D8.3 Dissemination, Communication, Exploitation and Stakeholders Engagement Report Final Version

Document Identification			
Status	Final	**Due Date**	31/08/2025
Version	1.0	**Submission Date**	16/09/2025

Related WP	WP8	**Document Reference**	D8.3
Related Deliverable(s)	D8.1, D8.2	**Dissemination Level (*)**	PU
Lead Participant	LISC	**Lead Author**	Mpampis Chatzimallis
Contributors	DBC, INTRA, FN et al.	**Reviewers**	Eilin Geraghty (ECO)
			Tomás Pariente, Iván Zaldívar (ATOS)

Keywords:
Dissemination, communication, exploitation, innovation, stakeholders' engagement, strategy

This document is issued within the frame and for the purpose of the TANGO project. This project has received funding from the European Union's Horizon Europe Framework Programme under Grant Agreement No. 101070052. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.
The dissemination of this document reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains. This deliverable is subject to final acceptance by the European Commission.
This document and its content are the property of the TANGO Consortium. The content of all or parts of this document can be used and distributed provided that the TANGO project and the document are properly referenced.
Each TANGO Partner may use this document in conformity with the TANGO Consortium Grant Agreement provisions.

Document Information

List of Contributors	
Name	Partner
Ioannis Drivas	DBC
Sotirios Michagiannis	DBC
Vasiliki Andriopoulou	DBC
Konstantinos Chisiridis	INTRA
Lina Giannivasili	FN
Chariton Palaiologk	FN
Claudia Mertinger	FSDE

Document History			
Version	Date	Change editors	Changes
0.1	20/05/2025	Mpampis Chatzimallis (LISC)	ToC
0.4	06/07/2025	Giannis Koutsos (FN), Ioannis Drivas (DCB), Konstantinos Chisiridis (INTRA), Mertinger Claudia (FSDE), Renato Santana (EGI)	Contributions from FN, DBC, INTRA, FSDE, EGI
0.6	25/07/2025	Giannis Koutsos (FN), Ioannis Drivas (DCB), Konstantinos Chisiridis (INTRA), Mertinger Claudia (FSDE), Renato Santana (EGI)	Contributions from FN, DBC, INTRA, FSDE, EGI
0.7	03/09/2025	Mpampis Chatzimallis (LC)	Final Draft ready for internal review
0.8	11/09/2024	Mpampis Chatzimallis (LC)	Final version after internal review
1.0	15/09/2025	Mpampis Chatzimallis (LC), Tomás Pariente (ATOS)	Final Version ready for submission

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Mpampis Chatzimallis (LC)	15/09/2025
Quality manager	Juergen Neises (FSDE)	16/09/2025
Project Coordinator	Tomás Pariente (ATOS)	16/09/2025

Table of Contents

Document Information 2
Table of Contents 4
List of tables 9
List of figures 10
List of Acronyms 12
Executive Summary 13
1 Introduction 14
1.1 Purpose of the document 14
1.2 Relation to other project work 14
1.3 Structure of the document 14
2 Dissemination, Communication, Exploitation, and Stakeholder Engagement Strategy Updates 15
3 Reporting of Dissemination Activities & Statistics 16
3.1 TANGO's website performance & analytics 16
3.2 Social media channels performance & analytics 18
3.2.1 LinkedIn 18
3.2.2 X 19
3.2.3 Mastodon 20
3.2.4 YouTube channel 21
3.3 TANGO newsletter 22
3.4 Project articles & news 26
3.5 Promotion through partners' network 30
3.6 Scientific Publications 33
3.7 Policy briefs/White Papers 38
3.7.1 Distributed Infrastructures, Secure Data Exchange & Data Spaces 38
3.7.2 Ensuring Data Sovereignty: TANGO Platform Solution for Secure and Trusted Data Flows Across Europe 39
3.7.3 Definition of Data Intermediation Services 39
3.8 Organisation & Participation in events & workshops 40
3.9 TANGO external synergies 43
3.9.1 Events & Meetings 43
3.9.2 Collaboration with MobiSpaces on Impact Analysis 45
4 Dissemination and Communication monitoring 47
5 Innovation Management Plan & Activities M18-M36 48
5.1 Updated exploitation plan 48

5.2 General description related to Intellectual Property 49
5.3 Record of intellectual property assets 51
5.3.1 Ownership schemas and IPR matrix 51
5.3.2 Instruments for protecting exploitable results 51
5.3.3 Management of knowledge and protection of results 52
6 Business Models and exploitation paths per KER 53
6.1 Methodology 53
6.2 Exploitation paths for KER2b-Ubiquitous Personal Context Vectors (UPCVs) 54
6.2.1 Competitor analysis 54
6.2.2 Market Analysis 55
6.2.3 Value proposition analysis 57
6.2.4 Barriers, obstacles and analysis of the standards and regulation 57
6.2.5 Technology and market watch 58
6.2.6 Business Model Canvas 58
6.2.7 Exploitation Pathway 59
6.3 Exploitation paths for KER3a-Confidentiality and Privacy by Design: PEP and Sticky Policies 59
6.3.1 Competitor analysis 59
6.3.2 Market Analysis 60
6.3.3 Value proposition analysis 60
6.3.4 Barriers, obstacles and analysis of the standards and regulation 60
6.3.5 Technology and market watch 61
6.3.6 Business Model Canvas 62
6.3.7 Exploitation Pathway 63
6.4 Exploitation paths for KER7-Seamless onboarding for users 63
6.4.1 Competitor analysis 63
6.4.2 Market Analysis 64
6.4.3 Value proposition analysis 67
6.4.4 Barriers, obstacles and analysis of the standards and regulation 67
6.4.5 Technology and market watch 68
6.4.6 Business Model Canvas 69
6.4.7 Exploitation Pathway 70
6.5 Exploitation paths for KER8-User continuous behavioural authentication 71
6.5.1 Competitor analysis 71
6.5.2 Market analysis 71
6.5.3 Value proposition analysis 74

6.5.4 Barriers, obstacles and analysis of the standards and regulation 74
6.5.5 Technology and market watch 75
6.5.6 Business Model Canvas 75
6.5.7 Exploitation Pathway 78
6.6 Exploitation paths for KER9 - Device continuous behavioural authentication 79
6.6.1 Competitor analysis 79
6.6.2 Market Analysis 79
6.6.3 Value proposition analysis 80
6.6.4 Barriers, obstacles and analysis of the standards and regulation 80
6.6.5 Technology and market watch 80
6.6.6 Business Model Canvas 81
6.6.7 Exploitation Pathway 83
6.7 Exploitation paths for KER14a- Privacy Threat Modelling and Identification for Trustworthy AI-Privacy Enhancing Component (PEC) 84
6.7.1 Competitor analysis 84
6.7.2 Market analysis 85
6.7.3 Value Proposition analysis 90
6.7.4 Barriers, obstacles and analysis of standard regulation 90
6.7.5 Technology and market watch 91
6.7.6 Business Model Canvas 92
6.7.7 Exploitation Pathway 96
6.8 Exploitation paths for KER16-Infrastructure Management based on AI 96
6.8.1 Competitor analysis 96
6.8.2 Market analysis 97
6.8.3 Value Proposition analysis 99
6.8.4 Barriers, obstacles and analysis of standard regulation 100
6.8.5 Technology and market watch 100
6.8.6 Business Model Canvas 101
6.8.7 Exploitation Pathway 102
7 Business and Sustainability Plan for the TANGO Platform (KER17) 104
7.1 Methodological framework for the designing the Business and Sustainability Plan of the TANGO Platform 104
7.2 Product description 105
7.3 User Interaction with the TANGO Platform 108
7.4 Business problems that the TANGO system solves 109
7.5 Core Target Markets of the TANGO System 110

7.6 Market size, trends and analysis 111
7.7 Competition analysis and alternative solutions 117
7.8 SWOT analysis for the TANGO Platform 117
7.9 PESTLE Analysis for TANGO Platform 118
7.10 Unique Selling Point USP - Unique Value Proposition UVP 120
7.11 Societal benefits and impact of the TANGO system 121
7.12 Settings – legal and regulatory aspects 121
7.13 Marketing Strategies and Channels 122
7.14 Go-to-market and Use model of the TANGO system 122
7.15 IPR of the Foreground and Partners' Roles in Exploitation 123
7.16 Future Exploitation Roadmap 123
7.17 Business Model Canvas Methodology 124
7.18 Business Model Canvas of the TANGO Platform 125
8 Exploitation Conclusions 127
9 Conclusions 129
10 References 130
Annex A – List of TANGO Exploitable Results 132
Annex B - Exploitable Results Standardisation Mapping 135
Annex C – Exploitation plan for ERs 138
Exploitation paths for ER1- Blockchain-based data storage and sharing 138
Exploitation paths for ER2a- Trustworthiness Scoring Module (TSM) 144
Exploitation paths for ER2c- Privacy Risk Score (PRS) 148
Exploitation paths for ER3b- Confidentiality and Privacy by Design: ABE-toolset 154
Exploitation paths for ER4- Self-encryption and Decryption Techniques with Multi-Factor Information Recovery Mechanisms 159
Exploitation paths for ER5- ePrivacy Mechanisms, Protocols and Processes 164
Exploitation paths for ER6a- SSI Wallet 165
Exploitation paths for ER6b- SSI Zero Knowledge Proof 170
Exploitation paths for ER6c- SSI Agent 175
Exploitation paths for ER6d- IoT Machine-to-Machine Device Authentication 178
Exploitation paths for ER10- Hardening against Side channel Attacks 182
Exploitation paths for ER11- Exploratory Data Analysis engine (EDAE) 188
Exploitation paths for ER12a- Energy efficient AI model training, support for MLOps 192
Exploitation paths for ER12b- Energy efficient AI model training, Support for Federated Learning (FLEVIDEN) 196
Exploitation paths for ER12c- Energy efficient AI model training, Support for AutoML 200

Exploitation paths for ER13-Dynamic Intelligent Execution 204
Exploitation paths for ER14b- Privacy Threat Modelling and Identification for Trustworthy AI, Privacy Assurance Tool (PAT) 210
Exploitation paths for ER15- X-AI for Privacy and Trust Enhancement 213
Annex D – List of TANGO Exploitable Results 220
Annex E – Joint Exploitation Agreement (JEA) Template 223
Annex - F Exploitation plan - Table for all partners 226
Annex G - TANGO Stakeholder Mapping per Target Market 233

List of tables

Table 1 TANGO website articles M19-M36 ..... *26*
Table 2 Presence of TANGO in partners' online platforms *30*
Table 3 Scientific publications M19-M36 ..... *33*
Table 4 TANGO events & workshops *40*
Table 5 TANGO external synergies *43*
Table 6 impact analysis *45*
Table 7 - Dissemination and Communication KPIs tracking *47*
Table 8: KER2b Technology and Market watch *58*
Table 9: KER3a Technology and Market watch *61*
Table 10: KER7 Technology and Market watch *68*
Table 11: KER8 Technology and Market watch *75*
Table 12: KER14a Technology and Market watch *91*
Table 13: KER16 Technology and Market watch *101*
Table 14 ERs per Service Cluster *106*
Table 15: Defined user roles by service cluster *108*
Table 16: ER1 Technology and Market watch *141*
Table 17: ER2a Technology and Market watch *146*
Table 18: ER2c Technology and Market watch *153*
Table 19: ER3b Technology and Market watch *158*
Table 20: ER4 Technology and Market watch *161*
Table 21: ER5 Technology and Market watch *165*
Table 22: ER6a Technology and Market watch *169*
Table 23: ER6b Technology and Market watch *173*
Table 24: ER6c Technology and Market watch *177*
Table 25: ER6d Technology and Market watch *181*
Table 26: ER10 Technology and Market watch *185*
Table 27: ER11 Technology and Market watch *191*
Table 28: ER12a Technology and Market watch *195*
Table 29: ER12b Technology and Market watch *199*
Table 30: ER12c Technology and Market watch *203*
Table 31: ER13 Technology and Market watch *209*
Table 32: ER14b Technology and Market watch *212*
Table 33: ER15 Technology and Market watch *216*

List of figures

Figure 1 - TANGO Website Homepage 16
Figure 2 User acquisition 17
Figure 3 Visits over time 17
Figure 4 Channel types 17
Figure 5 Engagement rate 18
Figure 6 Industry overview of TANGO LinkedIn visitors 19
Figure 7 - TANGO Account on X 20
Figure 8 - TANGO Account on Mastodon 20
Figure 9 - TANGO YouTube Account 21
Figure 10 Newsletter subscribe forms 22
Figure 11 TANGO Newsletter – Issue 1 23
Figure 12 TANGO Newsletter – Issue 2 23
Figure 13 TANGO Newsletter – Issue 3 24
Figure 14 TANGO Newsletter – Issue 4 25
Figure 15 TANGO Newsletter – Issue 5 26
Figure 16: T8.2 Exploitation Methodology 54
Figure 17: KER2b Recommendation Engine Market segments (source: Mordor Intelligence) 55
Figure 18: KER2b Recommendation Engine Market size and growth rate (source: Grand View Research) 56
Figure 19: KER7 Recommendation Digital Identity Verification segments (source: Fortune Business Insights) 65
Figure 20: KER7 Digital Identity Verification Market size and growth rate (source: Grand View Research) 66
Figure 21: KER8 and KER9 AI in Cybersecurity market segments (source: Grand View Research) 72
Figure 22: KER8 and KER9 AI in Cybersecurity market size (source: Grand View Research) 73
Figure 23: KER14a and ER 14b AI Governance market market segments (source: Grand View Research) 86
Figure 24: KER14a and ER 14b AI Governance market size (source: Grand View Research) 87
Figure 25: KER16 AI in Renewable Energy Forecasting market segments (source: Grand View Research) 97
Figure 26: KER16 AI in Renewable Energy Forecasting market size (source: Grand View Research) 98
Figure 27: Overview of the TANGO platform as a system of service clusters for specific business sectors 106
Figure 28 Market size for the TANGO Platform (source: Grand View Research) 112
Figure 29 Europe and Global cybersecurity Market (source: Grand View Research) 114
Figure 30: Europe and Global Enterprise Data Market (source: Grand View Research) 115
Figure 31: ER2c Privacy Enhancing Technologies (PET) market segments (source: Univ Datos) 150
Figure 32: ER2c Privacy Enhancing Technologies (PET) market size and growth rate (source: Grand View Research) 151
Figure 33: ER3b Encryption Software market segments (source: Grand View Research) 156
Figure 34: ER6a Self-Sovereign Identity (SSI) market size (source: Cognitive Market Research) 167
Figure 35: ER6b Decentralized Identity Market segments (source: Grand View Research) 171

Figure 36: ER12b Federated Learning market size (source: Grand View Research) *197*
Figure 37: ER12c AutoML market size and growth rate (source: Grand View Research)..... *201*
Figure 38: ER13 Green Data Centre market segments (source: Mordor Intelligence)..... *205*
Figure 39: ER13 Green Data Centre market drivers (source: Mordor Intelligence) *206*
Figure 40 ER13 Green Data Centre market restraints (source: Mordor Intelligence) *207*
Figure 41: ER15 Explainable AI market size and growth rate (source: MarketUS) *214*

List of Acronyms

Abbreviation / Acronym	Description
AI	Artificial Intelligence
API	Application Program Interface
BMC	Business Model Canvas
DoA	Description of action
Dx.y	Deliverable number y belonging to WP x
EBSI	European Blockchain Services Infrastructure
EC	European Commission
eIDAS	Electronic Identification and Trust Services
ER	Exploitable results
IP	Intellectual property
IPR	Intellectual property rights
KER	Key Exploitable Result
KPI	Key Performance Indicator
MBA	Master of Business Administration
Mxy	Month xy of the project's timeline
PCT	Project Coordination Team
PESTLE	Political-Economic-Social-Technological Legal and Environmental
SoTA	State-of-The-Art
SWOT	Strengths-Weaknesses-Opportunities-Threats
TANGO	Digital Technologies ActiNg as Gatekeepers to information flOws
TRL	Technology readiness level
WP	Work Package

Executive Summary

The main goal of TANGO is to establish stronger cross-sector data sharing in a citizen-centric, secure, and trustworthy manner by developing a novel platform that is user-friendly, compliant, fair, transparent, accountable, and environmentally sustainable. Alongside its core technical research, TANGO has placed strong emphasis on dissemination, communication, exploitation, and stakeholder engagement (WP8), which are critical to raising awareness, sharing results, and ensuring future adoption and impact.

Over the project's full duration, the dissemination and communication strategy outlined in D8.1 has been implemented and continuously refined. The first phase focused on raising awareness of TANGO's objectives and challenges, while the second phase promoted and distributed the project's technical developments and results to targeted stakeholders. In the final phase, dissemination and exploitation activities have converged to maximise impact, focusing on sustainability and the uptake of Key Exploitable Results (KERs).

The exploitation strategy has evolved in parallel with the project lifecycle, leading to an updated and consolidated plan at project completion. This includes the prioritisation of KERs, their continuous monitoring, SWOT and PESTLE analyses, business model development, and actions related to IPR protection and allocation. These steps ensure that TANGO outcomes are well-positioned for adoption beyond the project's lifetime.

This final report therefore captures the complete dissemination, communication, and exploitation journey of TANGO, reflecting the joint efforts of consortium partners to engage stakeholders, ensure visibility, and translate technical achievements into sustainable impact. It confirms the project's commitment to building a secure, trustworthy, and privacy-preserving data ecosystem, while paving the way for continued exploitation of its results.

1 Introduction

1.1 Purpose of the document

This document constitutes the final report of dissemination, communication, and exploitation activities conducted for project TANGO (Digital Technologies ActiNg as Gatekeepers to information flOws) from March 2024 (M19) to August 2025 (M36). The present report describes the dissemination and communication activities that took place during the last 18 months of the project and outlines the planned activities for the remaining duration of the project. In addition, it presents the tools and activities that were undertaken to accomplish the set objectives, disseminate the project, and implement the strategy as it was set out in deliverables D8.1 "Dissemination, Communication, Exploitation and Stakeholders Engagement Plan", and D8.2 "Dissemination, Communication, Exploitation and Stakeholders Engagement Plan - Intermediate Version".

1.2 Relation to other project work

Deliverable 8.3 "Dissemination, Communication, Exploitation and Stakeholders Engagement Report - Final Version" plays an important role within the TANGO project, directly addressing Objective No. 6, which centres on the extensive communication and scientific dissemination of the project results. This deliverable serves as an updated and comprehensive report on the status of dissemination, communication, and exploitation activities carried out by project partners. The report encompasses a wide array of initiatives, including scientific publications, conference presentations, workshops, and other means to share project outcomes with the research, academic, and international community. Additionally, it highlights the efficient exploitation activities related to TANGO concepts and tools across various domains. It also presents the actions that have taken place related to the allocation of the IPR of the exploitable results, with references to the legal requirements to ensure proper protection and the rules related to the exploitation and in general use in any way of the exploitable results. Finally, D8.3 ensures that the conducted activities align with the objectives outlined in the project's Description of Action, providing a comprehensive overview of the project's progress and impact on a broader scale.

1.3 Structure of the document

This document is structured in 10 chapters. Following this introduction, chapter 2 provides the updates on the dissemination and communication strategy of TANGO. Chapter 3 is the reporting of the activities for the period M19-M36, and chapter 4 is the KPIs overview. Chapter 5 presents the overview on the innovation management plan and activities conducted in M19-M36. Chapter 6 provides the partners' individual exploitation plans, while chapter 7 is the business models and exploitation paths of the TANGO KERs. Chapter 8 is the joint exploitation plan on the TANGO platform. The overview on the standardisation activities is also outlined in this chapter. Finally, the conclusions summarise the report.

2 Dissemination, Communication, Exploitation, and Stakeholder Engagement Strategy Updates

The concrete dissemination and communication strategy has been defined in detail in Project Deliverables 8.1 "Dissemination, Communication and Project Branding", and 8.2 "Dissemination, Communication, Exploitation and Stakeholders Engagement Report Intermediate Version" which are available, under the section "Public Deliverables" in the project website. The current section provides information on the updates on TANGO dissemination tools and channels, during this period of interest. During this reporting period, two updates were made in the dissemination and communication strategy: The new LinkedIn newsletter account, and the visualisation of the project materials through YouTube.

Tango Newsletter

The creation of the LinkedIn newsletter account aimed to amplify the reach of the TANGO newsletter, supporting the already active newsletter disseminated through Mailchimp. For Mailchimp, the user can visit the TANGO website, scroll down, and subscribe to the project newsletter easily. This process is straightforward, ensuring a user-friendly and transparent subscription experience. For LinkedIn, the user can subscribe to the TANGO newsletter dedicated page. This dual approach boosts engagement and covers a bigger audience with different demographic characteristics, as Mailchimp is a more typical way of sharing newsletters, while LinkedIn is a more flexible platform. More details can be found in 3.3.

Visualisation of project materials

During this reporting period, significant efforts were dedicated to the development of audiovisual materials aimed at disseminating and promoting TANGO's results. A total of thirteen new videos were produced with the support of eco, highlighting both the technological innovations and the pilot activities carried out within the project. Further details are provided in 3.2.4.

3 Reporting of Dissemination Activities & Statistics

This chapter maps the communication channels' progress for the respective reporting period. It includes metrics from the website and the social media accounts, the external activities the consortium has participated in, the newsletters, the scientific publications, and the promotion of TANGO through partners' and synergies' networks.

3.1 TANGO's website performance & analytics

The TANGO official website (https://tango-project.eu/) was created early in the project as the central hub for dissemination and communication. It consolidates results, supports knowledge exchange, and shares experiences and best practices. Continuously updated, it provides current information, materials, and news on project outcomes. The site is optimized and indexed through specialized, project-related content and articles. Serving as the most comprehensive information channel, it plays a key role in the dissemination strategy and often acts as the destination for content shared across social media platforms.

Figure 1 - TANGO Website Homepage

The performance of the website was constantly monitored to ensure the website remains relevant and the team has a clear view of its outreach. Through Google Analytics, it was possible to map the traffic and track the number of visitors, as well as other relevant metrics over the last year of the project. In the figures below, the results from this reporting period, from M19 to M36, are presented:

User Acquisition

To obtain an overview of our users' behaviour, the first category is User Acquisition. The figure below presents the traffic and users' behaviour for the current reporting period. The following numbers are presented: 7400 visits, with an average duration of 1m33s, 2 actions per visitor, and almost 400 downloads of the project material.

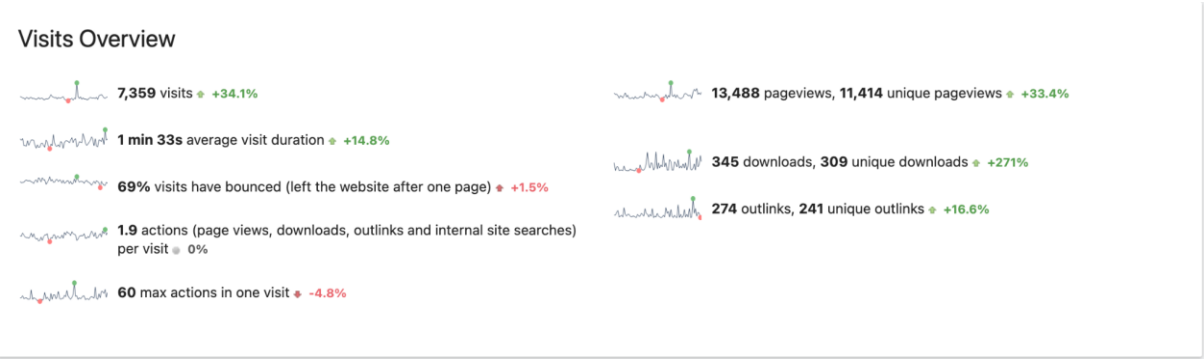


Figure 2 User acquisition

Visits & Channel types

Regarding the visits on the website, their rate presented stable, showing a steady interest in the TANGO project, while according to the channel types, most of the users found it through direct entry (4043) or search engines (2643).

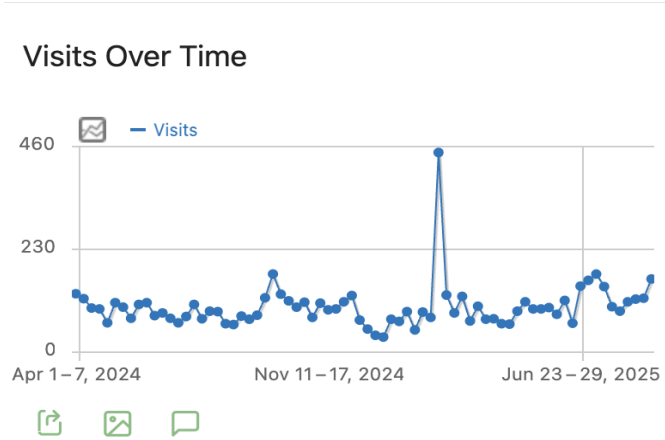


Figure 3 Visits over time

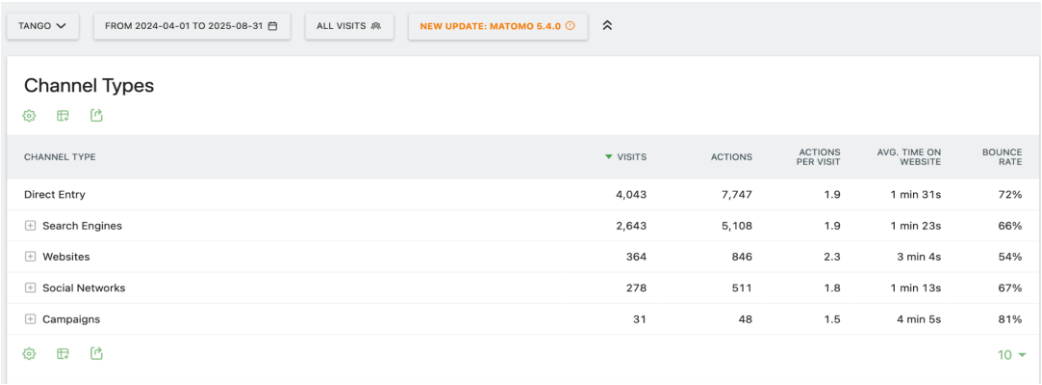


Figure 4 Channel types

3.2 Social media channels performance & analytics

TANGO maintains an active presence on LinkedIn, Twitter, Mastodon, and YouTube, ensuring wide visibility and targeted outreach. As outlined in the dissemination and communication strategy (D8.1), using multiple channels enables the project to reach diverse audiences, support scientific dissemination, and enhance overall impact. All profiles are consistently branded with the project logo and linked through the website footer, ensuring easy access and recognisability. Beyond sharing updates and project results, social media serves as a key reference point, promoting events, engaging with EU projects, policymakers, and stakeholders, and strengthening communication throughout the reporting period (M19–M36). The URLs of TANGO's social media accounts can be found below:

- LinkedIn: https://www.linkedin.com/company/tango-project-eu/
- X: https://x.com/tangoproject_eu
- Mastodon: https://mastodon.social/@tangoproject_eu
- YouTube: https://www.youtube.com/@tango-project

3.2.1 LinkedIn

LinkedIn is the most effective social network in terms of disseminating professional information. The TANGO page in LinkedIn is mainly used to connect with the scientific and technical community of the project, as well as the relevant industry partners. The news items on the website are replicated as posts and articles (depending on the content) on the LinkedIn page to attract more visitors to the website. In order to further engage the audience, along with the creation of traditional posts, several polls were also created with questions on cybersecurity, artificial intelligence and privacy, in order to increase the interactivity of the content created on the page. The follower base on this channel currently stands at 511 people, of which 218 were gained during the last 18 months, from April 2024 until August 2025. The traffic generated on this social network occurred organically, without using sponsored advertising. From April 2024 until August 2025, the engagement rate was around 18% with more than 27500 impressions (figure 5).

Figure 5 Engagement rate

Target industries that showed an interest to TANGO project during this period include IT Services and consulting (together almost 30% of the followers), Researchers and higher Education, as well as Software Development companies. Overall, it's clear that the targeted industries are aligned with the target personas identified in the communication funnel and can comprise relevant stakeholders for the project.

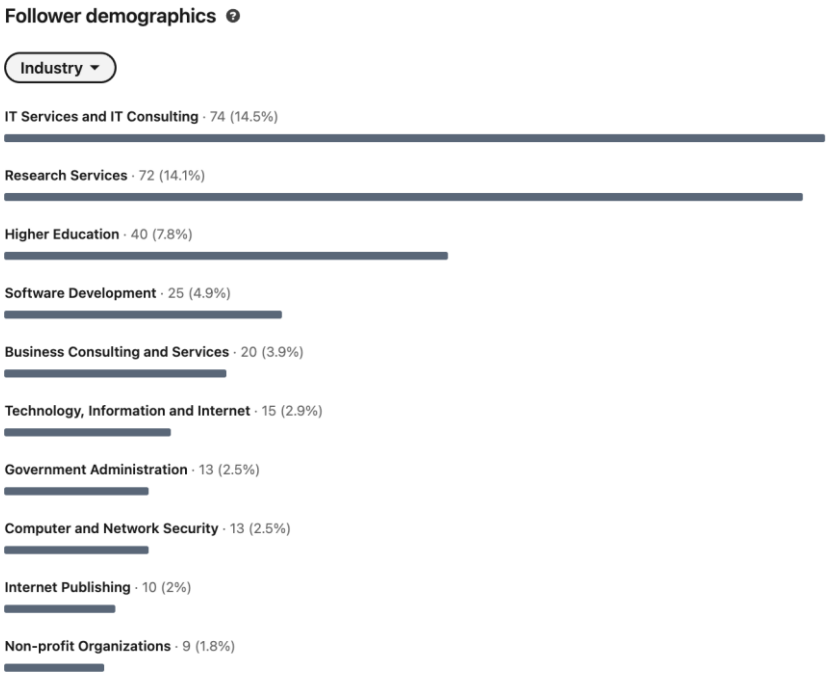


Figure 6 Industry overview of TANGO LinkedIn visitors

3.2.2 X

The project's X account has a total of 131 followers, marking only a modest increase from the 110 in the last period. This limited growth reflects a broader trend: following the acquisition of Twitter by Elon Musk in 2022 and its rebranding to X in 2023, the platform has undergone significant structural and policy changes that have reduced its overall credibility, user engagement, and relevance for professional and scientific dissemination. These external factors limit X's effectiveness as a communication channel. For this reason, close monitoring is required, but greater emphasis should be placed on other platforms—such as LinkedIn, Mastodon, and YouTube—that currently provide more stable and impactful opportunities for outreach and engagement with TANGO's target audiences.

Figure 7 - TANGO Account on X

Unfortunately, it is impossible to obtain insight data and metrics from X, which, since Elon Musk's acquisition, has implemented API costs.

3.2.3 Mastodon

As a response to the continuous degradation of X, the communication management team searched for an alternative. This alternative was Mastodon, an open-source microblogging platform composed of multiple servers, or "instances," each managed independently with its own moderation rules. Unlike mainstream platforms, it is decentralised, ad-free, and free of algorithms.

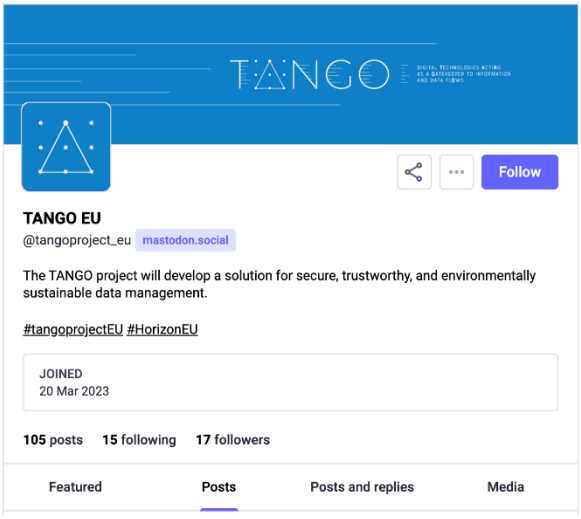


Figure 8 - TANGO Account on Mastodon

This platform was initially found relevant, because its user base largely consists of insiders and early adopters—an audience highly relevant to TANGO's dissemination strategy. By the end of the project, TANGO's presence on Mastodon counted 105 posts and 17 followers. Even though the project put effort in incorporating this social media platform in its armoury, interaction didn't grow, as Mastodont is still

a niche social network. This regression of the platforms has allowed LinkedIn to become the main channel for disseminating the project.

3.2.4 YouTube channel

During this reporting period, 13 new videos were uploaded on the project's channel, reaching a total of 15 videos, mainly focusing on presenting the technologies provided by TANGO. These videos serve as valuable resources for individuals interested in learning more about the project's goals, activities, and the technologies being developed. They offer a glimpse into the innovative solutions and research being conducted within the TANGO project, ultimately contributing to the advancement of border security policies and decision-making processes. The promotion of the videos has been executed through the project's website and social media channels, offering seamless access directly from these platforms. The videos have a total of 1094 views, a good result that denotes a high interest on the channel material. In addition, it is possible to argue that more than 2000 people has seen the TANGO videos, since they have been played in conferences & workshops.

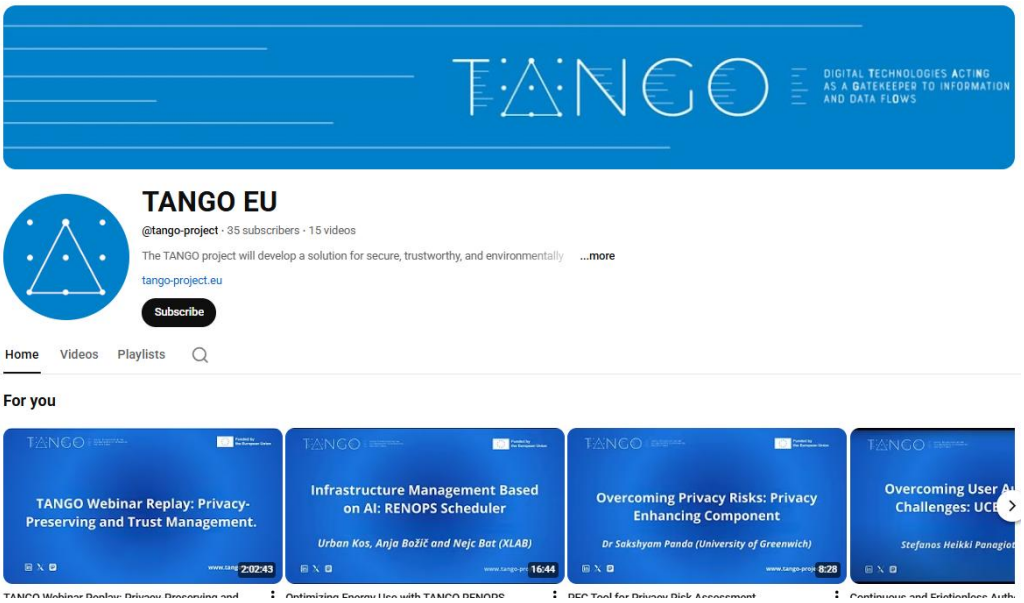


Figure 9 - TANGO YouTube Account

The list below contains the 13 videos that were published during this reporting period.

- TANGO Architecture: Powering Trustworthy and Intelligent Data Sharing
- Privacy-Preserving Recommendations with TANGO
- Optimizing Energy Use with TANGO RENOPS Scheduler
- PEC Tool for Privacy Risk Assessment
- DCBA: Validating Devices through Behaviour and Location
- Continuous and Frictionless Authentication with UCBA
- Rethinking Digital Identity – Seamless and Secure Onboarding with SOUD
- Gatekeepers of Trust: Exploring PEP & PDP in the TANGO Architecture

- From e-Passport to Trusted Access: Self-Sovereign Identity in TANGO
- TANGO Webinar Replay: Privacy-Preserving and Trust Management
- TANGO Interim Results
- Join the Data Revolution with TANGO
- Transform Your Services with TANGO: Secure, Insightful, and Impactful

3.3 TANGO newsletter

The TANGO project, during its lifecycle, maintained a regular newsletter schedule, typically around one every six months, depending on project updates and needs. As described in the strategy updates, the TANGO newsletters were disseminated through two channels: Mailchimp & LinkedIn. The TANGO newsletter reaches a dedicated audience of 188 people through LinkedIn and 120 through Mailchimp. subscribers.

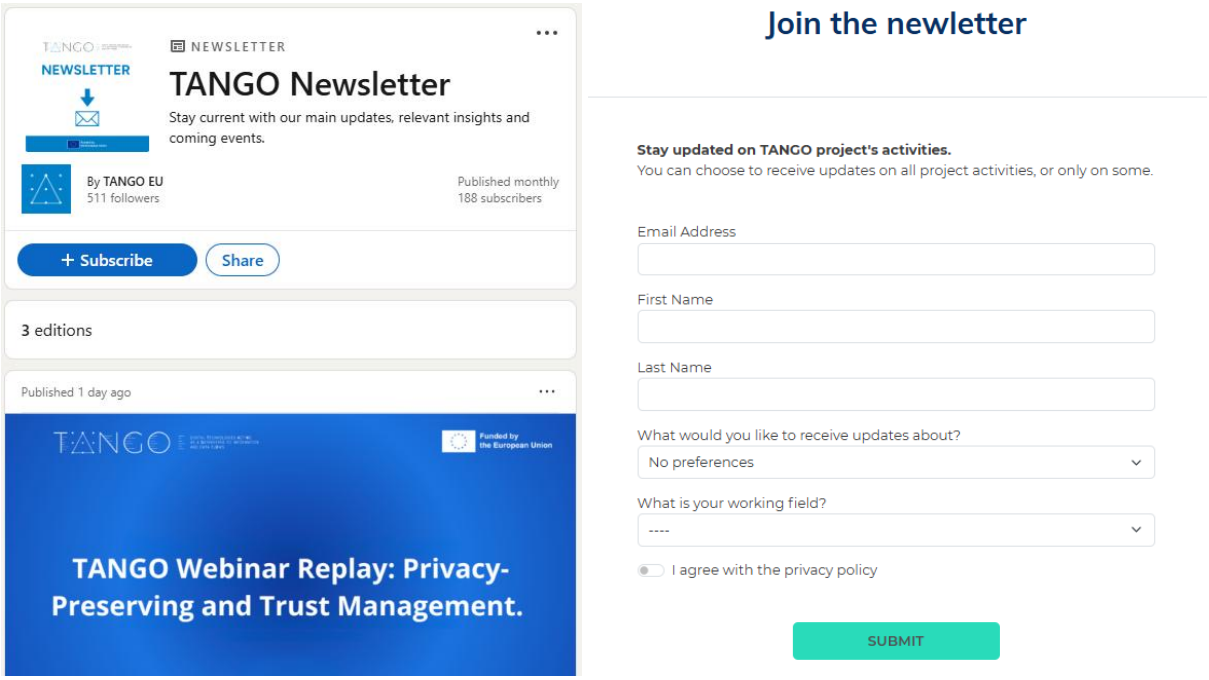


Figure 10 Newsletter subscribe forms

During the project, 5 newsletters were issued, with high engagement, since the newsletters, except for being sent through Mailchimp or published through LinkedIn, are also published on the website as news items. The topics of these newsletters covered the presentation of the project overall, the pilots, an interview series, and important events and webinars the project hosted.

1. **Issue 1 |** ***Introducing TANGO – Trusted Adaptive Next Generation Data Spaces*** **(April 2024)**

This first newsletter was disseminated through Mailchimp and it introduced the project to the audience and provides all the useful information to direct them to find more details on TANGO and engage with the website and the social media.

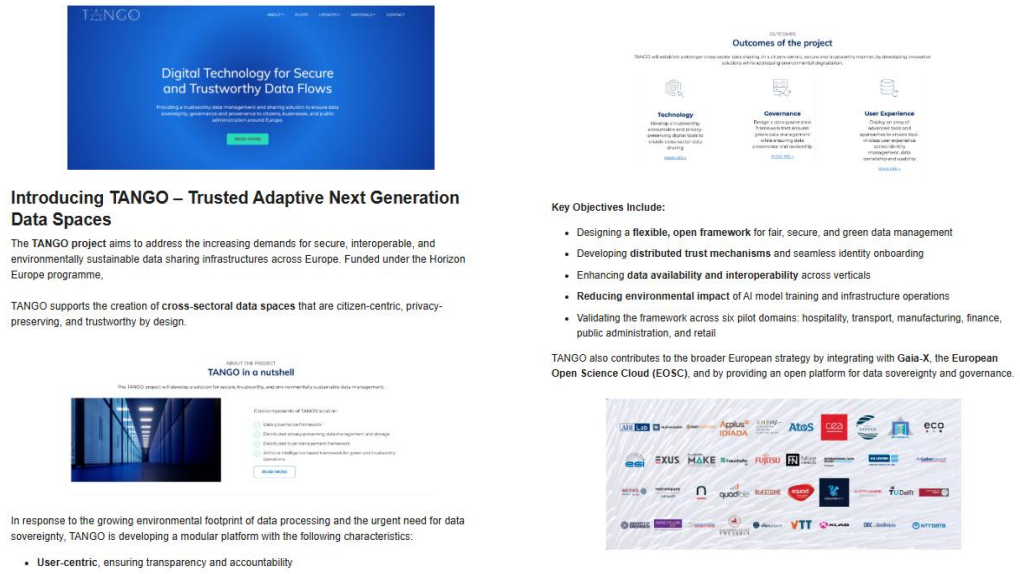


Figure 11 TANGO Newsletter – Issue 1

2. Issue 2 | *TANGO Pilots: Testing Trust and Privacy in Real-World Scenarios* (November 2024)

The second issue, disseminated via Mailchimp, introduced the TANGO pilots, presented six Real-World Scenarios. The audience was informed about the pilot objectives and was directed to the TANGO website for further reading.

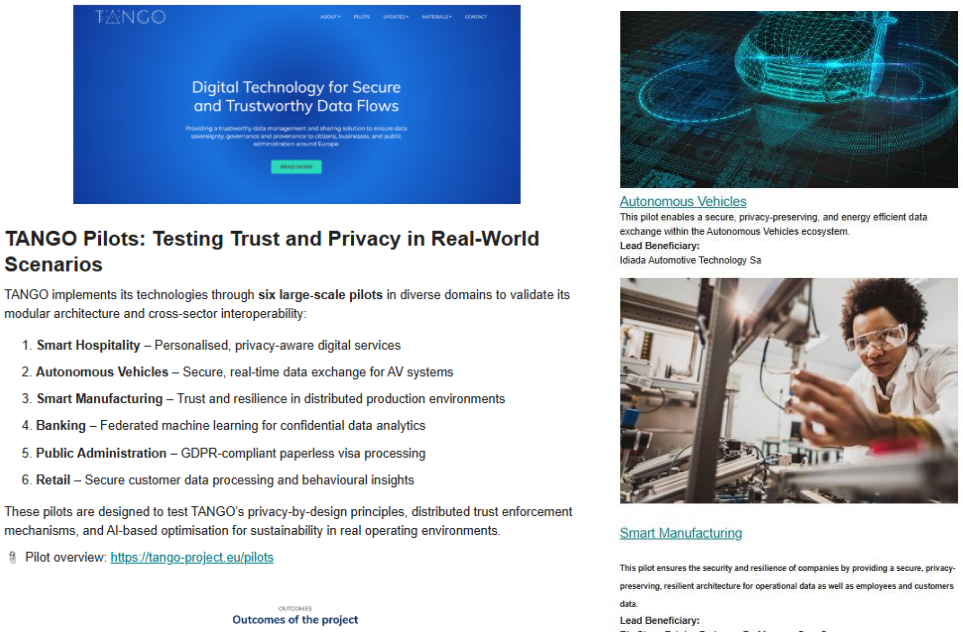


Figure 12 TANGO Newsletter – Issue 2

3. **Issue 3 | *TANGO Deep Dive Webinar – Privacy-Preserving and Trust Management Technologies* (July, 2025)**

In this 3rd (LinkedIn) newsletter, TANGO announced its **Deep Dive Webinar on Privacy-Preserving and Trust Management Technologies** (10 July 2025), presenting innovations in distributed trust, privacy-preserving data management, and self-sovereign identity. The event targeted developers and data governance experts, complemented by the **WP Leaders Interview Series** showcasing TANGO's technical achievements across privacy, trust, AI, and platform integration.

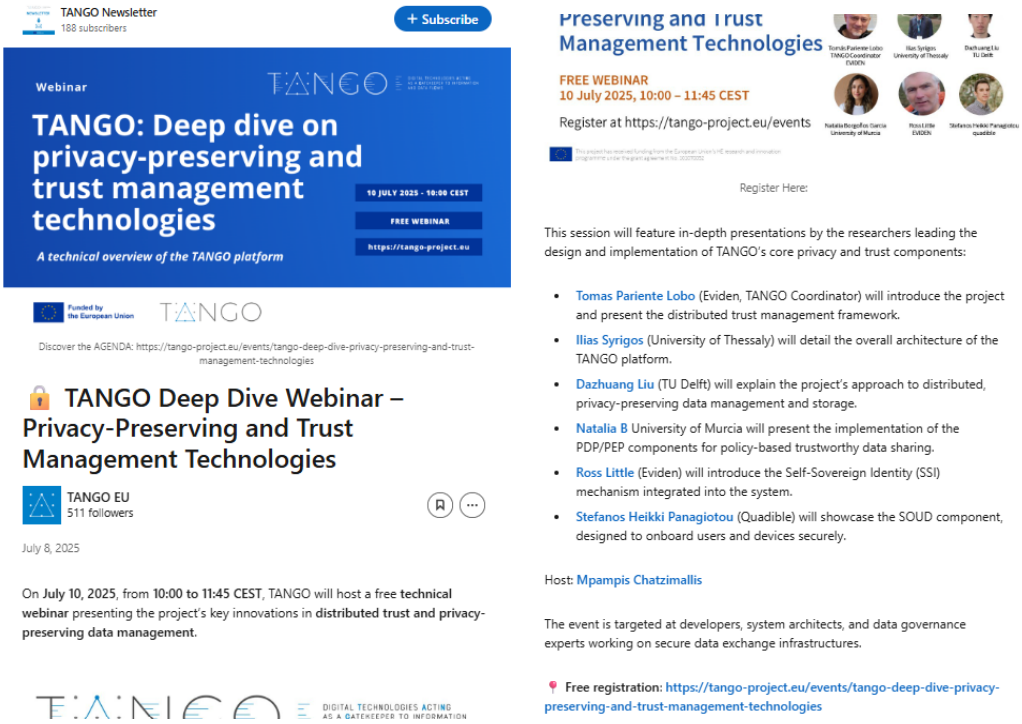


Figure 13 TANGO Newsletter – Issue 3

4. **Issue 4 | *TANGO Work Package Leaders Interview Series* (August, 2025)**

The 4th TANGO newsletter issue specifically promoted the **TANGO WP Leaders Interview Series**, highlighting technical achievements across the project, including privacy-preserving data management, distributed trust, sustainable AI, and platform integration.

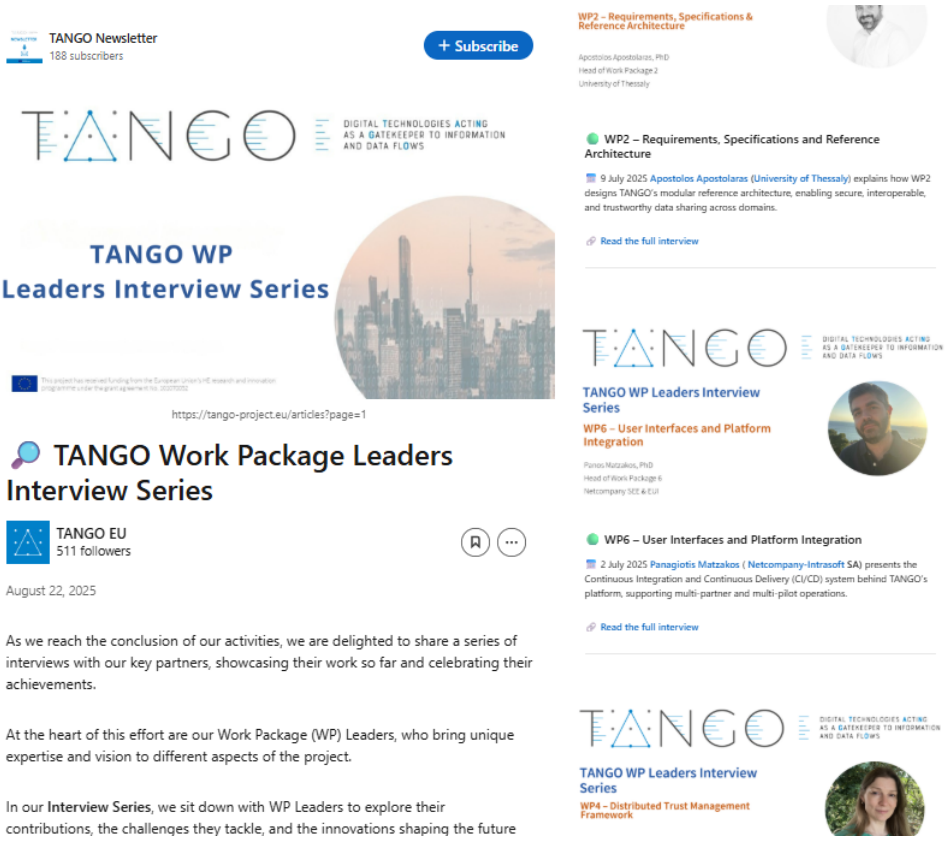


Figure 14 TANGO Newsletter – Issue 4

5. **Issue 5 | *Privacy-Preserving & Trust Management Technologies behind TANGO* (September, 2025)**

The last issue of the TANGO newsletters was dedicated to the webinar hosted in cooperation with ECO, on the topic of privacy-preserving and trust-enhancing technologies. Replay videos now showcase key exploitable results, including digital identity (SOUD), behavioural authentication (UCBA, DCBA), privacy risk tools, energy optimisation (RENOPS), and the TANGO Recommender. The series concludes with TANGO's modular reference architecture.

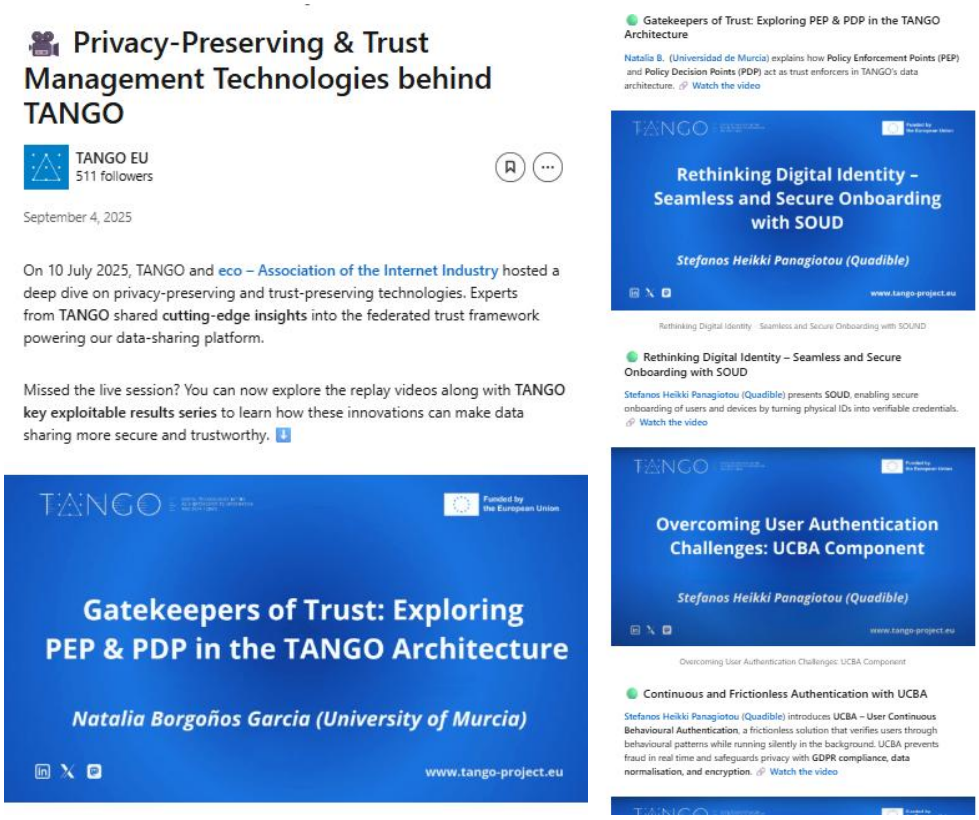


Figure 15 TANGO Newsletter – Issue 5

3.4 Project articles & news

On the project website, a dedicated page hosts the non-scientific articles from the project consortium, that help simplify and publicise the complex technical implementation of TANGO. The table below presents the articles published during this reporting period.

Table 1 TANGO website articles M19-M36

Title	Author	Summary
TANGO Architecture Powering Trusted and Intelligent Data Sharing	Ilias Syrigos (UTH), Peter Koller, Ladan Raeisian, Nelia Zinatullina (eco – Association of the Internet Industry)	In the final episode from the TANGO KERs series, Ilias Syrigos, Senior Research Engineer from the University of Thessaly, presents the TANGO Reference Architecture – a three-layered modular design that enables secure, decentralized and trustworthy data sharing.
Personalised yet Privacy-first Recommendations: The TANGO Approach	Ville Ollikainen (VTT), Peter Koller, Ladan Raeisian, Nelia Zinatullina (eco – Association of the Internet Industry)	In this episode from our video series on TANGO's key exploitable results, Ville Ollikainen from VTT – Technical Research Centre of Finland presents TANGO's Recommender – a novel solution that delivers

Title	Author	Summary
		personalised recommendations without collecting or storing personal data.
Optimizing Energy Use with TANGO RENOPS Scheduler	Urban Kos, Anja Božič and Nejc Bat (XLAB), Peter Koller, Ladan Raeisian, Nelia Zinatullina (eco – Association of the Internet Industry)	With electricity prices constantly fluctuating and carbon footprints on the rise, automated solutions for optimizing energy usage are becoming essential. That is why, in TANGO, we implemented RENOPS – the Renewable Energy Forecast Production Service. Urban Kos, Anja Božič and Nejc Bat from XLAB present the three-level tool which can shift tasks both geographically and in time, based on predicted renewable energy availability and the lowest expected price or carbon emissions.
PEC Tool: Redefining Privacy Risk Assessment for AI	Sakshyam Panda (UOG), Peter Koller, Ladan Raeisian, Nelia Zinatullina (eco – Association of the Internet Industry)	In this new TANGO KERs series video, Dr. Sakshyam Panda, Lecturer in Cyber Security at the University of Greenwich, introduced the Privacy Enhancing Component (PEC) Tool – an innovative, research-driven solution designed to support advanced privacy risk assessments.
Second TANGO White Paper: How Distributed Trust Ensures Secure Data Flows Across Europe	Dolores Ordóñez (ANYSOL), Ladan Raeisian, Lauresha Toska, Nelia Zinatullina, Peter Koller (ECO), Ilaria Fava, Renato Santana, Valeria Ardizzone (EGI), Ioannis Drivas (DBC), Alexandra Papageorgiou (KUL)	As the TANGO project is nearing completion, it presents its second white paper, on distributed trust frameworks and dataspaces.
TANGO: Key Recommendations for Standardisation	Claudia Mertinger (Fsas Technologies GmbH)	As the TANGO project is coming to an end, we are excited to share our experiences and thoughts on standardisation in TANGO and EU projects in general. While previous updates have highlighted technical innovations and collaborative efforts, this article focuses on how standardisation can shape and support the project's long-term impact.
DCBA: Validating Devices through Behaviour and Location	Stergios Lantzos (University of Thessaly), Peter Koller, Ladan Raeisian, Nelia Zinatullina (eco – Association of the Internet Industry)	TANGO's Device Continuous Behavioural Authentication (DCBA), presented by Stergios Lantzos from the University of Thessaly, is another ground-breaking TANGO's key exploitable result.
Continuous and Frictionless	Stefanos Heikki Panagiotou (QBE), Peter Koller, Ladan Raeisian,	As cyber threats grow more sophisticated, traditional authentication methods are no longer enough. In this new TANGO KERs Series video,

Title	Author	Summary
Authentication with UCBA	Nelia Zinatullina (eco – Association of the Internet Industry)	Stefanos Heikki Panagiotou from quadible presents the User Continuous Behavioural Authentication (UCBA) component.
Rethinking Digital Identity – Seamless and Secure Onboarding with SOUD	Stefanos Heikki Panagiotou (QBE), Peter Koller, Ladan Raeisian, Nelia Zinatullina (eco – Association of the Internet Industry)	In today's digital world, identity verification is more critical – and more challenging – than ever. In this video, Stefanos Heikki Panagiotou, Machine Learning Engineer at Quadible, presents SOUD (Seamless Onboarding of Users and Devices), a cutting-edge component of the TANGO project that redefines how we onboard users and devices securely and effortlessly.
Gatekeepers of Trust: Exploring PEP & PDP in the TANGO Architecture	Natalia Borgoños (UMU), Peter Koller, Ladan Raeisian, Nelia Zinatullina (eco – Association of the Internet Industry)	In this technical video, Natalia Borgoños Garcia from the University of Murcia provides a comprehensive overview of two key components in the TANGO architecture: the Policy Enforcement Point (PEP) and the Policy Decision Point (PDP).
From e-Passport to Trusted Access: Self-Sovereign Identity in TANGO	Ross Little (ATOS), Peter Koller, Ladan Raeisian, Nelia Zinatullina (eco – Association of the Internet Industry)	In this technical deep-dive, Ross Little (ATOS) explores the implementation of self-sovereign identity within TANGO. The presentation highlights the development of two types of digital wallets – standard and zero-knowledge proof (ZKP) versions – built on the walt.id framework and both integrated into mobile and web interfaces.
TANGO Webinar Replay: Privacy-Preserving and Trust Management	Mpampis Chatzimallis, (The Lisbon Council asbl) Peter Koller, Ladan Raeisian, Nelia Zinatullina (eco – Association of the Internet Industry), Tomás Pariente Lobo (ATOS), Ilias Syrigos (UTH), Dazhuang Liu (DUT), Natalia Borgoñós García (UMU), Stefanos Heikki Panagiotou (QBE), Ross Little (ATOS)	On 10 July 2025, the "TANGO Deep Dive on Privacy-Preserving and Trust Management Technologies" webinar was co-organised by the TANGO project and eco – Association of the Internet Industry. The session attracted participants from academia, industry, and public institutions and highlighted TANGO's progress in creating a secure, modular, and energy-efficient framework for data sharing.
TANGO Work Package Leaders Interview Series – WP2 Requirements, Specifications and	Apostolos Apostolaras (University of Thessaly), Peter Koller, Ladan Raeisian, Nelia Zinatullina (eco – Association of the Internet Industry)	In this final instalment of our interview series, we take a closer look at TANGO's work package 2 (WP2). Apostolos Apostolaras, head of WP2, shares insights into the design of TANGO's modular reference architecture, which enables secure, interoperable, and trustworthy data sharing across domains. We explore how this

Title	Author	Summary
Reference Architecture		architecture addresses key challenges such as data fragmentation and governance, laying the groundwork for a decentralised, federated TANGO data space.
TANGO Work Package Leaders Interview Series – WP6 User Interfaces and Platform Integration	Panagiotis Matzakos (Netcompany-Intrasoft) Peter Koller, Ladan Raeisian, Nelia Zinatullina (eco – Association of the Internet Industry)	In the fourth part of our TANGO WP Leaders Interview Series, we spoke with Panagiotis Matzakos from Netcompany-Intrasoft SA, who leads Work Package 6. We discussed how the Continuous Integration and Continuous Delivery (CI/CD) system of the TANGO platform operates in a multi-partner, multi-pilot environment, as well as the key strategies used to ensure the smooth integration of TANGO components.
TANGO WP Leaders Interview Series – WP4 Distributed Trust Management Framework	Anni Karinsalo (VTT), Peter Koller, Ladan Raeisian, Nelia Zinatullina (eco – Association of the Internet Industry)	In the third instalment of the TANGO interview series, we explore the contributions and innovations of Work Package 4 (WP4) withing the project, focusing on secure authentication and privacy-preserving identity management. We sat with Anni Karinsalo from VTT, who shared insights into key tools like Self-Sovereign Identity (SSI), Decentralized Identifiers, and Zero-Knowledge Proofs — highlighting both technical achievements and real-world user engagement.
TANGO WP Leaders Interview Series – WP3 Distributed Privacy-preserving Data Management and Storage	Kaitai Liang (TU Delft), Peter Koller, Ladan Raeisian, Nelia Zinatullina (eco – Association of the Internet Industry)	In this exclusive interview, we speak with Dr. Kaitai Liang, the head from TANGO work package 3 (WP3), to explore the technologies, challenges, and innovations behind privacy-preserving data management. Learn how user-centric design, advanced encryption, and real-world pilot feedback are shaping a secure and transparent digital future.
TANGO WP Leaders Interview Series – WP5 AI-based Framework for Green & Trustworthy Operations	Tomás Pariente Lobo (ATOS/EVIDEN), Peter Koller, Ladan Raeisian, Nelia Zinatullina (eco – Association of the Internet Industry)	The first edition of the **TANGO WP Leaders Interview Series** features Tomás Pariente Lobo (ATOS), lead of WP5 – AI-based Framework for Green & Trustworthy Operations. The interview highlights the challenges, innovations, and technical developments driving TANGO's work on AI-enabled, sustainable, and trustworthy data operations within the project.
TANGO General Assembly in Mallorca: Project Progress & Lessons Learned	Communication team	The 6th TANGO General Assembly (GA) took place in Alcúdia, Mallorca, from May 5 to 7, 2025. The TANGO project, funded by the EU's Horizon Europe programme, is now approaching its final phase, with key deliverables and reports

Title	Author	Summary
		due by the end of the summer 2025. During the meeting, project partners participated in on-site testing and evaluation of the Smart Hospitality Pilot and reviewed progress across all pilots and work packages.
A TANGO Project White Paper on Distributed Infrastructures, Secure Data Exchange & Data Spaces	Renato Santana, Ilaria Fava, Valeria Ardizzone (EGI), Lauresha Memeti, Ladan Raeisian (ECO), Giulia Giussani (IDSA), Ioannis Drivas (DBC), Andrea Palumbo (KUL), Dolores Ordóñez (ANYSOL)	TANGO released its first **White Paper** on Distributed Infrastructures, Secure Data Exchange, and Data Spaces.
Safeguarding Data Privacy: A Deep Dive into TANGO's Distributed Privacy-Preserving Data Management and Storage System	Kaitai Liang and Dazhuang Liu, Delft University of Technology	WP3 of TANGO develops the **Distributed Privacy-preserving Data Management and Storage system**, integrating blockchain-based storage, trustworthiness scoring, privacy-by-design principles, self-encryption, and secure sharing recommendations. These components enhance data security, trust, and privacy, seamlessly integrating into the TANGO framework to support secure, reliable, and compliant data management across the platform.
Navigating Data Ecosystems: Innovations and Challenges in Identity Management and Security	Anni Karinsalo, VTT Technical Research Centre of Finland	TANGO advances secure data ecosystems with its Distributed Trust Management Framework, featuring Self-Sovereign Identity, Seamless Onboarding, Behavioural Authentication for users and devices, and Side-Channel Attack Hardening. These innovations ensure fairness, accountability, and trust by safeguarding identity, enhancing privacy, and enabling continuous authentication, empowering end-users and organisations to share and manage data securely.

