumes project access rights.

From a management perspective, the preferred approach in CASTOR should be to resolve ownership at the most operationally meaningful level. Where a consolidated KER is composed of several distinguishable technical modules, ownership clarification should be carried out not only at KER level but, where necessary, also at the level of constituent components. This is particularly relevant for KERs such as TNDE and the orchestration-related KER family, where multiple technical functions and partner contributions may coexist. In such cases, precise ownership tracking helps avoid ambiguity during open-source release, licensing decisions, standardisation contributions, or post-project partner-specific exploitation.

Access rights should be managed consistently with the consortium framework and the grant agreement obligations. In practical terms, this means that partners should retain the ability to use the results necessary for project implementation and legitimate post-project exploitation, while ensuring that access to background assets and jointly relevant know-how is handled in a controlled and documented manner. The purpose of IPR management here is not to over-formalise technical collaboration, but to prevent uncertainty from becoming a barrier to exploitation once project results mature beyond the research phase.

8.5 Background IPR and newly generated foreground

The distinction between background IPR and project-generated foreground is fundamental in CASTOR. The MAQ responses show that several partners explicitly rely on pre-existing background IPR, whereas others report no such dependency or do not provide a declaration. This confirms that background knowledge, software, hardware-specific capabilities, and partner-specific prior know-how are important elements in the CASTOR innovation base. At the same time, multiple partners explicitly report new IPR generated through the project, particularly in the form of software-intensive methods, frameworks, orchestration logic, trust assessment mechanisms, trusted network device-side functions, and secure data handling components.

Background IPR in CASTOR may include pre-existing orchestration functions, trust evaluation concepts, platform components, V2X communication mechanisms, aerospace-related architectural concepts, device-side trusted computing functions, proprietary hardware dependencies, and partner-specific methodological know-how. Such background can be essential to implementing the project’s technical artefacts, but it can also constrain their post-project dissemination or reuse if licensing, ownership, or dependency con-

ditions are not properly understood. For this reason, each consolidated KER should be reviewed with respect to the background elements on which it depends, especially where those dependencies affect redistribution rights, sublicensing, open-source compatibility, or portability across partner environments.

Foreground IPR, by contrast, comprises the knowledge and assets generated through the project activities themselves. In CASTOR, foreground includes software implementations, orchestration logic, trust assessment mechanisms, trusted network device-side functions, secure oracle components, cryptographic methods, and integrated framework-level combinations of such elements. The appropriate form of protection for foreground depends on the exploitation route. For some results, especially those aligned with confirmed open-source release, software copyright and attribution clarity may be sufficient, with openness and ecosystem uptake providing the main exploitation value. For others, especially hybrid or non-open-source artefacts, foreground may need to be retained as proprietary know-how, protected through confidentiality, controlled access, or selective disclosure. In still other cases, the most valuable output may be methodological or framework-level knowledge better protected through authorship, documentation control, and consortium-level exploitation agreements rather than through formal registration alone.

8.6 IPR management in relation to open-source, hybrid, and non-open-source KERs

One of the defining features of CASTOR is that its exploitation logic is not uniform. As established in Chapter 7, the project distinguishes between confirmed open-source, hybrid, and non-open-source KERs. This means that IPR management must support differentiated treatment rather than a single protection strategy for all results.

For KERs classified as confirmed OSS, the core IPR task is not to prevent disclosure, but to ensure that disclosure is legally clean, strategically aligned, and technically sustainable. This requires verifying contribution provenance, background dependency compatibility, authorship clarity, and the suitability of the chosen licence for the intended ecosystem and adoption goals. In this category, IPR management functions primarily as an enabler of safe openness. It ensures that the open-source route does not create downstream uncertainty regarding ownership, derivative rights, or integration conditions.

For KERs classified as hybrid, the IPR challenge is more delicate. Hybrid KERs typically contain a combination of elements: some potentially suitable for open release, such as interfaces, protocol extensions, reference implementations, or interoperability layers, and others more appropriately retained under controlled access due to service-specific integration logic, deployment know-how, or commercial sensitivity. In such cases, IPR management must define the boundary between the open and the closed parts of the artefact, specify how those parts interact, and ensure that the selected release model does not accidentally disclose proprietary value or create licensing contradictions.

For KERs classified as non-open-source, the main role of IPR management is to preserve exploitation flexibility while preventing premature or uncontrolled disclosure. This does not necessarily imply aggressive formal protection in all cases. Rather, it implies clarity regarding ownership, restricted disclosure where needed, careful handling of technical documentation, and an exploitation-oriented choice between proprietary software, controlled service delivery, licensing, or know-how-based protection. In all three categories, the key principle is alignment between legal treatment and exploitation intention.