3.5 Promotion through partners' network

TANGO partners use their network and social media channels to facilitate the dissemination of the project and its activities. Partners reshare the communication material created by the communication team or produce their own, helping the project achieve prominent visibility. In total, the partners' online communication activities have generated an engagement of 23000 people. Below some examples can be found:

Table 2 Presence of TANGO in partners' online platforms

Partner	Type	Description	Target audience	Reach
FN	Social Media post	A LinkedIn post about our participation in the Majorca meeting, our work there and in Tango.	Industry, business	648 impressions
FN	Website article	UI & Exploitation at the 6th TANGO Assembly	All groups	N/A
FN	Website article	TANGO project	All groups	N/A
FN	Website article	How to Exploit Horizon EU Project Results: Steps for Maximum Impact	All groups	N/A
ECO	Website news item	DIGISUSTAIN 2024 Shows the Sustainability Potential of the Internet Industry	All groups	N/A
FMAKE	Website article	A blog post about the project and the 3D printing pilot	Industry, business partners	470 reads
FMAKE	LinkedIn post	Post to promote the blog article above	Industry, business partners	1162 views
ABI Lab	LinkedIn post	TANGO promotion	Industry, business partners	747 impressions
ABI Lab	Newsletter	TANGO activtities	Industry, business partners	1391 opens
ABI Lab	Interview	TANGO: ABI Lab guida la sfida europea alle frodi puntando su Federated learning e IA responsabile	Specific User Communities	N/A
NOR	Podcast	Penny Spyropoulou, legal associate, was norbloc's first podcast episode that looked to decipher the EU's latest legislation that provide new value for the Fides solution.	Industry, business partners	300
XLAB	LinkedIn post	Presentation of paper “Using Temporal Fusion Transformer Predictions to Maximise Use of Renewable Energy Sources”.	Specific User Communities	2035 impressions
XLAB	Facebook post	TANGO GA meeting	Specific User Communities	661 reaches
ANYSOL	LinkedIn post	TANGO joint activity with AETIB	Industry, business partners	299 impressions

Partner	Type	Description	Target audience	Reach
ANYSOL	LinkedIn post	Participating in the FIWARE iHub at Parc Bit	Industry, business partners	590 impressions
ANYSOL	LinkedIn post LinkedIn post LinkedIn post	Data Space Symposium	Industry, business partners	203/329/309 impressions
ANYSOL	LinkedIn post LinkedIn post	Tango Smart Hospitality pilot in Mallorca	Industry, business partners	1199/3044 impressions
ANYSOL	LinkedIn post LinkedIn post	Reunión del Grupo de Trabajo de Turismo en Gaia-X | FITUR2025	Industry, business partners	1145/448 impressions
ANYSOL	LinkedIn post LinkedIn post LinkedIn post LinkedIn post	Participation to the EBDVF 2024	Industry, business partners	594/1514/ 789/541 impressions
ANYSOL	LinkedIn post	World Tourism Day 2024	Industry, business partners	364 impressions
ANYSOL	LinkedIn post	TANGO 5th GA meeting	Industry, business partners	838 impressions
ANYSOL	LinkedIn post	Europe Day 2024	Industry, business partners	631 impressions
ANYSOL	LinkedIn post	World Environment Dat 2024	Industry, business partners	360 impressions
EGI	Newsletter	Promotion of the TANGO white papers	Research community	3000 recipients
eco	Website article	Digital Transformation in Business: Opportunities and Challenges in the Digital Economy, April 2024	Specific user communities	Sent out to dotmagazine subscribers
eco	Website article	Industry 4.0: Rising to the Cybersecurity Challenge in Smart Manufacturing	Specific user communities	Sent out to dotmagazine subscribers
eco	Media article	Federated Trust in Action: How TANGO Enables Federated and Sustainable Data Spaces in Europe. Eco article in dotmagazin, the industry magazine by led eco.	Industry, business partners	Distributed among 1,000 eco association member worldwide
VISA	Newsletter/ Report	Monthly TANGO progress update to Investors	Investors	3

3.6 Scientific Publications

During this reporting period the partners continued publishing several publications presented at relevant scientific events, with the aim of dissemination the project results. In the following table are the details of the materials published during this reporting period. It is crucial to mention that the initial KPI for the publications was 20 (both in conferences and in academic journals) and the consortium managed to reach a total of 38 publications, substantially surpassing the KPI. This reflects the great quality of the work that has been done in TANGO and the investment of the researchers and experts within the consortium to promote their work in the academic community.

Table 3 Scientific publications M19-M36

Partner(s)	Type	Title	Author(s)	Publisher/ Conference	DOI/Link
FHG	Conference paper	Towards Privacy-Preserving Machine Learning in Sovereign Data Spaces: Opportunities and Challenges	Mehdi Akbari Gurabi, Felix Hermsen, Avikarsha Mandal and Stefan Decker	Privacy and Identity 2023. IFIP Advances in Information and Communication Technology	https://doi.org/10.1007/978-3-031-57978-3_11
FHG	Conference paper	On Data Spaces for Retrieval Augmented Generation	Felix Hermsen, Lasse Nitz, Mehdi Akbari Gurabi, Roman Matzutt and Avikarsha Mandal	Europe meets Japan: Intercultural Workshop on Data Sovereignty and Generative AI: Applications, Design, Social, Ethical and Technological Impact	https://doi.org/10.18420/inf2024_57
FHG	Conference paper	A Conceptual Framework to Leverage Heuristics for Effective Human-Machine Collaboration in Incident Handling	Mehdi Akbari Gurabi, Muhammad Usman Mansoor, Roman Matzutt, Avikarsha Mandal, and Stefan Decker	Innovative Security Solutions for Information Technology and Communications. SecITC 2024	https://doi.org/10.1007/978-3-031-87760-5_3
FHG	Conference paper	Enhancing Cyber Threat Intelligence Sharing through Data Spaces in Critical Infrastructures	Mehdi Akbari Gurabi, Ömer Sen, Navid Rahimidanesh, Andreas Ulbig, Stefan Decker	IEEE International Conference on Cyber Security and Resilience (CSR)	https://doi.org/10.1109/CSR64739.2025.11130001

Partner(s)	Type	Title	Author(s)	Publisher/ Conference	DOI/Link
CEA	Conference paper	Combining Loop Shuffling and Code Polymorphism for Enhanced AES Side-Channel Security	Nicolas Belleville, Loïc Masure	COSADE 2024 conference - Springer	https://link.springer.com/chapter/10.1007/978-3-031-57543-3_14
ANYSOL	Paper	Conceptual Framework and Prospective Analysis of EU Tourism Data Spaces	Dolores Ordóñez-Martínez, Maurici Ruiz-Pérez	MDPI	https://doi.org/10.3390/su16010371
DUT	Conference paper	CCA-1 Secure Updatable Encryption with Adaptive Security	Huanhuan Chen, Yao Jiang Galteland & Kaitai Liang	ASIACRYPT 2023	https://eprint.iacr.org/2022/1339
DUT	Paper	Improved Wordpcfg for Passwords with Maximum Probability Segmentation	Wenting Li, Jiahong Yang, Haibo Cheng, Ping Wang, Kaitai Liang	IEEE ICASSP 2023	https://doi.org/10.1109/ICASSP49357.2023.10096535
ANYSOL	Paper	Toward Establishing a Tourism Data Space: Innovative Geo-Dashboard Development for Tourism Research and Management	Dolores Ordóñez-Martínez, Maurici Ruiz-Pérez	MDPI	https://doi.org/10.3390/smartcities7010026
XLAB	Workshop paper	Using Temporal Fusion Transformer Predictions to Maximise Use of Renewable Energy Sources	Jakob Jenko and Joao Pita Costa	IEEE	https://doi.org/10.1109/AIE61866.2024.10561261
UPRC	Conference paper	A theoretical framework for validating and evaluating the TANGO platform	Ioannis Katsanakis, Asterios Stroumpoulis, Evangelia Kopanaki	International Conference on Tourism (ICOT2024) - IATOUR	https://iatour.org/icot2024/wp-content/uploads/2024/06/Book-of-Abstracts-

Partner(s)	Type	Title	Author(s)	Publisher/ Conference	DOI/Link
		in smart hospitality			ICOT2024-FINAL.pdf
UPRC	Conference paper	Evaluation of the TANGO platform: Insights from the smart hospitality pilot	Ioannis Katsanakis, Asterios Stroumpoulis, Evangelia Kopanaki	International Conference on Tourism (ICOT2025) - IATOUR	https://iatour.org/icot2025/wp-content/uploads/2025/06/Book-of-Abstracts-ICOT2025-v4-1.pdf
UPRC, METRO	Conference paper	Enabling retail business intelligence through secure cross-border data analysis and visualisation: The TANGO platform approach	Giannopoulos, A., Katsanakis, I., Kopanaki, E., Kyriakopoulou, G., Stroumpoulis, A., & Tsiatiris, G.	International Conference on Business Analytics in Practice 2025, International Conference on Business Analytics in Practice (ICBAP2025) - Springer	*Pending publication*
UPRC, NTT DATA, SQUARED EV, EVIDEN	Conference paper	Enhancing fraud detection through privacy-preserving federated analytics: The banking pilot within the TANGO project	Currao F., Deimichei E., Katsanakis, I., Kopanaki, E., Martínez-Rodriguez I., Papadakis M. N., Pariente Lobo, T., Salmerón-Majadas S., Stroumpoulis, A., Theocharis S., Valentini G. & Zaras J.	International Conference on Business Analytics in Practice 2025, International Conference on Business Analytics in Practice (ICBAP2025) - Springer	*Pending publication*
XLAB	Conference paper	Learning from the COVID-19 Pandemic to Improve Critical Infrastructure Resilience using Temporal Fusion Transformers	Jakob Jenko, Joao Pita Costa, Daniel Vladušič, Urban Bavčar, Radoš Čabarkapa	19th Conference on Computer Science and Intelligence Systems (FedCSIS)	https://annals-csis.org/Volume_39/drp/pdf/2959.pdf
CEA	Paper	Genelle et al. Revisited: Masking an AES	Nicolas Belleville	IEEE Embedded Systems Letters	https://doi.org/10.1109/LES.2024.3516853

Partner(s)	Type	Title	Author(s)	Publisher/ Conference	DOI/Link
		Round With Only 4 Secure ANDs			
DUT	Paper	Stealthy Backdoor Attack Against Federated Learning Through Frequency Domain by Backdoor Neuron Constraint and Model Camouflage	Yanqi Qiao, Dazhuang Liu, Rui Wang, Kaitai Liang	IEEE Journal on Emerging and Selected Topics in Circuits and Systems	https://ieeexplore.ieee.org/abstract/document/10649604
DUT	Conference paper	LADDER: Multi-Objective Backdoor Attack via Evolutionary Algorithm	Dazhuang Liu, Yanqi Qiao, Rui Wang, Kaitai Liang, Georgios, Smaragdakis	Network and Distributed System Security (NDSS) Symposium	https://www.ndss-symposium.org/ndss-paper/ladder-multi-objective-backdoor-attack-via-evolutionary-algorithm/
KUL	Conference Paper	Essential Digital Skills for Digital Product Passports' Stakeholders under the Ecodesign for Sustainable Products Regulation	Alexandra Papageorgiou	IFAC-PapersOnLine – Elsevier, Volume 59, Number 10	*Pending publication*
UPRC	Conference paper	The Use of Digital Technologies in a Common Data Space and Sustainable Development Context: A Conceptual Framework Focus on Smart Hospitality	Ioannis Katsanakis, Asterios Stroumpoulis, Evangelia Kopanaki	ICOT 2023 CONFERENCE	https://iatour.org/icot2023/wp-content/uploads/2023/06/Book-of-Abstracts-ICOT2023-ver.1.pdf

Partner(s)	Type	Title	Author(s)	Publisher/ Conference	DOI/Link
UPRC	Conference paper	Exploring Digital Technology and Sustainable Development Integration in a Shared Data Environment: A Conceptual Framework on the Retail Sector	Ioannis Katsanakis, Asterios Stroumpoulis, Evangelia Kopanaki	HSSS 2023 CONFERENCE	https://confe.hsss.eu/wp-content/uploads/2023/10/HSSS-2023.pdf
UoM	Conference paper	Enabling Transparent Acceleration of Big Data Frameworks Using Heterogeneous Hardware	Maria Xekalaki, Juan Fumero, Athanasios Stratikopoulos, Katerina Doka, Christos Katsakioris, Constantinos Bitsakos, Nectarios Koziris, Christos Kotselidis	ACM, Proceedings of the VLDB Endowment - Volume 15, Issue 13	https://doi.org/10.14778/3565838.3565842
UoM	Conference paper	Beehive SPIR-V Toolkit A Composable and Functional API for Runtime SPIR-V Code Generation	Juan Fumero, György Rethy, Athanasios Stratikopoulos, Nikos Foutris, Christos Kotselidis	ACM, VMIL 2023: Proceedings of the 15th ACM SIGPLAN International Workshop on Virtual Machines and Intermediate Languages	https://doi.org/10.1145/3623507.3623555
UoM	Conference paper	Dynamic and Static Code Analysis for Java Programs on Heterogeneous Hardware	Athanasios Stratikopoulos, Tianyu Zuo, Umut Sarp Harbalioglu, Juan Fumero, Michail Papadimitriou, Orion Papadakis, Maria Xekalaki, Christos Kotselidis	22nd ACM SIGPLAN International Conference on Managed Programming Languages and Runtimes (MPLR '25)	https://doi.org/10.1145/3759426.3760984
UoM	Conference paper	TornadoViz: Visualizing Heterogeneous	Michail Papadimitriou, Maria Xekalaki,	22nd ACM SIGPLAN International Conference on	https://doi.org/10.1145/3759426.3760978

Partner(s)	Type	Title	Author(s)	Publisher/ Conference	DOI/Link
		Execution Patterns in Modern Managed Runtime Systems	Athanasios Stratikopoulos, Orion Papadakis, Juan Fumero, Christos Kotselidis	Managed Programming Languages and Runtimes (MPLR '25)	
UoG	Conference paper	Privacy Impact Assessment of Cyber Attacks on Connected and Autonomous Vehicles	Sakshyam Panda, Emmanouil Panaousis, George Loukas, Konstantinos Kentrotis	ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security	https://doi.org/10.1145/3600160.3605073
VTT	Conference paper	Obstacles In Implementing and Integrating Self-Sovereign Identity and Proposed Solutions	Erik Hieta-aho, Anni Karinsalo, Valtteri Lipiäinen	CENTRIC 2025, The 18th International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services"	*Pending publication*
DUT	Paper	MeetSafe: Enhancing Robustness Against White-Box Adversarial Examples	Ruben Stenhuis, Dazhuang Liu, Yanqi Qiao, Mauro Conti, Manos Panayotakis, and Kaitai Liang	Frontiers in Computer Science	https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2025.1631561/full

The publications made are in line with the main objectives of the outreach activity, enabling academia and other research organisations to build on TANGO developments for further research, provide key insights into technology offerings and lay the groundwork for future innovative projects.

3.7 Policy briefs/White Papers

3.7.1 Distributed Infrastructures, Secure Data Exchange & Data Spaces

Authors: Renato Santana, Ilaria Fava, Valeria Ardizzone (EGI), Lauresha Memeti, Ladan Raeisian (ECO), Giulia Giussani (IDSA), Ioannis Drivas (DBC), Andrea Palumbo (KUL), Dolores Ordóñez (ANYSOL)

The TANGO Project has published its first White Paper, dedicated to the critical themes of Distributed Infrastructures, Secure Data Exchange, and Data Spaces. This comprehensive document provides an in-depth overview of the current state of the art, reviewing available frameworks, tools, and

methodologies in these areas. It further explores how these concepts have been implemented and leveraged within the TANGO project, thereby offering practical insights into their application. In addition to mapping existing practices, the White Paper outlines a set of expert recommendations designed to strengthen the project's impact and guide future developments in distributed and privacy-preserving data ecosystems. By combining theoretical foundations with practical examples, it serves as a key reference point for stakeholders, policymakers, and researchers.

Link:https://tango-project.eu/sites/default/files/uploads/A%20First%20TANGO%20White%20Paper%20-%20T8-6%20-%20FINAL%20%281%29.pdf

3.7.2 Ensuring Data Sovereignty: TANGO Platform Solution for Secure and Trusted Data Flows Across Europe

Authors: Dolores Ordóñez (ANYSOL), Ladan Raeisian, Lauresha Toska, Nelia Zinatullina, Peter Koller (ECO), Ilaria Fava, Renato Santana, Valeria Ardizzone (EGI), Ioannis Drivas (DBC), Alexandra Papageorgiou (KUL)

As the TANGO project advances toward its final stages, the consortium released its second White Paper, focusing on the critical issue of data sovereignty in Europe. Building on the foundations established in the first White Paper, this new edition offers a deeper exploration of the security and privacy-preserving mechanisms underpinning the TANGO platform. This white paper focuses on the distributed trust framework that underpins the TANGO platform. It presents the key components that enable trustworthy data sharing and identity and access management as well as security and privacy mechanisms within TANGO's distributed infrastructure. Additionally, the paper outlines a set of policies and recommendations that are aligned with the TANGO platform's architectural principles.

Link:https://tango-project.eu/sites/default/files/uploads/TANGO%20Second%20White%20Paper%20%E2%80%93%20T8-6%20-%20FINAL%20version.pdf

3.7.3 Definition of Data Intermediation Services

Authors: Tervel Bobev, Vilte Kristina Dessers, Charlotte Ducuing, Michiel Fierens, Andrea Palumbo, Bert Peeters, Leander Stähler

The KU Leuven Centre for IT & IP Law - imec White Paper on the Definition of Data Intermediaries ('the White Paper') provides a detailed academic analysis of the definition of data intermediation services ('DIS') as introduced by the Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 ('the Data Governance Act' or 'the DGA'). The White Paper addresses the different criteria captured by the definition of DIS and offers a critical perspective on their interpretation. Notably, the definition provided by the DGA leaves considerable room for interpretation and does not provide certainty to organisations that may or may have not been targeted by the legislator. At the time of writing, there is neither institutional nor academic guidance with regard to the interpretation of DIS, and it will also take quite some time until the Court of Justice of the European Union ('the CJEU') will shed light on the matter. This White Paper aims to fill this gap by delineating the boundaries of what could eventually qualify as DIS and what would not, offering some guidance to the concerned organisations until the conclusive answers will be provided by the competent organisations and the CJEU.

Link: http://dx.doi.org/10.2139/ssrn.4589987

3.8 Organisation & Participation in events & workshops

All the events TANGO partners attended during the last 18 months of the project are reported in Table 4. The events consist of conferences, symposia and presentations in relevant events. Project partners were very active taking part in different events covering a wide variety of TANGO related topics, such as pilot activities, data spaces, big data, cybersecurity, retail and tourism sector. Most of the events partners attended had an international reach and audience, while the presentations of project results that took place were attended by a significant number of researchers, policy makers, social scientists, and public administration employees, resulting in widespread and effective dissemination of TANGO and its goals. The events that the partners participated in were both online and in presence.

Table 4 TANGO events & workshops

Type	Title	Description
Conference	Data Week 2024 Leuven 5-6/6/2024	Attendance to the Data Week 2024 in Leuven. Presentation at the event in the session "Data for Sustainability". [ATOS]
Conference	EBDVF 2024 Budapest 2-4/10/2024	Attendance to the European Big Data Value Forum. Presentation at the event in the session "Data Spaces across industries: sustainable and secure data management, use and re-use of data". [ATOS] Session "Digital technologies and processes for sustainable and secure data management, use and re-use of data: Tomas Pariente Lobo, coordinator of the TANGO EU project. Session "Value Creation in Data Spaces". Dolores Ordoñez, Daniel Alonso Román, Edward Curry, Natalie Bertels, Nuria De Lama, Tuomo Tuikka, Matthijs Punter, Tervel Bobev, Adam Tarcsi, Rafiqul Haque, and Gabriella Laatikainen. They discussed TANGO EU project, underlying the importance to generate impact with the data shared. [AnySol] Elicitation and explanation of the main ethical risks arising from the development of TANGO technologies, especially regarding data protection and AI (Objectives 1-3) [KUL]
Webinar	Webinar: TANGO Deep dive on privacy-preserving and trust management technologies 10/8/2025	Insights on privacy-preserving technologies, distributed trust, and Self-Sovereign Identity - 3 presentations and demos [ATOS] [QBE]
Conference	Data Space Symp11-12/3/25osium	Juan Ortells and Peio Oiz Arruti from AnySolution participated in Track 1 – Domain Session [Mobility & Tourism], presenting TANGO EU, among other projects. They highlighted how data spaces are enabling multimodal

Type	Title	Description
		mobility and sustainable tourism, driving smarter, more connected ecosystems IDSA participated to the session "Deep dive on the role of Privacy-Enhancing Technologies in data sharing initiatives" RIAS team presented a project pitch during the Symposium
Conference	FITUR 2025 25-26/1/25	Participation in the meeting of the Gaia-X Hub Spain Tourism Working Group, led by Anysol CEO Dolores Ordoñez, coordinator of the group. Anysol, as responsible for the Hospitality pilot, presented the TANGO project at FITUR 2024. At FITUR 2025, they attended the fair to learn about new developments and engage with various stakeholders in the tourism sector.
Webinar	Webinar of the Knowledge Centre Data & Society on the AI Act 13/3/24	Webinar on EU AI Act
Conference	EGI Conference 2024 30/9-4/10/24	Deep-Dive into Data Spaces: Choosing the Right Connector. Experiences from TANGO, CEDAR, DIVINE, DACAPO. This webinar was organised and disseminated by eco to highlight TANGO's progress in creating a secure, modular, and energy-efficient framework for data sharing. Focus was on the technological developments and implementations from respective WPs
Conference	EGI Conference 2025 2-4/6/25	Two posters, one about the TANGO Platform and the other about a preview of the second white paper, were presented at EGI2025
Conference	Digisustain 2024 - ECO 29/4/24	As hosts, eco has organized a full day with three sessions and multiple panels. Notably, in Session No. 3, eco has set aside a panel exclusively for TANGO and FAME (another EU-Horizon Project). Speakers from Fujitsu and VTT presented TANGO to IT industry leaders and digital community across Europe by highlighting its use cases, sustainable data exchange and GDPR compliance - eco, VTT, FSDE
Meeting	ABI Lab AI Hub 25/3/25	The goal was to demonstrate to the participating banks how artificial intelligence can be adopted in a collaborative and responsible way in the financial sector. The focus is on the use of Federated Learning, which enables banks to train AI models collaboratively across multiple institutions, without data leaving their respective environments. This approach ensures high levels of privacy, security, and compliance.
Conference	World Mobile Congress 2025 3-5/3/25	AnySol took part in MWC 2025 to explore key trends in smart cities, AI, cybersecurity, and sustainable mobility. It was an inspiring experience that helps them drive

Type	Title	Description
		innovation in their projects while connecting with professionals and stakeholders from across the sector.
Workshop	SeHAS 2025 workshop 17-19/1/25	Presentation of paper results "Genelle et al. Revisited: Masking an AES Round With Only 4 Secure ANDs"
Conference	eco interaction Day 2024 4/7/24	eco presented TANGO during its annual Interaction Day. Project managers discussed TANGO's design, mission and progress with more than 200 IT industry people
Workshop	Workshop: Build the professional qualification Data Space Technical Consultant 1/7/25	IDSA organised a workshop on their new professional qualification called "Data Space Business Consultant" with the aim of discussing and challenging the content of the certification
Conference /Expo	Tech Show Frankfurt 2025 4-5/6/25	Every year, eco has its own booth at the Tech Show Frankfurt, one of the biggest tech conferences in Europe. During 4-5 June, eco presented TANGO among other projects. We distributed TANGO flyers (project and pilot info) and engaged visitors
Conference	Tech Riders Summit Hürth 2025 3/7/25	TechRiders Summit in Hürth, Germany is a large event that combines conference, expo, and festival with inspiring content, live demos and networking. It showcases cutting-edge technologies with AI-powered panel discussions and interactive formats. Main topics are innovation, resilience, apractical solutions in IT infrastructure, security, data protection. Eco had its own booth in the premises and presented TANGO among other eco projects by distributing flyers and engaging industry partners and business people
Roundtable	De-Cix Roundtable Frankfurt 2025 May 2025	De-cix, eco's subsidiary, has a series of roundtables in major German cities to engage local tech community and pitch ongoing projects. Eco held a successful presentation on TANGO in May in Frankfurt's round
Education/ training event	Invited Talk at JUG Manchester October 2025	UoM gave an invited talk to the Java User Group in Manchester. They presented the work in the TornadoVM project as part of the TANGO project and tried to explain in simple terms the programming model, based on practical examples and demos.
Conference	HIPEAC Poster Presentation (2025) 20-22/1/25	Poster presentation in HIPEAC conference, a EU network that bridges industry and academia. In this poster, UoM presented the work of WP5 of TANGO regarding the hardware acceleration and energy efficiency.
Education/ training event	FOSDEM'24 3-4/2/24	Presentation during the Java Group of the biggest open-source event hosted in Europe (FOSDEM). UoM presented the work in the TornadoVM project as part of the TANGO project in WP5.

Type	Title	Description
Education/ training event	Devoxx YouTube channel 2024	Talk at Devoxx Manchester. This is the biggest industry-driven event attracting thousands of people from industry. UoM the work in the TornadoVM project as part of the TANGO project and tried to explain in simple terms the programming model, based on practical examples and demos.
Education/ training event	DevoxxBe 2025 - TornadoVM Tutorial DevoxxBe 2025 - Acceleration of GPULlama.java system with TornadoVM 6-10/10/25	[1] UoM will present a deep tech dive to the TornadoVM technology in the Devoxx Belgium venue, which attracts every yeat throusands of developers. The scope is to show the technology and how developers can use it, including utilities and extensions that we implemented in the context of the TANGO project for the Dynamic Intelligent Execution on Heterogeneous Hardware. [2] UoM will present a use case of an LLM inference engine implemented in Java and accelerated with TornadoVM in the Devoxx Belgium venue, which attracts every yeat throusands of developers. This project has been partly supported by funding of TANGO and can showcase how TornadoVM is used in the AI Java domain.Execution on Heterogeneous Hardware.
Consult	HS Booster services 2025	Cooeration between FSDE & Assigned expert on standardisation for a period of three months.
Conference	Fujitsu Distinguished Engineers Conference 2024	Presentation on Fujitsu's activities in HORIZON Europe projects. with TANGO and the Trustworthiness Module illustrating ongoing work and results

3.9 TANGO external synergies

The project partners collaborate with consortia from relevant projects and initiatives to enhance the visibility of each other, using their communication channels.

3.9.1 Events & Meetings

TANGO organises joint activities with other projects, while creating website and social media content. These joint activities are included below.

Table 5 TANGO external synergies

Title	Date	Description	Collaboration	Target audience
Convergence call with SEDIMARK project	13/8/24	Call to explain the TANGO project and initiate collaboration (coordinators and dissemination leaders) [ATOS]	SEDIMARK project	Research/Academia

Title	Date	Description	Collaboration	Target audience
GreenBridge DataSpace Cluster - Technical Coordinators Workshop	6/11/24	Online workshop with sister projects. Presentation of the project from the technical perspective [ATOS]	GreenBridge DataSpace Cluster	Innovators
Greenbridge Workshop ADRA-e conference	18/2/25	Representation (coordinator online, other partners physically at the ADRA-e conference in the scope of the GreenBridge cluster of projects [ATOS]	GreenBridge DataSpace Cluster	Innovators
Standardisation Co-Creation workshop	21/7/25	eco supported Fujitsu with organising a workshop within T8.4. TANGO united with MobiSpaces and NeMo.Bil in a joint Standardisation Co-Creation Workshop with restricted participation to explore synergies, exchange best practices and co-develop recommendations for interoperable and trustworthy mobility data spaces. ATOS presented also the project and their work with standards.	MobiSpaces NeMo.Bil	Innovators
Future-Ready: On-Demand Solutions with AI, Data, and Robotics	18-19/2/24	Showcasing TANGO technologies alignment with environmental sustainability goals with EU hard and soft law (Objectives 1-2)	Adra-e	Industry, business partners, EU Institutions, Regional authorities, Local authorities, Research communities
EGI2024	30-9/4-10/25	TANGO workshop in collaboration with CEDAR, DIVINE and DataMite at the EGI2024 conference, focused on the shared mission of these Horizon Europe projects: creating resilient, trusted, and	CEDAR DIVINE DataMite	Research community

Title	Date	Description	Collaboration	Target audience
		interoperable data spaces that align with Europe's digital sovereignty ambitions.		
MobiSpaces & TANGO synergy meeting	July 2025	Explore how the two project initiatives align and where they can join forces for greater societal and environmental hashtag impact.	MobiSpaces	Research communities
Participation to MobiSpaces Final event	5/3/25	On behalf of TANGO, eco took part in a panel discussion during the MobiSpaces final event in Rome to align on project activities and bring synergies	MobiSpaces	Research community
Presentation at DSSC Technology Thematic Group workshop	15/5/25	eco organised TANGO's participation in the workshop on 15 May 2025, Kaitai Liang held a presentation on TANGO's approach on data privacy and protection in data spaces	CSSC	Research community

3.9.2 Collaboration with MobiSpaces on Impact Analysis

MobiSpaces and TANGO, decided to join forces and identify their common impact areas in order to examine the potential impact their projects can have. These common denominators include the areas of Data Management & Governance, Edge Computing & AI, Environmental Sustainability, Societal Impact, Economic Impact, Public Administration, and Transport & Mobility. For each area they described the respecting impact of each project and at the end they identified the shared opportunities. The table below summarises this information.

Table 6 impact analysis

Impact Area	MobiSpaces Impact	Tango Impact	Shared Opportunities
Data Management & Governance	Data governance for mobility data spaces, integrating AI for data analysis and predictive maintenance.	Privacy-preserving data management platform ensuring data sovereignty and secure data exchange.	Collaboration on interoperable data governance frameworks to facilitate cross-sector data sharing.

Edge Computing & AI	Edge computing for real-time fleet management and vessel tracking.	AI frameworks ensuring data privacy, optimized energy consumption in data processing.	Joint development of privacy-preserving edge AI models for transport and maritime monitoring.
Environmental Sustainability	Optimization of electric fleets, reducing emissions through data-driven fleet management.	Reduction of digital infrastructure carbon footprint, sustainable data practices and energy efficient AI model training	Integration of environmental data to assess and mitigate transport-related emissions.
Societal Impact	Enhanced transport efficiency, improved air quality monitoring, maritime safety.	Empowering citizens with control over personal data, improving digital service trust.	Citizen-centric services: Data-driven transport optimization and enhanced digital service trust.
Economic Impact	New market opportunities in smart mobility, maritime monitoring, and data analytics.	Supporting SMEs with AI tools and secure data-sharing frameworks.	Joint initiatives to stimulate data-driven economic growth in the mobility and maritime sectors.
Public Administration	Integration of mobility data to improve urban transport services.	Enhanced policy-making through secure data-sharing platforms.	Combining mobility and public administration data to optimize city services and policy-making.
Transport & Mobility	Data-driven optimization of electric public transport fleets.	Data sharing between between user-to-car, car-to-user, environment-to-car and infrastructure for safer transport	Developing secure data-sharing frameworks for autonomous vehicle networks and public transport systems.

The collaboration between MobiSpaces & TANGO highlights the added value of aligning complementary areas of expertise and impact. By jointly examining their potential contributions across domains such as data governance, edge computing, environmental sustainability, and transport and mobility, the two projects demonstrate clear opportunities for synergies that extend beyond their individual scopes. This enables the development of interoperable frameworks, supports evidence-based policy-making, enhances economic and societal benefits, and contributes to the advancement of sustainable and citizen-oriented digital and transport ecosystems.

4 Dissemination and Communication monitoring

In retrospect, the TANGO project has successfully concluded its operations, with the culmination of its activities. A comprehensive assessment of the project's dissemination and outreach endeavors were undertaken. Monitoring and evaluating these activities have been an ongoing task, yielding valuable insights into their effectiveness and impact throughout the project's duration. This section provides an overview of the outreach of the TANGO activities in the whole project's lifecycle, based on the KPIs. The following table presents an indication of how effective these activities were during the last 18 months of the project (M19 – M36).

Table 7 - Dissemination and Communication KPIs tracking

Measure	KPI	Target	M18-M36	Status
TANGO Brochures	No. Of brochures distributed	600	350	620
Posters	No. Of posters produced	2	1	2
High-level materials for policy makers	Number of sets (mission statement, slide-deck, brochure)	3	1	3
TANGO Website	Number of unique visitors	3000	7400	13000
Social Networks	Number of followers on Twitter	500	21	131
	No. of followers on LinkedIn	2000	250	700 27500 impr.
	No. of followers on YouTube	100	12	35
TANGO Workshops	No. of workshops	3	2	3
	No. of participants	300	270	320
Videos	Number of videos published on the project's YouTube channel	2	13	15
	Avg. no. of views	1000	1000	1047
Scientific Publications	Number of peer-reviewed conference workshop/papers	At least 15	22	32
Scientific Publications	Number of peer-reviewed papers in academic journals	At least 10	6	6
Other Publications	White Papers	> 2	2	3

5 Innovation Management Plan & Activities M18-M36

5.1 Updated exploitation plan

The initial exploitation strategy of the project, encompassing innovation and Intellectual Property Rights (IPR) management, was outlined in Deliverable D8.1 and subsequently revised in D8.2. TANGO has adopted a dynamic approach to innovation management and exploitation, incorporating minor adjustments from previous versions to better support the effective uptake of project outcomes by relevant stakeholders. The strategy is structured into five distinct phases, each emphasising practical, impact-oriented, and business-driven methodologies, as detailed below.

Innovation Management
Innovation management log creation
Identify the project ER and KER
Taxonomy of ER (TRL, type, features, benefits)
Individual and joint exploitation paths per ER
Stakeholder groups, users and customer segments
Innovation management task force (INTRA, FN, DBC)

IPR Strategy
GA and CA analysis
IP Ownership
IPR Log (Foreground IP, Background IP)
IP protection, Access rights, Licenses

Visibility of Key Results
Innovation Radar and Standardisation Booster
Synergies with established initiatives (Gaia-X, EOSC, Catena-X)
Alliances with industrial and research organisations

Business modelling and Market Research
Barriers, obstacles and analysis of the standards and regulation
Market research and competition analysis
SWOT and PEST analysis
Business models for the KER

Roadmap to commercialisation
Business planning and marketing strategy
Go-to-market strategy
TANGO validation campaigns

The key points and activities of the TANGO exploitation plan are described below:

Initial Phase - Exploitable Results Identification

The consortium focused on updating and identifying new Exploitable Results (ER). Each Task Leader analysed technical activities, proposing modules, software components, datasets, or guidelines with academic or commercial potential. Exploitable results have been classified by type, TRL level, value proposition, and features. Two main exploitation types per result are considered: Individual Exploitation and Joint Exploitation. Out of the list of ER, a set of Key Exploitable Results (KER) has been identified and will be updated.

Innovation Management and IPR Strategy

The Innovation Management Log, jointly managed by INTRA, FN, and DBC, facilitates innovation management activities. It is an excel template aiding in ER and KER identification, classification, design of exploitation paths, and contributor definition. Simultaneously, DBC implemented IPR Management processes to meticulously identify and manage both Background (BG) and Foreground (FG) IP.

Diverse Partners for Joint Exploitation

The project involves diverse partners, categorized into technology providers, use case owners, universities/research organizations, and associations. Each partner group has different expertise, goals, networks, and geographical coverage, contributing to the joint exploitation of project results.

Visibility of the KER and Business Model Design

The dissemination phase involves uploading key project results to EC-backed platforms (i.e., Innovation Radar and Horizon Results Platform), emphasizing synergies with relevant initiatives and networking with associations. For each KER, a collaborative business model is designed, incorporating market analysis, competitive landscape evaluation, business barriers, regulatory frameworks, and a dedicated business plan.

TANGO Roadmap to Commercialization

The exploitation strategy follows a three-stage roadmap.

- ***Short-term Stage***: Design go-to-market strategies for the identified TANGO KER, validate innovations through real-life scenarios, and build viable business cases during the project's implementation.
- ***Mid-term Stage***: Design semi-commercial products and services, seek early adopters, expand the customer base, and utilize KER in further research activities 1-3 years post-project completion.
- ***Long-term Stage***: Commercialize validated KER with significant business potential based on partners' objectives, resources, and available funding 3 years after project completion.

5.2 General description related to Intellectual Property

The TANGO project aims to develop a comprehensive platform that facilitates data sharing across multiple economic sectors, such as smart hospitality, autonomous mobility and banking, in a manner that is citizen-centric, secure, and trustworthy, while simultaneously contributing to environmental sustainability and addressing the challenges of climate change. In line with this objective, by the end of

the project, a series of results will have been generated with regards to the platform's development, the exploitation of which is considered a priority for ensuring the sustainability and broader impact of the project outcomes.

As outlined in detail in Deliverable D8.2 and in accordance with the recommendations set forth in the Grant Agreement regarding the exploitation of project results and compliance with applicable IPR provisions, it is essential to establish clear IPR arrangements and adopt flexible ownership schemes tailored to the collaborative nature of the project.

To this end, the following aspects must be clearly identified and addressed:

i. A detailed description of the results developed during the implementation of the TANGO project,
ii. The management framework applicable to those results,
iii. The identification and handling of cases involving joint ownership,
iv. Measures to protect the results from unauthorised access or use,
v. The strategy for disseminating the results and
vi. The approach to exploiting the results for maximum value and impact.

In order to better address the allocations of IP related rights, it is essential to distinguish between the notion of ownership and contribution of IP. Specifically:

Ownership: The legal right of possession and control over an ER (e.g. a technology, dataset, algorithm, software) developed during the project.

The owner(s) of an ER holds the full legal rights to determine the conditions under which the result is further used, protected, disseminated or commercially exploited. This includes decisions regarding the protection of intellectual property, for instance, by filing for patents, trademarks, or other relevant IPR titles, as well as the licensing of the result to third parties, either exclusively or non-exclusively. Owners may also define the terms under which the result can be commercialised, whether directly by themselves or indirectly through partnerships, spin-offs, or technology transfer agreements.

Ownership of an ER may be either:

- **Individual**, where a single beneficiary has generated the result and therefore holds exclusive ownership rights, or
- **Joint**, where two or more beneficiaries have jointly generated the result and their respective contributions cannot be distinctly separated. In such cases, the result is subject to joint ownership, and the rights and obligations of each co-owner must be defined in a joint ownership agreement, which governs the use, licensing, and potential revenue sharing arising from the ER.

Contribution: The input or effort a partner has made in the development of an ER, regardless of whether they own it.

A project partner may contribute to the development of an ER through various forms of involvement, such as providing technical support, participating in software testing, conducting validation activities, or offering conceptual input. However, such contributions do not automatically confer ownership rights over the result. While the contributing partner may not hold legal title to the ER, their input may be substantial and should be appropriately acknowledged in accordance with the internal arrangements of the consortium.

Accurately tracking contributions is of critical importance. It enables the consortium to determine appropriate access rights for non-owning partners who need to use the ER in subsequent activities, whether for internal research or commercialisation. Furthermore, it provides a clear and defensible basis for asserting claims during intellectual property negotiations, particularly when determining licensing conditions or benefit-sharing arrangements. Beyond the legal and strategic dimensions, the recognition of partner contributions also supports transparency and trust within the consortium, ensuring fair treatment and promoting a collaborative project environment. This approach is in line with best practices advocated by the European IPR Helpdesk[1] and complies with the principles set out in the Horizon Europe Grant Agreement regarding the management and exploitation of project results.

To avoid redundancy and repetition, reference is made to the previous deliverable (D8.2), which provides the definitions of key terms related to IP management and IPR as well as an outline of the intellectual property planning methodology, the knowledge management framework and the categorisation of knowledge types, specifically Background and ERs.

5.3 Record of intellectual property assets

The updated list of TANGO Exploitable Results (ERs) is presented in **Annex A**. This table offers a comprehensive overview of each ER identified to date within the project, including details on ownership status (individual or joint), the names of the respective owners and contributors, the associated project tasks, the type of result and the current Technology Readiness Level (TRL). It serves as a consolidated record of the project's key innovations, each of which holds substantial potential for future exploitation. This list provides the foundation for subsequent business planning and the formulation of go-to-market strategies. It should be noted that, although no changes are currently anticipated, the list of ERs may be subject to further updates following the conclusion of the project, particularly in view of final technical developments and the evolving business perspectives of the consortium partners.

5.3.1 Ownership schemas and IPR matrix

Each partner has recorded in the TANGO innovation management log whether they consider themselves the owner of an exploitable result or a contributor to its development. Based on the input provided, two types of ownership have been identified for the exploitable results or components:

i. Single ownership
ii. Joint ownership

5.3.2 Instruments for protecting exploitable results

An essential phase in IP management involves taking the necessary steps and obtaining the appropriate rights to ensure the lawful and effective protection of exploitable results. Establishing the correct legal framework is of paramount importance to safeguard ownership and secure the associated rights.

[1] European Commission: European Innovation Council and SMEs Executive Agency. (2022). *Your guide to intellectual property management in Horizon Europe*. Publications Office of the European Union. https://data.europa.eu/doi/10.2826/409260.

Depending on the nature of each exploitable result, the applicable forms of protection include patents, copyrights, trademarks, and trade secrets. These protection mechanisms have been analyzed in detail in the previous deliverable D8.2.

5.3.3 Management of knowledge and protection of results

The management of knowledge and the protection of results, particularly in relation to access rights, ownership (including how it is established and addressed in cases of joint ownership), the transfer of results, licensing arrangements, exploitation strategies and publication procedures, have been comprehensively addressed in the previous deliverable D8.2. The guiding principles and procedures are outlined in that deliverable to ensure that results are managed effectively, in alignment with legal obligations and the consortium's strategic goals.

To provide greater clarity on how the aforementioned issues regarding licensing and exploitation arrangements are being made and thereby enhance the process of IPR protection, a dedicated template for a Joint Exploitation Agreement (JEA) has been developed and is included in Annex B. A JEA is a formal contractual arrangement entered into by multiple parties, typically partners in a collaborative research or innovation project, with the purpose of regulating the shared use, commercialization, and dissemination of jointly developed results. It ensures that the rights, responsibilities and benefits related to the exploitation of IP or other project outcomes are clearly defined and equitably distributed among the parties involved.

6 Business Models and exploitation paths per KER

6.1 Methodology

The methodology adopted for Task 8.2 in the context of the TANGO project was designed to ensure a structured, result-specific, and partner-informed approach to exploitation planning. The objective was to assess the exploitation potential of all Key Exploitable Results (KERs) and Exploitable Results (ERs) by combining partner input collection with independent desk research, ensuring that each result was linked to a clear exploitation pathway, aligned with relevant market dynamics, and supported by practical implementation strategies.

The process began with the identification and classification of all project results. The full list of KERs and ERs was retrieved directly from Task 8.3 (Intellectual Property Rights Management), ensuring consistency across the TANGO innovation management framework. Once the result inventory was consolidated, Future Needs, as the leader of T8.2, designed a series of structured exploitation templates to collect detailed partner input on each result.

Two tailored exploitation templates were developed: one for KERs and one for ERs. Both templates were composed of specific sections targeting the commercial and technical maturity of the results. These sections included: (i) Technology and Market Watch, focusing on emerging trends, technologies, and companies relevant to each result; (ii) Competition Analysis, requiring partners to list relevant competitors, their target customers, and known product or service pricing; (iii) Market Research and Analysis, aimed at defining the targeted market for each result; and (iv) Value Proposition Analysis, to identify the core innovation and differentiating aspects of each result. In addition, for each result, partners were asked to define a specific Exploitation Plan detailing the intended exploitation pathway (e.g., new product development, service provision, direct industrial use, licensing, joint ventures, consultancy, etc.), the desired business model, and any planned post-project development activities or funding applications. For KERs, the template also included the completion of a full Business Model Canvas (BMC), addressing key partners, activities, customer segments, channels, revenue streams, and cost structures.

Data collection was performed using a multi-step process. The initial request for input was sent to all partners via email, along with the templates. This was followed by an interactive exploitation workshop held during the final TANGO project meeting in Majorca. During this session, particular focus was given to KER17, for which a live completion of the BMC was facilitated in collaboration with attending partners. The session enabled partners to exchange ideas and assess exploitation options collaboratively. Following the workshop, Future Needs conducted targeted one-on-one calls with individual partners to complete and refine the exploitation inputs for all remaining KERs and ERs. This hands-on, result-specific engagement ensured that the exploitation inputs were grounded in each partner's practical perspective and commercial/educational/scientific ambition.

In parallel with the input collection process, Future Needs carried out structured desk research to support and validate the exploitation strategies. This included the identification of relevant markets for each individual ER and KER. Each result was matched to a specific market domain (e.g., Self-Sovereign Identity, Federated Learning, Green Data Centers, MLOps, Cyber-Physical Systems), and a dedicated market analysis was prepared for each, focused specifically on the European context. Each market analysis followed a standardized structure comprising: (i) Segments – detailing which specific market

sub-segments the result addressed and why; (ii) Size and Growth Rate – including quantitative market sizing and CAGR figures; (iii) Trends – highlighting current developments that supported the relevance of the result; (iv) Barriers – identifying potential obstacles to market entry or scalability; and (v) Opportunities – outlining concrete business or policy-driven openings relevant to the result's uptake. All insights in the market analyses were tailored to each result's technological and value proposition characteristics and were based exclusively on credible, sourced market reports.

By integrating direct partner engagement through structured templates and interviews with independent market intelligence, Task 8.2 ensured that exploitation planning in TANGO was both partner-driven and strategically grounded. This combined methodology, depicted in Figure 16 enabled the formulation of realistic, customized exploitation pathways and business models for each of the project's results.

Figure 16: T8.2 Exploitation Methodology

6.2 Exploitation paths for KER2b-Ubiquitous Personal Context Vectors (UPCVs)

6.2.1 Competitor analysis

KER2b operates in the rapidly evolving recommendation engine market, offering privacy-preserving, distributed behavioural prediction capabilities. Based on the partner input, three key competitor categories emerge. First, traditional recommendation engine providers—targeting online media and web shops—offer personalized recommendations, primarily through centralized platforms. Their advantage lies in mature deployment pipelines and wide adoption. However, their privacy practices often conflict with emerging European regulations. Second, advertising ecosystems like Facebook and Google deliver targeted cross-platform advertising based on extensive behavioural profiling. Their reach is massive, but their reliance on invasive data collection creates a regulatory vulnerability. Finally, shopping basket analytics providers focus on retailers, providing user-item clustering and simple analytics. While useful for segmentation, these tools lack the real-time, decentralized recommendation capabilities that KER2b introduces. The core distinction of UPCVs lies in its privacy-first architecture and ability to operate without cloud-based data aggregation, filling a critical compliance and ethical gap not addressed by competitors.

6.2.2 Market Analysis

6.2.2.1 KER2b – Ubiquitous Personal Context Vectors (UPCVs) Recommendation Engine Market Segments

KER2b directly aligns with the **content-based and context-aware recommendation engine segments** of the European recommendation engine market. The solution's ability to locally evaluate user preferences through volatile random numbers without persistent tracking positions it within **privacy-focused mobile recommender tools**, especially in **B2C services** like digital commerce, smart city ecosystems, and local service platforms. According to KBV Research, collaborative filtering and content-based filtering dominate the European market, with increasing demand for **hybrid and contextual systems**—the very area UPCVs operate in[2]. Additionally, MarketResearch.com notes that **web-based and mobile platform,** that refer to the cloud market segment depicted in Figure 17, are driving innovation in Europe, with retail, media, and entertainment sectors being top adopters[3].

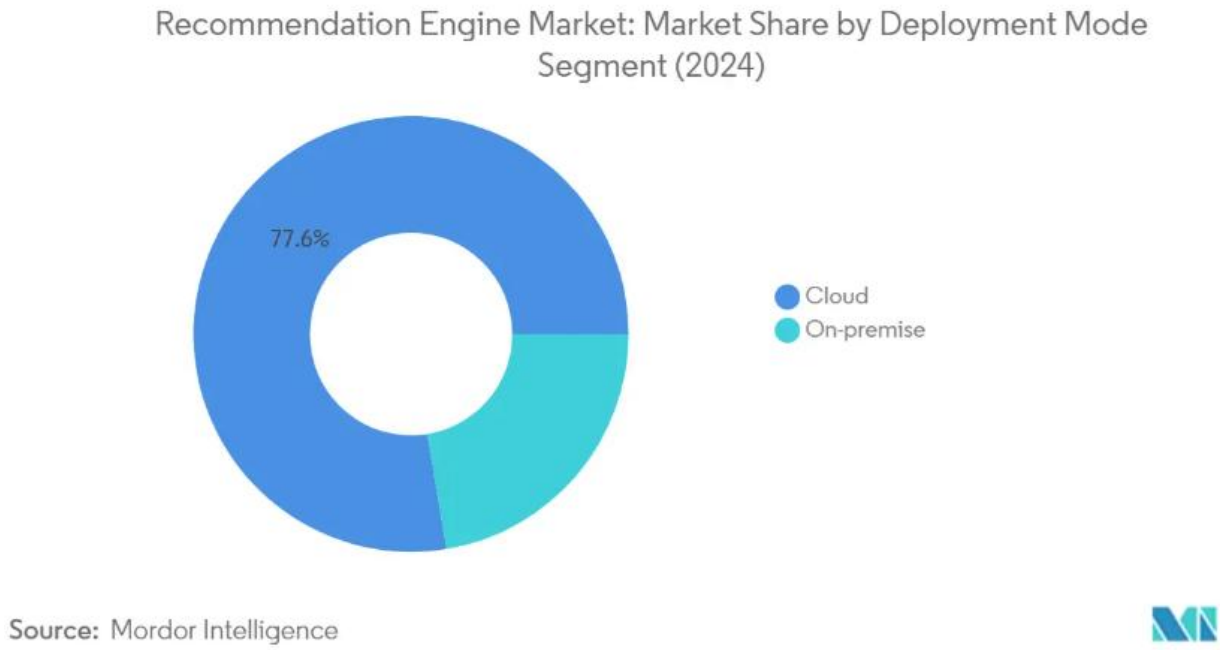


Figure 17: KER2b Recommendation Engine Market segments (source: Mordor Intelligence)

Size and Growth Rate

The European recommendation engine market is undergoing rapid expansion. As shown in Figure 18, Grand View Research reports that the global recommendation engine market size reached **USD 2.12**

[2] KBV Research
[3] MarketResearch.com

billion in 2022, and is projected to grow at a **compound annual growth rate (CAGR) of 36.4%** from 2023 to 2030, with Europe contributing significantly due to widespread digital commerce and AI adoption[4]. KBV Research forecasts that the **Europe recommendation engine market** alone will exceed **USD 1.2 billion by 2028**, driven by increasing personalization demand in sectors such as e-commerce, travel, and local services[5]. This high growth trajectory confirms the strategic relevance of UPCVs, especially as a privacy-aware engine in edge devices.

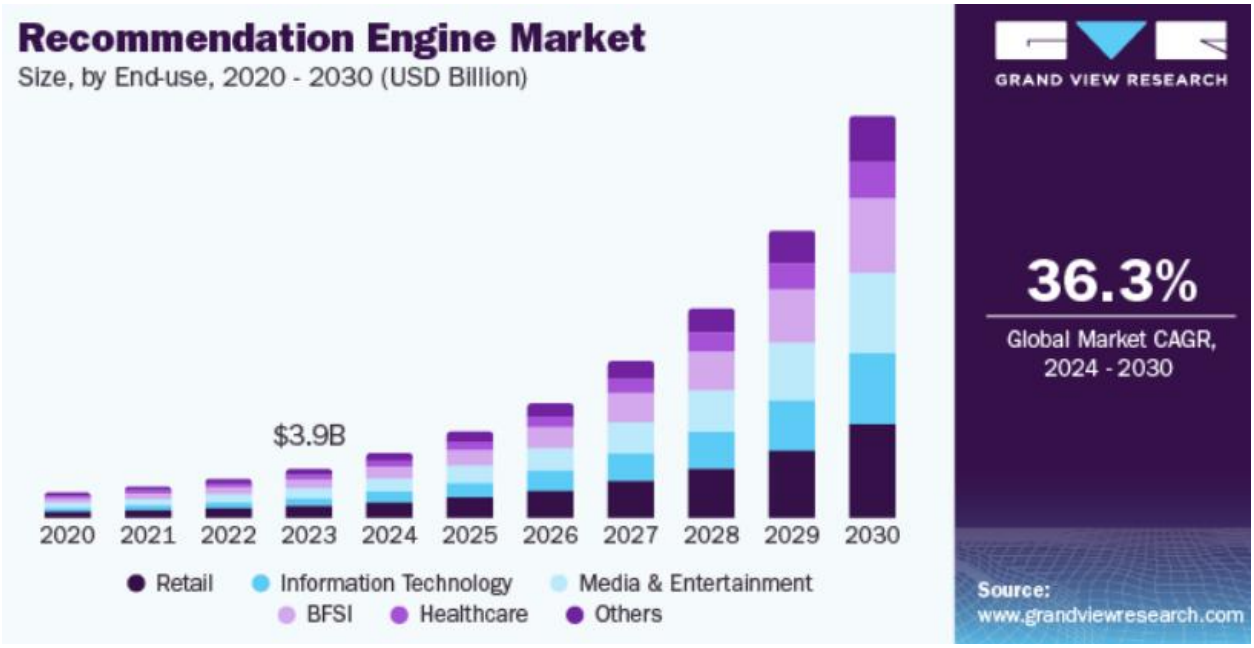


Figure 18: KER2b Recommendation Engine Market size and growth rate (source: Grand View Research)

Trends

Privacy-preserving personalization is one of the most prominent trends fueling innovation in the recommendation space. Precedence Research emphasizes that businesses across Europe are seeking **decentralized, explainable, and compliant recommendation engines** that align with GDPR and user-consent frameworks[6]. KER2b's approach—distributing recommendation logic to mobile devices and avoiding user profiling on the cloud—aligns with this shift. Furthermore, "Markets and Markets" highlights the rise of **context-aware and real-time recommendations**, particularly for mobile users in travel, retail, and content streaming, reinforcing the relevance of UPCVs' mobile-first, session-based logic[7]. Finally, IndustryARC identifies AI-enhanced personalization and **micro-segmentation in**

[4] Grand View Research
[5] KBV Research
[6] Precedence Research
[7] "Markets and Markets"

customer journeys as trends boosting demand for tools like KER2b that focus on engagement and loyalty over persistent tracking[8].

Barriers

Despite strong growth, barriers persist. Mordor Intelligence highlights that **lack of interoperability with legacy systems**, high computational requirements, and **data privacy concerns** are major hurdles in deploying next-gen recommendation engines, particularly in SMEs[9]. Although UPCVs overcome privacy issues, their **novelty and decentralization** may pose a barrier in terms of **market education and integration complexity**. Grand View Research also notes that **over-personalization and recommendation fatigue** could reduce long-term user trust, which decentralized systems must carefully navigate[10].

Opportunities

The European market presents clear opportunities for UPCVs. As per KBV Research, sectors such as **local marketplaces, sustainable commerce, and digital public services** are seeking **trust-centric recommendation tools** that enhance user experience without infringing on privacy[11]. Mordor Intelligence further identifies an opportunity in **niche recommender tools** for hyper-local ecosystems and community-driven platforms, where shared user pools can benefit from personalized suggestions without centralized tracking[12]. Given its edge-based deployment model, KER2b is also well-positioned to support **e-commerce personalization in regulated sectors**, such as health and finance, where data minimization is mandatory.

6.2.3 Value proposition analysis

The key value proposition of KER2b lies in enabling personalized, privacy-preserving recommendations through decentralized technology. Rather than relying on persistent tracking and cloud-based user profiling, UPCVs offer a symmetric approach that operates on both user and vendor sides. By exchanging volatile random numbers (VRNs), the system identifies preference patterns without storing personal data. This design supports compliance with GDPR and anticipates stricter privacy frameworks. From a user's perspective, UPCVs improve access to relevant goods and services, enhancing experience and loyalty. For vendors, it offers a transparent and ethical way to increase conversions without compromising user trust. KER2b's ability to perform mobile, session-based inference makes it well-suited for real-time use cases in retail, travel, or local digital ecosystems.

6.2.4 Barriers, obstacles and analysis of the standards and regulation

The primary barrier currently facing KER2b is the lack of market visibility and insufficient advertising, which has hindered customer acquisition and ecosystem engagement. This is a common hurdle for privacy-centric technologies that operate differently than mainstream AI tools. Additionally, the novel decentralized architecture of UPCVs may require integration effort and user education. According to Grand View Research, emerging recommendation engines often face friction in deployment due to

[8] IndustryARC
[9] Mordor Intelligence
[10] Grand View Research
[11] KBV Research
[12] Mordor Intelligence

interoperability challenges with legacy platforms. In terms of regulation, however, UPCVs are well-positioned: GDPR and the Digital Services Act in the EU are increasingly emphasizing data minimization and consent-based personalization. As such, while the tech faces outreach challenges, its compliance advantage aligns it with upcoming standards in digital services.

6.2.5 Technology and market watch

An ongoing trend in the European market, as declared by VTT and portrayed in Table 8, is the **tightening of privacy regulations**. For instance, Facebook and Google face increasing scrutiny and legal challenges over cross-platform data collection, as noted in recent EU policy actions. In this context, the UPCV approach—which enables personalization without data centralization—presents a viable and future-proof alternative. The trend toward **federated and privacy-aware recommender systems** is accelerating, creating a receptive environment for KER2b. A commercial proof-of-concept could target a localized service platform that seeks personalization without compromising compliance. Additionally, recent developments in **zero-knowledge proofs and decentralized identity** may further strengthen KER2b's technical foundation and relevance in both public and private sectors.

Table 8: KER2b Technology and Market watch

Item	Description	Possible Impact	Actions	Link
Emerging trend or development	EU restrictions for Facebook et al. to collect profiling data across services, breaching users' privacy.	UBEM (UPCV) approach is designed to enable personalised services without privacy concerns.	Find application(s) that would be used as a commercial PoC for the technology.	https://www.ibc.org/download?ac=10484

6.2.6 Business Model Canvas

Business Model Canvas				
Key Partners	**Key Activities**	**Value Propositions**	**Customer Relati**	**Customer Segments**
Digital ecosystem builders (e.g., Telecommunication companies like Telefónica), mobile service providers, open-source community, data privacy advocates, standards bodies	Service tailoring for specific use cases; integration into third-party platforms; development and maintenance of the recommendation engine	Make it easy for consumers to find goods and services that interest them, increasing sales and/or customer loyalty.	B2B service agreements; tailored onboarding for platform providers; support for open-source contributors; workshops for integrators	Business networks; online marketplaces; local service platforms; smart city data intermediaries; mobile app developers seeking GDPR-compliant personalization.
	Key Resources		**Channels**	

	Development team; deployment infrastructure; privacy framework (VRN engine); Web App delivery framework.		Direct sales (custom integration); collaborative EU projects; open-source publication and community; digital platforms like GitHub or Docker Hub	

Cost Structure	**Revenue Streams**
Development and support resources; hosting and distribution costs; integration costs per deployment; promotional and dissemination efforts	Yearly service provision payments; consulting on GDPR-compliant personalization; support contracts for open-source deployments; potential licensing of specialized modules.

6.2.7 Exploitation Pathway

The exploitation of KER2b will follow a B2B service model, focusing on tailoring and applying the recommender system to specific customer use cases. Although there are no clients at this point, Telefónica has been identified as a potential adopter. The solution is currently proprietary under patents EP2678815, US10423610, US9882790, FI126426, US11695838 and EP3583763 but is expected to be made open-source, promoting wider adoption, yet the value-added services—custom configuration, integration, and support—will be monetized through yearly service contracts. The result will not be exploited through further Horizon Europe funding unless the partner is explicitly invited into a relevant consortium. This pragmatic approach ensures sustainability without reliance on future public funding. The exploitation strategy is particularly suited for ecosystems where user trust and data compliance are paramount, aligning with the ongoing trend toward privacy-enhanced user experiences.

6.3 Exploitation paths for KER3a-Confidentiality and Privacy by Design: PEP and Sticky Policies

6.3.1 Competitor analysis

KER3a introduces a robust security solution focused on enhancing data confidentiality and privacy through the integration of **Sticky Policies** and **Policy Enforcement Points (PEPs)**, using **Ciphertext-Policy Attribute-Based Encryption (CP-ABE)**. This distinguishes it from traditional access control models by allowing policies to be embedded directly within the encrypted data and enforced dynamically throughout the data lifecycle.