The MAQ responses also confirm that open-source and IPR protection are not treated in CASTOR as mutually exclusive concepts. On the contrary, some partner responses indicate that permissive open-source release, software copyright, contributor agreements, and protection of implementation-specific know-how may coexist within the same exploitation logic. This is particularly relevant for hybrid or modular KERs, where openly released interfaces, reference implementations, or framework-level artefacts may

coexist with controlled deployment knowledge, proprietary optimizations, or service-specific integration assets.

8.7 Protection strategy and decision criteria

The protection strategy in CASTOR should be guided by the nature of the result, the maturity of the technology, the intended exploitation pathway, and the dependencies associated with the relevant technical artefact. Protection should not be understood narrowly as formal registration alone. In many research and innovation projects, and especially in software- and framework-intensive projects such as CASTOR, protection may take the form of copyright management, contributor traceability, confidentiality management, controlled disclosure, trade secret treatment of implementation know-how, careful repository governance, or selective public release timed in accordance with exploitation goals.

The first decision criterion should be *exploitation route*. If a result is intended for open-source release, then the relevant protection question is whether the project can release it under a legally appropriate licence without conflict with ownership or background dependencies. If a result is intended for licensing or controlled service provision, then the relevant protection question is how to preserve exclusivity or differentiation. The second criterion should be *technical modularity*. If a result can be decomposed into modules with different exploitation value, then protection measures should be designed at module level rather than forcing a single treatment on the whole artefact. The third criterion should be *partner dependency structure*. If multiple partners contributed substantially, or if a result depends critically on partner-specific background, then the protection decision must be taken in a coordinated way and documented with sufficient clarity to support post-project use.

In practical terms, CASTOR should treat the following protection measures as the main available options: clear copyright notice and contributor tracking for software and documentation; confidentiality and restricted-access measures for sensitive implementation details; consortium-level documentation of ownership and background dependencies; patentability assessment only where a clearly differentiating and protectable technical solution justifies that effort; and licence selection procedures for all artefacts considered for open release. The choice among these should be proportional to the likely exploitation value and to the legal complexity of the result in question.

The MAQ responses already suggest a range of such measures. Some partners refer to copyright-based protection, others to controlled source-code access and contributor agreements, while others mention possible patent-oriented routes, trade secrets, or open-source release under permissive licences. This confirms that CASTOR should not enforce a single protection form, but rather apply a result-dependent decision logic consistent with the technical and exploitation characteristics of each artefact.

8.8 IPR-related risks and mitigation measures

The MAQ responses indicate five recurring IPR-related risk categories across the consortium. The first concerns *uncertainty regarding final ownership or protection route*, especially for results still marked as “to be defined”. The second concerns *dependence on third-party, proprietary, or open-source components* whose licensing terms may constrain redistribution or commercialization. The third concerns *complexity arising from joint contribution patterns and contributor-right management*, especially in software- and orchestration-oriented artefacts. The fourth concerns *domain-specific regulatory or contractual constraints*, particularly in aerospace-related environments. The fifth concerns *platform or hardware dependency risks*, especially where implementation relies on specific trusted execution or hardware-rooted technologies.

These recurring risks can be expressed more concretely as follows. A first category concerns *ownership ambiguity*, especially in results that are technically composite or jointly developed. If contribution boundaries are not documented with sufficient precision, post-project exploitation may be delayed by uncertainty over ownership or rights to disclose. A second category concerns *background dependency risk*. A result may appear suitable for open release or broad licensing, yet depend on pre-existing proprietary components, internal know-how, or third-party technology that restricts such release. A third category concerns *licensing incompatibility*, especially for artefacts intended for open-source release but interacting with proprietary modules or externally sourced components under incompatible terms. A fourth category concerns *premature disclosure*, where dissemination, publication, or repository exposure occurs before the consortium has agreed on the appropriate protection or release route. A fifth category concerns *fragmented exploitation*, where different partners pursue legitimate but insufficiently coordinated post-project uses that generate conflict or uncertainty over shared assets.

The corresponding mitigation strategy should be embedded into project governance. First, each consolidated KER should be accompanied by a lightweight IPR status record covering ownership, main dependencies, intended exploitation route, and disclosure constraints. Second, any artefact proposed for open release should undergo a basic pre-release clearance process checking ownership, dependency compatibility, and licence suitability. Third, results with significant joint contribution should be reviewed early to determine whether joint ownership needs formal clarification or whether a component-level separation is more practical. Fourth, publication and dissemination processes should include a simple internal check to ensure that materials do not unintentionally disclose protected or not-yet-cleared foreground. Finally, the consortium should maintain a coordinated view of partner intentions for post-project use of shared results, especially where hybrid or modular exploitation strategies are envisaged.