In terms of competitors, three main categories were identified. The first includes **traditional access control solutions**, typically based on Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC). These systems are widespread across industries and offer basic mechanisms but

generally lack the policy embedding capabilities and dynamic enforcement enabled by KER3a's sticky policies and PEP architecture. The second competitor type involves **Federated Identity Management (FIM)** systems, such as single sign-on (SSO) platforms. These solutions focus on identity federation rather than fine-grained access policy enforcement and are unable to manage policy persistence throughout the data lifecycle. Lastly, **Access Control Lists (ACLs)** provide static, object-level permissions, which do not adapt well to dynamic environments and lack integration with modern cryptographic enforcement tools such as CP-ABE. All three competitor types address baseline access needs but do not provide the **granular, user-controlled, and cryptographically enforced policy framework** that KER3a delivers. This sets KER3a apart, particularly in contexts where **regulatory compliance, user trust, and lifecycle-level policy control** are essential.

6.3.2 Market Analysis

A formal market analysis for KER3a was not conducted as UMU does not foresee a commercial exploitation strategy in the traditional sense. Instead, the exploitation will be embedded within academic, research, and public sector activities. However, the security and data privacy domains in which KER3a operates continue to grow, particularly in response to evolving regulatory landscapes like the GDPR and increasing demand for data sovereignty in distributed systems and data spaces. The relevance of these domains reinforces the importance and potential impact of KER3a in public-private partnerships and non-commercial deployments.

6.3.3 Value proposition analysis

KER3a offers a **cutting-edge privacy-preserving security framework** that enables fine-grained, attribute-based access control enforced throughout the entire data lifecycle. By embedding sticky policies directly into the data using **CP-ABE**, the asset empowers users and data owners to dictate precisely how their data is accessed and used. The system leverages a modular architecture comprising **PEPs, PDPs, and the standardized XACML framework** to ensure continuous enforcement of these policies, even in distributed environments.

This innovation provides three clear benefits: (1) **Enhanced Data Protection**, through robust encryption and access mechanisms; (2) **Regulatory Compliance**, particularly with GDPR, thanks to its consent-aware and policy-driven controls; and (3) **User Trust**, as the data remains protected in both storage and transit, and access is always governed by owner-defined rules. Through this architecture, KER3a equips organizations to handle sensitive data with greater confidence and to meet regulatory expectations more efficiently.

6.3.4 Barriers, obstacles and analysis of the standards and regulation

While KER3a provides a technically advanced solution, it does face several challenges. First, **integration complexity** is a major obstacle. Implementing CP-ABE alongside PDP and PEP modules requires in-depth expertise in cryptography, system architecture, and access control, making deployment in existing environments technically demanding. Second, **policy complexity and management** represent another hurdle. Designing effective and compliant policies requires a clear understanding of both business needs and legal obligations. Ensuring their consistent enforcement across distributed endpoints can be especially challenging in real-world systems. Third, **security risks**, including insider

threats and unauthorized data access, remain ever-present and require robust operational safeguards beyond the scope of static enforcement alone.

From a regulatory standpoint, KER3a is fully aligned with the **GDPR**, offering built-in support for consent management and policy-based control of personal data. It is also compliant with technical standards such as **XACML** for policy enforcement and **RFC 7519 (JWT)** for secure token-based identity claims. Together, these alignments provide a strong regulatory and standards foundation for both research and institutional deployments.

6.3.5 Technology and market watch

The technological environment for privacy-preserving access control is shifting rapidly in favour of solutions like KER3a. One notable development is the widespread **adoption of Zero Trust architectures**, which require verification at every layer of system access. This model greatly benefits from the integration of PDP/PEP modules that enforce strict, contextual access policies, directly aligning with KER3a's architecture.

There is also increasing **interest from real-world clients in ABE-based technologies**, particularly for ensuring **GDPR compliance**. These organizations recognize the need for dynamic, user-controlled access solutions, and are actively exploring pilot implementations. This creates new opportunities for **client workshops and training programs**, where UMU can transfer knowledge and build early adoption pathways. Finally, by enhancing **granular control over access and usage**, KER3a provides organizations with a clear advantage in mitigating legal risk and improving customer trust—factors that are growing in importance across both public and private sectors.

Table 9: KER3a Technology and Market watch

Item	Description	Possible Impact	Actions	Link
New market opportunities	Several actual client projects that know about ABE technology and are interested in compliance with the EU General Data Protection Regulation (GDPR) on data protection and privacy.	High	Client awareness workshops	N/A
Emerging trend or development	Moving towards zero trust security models, where verification is required for every access request enhances the need for robust PDP/PEP implementations to enforce stringent access controls.	Positive	N/A	N/A
Impact of new technology adoption	Regulatory Compliance: organizations adopting Confidentiality and Privacy by Design technologies find it easier to comply with GDPR, and other privacy regulations, reducing legal risks and enhancing customer trust by ensuring consistent and controlled access and usage control (granular control)	Positive	N/A	N/A

6.3.6 Business Model Canvas

<table>
<tr><th colspan="5">Business Model Canvas</th></tr>
<tr><th>Key Partners</th><th>Key Activities</th><th>Value Propositions</th><th>Customer Relat</th><th>Customer Segments</th></tr>
<tr>
<td rowspan="3">Research Institutions & Technology Partners: University of Murcia, EVIDEN, with a focus on technical co-development and product evolution.
Regulatory Bodies: IDSA, Gaia-X, and DSBA to ensure regulatory alignment and compliance with EU data sovereignty frameworks.
Motivation for Partnership: Increase the technical maturity of the access control solution and reduce maintenance costs through collaborative research and regulatory oversight.</td>
<td>Research & Development (R&D) for advancing the sticky policy and CP-ABE engine.
Compliance Monitoring to ensure continued alignment with evolving standards such as GDPR and eIDAS.
Product Development, including implementation, modularization, and integration of the PDP/PEP components into privacy-enabling connectors.</td>
<td rowspan="3">Security solution designed to enhance data confidentiality and privacy by embedding sticky policies with data, leveraging Ciphertext-Policy Attribute-Based Encryption (CP-ABE), and utilizing Policy Decision Point (PDP) and Policy Enforcement Point (PEP) modules for robust policy decision and enforcement.
It provides enhanced security, regulatory compliance and user trust.</td>
<td>Customer Support for onboarding and troubleshooting related to policy integration and privacy enforcement.
Regular Engagement: Continuous communication on system updates, security patches, and privacy-preserving improvements.</td>
<td rowspan="3">Governmental Organizations that require fine-grained, context-aware access control and privacy-by-design in their data systems.
Business Enterprises, especially those in regulated industries seeking robust data protection.
European and National Research Agencies integrating privacy enablers in data-sharing frameworks.</td>
</tr>
<tr><th>Key Resources</th><th>Channels</th></tr>
<tr>
<td>Technical Experts in cryptography, privacy engineering, and software development.
Regulatory Knowledge to ensure legal compliance with GDPR, XACML, and related data privacy laws.</td>
<td>Outreach through Conferences and Webinars, especially in academic, policy, and Gaia-X-related venues.
Community Engagement via open-source repositories, targeted demos, and</td>
</tr>
</table>

			standardization groups.	

Cost Structure	Revenue Streams
R&D Expenses including ongoing development of encryption and enforcement modules. **Personnel Costs**, particularly technical staff and compliance experts supporting maintenance and implementation.	**Open-source Release** of the core components to foster adoption and standardization. **Training Programs** and workshops for system integrators and industry actors focused on privacy and access control in dataspaces.

6.3.7 Exploitation Pathway

The exploitation pathway for KER3a is **non-commercial** but strategically targeted. UMU intends to embed the **CP-ABE sticky-policy engine and the PEP/PDP privacy modules** into its existing research activities and EOSC-related projects. All outputs, including source code and design specifications, will be made available under **open-access licenses**. Knowledge transfer will be facilitated through **specialized training sessions and technical workshops**, enabling broader adoption of the approach across sectors dealing with sensitive data.

Short- and mid-term actions include **publishing reference implementations as open-source**, integrating them into university teaching at bachelor's and master's levels, and validating the components through ongoing EOSC and national projects in oceanography and food domains. Over the long term, UMU aims to **license these technologies to a wider network of industrial and public stakeholders**, expanding their impact across Europe. This strategy is not reliant on new Horizon Europe funding, but UMU remains open to participation in relevant future projects, especially those focused on **privacy-enabled data spaces**. Through this hybrid academic-industrial pathway, KER3a is expected to significantly influence the evolution of secure, compliant data infrastructures across multiple sectors.

6.4 Exploitation paths for KER7-Seamless onboarding for users

6.4.1 Competitor analysis

KER7 competes in the increasingly dynamic digital identity verification market, specifically targeting seamless onboarding services. Among its primary competitors is Mastercard, which offers identity verification solutions to sectors such as financial services, retail, e-commerce, gaming, and e-

government. While Mastercard benefits from wide-scale recognition and a diversified client base, its services are typically proprietary and not open-source, limiting flexibility for small-scale adopters. Another prominent competitor is Onfido Limited, which also targets highly regulated sectors but requires a coordinating central entity to manage user verification flows. Onfido offers biometric verification, document checking, and liveness detection—features that overlap partially with KER7's offering. Finally, Acuant provides a comparable solution aimed at organizations seeking digital onboarding capabilities, with pricing structures and integration models that vary per client setup. However, unlike KER7, these competitors are not specifically designed to support Self-Sovereign Identity (SSI) frameworks nor do they prioritize open-source delivery. This gives KER7 a unique value proposition in addressing cost reduction, regulatory compliance, and privacy transparency through a highly modular and customizable service model.

6.4.2 Market Analysis

KER7 ("Seamless Onboarding for Users") in the European Digital Identity Verification Market Segments

KER7 directly addresses the *solution* segment of the European digital identity verification market, which is the largest revenue contributor as of 2023, according to Grand View Research[13]. Specifically, this result aligns with the biometric authentication and multi-factor authentication sub-segments, as it enables remote user onboarding with a four-step verification process compliant with the eIDAS High Level of Assurance. The solution is relevant for end-user industries such as banking and financial services (BFSI), e-commerce and retail, and government digital services, portrayed in Figure 19, which are among the top segments adopting digital identity verification, according to both Fortune Business Insights and Zion Market Research[14].

[13] https://www.grandviewresearch.com/horizon/outlook/identity-verification-market/europe
[14] https://www.fortunebusinessinsights.com/identity-verification-market-106468; https://www.zionmarketresearch.com/report/digital-identity-verification-market

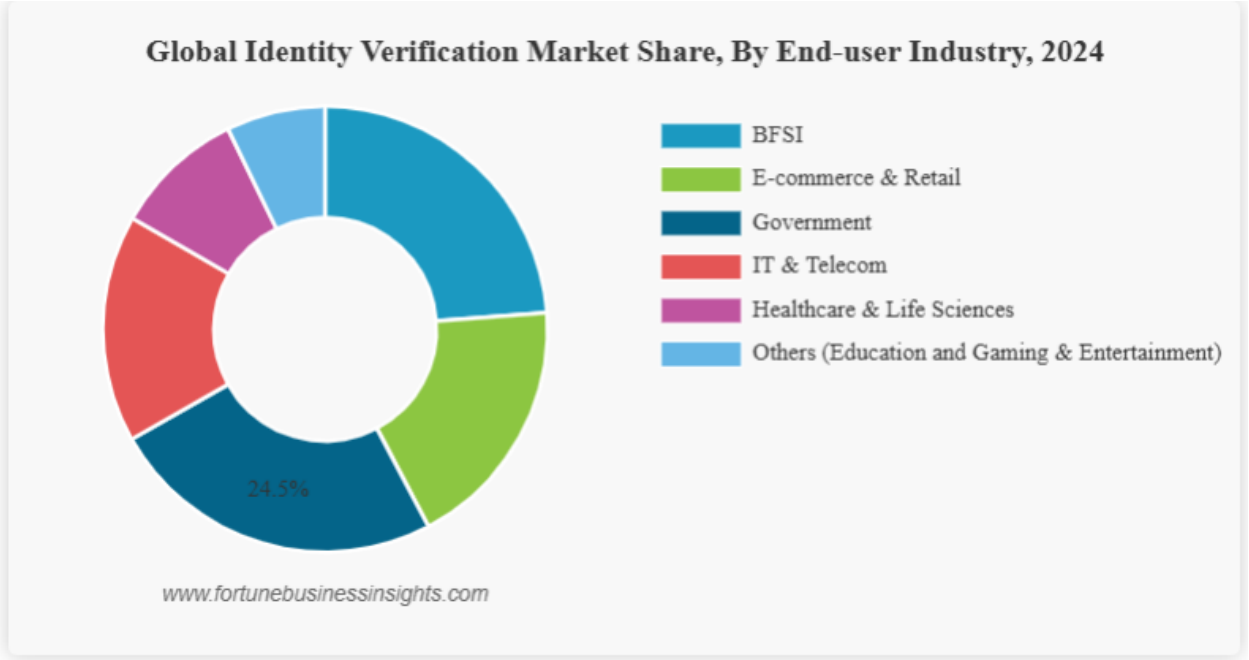


Figure 19: KER7 Recommendation Digital Identity Verification segments (source: Fortune Business Insights)

Size and Growth Rate

The European digital identity verification market is experiencing robust growth as shown in Figure 20, driven by strict data protection laws and accelerating digitization. According to Grand View Research, the market generated revenue of USD 2,496.3 million in 2023 and is projected to grow at a CAGR of 17.9%, reaching USD 7,913.8 million by 2030[15]. Inkwood Research corroborates this trend, projecting the market to reach approximately USD 10,980 million by 2032 with a CAGR of 15.65% from 2023 to 2032, emphasizing the sustained momentum of identity verification needs across European economies[16]. This high growth is supported by increasing digital service adoption and regulatory mandates such as eIDAS, which directly anchor the relevance of seamless onboarding solutions like KER7.

[15] https://www.grandviewresearch.com/horizon/outlook/identity-verification-market/europe
[16] https://www.inkwoodresearch.com/reports/europe-identity-verification-market/

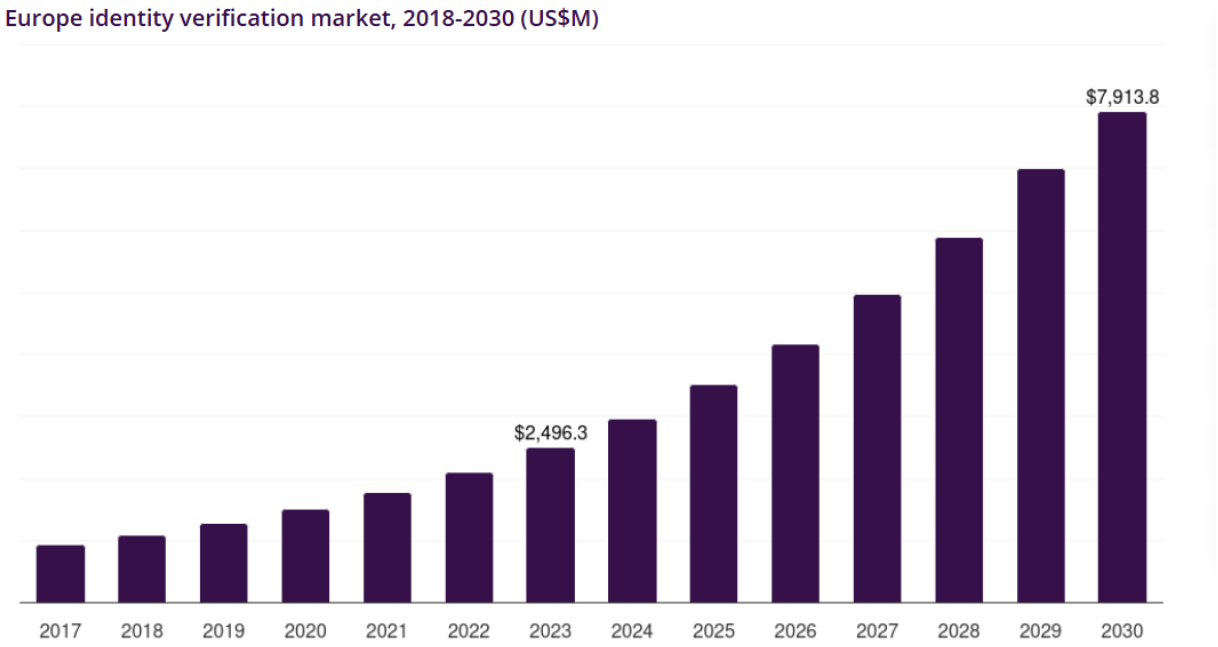


Figure 20: KER7 Digital Identity Verification Market size and growth rate (source: Grand View Research)

Trends

A key trend supporting KER7 is the surge in remote onboarding and the rapid adoption of cloud-based, AI-powered identity verification solutions. Fortune Business Insights highlights that the demand for biometric and AI-driven verification is booming due to the sophistication of cyber threats, including deepfakes and synthetic identity fraud, which drive organizations to strengthen their onboarding checks[17]. Additionally, KBV Research notes that biometric solutions are becoming mainstream due to their security and user experience advantages, aligning perfectly with KER7's promise to make remote onboarding frictionless yet compliant with the strictest assurance levels[18]. In Europe, the European Commission's push for a unified European Digital Identity Wallet will further accelerate adoption of trusted digital onboarding technologies[19].

Barriers

Despite robust market growth, barriers exist that could impact KER7's adoption speed. According to Fortune Business Insights, high implementation costs pose a challenge for small and medium-sized enterprises, which may hesitate to adopt advanced onboarding SDKs without clear ROI[20]. Furthermore, Inkwood Research points out the lack of technical expertise and the need for security awareness and

[17] https://www.fortunebusinessinsights.com/identity-verification-market-106468
[18] https://www.kbvresearch.com/europe-digital-identity-solutions-market/
[19] https://www.kbvresearch.com/europe-digital-identity-solutions-market/
[20] https://www.kbvresearch.com/europe-digital-identity-solutions-market/

training as limitations in Europe's identity verification market, which could hinder the effective deployment of sophisticated onboarding tools in some regions[21]. Moreover, Zion Market Research warns that data breaches and interoperability issues can undermine trust in digital identity solutions if providers fail to maintain seamless and secure integrations[22].

Opportunities

Despite these challenges, KER7 is strategically positioned to capitalize on multiple market opportunities. Europe's strict regulatory environment, including GDPR and eIDAS, makes robust and seamless onboarding a compliance necessity for banks, e-commerce platforms, and governments alike.[23] The increasing prevalence of remote customer interactions, especially in BFSI and public e-services, means demand for remote onboarding tools with high assurance levels is rising rapidly. Furthermore, the European Commission's plans for an interoperable Digital Identity Wallet open the door for KER7's SDK to become an essential integration point for businesses wanting to leverage the EU-wide digital identity infrastructure[24]. With France projected to register the highest growth among European countries, and Germany's government-led digital ID initiatives, market readiness for seamless, secure onboarding solutions is strong[25].

6.4.3 Value proposition analysis

KER7 is designed to enhance the onboarding experience for users while simultaneously reducing costs for service providers. It achieves this through a privacy-first approach that ensures transparency in cloud-based data processing and alignment with the eIDAS High Level of Assurance standards. Delivered via a four-step verification SDK, the solution allows users to remotely verify their identities without physical presence, enabling smooth integration of existing identity documents such as passports into a Self-Sovereign Identity (SSI) ecosystem. The value proposition is further strengthened by its open-source nature, which encourages wide adoption by allowing organizations to tailor and deploy the technology without proprietary restrictions. In practice, the technology helps customers in four concrete ways: (a) reducing the cost of implementing secure onboarding, (b) preserving user privacy, (c) offering customizable open-source integration options, and (d) ensuring compliance with the highest levels of identity assurance. This makes KER7 an appealing option for a wide range of industries, including financial services, e-commerce, gaming, and public administration.

6.4.4 Barriers, obstacles and analysis of the standards and regulation

Despite its strong value proposition, KER7 faces several key barriers to adoption. The market is already populated by strong commercial players such as Mastercard and Onfido that benefit from established customer bases and brand trust. While few competitors focus explicitly on SSI, their broad reach and financial backing present a commercial challenge. On the technical front, KER7 must address sophisticated attack vectors including deepfake-based spoofing and 3D mask presentation. These advanced fraud methods pose real threats in digital onboarding scenarios and necessitate continuous technological evolution. Regarding compliance, KER7 is designed to meet relevant regulatory

[21] https://www.inkwoodresearch.com/reports/europe-identity-verification-market/
[22] https://www.zionmarketresearch.com/report/digital-identity-verification-market
[23] https://www.fortunebusinessinsights.com/identity-verification-market-106468
[24] https://www.kbvresearch.com/europe-digital-identity-solutions-market/
[25] https://www.grandviewresearch.com/horizon/outlook/identity-verification-market/europe

frameworks, including the General Data Protection Regulation (GDPR), eIDAS, and industry-specific standards like ISO 27001 and ISO 9001, ensuring a solid foundation for trustworthy adoption across regions with strict data protection laws.

6.4.5 Technology and market watch

Based on QBE's input displayed in Table 10, the current market trend of digitizing public and private sector services is increasing the demand for robust Know-Your-Customer (KYC) and onboarding tools. This drives a shift towards solutions that address identity fraud while also enhancing customer experience. KER7 responds to this trend with its secure, four-step verification approach. A notable strength is its positioning as the first open-source solution combining remote identity verification with support for SSI and compliance with eIDAS. The growing emphasis on digital wallets and interoperable ID solutions in the EU adds to its relevance. To capitalize on this momentum, QBE is taking proactive steps to improve reliability across varied real-world conditions, collecting behavioural data, fine-tuning its fraud detection models, and gathering user feedback. Furthermore, QBE plans to grow an active community around the open-source version by engaging developers, organizing educational programs, publishing documentation, and supporting community events, ensuring both technical advancement and market uptake.

Table 10: KER7 Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date
Emerging trend or development	Digitalisation services drive stronger KYC to mitigate potential identity fraud	Increased customer experience, enhanced security, prevention of unauthorized access, and address specific challenges such as identity fraud and financial fraud while adhering to relevant regulations.	Continue focusing on enhancing the reliability of inference results in various conditions and use cases, collecting additional behavioural data, obtaining user feedback, fine-tuning the component based on specific use cases, and training improved models to prevent fraud and malicious activities	Ongoing
Hot startups and innovators	It's the first open-source solution that enables remote identity verification supporting SSI and eIDAS compliance	May witness rapid adoption among these entities looking for modern and efficient identity verification solutions. This will foster the growth of a collaborative ecosystem that may attract a community of developers, businesses, and experts who are passionate about	Deploy focused outreach efforts, developer engagement strategies, collaborative open-source initiatives, consistent updates, educational programs, support services, partnerships, feedback mechanisms, community events, and thorough documentation to promote adoption and cultivate a flourishing ecosystem for the open-source identity verification solution.	Ongoing

Item	Description	Possible Impact	Actions	Effective Date
		secure identity verification		

6.4.6 Business Model Canvas

Business Model Canvas				
Key Partners	**Key Activities**	**Value Propositions**	**Customer Relationships**	**Customer Segments**
Identity Providers, **Regulatory Compliance Services**, and **API Providers** for secure and scalable integrations. **Financial Institutions**, **Government Agencies**, and **Mobile Network Operators** as both stakeholders and adopters of the onboarding SDK. **Cybersecurity Firms**, **UX Designers**, and **Legal Experts** to ensure security, usability, and compliance. **Education Providers** and **CRM Platforms** for ecosystem	**Provision of Seamless Onboarding Services**, including document-based identity verification into SSI frameworks. **Security Model Maintenance**, ensuring continued compliance with eIDAS and fraud-resilience against threats like deepfakes. **Continuous Development** of open-source SDK, user interface refinement, and verification model updates.	Security solution designed to enhance data confidentiality and privacy by embedding sticky policies with data, leveraging Ciphertext-Policy Attribute-Based Encryption (CP-ABE), and utilizing Policy Decision Point (PDP) and Policy Enforcement Point (PEP) modules for robust policy decision and enforcement. It provides enhanced security, regulatory compliance and user trust.	**Responsive Customer Support** with rapid feedback handling and onboarding assistance. **Collaborative Engagement** to guide custom implementation and gather insights for product improvement. **Community Interaction** via online platforms and open-source discussions to build trust and transparency.	**Startups and SMEs** needing affordable, scalable onboarding tools. **Enterprises** requiring secure, customizable, and compliant integration of identity solutions. **Regulated Industries** (e.g., finance, e-gov, healthcare) with strict identity verification and privacy mandates. **Open-source Communities and Developers** interested in modular and privacy-preserving
	Key Resources		**Channels**	

engagement and user outreach.	**Technical Team** for software development, biometric verification integration, and SDK management. **Privacy and Regulatory Experts** ensuring alignment with GDPR, eIDAS, and ISO standards. **Community Infrastructure**, including documentation repositories and support platforms.		**Dedicated Forums, Chat Groups, and Email Support** for real-time interaction. **Newsletters and Webinars** to disseminate updates and demonstrate compliance capabilities. **Public Documentation Repository** providing open access to technical material and integration guides.	onboarding components.

Cost Structure	Revenue Streams
Personnel Costs (developers, support staff, privacy/legal experts). **Infrastructure Costs** related to cloud hosting, open-source repository maintenance, and training portals.	**Subscription Models** offering premium support, feature enhancements, and frequent updates. **Consultancy Services** tailored to specific client integration needs and regulatory contexts. **Training and Certification Programs** enabling developers and clients to gain expertise in deploying and maintaining the open-source onboarding solution.

6.4.7 Exploitation Pathway

KER7's exploitation pathway centres around delivering onboarding capabilities as a technology-enabled service. Specifically, the result will be provided as an open-source solution that allows users to onboard existing identity credentials—such as passports—into an SSI-compliant digital identity system. This modular approach enables organizations to adopt and tailor the technology while reducing the costs of compliance and enhancing security. Though the base technology is open source, QBE's business model emphasizes monetization through complementary services such as consultancy for integration, subscription-based premium features and support, and training programs aimed at developers and businesses. The exploitation plan is divided into three distinct phases: (1) development and validation of the SDK, ensuring security, usability, and compliance; (2) market deployment through open-source

release while simultaneously launching revenue-generating services; and (3) continuous customer engagement with iterative development based on user feedback. This structured roadmap allows QBE to maximize both societal impact and business sustainability while reinforcing the regulatory readiness of its technology.

6.5 Exploitation paths for KER8-User continuous behavioural authentication

6.5.1 Competitor analysis

KER8 targets the behavioural biometric authentication domain, where several advanced players are already active. Notable competitors include **BioCatch**, which focuses on real-time fraud detection using cloud-based behavioural analysis (e.g., mouse movements, typing patterns) tailored for banks, fintechs, e-commerce platforms, and telcos. BioCatch stands out prominently with its substantial funding rounds totalling $250M across Seed, Series A, B, and C rounds. **BehavioSec** offers device-interaction-based behavioural biometrics (such as typing speed, touch pressure) for banks and gaming firms. This differentiates it significantly from competitors relying on more static or session-based behavioural verification BehavioSec, acquired by LexisNexis, has also garnered attention, having secured multiple rounds of funding (Seed, Series A, and B) amounting to $25M. Another competitor identified by QBE is **FICO**. This competitor integrates machine learning for behavioural and transactional fraud detection, serving large financial and insurance institutions. However, unlike KER8, these solutions typically require more active user interaction and are not designed as continuously adaptive systems across devices. Shifting focus to the biometric authentication sector, CallSign has demonstrated a formidable presence, having secured funding across Preseed, Angel, Seed, and Series A rounds, amassing a total of $38.8M. Additionally, AimBrain, recently acquired by BioCatch, has made notable strides with its Seed and Series A rounds, accumulating £4.4M in funding.

These competitors collectively contribute to the dynamic landscape of continuous behavioural authentication and biometric authentication, each vying for market share and technological advancement. Nevertheless, KER8 stands out due to its unique value that stems from its non-invasive, continuous monitoring that includes over 14 behavioural traits and its positioning as a **primary authentication mechanism** that eliminates passwords and supports **Self-Sovereign Identity (SSI)** principles.

6.5.2 Market analysis

AI in Cybersecurity market analysis for KER8 (User Continuous Behavioural Authentication) and KER9 (Device Continuous Behavioural Authentication)

Segments

KER8 and KER9 fall within the *endpoint security* and *fraud detection/anti-fraud* segments of the European AI in Cybersecurity market. They deliver advanced behavioural authentication capabilities that reinforce endpoint protection and strengthen zero trust architectures by continuously verifying user and device legitimacy. According to Grand View Research, the network and endpoint security types collectively hold a substantial share of the AI in Cybersecurity market in Europe, as shown in Figure 21, with fraud detection being a critical application driving adoption in sectors such as BFSI, retail, and

government[26]. Moreover, these KERs leverage machine learning and context-aware computing, aligning with dominant AI technologies in the European cybersecurity landscape, as highlighted by KBV Research[27].

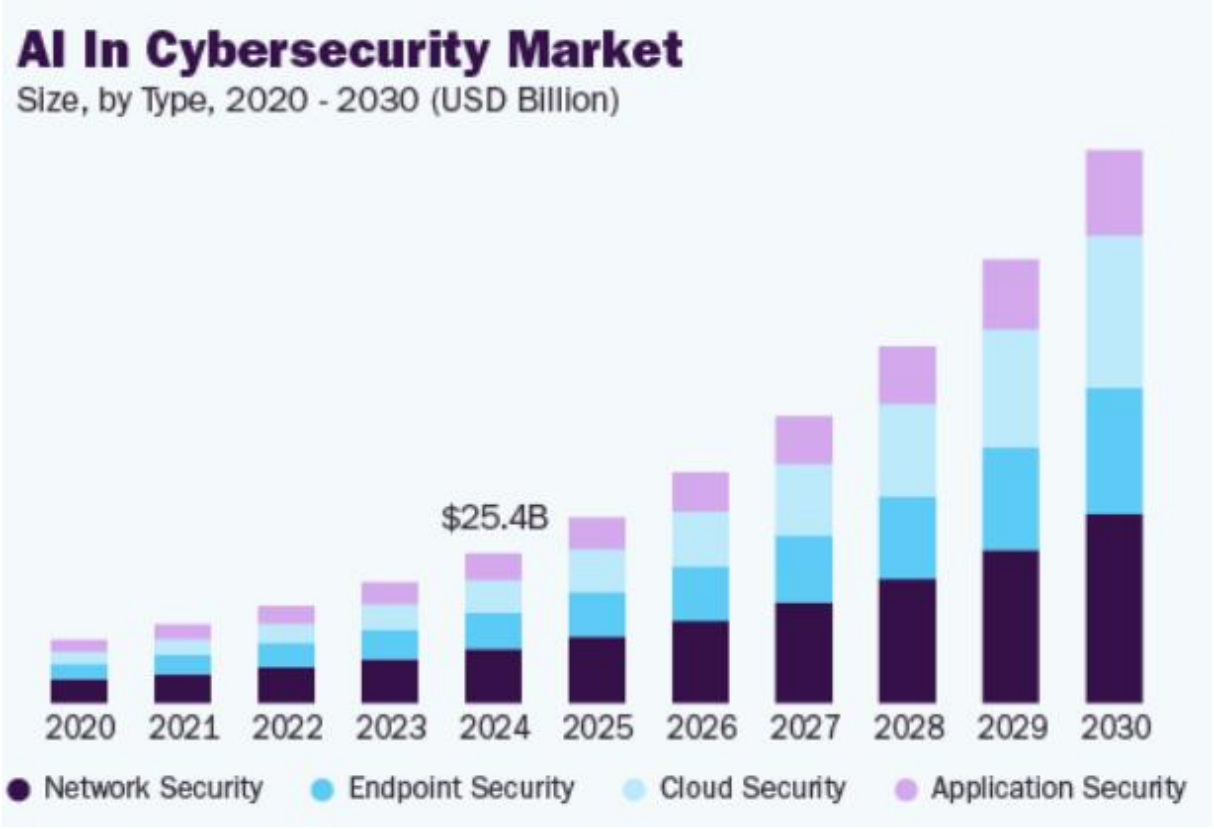


Figure 21: KER8 and KER9 AI in Cybersecurity market segments (source: Grand View Research)

Size and Growth Rate

The European AI in Cybersecurity market is on a sharp upward trajectory, as depicted in Figure 22, demonstrating significant market readiness for innovative solutions like KER8 and KER9. Grand View Research projects the market to expand from USD 4,806.5 million in 2023 to USD 18,139.0 million by 2030, representing a robust CAGR of 20.9% during 2024–2030[28]. KBV Research echoes this dynamic, forecasting the related AI-Based Data Security segment to grow at a staggering CAGR of 34.2% by 2031, driven by an urgent need for real-time, intelligent threat detection and response mechanisms across Europe's highly digitalized economies[29]. This rapid market expansion indicates substantial revenue potential for behavioural authentication solutions that secure endpoints and prevent fraud through continuous, AI-driven monitoring.

[26] https://www.grandviewresearch.com/horizon/outlook/ai-in-cybersecurity-market/europe
[27] https://www.kbvresearch.com/europe-ai-based-data-security-market/
[28] https://www.grandviewresearch.com/horizon/outlook/ai-in-cybersecurity-market/europe
[29] https://www.kbvresearch.com/europe-ai-based-data-security-market/

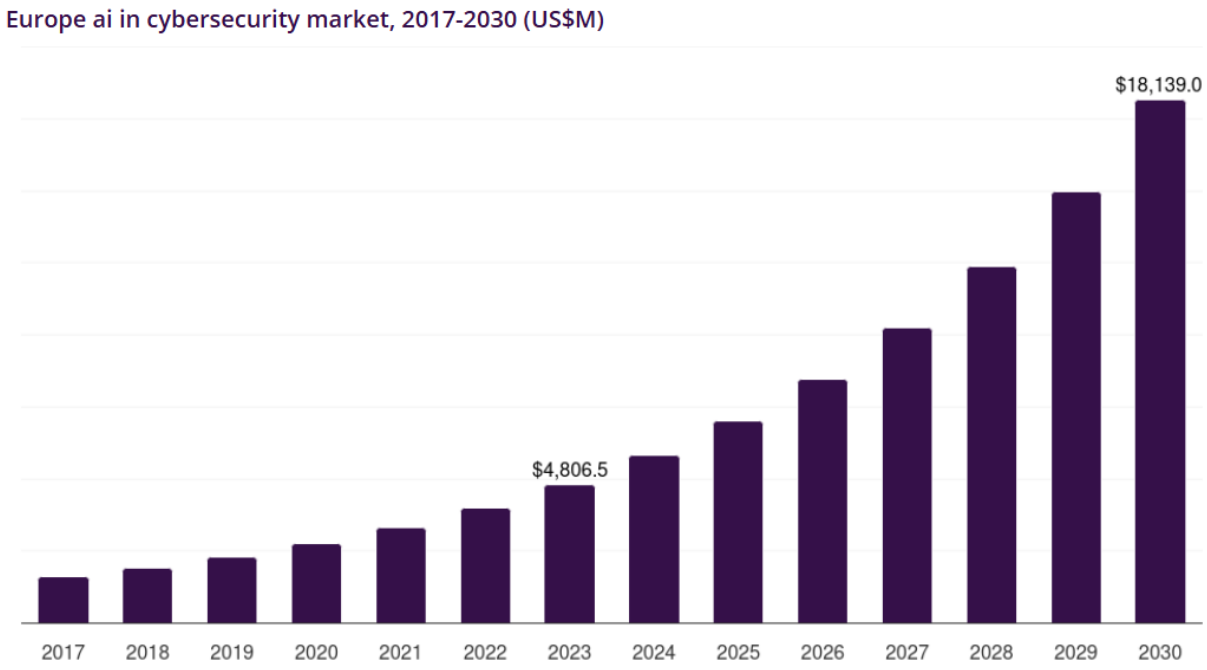


Figure 22: KER8 and KER9 AI in Cybersecurity market size (source: Grand View Research)

Trends

Several prominent trends underpin the demand for continuous behavioural authentication. KBV Research emphasizes that AI-driven Security Orchestration, Automation, and Response (SOAR) systems are increasingly critical as organisations automate threat detection and incident response to manage the complexity of modern attacks[30]. Grand View Research highlights how AI seamlessly integrates into endpoint security and fraud prevention workflows, offering real-time anomaly detection and automated user and device verification[31]. Furthermore, MMR reports that the prevalence of sophisticated attacks like ransomware and phishing intensifies the need for adaptive, behaviour-based security controls that KER8 and KER9 can uniquely deliver[32].

Barriers

Despite promising trends, there are barriers that could hinder KER8 and KER9's widespread adoption. One major obstacle is the growing labour crisis in AI cybersecurity; MMR notes a severe shortage of skilled AI professionals capable of developing, deploying, and managing advanced AI security solutions, with 3.5 million positions globally unfilled as of 2023[33]. This talent gap could slow the pace

[30] https://www.kbvresearch.com/europe-ai-based-data-security-market/
[31] https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-cybersecurity-market-report
[32] https://www.maximizemarketresearch.com/market-report/global-artificial-intelligence-in-cybersecurity-market/867/
[33] https://www.maximizemarketresearch.com/market-report/global-artificial-intelligence-in-cybersecurity-market/867/

at which organisations integrate sophisticated behavioural authentication into their security stacks. Additionally, KBV Research warns that implementing AI-powered security solutions often requires significant upfront investment and technical integration effort, posing challenges especially for small and medium enterprises with limited budgets[34]. Privacy and user consent concerns around continuous behavioural monitoring may also trigger regulatory scrutiny under GDPR, requiring clear compliance strategies.

Opportunities

Despite these barriers, KER8 and KER9 are positioned to tap into clear and growing opportunities within Europe's AI-driven security market. With European organisations facing escalating volumes of complex cyber threats — and traditional security tools struggling to keep pace — there is an urgent need for continuous, adaptive, low-friction authentication mechanisms[35]. By leveraging machine learning to verify users and devices without interrupting workflows, these KERs directly address the demand for robust zero trust frameworks and real-time fraud detection, which MMR identifies as key growth drivers in the region[36]. In particular, sectors like BFSI, retail, and government — which are prime targets for identity theft and fraud — offer high-value use cases for continuous behavioural authentication. As Europe further digitises and regulators tighten security requirements, KER8 and KER9 can become integral to compliance-ready, user-friendly, and AI-enhanced cybersecurity strategies[37].

6.5.3 Value proposition analysis

KER8 offers a transformative authentication solution that redefines security and user experience. Its **non-invasive, AI-driven, and continuous** nature surpasses traditional 2FA or biometric models by requiring no active user participation, thereby eliminating passwords and minimizing friction. UCBA autonomously learns and authenticates based on over **14 behavioural traits**, including gestures, device grip, swipes, and typing behaviour, establishing a **unique cross-device user profile**. Setup requires only a single passport scan or selfie, making onboarding simple. By meeting **PSD2 requirements** and enabling **forensic traceability**, the solution serves not just user verification but also investigative use cases. Its open architecture and SDK enable easy integration into existing systems, and its ability to act as a **primary standalone authenticator** makes it an attractive, secure, and scalable option for financial institutions, gaming platforms, enterprises, and law enforcement.

6.5.4 Barriers, obstacles and analysis of the standards and regulation

Despite its innovation, KER8 faces several challenges. The **competitive landscape** includes established behavioural biometrics providers with entrenched customer bases. Moreover, **potential clients may hesitate** due to unfamiliarity with behavioural authentication or anticipated **integration complexity and costs**. Regulatory barriers also exist due to **variations in regional data protection laws**—solutions must be tailored to align with both **EU GDPR** and **UAE-specific** regulations. However, KER8 is fully

[34] https://www.kbvresearch.com/europe-ai-based-data-security-market/
[35] https://www.grandviewresearch.com/horizon/outlook/ai-in-cybersecurity-market/europe
[36] https://www.maximizemarketresearch.com/market-report/global-artificial-intelligence-in-cybersecurity-market/867/
[37] https://www.kbvresearch.com/europe-ai-based-data-security-market/

compliant, already operating under **ISO27001 and ISO9001** certifications, strengthening its credibility. Privacy concerns around continuous monitoring must be addressed with **transparent data handling and informed user consent** mechanisms, especially under GDPR. In terms of standards, the KER is already aligned with major compliance frameworks including PSD2, giving it a significant regulatory edge.

6.5.5 Technology and market watch

The behavioural authentication space is rapidly evolving, with significant trends supporting KER8's relevance. Based on partners input portrayed in Table 11, there is a **rising adoption** of AI-powered authentication in sectors like **banking, gaming, and law enforcement**, driven by **escalating fraud threats** and regulatory requirements. This trend supports KER8's promise of seamless, real-time verification without user input. Furthermore, the **latest innovations** include AI algorithms that combine multimodal behavioural data (keystroke dynamics, gestures, geolocation) with **adaptive learning**, enabling **context-aware authentication**. KER8 will integrate these advances into its cloud platform and SDK while pursuing **patents** for its proprietary AI methods. Targeted marketing campaigns are planned to highlight the KER's security, ease-of-use, and forensic capabilities across relevant industries, helping to overcome market inertia and drive uptake.

Table 11: KER8 Technology and Market watch

Item	Description	Possible Impact	Actions	Link
Emerging trend or development	Rising adoption of AI-driven behavioural authentication in banking, gambling, gaming and law enforcement domains, fuelled by increasing fraud rates and regulatory demands for seamless, secure user verification.	Positive	Develop targeted marketing campaigns highlighting the KER's fraud prevention and user-friendly features for the domains	Ongoing
Latest innovations and IP	New AI algorithms integrating multimodal behavioural data (e.g., keystroke dynamics, touch gestures, geolocation) with adaptive learning for real-time, context-aware authentication.	Positive	Incorporate advanced multimodal AI algorithms into the KER's cloud platform and SDK to improve performance. Pursue patents for unique behavioural data integration methods.	Ongoing

6.5.6 Business Model Canvas

Business Model Canvas				
Key Partners	**Key Activities**	**Value Propositions**	**Customer Relat**	**Customer Segments**

-Identity Providers: Supply verified identity data to enhance authentication accuracy. -Cloud Service Providers: Provide scalable infrastructure for the cloud platform. -Cybersecurity Firms: Ensure robust security protocols and threat detection. -Financial Institutions: Supply PSD2 Open Banking APIs for transactional pattern analysis. -AI/ML Technology Providers: Provide advanced algorithms for behavioural analysis.	-Develop and maintain the AI-powered cloud platform for continuous behavioural authentication. -Design and update the SDK for seamless data collection and device communication. -Analyze behavioural traits (movement, device usage, social interactions, transactional patterns) for real-time authentication. -Ensure compliance with GDPR, PSD2, and other regulatory standards. -Conduct pilot testing with target customers to validate performance and refine functionality. -Provide training, documentation, and support for integration.	**Secure and User-Friendly Authentication**: Continuous, non-invasive authentication using behavioural traits, requiring no special hardware. **Enhanced Fraud Prevention**: AI-driven analysis detects fraudulent activities with high accuracy. **Forensic Traceability**: Links behavioural patterns to identities for digital investigations. **Regulatory Compliance**: Meets GDPR, PSD2, and other standards for secure authentication. **Seamless Integration**: Cloud platform and SDK enable easy integration into existing workflows. **Spoofing Resistance**: Behavioural traits (e.g., keystroke dynamics, gait) are harder to spoof than physical biometrics. **Characteristics**: Performance, Customization, Convenience/Usability, Risk Reduction, Accessibility.	**Responsive Support**: 24/7 technical support via email, chat, and forums to address integration and operational issues. **Collaborative Engagement**: Regular feedback sessions with customers to refine the solution. **Training and Onboarding**: Offer workshops, webinars, and documentation for adoption. **Developer Community**: Foster engagement through open-source forums and SDK support. **Integration**: Support and training align with	**Banks and Financial Institutions**: Need compliant, secure authentication for PSD2 Open Banking and fraud prevention. **Casinos and Gaming Platforms**: Require non-invasive, real-time fraud detection. **Law Enforcement Agencies (LEAs)**: Seek forensic-grade behavioural identification for investigations. **Enterprises**: Need scalable authentication for employee/customer access control. **Market Type**: Segmented (customized solutions for finance, gaming, LEAs, and enterprises).

-Regulatory Bodies: Support compliance with GDPR, PSD2, and other standards. -UX Designers: Optimize user-friendly SDK interfaces.	**Categories**: Platform/Network (cloud platform and SDK), Problem Solving (fraud prevention, authentication). **Key Resources** **Intellectual**: Proprietary AI algorithms, behavioural data models, SDK codebase, compliance documentation. **Human**: AI/ML engineers, cybersecurity specialists, UX designers, compliance experts. **Physical**: Cloud infrastructure for authentication platform hosting. **Financial**: Funding for R&D, pilot testing, and customer		subscription and consultancy services. **Cost**: Moderate, driven by support staff and training programs. **Channels** **- Direct Sales**: Dedicated account managers for enterprises and regulated industries. **- Community Channels**: Developer forums and chat groups for engagement and support. **- Webinars and Newsletters**: Regular updates and training via the project website. **- Partner Networks**: Leverage financial institutions and cybersecurity

	outreach. **Key Needs**: AI algorithms for value proposition, cloud infrastructure for platform delivery, human expertise for support and training.		firms for distribution.	

Cost Structure	Revenue Streams
▸ **Personnel**: Salaries for AI/ML engineers, cybersecurity experts, support staff, and trainers. ▸ **Infrastructure**: Cloud hosting and maintenance for the authentication platform. ▸ **Compliance and Testing**: Costs for regulatory audits and pilot deployments. ▸ **Marketing and Training**: Expenses for webinars, documentation, and customer acquisition. ▸ **Most Expensive**: Human resources (AI engineers, support staff) and cloud infrastructure. ▸ **Type**: Value-driven (focused on secure, user-friendly authentication and compliance).	▸ **Subscription Fees**: Recurring fees for premium features (e.g., advanced analytics, priority support) and platform updates. ▸ **Consultancy Services**: Fees for customizing and integrating the solution for specific customer needs. ▸ **Training and Certification**: Revenue from training programs and certifications for developers and businesses ▸ **Customer Value**: Security, compliance, ease of integration. ▸ **Pricing**: Fixed pricing (list price for subscriptions, feature-dependent for consultancy), volume discounts for enterprises. ▸ **Contribution**: Subscriptions (75%), consultancy (15%), training (10%).

6.5.7 Exploitation Pathway

KER8 will be commercialized through a **dual-pathway model** combining **SaaS** delivery (projected to contribute 80% of total revenue, ensuring recurring income and scalability) and **consultancy/training services** (projected to contribute 20% of total revenue, ensuring recurring income and scalability).

Initially, the cloud platform and SDK will be offered to early adopters in banking, gaming, and enterprise sectors under a **subscription model**, targeting **fraud prevention and forensic authentication** in Europe due to PSD3 and GDPR alignment. Consultancy services will assist with SDK integration, compliance audits, and application in forensic contexts. KER8 will also deliver **specialized training programs** to help clients maximize the value of behavioural authentication. Strategic partnerships with cybersecurity firms and regulators will support broader integration. The team also aims to expand into **North America and Asia-Pacific** post-European market establishment. Additionally, **intellectual property protections** through patenting and licensing will secure the commercial edge. Future Horizon Europe proposals will integrate KER8's expertise in behavioural data for next-generation security frameworks.

6.6 Exploitation paths for KER9 - Device continuous behavioural authentication

6.6.1 Competitor analysis

The competitive landscape for KER9 reveals a significant gap in offerings, which the TANGO result addresses with its unique technical approach. Most commercial solutions such as **BioCatch** and **BehavioSec** focus exclusively on **user-level behavioural biometrics**—capturing interactions like typing rhythm, swipe gestures, and mouse movements. These solutions operate primarily at the application layer and are designed for **non-rooted devices**, thereby missing out on device-level operational patterns that can enhance security assurance.

BioCatch targets enterprise banks, fintech companies, and high-volume SaaS platforms, offering cloud-based behavioural analytics, but does not access system-level logs. Similarly, **BehavioSec**, which is now part of LexisNexis, offers user-side behavioural authentication via SDKs focused on swipe and typing patterns, with compliance to standards like PSD2 and GDPR. However, both competitors charge substantial licensing fees, often exceeding **$50,000** for SDK integration, without providing the depth of continuous monitoring at the device-operating level.

In contrast, **KER9's Device Continuous Behavioural Authentication (DCBA)** offers a distinctive feature set by rooting Android 10.0 devices and accessing full **system logs** (battery, network, Bluetooth, etc.), which are streamed to a **BERT-based Risk Assessment Engine**. Furthermore, it uniquely integrates **Wi-Fi/BLE RSSI-based localization** to support **physical premises access control**—a feature absent in competitor offerings. This positions KER9 not only as a research-grade innovation but as a potential enabler for next-generation authentication systems in smart manufacturing environments.

6.6.2 Market Analysis

Despite UTH not wishing to monetise or commercialise KER9, the result has plenty of commercialisation potential and it closely relates to the AI in Cybersecuity market. Accordingly, the market analysis for KER9 is depicted in section "AI in Cybersecurity market analysis for KER8 (User Continuous Behavioural Authentication) and KER9 (Device Continuous Behavioural Authentication)".

6.6.3 Value proposition analysis

KER9 delivers a **research-grade, open-source authentication system** that goes beyond traditional login-based security by providing **continuous device-level verification** throughout a session. By rooting Android 10.0 devices using Magisk and granting deep access to logs (e.g., network, battery, Bluetooth), it builds unique behavioural profiles for individual devices. These profiles are then analyzed in real time using a **BERT-based machine learning model** to detect anomalies and trigger reauthentication if needed.

This **device-centric** approach not only improves **session integrity** but also supports **secure physical access** through RSSI-based indoor localization. As a **university-led initiative**, the primary mission is not commercialization but the dissemination of knowledge and methodologies to **academic institutions, non-profit cybersecurity consortia, and technology educators**. It provides a complete framework—from Android client to backend pipelines—designed for **integration into mobile security and IoT courses** and real-world lab pilots.

6.6.4 Barriers, obstacles and analysis of the standards and regulation

The primary technical barrier to KER9 adoption lies in the **need to root Android devices**, a process that adds complexity and potential stability issues. This limits usage to **research and testing environments**, rather than commercial deployment on end-user devices. Rooting can also void warranties or violate terms of service for many devices.

From a **standards** perspective, there is currently no ISO/IEC standard covering **device-log–based continuous behavioural authentication**, which may hinder formal validation or certification efforts. Regulatory challenges are also present, especially with **GDPR compliance**. The collection of detailed system logs—potentially including sensitive metadata—must be handled with strict consent and anonymization strategies. Furthermore, **local laws regarding device rooting** vary across EU member states, creating additional legal uncertainty for broader adoption.

6.6.5 Technology and market watch

While UTH has declared that KER9 is not intended for commercial exploitation, its **technological innovation places it at the forefront of behavioural authentication research**. Current market trends highlight the increasing importance of **AI-driven behavioural analytics** in security, particularly in contexts like **smart manufacturing**, **IoT security**, and **adaptive access control**. The use of **RSSI-based localization** combined with **machine learning** for anomaly detection aligns with cutting-edge approaches being explored in academia and emerging standards bodies such as **SSI working groups**, **IETF**, and **W3C**.

As part of its roadmap, KER9 will be disseminated through academic publications (e.g., IEEE Access), GitHub releases, and integration into **university-level course modules**. This not only ensures sustained visibility within the RTO ecosystem but also creates opportunities for future **open-source collaboration and research grants**.

6.6.6 Business Model Canvas

Business Model Canvas				
Key Partners	**Key Activities**	**Value Propositions**	**Customer Rela**	**Customer Segments**
Academic and Research Institutions: Collaborate with universities, research labs, to share findings, validate methodologies, and co-author publications. Open-Source Communities: Engage with Android and machine-learning open-source projects (e.g., AOSP, TensorFlow/PyTorch communities) to integrate continuous behavioural authentication modules and receive community feedback. Standards and Policy Bodies: Work with Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), and self-sovereign identity (SSI) working groups to align with emerging	Fundamental Research & Development Refinement of the Risk Assessment Engine (BERT-based ML model) for anomaly detection in device logs. Exploration of alternative data-collection mechanisms (e.g., optimizing RSSI-based localization, battery-friendly scanning). Proof-of-Concept Demonstrations Deploy 'Authenticator' on rooted Android devices in laboratory and smart-manufacturing pilot sites.	Continuous Device Identity Assurance: It extends security beyond one-time login by continuously verifying device behaviour in real time, thereby reducing risks from device theft, session hijacking, and insider threats. Open, Academic-Driven Framework: A fully documented, research-grade implementation released under permissive licensing, enabling other RTOs, universities, and non-profit organizations to adopt, replicate, and extend the work without commercial restrictions. Adaptable to Smart Manufacturing Use Cases: We aim to demonstrate its capability to	Collaborative Academic Engagement: aim to co-author publications and conduct joint supervision of graduate theses, and shared lab visits. Community-Driven Support: GitHub issue tracker and discussion forums for open-source code, with maintainers from the RTO guiding contributors.	Academic Researchers & Students: Universities and RTOs focusing on mobile security, continuous authentication, machine learning, and IoT security. Master's and PhD students seeking hands-on projects or thesis topics. Cybersecurity Consortia & Non-Profit Organizations: Groups interested in evaluating novel authentication mechanisms for broader public-sector or critical-infrastructure use.

authentication standards. Funding Agencies and European RTO Networks: Leverage Horizon Europe, national research councils, and University RTO funding channels to secure grants and in-kind contributions (e.g., compute time, test devices).	Validate continuous authentication accuracy under realistic usage patterns. **Key Resources** Technical Infrastructure Android Devices (Rooted): Lenovo tablets (Android 10.0) unlocked and rooted with Magisk Manager; dedicated devices reserved for continuous lab testing. Backend Servers (Cloud-based): Virtual machines or cloud instances running Node.js server containers, MongoDB, and InfluxDB (time-series data). Machine-Learning Environment: GPU-enabled compute cluster (on-premise or cloud) for training the	integrate RSSI-based localization with behavioural logs to provide fine-grained access control for physical premises (e.g., factory floors, clean rooms). Modular, Containerized Backend: It employs Docker containers for Node.js, MongoDB, and InfluxDB enabling easy replication of the backend environment for teaching, testing, and collaborative research.	**Channels** **- Direct Sales**: Dedicated account managers for enterprises and regulated industries. **- Community Channels**: Developer forums and chat groups for engagement and support. **- Webinars and Newsletters**: Regular updates and training via the project website. **- Partner Networks**: Leverage financial institutions and cybersecurity firms for distribution.	Technology Educators & Trainers: Institutions or instructors designing curricula on mobile security and need modules on behavioural authentication.

	BERT-based Risk Assessment Engine. Development Tools: Android Studio (Java), Docker and docker-compose for container orchestration, Git for version control, and CI/CD pipelines. Localization heatmap algorithms and datasets for indoor positioning within smart-manufacturing facilities.			

Cost Structure	**Revenue Streams**
Personnel Costs (Fixed & Recurring): Salaries for research staff (professors, postdocs, PhD students) and technical staff. Teaching and workshop instructors for training programs. Infrastructure & Equipment: Purchase and maintenance of Android devices (including spares for rooting experiments). Software & Licensing: Development tools	As UTH is a university its goal is knowledge dissemination and RTO objectives rather than direct commercialization, most revenue stems from non-commercial funding and capacity-building activities. UTH targets on receiving research Grants and subsidies through competitive grants (e.g., Horizon Europe, national research councils) covering project personnel, equipment, and dissemination.

6.6.7 Exploitation Pathway

KER9 is not intended for commercialization but follows an **open-source and academic dissemination pathway**. In the short term (within six months), the plan is to publish the complete DCBA stack—including the Android client, Node.js backend, Docker setup, and ML preprocessing tools—on GitHub under a permissive license (MIT/Apache) targeting non-commercial research consortia and public

laboratories under no-cost or minimal-fee agreements, as the result will be open source. This will be supported by comprehensive documentation, installation guides, and CI/CD tools.

Parallel to the release, the team will submit a **white paper or conference publication** on DCBA technology and its application in **smart-manufacturing physical access control**. In the midterm (12–24 months), UTH will develop and launch a **dedicated Master's-level course** titled "Continuous Device Behavioural Authentication" and integrate this topic into undergraduate/graduate modules on Mobile and IoT Security.

Long-term efforts include maintaining and enhancing the software stack, subject to availability of **research funding**, and potentially applying to **future Horizon Europe calls**. UTH's overall approach is aligned with its mission to generate and disseminate cutting-edge knowledge through **new use cases demonstrations and early adopter uses**, **academic teaching**, and **community-driven development**.

6.7 Exploitation paths for KER14a- Privacy Threat Modelling and Identification for Trustworthy AI-Privacy Enhancing Component (PEC)

6.7.1 Competitor analysis

KER14a – the Privacy Enhancing Component (PEC) – directly competes with advanced privacy risk management tools offered by leading vendors such as HiddenLayer, Robust Intelligence, and OneTrust. Each of these competitors serves organisations that incorporate machine learning (ML) and AI systems into their operations, particularly in highly regulated sectors such as finance, government, and defence.

HiddenLayer specialises in security solutions tailored for ML environments. Their Machine Learning Detection & Response (MLDR) platform and related consulting services focus on protecting models from adversarial threats. While the platform provides valuable model-level protection, it does not offer integrated privacy threat modelling or a comprehensive privacy risk scoring dashboard like PEC. Pricing for HiddenLayer's services is customised and not publicly disclosed, indicating a tailored enterprise approach.

Robust Intelligence focuses on securing enterprises from AI-related risks, providing platforms that monitor and test AI systems for vulnerabilities. Their clients include JP Morgan Chase & Co, Expedia, Cisco, Deloitte, Rakuten, NEC, Equinix, Tokio Marine, Survey Monkey, and the U.S. Department of Defence, suggesting deep market penetration in high-stakes environments. These clients represent various sectors, including finance, technology, consulting, retail, and government, indicating a broad application of Robust Intelligence's AI risk management solutions. Their pricing strategy is not available online. Typically, companies like Robust Intelligence offer customised pricing based on the specific needs and scale of an organisation's operations. This often involves a direct consultation with the company to understand the specific services required, the size and complexity of the AI models being used, and other factors that might affect pricing. However, their solutions cater primarily to large-scale enterprises, unlike PEC's emphasis on SME usability and multi-framework integration for GDPR and AI Act compliance.

OneTrust stands out as a broad-spectrum GRC (Governance, Risk, and Compliance) platform. Its Trust Intelligence Platform covers privacy, ethics, ESG, and compliance. OneTrust's pricing is segmented based on enterprise size and sector, with customised tiers for large corporations, growing businesses, and non-profits. While comprehensive, OneTrust's offering is generally compliance-focused, lacking the AI-specific privacy threat modelling and scoring capabilities that PEC provides. Moreover, OneTrust and similar vendors overlook usability challenges faced by SMEs, which PEC addresses explicitly through lightweight deployment and accessible scoring mechanisms. OneTrust offers a variety of pricing options for their Trust Intelligence Platform, catering to different types of organisations:

- Large Enterprise Pricing: this category is tailored for organisations with more than 500 employees.
- Growing Business Pricing: specifically designed for organisations with 500 employees or fewer, this pricing option addresses the needs and constraints of smaller, developing businesses.
- Special Industry Pricing: special pricing for educational institutions, public sector organisations, and non-profits, acknowledging the unique financial and operational contexts of these sectors.

While these players cover general governance or security risks, KER14a's competitive edge lies in its focus on quantifying privacy risks related specifically to AI/generative AI, offering a privacy risk score with actionable mitigation advice. Unlike most competitors, PEC is designed to support SMEs through usability, multi-framework support, and low-barrier integration.

6.7.2 Market analysis

AI Governance market analysis, Privacy Enhancing Technologies (PET) market for KER 14a (Privacy Enhancing Component) and ER 14b (Privacy Assurance Tool).

Segments

KER 14a and ER14b directly align with the *solutions* and *services* segments within the AI Governance market, providing privacy risk assessment, assurance, and compliance monitoring tools that support organizations' AI governance frameworks. These results are particularly relevant for high-risk sectors like BFSI, healthcare, and government, as shown in Figure 23, which must comply with stringent privacy and AI transparency regulations. According to Grand View Research, solutions such as auditing, bias detection, and explainability tools dominated the AI governance market in 2024, accounting for nearly 66.7% of market share, while services that help firms implement and maintain governance frameworks are a vital complementary segment[38]. Both KER 14a and 14b contribute to these core segments by delivering concrete privacy-centric tools, which are increasingly mandatory in Europe under the upcoming EU AI Act and existing GDPR[39].

[38] https://www.grandviewresearch.com/industry-analysis/ai-governance-market-report
[39] https://www.fortunebusinessinsights.com/ai-governance-market-105975

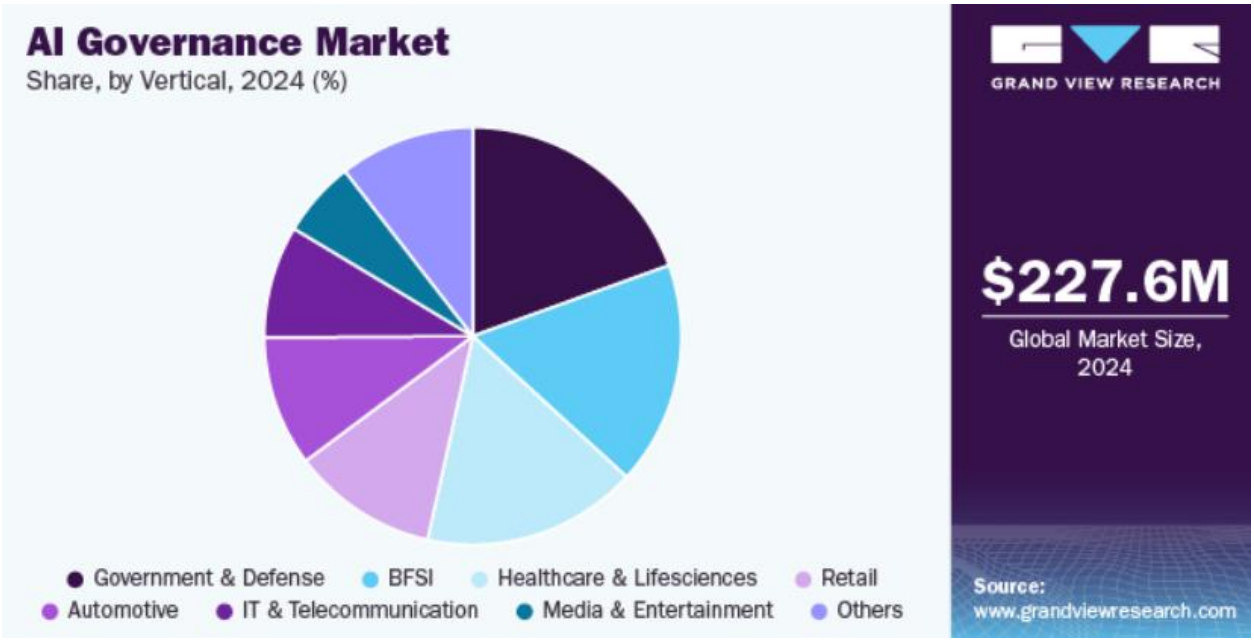


Figure 23: KER14a and ER 14b AI Governance market market segments (source: Grand View Research)

Size and Growth Rate

As depicted in Figure 24, the AI Governance market is in a phase of explosive growth globally and within Europe. Grand View Research estimates the global market at USD 227.6 million in 2024, with projections to reach USD 1,418.3 million by 2030, driven by a CAGR of 35.7% from 2025–2030[40]. Fortune Business Insights projects an even steeper trajectory, with the market expanding from USD 176.7 million in 2024 to over USD 2.29 billion by 2032, exhibiting a CAGR of 37.7%[41]. Europe's share is substantial due to the region's regulatory leadership: the AI Act and GDPR together create the world's most comprehensive privacy and AI governance regime, ensuring high demand for compliance solutions like PEC and PAT[42].