8.9 Operational IPR management process within the consortium

To be effective, CASTOR IPR management should operate as a process rather than as a static description. The process should begin with *identification*, namely the recognition of potentially exploitable results and their supporting assets. This is already supported by the MAQ and by the consolidated KER evaluation in Chapter 5. The second step is *classification*, where each result is associated with an intended exploitation route and corresponding openness category, as already reflected in the OSD logic of Chapter 6. The third step is *IPR clarification*, where ownership, background dependencies, and protection needs are recorded. The fourth step is *decision*, where the consortium or the relevant contributing partners agree on whether the result should be released, protected, licensed, further matured, or kept under controlled access. The fifth step is *monitoring*, in which changes in maturity, partner strategy, or dependency structure are reflected in updated IPR and exploitation decisions.

Responsibility for this process should be distributed but coordinated. Technical partners remain the primary source of information on technical contribution, dependencies, and implementation specifics. Use-case and integration partners provide essential input on operational use, access-right conditions, and integration-related background. The exploitation and management functions of the consortium should then consolidate this information into a project-level view, ensuring coherence across KERs and consistency between dissemination, OSD, and exploitation planning. This process-oriented view is especially important in CASTOR because the project does not converge toward a single commercial output, but toward a portfolio of modular technical enablers and framework-level results with differentiated post-project futures.

In practical terms, the consortium-level IPR process should include the following minimum actions:

- maintenance of an internal IPR tracking register for the consolidated KERs and their main supporting components;

- partner-level update of ownership, background, and foreground information whenever a KER or sub-component changes materially in maturity or scope;
- lightweight review of any artefact proposed for open-source release, external dissemination, or standardisation contribution;
- documentation of contributor roles and dependency structure for software-intensive artefacts;
- coordination between technical and exploitation leads before finalising the post-project release or protection route of a result.

These actions do not replace the formal provisions of the consortium and grant agreement framework. Rather, they operationalise those provisions in a way that is better aligned with the actual technical structure and mixed exploitation logic of CASTOR.

8.10 Concluding remarks

In summary, IPR management in CASTOR is a strategic enabler of exploitation rather than an isolated legal exercise. The project already recognises this through the expectation that D7.2 should define exploitation and IPR pathways, and through the dedicated IPR block included in the MAQ. The role of the present chapter is therefore to provide the project-level framework within which ownership, background dependencies, foreground generation, protection measures, and disclosure decisions can be handled consistently across the CASTOR result portfolio.

The MAQ responses show that CASTOR requires a differentiated IPR management model. Some results derive their value primarily from open release and ecosystem uptake; others are better aligned with hybrid treatment; and others appear more suitable for service-based, proprietary, or controlled exploitation routes. The effectiveness of this model depends on traceability of contributions, early clarification of ownership and dependencies, pre-release legal and technical checks for open-source candidates, and a coordinated consortium-level view of post-project exploitation intentions. By embedding these principles into the management of the consolidated KERs and their supporting components, CASTOR can pursue openness, interoperability, standardisation, and commercial or research exploitation in a balanced and strategically consistent manner.

Chapter 9

CASTOR External Advisory Board

The CASTOR External Advisory Board (EAB) has been established to provide high-level scientific and technical guidance to the project, ensuring that CASTOR's research and innovation activities remain well aligned with ongoing developments in trustworthy networking, trusted computing, runtime attestation, secure orchestration, and next-generation communication infrastructures. The Board brings together complementary expertise from academia, industry, and the Internet standardization community, covering the main areas that are central to CASTOR's scope, namely trusted path routing, path-aware networking, runtime trust assessment, and secure management of networked infrastructures. In this respect, the EAB is intended not only to review and challenge CASTOR's technical assumptions, but also to help position the project's results within the broader landscape of emerging standards, research directions, and industrial needs.

The current CASTOR EAB includes **Prof. David Basin (ETH Zurich)**, **Dr. Henk Birkholz (Fraunhofer SIT)**, **Prof. Frank Kargl (Ulm University)**, and **Dr. Diego Lopez (Telefónica)**. Prof. David Basin is Full Professor in the Department of Computer Science at ETH Zurich and heads the Information Security Group. His perspective is particularly relevant to CASTOR in view of ETH's longstanding work on secure and path-aware networking architectures, including SCION, and the broader relation between routing control, trust, and secure network operation. Henk Birkholz is one of the leading contributors in the IETF trust and attestation landscape. He is an author of the *Remote ATtestation procedureS (RATS) Architecture* and a co-author both of the current *Trusted Path Routing* draft and of the *runtime TPR* draft, the latter being especially relevant to CASTOR as it addresses the extension of trusted path routing towards runtime trust assessment and monitoring. Prof. Frank Kargl leads the Institute of Distributed Systems at Ulm University and contributes expertise in distributed systems security, vehicular communications, and trust assessment methodologies, which are directly relevant to CASTOR's Trust Assessment Framework. Diego Lopez, currently in charge of Technology Exploration activities within Telefónica's GCTIO unit, brings a strong operator-oriented perspective on network architectures, security, and service infrastructures, while also being a co-author of the current IETF *Trusted Path Routing* draft. Together, these experts provide CASTOR with a highly relevant advisory span across SCION-inspired path awareness, IETF trusted path routing and attestation, trust assessment methodologies, and operator-oriented networking practice.

The interaction with the EAB has already started and has proven valuable during the first reporting period. CASTOR has already organized an online discussion workshop with the Board members, through which targeted comments were collected on the project architecture and on the evolution of the runtime trust assessment approach. In particular, the feedback received reinforced the importance of treating trusted path routing as a dynamic process rather than a static one, thus further validating CASTOR's emphasis on runtime evidence collection, continuous trust re-evaluation, and adaptive trusted path establishment. These exchanges have already informed architectural refinements in CASTOR and have contributed to the consolidation of the project's approach towards extending existing trusted path routing models beyond largely static trust assumptions.

Two additional meetings with the CASTOR EAB are planned during the remainder of the project. The first one will take place around **M21**, in conjunction with the planned CASTOR research workshop conceived as a scientific debate on trustworthy networking. This meeting will be used to present the first integrated CASTOR framework, discuss the project's architectural progress and emerging results, and gather external feedback on the research and standardization directions pursued by the consortium. A second advisory interaction will follow at a later stage of the project, focusing on the maturity of the final technical artefacts, their positioning with respect to standardization and exploitation, and the broader impact of CASTOR's results on the evolution of trustworthy networking across the compute continuum.

Chapter 10

Conclusion

Deliverable D7.2 has documented the work that has been conducted within WP7 ”Dissemination, Standardization, Exploitation & Impact Creation” during the first reporting period (M1-M18) of the CASTOR project, offering a detailed description of the dissemination, communication, clustering and standardization activities of the project. It has also presented the plan for the second reporting period where the advancements in the CASTOR Framework will be showcased in the various interested audiences. Furthermore, deliverable D7.2 has described the Open Source Development Plan of the project regarding the different components that are developed in CASTOR. An extensive Market Analysis has been also conducted based on the different application domains of CASTOR, along with the definition of the CASTOR functional and business model, and a preliminary evaluation of its key exploitable results. The CASTOR value proposition for each different use case has been specified, while for each partner the individual exploitation plan has been identified. Moreover, an initial IPR management analysis regarding the key exploitable results of CASTOR project has been performed.

Deliverable D7.2 has received input from deliverable D7.1, which had been the basis for the planning of the communication, dissemination, standardization and exploitation activities at the early period of the project. Deliverable D7.3, an updated version of D7.2, will be delivered at the end of the project in M36, where all WP7 activities during the second reporting period (M19-M36) will be reported, including also a techno-economic impact analysis of CASTOR advancements for the modern compute continuum.

Appendix A

Market Analysis Questionnaire (MAQ) for CASTOR project

This appendix reproduces the *Market Analysis Questionnaire for CASTOR Project* as provided to project partners. The questionnaire aims to collect vital information on key exploitable results of CASTOR for the purpose of market analysis as well as exploitation and OSD planning within the project

Introductory text

This questionnaire aims to gather key information on exploitable results for the purpose of market analysis and exploitation planning within the CASTOR project. It is addressed to all project beneficiaries, including both technical partners leading or contributing to specific Exploitable Results (ERs) and use case partners validating and leveraging the CASTOR framework within concrete application domains.

For technical partners, the questionnaire focuses on individual exploitable artefacts or components. For use case partners, it provides the opportunity to contribute domain-specific, operational, and adoption-oriented insights based on the integration, demonstration, and evaluation activities carried out in WP6. Answers may therefore reflect technical differentiation, functional value, or market relevance, depending on the respondent's role and expertise.

"Results" are outputs generated during the project that may create impact during and/or after the funding period and are owned by the beneficiary that generates them. According to the Grant Agreement, all partners must take appropriate measures to ensure exploitation of project results.

The inputs collected will be consolidated to support CASTOR's market analysis, prioritisation of exploitable results, and definition of exploitation and IPR pathways. Partners are requested to complete one questionnaire per exploitable result they lead, contribute to, or actively use, and to provide best-effort estimates where precise data is not available.