[40] https://www.grandviewresearch.com/industry-analysis/ai-governance-market-report
[41] https://www.fortunebusinessinsights.com/ai-governance-market-105975
[42] https://www."Markets and Markets".com/blog/ICT/ai-governance-market

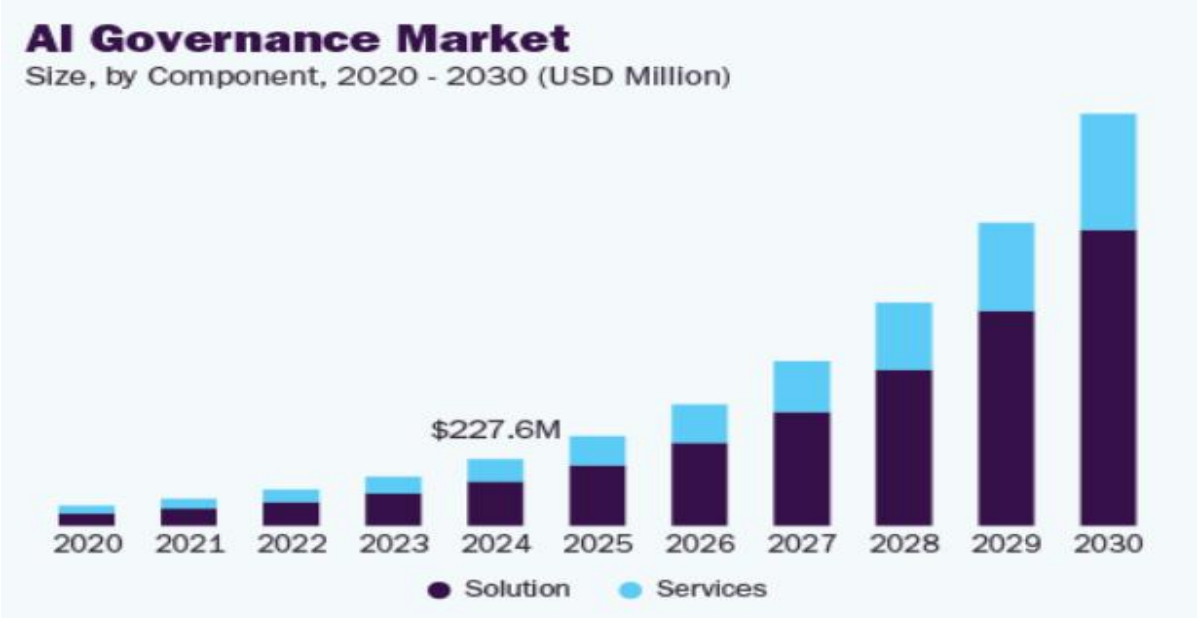


Figure 24: KER14a and ER 14b AI Governance market size (source: Grand View Research)

Trends

Key trends fuelling the market for KER 14a and ER14b include rising demands for explainable AI (XAI), increasing use of blockchain for audit trails, and a sharper regulatory focus on privacy and data security. Grand View Research highlights that sectors like BFSI and healthcare are integrating XAI and bias detection to address transparency mandates — areas where PEC and PAT can plug directly into organizations' AI workflows[43]. Global Market Insights underscores blockchain's role in ensuring unalterable logs of AI system decisions, reinforcing trust and accountability — a direction that complements PEC's privacy risk scoring and PAT's citizen-facing privacy monitoring[44]. Additionally, "Markets and Markets" points out that tightening legislation, including the EU AI Act's mandatory risk assessments for high-risk AI, guarantees sustained demand for privacy-centric governance tools like KER 14a and ER14b[45].

Barriers

While growth is strong, challenges remain that could slow the impact of KER 14a and ER14b. A critical barrier is the persistent shortage of skilled AI governance professionals, which Fortune Business Insights cites as a major hurdle, especially for companies lacking in-house expertise to implement complex privacy risk tools and interpret assessments[46]. Another risk is the lack of universal standards across industries and countries: while the EU sets the bar high with the AI Act, variations elsewhere could create integration complications for multinational firms using PEC and PAT. Furthermore, high upfront

[43] https://www.grandviewresearch.com/industry-analysis/ai-governance-market-report
[44] https://www.gminsights.com/industry-analysis/ai-governance-market
[45] https://www."Markets and Markets".com/blog/ICT/ai-governance-market
[46] https://www.fortunebusinessinsights.com/ai-governance-market-105975

implementation costs for tailored privacy auditing and monitoring tools may deter smaller firms despite cloud deployment options[47].

Opportunities

Despite these challenges, Europe offers significant opportunities for PEC and PAT. The upcoming EU AI Act mandates transparency and accountability, explicitly requiring explainability and privacy guarantees for high-risk AI — areas that PEC's risk scoring and PAT's assurance functions directly address[48]. Fortune Business Insights confirms that European governments and industries are proactively investing in AI compliance tools to build trust and avoid penalties, which creates a ready market for plug-and-play governance modules [49]. Moreover, the demand for sector-specific governance is expanding: sectors like finance, healthcare, and government show the fastest uptake of governance solutions because they manage highly sensitive personal data and are under intense regulatory scrutiny[50]. This sectoral demand means KER 14a and 14b can scale as core compliance building blocks for organizations that must demonstrate robust privacy management and data protection to regulators and customers alike.

Privacy Enhancing Technologies (PET) market

Segments

KER14a and ER14b primarily serve the **software** segment in PETs and align with the **compliance management** and **risk management** applications as detailed by Fortune Business Insights[51]. The PEC (KER14a) embeds privacy-by-design features like data minimization and secure encryption modules directly into digital services. Meanwhile, the PAT (ER14b) provides runtime assurance and automated checks that verify compliance with privacy policies and regulatory standards. In autonomous vehicles, both components enhance **application security** by protecting onboard systems and data exchanges — especially critical as vehicles rely on continuous data collection for AI-driven navigation and safety[52].

Size and Growth Rate

For these embedded solutions, the PET software segment alone was worth over USD 3 billion in 2024 and is forecast to grow strongly due to widespread adoption of cloud services and IoT devices, both of which benefit from integrated privacy safeguards[53]. Europe's push for digital sovereignty and privacy-first AI further amplifies demand for privacy-by-design modules and continuous compliance verification tools — reinforcing strong market fit for 14a and 14b. The autonomous vehicles cybersecurity market's

[47] https://www.gminsights.com/industry-analysis/ai-governance-market
[48] https://www.imarcgroup.com/ai-governance-market
[49] https://www.fortunebusinessinsights.com/ai-governance-market-105975
[50] https://www.grandviewresearch.com/industry-analysis/ai-governance-market-report
[51] https://www.fortunebusinessinsights.com/privacy-enhancing-technologies-market-111241
[52] Allied Market Research, https://www.alliedmarketresearch.com/cybersecurity-for-autonomous-vehicles-market-A324122
[53] Grand View Research, https://www.grandviewresearch.com/industry-analysis/privacy-enhancing-technologies-market-report

22.9% CAGR underlines an overlapping growth corridor where these tools can be built into vehicle platforms to assure privacy compliance dynamically[54].

Trends

A key trend benefiting 14a and 14b is the mainstream deployment of **advanced cryptographic techniques and privacy-enhancing design patterns**. Homomorphic encryption, differential privacy, and secure multi-party computation are increasingly adopted within PETs to guarantee privacy even during data processing[55]. 14a can encapsulate such techniques within modular components, while 14b ensures ongoing verification of their proper application. In vehicles, secure-by-design trends mean Original Equipment Manufacturers (OEMs) are embedding privacy protection deeper into hardware and software stacks to meet consumer expectations and new EU digital compliance laws[56].

Barriers

However, both solutions face the **barrier of high initial deployment costs** and the need for robust change management. Embedding privacy-enhancing functionality across heterogeneous systems can require costly software re-engineering, staff training, and operational adjustments[57]. In the automotive domain, compliance assurance tools must meet rigorous validation to avoid false positives or system conflicts, which can delay certification and market entry[58].

Opportunities

The surge in global privacy regulations (GDPR, AI Act) and the high financial risk of non-compliance create clear opportunities for 14a and 14b. Organizations can embed these tools to automate compliance tasks, reduce human error, and assure auditors of continuous privacy protection[59]. In the autonomous vehicle market, their inclusion can be marketed as a trust booster, reassuring passengers and regulators that data collected by smart sensors and AI systems is rigorously protected at all times — a critical enabler for public acceptance and regulatory approval[60].

---

[54] Allied Market Research, https://www.alliedmarketresearch.com/cybersecurity-for-autonomous-vehicles-market-A324122

[55] Fortune Business Insights, https://www.fortunebusinessinsights.com/privacy-enhancing-technologies-market-111241

[56] Allied Market Research, https://www.alliedmarketresearch.com/cybersecurity-for-autonomous-vehicles-market-A324122

[57] Fortune Business Insights, https://www.fortunebusinessinsights.com/privacy-enhancing-technologies-market-111241

[58] Allied Market Research, https://www.alliedmarketresearch.com/cybersecurity-for-autonomous-vehicles-market-A324122

[59] Grand View Research, https://www.grandviewresearch.com/industry-analysis/privacy-enhancing-technologies-market-report

[60] Allied Market Research, https://www.alliedmarketresearch.com/cybersecurity-for-autonomous-vehicles-market-A324122

6.7.3 Value Proposition analysis

PEC is a decision-support tool that empowers organisations to responsibly and ethically adopt AI and generative AI technologies. It addresses the dual imperatives of innovation and privacy compliance by identifying privacy threats inherent in AI-powered workflows. By accessing data flows and mapping them to cyber-physical threats, PEC quantifies privacy risks and offers targeted, actionable mitigation measures.

PEC's core value lies in its visual risk scoring dashboard, which integrates threat identification, impact assessment, and compliance insights. Unlike traditional tools that focus solely on regulatory checklists, PEC translates AI-specific data usage risks into a privacy score. This enables organisations to understand and manage their exposure, comply with GDPR and forthcoming AI-specific regulations, and maintain customer trust.

It is especially useful in sectors where ML is heavily used—such as finance, defence, and government—allowing organisations to prioritise resources and protect sensitive personal data. PEC is designed for long-term sustainability, offering quantifiable compliance while contributing to ethical AI deployment across the digital economy.

By offering an AI-specific privacy risk assessment that is accessible, visual, and regulatory-aware, PEC differentiates itself from high-end compliance platforms and provides real business value to under-served SMEs, tech startups, and highly regulated sectors.

6.7.4 Barriers, obstacles and analysis of standard regulation

KER14a faces several significant barriers. The first is the technical complexity inherent in assessing privacy risks in AI and generative AI systems, which require advanced knowledge of both AI architectures and legal compliance frameworks. This complexity can act as a deterrent for smaller firms or less technically sophisticated clients.

PEC's development is constrained by limited funding, manpower, and technology resources. These internal constraints could hinder scaling and long-term support. Additionally, the presence of large established players in cybersecurity and governance—such as OneTrust and TrustArc—creates intense market competition and raises the threshold for differentiation.

From a regulatory standpoint, PEC must navigate the diverse and evolving patchwork of data privacy rules globally, including GDPR, the EU AI Act, ISO 23894, and sector-specific regulations (e.g., in healthcare or finance). Each vertical has unique compliance needs, demanding that PEC be adaptable while maintaining coherence in its scoring methodology.

Furthermore, protecting the proprietary nature of KER14a's methodologies while managing legal liability for its recommendations presents a legal/operational challenge. The absence of universal standards for AI privacy threat quantification adds further uncertainty to PEC's regulatory alignment strategy.

6.7.5 Technology and market watch

The technological landscape around PEC is rapidly evolving, offering both validation and new challenges. Increasing regulatory complexity (GDPR, EU AI Act, ISO 23894) and rising SME awareness of AI-driven privacy risks strongly support the relevance of PEC. This trend positions PEC as an early entrant in a new compliance category that targets the SME segment. UOG plans to track regulatory changes and update the scoring engine accordingly, while building thought leadership via white papers and webinars.

Large firms like OneTrust and TrustArc are investing heavily in privacy tooling, but their focus remains on large enterprises and checkbox compliance. Their limited support for multi-framework integration and lack of SME-specific tools gives PEC a unique opportunity to address an underserved niche. UOG will emphasise PEC's usability and compliance coverage (GDPR, AI Act, NIST PRAM) as key differentiators.

Startups like PrivIQ and DPOrganizer show high traction in the SME compliance tooling space, validating demand. UOG intends to partner with SME innovation hubs to drive early adoption. Furthermore, the growing use of AI/LLM models in compliance workflows presents both risk and opportunity. PEC is well positioned to evolve into a complementary tool for AI pipeline compliance checks.

The adoption of AI in everyday SME workflows (CRM, HR, analytics) increases privacy exposure, widening PEC's relevance beyond governance into risk management and procurement. Finally, EU Digital Services Act funding and SME support schemes could subsidise PEC's adoption in regulated verticals. Table 12 below elaboratively depict the input provided by UOG regarding this matter.

Table 12: KER14a Technology and Market watch

Item	Description	Possible Impact	Actions	Effective date	Link
Emerging trend or development	Increasing regulatory complexity (GDPR, EU AI Act, ISO 23894) and SME awareness of AI-driven privacy risks. Rising demand for quantifiable, actionable compliance tools.	Positions the tool as an early entrant in a new compliance software category, especially for SME adoption.	Monitor regulatory updates and map changes into the scoring engine. Target thought leadership via white papers and SME-focused webinars.	Ongoing	https://artificialintelligenceact.eu, https://edpb.europa.eu/our-work-tools/our-documents/guidelines_en
Active companies and	OneTrust, TrustArc and IBM are investing in	Market validation supports growth,	Emphasise usability and multi-framework support	Immediate	https://www.onetrust.com, https://trustarc

Item	Description	Possible Impact	Actions	Effective date	Link
their R&D strategies	privacy compliance tooling but focus on large enterprises and checkbox compliance.	but existing tools overlook SME needs and lack multi-framework integration.	(NIST PRAM, PEO, GDPR, AI Act) to differentiate.		.com
Hot startups and innovators	PrivIQ, DPOrganizer, and emerging GDPR SaaS startups targeting SME privacy workflows.	Indicates high growth in SME-focused compliance tooling. Validates demand for lightweight, usable solutions.	Partner with SME networks and innovation hubs to increase early adoption.	Ongoing	https://www.priviq.com, https://www.dporganizer.com
Impact of new technology adoption	AI/LLM integration in compliance tooling creates new layers of risk and automation potential.	Validates focus on AI-related privacy risks; opens integration opportunities with existing LLM-based platforms.	Position tool as a complementary module for AI pipeline compliance checks. Explore SDKs for developers.	2025–2026	https://www.iso.org/standard/77609.html, https://www.nist.gov/itl/ai-risk-management-framework
Potential impact of technological change	Growing integration of AI in SME workflows (CRM, HR, data analytics) increases privacy exposure.	Expands relevance of your tool beyond compliance to risk management and procurement.	Engage in sector-specific pilots (e.g. HR tech, health tech) to capture wider markets.	2025	https://joint-research-centre.ec.europa.eu/ai-watch_en
New market opportunities	EU Digital Services Act and SME support schemes are funding adoption of trustworthy tech.	May support procurement or subsidised use of the tool in regulated sectors.	Explore onboarding via EIC Accelerator and national (UK) cybersecurity funds.	2025–2027	https://digital-strategy.ec.europa.eu/en/activities/digital-programme

6.7.6 Business Model Canvas

Business Model Canvas

Key Partners	Key Activities	Value Propositions	Customer Relationships	Customer Segments
TANGO consortium partners: co-developers and pilot collaborators providing technical validation, integration support and use case definition. **National Data Protection Authorities (DPAs)** offering regulatory guidance and helping align the tool with GDPR enforcement expectations. **ENISA and NIST Working Groups** contributing to alignment with cybersecurity and privacy risk frameworks (e.g. NIST PRAM, PEO). **Industry associations for SMEs (e.g. SMEunited)** enabling dissemination and trust-building within small business networks. **Cloud and API infrastructure providers** offering scalable and secure hosting environments	**Privacy risk modelling and scoring engine development:** implementing logic to assess and compute privacy risk scores using NIST PRAM, PEO, GDPR and EU AI Act dimensions. **Use case mapping and risk scenario definition:** capturing diverse small business data sharing scenarios to contextualise the tool's assessments. **Continuous framework alignment**: updating the scoring model to reflect evolving regulatory and policy changes (e.g. EU AI Act updates, GDPR case law). **Tool deployment and integration support**: ensuring SMEs can integrate the tool into existing data workflows (e.g. via dashboards, APIs). **User interface and experience design**: developing an accessible front-end tailored to non-	**Actionable privacy risk scoring**: translates complex regulatory requirements (GDPR, EU AI Act, NIST PRAM, PEO) into a clear understandable risk score **SME-focused usability**: designed specifically for small businesses with limited legal or technical expertise in privacy risk **Early compliance warning system**: alerts SMEs to potential privacy or AI governance non-compliance risks before they escalate **Cost-effective compliance support**: reduces the need for expensive consultancy by offering automated self-	**Guided onboarding support**: Offers SMEs step-by-step assistance during initial tool setup and use **Self-service documentation**: Provides manuals, FAQs and how-to guides to support autonomous use **Feedback-driven updates**: Incorporates customer feedback into iterative tool improvements **Lightweight support channel**: Maintains a minimal but responsive helpdesk or chatbot for ongoing queries **Trust-based engagement**: Builds long-term confidence	**Small and medium-sized enterprises (SMEs):** Core target group requiring practical, affordable privacy risk assessment tools **Data processors and controllers**: Organisations responsible for processing or managing shared data across partnerships **Legal and compliance officers in SMEs**: Non-expert users needing structured risk visibility for accountability and governance **Sector-specific SME clusters**: Particularly in health tech, edtech, logistics and financial

for deployment (e.g. AWS, Azure).

Legal tech advisors – contributing expertise in interpreting GDPR, EU AI Act and data sharing obligations.

Standardisation bodies (e.g. ISO/IEC, CEN-CENELEC) supporting mapping of tool outputs to recognised privacy risk standards.

experts in privacy or legal compliance.

Validation and testing with SME pilots: running real-world assessments with small businesses to refine usability and effectiveness.

Dissemination and outreach: engaging with SME networks, tech incubators and chambers of commerce for adoption and feedback.

Key Resources

Privacy scoring engine: Core software component implementing NIST PRAM, GDPR, PEO and EU AI Act alignment

Regulatory knowledge base: Continuously updated models and mappings of legal and policy frameworks

Human expertise: Development team, privacy engineers and regulatory analysts maintaining

service assessments

Framework-integrated: Combines established privacy risk assessment standards into a unified interoperable methodology

Deployment flexibility: Usable via SaaS, API or local deployment depending on SME requirements or sensitivity of data

Demonstrable accountability: Helps businesses document risk-based decision-making for audits, regulatory inquiries or DPIAs

Supports trust-building: Enhances transparency and trust when sharing data with partners, clients or regulators

through transparent risk reporting and regulatory alignment

Channels

SME networks and associations: Dissemination via chambers of commerce, industry alliances and innovation hubs

TANGO pilot use cases: Direct engagement and feedback loops from validation partners

Online platform and

services where data sharing is intensive

Technology providers to SMEs: Offering the tool as part of broader compliance or data protection bundles

Innovation hubs and digital accelerators: Distributors or multipliers supporting SME digital transformation and regulatory readiness

	and improving the tool **SME-centric UI/UX assets**: Interfaces and content designed for accessibility and usability by non-experts **Intellectual property assets**: Tool architecture, algorithms and compliance models developed within TANGO **Pilot feedback data**: Real-world usage and validation results from SME testing environments **Hosting and deployment infrastructure**: Cloud-based or local environments enabling secure tool access		**SaaS portal**: Centralised access point for tool use, documentation and updates **API integrations**: Embedded delivery through third-party compliance or data governance platforms **Workshops and webinars**: Awareness-building and capacity development among SME stakeholders

Cost Structure	Revenue Streams
Personnel costs: Salaries for software developers, privacy experts and legal analysts **Maintenance and updates**: Ongoing costs for regulatory alignment, software patches and scoring model refinement **Infrastructure and hosting**: Cloud service fees or local deployment support for SME users **User support and onboarding**: Lightweight helpdesk, training materials and community engagement **Dissemination and outreach**: Efforts to promote adoption through networks, events and online channels	**Subscription fees**: Tiered access model (e.g. basic, advanced, enterprise) based on organisation size or usage level **Licensing**: White-label or embedded integration licensing for compliance platform vendors or service providers **Consultancy add-ons**: Optional expert support or audits for high-risk data sharing use cases **Public procurement**: Adoption via digital transformation or compliance initiatives funded by local or national governments

Compliance assurance: Internal legal review to ensure accurate and up-to-date regulatory mapping	**Grants and research funding**: Continued development and scaling through Horizon Europe or similar programmes **Strategic partnerships**: Revenue sharing with SME associations, innovation hubs or digital compliance platforms

6.7.7 Exploitation Pathway

KER14a will be monetised by UOG through integration into a broader product suite, available at https://cyberiskradar.com. The product will be offered as a yearly subscription-based software-as-a-service (SaaS) solution, initially through a B2B model and with future potential to expand into B2C. The immediate goal is to deliver PEC as a compliance-focused, privacy risk assessment module tailored for SMEs, especially those adopting AI and generative AI technologies. UOG aims to secure further Horizon Europe and ICURe funding to support development, scale-up, and go-to-market activities[61]. In the short term, the exploitation plan focuses on validating the tool in high-risk sectors such as finance, healthcare, and government. Mid- to long-term goals include increasing market share from an initial 1–3% to 5–10% within five to ten years, establishing PEC as a trusted name in AI privacy compliance. Thought leadership through white papers, webinars, and SME workshops will support this trajectory, alongside participation in EU programmes such as the Digital Services Act support schemes and EIC Accelerator initiatives[62].

6.8 Exploitation paths for KER16-Infrastructure Management based on AI

6.8.1 Competitor analysis

The principal competitor identified for KER16 is **Electricity Maps**, which provides real-time data on electricity production and consumption. This service is geared toward **consumers of electricity data**, the same general audience targeted by KER16. Electricity Maps' platform offers open access via a visual web interface and API and is already in collaboration with **major global players like Google**, which could pose a competitive threat due to their ability to rapidly scale and integrate across platforms[63].

The risk from Electricity Maps lies in their technological reach and strong partnerships that could challenge the market positioning of KER16, particularly if such platforms expand their capabilities into renewable forecasting or infrastructure management services. Electricity Maps offers data consumption functionalities that overlap with the foundational layer of what KER16 does, although XLAB's solution focuses on **computational load shifting** and **forecast-based infrastructure decision-making**,

[61] https://iuk-business-connect.org.uk/programme/icure
[62] https://digital-strategy.ec.europa.eu/en/activities/digital-programme
[63] Electricity Maps Client Stories

which may still differentiate it from pure consumption trackers. However, the overlapping target audience and similarity in delivery formats (e.g. REST API) indicate clear competitive proximity.

6.8.2 Market analysis

KER16: Infrastructure Management based on AI, specifically targeting the AI in Renewable Energy Forecasting market

Segments

KER16 aligns primarily with the **AI in Renewable Energy Management and Forecasting** segment, depicted in Figure 25, which sits within the broader "AI in Energy" market. Its ensemble model, accessible via REST API, supports **renewable energy forecasting**, **energy load management**, and **smart infrastructure operations**—key components of the AI-enabled energy solutions landscape. As noted by InsightAce Analytic, AI is increasingly used in the renewable sector for predictive modelling and grid balancing, making KER16 relevant to utilities, renewable plant operators, and green data centres focused on energy optimization[64]. KBV Research also highlights growing adoption of AI in European energy utilities, particularly in applications like power forecasting and infrastructure automation[65].

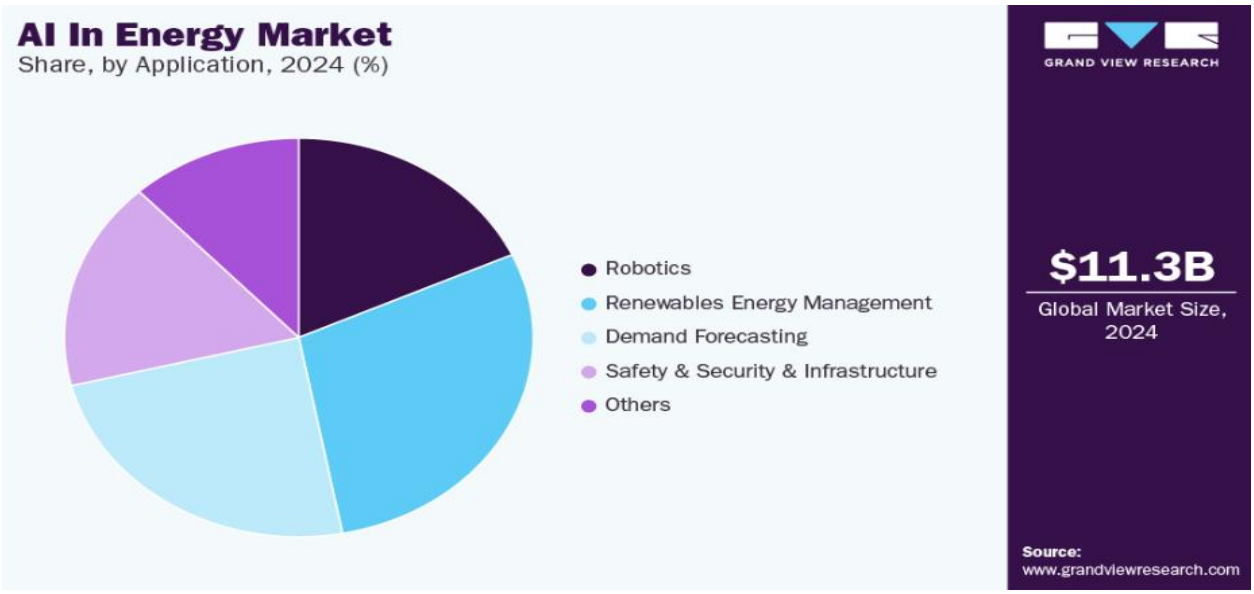


Figure 25: KER16 AI in Renewable Energy Forecasting market segments (source: Grand View Research)

[64] InsightAce Analytic

[65] KBV Research

Size and Growth Rate

As portrayed in Figure 26, the **EU AI in Energy** market was valued at **USD 2.59 billion in 2024** and is expected to grow to **USD 12.06 billion by 2030**, reflecting a **CAGR of 29.3%**[66]. Within this broader space, the **global AI in Renewable Energy** market—which encompasses KER16's core function—is projected to grow from **USD 863.9 million in 2024** to **USD 5.9 billion by 2034**, at a **21.3% CAGR**[67]. The European sub-market is a major contributor to this growth due to regulatory pressure and green infrastructure investments.

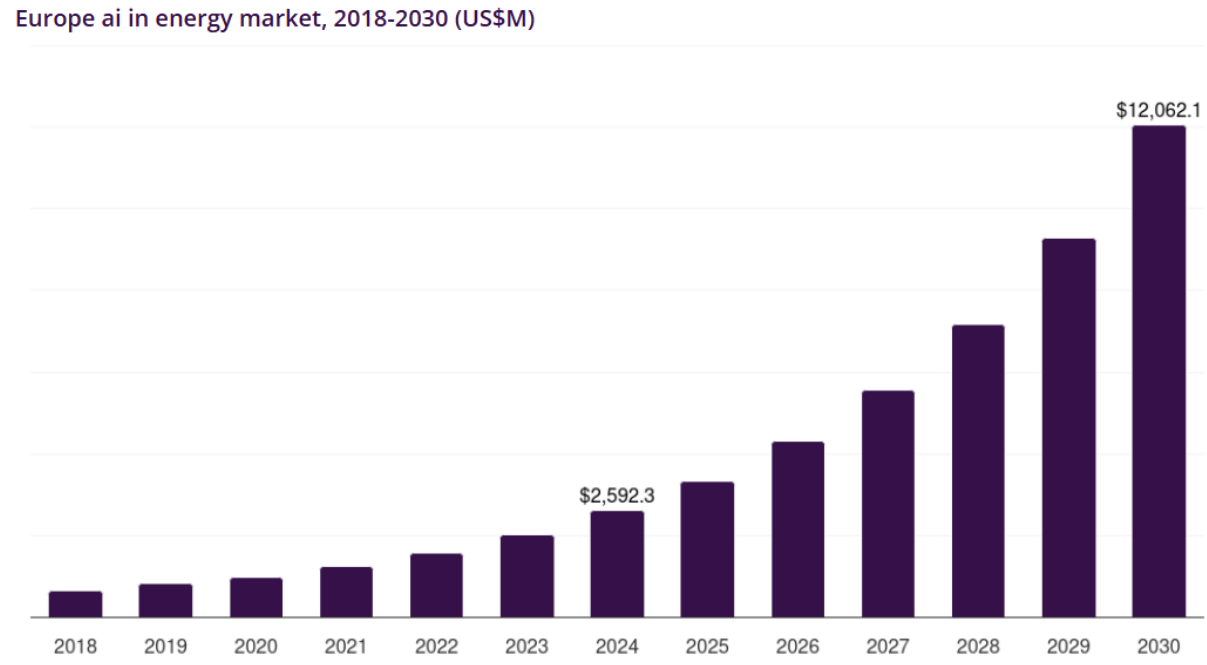


Figure 26: KER16 AI in Renewable Energy Forecasting market size (source: Grand View Research)

Trends

The dominant trends shaping this market—and creating tailwinds for KER16—include the rise of **AI-powered grid optimization**, **energy-aware data centre operations**, and **predictive load balancing**. According to Precedence Research, the rapid increase in intermittent renewable energy (like solar and wind) in Europe is driving demand for AI-based forecasting tools that can stabilize energy supply and reduce reliance on fossil-based peaker plants[68]. Furthermore, "Markets and Markets" emphasizes how utilities and digital infrastructure providers are integrating AI tools into SCADA systems and EMS (Energy Management Systems) to predict energy load, optimize resource usage, and reduce downtime[69].

[66] Grand View Research
[67] InsightAce Analytic
[68] Precedence Research
[69] "Markets and Markets"

KER16 directly supports this transition by enabling automated workload alignment with green energy peaks.

Barriers

Despite promising growth, several barriers may hinder the widespread deployment of KER16. According to Saudi Energy Consulting, challenges such as high upfront implementation costs, regulatory fragmentation across EU member states, and limited AI maturity among traditional energy utilities can delay adoption[70]. Allied Market Research further highlights concerns about data interoperability and cybersecurity in AI-driven systems, especially when using third-party APIs for location-specific forecasting as KER16 does[71]. These issues could require extensive localization, retraining of models, and compliance adaptation on a country-by-country basis.

Opportunities

The European energy market is undergoing a digital revolution driven by the **European Green Deal**, **REPowerEU**, and national decarbonization roadmaps—creating an unprecedented opportunity for AI-powered infrastructure tools. Grand View Research emphasizes the shift toward **green digital infrastructure** that optimizes operations in real time, and KER16's forecasting capabilities directly support this trend[72]. Additionally, as dynamic electricity pricing and time-of-use tariffs gain traction, KER16 offers businesses and data centers an intelligent way to minimize energy costs by scheduling workloads during peak renewable availability[73]. KBV Research projects strong adoption in Germany, France, and the Nordics due to their heavy investments in digital energy platforms and regulatory readiness[74].

6.8.3 Value Proposition analysis

The core value proposition of KER16 lies in its ability to give users the autonomy to **intelligently balance and shift their computational loads** in alignment with renewable energy availability. XLAB developed the **most comprehensive ensemble model in the industry**, capable of making renewable energy forecasts up to five days in advance for any location. This model is embedded in a user-accessible REST API, creating a seamless integration point for energy-intensive infrastructure, such as data centers and enterprise compute clusters.

The solution's automation capabilities significantly **surpass conventional approaches**, providing a holistic infrastructure management tool. The primary objective is to **empower users**—particularly those who consume large amounts of computing power—with the ability to **optimize their operational efficiency**, not just by reacting to energy signals but by **forecasting renewable energy potential** and proactively adjusting workflows. This enables smarter scheduling that aligns with both **cost efficiency**

[70] Saudi Energy Consulting
[71] Allied Market Research
[72] Grand View Research
[73] Precedence Research
[74] KBV Research

and **environmental sustainability**. In essence, KER16 turns infrastructure management into an **informed, forecast-driven decision-making process**, tailored to the user's specific needs.

6.8.4 Barriers, obstacles and analysis of standard regulation

The main **barriers** to KER16's adoption include challenges related to **data input quality** and a broader **reluctance to adopt new technologies**, especially within traditional infrastructure operations where legacy systems dominate. The effectiveness of the ensemble model is highly dependent on accurate and granular data—specifically **weather forecasts, electricity prices, and consumption trends**. Where such data is unreliable or unavailable, the model's output could be compromised, reducing user trust.

Another significant **obstacle** is the **acquisition of high-quality input data**, which remains critical for the model's predictive accuracy. Given the system's reliance on real-time and forecasted information, inconsistencies or delays in this input can undermine the value delivered to end-users. Additionally, **data interoperability and cybersecurity**, as raised in broader market reports (Allied Market Research), pose risks when using third-party APIs, especially when integrated with critical infrastructure like energy or computing systems.

As per the partner, no specific **standards or regulations** were cited for immediate compliance, but it is implied that **localized data adaptation** and possible country-specific constraints (e.g., data protection rules or energy regulations) could affect future scalability. This suggests that regulatory considerations may not yet be fully mapped, which could introduce hidden compliance obligations in the future.

6.8.5 Technology and market watch

The primary active competitor tracked is **Electricity Maps**, whose cooperation with Google is viewed as a serious market risk. This collaboration indicates the potential for large-scale rollout and integration into platforms with global reach and massive user bases (Electricity Maps Client Stories – Google). XLAB is actively **monitoring this development** and considers it a strategic factor in KER16's market positioning.

KER16 differentiates itself by providing **an ensemble forecasting model** that supports infrastructure-level decision-making, rather than just electricity data consumption. However, in terms of technological innovation, the field is rapidly advancing. AI-based forecasting, SCADA system integrations, and Energy Management System (EMS) enhancements are becoming the norm in green infrastructure development, as confirmed by "Markets and Markets" and Precedence Research. Thus, KER16 must continually adapt its capabilities to **remain competitive**, especially with the growing demand for predictive load balancing and time-of-use tariff optimization.

From a strategic standpoint, continued **data model development, adaptation, and retraining** are seen as core technological activities. The team also identifies partnerships with **data providers (e.g., for meteorological or solar input)** as critical to ongoing relevance and performance.

Table 13 below details the input provided by XLAB.

Table 13: KER16 Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date	Link
Active companies and their R&D strategies	Electricity maps	A technology that could push us out of the market, especially with the cooperations of big players as google	Keep on radar	ongoing	https://app.electricitymaps.com/map and https://www.electricitymaps.com/client-stories/google

6.8.6 Business Model Canvas

Business Model Canvas				
Key Partners	**Key Activities**	**Value Propositions**	**Customer Relationships**	**Customer Segments**
XLAB collaborates with data providers, including **meteorological, solar, and electricity market sources**, to feed accurate input into the ensemble model. These partnerships are essential to maintaining forecasting accuracy.	The primary technical focus includes **data model training**, **adaptation**, and **continuous development**, allowing for localisation and refinement based on real-world usage and performance.	Give users the autonomy to **intelligently balance and shift their computational loads** in alignment with renewable energy availability. The **most comprehensive ensemble model in the industry**, The solution's automation capabilities	Engagement is maintained through **ongoing collaboration with data centres**, tailored around their **urgent computational needs** and real-time responsiveness to energy forecasts. Relationships are built on the value of intelligent	KER16 targets **computing providers** looking to add green forecasting as a value proposition, and **computing customers** who seek **energy-efficient infrastructure solutions** aligned with cost and

		significantly **surpass conventional approaches**, providing a holistic infrastructure management tool. In essence, KER16 turns infrastructure management into an **informed, forecast-driven decision-making process**, tailored to the user's specific needs.	workload scheduling and performance efficiency.	environmental goals.
	Key Resources The backbone of the product is high-quality **input data**, including electricity prices, weather forecasts, and energy trends. These resources are essential to ensure prediction accuracy.		**Channels** Outreach is primarily conducted through **partner marketing**, **face-to-face meetings**, and **participation in relevant conferences**, reflecting a high-touch, B2B sales approach.	

Cost Structure	**Revenue Streams**
Fixed costs include infrastructure expenses, such as **cloud servers used for data aggregation and communication**, while **variable costs** involve retraining and developing new models based on evolving data and usage.	The business model is based on **fixed pricing** for the standalone product. The product is **proprietary**, and **integration or customisation services** are offered as additional, negotiable services.

6.8.7 Exploitation Pathway

The exploitation pathway for KER16 is already underway. XLAB has **initiated contact with energy distribution companies** in **Slovenia and Serbia**, as well as with a **Slovenian agency**, to validate and test the product. At this stage, exploitation is focused on **existing client networks** to ensure the robustness of the ensemble model. KER16 is being delivered as a **standalone proprietary product**, not as an open-source solution. However, XLAB also offers **integration and customization services**, which are determined on a **negotiated basis** depending on customer needs and the complexity of deployment.

In terms of revenue, the product follows a **one-time payment model** for the base platform, with **additional services priced individually**. The primary market focus is **B2B**, although **some B2C applications** may be explored, depending on the user's method of energy procurement.

Finally, XLAB has clarified that **no further Horizon Europe funding is currently being pursued**, though it remains open to future opportunities should they arise. The exploitation plan for now focuses on **validating the product in real-world deployments**, refining the model through client feedback, and gradually expanding the customer base within the European green energy infrastructure market.

7 Business and Sustainability Plan for the TANGO Platform (KER17)

7.1 Methodological framework for the designing the Business and Sustainability Plan of the TANGO Platform

The Sections that follow present, in detail, a business plan and analysis for the exploitation plan of the TANGO system and platform. The underlying business plan has been created by INTRA with the help of the TANGO partners. To perform this analysis, we relied on several activities and methodological frameworks, as presented below.

- We applied a structured methodology a structured methodology that combines the Business Model Canvas with the Lean Startup approach, tailored for the context of EU-funded innovation projects. This involves: (1) defining the value proposition based on Key Exploitable Results (KERs); (2) segmenting potential customers and stakeholders across EU markets; (3) validating problem-solution fit through early feedback from target adopters; (4) analyzing market size, competitive landscape, and regulatory factors; and (5) developing a go-to-market and exploitation strategy aligned with Horizon Europe impact pathways.
- Consultations with the Horizon Results Booster Service, where a dedicated expert supported us in designing a tailored business plan for the project. More specifically, we have benefited from 3 distinct service offerings from the Horizon Results Booster:
  - **TANGO 101070052 – Business Plan Development.** The service followed a structured process, starting with the appointment of the Expert in February 2024 and an initial contact with the project in April. Following a maturity assessment and consultation with the ATS and INTRA, it was agreed to organise two capacity-building sessions (June 3 and July 4) and a dedicated half-day BPD workshop. During the preparatory phase, the Expert provided templates, guidelines, and a preliminary report with detailed feedback on the project's initial business model canvas and draft business plan. The BPD session involved a focused group of six participants and aimed to review and consolidate the strategic elements of the TANGO business plan. The last workshop was organised on the 30th of September 2024, to elaborate and discuss on the TANGO system's business plan. In this framework, the key outcomes included the refinement of service bundles, agreement on the need for market segmentation, analysis of the state of the art, and formulation of a clear exploitation strategy. Post-workshop support included additional expert guidance and tools for defining the value proposition and commercial roadmap.
  - **TANGO 101070052 - G2M - Innov. Mgt.** Following the appointment of the Expert, an initial coordination process began, where the purpose of the initial call was to align expectations, review the state of play of the TANGO Platform, and introduce the Exploitation Booster service. Key recommendations were provided to support the project's business planning activities, including refining the value proposition canvases, designing a user journey for the cloud-based platform, developing a robust and sustainable business model, and drafting a business plan and exploitation

roadmap. Two targeted workshops were conducted on May 29th and 31st, 2024, covering topics such as innovation management, customer-driven development, open innovation, and strategic exploitation, with practical tools and case studies to guide the project team in enhancing the commercial readiness of the TANGO solution.

- **TANGO 101070052 - G2M - Support IPR**, where an expert supported use via online session in designing better our IPR Management Strategy.

- Physical workshop during the last GA Meeting of the project in Mallorca, on the 7th of May 2025, which was facilitated by INTRA, FN and DBC with the participation of all project partners. During the workshop, we discussed on the Business Model Canvas elements of the TANGO system, potential exploitation paths that can be followed, IPR Management for the platform (co-ownership by all involved partners), as well as we tried to better define the system's value proposition for the project use cases.

7.2 Product description

The integrated TANGO system constitutes a solution for secure user authentication, authorization, data sharing, which is designed to tackle the problem of real-world challenge of secure, privacy-preserving data sharing across multiple customer sites; it brings together distinct infrastructures into one orchestrated platform. At the core of the system, there are connector instances – comprising of microservices - to both central and pilot-specific Kubernetes clusters. The system has a modular architecture built around three core roles: Provider, Consumer, and Management. Each role runs as a set of containerised microservices on Kubernetes, making it easy to scale and manage.

- The **Provider Connector** shares data securely via verifiable credential APIs and enforces data policies based on attributes.
- The **Consumer Connector** helps users to onboard, authenticate and get authorized to the different services of the platform based on their role using different types of credentials, decrypt information, and verify trust scores—right from their mobile devices or workstations.
- The **Management Connector** oversees system deployments, stores critical artifacts, and enforces security policies using mutual TLS and Kubernetes Role-Based Access Control (RBAC).

The participants to the TANGO system can utilize it for secure data sharing and storage by integrating their data sources into the platform. They can manage data access and sharing permissions, ensuring that only authorized parties can access sensitive information. The system's advanced encryption and identity management features provide robust security, while its seamless onboarding process ensures that new users and devices can be easily and securely enrolled. In parallel, the continuous monitoring and behavioural authentication service further protects against unauthorized access and fraudulent activities, ensuring the highest levels of data security and trustworthiness.

Given the modular architecture of the TANGO system, from a business perspective, it can be offered and deployed to potential customers and end-users as a superset of the components that are needed in each case, forming service clusters of the system that tackle specific problems of the customers/end-users.

Basically, we have selected some prominent pilot cases of the project to serve as service clusters of the TANGO system, serving the business sectors of smart hospitality, smart manufacturing and retail.

- The **smart hospitality cluster** focuses on user-centric services such as digital onboarding, issuance of verifiable credentials, secure client check-in, privacy control, and real-time user experience monitoring.
- The **smart manufacturing cluster** is divided into two industrial pilots (FMAKE and RIAS) both of which share a common focus on data protection, trusted execution environments, behavioural authentication mechanisms and energy-efficient AI operations.
- The **retail cluster** supports privacy-aware customer interaction, secure analytics, and behavioural authentication tools.

The overall business concept of the TANGO's system service clusters is presented in the figure below. The Central Infrastructure of the TANGO system includes also the development and testing environment and associated procedures through a CI/CD (Continuous Integration/ Continuous Delivery) stack of tools following DevOps best practices. The CI/CD stack covers the development plane of the TANGO system offering automated build and testing capabilities, but it is also connected to its operational context by triggering centrally the deployments of TANGO components towards the different service clusters.

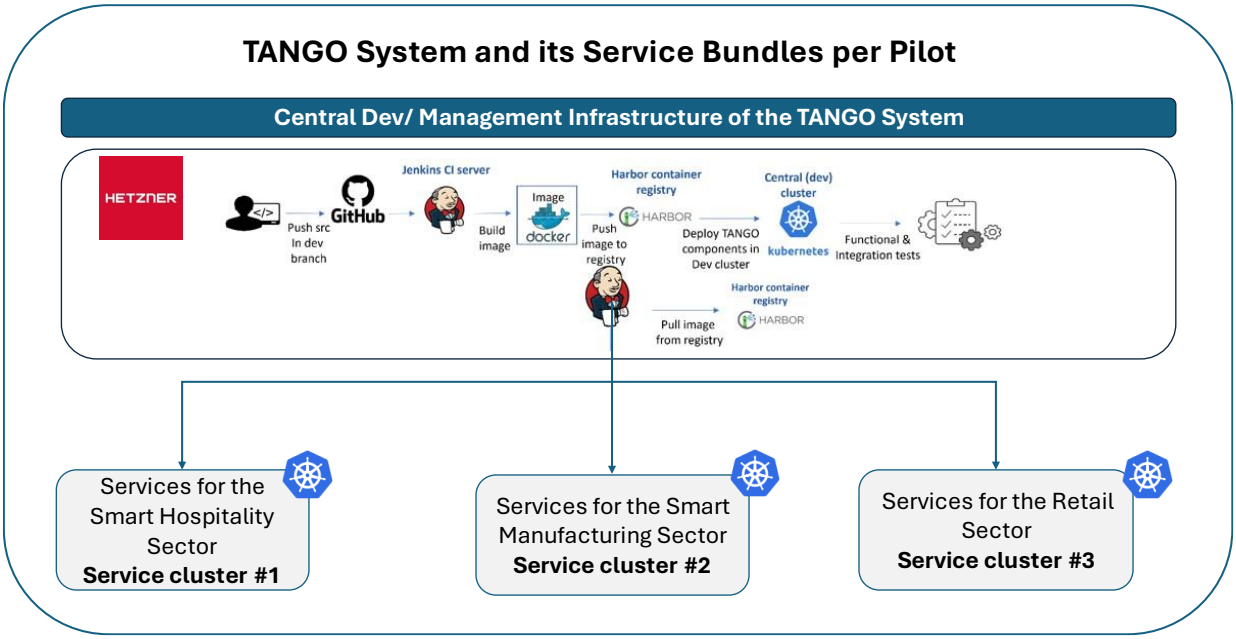


Figure 27: Overview of the TANGO platform as a system of service clusters for specific business sectors

To better understand and clarify the functionalities of each service cluster of the TANGO system, we have mapped TANGO's key exploitable results (ERs) against the three clusters. Each ER represents a concrete technological functionality, designed to support security, privacy, interoperability, and data-driven innovation within and across pilot domains. The TANGO's system ERs per Service Cluster are presented below.

Table 14 ERs per Service Cluster

Exploitable Result (ER)	Service Cluster #1: Hospitality	Service Cluster #2: Manufacturing		Service Cluster #3: Retail
Trustworthiness Scoring Module (TSM)			X	
Ubiquitous Personal Context Vectors (UPCVs)	X			X
Confidentiality and Privacy by Design: PEP and Sticky Policies (PEP/PDP)	X	X	X	X
Confidentiality and Privacy by Design: ABE-toolset	X	X	X	X
Self-encryption and Decryption Techniques with Multi-Factor Information Recovery Mechanisms (SEDSS)		X		
SSI Wallet	X	X	X	X
SSI Agent	X	X	X	X
Seamless onboarding for users (SOUD)	X	X	X	X
User continuous behavioural authentication (UCBA)			X	X
Device continous behavioural authentication (DCBA)			X	
Hardening against Sidechannel Attacks (SCA)	X			
Exploratory Data Analysis engine (EDAE)	X	X		X
Energy efficient AI model training Support for MLOps (MLOps)		X		
Energy efficient AI model training Support for Federated Learning (Fully extensible federated learning framework based on a pipes and filters design pattern- FLEVIDEN) (FLEVIDEN)		X		

Exploitable Result (ER)	Service Cluster #1: Hospitality	Service Cluster #2: Manufacturing		Service Cluster #3: Retail
Energy efficient AI model training Support for AutoML (Auto ML)		X		
Dynamic Intelligent Execution (TornadoVM)	X	X		X
Privacy Assurance Tool (PAT)	X			X
X-AI for Privacy and Trust Enhancement (XAI)		X		
Infrastructure Management based on AI (RENOPS)		X		
TANGO Modular Platform - UI	X	X	X	X
TANGO Modular Platform - VIS	X		X	X

7.3 User Interaction with the TANGO Platform

The TANGO system supports a range of user roles and interfaces, each with specific functionalities aligned to the operational and analytical needs of the underlying sectors. In each cluster, different user roles have been defined as presented below.

Table 15: Defined user roles by service cluster

Domain	Role(s)	Backend Component for Reporting
Smart Hospitality	Manager, Traveller	EDAE
Smart Manufacturing	Manager	DCBA
Retail	Manager	EDAE

Users can perform the following functionalities and business operations:

- Identity verification since users and devices are seamlessly onboarded and verified via self-sovereign identity management systems.
- Sharing important business data, securely with partners and collaborators using privacy-preserving mechanisms.
- Behavioural monitoring for continuous authentication processes so that only authorized users and devices can access sensitive data.
- Data analysis capabilities via exploratory data analysis engine to gain insights from sensitive data.

For smart hospitality service cluster, managers see an interface that provides real-time and historical insights derived from sensor data within hotel environments. These include parameters such as room comfort levels, occupancy rates, and usage trends. In addition, managers can access detailed guest satisfaction reports, which can be filtered by room number, floor level, or specific time periods. On the

other hand, travelers use the system for onboarding and interact with a post-stay interface that delivers personalized feedback centered on the hotel's environmental performance.

The smart manufacturing service cluster enhances the security monitoring capabilities of industrial facilities. Here, there is only the user role of the Manager, who is granted access to a suite of features aimed at identifying and mitigating unauthorized access incidents. Via the dashboard, managers can review logs detailing each unauthorized access attempt.

In the retail service cluster, the system supports managers in managing retail operations across multiple performance dimensions. The interface offers dynamic dashboards which present insights into customer behaviour patterns, individual product performance, and overall store efficiency. Managers can also have access to flexible filtering capabilities, so that data can be segmented and analyzed by parameters like time window, specific retail locations, and product lines.

7.4 Business problems that the TANGO system solves

Companies in many fields, from hospitality and retail to manufacturing, often have IT systems that are isolated, making it hard for people from different companies to work together. For instance, data and procedures are often stuck in "multiple silos" with no way to share or identify them, so companies *"don't have the privacy and security guarantees"*[75] to share information with one other or with partners. This lack of connection causes some bottlenecks. For example, onboarding new workers, partners, or devices is generally done by hand and takes a long time, which makes customers leave (for example, research shows that 67% of banks lost clients because their identity and onboarding processes were too complicated[76]). At the same time, compliance risk has grown a lot as more data privacy rules have been passed. By 2024, almost 75% of people will be subject to modern privacy laws, and regimes like GDPR impose substantial fines for any data mistreatment.[77]

Hence, these standards and the fact that data is spread out make it harder for corporations to come up with new ideas based on data, as they cannot quickly look at sensitive information. So, businesses are just starting to use complex privacy-enhancing analytics (like federated learning or homomorphic encryption)[78] that help them learn things without giving out raw data. Finally, as businesses become digital cybersecurity dangers grow including ransomware, supply-chain intrusions, and other threats are now targeting interconnected infrastructures and IoT deployments. According to industry reports, cyber risk is a major concern, and old or poorly coordinated systems make things much more dangerous.[79] In

[75] https://www.weforum.org/stories/2022/08/do-data-regulation-properly-protect-consumers/#:~:text=Many%20enterprises%20need%20to%20share,the%20information%20within%20regulatory%20requirements

[76] https://www.gleif.org/_documents/gleif-chainlink-paper/gleif-x-chainlink-identity-report.pdf#:~:text=cost%20of%20%242%2C598%20per%20client,3

[77] https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/mckinsey%20on%20risk%20number%2014/mckinsey%20on%20risk%20and%20resilience%20issue%2014.pdf#:~:text=Major%20data%20breaches%20and%20hacking,and%20creating%20new%20compliance%20demands

[78] https://www.weforum.org/stories/2022/08/do-data-regulation-properly-protect-consumers/#:~:text=There%20is%20an%20increasing%20awareness,Crucially%2C%20they

[79] https://www.occ.gov/publications-and-resources/publications/cybersecurity-and-financial-system-resilience/files/pub-2025-cybersecurity-report.pdf#:~:text=38%20Refer%20to%20Implementation%20of,Service%20Providers%2C%20October%2031%2C%202012

short, the TANGO system solves important problems by bringing together different technologies (TANGO components), protecting data interchange, making it easier to onboard new users, enforcing compliance (like GDPR), allowing analytics that protect privacy, and lowering cyber-risk.

7.5 Core Target Markets of the TANGO System

The target market and customers we target for the TANGO system are described below.

Target Market #1: Smart Hospitality Sector

- Mid-to-large scale hotel chains, resorts, and boutique hotels.
- Hospitality technology providers who want to enhance their SaaS offerings with identity verification and customer experience tools.
- Hotels or smart buildings which integrate guest feedback into environmental performance monitoring.

Potential users

User Role	Description
Hospitality Managers	Hotel IT managers or operations directors who are responsible for guest data, operational analytics, and service quality improvement.
Travelers/Guests	End-customers interacting with the hotel's digital systems for onboarding, personalized feedback, and privacy settings.

Target Market #2: Smart Manufacturing Sector

- OEMs and Tier-1 suppliers in sectors like automotive, aerospace, and electronics.
- Industrial automation providers integrating cybersecurity, identity verification, and secure data-sharing for factory operations.

Potential users

User Role	Description
Factory/Plant Managers	Security and IT managers responsible for access control, equipment monitoring, and operational resilience.

Target Market #3: Retail Sector

- Large retail chains, department stores, and e-commerce logistics centers looking to enhance customer interaction while preserving privacy.
- Retail analytics solution providers who need robust data privacy layers in customer analytics platforms.
- Smart shopping centers who deploy behavioural authentication and secure in-store analytics.

Potential users

User Role	Description
Retail Managers	Store operation managers or retail chain executives focusing on data-driven decision-making, customer behaviour, and privacy compliance.

7.6 Market size, trends and analysis

In principle, the TANGO platform aligns with the **data orchestration, governance, and sharing layer** of the European **Data Management Platform** and **Enterprise Data Management** markets. Specifically, it sits at the intersection of three segments: (i) data collection and integration, (ii) secure data access and exchange, and (iii) compliance-driven data governance. According to Future Market Insights, demand is surging for platforms that allow structured and unstructured data from varied sources (e.g., IoT, social, cloud, government) to be harmonized, tagged, and shared securely, which mirrors the architecture and objectives of TANGO's modular platform[80].

The smart hospitality market in Europe alone is expected to expand at a CAGR of about 27.7% from 2022 to 2028.[81] In 2021, smart-hospitality revenue was approximately $18.8 billion, and by 2031, it is expected to reach $133.7 billion (≈22% CAGR).[82]

Industry 4.0/IIoT is also strong in manufacturing. The smart manufacturing market in Europe was valued at $72.2 billion in 2024 and is projected to grow at a compound annual growth rate (CAGR) of about 13.6% to reach ~$159.8 billion by 2030.[83]

The European market for smart retail technology is currently smaller (approximately $11.7 billion in 2023), but it is expanding even more quickly (approximately 28.5% CAGR to 2030).[84]

Notably, Europe already controls a sizable portion of these markets (for example, the EU controls the largest share of global smart-hospitality demand markets and approximately 30.7% of smart-retail spending, according).[85]

All three clusters exhibit double-digit growth, boosted by trends such as the quick recovery of tourism, hotel digitization, Industry 4.0 projects, and retail "smart store" investments. For example, European hospitality chains are making significant investments in IoT and analytics (approximately 75% of hotels plan more digital services).[86]

---

[80] https://www.futuremarketinsights.com/reports/data-management-platforms-market

[81] https://www.researchandmarkets.com/reports/5659096/europe-smart-hospitality-market-size-share-and?srsltid=AfmBOorx89J8tMsoDA2nhPk1KO5k-cQi-wgWcEN8MI-TfJERw1E4aEif#:~:text=The%20Europe%20Smart%20Hospitality%20Market,2028

[82] https://www.alliedmarketresearch.com/smart-hospitality-market-A08160#:~:text=The%20global%20smart%20hospitality%20market,from%202022%20to%202031

[83] https://www.grandviewresearch.com/horizon/outlook/smart-manufacturing-market/europe#:~:text=,CAGR%20from%202025%20to%202030

[84] https://www.grandviewresearch.com/horizon/outlook/smart-retail-market/europe#:~:text=Europe%20smart%20retail%20market%20highlights

[85] https://www.arketsandarkets.com/Market-Reports/smart-hospitality-market-93242156.html#:~:text=Europe%20is%20estimated%20to%20hold,of%20the%20smart%20hospitality%20market

[86] https://www.deloitte.com/nl/en/Industries/transportation/research/european-hotel-industry-and-investment-survey-2024.html

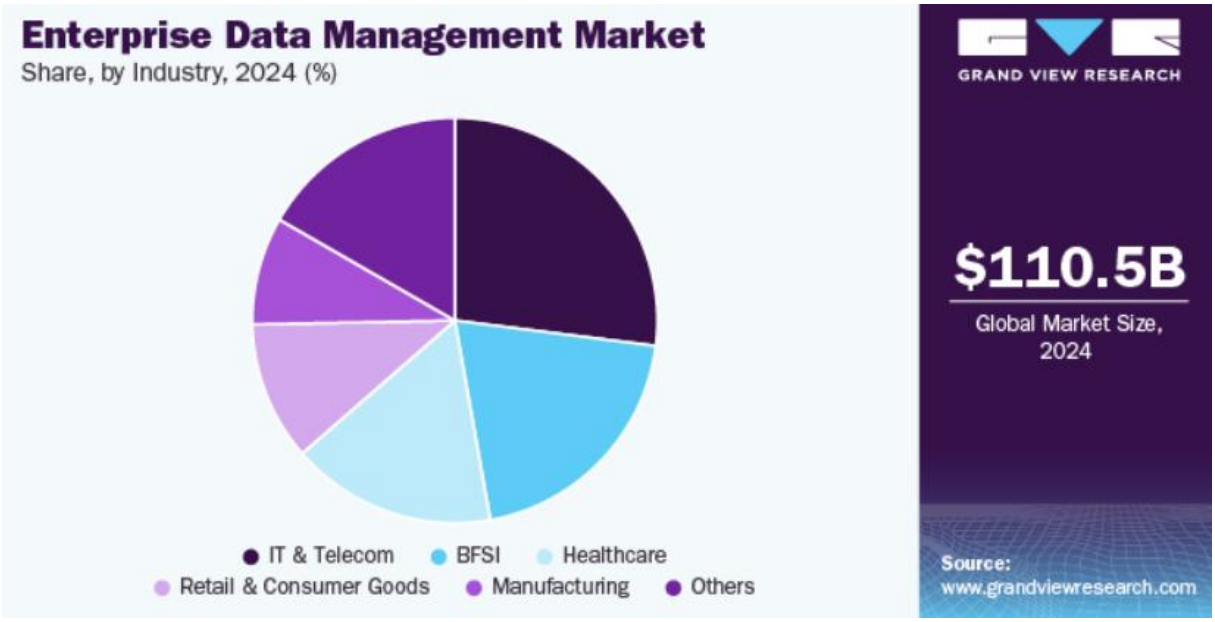
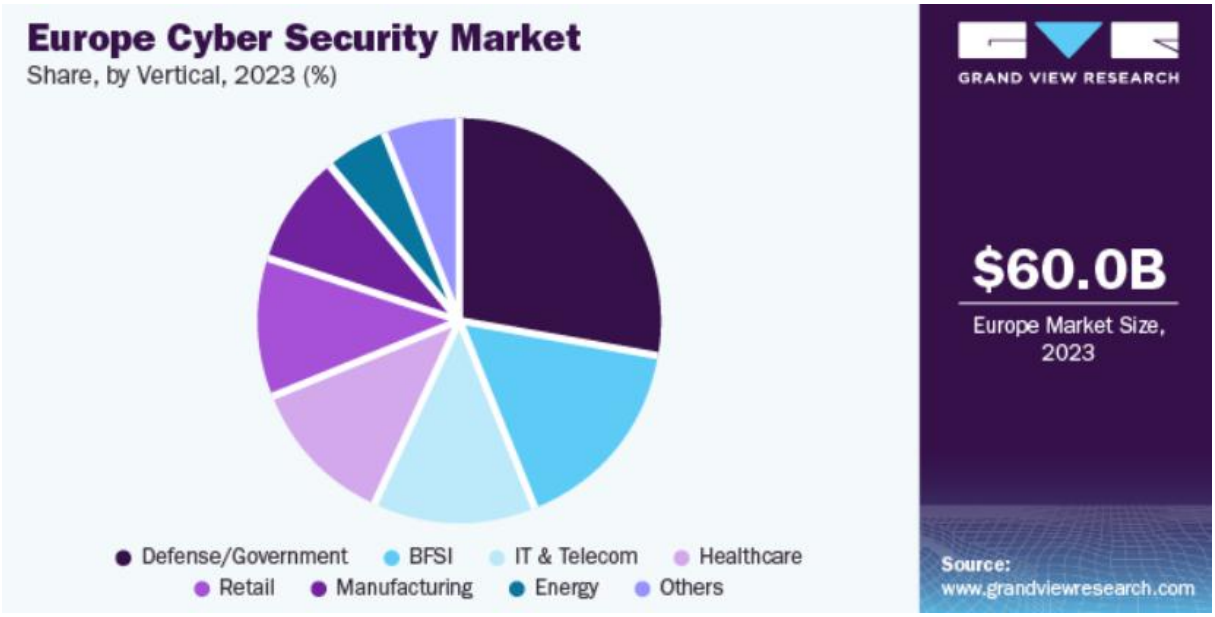
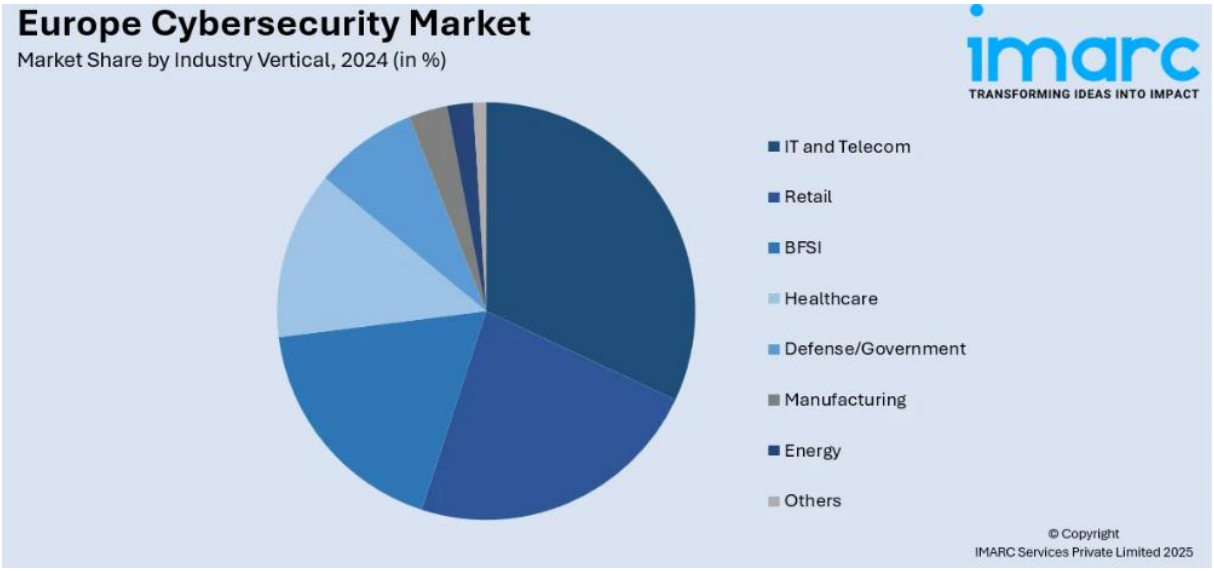


Figure 28 Market size for the TANGO Platform (source: Grand View Research)

Its inclusion of privacy-enhancing and decentralized identity features also embeds it firmly in the **cybersecurity data governance and privacy compliance** subsegment—critical in regulated verticals like finance, mobility, and public administration, as noted by "Markets and Markets"[87].