*** Indicates required question**

Questionnaire items

1. **Exploitable Result Name (max 120 characters)** *
   Technical partners: Please focus on the specific artefact or component.
   Use case partners: Please describe the CASTOR functionality as used in your application domain.
2. **Short description (max. 200 words)** *
3. **Lead Partner – Organisation name (max 150 characters)** *

4. **Lead Partner – Role in the project (max 150 characters)** *
5. **Lead Partner – Contact person (max 150 characters)** *
6. **Lead Partner – Email address (max 150 characters)** *
7. **Supporting organisation(s) (if any) (max 150 characters)**
8. **Role of Supporting Partner(s) in the exploitable result (max 150 characters)**
9. **Contact person(s) for Supporting Organisation(s) (max 150 characters)**
10. **Primary Sector (e.g., telecommunications, aerospace etc) (max 200 characters)** *
11. **Secondary Sector(s) (e.g., cybersecurity, cloud & edge computing, public sector) (max 250 characters)** *
12. **Estimated market size** *
    Technical partners: Please provide a high-level estimate for the relevant technology market.
    Use case partners: Please focus on the market size and scope of your application domain.
    - ○ Niche (typically $<$ €100M annual market value)
    - ○ Medium (typically €100M–€1B annual market value)
    - ○ Large (typically $>$ €1B annual market value)
    - ○ Other:
13. **Is this result intended for:** *
    - ☐ National market only
    - ☐ EU market only
    - ☐ Multi-country / Regional
    - ☐ Global market
14. **Expected time to market** *
    - ○ $<$ 1 year
    - ○ 1–3 years
    - ○ $>$ 3 years
15. **Present market behaviour** *
    Technical partners: Please focus on technology-driven trends relevant to the artefact.
    Use case partners: Please focus on domain-specific trends affecting adoption in your sector (e.g. Aerospace, Automotive, UAVs).
    - ○ Growing (Demand and market activity are increasing, with expanding adoption, investment, and new entrants)
    - ○ Stable (Demand and activity are steady, with limited growth or decline and relatively constant adoption levels)
    - ○ Declining (Demand and activity are decreasing, with reduced investment, shrinking adoption, or market consolidation)
16. **Key current trends (domain- or market-segment–specific) (max 1000 characters)** *
    Please identify the most relevant current trends specific to the market segment or application domain addressed by this exploitable result. Trends may relate to, for example:

- security, trust, or safety requirements in your domain;
- technology adoption patterns (e.g. secure edge, trusted data exchange, continuum orchestration);
- operational or organisational practices;
- regulatory, certification, or compliance developments.

High-level or cross-cutting trends (e.g. Zero Trust, cloud–edge convergence, automation) may be mentioned only if they concretely affect your domain or market segment.

17. **Barriers or constraints in the relevant market (max 1000 characters)** *
18. **References (if any) (max 1500 characters)**
19. **List key competitors (name, type, description, website). Explicitly mention solutions, tools, platforms, or practices that are currently used instead of (or alongside) CASTOR in your domain (max 1000 characters)** *
    Technical partners: Please list competing technologies, platforms, or frameworks.
    Use case partners: Please list competing solutions or practices currently used in your domain.
20. **References (if any) (max 1500 characters)**
21. **Primary target customers** *
    Technical partners: Please indicate expected adopters or integrators of the technology.
    Use case partners: Please indicate end users and stakeholders involved in the use case deployments.
    - ☐ Enterprises
    - ☐ SMEs
    - ☐ Telcos / network operators
    - ☐ Cloud / edge providers
    - ☐ Automotive OEMs
    - ☐ Public sector / governments
    - ☐ Other:
22. **End users (max 300 characters)** *
23. **Adoption drivers for the exploitable result (max 800 characters). For use case partners, please answer based on your experience from CASTOR integration, simulation, or field-testing activities.** *
24. **What worked particularly well when using CASTOR in your application domain? (Primarily for Use Case partners; optional for technical partners) (max 400 characters)**
25. **References (if any) (max 1000 characters)**
26. **Main barriers to adoption.** *
    Please indicate and briefly explain the main barriers, limitations, or trade-offs relevant to the adoption of this exploitable result.
    Technical partners: Please consider technical, integration, or standardisation barriers.
    Use case partners: Please consider operational, regulatory, safety, or organisational barriers observed.
    (Select all that apply and briefly explain where relevant)

- ○ Technical maturity
- ○ Integration complexity
- ○ Performance or scalability constraints
- ○ Standards and interoperability gaps
- ○ Certification/compliance/safety/regulatory constraints
- ○ Organisational or process-related barriers
- ○ Market awareness
- ○ Cost / business model
- ○ Skills or training requirements
- ○ Other:

27. **Please briefly explain the reasoning behind selected barriers (max 700 characters)** *
28. **Observed limitations or trade-offs (max 700 characters)** *
29. **How likely is this barrier or limitation to occur in real deployments?** *
    - ☐ Low
    - ☐ Medium
    - ☐ High
30. **If this barrier occurs, what is the expected impact on adoption or deployment?** *
    - ☐ Low
    - ☐ Medium
    - ☐ High
    - ☐ N/A
31. **Mitigation strategies for identified barriers (max 1000 characters)** *
32. **Where do you see potential for CASTOR to bring additional value or enable new capabilities? (max 400 characters)** *
33. **Expected future innovations and regulatory impacts (max 1000 characters)** *
    Technical partners: Please consider anticipated technology evolution and standards.
    Use case partners: Please consider expected regulatory, operational, or ecosystem changes in your application domain.
34. **Describe the problem addressed, value proposition, and innovation (max 1200 characters)** *
    Technical partners: Please describe the technical or functional innovation compared to existing approaches.
    Use case partners: Please focus on the operational value observed in simulations, PoCs, or field trials.
35. **On a scale of 1 to 5, how unique is the value proposition of this exploitable result compared to existing solutions?** *
    You may answer from a market or technical perspective. If you are not in a market-facing role, please describe how the result is technically or functionally different from existing approaches.

Not unique at all 1 2 3 4 5

Highly unique

36. **Justification (max 500 characters)** *

37. **What are the main strengths of this exploitable result compared to current solutions or practices? (Consider technical capabilities, operational benefits, compliance support, or domain-specific advantages) (max 400 characters)** *
Technical partners: focus on technical or functional strengths.
Use case partners: focus on operational or domain-specific strengths observed in your WP activities.

38. **What opportunities does this result create in your market or application domain? (Examples: new services, improved compliance, automation, cross-domain deployment, emerging needs.) (max 400 characters)** *

39. **Planned exploitation route** *
Technical partners: Please focus on technology-oriented exploitation (products, licensing, OSS).
Use case partners: Please focus on adoption, training, research, or “as-a-service” perspectives.

- ☐ Commercial product/service
- ☐ Open-source
- ☐ Licensing
- ☐ Standardisation contribution
- ☐ Internal use
- ☐ Training & research
- ☐ “As-a-service”
- ☐ Other:

40. **Justification (max 500 characters)** *

41. **Post-project role regarding the exploitable result (max 1000 characters)** *

42. **Which of the following describes the current Technology Readiness Level (TRL) of the exploitable result?** *

- ○ TRL 1: Basic principles observed
- ○ TRL 2: Technology concept formulated
- ○ TRL 3: Experimental proof of concept
- ○ TRL 4: Technology validated in lab
- ○ TRL 5: Technology validated in relevant environment
- ○ TRL 6: Technology demonstrated in relevant environment
- ○ TRL 7: System prototype demonstration in operational environment
- ○ TRL 8: System complete and qualified
- ○ TRL 9: Actual system proven in operational environment

43. **What is your expected TRL at End of Project (If applicable)?** *
Technical partners: Please assess TRL of the specific exploitable artefact.
Use case partners: Please assess TRL of the CASTOR framework as deployed in your use case.

- ○ TRL 1
- ○ TRL 2
- ○ TRL 3
- ○ TRL 4
- ○ TRL 5
- ○ TRL 6
- ○ TRL 7
- ○ TRL 8
- ○ TRL 9
- ○ N/A

44. **What is the anticipated pricing strategy for the exploitable result?** *
    - ○ Cost-plus pricing
    - ○ Value-based pricing
    - ○ Competitive pricing
    - ○ Penetration pricing
    - ○ Skimming pricing
    - ○ Option 6
45. **Rate the importance of the following factors in achieving successful market penetration:** *

Factor	Low	Moderate	High
Funding and investment secured	○	○	○
Clear Intellectual Property (IP) protection	○	○	○
Strong partner network/ecosystem	○	○	○
Regulatory compliance achieved	○	○	○
Trained personnel/expertise available	○	○	○

46. **List relevant studies / research / papers (title + source + year + link if available) (max 2000 characters)** *
47. **Upload references for relevant material (optional)**
48. **Intellectual Property Rights (IPR)**
    Please provide information on the Intellectual Property status and protection plans related to this exploitable result. Note that this question can be answered from a legal, technical, or usage perspective. If you are unsure about formal IPR ownership or protection, please provide your best understanding based on your role and experience or indicate “not applicable”.
49. **Which partner(s) own the exploitable result or its main components?**
    Technical partners, please indicate which type of ownership of the exploitable artefact or component you lead or contribute to. Use case partners, please indicate whether the result is used under project access rights or consortium agreements, or select “not applicable”.
50. **Is ownership:** *

- ☐ Single partner
- ☐ Joint ownership
- ☐ Access right
- ☐ To be defined
- ☐ Not applicable
- ☐ Other:

51. **Give more details (max 200 characters)**

52. **Does this result rely on pre-existing (background) IPR?** *

- ☐ Yes
- ☐ No
- ☐ Not applicable

53. **Has new IPR been generated in the project through this result?** *
Technical partners: please select Yes/No based on any pre-existing software, hardware, or know-how incorporated in the result.
Use case partners: Please select Yes/No based on background systems, platforms, or datasets used in the use case integration.