[87] https://www."Markets and Markets".com/Market-Reports/cyber-security-market-505.html


Europe Cyber Security Market
Share, by Vertical, 2023 (%)
Defense/Government
BFSI
IT & Telecom
Healthcare
Retail
Manufacturing
Energy
Others
GRAND VIEW RESEARCH
$60.0B
Europe Market Size, 2023
Source:
www.grandviewresearch.com


Europe Cybersecurity Market
Market Share by Industry Vertical, 2024 (in %)
imarc
TRANSFORMING IDEAS INTO IMPACT
IT and Telecom
Retail
BFSI
Healthcare
Defense/Government
Manufacturing
Energy
Others
© Copyright
IMARC Services Private Limited 2025

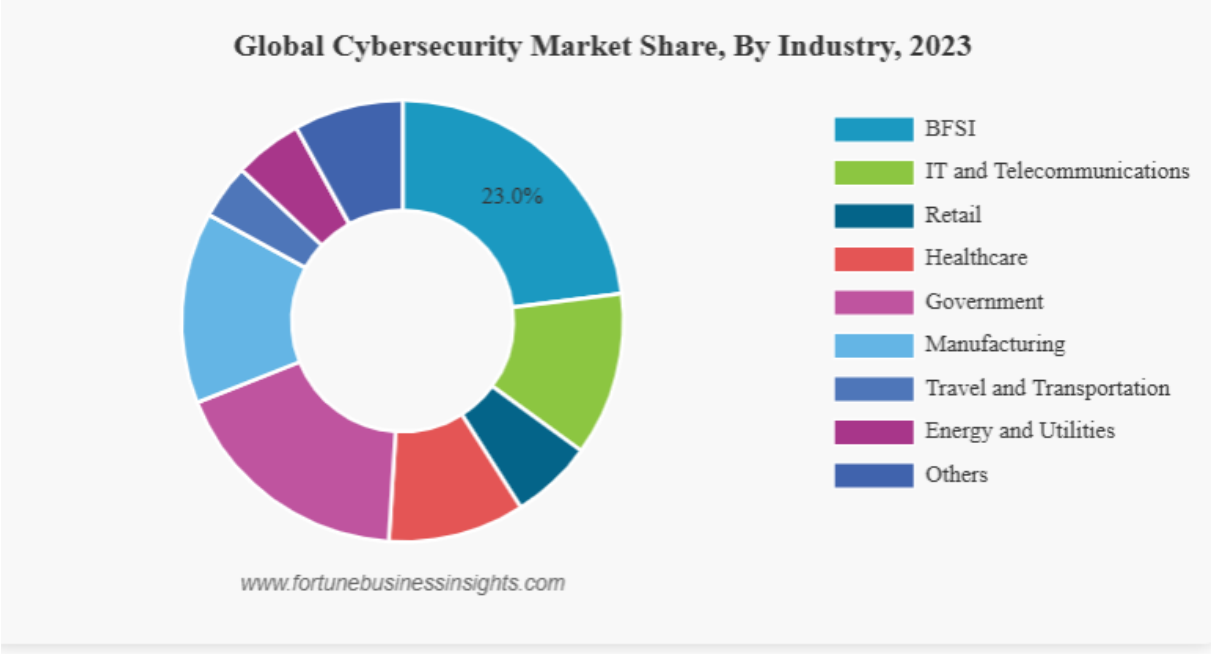


Figure 29 Europe and Global cybersecurity Market (source: Grand View Research)

Market Size and Growth Rate

The **European Data Management Platform (DMP)** market is experiencing robust growth, driven by increasing volumes of privacy-sensitive data and the need for contextual decision-making. The market is projected to expand at a CAGR of over **13.5%** during 2024–2030, with Europe contributing a significant portion due to digital transformation across enterprises[88]. Meanwhile, the **Enterprise Data Management (EDM)** market globally was valued at **USD 94.6 billion in 2023** and is expected to reach over **USD 189 billion by 2032**, growing at a **CAGR of 8.1%**, according to Precedence Research[89]. Europe, led by Germany, France, and the Nordics, is a central growth hub due to stringent GDPR enforcement and rising public-private data collaborations.

[88] https://www.marketresearchfuture.com/reports/data-management-platform-market-4573
[89] https://www.precedenceresearch.com/enterprise-data-management-market

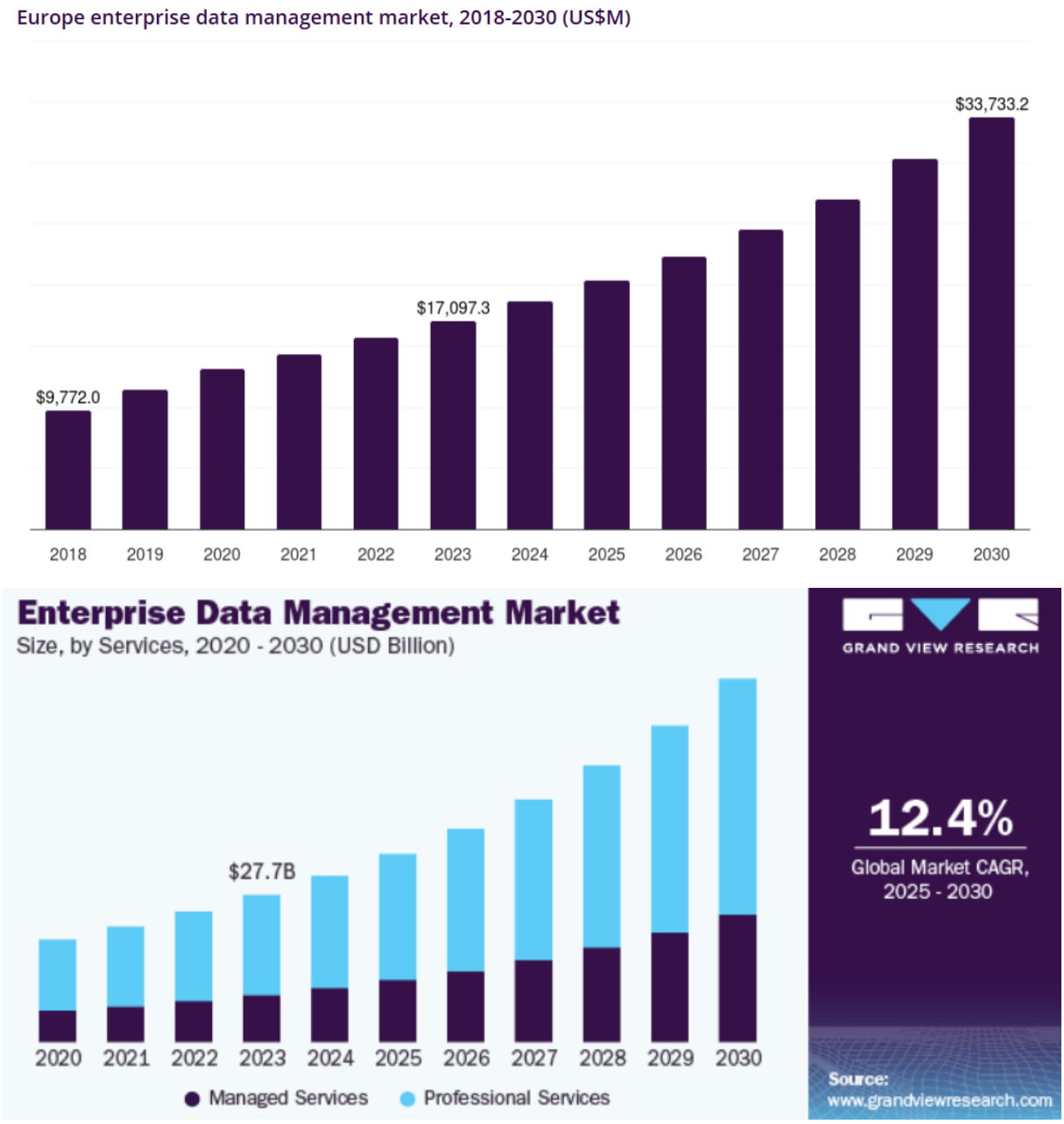


Figure 30: Europe and Global Enterprise Data Market (source: Grand View Research)

Trends

Several key trends across these markets converge in support of the TANGO platform's vision. First, the rise of data sovereignty and decentralization - driven by EU regulations like the Data Governance Act and Data Act - is accelerating demand for modular, interoperable, and standards-compliant data

platforms. Grand View Research highlights that the shift from centralized repositories to federated and edge-based data architectures is a defining characteristic of next-gen data management solutions[90].

Second, there's a sharp increase in GDPR-aligned identity solutions as governments and corporations seek to enable cross-border data sharing without compromising compliance, a challenge that the TANGO platform directly addresses through its sovereign identity integration[91]. On the cybersecurity side, Mordor Intelligence notes the rise of Zero Trust Architecture (ZTA) and secure multi-party computation as essential for trusted data access across distributed networks; again aligning with TANGO's privacy-enhancing cryptographic components[92].

Barriers

Despite favorable trends, TANGO platform faces notable adoption hurdles. A primary challenge is the lack of standardization and maturity in pan-European data sharing ecosystems. According to Grand View Research, many enterprises still rely on siloed legacy systems, complicating the adoption of decentralized or modular frameworks such as TANGO[93]. Furthermore, integration with legacy IAM systems, data lakes, and analytics tools poses a technical onboarding barrier, particularly for public sector stakeholders that operate under strict procurement and interoperability constraints[94].

On the cybersecurity side, while regulation creates opportunity, it also introduces complexity. "Markets and Markets" notes that growing regulatory scrutiny increases the cost and complexity of compliance for multi-tenant platforms operating across borders[95]. Additionally, the need for trust and transparency in decentralized data governance remains a challenge, as many organizations remain reluctant to share sensitive datasets outside their control.

Opportunities

The TANGO platform is well-positioned to capture emerging demand in Europe's sovereign data ecosystem initiatives such as GAIA-X, IDSA, and European Data Spaces. Straits Research highlights that European industries are increasingly investing in platforms that offer customizable data sharing frameworks, trust mechanisms, and integration with eIDAS 2.0—TANGO's architecture supports all three[96].

Furthermore, as enterprises seek to unlock data monetization and reuse across ecosystems, solutions that balance security, privacy, and interoperability will become indispensable. Persistence Market Research projects strong growth in data collaboration software designed for GDPR-compliant usage across multiple stakeholders, particularly in sectors like healthcare, manufacturing, and public services[97]. TANGO's modularity allows it to serve as a bridge between siloed architectures and evolving cloud-edge deployments.

[90] https://www.grandviewresearch.com/industry-analysis/enterprise-data-management-market
[91] https://www.grandviewresearch.com/horizon/outlook/enterprise-data-management-market/europe
[92] https://www."Markets and Markets".com/Market-Reports/cyber-security-market-505.html
[93] https://www.grandviewresearch.com/industry-analysis/enterprise-data-management-market
[94] https://www.marketresearchfuture.com/reports/data-management-platform-market-4573
[95] https://www."Markets and Markets".com/Market-Reports/cyber-security-market-505.html
[96] https://straitsresearch.com/report/database-management-platform-market
[97] https://www.persistencemarketresearch.com/market-research/data-management-platforms-market.asp

7.7 Competition analysis and alternative solutions

We also conducted a competition analysis for our key service clusters in TANGO, as presented in this Sub-Section.

- For the hospitality tech domain, we identify established vendors (e.g. Cisco, Schneider Electric, IBM, NEC, Huawei) who offer hotel automation and PMS solutions
  - Niche leaders like Sonifi (an IoT guest-room platform) are also cited by hotel professionals.
  - Many competitors provide "smart room" devices (locks, controls) or integrate with property management systems.
- For the domain of smart manufacturing (Industry 4.0), there are major industrial IoT providers – Siemens, ABB, GE, Rockwell Automation, Schneider, Honeywell, etc. – who dominate with automation platforms. They supply both hardware (PLCs, robots) and software (MES, analytics).
- For the retail segment, there are global tech giants (Amazon, Cisco, IBM, Alphabet/Google, etc.) are moving into retail IoT and analytics.

7.8 SWOT analysis for the TANGO Platform

The SWOT analysis outlined below aims to provide a structured and critical evaluation of the TANGO Platform's internal and external environment, with the goal of guiding future exploitation strategies and promoting sustainable market deployment. This analysis examines the strengths and weaknesses inherent to the platform's technical and organizational structure, as well as the external opportunities and threats arising from the changing technological, regulatory, and market conditions. The TANGO Platform, as a Key Exploitable Result (KER17), serves as the flagship output of the project and incorporates a wide range of modular, privacy-preserving, and trustworthy technologies. It responds to the growing demand for secure, interoperable, and citizen-focused data management solutions across various sectors. Therefore, the SWOT analysis acts as a strategic tool to determine the current position of the platform, forecast potential adoption challenges, and identify advantageous conditions that can be exploited to support its future deployment in both commercial and non-commercial settings. The four components of the SWOT analysis are presented in the sections below:

Strengths

The TANGO Platform's principal strength lies in its modular, secure-by-design architecture that supports decentralized and privacy-preserving data sharing across diverse sectors. Unlike monolithic data platforms, TANGO is built around three distinct service clusters (smart hospitality, manufacturing, and retail) demonstrating flexibility in responding to domain-specific needs. Technologically, it integrates a wide range of cutting-edge features such as self-sovereign identity (SSI), behavioural and device authentication, and confidential computing via ABE and sticky policy enforcement. Furthermore, it is fully aligned with key European regulations such as GDPR and eIDAS 2.0, which enhances its legal readiness and potential for institutional adoption. Its compatibility with GAIA-X and IDSA standards positions it as a compliant and future-proof component within the emerging European data ecosystem. The emphasis on energy-efficient AI, federated learning, and zero-trust principles also increases its appeal in terms of sustainability and trustworthiness, two major pillars of modern digital infrastructure.

Weaknesses

Despite its innovative design, the TANGO Platform faces certain internal limitations. Its complexity, encompassing both technical setup (e.g., Kubernetes orchestration, containerized microservices,

DevOps practices) and integration with existing IT infrastructures, could hinder rapid deployment, especially for small to medium-sized enterprises (SMEs) or conservative public bodies. The requirement for a high level of IT maturity among users may delay adoption in less digitally advanced sectors. Furthermore, the platform's co-ownership structure among multiple consortium members might impede streamlined decision-making, governance, and post-project commercialization. From a product maturity perspective, some advanced components (e.g., continuous behavioural authentication or FLEVIDEN for federated learning) still need validation under real-world load conditions to confirm performance, scalability, and reliability.

Opportunities

The TANGO Platform is well-positioned to benefit from several strategic developments in the European digital landscape. The growing policy and market focus on sovereign data sharing frameworks, as demonstrated by initiatives such as the European Data Spaces, the Data Act, and the AI Act, creates a strong demand for solutions that incorporate data protection, accountability, and trust by design. TANGO's alignment with GAIA-X principles enables integration with wider federated infrastructures, while its modular design allows for targeted entry into high-growth sectors such as e-commerce, smart mobility, sustainable tourism, and smart manufacturing. Additionally, its capacity to support new business models centered on data monetization, regulatory compliance, and secure interoperability (including cross-border data flows) makes it especially appealing to organizations seeking a competitive edge in the digital single market. Its privacy-enhancing technologies also enable it to serve as a facilitator for GDPR-compliant AI applications and analytics.

Threats

On the external front, several threats could hinder the successful deployment and long-term adoption of the TANGO Platform. One significant challenge is the inertia and fragmentation of legacy IT systems, especially in sectors where standardization and interoperability are lacking. Public administrations and some enterprises may resist adopting decentralized models due to perceived complexity or lack of internal expertise. Additionally, competing solutions from large incumbents (e.g., AWS, Microsoft, Google Cloud) might offer integrated but proprietary alternatives with established client bases, aggressive pricing strategies, and broader support ecosystems. Regulatory uncertainty or slow adoption of frameworks like eIDAS 2.0 and GAIA-X could also delay the development of a fully mature European market for sovereign data infrastructure. Finally, although TANGO promotes energy-efficient AI, its resource-intensive features (e.g., behavioural monitoring, federated learning orchestration) may raise concerns over computational overhead, particularly in carbon-conscious sectors.

7.9 PESTLE Analysis for TANGO Platform

The following PESTLE analysis offers a macro-environmental assessment of external factors affecting the sustainability, adoption, and long-term impact of the TANGO Platform. As a cross-sectoral, privacy-preserving, and modular data management system, the TANGO Platform operates within a complex and highly regulated European environment. It is directly influenced by political, economic, social, technological, legal, and environmental factors at both EU and national levels. This analysis aims to highlight the external conditions shaping the market readiness and regulatory compliance of the TANGO solution. It also provides insights into the ecosystem where the platform can be further developed, scaled, or integrated after the project. The six components of the PESTLE framework are presented in the sections below.

Political

The TANGO Platform aligns well with the EU's strategic political agenda surrounding digital sovereignty, secure data spaces, and the protection of citizen rights in the digital age. European initiatives such as the Data Governance Act, the Data Act, and the European Strategy for Data offer a supportive political framework that encourages the development of decentralised and interoperable platforms like TANGO. Furthermore, TANGO is designed to operate in accordance with frameworks such as GAIA-X and IDSA, which are politically backed efforts to build federated data infrastructures among member states. These initiatives provide political legitimacy and promote public sector adoption. However, political fragmentation or inconsistent commitment to these frameworks across member states might hinder harmonised uptake.

Economic

From an economic perspective, the TANGO Platform meets increasing demand for affordable and compliant data-sharing tools, especially within fast-growing sectors such as hospitality, manufacturing, and retail. These industries are increasingly investing in digitalisation and data governance, and TANGO's ability to lower costs related to onboarding, compliance, and cybersecurity provides a measurable return on investment. Market trends show strong CAGR across all three sectors, with the European smart manufacturing market expected to reach nearly €160 billion by 2030, and smart hospitality and retail even surpassing these growth rates. TANGO's modular structure allows for selective deployment of components, making it cost-effective for both SMEs and larger companies. However, its value must be clearly demonstrated to compete with dominant private cloud providers that may offer bundled, lower-cost proprietary solutions.

Social

Socially, the TANGO Platform responds to growing public concerns about data privacy, trust, and control over personal information. Citizens are becoming more aware of their digital rights, and public discussions are shifting towards responsible data use, ethical AI, and transparency in algorithmic decision-making. By including features such as self-sovereign identity, behavioural authentication, and user-focused privacy settings, TANGO empowers users to manage their data and interactions. The platform also offers citizen-facing dashboards and interfaces, which encourage digital inclusion. However, societal adoption depends on building trust, clearly communicating benefits, and educating users, especially when dealing with new concepts like decentralised identity or federated learning.

Technological

TANGO is at the forefront of technological innovation in distributed data management, privacy-enhancing technologies (PETs), AI-based orchestration, and secure authentication mechanisms. Its architecture combines verifiable credentials, dynamic access control, and DevOps-based CI/CD practices for modular deployment. Furthermore, TANGO utilises cutting-edge frameworks for energy-efficient AI, federated learning, and explainable AI (XAI), supporting both performance and transparency. These features directly address significant gaps in existing platforms. However, integration with legacy systems and interoperability with diverse infrastructures (particularly in the public sector) continue to pose technological challenges. The absence of pan-European standards for decentralised data sharing could also restrict cross-border scalability.

Legal

The TANGO Platform has been designed to ensure compliance with current and emerging European legal frameworks, notably the General Data Protection Regulation (GDPR), the eIDAS Regulation, the Cybersecurity Act, and the AI Act (Regulation EU 2024/168). It incorporates privacy-by-design

principles, supports consent management, and provides granular data governance through policy enforcement modules. As noted in D8.3, its functionalities—such as verifiable credential issuance, encrypted onboarding, and behavioural analytics—enable legally compliant data exchange across domains. Furthermore, the platform facilitates adherence to commercial and consumer protection laws, where applicable. However, navigating co-ownership of platform components and defining post-project IPR and liability models will be essential to ensure legal clarity and long-term exploitability, especially in collaborative or multi-tenant environments.

Environmental

Environmental sustainability is a core objective of the TANGO Platform. Its architecture promotes eco-friendly computing through energy-efficient AI, local data processing (to decrease reliance on cloud resources), and dynamic execution technologies that minimise energy use. The platform advocates for edge-based analytics and federated model training, which reduce data transfer overheads and carbon emissions. These features align with the European Green Deal's vision for sustainable digital transformation. In the hospitality and manufacturing sectors, TANGO's environmental monitoring dashboards and optimisation tools (e.g., real-time energy visualisation) directly support sustainability objectives. However, the energy impact of elements such as continuous monitoring or machine learning orchestration should be transparently benchmarked to validate environmental claims.

7.10 Unique Selling Point USP - Unique Value Proposition UVP

TANGO offers a secure and interoperable data management system that enhances data privacy, integrity, and trust, with an improvement in privacy control and security over traditional centralized systems. The use of the system reduces privacy violations and delivers optimal performance and efficiency, ensuring compliance with industry-specific regulations and generating new revenue streams for adopters.

1. Through decentralized identity management (eIDAS/OpenID compatibility), TANGO offers faster user verification processes and improvement in data access control.
2. ePassport usage will enable companies and citizens to comply with (future) EU regulations.
3. TANGO's energy-efficient AI and dynamic intelligent execution reduce energy consumption compared to conventional systems.
4. It can help companies to meet sector-specific regulations on data and security like GDPR, eIDAS, and banking regulations.
5. TANGO enables secure data sharing that facilitates new revenue streams from data monetization, estimated to increase revenues by 10-15% due to its ability to share customer insights securely across partners.[98]

We have also made an exercise to identify the value proposition per service cluster, as follows.

For the smart hospitality service cluster:

[98] Studies and reports show that data monetization efforts can contribute up to 10-20% of company revenues in high-performing businesses. https://cdp.com/articles/data-monetization-cdp-2/ and https://revelate.co/blog/data-monetization-business-model/

- Faster check in and registration of guests, paperless via their phones using secure digital IDs—no front-desk lines. Guests spend less time in check-in. Faster registration. The receptionist can accommodate more people – increase effectiveness.
- Managers view live dashboards of temperature, lighting and occupancy to adjust settings instantly and cut energy costs.
- Travelers choose exactly what data they share, then get tailored offers (e.g., spa discounts) without any privacy worries.

For the smart manufacturing service cluster:

- Behavioural analytics flag unusual log-ins or deviations in real time, so proactive mitigation of breaches before they happen.
- Run AI models on local edge devices securely, cutting cloud compute bills—and carbon emissions.

For the retail service cluster:

- Store managers see sales trends and customer flow, without ever viewing personal shopper data; this enhances tailored promotions and increases the ROI of promotions and marketing campaigns.

7.11 Societal benefits and impact of the TANGO system

The TANGO system brings together identity management, secure data sharing, and privacy-preserving analytics into a single, modular platform. This gives society and the economy measurable value by helping organizations protect people's privacy rights and build trust in digital services, which lowers fraud, data breaches, and regulatory fines. It also makes it easier for customers and employees to get started with digital services. TANGO saves a lot of money on configuration, compliance, and security management by automating manual tasks and bringing together fragmented IT infrastructures. It also speeds up the time it takes to bring new services to market by using reusable microservices and opens up new revenue streams through advanced data-driven insights (for example, personalized guest experiences, predictive maintenance in manufacturing, and privacy-aware retail analytics). In addition, its support for energy-efficient AI and federated learning models encourages sustainable operations, which helps the company make money and also helps the environment and society as a whole.

7.12 Settings – legal and regulatory aspects

Having in mind the nature of the provided services through the platform, the applicable legal and ethical framework affecting its operations could be related to:

- Data protection legislation (GDPR, national legislation)
- Regulations related to cybersecurity, in order to ensure secure data exchange (such as for instance **Regulation (EU) 2019/881**)
- The Artificial Intelligence related framework (Regulation EU 2024/168), alongside the ALTAI requirements
- Commercial law and especially to the consumers protection legislation (Directives such as the Modernisation Directive (EU) 2019/2161), since the platform will be used by consumers (although this is not directly linked to the platform provider but to the entity utilizing the platform in order to provide the services)

In general, depending on the expected by each entity, several applicable laws may be identified, related to their operations per se. Since the TANGO framework will be used for the purposes of provision of

the relevant services and is in a way directly linked to them, the relevant legislation may apply on its function, for instance in terms of the provision of specific information to the consumers as a result of applicable commercial legislation.

7.13 Marketing Strategies and Channels

We aim to employ several channels in order to engage stakeholders and marketise the project offering via the platform:

- **Create strategic partnerships and promotion via events and marketplaces**. We aim to collaborate with technology providers and industry leaders to enhance credibility and reach. In parallel we publish white papers, research reports, and participate in industry conferences to establish TANGO in the domains of interest.
- Showcasing TANGO at sector-specific exhibitions (e.g., Advanced Factories, Smart Retail Tech, Hospitality Tech Europe) to attract leads, conduct live demos, and build credibility.
- Upload the TANGO KER on the Horizon Results Platform to enhance their visibility.
- Via the TANGO website, so that stakeholders and customers can learn more about the project offerings.
- Leveraging established EU-wide networks to co-promote TANGO's capabilities and access SMEs and public sector organisations interested in secure data sharing and digital transformation.
- **Market penetration by using our project use cases as initial adopters**. For instance, we aim to target specific industries with tailored solutions and case studies, based on the outcomes of the pilot use cases.

7.14 Go-to-market and Use model of the TANGO system

A realistic pricing model would combine **software licensing** with ongoing services. In principle, we foresee 3 core use models for the TANGO system, after the end of TANGO.

- **Use model #1**: We foresee exploitation of the system via a **licensing agreement**. A license could be offered to potential end-users/ customers (mostly in the 3 core service clusters of TANGO). The licensing agreement will define the specific use terms, duration, and pricing, among other things. A yearly licensing fee should be expected for the use of the as is version of the TANGO system, and for some basic deployment support and support for maintenance. The duration of the license will depend on the needs of the end user. On top of that, if extra features are needed by the end user, a service contract be established, and TANGO partner could charge person months pending on the effort needed to develop the new features. For organizations with strict data sovereignty and security requirements, TANGO system could be offered via an on-premises installation of the whole platform. This option could include setup, configuration, and ongoing maintenance support, ensuring compliance with local regulations and internal policies.
- **Use model #2**: **An IT consulting and customization service model**; offering expert help to customers who want to make the system work better for their specific needs. Some of the services which could be offered are: aligning business processes, adapting technological architecture, integrating IT and OT, and helping with compliance (for example, GAIA-X and GDPR). This model will be based on a fee-for-service and time-and-materials system. For example, workshops cost between €2,000 and €5,000, engineering services could cost between €800 and €1,200 per day, and

training packages cost between €5,000 and €12,000. Of course, these are just some indications, since prices will depend on the scope, the industry, and how much customization is needed.

- **Use model #3**: We could also scale the components of TANGO and the system as a whole via new research projects which are closer to the market, for instance, moving from an RIA project to an IA (Innovation Action) project. The transition from an RIA (low TRL, focus on research and proofs-of-concept) to an IA (high TRL, close to market) is a good way to exploit the validated components of the system and the system itself in new use case scenarios, or even in adjacent domains; and of course re-use the frameworks, APIs, and orchestration templates created in the project.

7.15 IPR of the Foreground and Partners' Roles in Exploitation

In line with the consortium agreement, and as reported in the Innovation Management Log of the project, the TNAGO system and integrated platform is protected with Copyrights and the underlined know-how with confidentiality. The system's individual components are owned by their creators, as highlighted in the Results Ownership List. The integrated version of the TANGO platform all partners who contribute act as owners, making a co-ownership scheme (all the partners who contribute with components, and the ones who contribute with connectors and the CI/CD stack). INTRA, as an industrial partner, also acts as co-owner of the system, and could be just for communication purposes, the exploitation partner point of reference.

7.16 Future Exploitation Roadmap

The consortium's post-project goal is to (i) further promote the service clusters of the TANGO system and acquire extra initial adopters, (ii) make collaborations with providers and vendors to enhance the TANGO offering, and (iii) increase the TRL of the components and the system as a whole; either by adding new functionalities or by testing the system in new use case scenarios (TRL from 5-6 to 7-8).

Actions:

- Identify 2–3 strategic pilot sites among project partners or external stakeholders (e.g., municipalities, hospitals, logistics hubs, manufacturing plants).
- Co-create pilot execution plans with end users and align their operational needs with the platform's functionalities.
- Apply for new funding research projects.
- Present the TANGO offering in industrial fairs to gain access to potential initial adopters.
- The overall business and exploitation framework for the TANGO system is ready. We know what we offer, whom might be interested and we also have an exploitation plan; we know how to offer the system from an exploitation/business perspective to potential initial adopters and customers.

Some KPIs we could consider in order to assess post project exploitation actions are:

- Number of licenses granted
- Revenues or cost savings generated
- Number of end-users reached
- TRL progression post-project
- Publications, citations, or standards contributions

7.17 Business Model Canvas Methodology

To better analyse the business prospects of the TANGO Platform, we also made an analysis of making a business model canvas that depicts our view for the TANGO Platform as a whole (having of course in mind, that the platform will be offered via service bundles of specific components, and not as a one size fits all solution). Each service bundle of the TANGO platform serves a different market and vertical. We use the Business Model Canvas (BMC)[99] methodology, since it provides a structured way to analyse the value creation, delivery, and capture mechanisms of the platform developed in TANGO. The BMC enables all stakeholders—technical partners, end users, and business developers—to align on key aspects such as value proposition, customer segments, channels, and revenue streams. It is widely recognized for simplifying complex strategic management concepts into practical visual frameworks.

[99] The Business Model Canvas was developed by Strategyzer, a Swiss-based company founded by Alexander Osterwalder, who co-authored the influential book "Business Model Generation".

7.18 Business Model Canvas of the TANGO Platform

Key Partners

- Technology providers for integration
- Regulatory bodies for compliance
- Industry associations for outreach and credibility
- Cloud service providers for infrastructure support
- European data spaces organisations
- IDSA
- GAIA-X
- BDVA

Key Activities

- Developing and maintaining the platform
- Customizing solutions for different industries
- Marketing and outreach
- R&D

Key Resources

- Tech infrastructure (physical and cloud)
- SW engineer and developers
- Project managers
- Intellectual property and proprietary technologies

Value Propositions

- Enhanced data sharing using novel technologies
- Improved identity management
- Improved data privacy and confidentiality of information
- Faster check in for guests. Greener check in. Better experience for guests.
- Hotel reception can accommodate more people so, the efficiency is increased.

Customer Relationships

Personalized consulting services
Tier 1 support (basic) to the end user
We can help the with basic integration/ customisation per use case support

Channels

- Online platforms and marketplaces
- Industry conferences and events
- Strategic partnerships and alliances
- Direct sales teams of industrial partners in TANGO
- Via IDSA marketplace

Customer Segments

- Hospitality providers (hotels, booking platforms)
- Manufacturing companies
- Retailers (supermarkets, supply chains)

Secondary markets

- Event organisers (e.g., for concerts, football matches, etc.)
- Technology providers and IT services

Cost Structure	Revenue Streams
▸ Technology infrastructure and maintenance ▸ Marketing and sales expenses ▸ Personnel costs ▸ Compliance and regulatory costs	▸ Licensing fees for the service clusters (using the TANGO system) ▸ Consulting and customization services (for new use cases and customisation of existing proprietary solutions of partners into new contexts based on customers' needs) ▸ New projects based on the platform components (and knowledge gained in the project -> from RIA to IA)

8 Exploitation Conclusions

The deliverable at hand represents a significant asset in project TANGO as it provides the consortium with a clear overview on the progress of the communication, dissemination and exploitation activities conducted so far. The following are the main highlights of the deliverable. The deliverable provides a report on the joined efforts of the consortium to effectively communicate and disseminate the project's results, with an update on the KPIs status that are under way on reaching the target value by the end of the project. The information provided is essential to all the partners in order to monitor the progress made so far and for the WP leader to coordinate the joint efforts towards the final outcome of TANGO's impact on society and its long-term success. The deliverable also offers a comprehensive a well-structured plan for the innovation management and exploitation activities, outlining the legal requirements regarding the IPR allocation and protection, the exploitable results of the project identified until now and the initial exploitation activities for the 5 prioritized KERs, including the actions put in place for the standardisation activities. The outlined information is essential for the consortium in order to validate the potential for further exploitation of the project results. The deliverable provides a well-developed and detailed SWOT and PESTLE analysis; moreover the 5 prioritized KERs of the project have been further analysed and examined by the SWOT and PESTLE analysis introduced in Section 5. The Business Model Canvas of 1 prioritized KER is also presented as part of the exploitation activities. In conclusion, the efforts of the consortium on the communication, dissemination and exploitation of TANGO for the first 18 months of the project have been successful. In the next version of the deliverable, the definitive overview on the impact of communication and dissemination will be provided, along with the final list of ERs following the project's technical developments.

Some conclusions from FN's work:

Deliverable D8.2 presents a comprehensive analysis of the exploitation potential of TANGO's Key Exploitable Results (KERs) and Exploitable Results (ERs), consolidating business models, market pathways, and individual partner strategies to ensure long-term impact and sustainability of project innovations. The methodology employed in this deliverable was based on a standardized framework developed under Task 8.2, including structured partner input templates, desk research on relevant markets, and iterative refinement through partner reviews. Each result was assessed through a unified set of sections: competitor analysis, market analysis, value proposition, barriers and standards, technology and market watch, and exploitation pathway. For the key results of the project, we also include a BMC in the exploitation analysis, shifting towards a more commercially/business oriented strategy. This systematic approach enabled comparability and completeness across all outputs.

Section 3 – Business Models and Exploitation Paths per KER and ER outlines the detailed exploitation framework for each of the project's results. A total of 26 results (9 KERs and 17 ERs) were individually analyzed using a consistent template. The section highlights the value propositions offered by each result, the current competitive landscape, addressable markets (in size and trends), regulatory and standardization contexts, and the specific exploitation intentions of the responsible partners. The results show strong alignment with high-growth technology markets including AI model explainability, green computing, federated data spaces, privacy-preserving identity management, and MLOps. A diversity of exploitation modes is identified, such as product integration, internal process improvement, service provision, software licensing, consultancy offerings, and follow-up R&D investment.

Annex E – Exploitation Plan for ERs compiles the exploitation pathways for each individual result as provided by the partners responsible for their development. The annex synthesizes practical exploitation intentions across use cases—ranging from internal adoption and commercial services to open-source dissemination and Horizon Europe continuation strategies. It emphasizes the importance of aligning exploitation plans with sector-specific needs (e.g. privacy in healthcare, trust in AI for finance, green performance for data centers) and indicates the maturity level of various results, from prototypes already tested in pilots to advanced research components.

Annex F – Exploitation Plan Table for All Partners presents a consortium-wide view of the post-project exploitation landscape. For each partner, an overarching exploitation plan was defined—either based on their role in specific results or their broader participation in TANGO. Partners that were not directly responsible for technical results were still included, with custom exploitation plans reflecting institutional learning, portfolio enhancement, strategic collaborations, and future participation in EU-funded research. This annex clearly distinguishes between types of organizations—technology providers, universities and RTOs, associations, and use case providers—highlighting differences in exploitation focus: commercial uptake, research reuse, policy influence, or cross-sector technology transfer.

Together, these sections confirm that the TANGO consortium has developed not only high-quality technical innovations but also robust plans to carry these results forward. The coordinated methodology ensures that each partner's contributions are translated into actionable post-project strategies. The integration of market intelligence, regulatory foresight, and partner-driven insights positions TANGO's outputs for sustainable exploitation, aligned with European priorities in digital trust, data sovereignty, and responsible AI. This deliverable provides a strong foundation for the long-term impact of TANGO's work beyond the project's conclusion.

9 Conclusions

The deliverable at hand represents a significant asset in project TANGO as it provides the consortium with a clear overview on the progress of the communication, dissemination and exploitation activities conducted so far. The following are the main highlights of the deliverable. The deliverable provides a report on the joined efforts of the consortium to effectively communicate and disseminate the project's results, with an update on the KPIs status that are under way on reaching the target value by the end of the project. The information provided is essential to all the partners in order to monitor the progress made so far and for the WP leader to coordinate the joint efforts towards the final outcome of TANGO's impact on society and its long-term success. The deliverable also offers a comprehensive a well-structured plan for the innovation management and exploitation activities, outlining the legal requirements regarding the IPR allocation and protection, the exploitable results of the project identified until now and the initial exploitation activities for the 5 prioritized KERs, including the actions put in place for the standardisation activities. The outlined information is essential for the consortium in order to validate the potential for further exploitation of the project results. The deliverable provides a well-developed and detailed SWOT and PESTLE analysis; moreover the 5 prioritized KERs of the project have been further analysed and examined by the SWOT and PESTLE analysis introduced in Section 5. The Business Model Canvas of 1 prioritized KER is also presented as part of the exploitation activities. In conclusion, the efforts of the consortium on the communication, dissemination and exploitation of TANGO for the first 18 months of the project have been successful. In the next version of the deliverable, the definitive overview on the impact of communication and dissemination will be provided, along with the final list of ERs following the project's technical developments.

10 References

[1] Matomo Analytics https://matomo.org/

[2] RISE Research Institutes of Sweden https://www.ri.se/en

[3] European Federation of Data Driven Innovation Hubs https://euhubs4data.eu/

[4] European Big Data Value Forum https://www.bdva.eu/

[5] GLACIATION project https://glaciation-project.eu/

[6] MobiSpaces project https://mobispaces.eu/

[7] PISTIS project https://www.pistis-project.eu/

[8] TEMA project https://tema-project.eu/

[9] GovTech Connect https://joinup.ec.europa.eu/collection/govtechconnect

[10] Horizon Trustee https://horizon-trustee.eu/

[11] TEADAL project https://www.teadal.eu

[12] GLASS project https://www.glass-h2020.eu

[13] Human Compatible AI project https://humancompatible.org

[14] Prometheus -X Portal https://prometheus-x.org

[15] OASEES project https://oasees-project.eu

[16] European Union. (n.d.). Intellectual Property. Retrieved from https://eur-lex.europa.eu/EN/legal-content/glossary/intellectual-property.html

[17] European Commission High-Level Expert Group on AI European Commission High-Level Expert Group on AI - High-level expert group on artificial intelligence | Shaping Europe's digital future (europa.eu)

[18] ISO/IEC JTC 1/SC 42 (Artificial Intelligence) ISO/IEC JTC 1/SC 42 - Artificial intelligence

[19] CEN-CENELEC JTC 21 (Artificial Intelligence) CEN-CENELEC JTC21 – Artificial Intelligence

[20] NIST AI Risk Management Framework AI Risk Management Framework | NIST

[21] ITU-T Focus Group on AI for Autonomous and Assisted Driving Focus Group on AI for autonomous and assisted driving (FG-AI4AD) (itu.int)

[22] Cybersecurity Working Group promoted by the European Banking Federation (EBF) - CYBERSECURITY - EBF

[23] FS-ISAC (Financial Services Information Sharing and Analysis Centre promoted by ENISA) - Financial Services Information Sharing and Analysis Center (fsisac.com)

[24] ECSO (European Cyber Security Organisation) - Home - ECSO (ecs-org.eu)

[25] ENISA Guidelines on Authentication - Authentication Methods — ENISA (europa.eu)

[26] Privacy Threat Modelling and Identification for Trustworthy AI - NIST AIRC - AI Risks and Trustworthiness

[27] NIST Special Publication 800-53 (Security and Privacy Controls) - SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC (nist.gov)

[28] ISO/IEC JTC 1/SC 38 (Cloud Computing and Distributed Platforms) - ISO/IEC JTC 1/SC 38 - Cloud computing and distributed platforms

[29] ITU-T Study Group 13 (Future networks including cloud computing, mobile and next-generation networks) - SG13: Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures (itu.int)

[30] European Union Blockchain Observatory and Forum - Homepage - European Commission (europa.eu)

[31] Dataspace Protocol - Dataspace Protocol overview - International Data Spaces

[32] International Data Spaces Association - Home - International Data Spaces

[33] ECLIPSE Data Spaces WG - Eclipse Dataspace | The Eclipse Foundation

[34] CEN/CENELEC Trusted Data Transactions - CEN Workshop on Trusted Data Transaction - CEN-CENELEC (cencenelec.eu)

[35] GDPR (General Data Protection Regulation) - General Data Protection Regulation (GDPR) – Legal Text (gdpr-info.eu)

[36] Payment Security Support Group and Card Fraud Prevention Forum promoted by European Payment Council (EPC) - Fraud prevention and payment security | European Payments Council

[37] Privacy-preserving distributed ABC scheme - Implementation and evaluation of a privacy-preserving distributed ABC scheme based on multi-signatures - ScienceDirect

[38] FIDO Alliance - FIDO Alliance - Open Authentication Standards More Secure than Passwords

[39] HS Booster (Horizon Standardisation Booster) - HSBooster.eu

Annex A – List of TANGO Exploitable Results

#	Exploitable Result (ER)	Ownership	Owner(s)	Contrib.	Related Task(s)	Result type	Current TRL
1	Blockchain-based data storage and sharing	Single	NOR	NOR	T3.1	Integrated platform	TRL 6
2a	UCON	Single	FHG	FHG	T3.2	SW (standalone)	TRL 4
2b	Trustworthiness Scoring Module	Single	FUJ	FUJ, NOR, SVI, SQD, FHG, VTT, DUT, UOG	T3.2	System/ Model	TRL 4
2c	User Behaviour Exchange Module (UBEM)	Single	VTT	VTT	T3.2	SW (standalone)	TRL 3
3	Confidentiality and Privacy by Design	Joint	UMU, ATOS	NOR, QBE, FHG, DUT	T3.3, T4.1	SW (standalone)	TRL 4
4	Self-encryption and Decryption Techniques with Multi-Factor Information Recovery Mechanisms	Joint	DUT	NOR, FHG, DUT, UMU	T3.4	Algorithm	TRL 3
5	ePrivacy Mechanisms, Protocols and Processes	Single	KUL	NOR, SQUAD, DBC, DUT, UTH, LIC	T3.5	Guideline	N/A
6a	Personal Credential Manager	Single	VTT	UMU, ATOS	T4.1	SW (standalone)	TRL 4
6b	Privacy-preserving distributed ABC scheme	Single	UMU	VTT, ATOS	T4.1	SW (standalone)	TRL 4
6c	Issuer and Verifier for SSI Mgmt	Single	ATOS	Dependency: - ZKP Library (UMU)	T4.1	SW (standalone)	TRL 4
7a	Seamless onboarding for users	Single	QBE	ATOS, SVI, QBE, KUL	T4.2	SW (standalone)	TRL 5

#	Exploitable Result (ER)	Ownership	Owner(s)	Contrib.	Related Task(s)	Result type	Current TRL
7b	Seamless onboarding for devices	Single	ATOS	ATOS, SVI, QBE, KUL	T4.2	SW (standalone)	TRL 5
8	User continuous behavioural authentication	Single	QBE	SVI, QBE, UMU, KUL, UTH	T4.3	SW (standalone)	TRL 5
9	Device continuous behavioural authentication	Single	UTH	UTH	T4.4	SW (standalone)	TRL 4
10	Hardening against Sidechannel Attacks	Joint	CEA	CEA, VTT, DUT	T4.5	SW (standalone)	TRL 2
11	Exploratory Data Analysis engine (EDAE)	Joint	EXUS	EXUS, UOM, UOG	T5.1	SW (standalone)	TRL 3
12a	Energy efficient AI model training Support for MLOps	Joint	ATOS	ATOS, EXUS, XLAB, UOM, ANYS	T5.2	SW (standalone)	TRL 4
12b	Energy efficient AI model training Support for Federated Learning	Joint	ATOS	ATOS, EXUS, XLAB, UOM, ANYS	T5.2	SW (standalone)	TRL 4
12c	Energy efficient AI model training Support for AutoML	Joint	ATOS	ATOS, EXUS, XLAB, UOM, ANYS	T5.2	SW (standalone)	TRL 4
13	Dynamic Intelligent Execution	Joint	UOM	UOM, ATOS, UTH, EXUS, TUB, ETH, FORTH, LUX	T5.3	SW (standalone)	TRL 6 – TRL7
14a	Privacy Threat Modelling and Identification for Trustworthy AI Privacy Enhancing	Single	UOG	UOG, FUJ_LU, SQUAD, EXUS, QBE, SQD, IDIADA	T5.4	SW (standalone)	TRL 4

#	Exploitable Result (ER)	Ownership	Owner(s)	Contrib.	Related Task(s)	Result type	Current TRL
	Component (PEC)						
14b	Privacy Threat Modelling and Identification for Trustworthy AI Privacy Assurance Tool (PAT)	Single	FUJ_LU	UOG, FUJ_LU, SQUAD, EXUS, QBE, SQD, IDIADA	T5.4	SW (standalone)	TRL 3
15	X-AI for Privacy and Trust Enhancement	Joint	SQD	SQD, ATOS, EXUS, SVI, QBE, XLAB, KUL, UOG	T5.5	AI & ML Model/ Method	TRL 4
16	Infrastructure Management based on AI	Joint	XLAB	XLAB, ATOS, EXUS, UOM, IDIADA	T5.6	AI & ML Model/ Method	TRL 4
17	TANGO Platform	Joint	All involved partners	-	T6.1, T6.2, T6.3, T6.4	Integrated platform	TRL 4
18	TANGO Connectors	Joint	UTH, INTRA	Other partners	T2.5, T6.1	SW (standalone)	TRL 4

Annex B - Exploitable Results Standardisation Mapping

Number	Exploitable Result	Relevant Standardisation Bodies
1	Blockchain-based data storage and sharing	▸ ISO/TC 307 (Blockchain and Distributed Ledger Technologies) European Union Blockchain Observatory and Forum ▸ ITU-T Focus Group on Application of Distributed Ledger Technology
2a	UCON	▸ ISO/IEC 29100 (Privacy Framework) ▸ NIST Privacy Framework ▸ ENISA Guidelines on Data Protection
2b	Trustworthiness Scoring Module	▸ ISO/IEC 25010 (System and Software Quality Models) ▸ IEEE Standards Association (Trust and Reputation Systems) ▸ ITU-T X.1255 (Framework for Discovery of Identity Management Information)
2c	User Behaviour Exchange Module (UBEM)	▸ GDPR (General Data Protection Regulation) ▸ ISO/IEC 27001 (Information Security Management) ▸ NIST Special Publication 800-53 (Security and Privacy Controls)
3	Confidentiality and Privacy by Design	▸ ISO/IEC 27018 (Code of Practice for Protection of Personal Data in Cloud) ISO/IEC 27701 (Privacy Information Management) ▸ GDPR
4	Self-encryption and Decryption Techniques with Multi-Factor Information Recovery Mechanisms	▸ ISO/IEC 29192 (Lightweight Cryptography) ▸ NIST Special Publication 800-57 (Recommendation for Key Management) ▸ ENISA Guidelines on Cryptography
5	ePrivacy Mechanisms, Protocols and Processes	▸ ePrivacy Directive ISO/IEC 29184 (Online Privacy Notices and Consent) ▸ GDPR
6a	Personal Credential Manager	▸ FIDO Alliance (Fast Identity Online) ISO/IEC 24760 (A Framework for Identity Management)

Number	Exploitable Result	Relevant Standardisation Bodies
		▸ NIST Special Publication 800-63 (Digital Identity Guidelines)
6b	Privacy-preserving distributed ABC scheme	▸ ISO/IEC 29101 (Privacy Architecture Framework) ▸ NIST Privacy Framework ▸ W3C Verifiable Credentials Data Model
6c	Issuer and Verifier for SSI Mgmt	▸ Decentralized Identity Foundation (DIF) ▸ W3C DID (Decentralized Identifiers) ▸ ISO/IEC 18013 (Personal Identification)
7a	Seamless onboarding for users	▸ ISO/IEC 29115 (Entity Authentication Assurance Framework) ▸ FIDO Alliance ▸ NIST Special Publication 800-63
7b	Seamless onboarding for devices	▸ ISO/IEC 27033 (IT Network Security) ▸ IEEE 802.1X (Port-Based Network Access Control) ▸ IETF (Internet Engineering Task Force) Standards
8	User continuous behavioural authentication	▸ ISO/IEC 30107 (Biometric Authentication) ▸ FIDO Alliance ▸ ENISA Guidelines on Authentication
9	Device continous behavioural authentication	▸ ISO/IEC 30107 (Biometric Authentication) ▸ NIST Special Publication 800-63 ▸ ENISA Guidelines on Authentication
10	Hardening against Sidechannel Attacks	▸ ISO/IEC 19792 (Security Evaluation of Biometrics) ▸ NIST Special Publication 800-57 ▸ ENISA Guidelines on Cryptography
11	Exploratory Data Analysis engine (EDAE)	▸ ISO/IEC 27045 (Information Security Incident Management) ▸ NIST Big Data Interoperability Framework ▸ IEEE Big Data Standards
12a	Energy efficient AI model training Support for MLOps	▸ ISO/IEC JTC 1/SC 42 (Artificial Intelligence) ▸ IEEE Standards Association (AI Standards) ▸ European Commission AI HLEG (High-Level Expert Group on AI)

Number	Exploitable Result	Relevant Standardisation Bodies
12b	Energy efficient AI model training Support for Federated Learning	▸ ISO/IEC JTC 1/SC 42 (Artificial Intelligence) ▸ IEEE Standards Association (AI Standards) ▸ European Commission AI HLEG
12c	Energy efficient AI model training Support for AutoML	▸ ISO/IEC JTC 1/SC 42 (Artificial Intelligence) ▸ IEEE Standards Association (AI Standards) ▸ European Commission AI HLEG
13	Dynamic Intelligent Execution	▸ ISO/IEC 2382 (Information Technology Vocabulary) ▸ IEEE Standards Association (AI Standards) ▸ ITU-T Focus Group on AI for Autonomous and Assisted Driving
14a	Privacy Threat Modelling and Identification for Trustworthy AI Privacy Enhancing Component (PEC)	▸ ISO/IEC JTC 1/SC 42 (Artificial Intelligence) ▸ IEEE Standards Association (AI Standards) ▸ GDPR
14b	Privacy Threat Modelling and Identification for Trustworthy AI Privacy Assurance Tool (PAT)	▸ ISO/IEC JTC 1/SC 42 (Artificial Intelligence) ▸ IEEE Standards Association (AI Standards) ▸ GDPR
15	X-AI for Privacy and Trust Enhancement	▸ ISO/IEC JTC 1/SC 42 (Artificial Intelligence) ▸ IEEE Standards Association (AI Standards) ▸ GDPR
16	Infrastructure Management based on AI	▸ ISO/IEC JTC 1/SC 42 (Artificial Intelligence) ▸ IEEE Standards Association (AI Standards) ▸ ITU-T Focus Group on AI for Autonomous and Assisted Driving
17	TANGO Platform	▸ ISO/IEC JTC 1/SC 42 (Artificial Intelligence) ▸ IEEE Standards Association (AI Standards) ▸ European Commission AI HLEG
18	TANGO Connectors	▸ ISO/IEC JTC 1/SC 42 (Artificial Intelligence) ▸ IEEE Standards Association (AI Standards) ▸ European Commission AI HLEG

Annex C – Exploitation plan for ERs

Exploitation paths for ER1- Blockchain-based data storage and sharing

Competitor analysis

The competitive landscape for ER1 centers around three main categories of solutions currently used by institutions handling regulated data. The first category involves one-to-one data sharing connections, where banks or institutions directly connect to licensing authorities via APIs. These solutions typically rely on existing technical infrastructure within each country and vary significantly in pricing and structure depending on how the connectivity and file sharing are managed. While they serve the same core target—institutions needing to exchange regulated, verified data such as KYC—they often lack the systemic coordination and mutualization advantages provided by NOR's Fides platform.

The second group of competitors includes companies offering similar solutions but using centralized architectures. These have largely failed to scale effectively, although there are limited efforts in decentralized solutions that attempt to serve this market. These offerings target the same customer base—institutions needing coordinated, secure data sharing—but generally require an entity to act as a coordinator or central authority to enable implementation. These constraints limit their scalability and resilience, especially compared to ER1's fully decentralized and blockchain-based architecture.

The third competitor archetype involves internal, custom-built solutions developed by two or more organizations for their own collaborative data-sharing needs. These projects typically vary in structure and pricing depending on context and can be resource-intensive to implement and maintain. NOR's competitive edge lies in having a fully functioning product ecosystem already operational, which differentiates Fides by offering a proven solution with high levels of decentralization, redundancy, and compliance out of the box.

Market Analysis

- **ER1: Blockchain-based data storage and sharing, focused specifically on the KYC and Regulatory Technology (RegTech) markets**
  - **Segments**

ER1 directly targets the **eKYC software** and **RegTech identity management** segments within the broader financial compliance and digital onboarding ecosystems. According to Grand View Research, the European Know Your Customer software market is segmented by deployment mode (on-premise vs. cloud), end-user (BFSI, government, telecom), and application type (customer onboarding, fraud prevention, compliance), with **BFSI being the dominant sector** due to regulatory pressure and the operational burden of manual KYC checks[100]. ER1's decentralized sharing model is especially relevant for banks, enabling multiple institutions to collaborate securely in verifying and re-using KYC data while staying compliant. Similarly, in the RegTech space, identity verification and regulatory reporting are key segments seeing growing demand, especially under GDPR and AMLD regulations, as highlighted by KBV Research's analysis of the European RegTech market[101].

  - **Size and Growth Rate**

[100] Grand View Research
[101] KBV Research

The **European eKYC market** is experiencing robust growth, driven by digitization, financial crime regulations, and demand for seamless onboarding. According to IMARC Group, the global eKYC market reached **USD 1.6 billion in 2022** and is projected to grow at a **CAGR of 19.2%** to reach **USD 4.4 billion by 2028**, with Europe accounting for a significant portion of this expansion due to GDPR and eIDAS adoption[102]. Mordor Intelligence corroborates this growth, noting that the KYC market is expanding rapidly in Europe as financial institutions seek cost-effective, scalable solutions to meet compliance demands[103]. In parallel, the European RegTech market is set to grow by over **23% in 2024**, reaching **USD 4.59 billion** that year alone, and continuing on a high-growth trajectory as governments tighten oversight and institutions modernize compliance systems[104].

- **Trends**

ER1 benefits from several current trends in the EU's KYC and RegTech landscape. First, the shift toward **collaborative compliance models** is becoming more common, where financial institutions share validated KYC data to eliminate redundant onboarding—a model ER1 directly supports. According to Polaris Market Research, banks are increasingly adopting KYC platforms that integrate blockchain and advanced identity management systems to address redundancy and inefficiency in onboarding processes[105]. In the RegTech sector, Fortune Business Insights reports that **blockchain and AI** are increasingly seen as transformative technologies in regulatory compliance, especially for real-time identity verification and fraud detection systems[106]. Furthermore, digital onboarding is being prioritized by banks in response to increased customer demand for frictionless account access—a trend reinforced by Market Statsville, which emphasizes the role of secure, remote, and API-driven KYC methods[107].

- **Barriers**

Despite strong tailwinds, ER1 faces significant barriers that could slow adoption. One of the most pressing is the **fragmentation of regulatory interpretations** across EU member states, particularly around blockchain technologies. Grand View Research notes that while the KYC software market is expanding, concerns around **interoperability, data privacy, and auditability** remain for decentralized systems[108]. Additionally, the RegTech adoption rate is uneven across the EU, with legacy systems and **institutional resistance to data-sharing platforms** posing challenges, especially in countries with stricter data localization laws, as reported by the Trends & Analysis Forum via LinkedIn regarding European RegTech software adoption[109]. Another barrier is the lack of **standardized APIs or open access to government-issued identity data**, which ER1 requires for national-level interoperability. This infrastructure gap limits the full implementation of decentralized KYC-sharing solutions.

- **Opportunities**

Despite these barriers, ER1 is strongly positioned to leverage multiple emerging opportunities. First, as noted by Fortune Business Insights, Europe's increasing investment in **digital identity frameworks and AMLD6 enforcement** is creating demand for scalable, cross-institutional compliance platforms—precisely the kind of use case ER1 enables[110]. Second, the **cost savings from mutualized KYC**—

[102] IMARC Group
[103] Mordor Intelligence
[104] Fintech Futures
[105] Polaris Market Research
[106] Fortune Business Insights
[107] Market Statsville
[108] Grand View Research
[109] Trends & Analysis Forum
[110] Fortune Business Insights

estimated at 30–40% for banks according to Polaris Market Research—make ER1 highly appealing in a financial landscape pressured by compliance costs[111]. Third, the shift toward **RegTech-as-a-Service (RaaS)** business models, as outlined in the KBV Research report, means ER1 could be deployed in a modular, API-accessible format to scale adoption among smaller institutions that cannot afford full system overhauls[112]. Lastly, the opportunity to **extend beyond the BFSI sector**—into telecom, energy, and healthcare where regulatory compliance is rising—positions ER1 as a multi-sector solution for the EU digital economy.

- **Value proposition analysis**

The core value of ER1 lies in the Fides platform's (NOR's platform that integrates ER1) ability to offer a decentralized, blockchain-based solution for legally compliant, high-redundancy data sharing. The primary use case is KYC, where NOR has identified significant inefficiencies in how banks typically manage customer data in siloes. Fides mutualize the KYC workload, allowing multiple banks or institutions to securely reuse validated customer data. This results in substantial time and cost savings—up to 30–40% in a typical bank—and enhances compliance and customer satisfaction. Moreover, it creates new revenue opportunities for banks by enabling monetization of their existing validation processes.

Built on NOR's proprietary IP and decentralized architecture, Fides empowers data owners by requiring consent for all data sharing, ensuring full control and compliance with privacy regulations like GDPR. The solution enhances operational efficiency while also acting as a trust enabler in increasingly regulated environments. NOR's strategy has already demonstrated success in production ecosystems in the UAE and seeks to replicate that model in Europe and other regions.

- **Barriers, obstacles and analysis of the standards and regulation**

A key barrier to ER1 adoption is the requirement for ecosystem-level participation—since ER1 and Fides is a sharing solution, at least two or more entities must coordinate to launch and sustain its use. This coordination barrier can delay adoption, especially in markets without centralized initiatives or a lead institution to organize stakeholders. As highlighted by partner NOR, the initial bootstrapping of a Fides ecosystem often requires strong partnership with regulators, licensing authorities, or industry bodies to build trust and commitment among participants.

Another challenge involves the lack of standardized APIs or access to government-issued identity data, which limits the ability to scale interoperable solutions across EU member states. Fragmented regulatory interpretations, especially concerning blockchain's use in regulated data systems, can further complicate deployment. Despite these challenges, NOR ensures compliance with all relevant regulations and standards in the countries it operates in. Fides is certified under ISO 27001 and ISO 9001 and operates in compliance with GDPR and UAE-specific privacy laws, affirming its credibility in highly regulated environments.

- **Technology and market watch**

The regulatory landscape is evolving rapidly, with increasing pressure on organizations in various verticals—including financial services, marketplaces, and ESG data handlers—to strengthen KYC and AML compliance. These tightening regulations are expected to expand the addressable market for solutions like Fides, which enable secure and auditable sharing of verified data. NOR is proactively

[111] Polaris Market Research
[112] KBV Research

monitoring these developments to identify new customer segments and opportunities for ecosystem deployment.

At the same time, competitive pressures are rising as new startups and decentralized solutions begin to emerge. NOR acknowledges the possibility that competitors with a compelling use case could replicate or undercut Fides' value proposition. As such, NOR is committed to maintaining its lead by staying ahead on technology development and ecosystem implementation, capitalizing on its proven deployment experience and operational ecosystems.

New markets are also emerging due to regulatory changes. ESG data, for instance, is now subject to audit requirements, and marketplaces are increasingly mandated to perform rigorous KYC. NOR plans to adapt its offerings quickly to remain relevant to these evolving demands and client types. Agile technology updates, market alignment, and use-case diversification are core to NOR's strategy in maintaining competitiveness.

NOR's input on this matter is reflected in Table 16.

Table 16: ER1 Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date	Link
Emerging trend or development	Regulations are tightening around KYC/AML for more verticals/industries (e.g. ESG data will be audited, and Marketplaces regulated around their KYC)	Regulations like these work in our favour as our solution becomes more relevant for more industries/segments that will have to do more around handling regulated, verified data, and with that possibly seeing a benefit from a suitable data sharing solution and building ecosystems	Be proactive and grasp opportunities/target the new segments as there are developments	Ongoing	NA
Hot startups and innovators	There are some ongoing/developing efforts similar to ours and more could come	Could disrupt our unique proposition, and if they get a good use case - take away our unique experience and POC with a well-functioning and significant ecosystem in production	Our extensive IP and POC we have in place should be a good protection here - but we need to keep working on both our technology and market presence	Ongoing	NA
New market opportunities	See row 2, regulations and	Possibility to get more and a new	Be up to date and quick to adjust our	ongoing	NA

	changes in markets are creating new potential opportunities and target customers for us	type of clients	offerings (and as suitable also tweak our technology/solution) so we are relevant to new types of clients		

Business Model Canvas

Even though ER1 is not considered a key outcome of TANGO, NOR has provided a thorough BMC that elaboratively summarizes the organisation's plans for the result beyond the project's lifetime.

<table>
<tr><th colspan="5">Business Model Canvas</th></tr>
<tr><th>Key Partners</th><th>Key Activities</th><th>Value Propositions</th><th>Customer Relat</th><th>Customer Segments</th></tr>
<tr>
<td rowspan="2">Our partners could be e.g. licensing authorities, central banks or regulators that wish to be part of developing (or enforcing) KYC/KYB data sharing ecosystems in a specific market.

Since our solution can be relevant for e.g. ESG and other regulated data as well - partners can also be relevant companies and coordinates in those industries.</td>
<td>We offer a platform, that allows decentralized, blockchain-based data sharing</td>
<td rowspan="2">Our solution offers enhanced operational efficiency, enhanced compliance and enhanced customer experience and service.

This leads to cost savings linked to operational gains, better compliance and meeting of regulations and other requirements, and increased customer satisfaction/revenue potential.</td>
<td>We are a technology provider to our customers and in some cases, we also offer managed services.
We have an ecosystem up and running in the UAE with many banks and licensing authorities as our clients, working together.</td>
<td rowspan="2">Our customers could be e.g. financial institutions that will share KYC/KYB data, companies that need to handle and share ESG data, or companies and authorities that handle e.g. VISA or other personal data.

The customers will benefit from secure and legally compliant data sharing that allows for operational savings and an improvement in and streamlining of the data.

The end customers (owners of the data) have full control of their data, as nothing</td>
</tr>
<tr>
<td>Key Resources
Explainability libraries and in-house IP

Streamlit UI and FastAPI backend components

Docker containers for deployment

Skilled AI/ML and DevOps team</td>
<td>Channels
Direct partnerships with AI vendors and system integrators

Online deployment via cloud marketplaces

Tech workshops and demos for</td>
</tr>
</table>

	Secure data environments for privacy testing		enterprise clients GitHub and developer portals for adoption	is shared without their consent, and they benefit from more efficient and easier-to-handle processes around their data (e.g. they need to upload and update their data only once, and it can then be shared, at the customers' consent, to the other entities in the ecosystem as suitable)

Cost Structure	Revenue Streams
Personnel (incl. developers) and infrastructure costs. We are value-driven and aim to create solutions that benefit our customers and society. Personnel and finding and keeping the right people to develop and maintain our solutions, and support our clients is the most challenging aspect and our most important cost bucket.	Fees related to implementation, licensing and usage, support, and managed services Our customers need to see that our solutions are credit-positive, leading to operational savings, and also add additional benefits (e.g. improved compliance and increased customer satisfaction

▸ Exploitation Pathway

ER1 is already a standalone commercial product with proven deployment. Through TANGO, NOR developed version 3 of this component of the Fides platform, introducing key enhancements to decentralization and privacy. The current exploitation focus is twofold: first, to improve satisfaction and retention among existing clients by validating the solution in new regulatory contexts such as visa processing and public sector applications; and second, to expand NOR's clientele by promoting Fides as a modular, scalable solution adaptable to multiple verticals.

The product is not open-source and follows a proprietary development model. NOR operates primarily under an annual licensing model with a tiered structure: clients pay based on the amount of data shared, with additional revenue streams from support, implementation, and managed services. The solution is targeted at licensed financial institutions, but NOR also aims to serve regulators and public institutions seeking to streamline operations while ensuring compliance.

No immediate plans exist for further Horizon Europe funding, although NOR remains open to opportunities as they arise. Instead, the company is focused on scaling Fides through direct sales, partnerships, and ecosystem expansion, using its successful deployments as proof points for market replication. The platform's flexible architecture and cross-sector applicability make it a strong candidate for long-term scalability within the EU and beyond.

Exploitation paths for ER2a- Trustworthiness Scoring Module (TSM)

Competitor analysis

The primary competitors identified for the Trustworthiness Scoring Module (TSM) are major industrial players such as Bosch, Siemens, Hitachi, Toshiba, and Waterfall Security. These firms contribute to trustworthiness and secure intercompany data sharing primarily through their involvement in industry associations and standards development organizations (SDOs). Their offerings span a broad portfolio of cybersecurity and industrial IT solutions, with pricing models that are complex and customized based on client needs. While these companies have a strong market presence and broad customer bases in the manufacturing sector, their solutions often lack the modular and highly customizable scoring framework proposed by the TSM. Moreover, none of the listed competitors appear to have translated trustworthiness models into a lean, deployable scoring solution as FUJ aims to demonstrate within TANGO, providing a unique positioning for the TSM in this niche.

Market Analysis

- **ER2a: Trustworthiness Scoring Module (TSM) using only your provided sources on the Cyber-Physical Systems (CPS) market**
  - **Segments**

ER2a aligns with the **system assessment and security assurance segment** of the Cyber-Physical Systems market. Specifically, it targets the evaluation of **operational trustworthiness in CPS architectures**, which is increasingly in demand across sectors like **automotive, industrial automation, and smart infrastructure**. According to Grand View Research, CPS in Europe is evolving through the integration of sensing, computation, control, and networking, where trust and performance assessments at system-level are critical for safety and reliability—especially in **autonomous vehicles and manufacturing systems**, which are key sectors for ER2a's application[113]. The market is segmented by component (hardware, software, services), deployment mode, and verticals, with **automotive and manufacturing industries** leading adoption, making ER2a's target use cases highly relevant within the **software/services** component segment[114].

- **Size and Growth Rate**

The European CPS market is experiencing accelerated growth due to the adoption of AI-driven smart systems and industrial automation. According to Credence Research, the **Europe CPS market was valued at USD 16.25 billion in 2022** and is projected to grow at a **CAGR of 8.2%**, reaching USD 28.91 billion by 2030[115]. Grand View Research echoes this trajectory, attributing market expansion to the increasing deployment of intelligent CPS solutions in sectors such as mobility, energy, and critical infrastructure across the EU[116]. This strong growth supports the market readiness for tools like ER2a, especially in verticals requiring continuous trust assessment of interconnected systems.

- **Trends**

Several trends support ER2a's momentum in the European CPS market. A key trend is the **rising demand for runtime assurance and trust metrics** in CPS applications, particularly where autonomous operation and human-machine interaction coexist. The TechInnovate Analytics analysis notes that trustworthiness frameworks and real-time system scoring are gaining traction in **cyber-physical**

[113] Grand View Research – Europe Outlook
[114] "Markets and Markets"
[115] Credence Research
[116] Grand View Research – Market Report

security solutions, which are increasingly embedded in edge computing and automotive systems[117]. Additionally, with the EU's push for **safe and explainable AI**, tools that quantify system behaviour and trust—as ER2a does—can be integrated into broader **AI governance** and **mission-critical CPS validation pipelines**. "Markets and Markets" highlights the growing adoption of CPS in **Industry 4.0 and autonomous mobility**, further validating the relevance of scoring modules in safety-critical decision-making contexts[118].

- **Barriers**

However, ER2a faces specific barriers to adoption. One major hurdle is the **lack of standardization for trust scoring metrics across CPS domains**. As Grand View Research points out, the heterogeneity of CPS architectures—ranging from embedded automotive systems to smart grid controllers—makes it difficult to apply one-size-fits-all trust models, complicating productization and cross-sector deployment[119]. Another challenge is the **integration overhead**: companies may be hesitant to adopt additional scoring layers if they perceive them as increasing system complexity or introducing new points of failure. The Mordor Intelligence report on physical systems and infrastructure adds that **data integrity, real-time responsiveness, and system resilience** remain top concerns in CPS environments, which could delay uptake of experimental scoring solutions without robust validation[120].

- **Opportunities**

Despite these barriers, ER2a is well-positioned to capitalize on emerging market needs. First, its modular and customizable design supports **domain-specific configuration**, making it an attractive component for CPS integrators aiming to enhance **compliance with functional safety standards like ISO 26262** in automotive or **IEC 61508** in industrial settings. Credence Research emphasizes that **Europe's CPS market is increasingly driven by demand for modular, reliable software services**, particularly those that enhance system observability and decision autonomy[121]. Furthermore, as Europe invests in **secure, sovereign, and AI-powered infrastructure under the Digital Europe Programme**, trust metrics like ER2a's scoring system will be critical enablers of **transparent, resilient automation**, offering vendors a niche but fast-growing market segment to address[122].

Value proposition analysis

The Trustworthiness Scoring Module (TSM) delivers a flexible, customizable framework for assessing trustworthiness in cyber-physical systems based on configurable system characteristics and attributes. Its primary value lies in bridging the gap between conceptual trust models—such as the IIC Trustworthiness Framework—and real-world implementations. Within TANGO, the TSM has been demonstrated and validated in practical manufacturing use cases, including automotive applications, advancing its readiness from TRL 4 to TRL 5. FUJ emphasizes that the TSM has already achieved conceptual acceptance in global industry forums like IIC and Platform Industry 4.0, something that could spur best practice configurations and facilitate the customization effort step by step. Through ER2a, customizing shall be easy and should be offered as a consulting service. However, complexity and lack of best practices currently hinder broader adoption. TSM addresses this by providing a

[117] TechInnovate Analytics
[118] "Markets and Markets"
[119] Grand View Research – Market Report
[120] Mordor Intelligence
[121] Credence Research
[122] Grand View Research – Europe Outlook

structured, lean, and practical method for scoring trust, offering a compelling tool for industrial organizations seeking to operationalize trust and secure data sharing in intercompany environments.

- **Barriers, obstacles and analysis of the standards and regulation**

A key barrier to adoption is the perception of complexity and the integration burden associated with trust scoring mechanisms. Target audiences may struggle with identifying the most relevant data sources for evaluation, and currently lack trusted reference implementations. Additionally, there is a broader lack of best practice configurations, leading to insecurity among potential adopters about feasibility. The TSM also faces challenges posed by global cybersecurity regulations, which may limit its cross-border applicability and create regional "islands" of use. While IEC JTC1 is actively working on standardizing trustworthiness evaluation approaches, the absence of universally accepted metrics still complicates widespread deployment. Nevertheless, the proactive participation of FUJ in standardization and industry groups (e.g. IIC, Platform Industry 4.0, and RRI) positions the TSM to align with future regulatory expectations.

- **Technology and market watch**

As indicated by FUJ and depicted in Table 17, several emerging trends reinforce the relevance and potential of the TSM. The topic of trustworthiness in Industrial IoT (IIoT) has become globally significant, with the IIC Trustworthiness model widely accepted at a conceptual level. However, practical implementations remain scarce. FUJ's work within TANGO aims to address this gap by demonstrating feasibility in real-life industrial environments, particularly via use-case-based showcases at IIoT and data-sharing forums such as Platform Industry 4.0. Moreover, while active R&D efforts by industrial firms remain limited, a demonstrated working implementation is likely to catalyse new investments and increase adoption. As companies look for lean, reliable methods to validate system integrity, FUJ's TSM—once validated—could enable new service offerings, including consultancy and scoring-as-a-service (SaaS) options. With the rise of sovereign and secure AI-powered infrastructure under the EU Digital Europe Programme, the TSM's integration into runtime decision-making and trust monitoring become increasingly vital.

Table 17: ER2a Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date	Link
Emerging trend or development	The topic of Trustworthiness and its measurement in the industrial IoT domain has been issue of global relevance and associations (IIC, Platform Industrie 4.0, RRI) and SDOs (IEC JTC1) are dealing with this topic of	The implementation of the Trustworthiness Scoring Module within TANGO shall demonstrate the feasibility of the IIC Trustworthiness model in real life environments and illustrate a way of purposeful integration into	The most relevant actions will be use case related demonstrations in the IIOT communities like Platform Industrie 4.0 in Germany or at data space / data sharing conferences demonstrating the feasibility of the TSM.	The discussions within the associations and SDOs are ongoing. There are specific opportunities at conferences or by contributing to papers of the entities.	https://www.iiconsortium.org/pdf/Trustworthiness_Framework_Foundations.pdf https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/IIoT_Value_Chain_Security3.html https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/IIoT_Value_Chain_Security.pdf?__blob=publicationFile&v=9 https://www.iiot-

Item	Description	Possible Impact	Actions	Effective Date	Link
	secure cross-company communication and data exchange. The IIC Trustworthiness model is widely known and accepted as a conceptual model but it lacks real life implementations and demonstration.	data sharing environments. It illustrates the path towards a broader application of a lean scoring model			world.com/industrial-iot/connected-industry/trustworthiness-methods-in-industrial-system-design/ https://jtc1info.org/technology/working-groups/trustworthiness/ https://jtc1info.org/sd-2-history/jtc1-working-groups/wg-13/ https://www.dke.de/resource/blob/2244406/dbbd9c02812f04cc1ab0063647262645/german-standardization-roadmap-industry-4-0-version-5-data.pdf
Active companies and their R&D strategies	Even if the principle model is accepted for its lean approach the feasibility is unclear. Thus companies follow that route only by a few candid R&D teams	Demonstrating feasibility will most probably increase activities in R&I for this way of scoring Trustworthiness	The most relevant actions will be use case related demonstrations in the IIOT communities like Platform Industrie 4.0 in Germany or at data space / data sharing conferences demonstrating the feasibility of the TSM.	not yet clear	N/A
Potential impact of technological change	Even if the principle model is accepted for its lean approach the feasibility is unclear. Thus, companies follow that route only by a few candid	Demonstrating feasibility will most probably increase activities in R&I for this way of scoring Trustworthiness	The most relevant actions will be use case related demonstrations in the IIOT communities like Platform Industrie 4.0 in Germany or at data space / data sharing conferences	not yet clear	N/A

Item	Description	Possible Impact	Actions	Effective Date	Link
	R&D teams		demonstrating the feasibility of the TSM.		
New market opportunities	Demonstration of feasibility of the TSM shall improve and simplify the assessment of Trustworthiness in data sharing. The specific implementation will need some consulting and data assessment per company for integration and customization of the TSM.	With a clear approach and its demonstrated feasibility, new opportunities for consulting and integration emerge. Most probably the demand of aaS like offerings will emerge.	When feasibility can be demonstrated potential offerings shall be illustrated. Potential customers will get the opportunity for co-creation of those offerings.	The specification of offerings is part of the exploitation and business planning process of the project. Effective dates are bound to the project planning.	N/A

Exploitation Pathway

The Trustworthiness Scoring Module (TSM) is currently being validated within TANGO, with no formal monetization plan yet. However, FUJ foresees several pathways for exploitation. The most immediate route would be integrating TSM into FUJ's existing consulting services as an added tool for trust assessment in data and service access management. Given its customizable nature, TSM could also be licensed or transferred to other vendors in need of modular trust-scoring capability. In addition, FUJ plans to extend the TSM with AI functionalities after TANGO to increase scalability and real-time capabilities. There is also potential for knowledge transfer and engagement in additional Horizon Europe proposals, should funding opportunities arise. Moreover, by aligning with leading standards organizations, FUJ is laying the groundwork for broader industry uptake of the TSM approach as standardization matures. According to FUJ, as ER2a is an innovative approach and emerging solution the market uptake will take some time. There will be some innovators and front runners across the globe, who will apply the TSM approach and this way open the market together with Fujitsu. Hence a small but fast-growing market share should be expected.

Exploitation paths for ER2c- Privacy Risk Score (PRS)

Competitor analysis

The Privacy Risk Score (PRS) operates in a competitive landscape of video anonymization and privacy compliance tools, particularly those tailored to the autonomous vehicle (AV) domain. One of the main competitors is Brighter AI, a Berlin-based company offering AI-driven anonymization technologies such as Precision Blur and Deep Natural Anonymization. These tools automatically detect and redact

faces and license plates in visual data, ensuring compliance with global data protection laws. Brighter AI primarily targets car manufacturers, making it a direct competitor in the AV privacy compliance market.

Another strong player is Caseguard, a broader AI-powered redaction platform that supports multi-modal anonymization (video, audio, images, documents). It is designed for industries like law enforcement, healthcare, and government, and offers bulk processing, transcription, translation, and on-premises deployment. Pricing ranges from $200–400 depending on the selected plan. Though Caseguard is not focused exclusively on AV, its comprehensive feature set and regulatory alignment make it a credible indirect competitor.

Fast Redaction is a more basic, cost-efficient alternative, offering quick face-blurring services priced at $19 plus $1 per video minute. Its simplicity and affordability may attract smaller AV solution providers or early-stage adopters of video anonymization.

Compared to these, PRS's key differentiator lies in its integration with the Trustworthiness Scoring Module (TSM) and its ability to dynamically compute privacy scores based on multiple policies and over time windows. Unlike typical anonymization tools that focus solely on redaction, PRS emphasizes privacy risk quantification—giving it a unique position in analytics-enhanced privacy compliance for AVs.

- **Market Analysis**
  - **ER2c (Privacy Risk Score) Privacy Enhancing Technologies (PET) market, the Cybersecurity for Autonomous Vehicles market**
    - **Segments**

The Privacy Risk Score (PRS) directly targets the **risk management** and **reporting & analytics** segments within the Privacy Enhancing Technologies (PET) market. According to Grand View Research, the risk management segment, depicted in Figure 31, benefits significantly from solutions that quantify exposure to privacy threats, automate compliance checks, and provide continuous monitoring — functions that ER2c operationalizes through dynamic scoring of privacy risks in real time[123]. In the context of autonomous vehicles, ER2c supports **application security** and **endpoint security** by evaluating privacy risks related to in-vehicle data handling and external communications, thus helping manufacturers comply with data privacy aspects of the GDPR and sector-specific standards[124].

[123] https://www.grandviewresearch.com/industry-analysis/privacy-enhancing-technologies-market-report
[124] Allied Market Research, https://www.alliedmarketresearch.com/cybersecurity-for-autonomous-vehicles-market-A324122

Figure 31: ER2c Privacy Enhancing Technologies (PET) market segments (source: Univ Datos)

- **Size and Growth Rate**

The addressable market for PRS is substantial. PET risk management solutions are expanding rapidly due to regulatory pressures: as portrayed in Figure 32, the PET market is projected to grow at a 25.3% CAGR from USD 3,120.9 million in 2024 to USD 12,094.4 million by 2030[125]. ER2c aligns perfectly with this, as organizations seek robust tools to measure and report privacy risk levels to auditors and regulators. Additionally, the growing integration of privacy risk management into automotive cybersecurity strategies suggests that the PRS can scale within the autonomous vehicles segment, which itself will grow at a 22.9% CAGR through 2032[126].

[125] Grand View Research, https://www.grandviewresearch.com/industry-analysis/privacy-enhancing-technologies-market-report

[126] Allied Market Research, https://www.alliedmarketresearch.com/cybersecurity-for-autonomous-vehicles-market-A324122

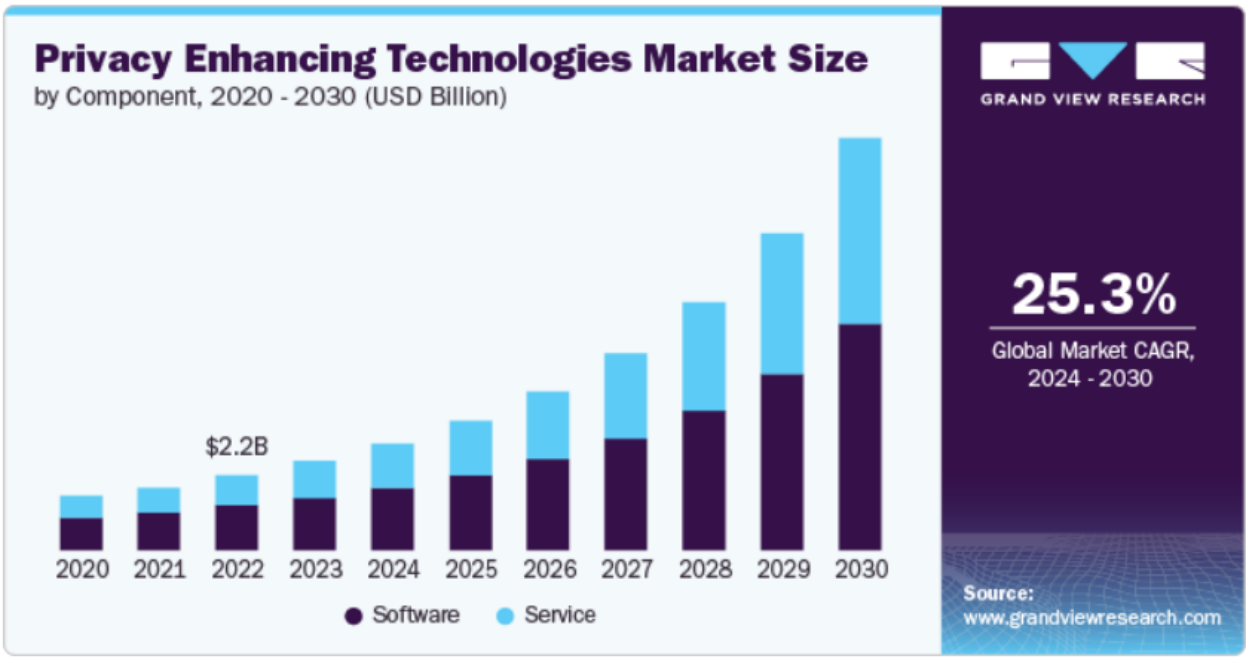


Figure 32: ER2c Privacy Enhancing Technologies (PET) market size and growth rate (source: Grand View Research)

- **Trends**

A notable trend fuelling ER2c's adoption is the shift towards **automated, data-driven risk scoring**. Organizations increasingly demand continuous, evidence-based insights into their privacy posture to comply with evolving regulations like the EU AI Act and GDPR[127]. This is reinforced by the surge in data breaches — IBM reports a global average cost of USD 4.88 million per breach — which underlines the need for proactive privacy risk quantification to manage cyber liability[128]. For autonomous vehicles, trends in AI-powered security analytics create an opportunity for ER2c to function as a privacy-specific scoring layer within broader vehicle security monitoring[129].

- **Barriers**

A significant barrier for ER2c is **integration complexity**. Many organizations lack in-house expertise to link dynamic risk scoring with existing compliance workflows and security dashboards[130]. For automotive contexts, the challenge is even greater: ER2c must interface seamlessly with real-time

[127] Fortune Business Insights, https://www.fortunebusinessinsights.com/privacy-enhancing-technologies-market-111241
[128] Grand View Research, https://www.grandviewresearch.com/industry-analysis/privacy-enhancing-technologies-market-report
[129] Allied Market Research, https://www.alliedmarketresearch.com/cybersecurity-for-autonomous-vehicles-market-A324122
[130] Fortune Business Insights, https://www.fortunebusinessinsights.com/privacy-enhancing-technologies-market-111241

automotive data streams and meet strict automotive safety certifications, which can extend development timelines and increase cost[131].

- **Opportunities**

However, ER2c's market opportunities are compelling. Regulators increasingly demand proof of continuous privacy oversight, so companies adopting PRS can demonstrate accountability and reduce regulatory fines[132]. For vehicle OEMs and fleet managers, embedding PRS provides a competitive differentiator by showcasing robust privacy risk controls alongside cybersecurity measures — a key trust factor for consumer adoption of autonomous driving[133].

Value proposition analysis

ER2c delivers unique value both as a standalone module and as an integral component of the Trustworthiness Scoring Module (TSM). Its primary function is to validate anonymization in video sequences according to specified privacy policies, producing a quantifiable privacy score for a given time window. This functionality enables autonomous vehicle providers to more easily assess and demonstrate GDPR compliance, a critical requirement in the EU and increasingly elsewhere.

Beyond basic compliance, PRS helps AV developers identify and prevent faulty implementations that could lead to privacy violations. It also provides intuitive communication of privacy protection levels to consumers, enhancing transparency and trust. By calculating varying privacy scores based on different privacy policies, PRS offers flexibility and relevance across jurisdictions and operational contexts. Its core value proposition lies in simplifying compliance, reducing legal exposure, and strengthening customer trust through objective privacy risk evaluation.

Barriers, obstacles and analysis of the standards and regulation

The development and adoption of PRS face several barriers and obstacles. One key barrier is funding dependency: reaching higher TRLs (Technology Readiness Levels) will require additional support from Horizon Europe or national sources. There is also limited access to real-world data, which constrains PRS's ability to be tested across diverse real-world conditions. Moreover, the legal landscape imposes constraints on testing anonymization in uncontrolled environments, further impeding iterative improvements.

From a technical standpoint, current implementations rely on standard techniques like Gaussian blurring and utilize state-of-the-art detectors such as the YOLO-face model. However, full alignment with regulatory expectations—especially under GDPR and the EU AI Act—requires PRS to maintain strong accuracy and transparency in anonymization.

Regarding standards, existing implementations align with accepted anonymization norms. But more advanced expectations under the GDPR and new frameworks like the EU AI Act introduce regulatory challenges. Ensuring traceable and verifiable anonymization processes is essential for compliance, especially in edge use cases such as AVs, where video data is captured continuously and often in public spaces.

Technology and market watch

---

[131] Allied Market Research, https://www.alliedmarketresearch.com/cybersecurity-for-autonomous-vehicles-market-A324122

[132] Grand View Research, https://www.grandviewresearch.com/industry-analysis/privacy-enhancing-technologies-market-report

[133] Allied Market Research, https://www.alliedmarketresearch.com/cybersecurity-for-autonomous-vehicles-market-A324122

Based on FHG's input, shown in Table 18, several trends and developments highlight both the opportunity and competitive pressure for ER2c. One emerging trend is the deployment of real-time, on-device anonymization in autonomous vehicles. These technologies blur identifiable visual elements like faces and license plates before data is stored or transmitted, addressing regulatory pressures such as GDPR and CCPA and increasing public sensitivity to surveillance. In this context, PRS stands out by not only anonymizing but also quantifying residual risk.

There is also increasing research attention on Generative AI and its potential for privacy preservation. Unlike traditional blurring, these advanced techniques can achieve better privacy protection with minimal utility loss. Incorporating such techniques into PRS could enhance its competitiveness and technical robustness. Research like the ACM paper on generative anonymization has shown promising directions, which PRS may need to follow to remain state-of-the-art.

Moreover, the demonstration of PRS within TANGO contributes to raising awareness and building trust. Initiatives like the Privacy Risk Demonstrator visually communicate privacy protection levels and risks, potentially increasing user engagement and industry buy-in. There is a clear opportunity to further commercialize PRS through consulting services or privacy assessment tools once its feasibility is fully validated.

Table 18: ER2c Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date	Link
Emerging trend	An emerging trend in autonomous car privacy is the integration of real-time anonymization technologies to protect individuals captured in street footage. Companies are developing on-device AI systems that blur faces, license plates, and other identifiable features before data is stored or transmitted.	Addresses growing regulatory pressures, such as GDPR and CCPA, and public concerns over constant surveillance.	It is also important to raise user awareness of these issues through tools like the Privacy Risk Demonstrator, developed in the Tango project as part of the TSM, which visually illustrates potential privacy risks or privacy protection associated with autonomous vehicle data.	not yet clear	N/A
Impact of new technology adoption:	Research focuses on Generative AI instead of simple blurring techniques	Better privacy protection with minimal utility loss.	Include research Sota in toolkit.	not yet clear	https://dl.acm.org/doi/full/10.1145/3708501?casa_token=2POcnq2QnioAAAAA%3A4Ijl1IGEsupWShbkxldeTRbA0mGCxxzg92RxbhOOIojiLKwOIlLbie8bLroC10D2

					qA0WkiotpC0
New market opportunities	Demonstration of feasibility of the TSM-PRS shall improve and simplify the assessment of anonymization techniques for videos.	With a clear approach it can be feasible to allocate new consulting projects.	Improve TRL level.	not yet clear	N/A

Exploitation Pathway

ER2c is currently not a profit-generating product but is intended to reach TRL 4–5 through the TANGO project. Its initial exploitation route is knowledge transfer via know-how services and private training courses targeted at industry clients once the result matures. The immediate target group for these services includes FHG's existing client base, particularly in the automotive and data privacy domains.

ER2c is intended to be open-source, operating primarily in a B2B context within the automotive sector. The business model does not rely on direct software sales but focuses instead on know-how dissemination, consulting, and potential licensing agreements. Future pricing would depend on the licensing scheme and the level of integration required. While source code would be openly available, FHG anticipates value generation through support, demonstrations, and domain-specific adaptations.

A potential exploitation route is the development of a prototype once TRL increases, followed by licensing if market interest is confirmed. FHG is open to further developing the result either independently or through Horizon Europe or national funding, contingent on future opportunities. The tool is envisioned as a supplementary privacy analytics module that can enhance the compliance posture of automotive platforms, especially those integrating real-time video processing.

The overall exploitation plan includes leveraging PRS as a strategic component within FHG's broader privacy and security consultancy portfolio. Successful demonstrations and use cases inside and outside TANGO will be used to attract new customers and collaborations. Over time, the aim is to position PRS as a recognized benchmark for video anonymization scoring and privacy compliance evaluation, thereby creating pathways for long-term sustainability through modular licensing and targeted consulting projects.

Exploitation paths for ER3b- Confidentiality and Privacy by Design: ABE-toolset

Competitor analysis

The ABE-toolset enters a market where few actors offer comparable fine-grained encryption capabilities. One notable competitor is Kudelski Security, which is developing a prototype using an inner product Functional Encryption (FE) scheme aimed at detecting motion in video streams between surveillance cameras and backends at the gateway level, using the so-called "motion vectors" that are present in the H.264/MPEG-4 AVC standard. This positions Kudelski in privacy-preserving video analysis and data protection at the edge, targeting data owners and processors—particularly in video surveillance domains. Their solution, while innovative, differs from ABE in terms of cryptographic approach and application focus.

Other significant alternatives come from Fully Homomorphic Encryption (FHE) and Secure Multiparty Computation (SMC). These cryptography-based approaches have been explored extensively in high-sensitivity sectors such as healthcare and finance. Other target sectors of these competitors are marketing

(privacy-preserving audience measurement and targeted advertising) and government/defense that needs privacy preserving computation.

Indirectly they also target cloud service providers (CSP) offering privacy-preserving data processing as a service (e.g., confidential cloud computing).

Their methods allow encrypted computations and collaborative analytics without exposing raw data. Although FHE and SMC provide robust privacy guarantees, they are generally heavier in computational requirements and integration complexity compared to ABE, which is more adaptable to modular use cases.

Another competitor is NTT, which also implements Attribute-Based Encryption in their solutions for protecting privacy in surveillance camera images. NTT's target market overlaps partially with ATOS's ABE-toolset, especially concerning data access control in video and streaming data environments. However, the modular structure and multi-domain applicability of ATOS's ABE-toolset—beyond surveillance—give it broader market potential.

- **Market Analysis**
  - **ER3b (ABE-toolset) Encryption Software / Data Encryption Software Market**
    - **Segments**

The ABE-toolset (Attribute-Based Encryption toolset) directly aligns with the **database encryption**, **file/folder encryption**, and **communication encryption** segments in the European encryption software market, as depicted in Figure 33. ABE provides fine-grained, policy-based access controls over encrypted data — making it particularly valuable for applications where selective disclosure is needed, such as secure sharing of patient records, financial data, or IoT streams within the EU's highly regulated sectors[134]. It fits naturally into on-premises and cloud-based deployments where policy-based decryption is vital for GDPR-compliant data governance.

[134] KBV Research, Europe Encryption Software Market

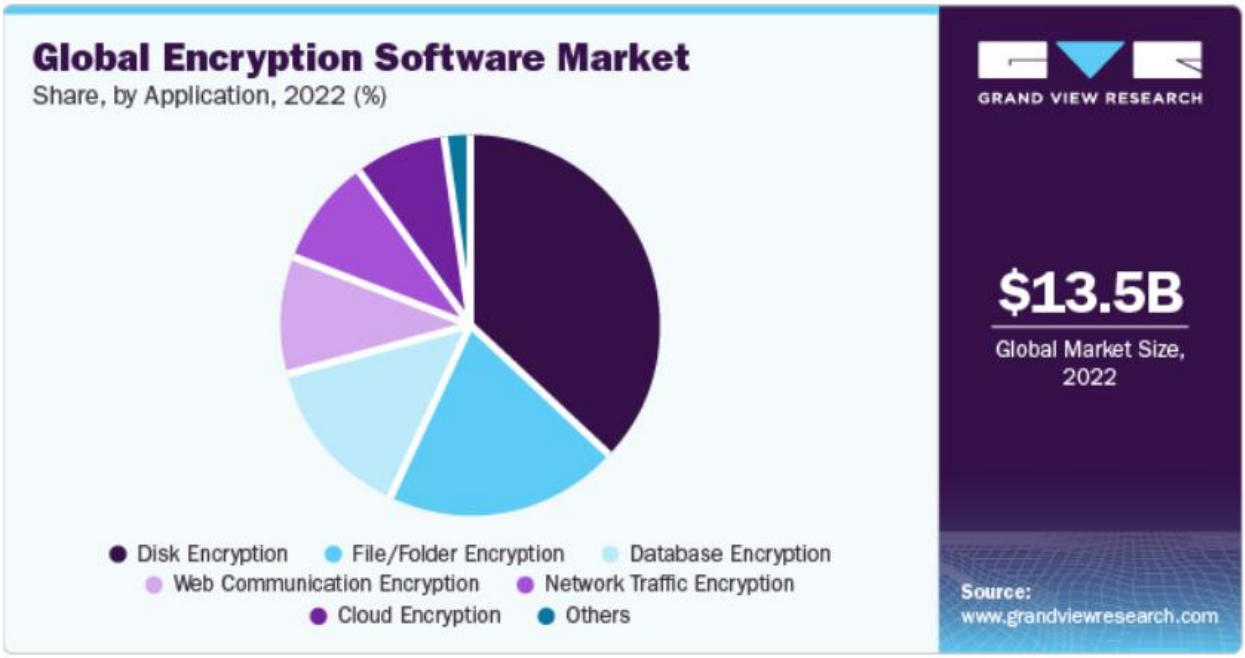


Figure 33: ER3b Encryption Software market segments (source: Grand View Research)

- **Size and Growth Rate**

Europe's encryption software market is projected to grow at a CAGR of 15.6% from 2024 to 2031, with Germany alone expected to reach USD 2.89 billion by 2031[135]. Within this, the database encryption and file/folder encryption segments are core contributors — as granular access control tools like ABE complement standard symmetric encryption by enabling dynamic, attribute-based permission management. The underlying demand is reinforced by the EU's strict GDPR regime and increasing cloud adoption.

- **Trends**

One powerful trend underpinning ABE adoption is the pivot toward **context-aware, zero-trust security models**. Organizations need encryption that supports dynamic access decisions based on attributes like user roles, device trust scores, and time of access — exactly what ABE enables[136]. Furthermore, the rise of hybrid cloud architectures in Europe drives demand for cross-domain encryption solutions where ABE can enforce unified data policies across multiple providers and jurisdiction[137].

- **Barriers**

However, the deployment complexity of ABE remains a challenge. Unlike simpler key-based methods like AES, ABE requires more computational overhead and careful policy design. This can slow integration into legacy IT stacks and elevate operational costs, which can deter resource-constrained

[135] KBV Research, Europe Encryption Software Market
[136] Fortune Business Insights, Encryption Software Market
[137] "Markets and Markets", Encryption Software Market

SMEs from adopting it broadly[138]. Additionally, a shortage of specialized cryptographic expertise in the EU market may further impede implementation speed[139].

- **Opportunities**

Nonetheless, the market opportunity is compelling: Europe's regulatory push for **data sovereignty**, combined with growing cross-border data sharing in healthcare, finance, and supply chains, demands fine-grained, auditable access controls. ABE can uniquely fulfil this need by allowing organizations to encrypt once and delegate decryption securely based on attribute policies, ensuring minimal data exposure while maximizing compliance[140]. This positions ER3b as a critical enabler for secure digital ecosystems under Europe's Digital Decade strategy.

Value proposition analysis

The ABE-toolset provides a robust mechanism for organizations to protect and control access to sensitive data while enabling secure data opening, sharing, and monetization. Built on Attribute-Based Encryption (ABE), the toolset allows organizations to define encryption policies based on user attributes such as department, role, or location. This permits partial views over encrypted data without revealing the entire dataset, making the solution particularly suitable for regulated sectors.

Each module—Key Generator (Issuer Authority), Encryptor, and Decryptor—contributes to a comprehensive access control system that is modular, integrable, and scalable. It protects organizations from internal threats, data leakage, and compliance failures. ATOS targets organizations under high regulatory pressure or involved in ecosystems where strategic data collaboration is essential. These include SaaS/cloud companies, confidential computing initiatives, and sectors pursuing data monetization while maintaining strict privacy and compliance.

Barriers, obstacles and analysis of the standards and regulation

The ABE-toolset, while technically advanced, faces several barriers to adoption. Technology maturity and performance are key concerns, particularly as post-quantum cryptography scenarios could eventually challenge the robustness of current ABE schemes. Market demand for ABE is still under development, and organizations may not yet recognize the added value over simpler encryption methods like symmetric key encryption.

In terms of standards, ABE currently lacks a dedicated ISO standard. However, related areas are covered under standards such as ISO/IEC 18033-3 (Encryption Algorithms), ISO/IEC 11770 (Key Management), and ISO/IEC 29100 (Privacy Framework). Internet-Draft proposals have also been issued for integrating ABE in IETF protocols, suggesting ongoing but not yet finalized standardization. According to ATOS, in the absence of mature commercial standards, ABE and FE often rely on reference frameworks from cryptography libraries.

From a regulatory standpoint, GDPR remains the dominant regulation impacting the marketability and design of the ABE-toolset. It ensures that ATOS's solution must deliver strong, auditable, and lawful access control mechanisms—requirements that ABE is well-positioned to meet.

Technology and market watch

Two relevant developments influence the strategic direction of the ABE-toolset and are shown as ATOS in Table 19. First, real-world implementations of similar technologies—such as NTT's ABE use in

[138] Nature Vault, Data Encryption Software Market Trends & Innovations
[139] Research and Markets, Encryption Software Market
[140] Grand View Research, Encryption Software Market

privacy-preserving surveillance—validate the commercial relevance of ABE schemes in sensitive data environments. Second, real-world applications in hospital settings, although not yet fully detailed, suggest growing demand for fine-grained access control at the data layer, particularly in regulated, high-stakes environments like healthcare.

ATOS is also observing broader efforts to integrate ABE-like cryptographic tools into edge devices for enforcing data policies at the source, and in telemetry sharing where access is granted dynamically based on context. These developments are shaping ATOS's future R&D focus, particularly around lightweight ABE integration.

Table 19: ER3b Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date	Link
N/A	People integrating similar technologies in hospitals in projects	N/A	N/A	N/A	N/A
N/A	NTT (Japanese company with vast research in EU) is offering something similar in their solution	N/A	N/A	N/A	N/A

- **Exploitation Pathway**

ATOS outlines a multi-pronged exploitation strategy for the ABE-toolset. One pathway is integration into existing Identity and Access Management (IAM) solutions—particularly those ATOS already offers, such as Eviden's digital identity solutions. Another strategy is to incorporate ABE-enhanced cloud services into ATOS's broader cybersecurity and cloud portfolios, with a focus on consulting and advisory services. Use cases such as confidential computing and policy-based data sharing in multi-cloud environments are early targets.

Regarding further research, ATOS plans to embed lightweight ABE in edge devices to enforce data access policies at the source, as well as to enable secure telemetry sharing where decryption is policy-bound to entity characteristics (e.g., department, trust level, timestamp), as per this example.

ATOS also plans to support advanced use cases through tools like an "encryption policy engine" with GUI support for authoring and managing policies. In parallel, internal messaging will frame the toolset under a branding theme like "Encryption that understands identity" to generate awareness within Eviden's existing product teams.

Future developments may include participation in additional Horizon Europe projects to further increase the TRL and market readiness of the toolset.

ER3b is built atop open-source libraries, but the result itself will be proprietary. ATOS foresees multiple monetization approaches. For example, B2B SaaS subscriptions are envisaged—especially when integrated with cloud offerings—and can be charged per user, data volume, or number of encryption/decryption events. Where partnerships with SaaS providers exist, tiered pricing will be based on platform scale and service complexity.

Additionally, ATOS explores models such as backend-as-a-service (BaaS) or embedded SDKs to integrate ABE functionality directly into client platforms, including healthcare systems (e.g., FHIR, HL7) and financial tools. System integration services will also be a revenue stream, especially in use cases where the ABE engine needs customization or sector-specific policy enforcement.

Vertical offerings are being developed for healthcare, finance, and government, each configured with sector-specific decryption policies, offering ATOS flexibility in monetization and deployment. These

will allow data to be encrypted once and decrypted only under tightly defined, context-aware criteria, thereby maximizing both security and compliance.

ATOS expects that increasing demand for specialized fine-grained access control and secure data sharing, with an ever-growing market is foreseen to follow the company's growth in the overall encryption market. Based on the previous experiences, ATOS expects to address 3-5% of the total market.

Exploitation paths for ER4- Self-encryption and Decryption Techniques with Multi-Factor Information Recovery Mechanisms

- **Competitor analysis**

The primary competition for ER4 stems from existing hardware-based self-encryption solutions, such as Self-Encrypting Drives (SEDs), which encrypt data as it is written to the disk using a Disk Encryption Key (DEK) stored on the drive. This process is entirely transparent to the user, enabling seamless read/write access while protecting data at rest. These solutions target enterprise users with data confidentiality demands and follow a case-by-case pricing model based on storage and user scale. A second group of competitors includes encrypted hard drives with built-in BitLocker integration. These solutions offload cryptographic processes to hardware, reducing CPU load and allowing for easy enterprise-scale deployment — especially in environments where high performance is critical. Their pricing is typically bundled into broader IT offerings, often discounted or free for educational use. A third competitor type includes advanced RAID-based SEDs, where drives dynamically regenerate encryption key shares upon removal from the array, thus securing data in multi-disk environments. While these hardware solutions are effective, ER4's software-based approach offers more flexibility, especially by incorporating customizable multi-factor recovery and user-defined confidentiality levels, which are currently absent in hardware-driven alternatives.

The primary competition for ER4 stems from existing hardware-based self-encryption solutions, such as Self-Encrypting Drives (SEDs), which encrypt data as it is written to the disk using a Disk Encryption Key (DEK) stored on the drive. This process is entirely transparent to the user, enabling seamless read/write access while protecting data at rest. These solutions target enterprise users with data confidentiality demands and follow a case-by-case pricing model based on storage and user scale. A second group of competitors includes encrypted hard drives with built-in BitLocker integration. These solutions offload cryptographic processes to hardware, reducing CPU load and allowing for easy enterprise-scale deployment — especially in environments where high performance is critical. Their pricing is typically bundled into broader IT offerings, often discounted or free for educational use. A third competitor type includes advanced RAID-based SEDs, where drives dynamically regenerate encryption key shares upon removal from the array, thus securing data in multi-disk environments. While these hardware solutions are effective, ER4's software-based approach offers more flexibility, especially by incorporating customizable multi-factor recovery and user-defined confidentiality levels, which are currently absent in hardware-driven alternatives.

- **Market Analysis**
  - **ER4 — Self-Encryption and Multi-Factor Recovery Encryption Software / Data Encryption Software Market**
    - **Segments**

ER4 aligns primarily with the **disk encryption** and **cloud encryption** segments. Self-encryption mechanisms embed encryption directly into devices or storage volumes, ensuring that data is protected at rest and when devices are lost or stolen — highly relevant given Europe's regulatory mandates for

safeguarding data at endpoints[141]. The Multi-Factor Recovery aspect addresses a critical gap in traditional encryption: secure, user-friendly key recovery in case of loss, an issue often cited by IT admins managing disk encryption at scale.

- **Size and Growth Rate**

Disk encryption remains the dominant application, capturing 36.7% of global market revenue, while cloud encryption is projected to grow at a 19.5% CAGR, driven by Europe's cloud-first policy and increasing BYOD risks[142]. The synergy of these segments underlines robust demand for ER4's dual functionality: seamless encryption combined with robust recovery methods that prevent data loss — a major pain point for European financial and healthcare providers[143].

- **Trends**

Key trends reinforcing ER4's relevance include the explosion of **remote work**, which multiplies endpoint risks, and the EU's push for encryption to secure not just storage but also distributed cloud and edge workloads[144]. Multi-Factor Recovery taps directly into the trend of **multi-factor authentication** (MFA) adoption, extending it to recovery workflows to reduce human error and insider threats. This convergence of encryption and MFA is a clear competitive advantage[145].

- **Barriers**

Yet, a common barrier is the **cost and user friction** associated with self-encrypting drives and integrated recovery solutions. Organizations worry about balancing strong encryption with usability: if recovery processes are cumbersome, staff may resist full disk encryption rollouts or rely on insecure workarounds[146]. This risk is particularly acute for SMEs with limited IT support capacity and low cryptographic literacy[147].

- **Opportunities**

However, the opportunity for ER4 is clear: by combining zero-effort self-encryption with frictionless but secure multi-factor recovery, organizations can meet Europe's stringent compliance standards without compromising productivity. This is critical in sectors where data loss could lead to GDPR penalties or operational downtime. Moreover, the EU's planned updates to the Cybersecurity Act and the push for quantum-safe encryption open new avenues to position ER4 as a future-proof, easy-to-deploy safeguard across laptops, mobile endpoints, and cloud storage[148].

▸ **Value proposition analysis**

The core value of ER4 lies in offering an integrated software-based solution that unites self-encryption with multi-factor information sharing and recovery. Unlike traditional disk encryption solutions that primarily focus on securing local storage, ER4 allows data to be encrypted using the intrinsic properties of the file itself, removing dependency on user-defined passwords. This strengthens protection against credential-based attacks. Furthermore, its multi-factor recovery mechanism enables credentials to be distributed among multiple stakeholders, with data decryption possible by a subset of keyholders,

[141] KBV Research, Europe Encryption Software Market
[142] Grand View Research, Encryption Software Market
[143] Horizon Grand View Research, Europe Banking Encryption Software Market
[144] "Markets and Markets", Encryption Software Market
[145] Research and Markets, Encryption Software Market
[146] Fortune Business Insights, Encryption Software Market
[147] Nature Vault, Data Encryption Software Market Trends
[148] Grand View Research, Encryption Software Market

depending on a user-defined confidentiality threshold. This model is particularly useful in distributed or collaborative environments. In terms of performance, despite the inherently high cost of encrypting large files, ER4 is optimized to avoid extra computational burden compared to traditional tools, thus ensuring usability in real-world enterprise scenarios. Overall, ER4 provides a powerful encryption suite that enhances both security and flexibility, catering to enterprise and personal users with sensitive data protection needs.

- **Barriers, obstacles and analysis of the standards and regulation**

One significant barrier to widespread adoption of ER4 is the high computational overhead required to encrypt large volumes of data, which may limit its scalability in resource-constrained environments. Additionally, while ER4 supports multi-factor information sharing, it currently lacks a property-factor mapping toolkit. This requires users to define mapping relationships manually, which could increase implementation complexity and slow adoption. The development team acknowledges that their solution does not yet offer automated configuration of security parameters per application domain. Obstacles also include the lack of mainstream awareness or understanding of this type of flexible, software-based encryption—especially in environments dominated by hardware-centric approaches. From a compliance perspective, ER4 adheres to GDPR data protection principles and is developed in accordance with standard software engineering practices, using the Apache 2.0 license. Although the encryption domain lacks a specific international standard for multi-factor recovery-based self-encryption, ER4 remains compatible with emerging regulatory frameworks and anticipates future alignment with broader EU cybersecurity directives.

- **Technology and market watch**

Based on DUT's input, depicted in Table 20, demand for secure, flexible data protection and sharing solutions is on the rise globally, and particularly in Europe, where regulatory and commercial pressures are driving adoption of encryption technologies beyond static storage models. ER4 is well-positioned within this context as it meets both operational and compliance requirements. One emerging trend is the shift from static encryption systems to dynamic, policy-driven ones, which incorporate recovery mechanisms that are adaptable to user-defined confidentiality levels. ER4's modular design supports such flexibility and paves the way for user-level control of access management. However, DUT also notes the risk posed by startups or larger vendors with more advanced software engineering capacity, who may be able to replicate or extend ER4's functionality within commercial ecosystems. To counter this, DUT plans to release ER4 as open-source and offer optional enterprise support. This strategy supports community adoption and helps build a base of users and use cases. Ongoing actions include continuous software updates, simplification of the user interface and API, and development of comprehensive documentation to ease integration into existing information systems.

Table 20: ER4 Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date	Link
Emerging trend or development	Data protection is becoming more and more important in the whole world, hereby the demand for secured and flexible data storage/sharing method is becoming highly demanded.	The demand of our software package will increase in the near future. Meanwhile, more customization demands can be seen in the future.	Build a solid user guid for potential software users, simplify user API and make it easy to integrate our software package into any information system.	Ongoing	NA

Hot startups and innovators	There are some ongoing/developing efforts similar to ours and more could come	Could disrupt our unique proposition. Some solution providers are more skilled with provide customized integral system solution to users due to powerful supporting teams and commercial software development environment.	Explore a new niche for our product, such as make our software open-source along with commercial enterprise support in order to build a solid user community and accumulate successful use cases	Ongoing	NA
New market opportunities	See row 2, create new niche enables our product to occupy part of the market	Possibility to get more and long-term customers	Keep on updating the software package and user manual, and give users regular update report in a certain period.	ongoing	NA

Business Model Canvas

Even though ER4 is not considered a key outcome of TANGO, SQD has provided a thorough BMC that elaboratively summarizes the organisation's plans for the result beyond the project's lifetime.

Business Model Canvas				
Key Partners	**Key Activities**	**Value Propositions**	**Customer Relationships**	**Customer Segments**
Key partners for self-encryption software include cybersecurity firms for distribution and integration partners for seamless deployment. Suppliers encompass hardware manufacturers providing secure components and cloud service providers for scalable infrastructure. Partners contribute encryption expertise, distribution channels, and logistical support, enhancing product development,	Self-encryption software requires encryption algorithm development, direct sales, and partnerships. Customer trust is built through transparent communication, with revenue from subscriptions and licensing.	Our self-encryption software offers cutting-edge security, solving the pressing issue of data privacy breaches. Tailored encryption solutions ensure data protection for various customer segments. By reducing the risk of data breaches, we fulfill the crucial need for safeguarding sensitive information. Our value proposition emphasizes	Each customer segment expects personalized support and continuous communication regarding security updates. Our software package will be provided to potential customers for free at the beginning stage. Integrated into our subscription model, these relationships incur moderate costs, justified by increased commercial scale.	Our customer segments primarily consist of businesses and organizations across various industries, prioritizing data security. These include enterprises handling sensitive information, financial institutions, healthcare providers, and government agencies. Our focus is on a segmented market

marketing, and customer support activities.	**Key Resources** Intellectual resources like encryption patents, human resources for algorithm development, and financial resources for research, marketing, and infrastructure investments.	performance, customization, and risk reduction, providing peace of mind at competitive prices.	**Channels** Customer segments prefer digital channels for outreach, including email, website, and social media. Channels are integrated for consistent messaging and branding. Digital channels prove most effective and cost-efficient, integrated seamlessly into customer routines through timely updates and reminders.	approach, tailoring solutions to meet the unique security needs of each sector, ensuring maximum value delivery and customer satisfaction.

Cost Structure	**Revenue Streams**
We will implement different cost structures tailored to various customer segments. Private and small-scale customers will be charged a fixed cost per user license. For large-scale customers, charges will be based on transaction volumes, including data volume for encryption per 24 hours and the number of encryption requests per subscription period.	Customers are willing to pay for the peace of mind and robust security our self-encryption software offers. Currently, most of the security software are subscribed by fixed subscription fees. We believe customers prefer flexible payment options, such as subscription-based or volume-dependent pricing for small business and price-by-negotiation for large business. Hereby we will create different pricing models for various business scenarios. Subscription fees constitute the majority of revenues, supplemented by consultancy fee and secondary development fees.

Exploitation Pathway

DUT's exploitation pathway for ER4 begins with releasing the module as an open-source software package, accessible via GitHub and the Dutch 4TU data repository (https://data.4tu.nl/). This initial step supports wide dissemination and lays the foundation for community-driven testing, feedback, and enhancement. Although there is potential for monetization, no specific commercial plan has been developed at this stage. Instead, DUT is focusing on increasing the Technology Readiness Level (TRL) of ER4 through further research and development using internal resources. The current goal has advanced the module from TRL 3 to TRL 4–5 within the TANGO project timeframe. Future exploitation

activities may include the integration of ER4 as a plugin into mainstream data storage and sharing applications. DUT anticipates that the solution's unique capability—combining feature-based encryption with customizable multi-factor recovery—will make it attractive across many application scenarios, especially in regulated sectors. The university also plans to publish research papers based on the toolkit, helping raise visibility in both academic and industrial communities. Longer-term, there is a vision to refine the offering/product and explore licensing opportunities should demand emerge from enterprise stakeholders. Further Horizon Europe funding may also be pursued to support continued maturation and industrial validation.

Exploitation paths for ER5- ePrivacy Mechanisms, Protocols and Processes

Competitor analysis

Due to the nature of ER5 as a legal and academic deliverable rather than a commercial or market-oriented product, there are no direct competitors in the traditional sense. The output focuses on legal analysis and regulatory interpretation, not on a tool or service for sale. While there are other academic and research entities conducting legal studies on the GDPR, ePrivacy Directive, and Trade Secrets Directive, KUL distinguishes itself through the practical integration of this analysis with specific technologies developed in WP3 of the TANGO project. The value of ER5 lies in its role as a live, evolving legal interpretive framework — one that can be enriched over time with additional use cases, thus staying updated and relevant, unlike many purely academic legal analyses that remain static or retrospective. In this regard, its position is unique, as it offers actionable recommendations specifically tailored to data sharing scenarios involving personal and non-personal data, rather than generic compliance commentary.

Market Analysis

KUL has explicitly indicated that ER5 has no commercial potential or monetization intent, and as such, it does not target a conventional market or operate within a monetizable ecosystem. The result is positioned strictly within the academic and research community, supporting educational, policy, and compliance work rather than targeting enterprise sales or licensing. Nonetheless, the value of the result in a broader ecosystem context is notable: ER5 contributes to the overall trust, compliance, and legal clarity needed for the digital economy, particularly within HE projects and policy-driven data ecosystems. The insights are applicable for policymakers, cloud service providers, enterprises handling sensitive data, and legal researchers who must navigate increasingly complex EU data frameworks. Though not monetized, the result is a core enabler of trust and legal robustness across research and innovation activities that depend on lawful and ethical data sharing.

Value proposition analysis

The value proposition of ER5 lies in its ability to provide **actionable legal insights** that help organizations — particularly those dealing with sensitive or personal data — improve data security and regulatory compliance. Rather than offering only a theoretical overview, ER5 delivers concrete guidance on the applicability of EU legislation (including the GDPR, ePrivacy Directive, and Trade Secrets Directive) in the context of specific technologies developed in TANGO's WP3. This gives it particular utility for stakeholders seeking up-to-date and practical interpretations. Furthermore, ER5 is not a static analysis: KUL emphasizes the ongoing enrichment of the framework through new use cases, which increases the robustness and relevance of the legal recommendations. This makes the result especially valuable for legal compliance officers, cloud service providers, and HE research consortia who must stay aligned with evolving data protection norms and practices.

Barriers, obstacles and analysis of the standards and regulation

KUL did not identify any formal barriers or obstacles for ER5, which is consistent with the result's academic nature and non-commercial intent. However, implicitly, one can note that the effectiveness of legal research in influencing practice or policy may be dependent on uptake by stakeholders beyond academia — such as regulators, industry consortia, or technical standardization bodies. There is also an inherent challenge in translating legal recommendations into standardized practices for hybrid data-sharing models, particularly when regulatory frameworks like the ePrivacy Regulation remain in flux or incomplete. Nonetheless, ER5 is firmly grounded in the interpretation of well-established legal instruments: the GDPR, the ePrivacy Directive, and the Trade Secrets Directive. It provides interpretive clarity on how these frameworks apply to personal and non-personal data flows, and thus contributes meaningfully to the informal standard-setting needed in digital innovation projects like TANGO.

- **Technology and market watch**

No explicit inputs were provided by KUL for this section, reflecting again the non-technical nature of the result. However, from the result description, it is clear that ER5 stays aligned with ongoing legal and regulatory developments in the data protection and privacy domain. Its relevance is bolstered by continuous legislative shifts, such as ongoing negotiations around the ePrivacy Regulation, enforcement patterns around GDPR (e.g., around lawfulness, purpose limitation, and transparency), and new discussions about non-personal data sharing under the Data Act and Data Governance Act. As such, while there is no "technology watch" per se, ER5 is highly sensitive to the evolving legal landscape, and its continued value depends on maintaining this responsiveness through legal monitoring and scholarly analysis. It acts as a legal observatory for digital data-sharing technologies and will remain relevant as long as regulatory frameworks evolve.

Table 21: ER5 Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date	Link
N/A	N/A	N/A	N/A	N/A	N/A

- **Exploitation Pathway**

KUL has a clearly articulated non-commercial exploitation strategy for ER5. The result is open source and copyrighted, meaning its findings are publicly available but protected in terms of authorship. Its primary exploitation pathway is through **academic and research integration**. Specifically, ER5 will be used to reinforce KUL's own **research competencies, position, and capacity**, ensuring continued leadership in privacy and data protection research. The findings from TANGO will directly **enrich the university's curricula**, enabling both current and future researchers to gain deep, practical insight into EU data law through applied case studies.

KUL also aims to use the result to **expand collaborations with industry and applied research institutions**, creating bridges between legal academia and real-world technology developers. Exploitation activities will include the **publication of scientific articles** in high-impact journals, **participation in international conferences**, and the **attraction of further R&D funding** through new EU or nationally funded projects. Teaching is another central axis of exploitation, with ER5 forming part of legal education content for students and legal researchers. In sum, the result is being leveraged to strengthen institutional capacity, contribute to the broader scientific community, and create new academic and research collaborations with long-term impact.

Exploitation paths for ER6a- SSI Wallet

- **Competitor analysis**

The primary competitor identified by VTT for ER6a is the broad group of **existing SSI wallet providers**. These competitors target users of digital credentials and typically offer products in a **freemium model**, where the core wallet is available free of charge and additional premium features are accessed via a monthly or yearly subscription. This model supports user acquisition at scale while offering value-added services to enterprise or institutional users. Although specific names were not listed by VTT, it can be inferred that major industry players such as **Trinsic**, **Lissi**, **Dock**, and **Evernym** fall into this category, all of which provide verifiable credential (VC) management platforms based on decentralized identity standards. These wallets focus on secure credential storage, selective disclosure, and DID-based authentication — overlapping directly with ER6a's design goals. Notably, the key differentiator for ER6a lies in its **integration with issuer and verifier infrastructure** and its capacity to track where and how often users present their VCs, offering enhanced visibility and control to the user.

- **Market Analysis**
  - **ER6a – SSI Wallet, using the Self-Sovereign Identity (SSI) market**
    - **Segments**

ER6a fits squarely within the **Self-Sovereign Identity Wallet segment**, a critical component of the broader **SSI infrastructure stack**, which includes verifiable credentials, decentralized identifiers (DIDs), credential issuers, and verifiers. The personal credential manager (PCM) described in ER6a specifically aligns with the **"Identity Wallet" sub-segment**, where users securely store and manage their verifiable credentials, and is directly applicable to European initiatives such as the **EU Digital Identity Wallet** under eIDAS 2.0. According to Grand View Research, SSI wallets are being adopted primarily in **government ID programs, financial services, and healthcare**, as these sectors demand high assurance levels and strict user control over data usage[149]. This puts ER6a within a segment that is both technically foundational and strategically targeted by EU digital identity legislation.

- **Size and Growth Rate**

The **European SSI market** is experiencing exponential growth, as shown in Figure 34, driven by increasing regulatory alignment, technological maturity, and public-sector adoption. Cognitive Market Research reports that the **European SSI market was valued at USD 6.18 million in 2023** and is forecast to reach **USD 264.33 million by 2031**, growing at a **CAGR of 64.56%** from 2024 to 2031[150]. This is consistent with the global outlook, where the total SSI market is projected to grow to USD 589.02 billion by 2034, registering a staggering **CAGR of 82.50%**[151]. These figures underscore the explosive market potential for SSI wallets like ER6a, especially within Europe where regulatory frameworks are already in motion.