- ☐ Yes
- ☐ No
- ☐ Not applicable

54. **If yes, indicate type**

- ○ Software copyright
- ○ Patentable invention
- ○ Trade secret / know-how
- ○ Database / dataset
- ○ Methodology / framework
- ○ Not applicable
- ○ Other:

55. **Protection measures planned (max 300 characters)** *

56. **IPR risk or constraints (max 300 characters)** *

57. **Additional Comments**

Appendix B

CASTOR Logos

CASTOR Visual Identity

CASTOR has established a distinctive visual identity that has been consistently applied across all communication and dissemination activities. This cohesive branding ensures a recognisable and professional presence across digital and physical channels, reinforcing the project's identity and making its materials instantly identifiable.

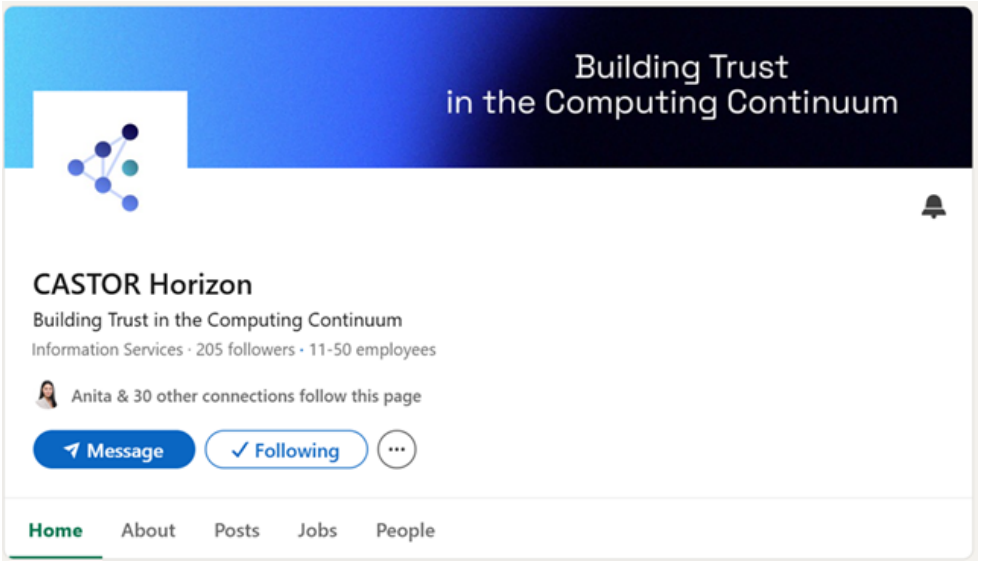

Figure B.1: CASTOR Visual Branding

Logo

Main version of the CASTOR logo with technical specifications.

Figure B.2: CASTOR Logos

B.0.0.0.1 Logo variations The main logo is also provided in the variations depicted here below, to allow readability over dark backgrounds or for black and white printing purposes.

Figure B.3: Logo variations

B.0.0.0.2 Do's and Dont's 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 dont's.

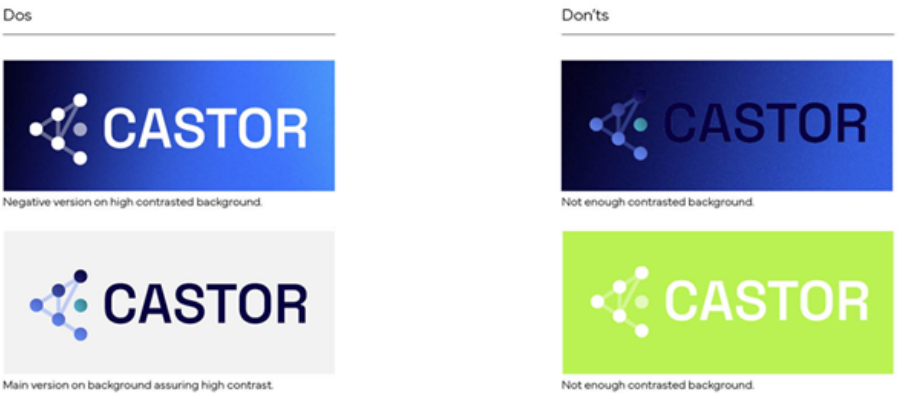

Figure B.4: Logo do's and dont's

B.0.0.0.3 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.

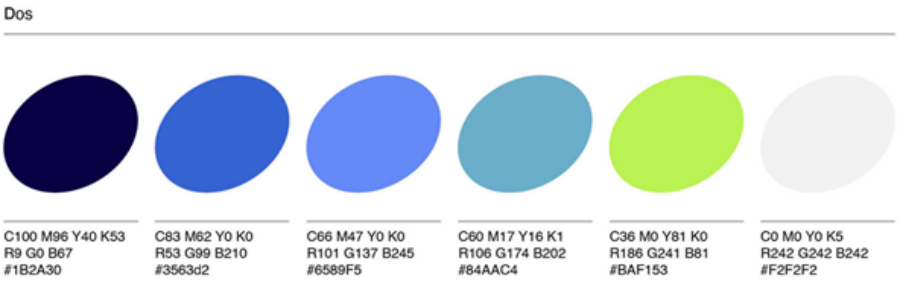

Figure B.5: Corporate colours

B.0.0.0.4 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.