[149] Grand View Research – Europe Outlook
[150] Cognitive Market Research
[151] Prophecy Market Insights via GlobeNewswire

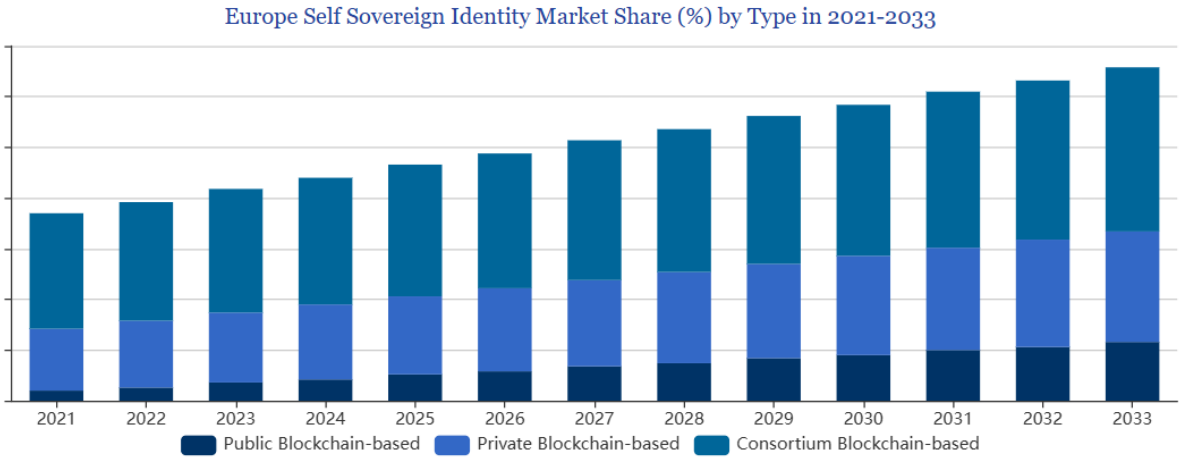


Figure 34: ER6a Self-Sovereign Identity (SSI) market size (source: Cognitive Market Research)

- **Trends**

One of the most influential trends supporting ER6a is the **rising implementation of digital identity wallets within national ID ecosystems**. In Europe, the eIDAS 2.0 regulation mandates the development of a European Digital Identity Wallet by 2026, which is expected to catalyze wallet adoption across public and private sectors. Grand View Research emphasizes the growing demand for **user-centric identity solutions** that support **interoperable, verifiable credentials** and enable **cross-border digital trust**[152]. Meanwhile, Precedence Research points out that blockchain-enabled wallets with selective disclosure and consent management features—key attributes of ER6a—are increasingly seen as the preferred tool for privacy-preserving digital identity interaction [153]. The **European Commission's funding of pilot projects under the Digital Europe Programme** is further accelerating adoption, making now a critical window for ER6a to align with interoperable infrastructure.

- **Barriers**

Despite favourable momentum, ER6a faces several barriers to market adoption. First, **fragmented adoption among EU member states** may slow down the interoperability and standardization needed for cross-border SSI solutions. KBV Research notes that **regulatory heterogeneity and inconsistent readiness of national infrastructure** could hinder full-scale wallet deployment in the short term[154]. Moreover, **limited public awareness and trust in SSI frameworks** remains a challenge. Although users increasingly care about data privacy, they are often unfamiliar with decentralized identity models, which could slow user onboarding and retention. Technical complexity, particularly in ensuring **seamless issuer-verifier-wallet integration** (as proposed in ER6a), could further complicate early-stage deployments. Grand View Research also flags the **lack of industry-wide governance frameworks** as a risk, especially for commercial players entering the EU identity wallet ecosystem[155].

- **Opportunities**

Despite these hurdles, ER6a is strongly positioned to capitalize on multiple concrete opportunities. The introduction of **mandatory EU Digital Identity Wallets under eIDAS 2.0** provides a near-term

[152] Grand View Research – Market Report
[153] Precedence Research
[154] KBV Research
[155] Grand View Research – Europe Outlook

regulatory tailwind. As the European Commission mandates wallet adoption for key use cases—banking, travel, healthcare, and education—there is a significant opportunity for PCM-based solutions like ER6a to serve as **modular components or white-label implementations** for national or corporate wallet offerings. According to Cognitive Market Research, the surge in wallet deployments across public and financial sectors is expected to generate **new business models around credential monetization, consent management, and compliance automation**—all functions aligned with ER6a's design[156]. Furthermore, the global spotlight on **digital sovereignty and GDPR compliance** gives ER6a a strong competitive advantage as a **European-built, privacy-by-design solution**, increasing its appeal among EU institutions and enterprises looking for trusted local solutions[157].

- **Value proposition analysis**

The **value proposition of ER6a** is rooted in its role as a **secure, privacy-preserving solution for managing verifiable credentials** in a human-centric digital society. VTT emphasizes that the core of its mission is **research and development**, with the goal of adapting technologies that are **fit for the future**. The ER6a SSI Wallet, provides users with the ability not only to store VCs securely, but also to **track the context and frequency of their use**, enhancing transparency and accountability. Integration with both the **issuer and verifier systems** as well as **dp-ABC** strengthens its position as a holistic self-sovereign identity solution. The wallet reflects VTT's broader mission to develop **privacy-enhancing technologies** and deliver **secure digital identity infrastructures** that support compliance, user autonomy, and technological sovereignty. Compared to existing tools, ER6a's focus on **user-side control and traceability** sets it apart, especially in institutional or regulated environments where auditability and consent tracking are critical.

- **Barriers, obstacles and analysis of the standards and regulation**

One of the current **barriers** to ER6a's wider deployment is the fact that the product is still in **webapp form**, limiting its maturity, marketing potential and readiness for full-scale user adoption. In terms of **technical obstacles**, **interoperability with other SSI ecosystems** is still constrained — a key consideration given the EU's push for **cross-border digital identity** via eIDAS 2.0 and initiatives like EBSI. Overcoming these limitations will require aligning with established and emerging standards.

ER6a is designed in compliance with relevant **regulatory frameworks**, particularly the **European Digital Identity (EUID)** initiative and the **European Blockchain Services Infrastructure (EBSI)**, both of which are setting the stage for interoperable digital identity systems across the EU. Technologically, ER6a adheres to the **W3C Verifiable Credentials and Decentralized Identifiers** standards — foundational protocols for any SSI-compatible infrastructure. These standards are critical for ensuring vendor-neutral implementation and future-proofing against changes in the EU regulatory landscape. Still, the **fragmented national readiness** and varying levels of regulatory and infrastructure adoption across EU member states present ongoing implementation risks that must be actively managed.

- **Technology and market watch**

VTT's market and technology watch, detailed in Table 22, indicates a highly dynamic innovation landscape around SSI. Several **emerging trends** are reinforcing the relevance of ER6a. Firstly, there is a **growing interest in models where users control their own identities**, consistent with both the philosophy and implementation of SSI. Secondly, the **adoption of DIDs and verifiable credentials** is

[156] Cognitive Market Research
[157] Grand View Research – Market Report

accelerating, driven by global projects such as **Microsoft's ION** on the Bitcoin blockchain and **Hyperledger Indy**, both of which prioritize **interoperability and privacy**.

Active companies such as **IBM** are investing heavily in blockchain-based digital identity platforms for enterprise contexts, applying advanced cryptographic techniques for secure credential handling. Microsoft is similarly advancing its **decentralized identity stack** via U-Prove and ION, demonstrating commitment to **privacy-preserving, scalable solutions**. Meanwhile, startups like **uPort** are innovating in **ZKP-based user-centric identity verification**, further validating ER6a's relevance.

A particularly important development is the **EUDIw initiative**, which is expected to drive widespread adoption of digital identity wallets throughout the EU. This initiative aligns perfectly with ER6a's architecture and ambition, and its advancement is likely to increase both demand for and compatibility expectations of products like ER6a.

Table 22: ER6a Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date	Link
Emerging trend or development	Growing interest in SSI models where users control their own identities.	Positive	N/A	N/A	N/A
Emerging trend or development	Increasing adoption of DIDs and verifiable credentials, driven by projects like Microsoft's ION and Hyperledger's Indy, ensuring interoperability and security.	Positive	N/A	N/A	N/A
Active companies and their R&D strategies	IBM: Investing in secure digital identity solutions using blockchain and advanced cryptographic techniques, focusing on enterprise applications.	Positive	N/A	N/A	http://primelife.ercim.eu/results/opensource/55-identity-mixer
Active companies and their R&D strategies	Microsoft: Developing decentralized identity solutions with the ION project on the Bitcoin blockchain, emphasizing scalability and privacy.	Positive	N/A	N/A	https://www.microsoft.com/en-us/research/project/u-prove/ https://www.microsoft.com/en-us/research/project/ion/
Hot startups and innovators	uPort: Providing user-centric identity solutions with secure and private	Positive	N/A	N/A	

	verification processes using blockchain and ZKP technologies.				
Emerging trend or development	The EUDIw initiative is likely to drive widespread adoption of digital identity solutions across the EU, providing a significant boost to technologies like DP-ABC with ZKP.	Positive	N/A	N/A	https://eudiwalletconsortium.org

▸ **Exploitation Pathway**

VTT has not yet finalized a precise exploitation pathway for ER6a, but its strategy includes both **open access and commercialization considerations**. One potential route is to continue developing the solution within **future Horizon Europe projects**, particularly focusing on integrating **post-quantum cryptographic resilience** — ensuring the wallet remains secure even in future cryptographic paradigms. The ER6a product is already designed with **modular expansion and secure credential handling** in mind, and the goal is to build it into a **mature, user-ready identity wallet** that aligns fully with evolving standards like **eIDAS 2.0**.

As for business models, VTT considers the **freemium model** as a viable strategy. In this approach, the wallet would be **free for individual users**, thus ensuring wide accessibility and adoption, while **more advanced functionality** (such as organizational management tools, analytics dashboards, or enterprise integrations) could be monetized through **monthly or yearly subscriptions**. This would allow ER6a to scale gradually while remaining true to its privacy-by-design and user-centric roots.

The **exploitation plan** also includes deepening R&D activities through further **EU-funded projects**, specifically targeting **integration with modern cryptographic algorithms** and ensuring alignment with **post-quantum security standards**. These efforts are expected to strengthen the solution's security posture and broaden its appeal across both governmental and commercial domains.

Exploitation paths for ER6b- SSI Zero Knowledge Proof

▸ **Competitor analysis**

The competitive landscape for ER6b centers on digital identity solutions that leverage privacy-preserving technologies. The most relevant competitor category is Single Sign-On (SSO) identity solutions, which simplify user authentication across multiple applications using a single credential set. While these systems enhance usability and administrative control, they typically lack robust privacy guarantees and selective disclosure, positioning ER6b as a more secure alternative. The primary target customers for these solutions are enterprises that manage access to numerous internal and external systems and aim to reduce password fatigue and streamline access control for employees.

In addition, IBM's Identity Mixer (Idemix) represents a significant competitor in the space. This protocol suite enables anonymous credential management and selective disclosure without revealing excessive personal information. It allows users to prove possession of attributes and claims without revealing more information than necessary, focusing on privacy-preserving authentication. Its main market comprises privacy-focused digital services, secure voting systems, and applications requiring unlinkability. Similarly, Microsoft's U-Prove technology offers users the ability to obtain verifiable tokens and selectively disclose identity attributes. It targets access control systems and online services that prioritize confidentiality in identity verification. These technologies compete directly with ER6b's focus on selective attribute disclosure, anonymity, and security via Zero-Knowledge Proofs (ZKPs). However,

ER6b differentiates itself through its integration with W3C Verifiable Credentials and OIDC4VP specifications and its use of the Pointcheval-Sanders multi-signature scheme for distributed, privacy-preserving authentication.

- **Market Analysis**
  - **ER6b – SSI Zero Knowledge Proof within the Decentralized Identity Market**
    - **Segments**

ER6b, which combines **Self-Sovereign Identity (SSI)** with **Zero-Knowledge Proofs (ZKP)**, aligns directly with the **non-biometric identity verification**, **credential management**, and **privacy-preserving authentication** segments of the European decentralized identity market. Zero-Knowledge Proofs allow users to prove facts about their identity without disclosing underlying sensitive data—an essential fit for the SSI model, which emphasizes user-owned, self-managed identity credentials. This combination is especially relevant for end-users in the **BFSI, government, and healthcare verticals**, depicted in Figure 35,where privacy and compliance with GDPR are paramount[158].

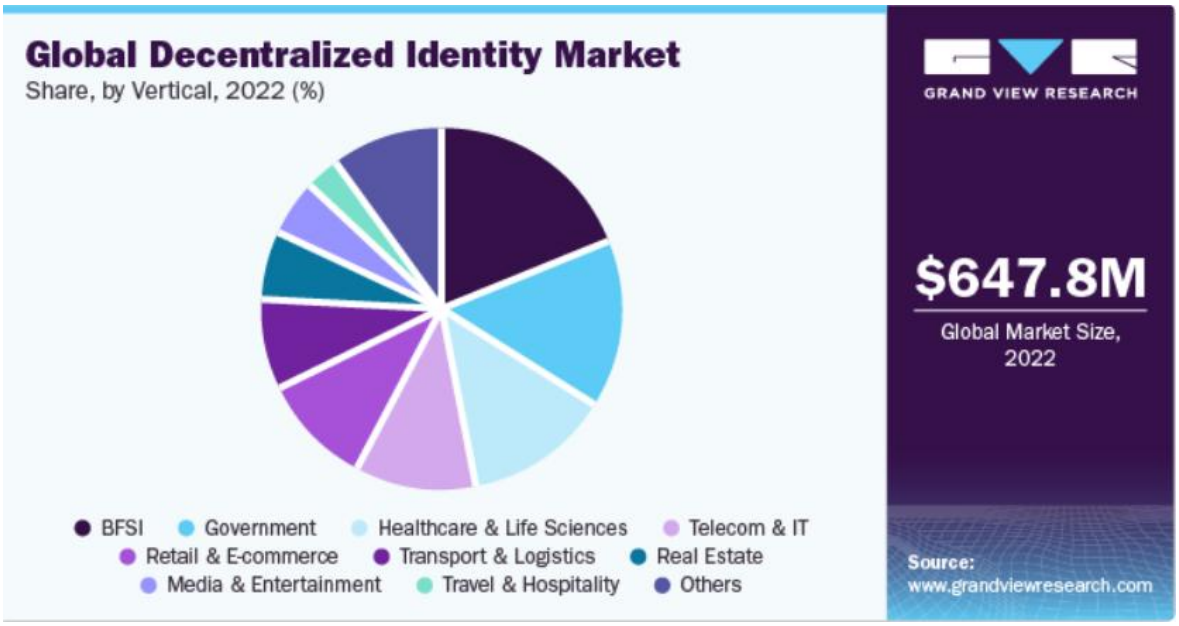


Figure 35: ER6b Decentralized Identity Market segments (source: Grand View Research)

- **Size and Growth Rate**

The European decentralized identity market is poised for explosive growth, with forecasts projecting a leap from **USD 298.8 million in 2023 to USD 27.4 billion by 2030**, marking an unprecedented **CAGR of 90.7%**[159]. Within this, technologies like Zero-Knowledge Proofs are expected to carve out a growing niche, projected globally to reach USD 0.45 billion by 2035, reflecting their emerging but pivotal role in next-generation privacy frameworks[160]. This indicates a ripe and expanding addressable market for KER6b, especially as European sectors transition toward privacy-first digital identity solutions.

[158] Data Bridge Market Research, Decentralized Identity Market; Grand View Research, Decentralized Identity Market
[159] Horizon Grand View Research, Europe Decentralized Identity Market
[160] Market Research Future, Decentralized Identity Market

- **Trends**

A core trend driving adoption for ER6b is the **surge in privacy-centric regulations** like the EU's GDPR and upcoming eIDAS 2.0 framework, which demand user-centric data control and minimal data disclosure. Zero-Knowledge Proofs directly enable organizations to verify users' attributes without handling or storing personal information—aligning with the EU's vision of data minimization[161]. Moreover, SSI and ZKP are at the forefront of the push toward **passwordless authentication** and **cross-border interoperable digital identities**, which the European Commission actively supports through initiatives like the European Digital Identity Wallet[162].

- **Barriers**

However, barriers to KER6b adoption exist, notably **technical complexity** and a lack of widespread expertise in implementing Zero-Knowledge cryptography within operational systems. Many enterprises lack in-house capability to integrate advanced cryptographic protocols into existing infrastructure, slowing large-scale rollouts[163]. Regulatory uncertainty and the absence of universally agreed interoperability standards across EU member states further complicate deployment, with some national digital ID strategies still preferring centralized solutions[164].

- **Opportunities**

Nevertheless, the opportunity for ER6b in Europe is substantial. Sectors like banking, e-government, and healthcare urgently require robust identity verification solutions that ensure compliance with strict EU data privacy laws while enabling seamless user experiences. Zero-Knowledge Proofs unlock the possibility for users to share verifiable credentials (like age, citizenship, or creditworthiness) without disclosing full documents, thereby reducing fraud risk and protecting privacy—a capability highly valued in cross-border finance, telehealth, and online voting use cases[165]. Additionally, Europe's ambitious push for interoperable digital wallets under the Digital Europe Programme means ER6b's privacy-preserving proofs could become a core enabling technology for trusted, user-controlled identity verification across the continent[166].

▸ Value proposition analysis

The primary value proposition of ER6b lies in its ability to deliver secure, selective identity attribute disclosure without revealing users' full credentials or sensitive data. This is achieved through the combination of distributed privacy-preserving Attribute-Based Credentials (ABC) and Zero-Knowledge Proofs. Unlike traditional centralized authentication methods, ER6b empowers users to manage their own digital identities, offering a higher level of privacy and control. The cryptographic engine, built on Pointcheval-Sanders multi-signatures and fully compatible with W3C Verifiable Credentials, ensures that only the minimum necessary data is revealed. Verifiable credentials are issued by a trusted authority and stored under the control of the user, who can present derived proofs to verifiers in compliance with SIOP and OIDC4VP protocols. This system enables security, user empowerment, and GDPR compliance. The value delivered to customers includes strong identity protection, reduced exposure to data breaches, and regulatory alignment for applications where trust and privacy are essential.

---

[161] IMARC Group, Decentralized Identity Market
[162] "Markets and Markets", Decentralized Identity Market
[163] Globenewswire, Decentralized Identity Systems Market
[164] "Markets and Markets", Decentralized Identity Market
[165] Data Bridge Market Research, Decentralized Identity Market; Allied Market Research, Decentralized Identity Market
[166] Horizon Grand View Research, Europe Decentralized Identity Market

- **Barriers, obstacles and analysis of the standards and regulation**

Although ER6b is technically advanced and aligns with regulatory demands, its market rollout is likely to face a number of obstacles. One key challenge is the technical complexity involved in developing and deploying ZKP protocols. These require specialized cryptographic expertise and are difficult to integrate into existing authentication systems. Additionally, computational limitations remain a significant hurdle—ZKPs are more resource-intensive than traditional signature-based systems, which may slow performance, particularly in large-scale environments.

Despite these issues, ER6b is fully compliant with leading standards and regulations. It supports DLT architectures and follows major standards such as W3C Decentralized Identifiers (DID), Verifiable Credentials (VC), OpenID Connect (OIDC), and the OIDC4VP protocol. On the regulatory side, the design fully respects and supports the principles and obligations set out in the General Data Protection Regulation (GDPR), ensuring lawful data processing, user consent, and minimization.

- **Technology and market watch**

The SSI and ZKP space is witnessing accelerated momentum, with key emerging developments closely aligned with ER6b's trajectory. As stated by UMU and presented in There is increasing interest in user-controlled SSI models integrated with ZKP for enhanced privacy. Projects such as Microsoft's ION (on the Bitcoin blockchain) and IBM's Identity Mixer are advancing scalable, privacy-enhancing identity systems. Hyperledger Indy is also a leading initiative promoting verifiable credentials and interoperability.

Startups like uPort are pushing forward with blockchain-based identity solutions that utilize Zero-Knowledge Proofs and selective disclosure mechanisms. These innovations point to a growing ecosystem in which ER6b can compete and differentiate itself through technical sophistication and integration flexibility.

The European Digital Identity Wallet (EUDIw) initiative represents another critical trend. As the EU moves toward broad adoption of digital identity systems with privacy-preserving features, technologies like ER6b will gain traction as foundational components. The EUDIw push provides a policy-aligned context in which to position ER6b as both a research and applied solution.

Table 23: ER6b Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date	Link
Emerging trend or development	Growing interest in SSI models where users control their own identities, integrating ZKP for enhanced privacy.	Positive	N/A	N/A	
Emerging trend or development	Increasing adoption of DIDs and verifiable credentials, driven by projects like Microsoft's ION and Hyperledger's Indy, ensuring interoperability and security.	Positive	N/A	N/A	
Active companies and their R&D	IBM: Investing in secure digital identity solutions	Positive	N/A	N/A	http://primelife.ercim.

Item	Description	Possible Impact	Actions	Effective Date	Link
strategies	using blockchain and advanced cryptographic techniques, focusing on enterprise applications.				eu/results/opensource/55-identity-mixer
Active companies and their R&D strategies	Microsoft: Developing decentralized identity solutions with the ION project on the Bitcoin blockchain, emphasizing scalability and privacy.	Positive	N/A	N/A	https://www.microsoft.com/en-us/research/project/u-prove/ https://www.microsoft.com/en-us/research/project/ion/
Hot startups and innovators	uPort: Providing user-centric identity solutions with secure and private verification processes using blockchain and ZKP technologies.	Positive	N/A	N/A	
Impact of new technology adoption	Enhanced Privacy: Adoption of ZKP significantly improves privacy, allowing users to prove attributes without revealing sensitive information.	Positive	N/A	N/A	
Impact of new technology adoption	Regulatory Compliance: Adoption of ZKP helps organizations comply with stringent data protection laws, reducing legal risks and penalties.	Positive	N/A	N/A	
New market opportunities	Fields which require an extra layer of privacy and security: financial, healthcare, government services.		N/A	N/A	

Exploitation Pathway

UMU plans to exploit ER6b by embedding it into its ongoing research activities and related EU-funded projects. The identity wallet component will be released as open-source, with all designs and cryptographic implementations made publicly accessible. Specialized training and outreach will be offered to foster understanding and adoption of the solution in academic and industrial circles.

Furthermore, the team will pursue non-exclusive licensing agreements to support uptake in identity-focused applications across both public and private sectors.

The broader exploitation strategy is multi-phased. In the short term, UMU will integrate the ER6b prototype into university curricula to derive feedback from students and researchers. In the mid-term, the plan includes launching advanced GDPR/eIDAS-compliant identity training programmes, alongside engaging regional stakeholders for technology validation. Over the long term, the goal is to scale the licensing model and apply for new Horizon Europe calls, using real-world deployments to inform standardization and market-readiness.

UMU will pursue a hybrid business model to sustain and grow ER6b. First, the solution will be released as open-source software to encourage adoption and transparency. Alongside this, UMU will monetize expertise through structured training courses, capacity-building workshops, and integration support for institutional partners. The wallet will serve as a modular, adaptable component that can be embedded into identity management ecosystems, making it especially attractive to public-sector clients and academic consortia.

Key revenue streams will come from tailored training programs and service-based agreements for integration support. Primary customers are expected to include governmental agencies, national digital identity schemes, and European R&D consortia. UMU will also continue leveraging its academic reputation and regulatory knowledge to pursue further Horizon Europe funding aligned with post-quantum cryptography and decentralized identity.

Exploitation paths for ER6c- SSI Agent

- **Competitor analysis**

ER6c enters a competitive field with several established SSI component providers already active in the European and global markets. Key competitors include Signicat (Norway), Validated ID, Talanche (France), Izertis, Thales, Gataca, and Jolocom. These providers offer a range of SSI issuance and verification components targeting both public and private sector customers. Their target customers typically align with those of ER6c: issuers such as government agencies, certification bodies, and training centers; verifiers such as HR departments, banks, and online service providers conducting KYC or onboarding procedures; and citizens using SSI as a form of digital notarization.

What distinguishes ER6c is its high degree of alignment with the eIDAS 2.0 framework, European Blockchain Services Infrastructure (EBSI), and the Data Spaces Business Alliance. While competitors may offer partial interoperability or sector-specific solutions, ER6c provides end-to-end interoperability with both decentralized SSI ecosystems and legacy federated systems via OpenID Connect protocols. Furthermore, ER6c is specifically designed to ensure reusability and conformance with EBSI Wallet testing protocols, making it more robust for cross-border implementations.

- **Market Analysis**
  - **Self-Sovereign Identity (SSI) Market analysis for ER6c**
    - **Segments**

ER6c corresponds primarily to the *software infrastructure and credential issuance/verification* segment of the SSI market. Its role as an issuer/verifier tool places it in the backbone of interoperable digital identity frameworks in Europe. According to KBV Research, this segment is experiencing accelerated adoption across public and private sectors, especially as governments, academic institutions, and large enterprises seek secure methods for issuing and verifying digital credentials. The ER6c component's alignment with the European Blockchain Services Infrastructure (EBSI) and eIDAS 2.0 architecture

positions it as a key enabler of cross-border trust frameworks and data exchange protocols, which is crucial in the credential exchange and verification subsegment outlined in Grand View Research.

- **Size and Growth Rate**

The European Self-Sovereign Identity market is expanding at a rapid pace. According to Cognitive Market Research, the market in Europe is projected to grow at an exceptional CAGR of **64.56% between 2024 and 2031**, reflecting regulatory momentum and increasing institutional investment in decentralized identity solutions. Globally, Prophecy Market Insights estimates the total SSI market will reach **USD 589.02 billion by 2034**, supported by government and enterprise initiatives—especially in the EU, where trust frameworks like eIDAS 2.0 create a strong foundation for adoption. Grand View Research adds that Europe is expected to be one of the largest regional contributors due to the EU's aggressive push for digital identity sovereignty.

- **Trends**

One of the most prominent trends supporting ER6c is the adoption of the **European Digital Identity Framework (EUDI Wallet)** under eIDAS 2.0, which requires tools like ER6c for credential issuance and verification. Precedence Research notes that government-led projects are increasingly driving the implementation of decentralized identity infrastructures, where issuer-verifier interoperability is critical. Moreover, Grand View Research points to the growing importance of integrating SSI solutions with legacy systems via standards like OpenID Connect, a feature explicitly supported by ER6c. The trend of creating **interoperable and reusable digital identity components** across sectors—especially for government, education, and finance—is underlined by KBV Research, which identifies these as high-priority application areas for SSI agents and credentialing tools.

- **Barriers**

Despite promising growth, ER6c may face challenges that affect its market impact. According to Cognitive Market Research, one significant barrier is **fragmentation in protocol standards** and limited cross-border interoperability, especially for entities outside the eIDAS ecosystem. Precedence Research emphasizes that **slow institutional adaptation** to decentralized models—due to risk aversion or lack of technical expertise—may delay SSI agent deployment in legacy systems. Additionally, Grand View Research points out that the cost and complexity of certifying tools against frameworks like EBSI or the Data Spaces Business Alliance may deter smaller entities from adopting issuer/verifier components like ER6c.

- **Opportunities**

ER6c is ideally positioned to capture opportunities arising from the convergence of **regulatory compliance and digital identity modernization**. KBV Research reports a sharp rise in demand for reusable SSI components as public institutions move to align with eIDAS 2.0 and the European Digital Identity initiative. In particular, ER6c's ability to integrate with both **federated legacy systems** and **decentralized infrastructures** presents it as a unique bridge technology, offering dual value to both early adopters and conservative institutions. Moreover, Grand View Research suggests that cross-border credential interoperability and support for European Data Spaces are crucial differentiators in the EU market, areas where ER6c is directly compliant. Finally, Prophecy Market Insights projects explosive global market growth, meaning early alignment with EU frameworks could enable ER6c to scale beyond Europe in the medium term.

▸ Value proposition analysis

The core value proposition of ER6c lies in offering customizable components for SSI ecosystems that reduce credential issuance costs while ensuring high interoperability. The component provides robust

support for issuers and verifiers by aligning with the European Digital Identity architecture. It delivers full compliance with the European Blockchain Services Infrastructure (EBSI) Wallet Conformance Testing and eIDAS 2.0 standards, ensuring reusability across European Data Spaces.

By enabling integration with legacy federated identity systems through OpenID Connect, ER6c further supports seamless migration paths for institutions hesitant to transition to full decentralization. The solution empowers users and organizations with control over identification and authentication data, allowing them to issue and verify credentials without dependence on central authorities. In doing so, it addresses both technical and regulatory demands for trust, security, and digital sovereignty in a scalable way.

- **Barriers, obstacles and analysis of the standards and regulation**

While ER6c is well-positioned, it faces specific barriers. First, the monetization model—charging issuers or verifiers for operations like DID document creation, VC signing, or credential verification—could discourage adoption, especially among public institutions. This is particularly relevant given that these services are often expected to be cost-neutral or subsidized. Secondly, while ER6c has potential to support data-driven services (e.g., a job data marketplace using VCs), implementing dynamic user consent mechanisms remains a legal and technical hurdle.

In terms of standards, ER6c operates in a landscape characterized by emerging frameworks. The main standards it adheres to include W3C Verifiable Credentials, Decentralized Identifiers (DIDs), and OpenID Connect for Verifiable Presentations (OIDC4VP). Regulatory frameworks such as the eIDAS 2.0 regulation are still being refined, which presents both a challenge and an opportunity: while standards may shift, early compliance could yield a first-mover advantage once finalized.

- **Technology and market watch**

Based on ATOS' input, detailed in Table 24, several emerging trends and market dynamics are highly relevant to ER6c. First, the digitization of documents—such as diplomas, licenses, and certificates—is a driving force behind the growing demand for verifiable credential issuance and verification tools. ER6c supports this shift directly through its issuer and verifier capabilities. Furthermore, there's increasing insight into SSI transactions that can be monetized, leading to new business models such as charging per transaction or licensing usage to credential issuers and verifiers.

The formation of ecosystems with clear roles—issuers, verifiers, attribute providers, and product owners—is another critical development. This structured growth in the SSI ecosystem supports standardization and makes market entry easier for compliant, interoperable solutions like ER6c. These trends are expected to intensify as the European Digital Identity Framework (EUDI Wallet) matures, further reinforcing the need for components like ER6c.

Table 24: ER6c Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date	Link
New market opportunities	There is more market insight into SSI operations and transactions that are valuable and could be charged.	New business models	Continue market watch	Project duration	N/A
Emerging trend or development	Digitization of documents	Docs (certificates etc) that can be VC	Continue market watch	Project duration	N/A
Active companies	Formation of ecosystem with	Increase of	Continue	Project	N/A

and their R&D strategies	issuers, verifiers, product owners, etc	market demand, standardization	market watch	duration	

Exploitation Pathway

ATOS intends to exploit ER6c by integrating the result into its existing portfolio of identity and access management (IAM) products, such as Evidian Orbion. This integration will offer updated functionalities to existing customers while enabling expansion into new markets. The SSI Agent will serve both as a standalone component and as part of a full platform, depending on the partnership model. ATOS envisions scenarios where it provides a complete credential issuance platform or, alternatively, supplies APIs for credential generation that can be embedded into backend systems like HR, licensing, or student records management.

The aim is to leverage synergies with the European Digital Identity Wallet initiative and align the product with evolving eIDAS 2.0 standards. ATOS is pursuing a proprietary model—not open source—with commercial pathways that may include one-time sales, annual licensing, or transaction-based pricing, depending on the deployment scenario. The issuer module targets organizations such as universities and governments, while the verifier module is intended for banks, event organizers, or online service providers. A bundled solution will address full SSI lifecycle needs, especially in sectors like healthcare, where a chain of private institutions may adopt the system as a common credentialing infrastructure.

ATOS also plans to channel additional internal R&D resources and pursue future Horizon Europe projects to enhance ER6c. Particular attention will be given to maintaining compliance with specifications from the European Digital Identity Wallet and the Data Spaces Business Alliance. Integration into Eviden's cybersecurity offerings and positioning within broader IAM solutions will be a core part of the long-term exploitation strategy.

Exploitation paths for ER6d- IoT Machine-to-Machine Device Authentication

Competitor analysis

ER6d operates in a competitive environment that includes major cloud providers, decentralized identity ecosystems, and IoT-focused blockchain frameworks. One key competitor is Microsoft's Azure IoT Hub combined with its Device Provisioning Service (DPS), a fully managed cloud solution offering device lifecycle management and authentication using X.509 certificates or TPM-based identities. Its deep integration with Azure analytics and edge services makes it attractive to enterprise-scale smart city operators, industrial facilities, and retail chains already within Microsoft's ecosystem. Pricing is tiered, with IoT Hub S1 costing approximately €22 per unit/month and additional messages billed at €0.40 per million.

A second competitor is the Hyperledger stack—Indy, Aries, and Ursa—which forms a modular, production-ready open-source SSI infrastructure. These tools are widely adopted in government pilots and enterprise settings requiring a decentralized credentialing system.

They generally attract organizations and integrators building their own SSI networks that require battle-tested ledger infrastructure and agent frameworks but are comfortable assembling transport and edge components themselves. Although free to use under Apache 2.0, deployment requires self-hosting or reliance on commercial ledger nodes (often free community nodes or € per-month commercial node services), and integrators must assemble components independently.

A third notable alternative is IOTA Identity, designed specifically for constrained IoT and mesh networks. It leverages the IOTA Tangle for zero-fee, lightweight deployments and includes support for DIDs and ZKPs. Its appeal lies in offline-first scenarios such as smart agriculture and energy microgrids, where minimal connectivity and low power usage are critical. Software is open-source, with hosting options ranging from free community nodes to modest commercial plans.

Compared to these, ER6d distinguishes itself by combining SSI and Zero-Knowledge Proofs (ZKPs) into a turnkey M2M authentication component embedded within the FIWARE ecosystem. This positions it as a high-assurance, privacy-preserving solution particularly suited for European compliance environments and edge scenarios where resource constraints are acute.

- **Market Analysis**
  - **ER6d IoT Device Management Market and IoT Identity and Access Management (IAM) Market**
    - **Segments**

ER6d's focus on secure, privacy-preserving machine-to-machine (M2M) authentication for IoT devices places it at the intersection of two core segments: **IoT Device Management** and **IoT Identity and Access Management (IoT IAM)**. Specifically, it addresses security and authentication within the rapidly expanding device connectivity ecosystem. The **IoT IAM segment** is crucial because managing trust between autonomous devices is becoming a core requirement across verticals like smart cities, industrial automation, and e-health, as noted in the Emergen Research report, which highlights increasing demand for decentralized identity solutions within IoT infrastructures[167]. Meanwhile, the **IoT Device Management segment** supports this need from an operational standpoint by enabling secure onboarding, monitoring, and maintenance of IoT endpoints[168].

- **Size and Growth Rate**

The **European IoT device market** is experiencing robust growth driven by adoption in sectors like energy, manufacturing, and logistics. According to Grand View Research, the **IoT Device Management market** is projected to exceed USD 20 billion globally by 2030, with the EU contributing significantly due to its advanced regulatory frameworks and industrial base[169]. The **IoT IAM market** is forecasted to grow at a **CAGR of 16.2%**, reaching USD 8.8 billion by 2030, as per "Markets and Markets", fuelled by the increasing complexity and scale of identity management challenges in IoT ecosystems[170]. This growth confirms a fertile environment for ER6d's privacy-preserving authentication innovation.

- **Trends**

A key trend relevant to ER6d is the shift toward **zero-trust security** and **decentralized identity models** for IoT. Allied Market Research reports a growing emphasis on blockchain and Self-Sovereign Identity (SSI) frameworks within IoT IAM platforms, aligning perfectly with ER6d's ZKP-based M2M authentication approach[171]. Additionally, Emergen Research highlights a trend toward **privacy-enhancing technologies** for smart city infrastructure, smart homes, and industrial IoT systems, all of

[167] Emergen Research
[168] Grand View Research – IoT Device Management
[169] Grand View Research – Europe Outlook
[170] "Markets and Markets"
[171] Allied Market Research

which demand secure machine-to-machine communications[172]. These trends establish a direct trajectory for ER6d's value proposition in future-proof identity frameworks.

- **Barriers**

Despite the growth potential, several barriers could hinder ER6d's market uptake. The IoT IAM market still suffers from **fragmentation and lack of interoperability**, which complicates integration across heterogeneous systems, according to Market Research Future[173]. In addition, the **shortage of skilled cybersecurity professionals** and the **high cost of implementing secure IAM systems** in smaller organizations limit adoption in the SME segment[174]. Moreover, device-level authentication solutions like ER6d must also contend with **hardware constraints** in embedded systems, which often lack the computational resources for cryptographic protocols like Zero-Knowledge Proofs.

- **Opportunities**

The implementation of **GDPR**, **eIDAS 2.0**, and Europe's push for a **European Digital Identity framework** create strong regulatory incentives for privacy-preserving identity management across IoT networks. Maximize Market Research underscores that manufacturers and platform providers are investing in **SSI-compliant IoT authentication frameworks** to meet evolving compliance demands and consumer expectations[175]. The Insightful Inventor Matrix report of the European IoT IAM market report notes that EU-funded initiatives are supporting innovation in identity decentralization, a perfect fit for ER6d's architecture[176]. Finally, the integration of SSI with IoT IAM, highlighted by "Markets and Markets", is an emerging niche where ER6d can position itself as a lightweight, secure M2M authentication layer in **smart manufacturing**, **eHealth**, and **critical infrastructure sectors**[177].

▸ Value proposition analysis

ER6d offers a secure and privacy-preserving machine-to-machine authentication flow for IoT systems by embedding decentralized identifiers (DIDs) and zero-knowledge proofs (ZKPs) directly within the FIWARE Device Connector. This approach allows IoT devices to establish trust and verify credentials without disclosing unnecessary data or relying on centralized authorities, while drastically reducing data exposure enabling businesses to confidently deploy and manage IoT devices. The result is a lightweight, fully automated onboarding and authentication framework that protects sensitive metadata and minimizes the attack surface. For users, particularly IoT platform operators and embedded system providers, ER6d empowers runtime device authentication while supporting regulatory compliance (e.g., GDPR and the EU Cybersecurity Act). It transforms complex device onboarding and credentialing into an efficient, verifiable, and privacy-first process—critical for secure IoT infrastructure at scale.

▸ Barriers, obstacles and analysis of the standards and regulation

Despite its promise, ER6d faces several technical and regulatory obstacles. A key challenge lies in the computational intensity of ZKP operations, which are resource-heavy and unsuitable for many edge devices that lack cryptographic accelerators or adequate power budgets. Additionally, while standards such as W3C DIDs and Verifiable Credentials are maturing, vendor-specific implementations still vary,

[172] Emergen Research
[173] Market Research Future
[174] The Business Research Company
[175] Maximize Market Research
[176] Insightful Inventor Matrix
[177] "Markets and Markets"

which impedes interoperability. Legacy protocols like MQTT and CoAP were not designed to accommodate decentralized identity flows, complicating integration into existing IoT architectures.

From a regulatory standpoint, ER6d operates in a favorable but demanding landscape. GDPR mandates data minimization—a principle well-served by ZKPs—and the EU Cybersecurity Act creates certification requirements that privacy-preserving solutions like ER6d can help satisfy. Compliance with these frameworks is both a necessity and a market differentiator, but it also demands careful design, extensive documentation, and ongoing alignment with evolving policy and technical standards.

- **Technology and market watch**

Multiple trends and developments, presented in Table 25, validate the strategic relevance of ER6d. The increasing adoption of W3C Verifiable Credentials for device identity and the emergence of the FIDO Device Onboard (FDO) standard suggest a movement toward harmonized, zero-touch provisioning and decentralized authentication. ER6d's integration with these standards and its potential to prototype hybrid SSI-ZKP + FDO workflows positions it at the cutting edge of this evolution.

Additionally, market opportunities are emerging in Vehicle-to-Everything (V2X) communications in the automotive sector, where stringent requirements for privacy, verifiability, and auditability align closely with ER6d's capabilities. The European regulatory push, particularly under the Cybersecurity Act, creates demand for exactly the type of privacy-preserving, automated authentication that ER6d delivers.

The broader trend toward data sovereignty and decentralization across IoT, smart cities, and edge computing further reinforces the growing demand for ER6d's approach to secure M2M interactions. Continued contributions to the W3C DID Working Group and documentation for FIWARE integration will extend ER6d's technological and market relevance over time.

Table 25: ER6d Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date	Link
New market opportunities	Vehicle-to-everything (V2X) in automotive, where regulators (EU Cybersecurity Act) demand privacy, auditability, and minimal credential exposure	Opens a high-value segment (billions in automotive cybersecurity), showcasing how SSI ZKP ensures secure, verifiable V2X sessions without leaking vehicle metadata.	N/A	N/A	
Emerging trend or development	Broad adoption of W3C Verifiable Credentials for device IDs and FIDO Device Onboard (FDO) standard for zero-touch provisioning.	Harmonizes identity management across platforms, enabling fully automated, privacy-preserving device onboarding.	Prototype a hybrid SSI-ZKP + FDO onboarding flow. Contribute a sample credential schema to the	N/A	https://www.w3.org/TR/vc-data-model/

			W3C DID Working Group. Document the integration for the FIWARE community.		

Exploitation Pathway

UMU intends to exploit ER6d through a mixed open-access and commercial strategy. The IoT Machine-to-Machine Authentication module will be embedded into existing FIWARE projects and demonstration platforms, with the SDK and usage examples published under an open-source license to stimulate community uptake. In parallel, UMU will offer targeted workshops and consultancy support to integrators and IoT service providers, fostering early adoption through practical engagement.

Over time, the solution will be transferred to industry via non-exclusive licensing and value-added services. ER6d will serve as a foundational building block in privacy-preserving IoT architectures, allowing industrial partners to adopt secure M2M authentication without having to build from scratch. This exploitation approach emphasizes both dissemination through education and direct uptake through business and technology transfer.

The business model for ER6d will combine SaaS, SDK licensing, and training services. Specifically:

- **SaaS**: A managed FIWARE DSC service embedding the M2M authentication component will be offered, with billing tiers based on device count or usage level.
- **SDK Licensing**: Organizations seeking on-premise or embedded solutions can license the SDK on an annual basis.
- **Training & Support**: UMU will offer modular workshops and technical assistance packages to accelerate deployment and compliance.

In the short term, ER6d will be published on GitHub alongside practical lab exercises for use in UMU's bachelor's and master's programmes. In the mid-term, UMU will develop advanced GDPR- and eIDAS-compliant training modules and run pilot projects with regional innovation hubs and external partners. In the long term, the solution will be licensed to industrial and public-sector adopters, with UMU continuing to lead standardization contributions and apply for Horizon Europe funding to sustain further development.

Exploitation paths for ER10- Hardening against Side channel Attacks

Competitor analysis

ER10 enters a competitive landscape populated by established companies that offer a wide range of side-channel attack protection services and technologies for embedded systems. One key competitor is Secure-IC, which provides an extensive product suite including the Securyzr™ iSSP chip, secure software solutions, and robustness analysis tools against side-channel and fault injection attacks. They also offer security certification services, making them an end-to-end provider targeting the same customer base as ER10—industrials requiring robust protection for embedded systems and IoT devices.

Another notable competitor is Fortify-IQ, which specializes in countermeasures against side-channel attacks, particularly for cryptographic cores such as AES and HMAC SHA2. Their offerings include

protected IP cores, security assessments, and pre-silicon testing solutions tailored for companies building secure embedded systems.

Riscure, also operating in this domain, focuses on tools for pre-silicon vulnerability assessment, including side-channel and fault injection testing. Their services extend to certification, secure development support, and training classes. Like CEA, they cater to the full spectrum of companies with embedded systems security needs.

Unlike these companies, which mainly focus on assessment tools, IP cores, and comprehensive evaluation services, ER10's strength lies in its unique combination of masking and hiding countermeasures, code polymorphism, and a targeted focus on AES protection. CEA's approach emphasizes technology transfer through licensing of patents and the provision of expert consultancy tailored to the specific needs of industrial partners, making ER10 particularly attractive for companies that want to innovate securely without developing their own in-house expertise in side-channel attack mitigation.

- **Market Analysis**
  - **ER10 — Hardening against Side-Channel Attacks in the Embedded Systems Security Market**
    - **Segments**

ER10 directly addresses the **hardware security** and **authentication & access management** segments within the European embedded security market. Specifically, side-channel attack hardening enhances the resilience of hardware security modules (HSMs), secure elements (SEs), trusted platform modules (TPMs), and embedded processors, which are widely used in smart identity cards, payment systems, automotive electronics, industrial IoT controllers, and secure mobile devices. As hardware is the dominant component segment for embedded security, representing the largest revenue share, ER10's focus aligns with the core demand for robust physical security that prevents leakage of cryptographic keys and sensitive data through physical side channels[178].

- **Size and Growth Rate**

The European embedded security market is projected to grow steadily, rising from USD 1,487.4 million in 2023 to USD 2,230.6 million by 2030 at a CAGR of 6%[179]. According to KBV Research, the market may expand even faster at an 8.4% CAGR between 2022 and 2028, with Germany remaining the largest national market, followed closely by the UK and France[180]. Given that hardware is the fastest-growing component and side-channel countermeasures are critical for secure hardware, ER10 is well-positioned in a sizeable and growing segment with high security stakes.

- **Trends**

Key market trends relevant to ER10 include the surge in **IoT device proliferation**, stricter compliance mandates for secure hardware design, and the increasing sophistication of physical and side-channel attacks. The adoption of connected automotive electronics, smart medical devices, and industrial IoT systems amplifies the risk of hardware-level exploits, driving demand for advanced cryptographic shielding and side-channel attack resistance[181]. Furthermore, new regulatory pushes in Europe, especially for automotive and payment security, are intensifying requirements for hardware that is

[178] Grand View Research, Europe Embedded Security Market; MMR, Europe Embedded Security Market
[179] Horizon Grand View Research, Europe Embedded Security Market
[180] KBV Research, Europe Embedded Security Market
[181] "Markets and Markets", Embedded Security Market

secure against both logical and physical attacks — making ER10's protective solutions highly relevant[182].

- **Barriers**

However, barriers persist that could affect ER10's potential impact. The main challenge is the **high cost and complexity** of developing, validating, and integrating side-channel resistant hardware designs. Legacy HSMs and security ICs may require redesigns or replacements to meet new physical security benchmarks, which can be cost-prohibitive for SMEs and even larger device makers[183]. Additionally, the **lack of skilled professionals** specializing in advanced hardware security engineering remains a bottleneck in Europe, slowing the deployment of next-generation secure elements that embed robust side-channel protections[184].

- **Opportunities**

Despite these barriers, ER10's market opportunity in Europe is compelling. The rise of **autonomous and connected vehicles**, the migration to **5G-enabled IoT**, and Europe's leadership in **industrial automation** present fertile ground for security solutions that guarantee data integrity and confidentiality at the hardware level. Side-channel hardening directly addresses vulnerabilities that could compromise the trustworthiness of secure elements in critical infrastructure, automotive ECUs, and industrial controllers — sectors forecasted to maintain high growth within Europe's embedded security market[185]. Moreover, the EU's continuous updates to cybersecurity certification frameworks for hardware devices, such as the upcoming EU Cyber Resilience Act, will create a regulatory push for widespread adoption of side-channel resilient secure hardware — opening a clear path for ER10 to support compliance and strengthen Europe's digital sovereignty[186].

Value proposition analysis

ER10 delivers a high-impact solution to a pressing cybersecurity challenge: protecting embedded systems and IoT devices against side-channel attacks. These attacks are among the most effective and least invasive methods for extracting sensitive cryptographic keys and data from secure devices. The novelty of ER10 lies in its optimized and combined countermeasures, specifically the integration of loop shuffling and code polymorphism, as well as the pairing of masking with code polymorphism and optimized masking for AES.

CEA's value proposition includes transferring not just technology, but expertise. They assist industrial clients in integrating advanced security measures, licensing patented countermeasures, and adapting solutions to client-specific contexts. ER10 is not just a product but a consultative service offering, allowing clients to improve the security of their products through tailored advice, hardened implementations, and differentiated offerings in their own markets.

Barriers, obstacles and analysis of the standards and regulation

Several external barriers could influence ER10's uptake. One major issue is that security-sensitive industries are often hesitant to incorporate new countermeasures due to the high cost of certification, which discourages rapid innovation. Certification for secure embedded systems, particularly those

[182] Grand View Research, Embedded Security Market Report
[183] Fortune Business Insights, Embedded Security Market
[184] Globenewswire, Embedded Security Market
[185] "Markets and Markets", Embedded Security Market
[186] Grand View Research, Europe Embedded Security Market

requiring Common Criteria compliance, can be prohibitively expensive and time-consuming, making conservative, known solutions more attractive even if they are less robust.

In terms of standards, the landscape remains fragmented. While smartcard security benefits from well-established Common Criteria certification schemes, no such universal benchmark exists for IoT devices. Nevertheless, standards like AES, SHA-3, and ongoing post-quantum cryptography (PQC) efforts by NIST provide important technical anchors. ER10 aligns with these evolving standards but still faces an adoption lag, as new countermeasures require extensive validation.

CEA also highlights that advanced countermeasures like theirs are often met with market inertia, as industrial players prefer tried-and-tested methods. Additionally, many SMEs and public sector clients lack the in-house expertise required to evaluate and adopt such advanced security techniques.

- **Technology and market watch**

ER10 is informed by active monitoring of technological innovations and security trends. Based on CEA's input, detailed in Table 26, one emerging threat is the increasing effectiveness of machine learning-based side-channel attacks. These data-driven attacks can bypass traditional countermeasures, posing a novel threat that CEA aims to test against their combined masking and hiding approaches. Conferences such as CHES and CARDIS 2023 are key venues for tracking and responding to these developments.

Masking remains a fertile area for innovation. Recent advances in code-based masking schemes, and the possibility of combining these with hiding techniques, offer promising directions that CEA is exploring. Active companies in this field include Secure-IC, Fortify-IQ, NinjaLab, and CryptoExperts, which disseminate their research and IP aggressively. CEA distinguishes itself through its advanced software-level countermeasures, an area with limited competition.

Market opportunity is also being shaped by regulatory and technological shifts. The IoT market, while not new, continues to expand into verticals such as medical devices, hospitality, and industrial controls. As these domains grow, so too will the demand for robust side-channel protection. CEA plans to increase visibility through dissemination, scientific publication, and direct industry engagement to ensure ER10 remains on the radar of decision-makers and developers alike.

Table 26: ER10 Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date	Link
Latest innovations and IP	Research on masking schemes results in new masking schemes (e.g. Code-based masking) and improvement of existing schemes.	The masking countermeasure could combine well with our hiding countermeasures	Potentially test masking countermeasure combined with our hiding countermeasures	N/A	
Emerging trend or development	Machine learning based attacks: these are getting a lot of attention, and are quite powerful	They could threaten the countermeasures	Try testing countermeasure with machine learning attacks	N/A	https://ches.iacr.org/2023/program.php https://sbd-research.nl/cardis-2023/program.html

Item	Description	Possible Impact	Actions	Effective Date	Link
Active companies and their R&D strategies	Secure-IC, Quarkslab, NinjaLab, CryptoExperts, Fortify-IQ, Tiempo-secure, Riscure, Thalès, eShard	Most of them sell IPs, libraries, and expertise. Most of them are visible thanks to their research publication and conference sponsoring.	Disseminate our results to the best we can so that community is aware of our results. Cultivate our differences: few companies support advanced software hiding countermeasures	N/A	
Hot startups and innovators	See above (active companies)			N/A	
Impact of new technology adoption	New technology adoption is quite slow in the security market, as people prefer to use countermeasures that they know well, and that the already tested on several product.	This could make our countermeasure transfer to industry longer.	Show as well as we can the impact of our countermeasures on security	N/A	
Potential impact of technological change	Having new countermeasures that are easy to apply to a software	Higher security in products	Keep looking for innovative ways to combine and design countermeasures	N/A	
New market opportunities	The IoT market, while not completely new, represents a large market, spread over many different domains	The market is large and security should become more and more a concern	Disseminate our results to the best we can so that community is aware of our results. Cultivate our differences: few companies support advanced software hiding countermeasures	N/A	https://www.grandviewresearch.com/industry-analysis/iot-market

- **Business Model Canvas**

Even though ER10 is not considered a key outcome of TANGO, CEA has provided a thorough BMC that elaboratively summarizes the organisation's plans for the result beyond the project's lifetime.

Business Model Canvas				
Key Partners	**Key Activities**	**Value Propositions**	**Customer Relationships**	**Customer Segments**

<table>
<tr>
<td rowspan="2">Our key partners are other entities specialized in security products. In particular, partnership with governmental agencies like ANSSI could help for reaching our end customers.</td>
<td>Our key activity is related to problem solving, as we find solutions to secure use-cases trying to get the best trade-off for the client's need.

Key Resources
Our main resources are human (experts) and intellectual (patents).</td>
<td rowspan="2">We help customers reaching decent security w.r.t. side-channel attacks, while keeping performance overheads low enough for their systems.

Alternatively, we help security providers to extend their portfolio with innovative efficient countermeasures.</td>
<td rowspan="2">Customers would expect support in securing their product, either for the implementation of countermeasures, either for their evaluation.

Channels
We reach our customers mostly through dissemination (e.g. scientific publications and presentations in conferences). In addition, we contact directly potentially interested customers during trade shows.</td>
<td rowspan="2">All sectors where side-channel attacks are a threat – in particular most IoT and embedded systems. Such systems are employed in various segments, such as medical devices, smart hospitality, payment, etc. As such, the customer segments are diversified.</td>
</tr>
<tr>
<td colspan="2">Cost Structure
Personnel and infrastructure are our most important costs. Our business is more value driven.</td>
<td colspan="2">Revenue Streams
Our customers would pay for either software licensing, either patent exploitation, either support and consulting to help them for their secure implementations, either for research & development to find new countermeasures for their use-case.</td>
</tr>
</table>

▸ Exploitation Pathway

CEA plans to commercialize ER10 primarily through advisory services and patent licensing. The exploitation strategy includes selling expertise to industrial clients seeking to secure embedded devices, as well as licensing patented countermeasures for integration into client products. CEA intends to engage companies that may not have extensive internal cybersecurity capacity but nonetheless require strong protection for their systems.

The business model is not based on open source. Instead, it adopts a B2B (and potentially B2G) model, targeting the industry and public sector. Customers will pay per service—ranging from advice and consultation to software licensing and patent use—tailored to each project. The licensing structure for patented countermeasures is still under consideration but will aim to remain flexible for a wide range of customers. CEA aims to reach its customers mostly through dissemination (e.g. scientific publications and presentations in conferences). In addition, the organization contacts directly potentially interested customers during trade shows.

CEA also foresees applying for national and European funding to support the transition of ER10 from a research prototype to high-TRL implementations. Participation in future Horizon Europe projects will help validate and further mature the technology, expanding its adoption and impact. The long-term plan includes expanding collaborations with key security partners, especially national agencies such as ANSSI, and ensuring integration of ER10's techniques into commercial and public-sector solutions through continued R&D, demonstration, and knowledge transfer.

Some key partners in aiding CEA fulfilling their plan for ER10 are other entities specialized in security products. In particular as CEA has declared, partnership with governmental agencies like ANSSI could help for reaching our end customers.

Exploitation paths for ER11- Exploratory Data Analysis engine (EDAE)

- **Competitor analysis**

In the hospitality sector, EDAE competes with several established and emerging analytics platforms. STR, Inc. (a CoStar Group company) is a global leader in hotel benchmarking analytics, providing performance metrics such as occupancy, ADR, and RevPAR. However, its heavy focus on historical benchmarking limits its utility for real-time decision-making. MKG Group, a prominent player in EMEA, offers market intelligence and guest satisfaction tools but lacks global reach and modern integrations. Analytic Partners delivers in-depth marketing analytics but is complex and costly due to its consulting-heavy approach. Livelytics offers agile, real-time dashboards with sustainability metrics but is a relatively new player with limited enterprise maturity and brand visibility.

However these competitors have a series of weaknesses. More specifically STR's platform is heavily focused on historical benchmarking and lacks real-time operational insights, making it less actionable for daily decision-making. MKG Group has limited global reach, primarily serving EMEA markets, and its tools are more traditional and less integrated. Analytic Partners offers deep marketing analytics but requires heavy consulting support, making it complex and costly to implement. Livelytics, while agile and real-time, is a newer player with limited brand recognition and may lack mature integrations or enterprise-grade support.

In contrary EDAE's competitive advantage stems from the fact that it offers real time analytics in an integrated manner linked with a series of sensors located at the room through the NADIA platform, fusing with visitor and satisfaction related information, while shares the high advantage offered through the TANGO of secure and trustworthy data-flows. Furthermore, in TANGO with focused also on greener operations targeting the even more niche market of hotels that want to be environmentally friendly and similarly visitors caring about environmental sustainability. It also targets sustainability-conscious hotels, aligning with a niche yet growing segment of environmentally aware consumers and eco-certified accommodation providers.

In the retail domain, competitors like Manthan, Retail Solutions Inc. (RSi), InfoPrice, and IT Retail offer AI-powered or POS-integrated analytics solutions. However, these tools often require significant IT support (Manthan, RSi), lack international scalability (InfoPrice), or provide limited analytical depth (IT Retail).

Similarly, a series of weaknesses are existent for those product offerings. Manthan and RSi offer robust, AI-driven enterprise tools but often require heavy IT support and long deployment times. InfoPrice's solution is strong in dynamic pricing but primarily focused on Latin America, limiting global expansion. IT Retail excels in usability for small chains but lacks the advanced analytics depth needed by large-scale supermarkets or multinationals.

In the framework of TANGO, EXUS has showcased a easy to follow multicounty support in data-analytics, showing a quite dynamic and modular version based on user defined roles, while the overall system was deployed locally in local servers ensuring system sovereignty compared to cloud based solutions enhancing the high level of data security. Reports were co-designed to end user needs, while the overall deployment architecture offered easy maintenance and support. In essence, EDAE has been demonstrated as a modular, multi-country solution offering user-defined roles, dynamic analytics, secure local deployment, and high sovereignty of data. The ability to co-design reports with end users and maintain the platform easily further differentiates EDAE from these offerings.

- **Market analysis**
  - **ER11 Market Analysis Data Management Platforms, Enterprise Data Management (EDM), hospitality and retail sectors**
    - **Segments**

EDAE sits at the intersection of three strategic markets: Data Management Platforms, Enterprise Data Management (EDM), and Cybersecurity, all within the context of the hospitality and retail sectors. Specifically, it serves the data preparation and quality assurance subsegments—functions that are critical for training AI/ML models and generating insights from large heterogeneous data sets. Given its modular architecture and emphasis on secure, privacy-compliant analytics pipelines, EDAE also plays a vital role in cybersecurity-conscious analytics workflows, especially for customer-facing industries like tourism and retail.

- **Size and Growth Rate**

The hospitality analytics space is expanding rapidly. According to Market Research Future, the hospitality management software market (including analytics) is projected to grow from €3.65 billion in 2023 to €5.79 billion by 2030 (CAGR 7.6%)[187]. A broader Emergen Research estimate for the smart hospitality market—which includes AI-driven analytics and digital platforms—foresees growth from €39.8 billion in 2023 to €158.0 billion by 2030 (CAGR 21.8%)[188]. Similarly, in the tourism analytics niche, Future Market Insights projects growth from €16.9 billion in 2025 to €38.6 billion by 2035 (CAGR 8.6%)[189].

Retail analytics shows similar promise. Market Research Future expects the market to hit €6.44 billion by 2030 (CAGR ~17%)[190], while Emergen Research forecasts a jump from €4.19 billion in 2020 to €19.16 billion by 2028 (CAGR 21.2%)[191]. IMARC projects even greater expansion—from €9.57 billion in 2024 to €41.58 billion by 2033 (CAGR 16.9%)[192].

- **Trends**

Key market trends supporting EDAE's growth include the rise of data-driven sustainability reporting in hospitality and the push for real-time, AI-supported analytics in retail. The European Commission's Transition Pathway for Tourism emphasizes sustainability metrics (energy, water, waste), offering a clear path for EDAE integration into ESG-compliant hotel operations[193]. In retail, EU policies push for

[187] source
[188] source
[189] source
[190] source
[191] source
[192] source
[193] source

customer-centric, real-time data usage in inventory and pricing strategies[194], aligning perfectly with EDAE's multivariate analysis and trend-forecasting capabilities.

- **Barriers**

Several barriers may hinder adoption. These include fragmented data ecosystems in both sectors, low data literacy among end-users, and integration challenges with legacy systems. Additionally, resistance to automation in traditional organizations and persistent trust issues regarding data processing pose non-technical challenges. The need to comply with GDPR, the EU AI Act, and the Digital Services Act also imposes regulatory constraints on analytics tools.

- **Opportunities**

EDAE can take advantage of growing demand for modular, secure analytics platforms that support ESG, privacy, and scalability. Hotels and retailers alike require tools that not only generate insights but also support sovereign deployment models. With sustainability targets and AI trust becoming mainstream concerns, the market is primed for analytics engines that integrate compliance, usability, and advanced statistical capabilities.

Value proposition analysis

EDAE offers a structured, modular toolset for high-quality, scalable, and secure exploratory data analysis tailored to the hospitality and retail sectors. It comprises three sub-modules: (1) a data analytics module for univariate, bivariate, and multivariate analysis; (2) a data cleaning module that handles missing/duplicate data with user-guided control; and (3) a data preparation module optimized for AI/ML model training. These have all been tightly integrated within TANGO, enabling interoperability with upstream and downstream components. The system empowers organizations to convert raw, fragmented data into actionable insights—dramatically reducing time to analysis while enhancing data quality. It is particularly beneficial for data-rich but insight-poor businesses in hospitality and retail that need to elevate decision-making capabilities while maintaining high security and compliance standards.