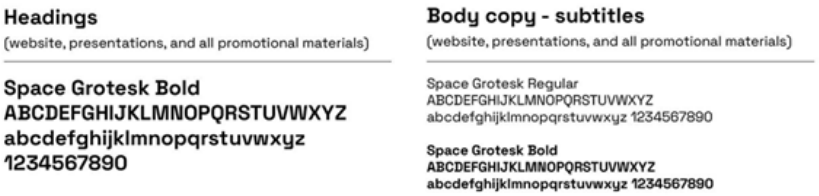

Figure B.6: Font types

Adherence to the European Commission's rules of communication of results & acknowledgement 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 B.7), 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.

Figure B.7: 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."

Bibliography

[1] David Barrera, Laurent Chuat, Adrian Perrig, Raphael M. Reischuk, and Pawel Szalachowski. The SCION internet architecture. *Communications of the ACM*, 60(6):56–65, 2017.

[2] CASTOR Consortium. D2.1 operational landscape, requirements and reference architecture – initial version. Technical report, CASTOR Project, 2025. Public deliverable.

[3] CASTOR Consortium. D3.1 conceptual architecture of castor trusted computing base and composable attestation model specification. Technical report, CASTOR Project, 2025. Public deliverable.

[4] CASTOR Consortium. D4.1 architectural specification of castor continuum-wide trust assessment framework. Technical report, CASTOR Project, 2025. Public deliverable.

[5] CASTOR Consortium. D5.1 architectural specification of dynamic enforcement of trust-/network-aware path establishments. Technical report, CASTOR Project, 2025. Public deliverable.

[6] CASTOR Consortium. Plan for dissemination and exploitation incl. communication. Deliverable D7.1, Project 101167904 within HORIZON-CL3-2021-CS-01, 2025.

[7] CEN-CENELEC Focus Group on Quantum Technologies. Standardization Roadmap on Quantum Technologies. https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Quantum%20technologies/Documentation%20and%20Materials/fgqt_q06_standardizationroadmapquantumtechnologies_release1-1.pdf, August 2024. Accessed: 2026-03-22.

[8] Corine de Kater, Nicola Rustignoli, and Samuel Hitz. SCION Control Plane. Internet-Draft draft-dekater-scion-controlplane-12, IETF, November 2025. Work in Progress.

[9] Corine de Kater, Nicola Rustignoli, Jean-Christophe Hugly, and Samuel Hitz. SCION Data Plane. Internet-Draft draft-dekater-scion-dataplane-08, IETF, November 2025. Work in Progress.

[10] European Cluster for Securing Critical Infrastructures. https://www.ecsci.eu/. Accessed: 2026-03-03.

[11] IEEE Standards Association Working Group P3155. P3155 Standard for Programmable Quantum Simulator. https://sagroups.ieee.org/3155/, 2026. Working group page, accessed: 2026-03-22.

[12] European Innovation and Research for Next Generation Networks. https://6g-ia.eu/. Accessed: 2026-02-06.

[13] International Organization for Standardization. ISO/IEC 4879:2024 Information technology — Quantum computing — Vocabulary. https://www.iso.org/standard/80432.html, 2024. Accessed: 2026-03-22.

[14] Meni Orenbach, Rami Ailabouni, Nael Masalha, Thanh Nguyen, Ahmad Saleh, Frank Block, Fritz Alder, Ofir Arkin, and Ahmad Atamli. Blueguard: accelerated host and guest introspection using dpus. In *Proceedings of the 34th USENIX Conference on Security Symposium*, SEC '25, USA, 2025. USENIX Association.

[15] CyberNEMO project. https://cybernemo.eu/. Accessed: 2026-03-27.

[16] ENTRUST project. https://www.entrust-he.eu/. Accessed: 2026-03-27.

[17] GuardAI project. https://www.kios.ucy.ac.cy/guardai/. Accessed: 2026-03-27.

[18] HEISINGBERG project. https://www.heisingberg.eu/. Accessed: 2026-03-27.

[19] INTACT project. https://intact-horizon.eu/. Accessed: 2026-03-27.

[20] MEDIATE project. https://mediate-horizon.eu/. Accessed: 2026-03-27.

[21] MIRANDA project. https://www.mirandaproject.eu/. Accessed: 2026-03-27.

[22] RESCALE project. https://rescale-project.eu/. Accessed: 2026-03-27.

[23] SCION Documentation. SCION overview. https://docs.scion.org/en/latest/overview.html, 2026. Accessed: 2026-03-12.