Barriers, obstacles and analysis of the standards and regulation

The main barriers include highly fragmented data environments, lack of data literacy, and integration difficulties with existing legacy systems. Additional obstacles involve resistance to automation, particularly in SMEs, and trust issues concerning data governance. From a regulatory standpoint, EDAE must comply with GDPR, the Digital Services Act, and the upcoming EU AI Act. Standards that apply include ISO/IEC 27001 (information security), ISO/IEC 25012 (data quality), and ETSI/CEN guidance for trust, QoS, and data interoperability in digital platforms. Furthermore, EDAE aligns with the goals of CEN/CLC JTC 25 for European data governance frameworks under the EU Data Strategy.

Technology and market watch

Several developments directly enhance EDAE's positioning, as shown in Table 27. In the hospitality domain, the growing relevance of green metrics and sustainable tourism practices calls for tools that monitor energy, waste, and resource consumption. EDAE is well-placed to integrate these KPIs into its models and partner with eco-certified hotels on pilot initiatives[195]. In retail, the demand for advanced data-driven decision-making continues to rise. By incorporating features like customer segmentation, trend forecasting, and market basket analysis, EDAE can become indispensable for real-time retail optimization source.

[194] source
[195] source

Table 27: ER11 Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date	Link
Emerging trend or development	Sustainable Tourism that involves both Greener Hotels and visitor that promote environmental sustainability	Positive – Growing demand for data analytics tools that support sustainability reporting, resource optimization, and regulatory compliance in smart hospitality	Integrate sustainability metrics (e.g., energy, water, waste KPIs) into EDAE's data models. Align modules with ESG reporting standards. Target eco-certified hotels and green tourism initiatives for pilot collaborations.	2026-2030	https://ec.europa.eu/growth/news/transition-pathway-tourism-now-available-2022-02-04_en
Emerging trend or development	Data driven decision making for retail stores, product and consumers	**Positive** – Increased market demand for advanced analytics tools that support real-time decisions in retail inventory, pricing, and consumer behaviour optimization	Continue enhancing EDAE's bivariate/multivariate analysis and integrate support for market basket analysis, customer segmentation, and trend forecasting. Collaborate with retail innovation clusters or digital hubs.	2027-2032	https://single-market-economy.ec.europa.eu/sectors/retail_en

Exploitation Pathway

EXUS intends to commercialize EDAE by integrating it into its managed data analytics service portfolio under the EXUS Financial Suite. This will be done via B2B licensing contracts (SaaS model), with the technology retained as a trade secret. Customers in the retail and smart hospitality sectors will subscribe through annual licensing fees, allowing flexible scalability and continuous updates. The platform is modular, making it suitable for tiered pricing based on features or volume. A freemium or pilot/demo phase may be considered to support adoption. EDAE will also be embedded in broader data solutions sold via EXUS's existing global sales and channel network, and can be leveraged for training, and data governance auditing within existing data flows as sub-modules as additional revenue streams. The exploitation pathway also includes internal transfers to other EXUS verticals, joint ventures, and strategic partnerships for broader market deployment. EXUS envisions using royalty-based commercial agreements with local integrators across the EU, particularly in Greece, where the €16B hospitality sector presents a high-impact pilot market.

To reach TRL 9, EXUS will pursue a blended financing model combining internal funds and EU grants. Additionally, EDAE will serve as a foundation for future Horizon Europe proposals (particularly IA calls) in various domains. Over time, EXUS plans to evolve EDAE into an agentic-based AI engine that offers autonomous decision-making support, extending its relevance far beyond exploratory data analysis. This strategy aligns with EXUS's core model of recurring annual licenses supplemented by training, auditing, and modular integration services—ensuring broad applicability, sectoral scalability, and continuous innovation.

Exploitation paths for ER12a- Energy efficient AI model training, support for MLOps

Competitor analysis

ER12a enters a highly competitive landscape dominated by global cloud and AI service providers, yet differentiates itself through its focus on energy efficiency and internal modular design supporting MLOps life-cycle automation. The most prominent competitor is **Databricks**, which offers a full-stack AI suite, including MLOps capabilities, based on its open-source MLFlow platform. Databricks is widely adopted due to its seamless integration with data engineering workflows and scalable cloud-native architecture. Its pricing model is pay-as-you-go, generally based on data usage units, targeting companies looking to productize AI applications with flexible deployments. ER12a, while also building upon open-source MLFlow, offers a more energy-aware approach and internal deployment use, targeting specific enterprise demands such as federated learning and internal optimization practices.

Amazon Web Services (AWS) is another major player, providing a robust MLOps and AutoML solution through Sagemaker and AutoPilot. Its service tiers range from a free starter package to expensive pay-as-you-use deployments, making it accessible to a wide spectrum of AI users. AWS's strength lies in its end-to-end ecosystem integration, yet its generalized cloud-dependence may pose challenges for organizations concerned with sovereignty or green compute optimization, areas where ER12a excels with its focus on energy-efficient training and internal toolset usage.

Microsoft Azure also offers a comprehensive suite for MLOps and AutoML within Azure ML, featuring versatile pricing models from reserved instances to modular service plans. However, while Azure excels in scalability and enterprise-grade support, ER12a targets a more specific use-case: supporting internal ML teams in reducing model development complexity and enhancing the speed and energy-efficiency of the pipeline through reusable components and holistic life-cycle tooling.

In sum, while ER12a shares foundational elements with these larger solutions, its unique advantage lies in its focused support for internal product development within ATOS's BDS department, its integration with federated learning workflows, and its explicit emphasis on energy-aware training and deployment.

Market Analysis

- **ER12a: Energy Efficient AI – Support for MLOps, European MLOps market**
  - **Segments**

ER12a targets two key MLOps market segments in Europe: **platforms** and **services**. According to Grand View Research, the **platform segment** accounted for the largest revenue share in 2023, driven by enterprise adoption of MLOps to manage complex machine learning pipelines[196]. ER12a supports lifecycle management by tracking experiments, managing versions, and deploying models—key capabilities aligned with this dominant segment. Furthermore, the **services segment**—which includes consulting, deployment, and system integration—is the fastest growing, expected to expand at a significant CAGR through 2030. ER12a can be packaged as a service to help organizations implement energy-efficient MLOps practices, further embedding it into the value-added service stack, particularly as companies seek to optimize compute usage and reduce AI-related energy costs[197].

- **Size and Growth Rate**

[196] https://www.grandviewresearch.com/horizon/outlook/mlops-market/europe
[197] https://www.grandviewresearch.com/press-release/global-mlops-market

The European MLOps market is currently in a rapid growth phase, providing strong tailwinds for ER12a. According to Grand View Research, the European market was valued at **USD 587.7 million in 2024** and is projected to grow to **USD 4.22 billion by 2030**, representing a **compound annual growth rate (CAGR) of 39.3%** during the forecast period[198]. This high CAGR is attributed to rising adoption of AI across sectors such as manufacturing, finance, and telecom, where operationalizing ML models at scale is essential. Globally, the MLOps market is also expanding, with Exactitude Consultancy projecting it to reach **USD 20 billion by 2034**, growing at a **16.5% CAGR**—underscoring Europe's even stronger pace of expansion in relative terms[199].

- **Trends**

Several structural trends in the EU MLOps market align directly with ER12a's value proposition. The growing **demand for hybrid cloud and on-prem MLOps solutions** is a key trend, particularly in sectors that require compliance with EU data governance rules, such as healthcare and finance. As Maximize Market Research notes, hybrid and multi-cloud deployment models are being prioritized to meet both scalability and sovereignty requirements[200]. ER12a's toolset, which supports deployment-agnostic versioning and monitoring, can capitalize on this infrastructure flexibility. Another important trend is the **increasing prioritization of energy efficiency and environmental sustainability**. The EU's Green Deal and broader "green AI" agenda are encouraging the development of models and tools that reduce computational waste. ER12a's emphasis on streamlining model training and automating workflows directly responds to this demand, offering both environmental and cost savings[201].

- **Barriers**

Despite the strong growth trajectory, several specific barriers may hinder ER12a's market penetration. A key challenge is the **shortage of skilled MLOps professionals** in Europe. As outlined by Market Research Future, many companies face difficulties in recruiting or retaining personnel capable of building and maintaining complex MLOps pipelines, which slows adoption and complicates deployment[202]. This skills gap is particularly acute in smaller organizations that may not have dedicated DevOps or data science teams, making tools like ER12a more reliant on effective onboarding and low-friction integration. Another structural barrier is the **fragmentation of toolchains and interoperability limitations**. As KBV Research notes, many organizations use a mix of proprietary and open-source tools, making the integration of new components such as ER12a's monitoring and versioning features technically demanding[203]. This necessitates an emphasis on standards-compliant APIs and modularity to ensure smooth adoption.

- **Opportunities**

Europe offers strong, concrete market opportunities for ER12a, particularly through **service integration** and **sector-specific applications**. France, for example, is forecasted to be the fastest-growing country in the European MLOps market, with a projected CAGR of **40.8%**, and is expected to reach **USD 763.8 million by 2030**, according to Grand View Research[204]. This makes it an ideal early market for ER12a,

198 https://www.grandviewresearch.com/horizon/outlook/mlops-market/europe
199 https://www.globenewswire.com/news-release/2025/06/13/3099080/0/en/Machine-Learning-Operations-MLOps-Market-is-expected-to-reach-USD-20-billion-by-2034-growing-at-a-CAGR-of-16-5-Exactitude-Consultancy.html
200 https://www.maximizemarketresearch.com/market-report/mlops-market/186990/
201 https://www.linkedin.com/pulse/europe-mlops-market-size-new-entrants-pricing-trends-ceuze/
202 https://www.marketresearchfuture.com/reports/mlops-market-18849
203 https://www.kbvresearch.com/machine-learning-model-operationalization-management-market/
204 https://www.grandviewresearch.com/horizon/outlook/mlops-market/europe

especially in industries like finance and healthcare where explainability and efficiency are required. Additionally, Fortune Business Insights identifies **automated model management** and **lifecycle tracking** as core features driving investment in MLOps platforms[205]. ER12a is already validated in pilot cases, which strengthens its value proposition in procurement-heavy sectors such as public administration or regulated industries. The push for **green AI compliance** also opens up collaborations with EU-funded digital infrastructure initiatives, giving ER12a a pathway into sustainability-focused procurement frameworks[206].

- **Value proposition analysis**

ER12a offers a suite of assets and best practices designed to streamline and enhance various stages of the ML model training lifecycle, covering AutoML, MLOps, and Federated Learning. The primary value lies in supporting internal ATOS teams across their AI lifecycle operations, particularly those involved in developing or maintaining AI-enabled products. By automating repetitive tasks such as experiment tracking, version control, model serving, and workflow orchestration, ER12a significantly reduces delivery times, increases model traceability, supports experimentation at scale, enables companies to track experimentation, improve delivery time and make ML science more productivity. This contributes to faster, higher-quality deployment of AI in commercial products and services.

Already partially validated through two pilot use cases, ER12a demonstrates practical utility and technology readiness. Its design adapts DevOps principles to AI/ML development, offering enhanced automation and collaboration capabilities. Moreover, by reusing open-source components—particularly MLFlow—and augmenting them with custom tooling for federated learning and energy-aware training, ER12a offers a low-friction, adaptable MLOps support framework that internal teams can use to align AI development with performance, cost, and sustainability goals.

- **Barriers, obstacles and analysis of the standards and regulation**

A number of barriers could hinder the full deployment of ER12a. The AI domain is characterized by rapid technological shifts, including the widespread emergence of GenAI and new ML architectures that demand continuous adaptation of MLOps tools. ER12a must remain agile to address these evolutions. Additionally, retraining and fine-tuning large-scale AI models can require significant computational resources, which may limit applicability in lower-capacity environments and raise deployment costs. While ER12a focuses on energy efficiency, high up-front investment in infrastructure remains a challenge.

Interoperability and standardization are also key obstacles. Many enterprises rely on mixed AI toolchains, often involving proprietary and open-source platforms, complicating the smooth integration of new modules. ER12a must thus ensure compliance with ongoing ISO and EU standardization initiatives, such as the upcoming AI Act and Data Act. These regulatory instruments, although still evolving, will influence model transparency, lifecycle tracking, data management, and environmental impact assessment—all directly relevant to ER12a's functionalities.

- **Technology and market watch**

MLOps continues to be a maturing market, with substantial space for innovation. As stated by ATOS and depicted in Table 28, ER12a responds to the increasing need for modular, scalable MLOps components by integrating energy-efficient practices and support for federated learning. ATOS sees new opportunities in this growing domain and maintains active internal engagement with its CTO and

[205] https://www.fortunebusinessinsights.com/mlops-market-108986
[206] https://www.grandviewresearch.com/press-release/global-mlops-market

commercial units to align the toolset with evolving business needs. These discussions also support internal product enhancements, including integration into client-facing solutions and potential adaptation to address generative AI workflows.

ATOS notes that many market actors (e.g., AWS, Microsoft, Google) offer comprehensive MLOps stacks, but the domain is still in flux, with continuous iteration in practices, tools, and market expectations. As such, ER12a remains under close internal watch and may evolve further through follow-up activities beyond TANGO. Future exploitation paths are shaped by ATOS's ongoing assessment of market demands, particularly as enterprises seek to operationalize AI at scale while minimizing infrastructure overhead and ensuring compliance with emerging European digital regulations.

Table 28: ER12a Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date	Link
New market opportunities	MLOps is a relatively new field. Therea are several solutions in the market, but still plenty of opportunities	New business models	Continue market watch	Project duration	N/A
Active companies and their R&D strategies	Potential internal exploitation in our department for ML products.	Value added to existing products	Meetings with CTO and commercial workforce in our organisation	Project duration	N/A

- **Exploitation Pathway**

The exploitation pathway for ER12a is oriented around internal integration, knowledge transfer, and potential evolution into future commercial offerings. ATOS plans to use ER12a to support existing AI-enabled products within its Big Data and Security (BDS) department. This will be done by embedding the developed MLOps tools and practices into current production environments, enhancing the efficiency and reliability of AI life-cycle management for existing clients. Teams interacting with customers will utilize the ER12a toolset to offer best practices, boost AI development productivity, and ensure consistent model tracking and versioning.

Currently, ER12a's exploitation is internal, but ATOS acknowledges that the result could evolve into a commercial product. The chosen model is open source, consistent with its MLFlow foundation. This approach ensures broad usability and encourages adoption, while still enabling ATOS to offer added-value consulting and integration services around the toolset. Looking ahead, ER12a will also be indirectly linked to new funding initiatives. ATOS foresees submitting proposals for additional public financing to refine the tool, enhance its capabilities in federated learning and GenAI contexts, and support its evolution toward higher TRL (Technology Readiness Level) for broader commercialization.

In summary, ER12a is an enabling component that strengthens ATOS's AI product development capacity while positioning the company for future service offerings and regulatory-compliant deployments across AI-intensive domains.

Exploitation paths for ER12b- Energy efficient AI model training, Support for Federated Learning (FLEVIDEN)

Competitor analysis

In the space of federated learning (FL), ER12b competes with several prominent solutions. NVIDIA Flare is currently regarded as one of the most advanced open-source federated learning tools. Released under the Apache 2.0 license, it is supported by a robust development community and integrates effectively with a wide range of AI infrastructures. Its target customers include organizations that need to train machine learning models without sharing raw data, including users of Microsoft Azure and specialized health-tech platforms like Rhino Health.

IBM Federated Learning is another major player in the market. While IBM provides a free version for non-commercial usage, its enterprise-grade capabilities are integrated into IBM's CloudPak for Data and sold as a commercial service. This positioning allows IBM to reach enterprise customers looking for integrated data and AI lifecycle management.

A third competitor, Flower, has gained traction for its flexible and unified framework supporting federated learning, analytics, and evaluation. It offers broad programming language and ML framework compatibility and is already adopted by high-profile clients such as Orange, Samsung, and the NHS. While its orchestration and configuration capabilities are still maturing, Flower's strong community and simulation functionality make it a notable competitor. Flower is released under an Apache 2.0 license.

In comparison, ER12b (FLEVIDEN) brings a unique value proposition by focusing on internal product enhancement at ATOS/EVIDEN, offering privacy-preserving, energy-efficient ML model training without data disclosure. The solution emphasizes modular extensibility and alignment with EU regulations and future customer-specific deployment needs, including internal services and long-term support. While competing open-source tools may lead in adoption, ER12b is differentiated through integration within ATOS's trusted BDS portfolio and niche application targeting sectors such as manufacturing and health where data cannot be shared.

Market Analysis

- **ER12b – Energy Efficient AI: Federated Learning (FLEVIDEN), Federated Learning market**
  - **Segments**

ER12b—Energy Efficient AI via federated learning—primarily corresponds to the **Industrial Internet of Things (IIoT)** and **Drug Discovery** segments. In Europe, IIoT was the largest federated learning application in revenues for 2024, explicitly noted in the Grand View Research[207] EU report. Drug Discovery is concurrently identified as the fastest-growing subsegment in the same source,[208] indicating relevance to health-oriented, energy-efficient federated approaches such as FLEVIDEN. These two segments align closely with FLEVIDEN's focus on decentralized, low-energy AI—IIoT for on-device intelligence across industrial sensors and drug discovery for privacy-aware medical collaboration.

  - **Size and Growth Rate**

The European federated learning market reached **USD 29.4 million in 2024** and is forecasted to increase to **USD 65.4 million by 2030**, representing a **15.1% CAGR** between 2025–2030, according to the

[207] https://www.grandviewresearch.com/horizon/outlook/federated-learning-market/europe
[208] https://www.grandviewresearch.com/horizon/outlook/federated-learning-market/europe

Grand View Europe report[209]. Comparatively, global figures, depicted in Figure 36, show consistent growth trajectories—from **USD 138.6 million (2024) to USD 297.5 million (2030)** at a **14.4% CAGR** , and forecasts from Emergen Research[210] and IMARC[211] confirm broader momentum through 2033–2034. The European figure of USD 65.4 million by 2030 thus sits in proportion with a robust, continent-scale subsegment of a globally expanding market.

Figure 36: ER12b Federated Learning market size (source: Grand View Research)

- **Trends**

A key trend fuelling FLEVIDEN is the **stringent data privacy and GDPR-driven regulations** in Europe, actively aligning with federated learning's decentralized, non-central data model. The rise of **edge computing and hybrid-cloud architectures**, noted in Grand View's global report[212], further bolsters IIoT and energy-efficient federated models for on-device training. Furthermore, the international emphasis on **energy efficiency in AI**, especially for distributed training, underlies FLEVIDEN's rationale, as detailed by IMARC[213]. Additionally, a marked upswing in federated learning for **drug discovery and healthcare applications**—driven by privacy safeguards—is highlighted across Grand View Europe[214], Precedence[215], and Emergen[216].

[209] https://www.grandviewresearch.com/horizon/outlook/federated-learning-market/europe
[210] https://www.emergenresearch.com/industry-report/federated-learning-market?srsltid=AfmBOooZ7nYE4jbR9czlEKlAcN96dNQv7sDs-N7-jkGb87I6ZNW0R89U
[211] https://www.imarcgroup.com/federated-learning-market
[212] https://www.grandviewresearch.com/industry-analysis/federated-learning-market-report
[213] https://www.imarcgroup.com/federated-learning-market
[214] https://www.grandviewresearch.com/horizon/outlook/federated-learning-market/europe
[215] https://www.precedenceresearch.com/federated-learning-in-healthcare-market
[216] https://www.emergenresearch.com/industry-report/federated-learning-market?srsltid=AfmBOooZ7nYE4jbR9czlEKlAcN96dNQv7sDs-N7-jkGb87I6ZNW0R89U

- **Barriers**

One significant barrier is the **lack of specialized federated-learning talent**, which Emergen Research[217] flags as a global impediment due to complex workflows and scarce expertise. Meanwhile, the **high computational burden** associated with federated aggregation across distributed nodes—particularly in IIoT or drug-discovery contexts—is underscored by Markets & Markets[218]. Challenges around **non-IID data handling**—where devices or institutions have skewed, heterogeneous datasets—are repeatedly noted as algorithmic hurdles by the same report. Within the EU-style framework, **cross-border GDPR interpretations and data sovereignty standards** create added complexity for federated schemes, emphasized by IMARC[219].

- **Opportunities**

In healthcare and pharmaceuticals, Europe holds concrete potential for **collaborative, energy-efficient drug discovery** platforms such as HealthChain, empowered by privacy-compliant federated systems that respect GDPR, as noted by Precedence[220] and Grand View Europe[221]. In the **industrial IoT** sphere, Germany and France—as highest CAGR countries in Europe—offer strong use cases for FLEVIDEN's localized, low-power edge processing[222]. The proliferation of **edge/cloud-integrated AI ecosystems** across EU manufacturing aligns directly with FLEVIDEN's low-overhead, hybrid-deployment model—supported by Markets & Markets[223] and IMARC insights[224]. Finally, the EU's green objectives and **sustainability mandates** amplify demand for energy-conscious AI systems, creating a direct niche for FLEVIDEN's federated, low-power architecture[225].

▸ Value proposition analysis

ER12b delivers a federated learning solution that addresses the growing need for secure and privacy-preserving machine learning training. In scenarios where data cannot be shared—due to regulatory, privacy, or organizational constraints—ER12b enables collaborative model development by exchanging only model parameters rather than raw data. This approach improves the accuracy and robustness of ML models while maintaining compliance with stringent data protection rules. The solution offers security assurances and extensibility for evolving customer demands. It directly benefits ATOS's internal development teams by streamlining operations and also supports broader customer-facing applications in sectors like health, banking, and manufacturing. The offering is tailored to support productized deployments and internal AI initiatives, and it is aligned with emerging sustainability and green AI agendas.

▸ Barriers, obstacles and analysis of the standards and regulation

Although the federated learning field offers significant promise, ER12b must navigate several market and regulatory challenges. A key barrier is the competitive advantage held by mature tools already established in the field, such as NVIDIA Flare, Flower, and IBM FL. These tools enjoy higher market

[217] https://www.emergenresearch.com/industry-report/federated-learning-market?srsltid=AfmBOooZ7nYE4jbR9czlEKlAcN96dNQv7sDs-N7-jkGb87I6ZNW0R89U
[218] https://www.marketsandmarkets.com/Market-Reports/federated-learning-solutions-market-151896843.html
[219] https://www.imarcgroup.com/federated-learning-market
[220] https://www.precedenceresearch.com/federated-learning-in-healthcare-market
[221] https://www.grandviewresearch.com/horizon/outlook/federated-learning-market/europe
[222] https://www.grandviewresearch.com/horizon/outlook/federated-learning-market/europe
[223] https://www.marketsandmarkets.com/Market-Reports/federated-learning-solutions-market-151896843.html
[224] https://www.imarcgroup.com/federated-learning-market
[225] https://www.imarcgroup.com/federated-learning-market

visibility, broader ecosystem support, and early adoption traction. Additionally, ER12b's own solution maturity remains a limiting factor for immediate deployment, requiring further development and internal testing to reach production-grade readiness.

From a regulatory and compliance perspective, ER12b must navigate complex landscapes governed by the EU's AI Act and Data Act. These emerging legal frameworks aim to standardize and regulate AI usage, particularly where sensitive data or cross-border collaboration is involved. On the standards front, while numerous ISO and EU-level initiatives exist—many remain under development. This introduces uncertainty and demands that ER12b maintain strong modularity and flexibility to ensure compliance with evolving norms.

Technology and market watch

ATOS remains closely engaged with ongoing developments in the federated learning field, recognizing its relatively nascent status and the rapid evolution of competing offerings. Their input on this matter is presented in Table 29. Continuous monitoring of technological trends is a strategic action item for ATOS, with a particular focus on identifying new business models and assessing the commercial maturity of peer solutions. Internally, ER12b is expected to be integrated within existing ATOS products, with regular reviews conducted alongside the company's CTO and commercial departments to assess value-added opportunities.

Additionally, the company is evaluating the potential of launching a standalone federated learning product or incorporating the module into future service offerings. As a new technology domain, federated learning also offers transformative potential for ATOS's product portfolio, especially when tied to energy-efficient deployment models. The intersection of privacy, efficiency, and sustainability will remain a focal point for continued innovation and external funding engagement.

Table 29: ER12b Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date	Link
New market opportunities	Federated Learning is a relatively new field. Therea are several solutions in the market, but still plenty of opportunities	New business models	Continue market watch	Project duration	N/A
Active companies and their R&D strategies	Potential internal exploitation in our department for ML products.	Value added to existing products	Meetings with CTO and commercial workforce in our organisation	Project duration	N/A
Impact of new technology adoption	New product. Potential addition to our product portfolio	New product	Meetings with CTO and commercial workforce in our organisation	Project duration	N/A

Exploitation Pathway

The primary exploitation pathway for ER12b is internal adoption and integration within ATOS's AI and ML product ecosystems. As a proprietary tool, it is being developed as an asset to enhance existing services and support use cases where data cannot be shared. The immediate focus is on deploying the solution internally to ATOS's Big Data and Security (BDS) teams, thereby improving operational efficiency and strengthening the company's in-house AI capabilities.

The foreseen business model for ER12b is proprietary, although the exact pricing structure remains to be finalized. One option under consideration is offering the federated learning module at zero cost to existing clients as a value-added component within existing service contracts. Alternatively, it may be marketed as a standalone product with fixed pricing or as part of a subscription-based service tier. Regardless of pricing, ER12b will be positioned to support ATOS's broader goal of reducing vendor dependency, enriching its AI portfolio, and delivering energy-efficient ML solutions in compliance with EU data governance mandates.

Externally, the federated learning tool may eventually be offered to clients as an added-value service or as a fixed-price standalone product. Its application across manufacturing (where each machine can perform local training), banking (where privacy and regulatory barriers limit data sharing), and health (where GDPR compliance is critical) reflects its strategic importance. ATOS is also planning to apply for further Horizon Europe funding to expand the tool's features and validate it across additional sectors. Long-term, the exploitation strategy is geared toward finding niche market entry points, minimizing vendor-lock-in, and enhancing the AI lifecycle management stack for ATOS clients.

Exploitation paths for ER12c- Energy efficient AI model training, Support for AutoML

- **Competitor analysis**

ER12c operates within the competitive landscape of Automated Machine Learning (AutoML) platforms. Major competitors include DataBricks, Microsoft Azure, and Amazon Web Services (AWS), all offering end-to-end AutoML capabilities integrated with their broader cloud ecosystems. DataBricks, for instance, provides a comprehensive AI suite incorporating AutoML and MLOps via MLFlow, targeting data scientists and enterprise users needing to deploy and operationalize ML applications at scale. Their pay-as-you-go pricing based on data usage positions them flexibly for various enterprise sizes.

Microsoft Azure's AutoML tools are bundled within the Azure Machine Learning suite, supporting a wide range of ML pipelines with features for hyperparameter tuning and model selection. Azure's flexible pricing (plans, reservations, pay-as-you-go) makes it accessible for diverse enterprise users. Similarly, AWS's AutoPilot (AutoML) and Sagemaker (MLOps) serve customers looking for automated ML model development and deployment. AWS offers pricing tiers from free trials to enterprise-level packages depending on service consumption.

In contrast, ER12c is designed as a lightweight, energy-efficient AutoML tool developed for internal use within ATOS. It is partially validated through two pilot use cases and focuses specifically on reducing ML development time by automating tedious processes such as hyperparameter optimization and model evaluation. ER12c leverages open-source tools, offering faster initial prototyping and support for internal data science teams. Its limited commercialization makes it a niche internal asset rather than a commercial competitor to cloud-native behemoths like AWS or Azure. However, it can offer comparative energy efficiency, modularity, and integration simplicity in specific internal or future productized contexts.

- **Market Analysis**
  - **ER12c – Energy Efficient AI: Support for AutoML Automated Machine Learning (AutoML) market**
    - **Segments**

ER12c directly serves the **platform/software segment** of the Automated Machine Learning (AutoML) market. According to "Markets and Markets", the software/platform segment accounted for the largest share of the AutoML market in 2023, driven by growing demand from data scientists and machine learning engineers seeking to reduce time-to-model and automate repetitive development steps[226]. In particular, ER12c's support for model evaluation, selection, and comparison places it within the **model development and optimization** sub-segment, which is becoming essential in enterprise AI pipelines. Zion Market Research confirms that this type of tool is crucial for companies deploying AI at scale while minimizing infrastructure and talent costs[227].

- **Size and Growth Rate**

As depicted in Figure 37, the AutoML market is experiencing explosive growth globally and in Europe. According to Grand View Research, the global AutoML market was valued at USD 1.2 billion in 2022 and is projected to grow at a CAGR of 43.7% through 2030, reaching approximately USD 14.5 billion[228]. European growth mirrors this trend, with Research and Markets estimating the European autonomous learning market to reach over USD 3.5 billion by 2030, growing at a CAGR of 35.8%[229]. The Business Research Company further projects the global AutoML market will exceed USD 6.4 billion by 2028, driven by increased adoption across finance, healthcare, and retail sectors[230].

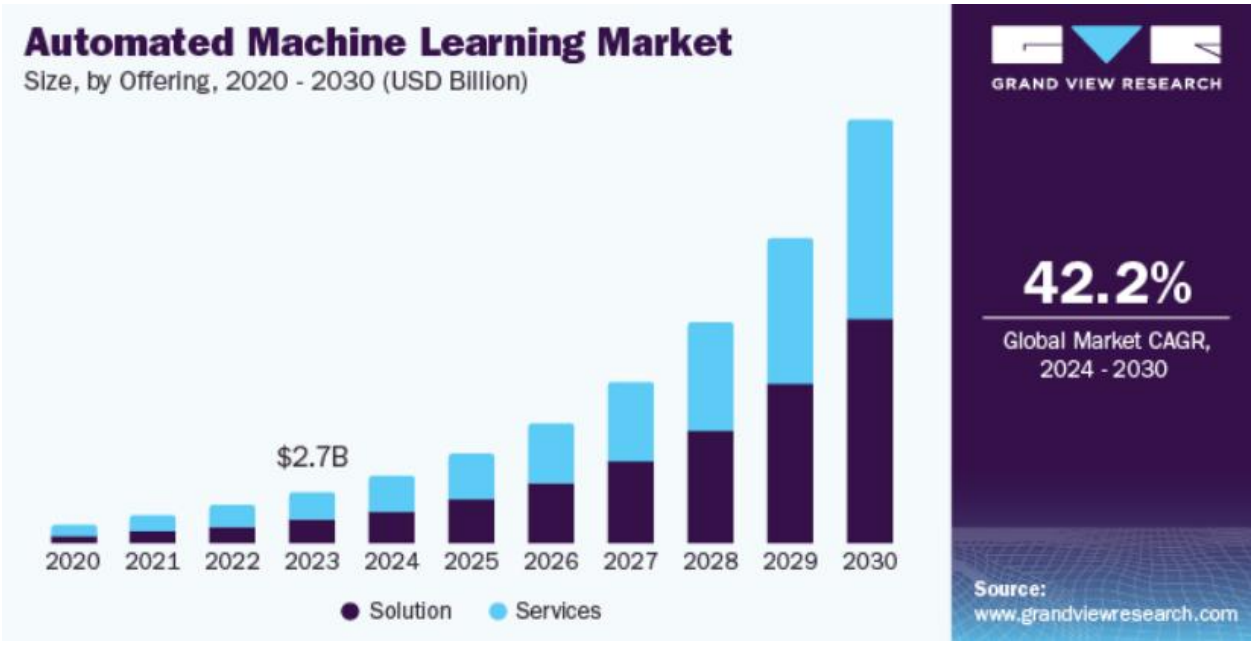


Figure 37: ER12c AutoML market size and growth rate (source: Grand View Research)

- **Trends**

One of the key trends shaping the AutoML landscape is the **integration of AutoML into cloud-native MLOps pipelines**, which aligns directly with ER12c's goal of accelerating model development and reducing iteration cycles. According to GMI Insights, the push for operationalizing AI is driving

[226] "Markets and Markets"
[227] Zion Market Research
[228] Grand View Research
[229] Research and Markets
[230] The Business Research Company

adoption of tools that automate hyperparameter tuning, model selection, and training—exactly the capabilities ER12c supports[231]. Additionally, **green AI practices**—which emphasize energy-efficient training—are gaining traction in Europe, particularly in Germany and the Nordics. ER12c's energy-aware design places it squarely within this emerging niche. BusinessWire also highlights the rise of AutoML for non-technical users and domain experts, allowing companies to democratize machine learning workflows and scale innovation internally[232].

- **Barriers**

Despite rapid growth, several challenges could impact ER12c's adoption. A major barrier is the **lack of explainability in AutoML-generated models**, which poses compliance risks in regulated industries. The Business Research Company notes that explainability remains a top concern among European adopters, particularly in banking and healthcare sectors[233]. Furthermore, **integration complexity** with existing data infrastructure and MLOps tools can hinder deployment in enterprises, particularly SMEs with limited in-house AI expertise. According to "Markets and Markets", interoperability limitations between AutoML solutions and enterprise-grade systems remain a major constraint for adoption in the EU[234]. Finally, **data privacy regulations** like GDPR add friction when handling cross-border data for federated AutoML setups, requiring region-specific model training protocols.

- **Opportunities**

ER12c is well-positioned to benefit from multiple high-growth opportunities in Europe. According to Zion Market Research, the finance, retail, and healthcare sectors are driving demand for rapid prototyping tools that minimize manual tuning and reduce the carbon footprint of AI development—aligning directly with ER12c's AutoML approach[235]. Moreover, the expansion of **AI-as-a-Service offerings** by AWS, Google Cloud, and Azure in Europe creates a favorable deployment environment for lightweight AutoML components like ER12c, especially in multi-cloud settings. GMI Insights reports that scalable, cloud-native AutoML tools are gaining favor in European enterprises looking to operationalize AI with minimal DevOps overhead[236]. With rising labor costs and AI talent shortages across the EU, ER12c's automation potential makes it an attractive proposition for organizations needing to streamline and scale AI workflows efficiently.

▸ Value proposition analysis

ER12c delivers a tangible value proposition by reducing development time and energy consumption in the early stages of ML model creation. It supports ATOS data scientists by automating labor-intensive tasks such as hyperparameter optimization and network architecture search. This accelerates the development cycle and minimizes computational iterations, contributing to greener AI practices. The component enables efficient model evaluation, comparison, and selection, providing foundational support for predictive model training.

By integrating open-source tools and tailoring them to internal workflows, ER12c addresses both productivity and sustainability. Its impact is already partially validated through two pilot cases, indicating its operational readiness. ER12c is not designed for immediate commercialization but rather

[231] GMI Insights
[232] BusinessWire
[233] The Business Research Company
[234] "Markets and Markets"
[235] Zion Market Research
[236] GMI Insights

as an internal capability enhancement—offering immediate utility to ATOS's data science teams and potentially forming the foundation for future external services or products.

- **Barriers, obstacles and analysis of the standards and regulation**

ER12c faces several challenges that may limit its broader deployment. First, the competitive landscape includes highly mature commercial AutoML tools, many of which have established user bases and full integration into enterprise cloud environments. ER12c, being less mature and internally focused, must carve its value in specific, controlled use cases within ATOS.

From a standards perspective, the solution must anticipate ongoing developments in ISO and EU regulatory frameworks for AI, including the AI Act and Data Act. These evolving policies may impact how AutoML tools are evaluated, especially concerning transparency and model auditability. Moreover, the GDPR imposes additional data protection constraints that complicate training and testing environments for automated systems.

The lack of explainability in AutoML solutions is a recognized risk in sectors like banking or healthcare, where model outputs must be interpretable and justifiable. Integration complexity is another practical barrier, particularly for enterprises with heterogeneous data infrastructures or minimal MLOps maturity. ER12c must be carefully positioned as a flexible and compliant solution that minimizes these obstacles.

- **Technology and market watch**

ATOS maintains an active market watch on AutoML and MLOps developments, recognizing the rapid evolution and opportunity in this space. The partner's input in presented in Table 30. AutoML remains a relatively young field, with significant innovation expected in orchestration, explainability, and energy optimization. ER12c is being evaluated for its potential integration into ATOS's internal machine learning products, with regular review by the CTO and commercial teams.

The continued adoption of cloud-based AI services by Google, AWS, and Microsoft reinforces the strategic importance of developing lightweight, deployable AutoML components. ATOS sees AutoML not only as a technology enhancement but also as a potential driver for new business models, particularly in hybrid deployment contexts and low-code ML enablement. ER12c supports these explorations through its modularity and integration with other internal TANGO outcomes.

Table 30: ER12c Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date	Link
New market opportunities	Federated Learning is a relatively new field. Therea are several solutions in the market, but still plenty of opportunities	New business models	Continue market watch	Project duration	N/A
Active companies and their R&D strategies	Potential internal exploitation in our department for ML products.	Value added to existing products	Meetings with CTO and commercial workforce in our organisation	Project duration	N/A
Impact of new technology adoption	New product. Potential addition to our product portfolio	New product	Meetings with CTO and commercial workforce in our organisation	Project duration	N/A

Exploitation Pathway

The exploitation strategy for ER12c is focused on internal integration within ATOS's product development and ML lifecycle support systems. The tool will be used by the internal data science team to improve efficiency in early-stage model training. This will support the creation and maintenance of existing AI-powered products by accelerating development workflows and reducing compute costs through energy-aware training optimization.

ER12c will follow a hybrid business model. The core component is expected to be open source, released via project deliverables, to facilitate transparency and adoption. However, the user interface (UI) component leverages third-party knowledge and will not be open source, ensuring a degree of proprietary control. There is currently no commercial pricing strategy, as the primary value of ER12c lies in its contribution to ATOS's internal productivity and cost-efficiency. Nonetheless, this model leaves the door open for future commercialization—either as an integrated feature in larger offerings or as a standalone value-added tool.

Although there is currently no intention to seek Horizon Europe follow-up funding for this result, ATOS remains open to future productization. ER12c could evolve into a service offering or form part of a packaged toolset for enterprise AI solutions. Internally, it supports ATOS's strategic goal of reducing vendor dependency and providing tailored ML tools aligned with company priorities and sustainability goals.

Exploitation paths for ER13-Dynamic Intelligent Execution

Competitor analysis

ER13 operates within a specialized niche in the Java-based acceleration and green data center orchestration landscape. Three notable competitors have been identified. **AMD Aparapi**[237] is an open-source solution that enables Java developers to write GPU-accelerated code. While it directly targets Java developers, Aparapi is no longer actively maintained, reducing its long-term competitiveness and reliability. **IBM J9**, an open-source JVM implementation[238], also supports performance optimization but lacks specific features for dynamic energy-aware orchestration. **Oracle's Babylon HAT project**[239], which is still under development, aims to introduce hardware acceleration in Java through improved abstractions. Though not production-ready, it poses a significant competitive threat in the medium term, especially given Oracle's ecosystem dominance.

Compared to these, ER13 differentiates itself by leveraging TornadoVM and enhancing it with ML-based logic for dynamic execution planning. This allows automatic launching of Java code to the most suitable accelerator (e.g., GPU) without requiring the developer to understand GPU programming. This advantage is particularly important for Java enterprise developers and big data providers who lack specialized hardware knowledge. Furthermore, ER13's integration into the TornadoVM open-source project and its runtime intelligence make it more flexible and adaptable than current alternatives, particularly for energy-efficient execution and AI development within the Java ecosystem.

Market Analysis

- **Green Data Center Market ER13 – Dynamic Intelligent Execution**
  - **Segments**

[237] https://aparapi.github.io/
[238] https://www.ibm.com/docs/da/call-center/10.0.0?topic=machines-j9-jvm
[239] https://inside.java/tag/babylon

ER13 aligns predominantly with the **Solutions** and **Services** segments in the European green data center landscape. According to **Grand View Research: Europe Green Data Center Outlook**[240], the Solutions segment—which includes monitoring/management systems, cooling, networking, and power systems and is presented in Figure 38 —generated the largest revenue share in 2024, driven by demand for energy-efficient infrastructure aligned with ER13's capabilities. Meanwhile, Advisory and Support services—installation, deployment, consulting, and maintenance—are cited as the fastest-growing segment by CAGR (>21%), according to both **Grand View Research: Global Green Data Center Market**[241] and **Polaris Market Research**[242], representing a prime opportunity for ER13 to embed dynamic orchestration within managed service offerings.

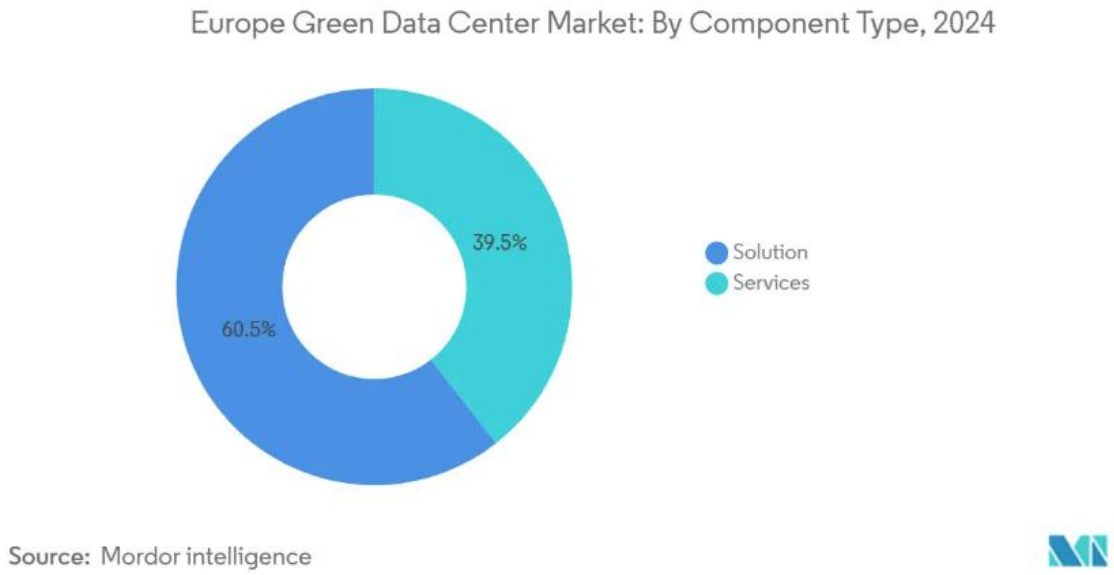


Figure 38: ER13 Green Data Centre market segments (source: Mordor Intelligence)

- **Size and Growth Rate**

Europe's green data center market was valued at **USD 21.8 billion in 2024**, with projections expecting it to reach **USD 64.8 billion by 2030** at a **CAGR of 19.9%**, as stated in Grand View Research: Europe Green Data Center Outlook[243]. Complementing this, Credence Research: Europe Green Data Center Market[244] projects expansion from **USD 12.6 billion in 2024** to **USD 47.1 billion by 2032** at a **17.9% CAGR**, confirming long-term growth. Mordor Intelligence: Europe Green Data Center Industry Analysis[245] also reports an increase from **USD 26.6 billion in 2025** to **USD 59.4 billion by 2030** (17.4% CAGR). Collectively, these forecasts establish ER13 firmly within a fast-growing market set to approximately double by the decade's end.

[240] https://www.grandviewresearch.com/horizon/outlook/green-data-center-market/europe
[241] https://www.grandviewresearch.com/industry-analysis/green-data-center-market
[242] https://www.polarismarketresearch.com/industry-analysis/green-data-center-market
[243] https://www.grandviewresearch.com/horizon/outlook/green-data-center-market/europe
[244] https://www.credenceresearch.com/report/europe-green-data-center-market
[245] https://www.mordorintelligence.com/industry-reports/europe-green-data-center-industry

- **Trends**

A key trend identified by **Credence Research**[246] and **Grand View Research**[247] is the rise of **modular and edge data centers**, which enhance scalability and low-latency processing—ideal environments for ER13's intelligent execution. Generative and AI-based energy optimization, highlighted by Fortune Business Insights: Green Data Center Market[248] and "Markets and Markets": Green Data Center Market[249], is another driver, closely matching ER13's dynamic orchestration architecture. The widespread adoption of renewable energy and PPAs, especially in Nordic countries and Germany, is noted by Mordor Intelligence [250]and Credence Research[251], providing ER13 with opportunities to manage low-carbon power sources intelligently. Lastly, advanced cooling solutions—liquid immersion and free cooling—emphasized by Credence Research[252] and Grand View Research[253], align with ER13's ability to refine thermal and workload responses dynamically. A plethora of market drivers, some which fit ER13, are depicted in Figure 39.

DRIVER	(~) % IMPACT ON CAGR FORECAST	GEOGRAPHIC RELEVANCE	IMPACT TIMELINE
Cloud and Big-Data Workload Surge	+4.2%	Global, concentrated in FLAP-D markets	Short term (≤ 2 years)
EU Green Deal and Fit-for-55 Mandates	+3.8%	EU-wide, strongest in Germany and Nordic countries	Medium term (2-4 years)
Hyperscale and Edge Build-outs in FLAP-D Hubs	+3.1%	Frankfurt, London, Amsterdam, Paris, Dublin	Medium term (2-4 years)
Nordic PPAs Enabling Ultra-Low PUE	+2.4%	Sweden, Norway, Denmark, Finland	Long term (≥ 4 years)
District-Heating Waste-Heat Subsidies	+1.8%	Germany, Denmark, Netherlands	Long term (≥ 4 years)
Scope-3-Focused Green SLAs Demand	+1.3%	EU-wide, led by multinational enterprises	Medium term (2-4 years)

Source: Mordor Intelligence

Figure 39: ER13 Green Data Centre market drivers (source: Mordor Intelligence)

- **Barriers**

Despite favorable trends, ER13 faces notable hurdles, portrayed in Figure 40. The **high upfront CAPEX** for advanced cooling, renewables, and power infrastructure in Europe, cited by **Mordor**

246 https://www.credenceresearch.com/report/europe-green-data-center-market
247 https://www.grandviewresearch.com/horizon/outlook/green-data-center-market/europe
248 https://www.fortunebusinessinsights.com/green-data-center-market-105173
249 https://www.marketsandmarkets.com/Market-Reports/green-data-center-gdc-market-1032.html
250 https://www.mordorintelligence.com/industry-reports/europe-green-data-center-industry
251 https://www.credenceresearch.com/report/europe-green-data-center-market
252 https://www.credenceresearch.com/report/europe-green-data-center-market
253 https://www.grandviewresearch.com/industry-analysis/green-data-center-market

Intelligence[254] and **Fortune Business Insights**[255], may slow adoption among mid-sized data centers. Additionally, **grid-connection delays**, especially in Germany, Ireland, and the UK, are highlighted by **Mordor Intelligence**[256] as structural bottlenecks, potentially limiting real-time optimization by ER13. Finally, **policy fragmentation** across EU countries concerning PUE thresholds, energy reporting, and green certifications is acknowledged by **Credence Research**[257] and **Mordor Intelligence**[258] as a compliance challenge—requiring ER13 to include robust regulatory-framework intelligence.

RESTRAINT	(~) % IMPACT ON CAGR FORECAST	GEOGRAPHIC RELEVANCE	IMPACT TIMELINE
High CAPEX for Liquid-Cooling and On-site RE	-2.1%	Global, acute in retrofit scenarios	Short term (≤ 2 years)
Grid-Connection Delays in Power-Scarce Hubs	-1.8%	UK, Germany, Netherlands	Medium term (2-4 years)
Embodied-Carbon Steel and Concrete Scrutiny	-1.2%	EU-wide, strongest in Germany and Nordic countries	Long term (≥ 4 years)
Sustainable-DC Engineering Talent Shortage	-0.9%	FLAP-D markets, spreading to secondary cities	Medium term (2-4 years)

Source: Mordor Intelligence

Figure 40 ER13 Green Data Centre market restraints (source: Mordor Intelligence)

- **Opportunities**

ER13 can leverage several strategic openings in the EU market. There is strong demand for AI-driven energy management, with current generative AI deployments (from Google to Huawei) creating fertile ground for ER13's dynamic orchestration systems, as noted by Fortune Business Insights[259] and "Markets and Markets"[260]. EU-wide incentives and renewable energy availability, especially in Northern and Western Europe, underscore potential for ER13 to manage and adapt workloads to low-carbon power using intelligent logic, as detailed by Credence Research[261] and Mordor Intelligence[262]. The surge in service-sector growth (CAGR >21%), with rising need for consulting, compliance, and optimization services, offers ER13 a market for embedded orchestration-as-a-service, as seen in Grand View Research[263] and Polaris Market Research[264]. Finally, the rapid expansion of modular and edge data

254 https://www.mordorintelligence.com/industry-reports/europe-green-data-center-industry
255 https://www.fortunebusinessinsights.com/green-data-center-market-105173
256 https://www.mordorintelligence.com/industry-reports/europe-green-data-center-industry
257 https://www.credenceresearch.com/report/europe-green-data-center-market
258 https://www.mordorintelligence.com/industry-reports/europe-green-data-center-industry
259 https://www.fortunebusinessinsights.com/green-data-center-market-105173
260 https://www.marketsandmarkets.com/Market-Reports/green-data-center-gdc-market-1032.html
261 https://www.credenceresearch.com/report/europe-green-data-center-market
262 https://www.mordorintelligence.com/industry-reports/europe-green-data-center-industry
263 https://www.grandviewresearch.com/industry-analysis/green-data-center-market
264 https://www.polarismarketresearch.com/industry-analysis/green-data-center-market

centers, driven by IoT, 5G, and AI, highlighted by Credence Research[265] and Grand View Research[266], presents a prime opportunity for ER13 to deliver AI-native orchestration across distributed green infrastructure.

- **Value proposition analysis**

ER13 delivers a strong and differentiated value proposition by enabling **automatic execution of Java applications on the most suitable accelerator hardware**, such as GPUs, **without requiring the developer to have GPU-specific programming knowledge**. This makes the solution highly attractive to **Java enterprise developers** and **big data providers**, allowing them to harness the power of hardware acceleration in a fully automated and energy-efficient way.

The use of **TornadoVM**, enhanced with a **machine-learning-based runtime system**, allows the generation of hardware-specific code artifacts and the creation of intelligent execution plans. This supports dynamic workload optimization based on the energy-performance trade-offs of available system resources. Importantly, the system is designed for high usability, allowing seamless integration into existing Java codebases while abstracting away hardware-specific complexities.

This solution is particularly relevant for organizations aiming to reduce energy costs and carbon footprint while maximizing system throughput, thereby addressing both technical and sustainability goals. The offering also includes customized development and bug fixes, emphasizing its adaptability to diverse industrial use cases.

- **Barriers, obstacles and analysis of the standards and regulation**

Despite its potential, ER13 faces several concrete barriers. A primary internal challenge is the **lack of dedicated staff at UOM**, which undermines the sustainability and long-term development of the solution. Without sufficient human resources, the ability to maintain and evolve the tool—particularly to compete with fast-developing commercial solutions—remains uncertain.

Additionally, **commercial integration is not guaranteed**, particularly among big data providers. These organizations may be hesitant to adopt new, niche orchestration tools unless there is strong compatibility with existing infrastructure or demonstrable cost savings. The solution must thus prove its value convincingly in real-world settings.

No specific **technical standards or regulations** were cited as applicable, but it is worth noting that ER13 would likely need to align with emerging **European energy performance metrics and reporting requirements** for green data centers. In that context, future iterations should anticipate compliance with evolving ISO standards for energy-aware computing.

- **Technology and market watch**

The technology landscape around ER13 is evolving rapidly. One emerging trend of direct relevance is **Oracle's Babylon HAT project**, which is set to bring hardware acceleration capabilities to the Java platform. While still under development, this initiative could become a strong competitor to TornadoVM-based solutions within three years, given Oracle's widespread adoption in the enterprise Java space.

[265] https://www.credenceresearch.com/report/europe-green-data-center-market
[266] https://www.grandviewresearch.com/industry-analysis/green-data-center-market

Internally, UOM is monitoring these developments but has not yet specified a mitigation strategy. UOM's input is presented in Table 31. It is therefore critical for ER13 to maintain a first-mover advantage by maturing its runtime orchestration capabilities and demonstrating tangible value in live deployments. The intelligent adaptation to multiple hardware accelerators remains a distinct technological differentiator that must be further developed and validated.

Table 31: ER13 Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date	Link
Emerging trend or development	Oracle has released a new project to consider hardware acceleration for Java: Oracle Babylon HAT project: https://inside.java/tag/babylon https://cr.openjdk.org/~psandoz/conferences/2024-JVMLS/JAVA_BABYLON_HAT-JVMLS-24-08-05.pdf	This can be a competitive technology for TornadoVM (the open-source software developed in UoM and used in T5.3)	N/A	ongoing, probably in 3 years	N/A

- **Business Model Canvas**

Even though ER13 is not considered a key outcome of TANGO, UOM has provided a thorough BMC that elaboratively summarizes the organisation's plans for the result beyond the project's lifetime.

Business Model Canvas				
Key Partners	**Key Activities**	**Value Propositions**	**Customer Relationships**	**Customer Segments**
Java providers Hardware providers Cloud providers EXUS (provider of EXUS EDAE)	Release Management Testing (CI/CD) Support (Fix bugs/issues)	An energy efficient execution plan for automatically running highly parallel workloads from Java and Python on the most energy efficient and high-performing hardware device.	Social media (Twitter, LinkedIn, TornadoVM Slack community) Industry-based conferences (DevoxxBE, DevoxxUK, FOSDEM) Blogs (TornadoVM Blogs, TANGO Blogs)	Java enterprise software businesses Big data providers
	Key Resources		**Channels**	

	TornadoVM (to be maintained by UoM) GraalVM-TornadoVM docker images (to be maintained by UoM)		Website GitHub, DockerHub	

Cost Structure	Revenue Streams
Part-time one developer to maintain the TornadoVM/GraalVM docker images	Services (consultancy/training, etc) Maintenance

Exploitation Pathway

ER13's exploitation strategy involves both academic and commercial pathways. Academically, **TornadoVM is being integrated into the curriculum of undergraduate and postgraduate programs** at UOM. This use of the tool in thesis research and teaching ensures knowledge dissemination and skill development among the next generation of developers, potentially enlarging the community around TornadoVM.

The business model foreseen for ER13 is based on an **open-core approach**. An **open-source version** of the tool will be made available to attract early adopters and build a developer community. This community engagement model facilitates feedback, validation, and incremental adoption.

In parallel, a **commercial enterprise edition** will be offered under various licensing options, delivering higher performance, advanced orchestration features, and possibly integration support. This dual-licensing strategy allows UOM to build a user base while developing revenue streams through professional support, licensing, or cloud deployment services.

Adding to the commercialization front, **UOM is currently in the process of spinning off a company** to productize TornadoVM and the ER13 technologies. This includes packaging the enhanced runtime as a solution for Java-based AI and green computing. Furthermore, UOM plans to **apply for additional research grants** to continue bridging the hardware-acceleration gap in the Java ecosystem, particularly targeting energy efficiency, orchestration, and AI-readiness.

Exploitation paths for ER14b- Privacy Threat Modelling and Identification for Trustworthy AI, Privacy Assurance Tool (PAT)

Competitor analysis

The Privacy Assurance Tool (PAT) will enter a market already populated by several prominent providers of privacy management and compliance solutions. One of the main competitors is **OneTrust**, a widely adopted platform that supports organizations in managing privacy, security, and data governance. OneTrust caters to both large enterprises and SMEs, offering a wide suite of risk management and compliance tools. However, it does not provide specific pricing details and does not specifically focus on citizen-driven consent monitoring, which distinguishes PAT's end-user-oriented architecture.

Another key competitor is **TrustArc**, a platform that delivers privacy and data governance solutions with a focus on automating compliance processes. Like OneTrust, TrustArc targets large and small

enterprises, offering tools for responsible AI and data trust, but lacks PAT's strong citizen-centric consent and assurance layer.

A third competitor is **Didomi**, which specializes in privacy and consent management and is tailored to brands and publishers. It supports regulatory compliance and enhances user trust but primarily targets marketing environments rather than end-to-end data lifecycle monitoring. None of these competitors appear to provide an integrated, plug-and-play consent engine that emphasizes GDPR-aligned user monitoring and policy compliance enforcement across sectors like hospitality and public services, which is PAT's primary innovation vector.

- **Market Analysis**

Since ER14b fits within the AI Governance market and Privacy Enhancing Technologies (PET) market, similar to KER14a, its market analysis in depicted in Section 6.7.2.

In summary, in the AI Governance domain, it contributes directly to the core compliance functions—privacy assurance, data risk assessment, and auditability—which are essential under the incoming **EU AI Act** and existing **GDPR**. According to Grand View Research, the AI Governance market reached USD 227.6 million in 2024 and is forecast to grow to USD 1,418.3 million by 2030 at a CAGR of 35.7%[267]. Europe's dominant regulatory role ensures sustained demand for tools like PAT that offer runtime compliance verification.

Within the PET market, PAT aligns with software solutions for compliance and risk management. The PET software segment alone exceeded USD 3 billion in 2024, fueled by the spread of cloud, IoT, and AI systems that need continuous data protection[268]. PAT's runtime support for privacy assurance positions it uniquely to address automated GDPR compliance across data-sharing platforms, especially in hospitality and health—sectors where sensitivity to user data is highest.

- **Value proposition analysis**

The Privacy Assurance Tool (PAT) has been conceived to return control of personal data to individuals while enabling organizations to respect and enforce consent agreements under GDPR. By embedding a secure, encrypted, and consent-based data-sharing platform, PAT ensures both legal and technical compliance. It allows organizations to enforce privacy rules, log user interactions, and audit compliance systematically. For end-users—especially in the hospitality domain—it enables citizens to define their privacy requirements when contracting services and monitor how their data is used and protected over time. Its value lies in providing a scalable, flexible, and auditable solution that integrates easily across domains while empowering citizens and reducing organizational compliance risks.

- **Barriers, obstacles and analysis of the standards and regulation**

Despite its strengths, PAT faces several challenges in market deployment. A key barrier is the **fragmented data infrastructure** in target sectors such as hospitality and healthcare, which limits interoperability and slows integration. Additionally, there is **low awareness of GDPR's technical compliance requirements**, especially among SMEs, which may reduce demand for advanced assurance tools like PAT.

Obstacles include the difficulty of **integrating PAT into legacy systems** that were not designed for consent monitoring and compliance tracking. Another issue is **gaining user trust in novel consent interfaces**, especially in sectors where user experience is a major commercial driver. On the regulatory

[267] Grand View Research
[268] Grand View Research

side, PAT is directly shaped by **GDPR Articles 5, 6, and 7**, which cover data minimization, consent, and security, as well as national data protection laws across the EU. These legal standards are both a driver for adoption and a compliance burden that must be met precisely by PAT's architecture.

‣ Technology and market watch

FUJ_LU's input on market watch, presented in Table 32, identifies multiple opportunities for PAT. First, **consultancy services around GDPR-compliant system architecture** are a key use case. These services will enhance digital trust by enabling organizations to enforce consent dynamically while helping end-users specify how their data should be used. This service layer will be offered alongside the core product and is already planned for deployment in the hospitality sector across Europe.

Additionally, PAT is intended for **integration and adaptation within Horizon Europe projects** focused on secure and privacy-preserving data systems. FUJ_LU will collaborate with EU partners to integrate PAT into ongoing and future R&D efforts, helping build a reputation as a reference point in privacy-preserving solutions. These efforts will involve both technical deployments and the analysis of national and European call opportunities to extend the tool's reach.

Table 32: ER14b Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date	Link
Other	Consultancy services around PAT for GDPR-compliant system architecture design.	* Enhancing confidence for digital end users by ensuring GDPR compliance and auditability. * Empowering end users to specify terms and conditions for the use of their data by organizations.	* Offer consultancy and auditing services, leveraging expertise in GDPR compliance. * Organize events to promote the tool, targeting the smart hospitality sector for use and integration across Europe and nationally.	Immediate, with ongoing consultancy offerings.	Not Defined
Other	Integration and adaptation of PAT within Horizon Europe projects focused on security and privacy-preserving systems.	* Enhanced collaboration and innovation in security and privacy technologies. * Contributing to the development of cutting-edge solutions in data protection. * FUJITSU as a reference in privacy-preserving solutions.	* Collaborate with Horizon Europe partners to integrate PAT into ongoing and future research projects. * Leverage PAT's capabilities to address privacy challenges across various sectors. * Analyze upcoming European and national calls.	Align with the timelines of national and Horizon Europe calls.	Not Defined

‣ Exploitation Pathway

PAT will follow a multi-pronged exploitation strategy. First, it will be **integrated as a consent engine into existing data-sharing platforms**, providing runtime assurance and enabling auditability. This will be supported by **consultancy and auditing services** targeting GDPR-compliant system design—especially for sectors like tourism, hospitality, healthcare, and public services. These services may include software integration, development, or customization tailored to specific client needs.

The foreseen business model for PAT is a **hybrid between consultancy services and product sales**. On one hand, FUJ_LU will offer PAT as a standalone consent engine that can be integrated into organizational infrastructures. On the other hand, the organization will generate revenue through GDPR compliance consultancy, offering auditing, system design, and privacy enhancement services. This hybrid model ensures both tool adoption and long-term value creation through expert guidance, making PAT a cornerstone of scalable, trustworthy AI and data governance in Europe.

Furthermore, PAT will be **used and further developed in Horizon Europe projects**, ensuring continued evolution and alignment with cutting-edge privacy-preserving architectures. FUJ_LU plans to offer consultancy around PAT while supporting its adoption through organized events, promotional activities, and direct collaboration with relevant EU sectors. Pilot deployments will begin in the tourism domain, and expansion into other regulated domains is already envisioned.

Exploitation paths for ER15- X-AI for Privacy and Trust Enhancement

Competitor analysis

ER15 enters a competitive but highly dynamic Explainable AI (XAI) market, populated by both research-driven frameworks and sector-specific commercial solutions. One major competitor is **XAIport**, an academic framework that delivers early explanations as microservices via Open APIs. Its architecture targets AI/ML development teams and data scientists looking to integrate configurable XAI operations in the early stages of model development. XAIport is designed with a service-oriented approach but is primarily academic in nature and likely distributed under open-source or research licenses, with enterprise adoption requiring custom integration.

A second competitor, **Athena XAI**, focuses on the eCommerce sector. Its platform offers human-centric explainability across various products like intelligent search, product recommendations, and analytics. With a clear SaaS model and tiered pricing strategy, Athena XAI serves digital retailers aiming to enhance customer experience and conversion rates through transparent AI-driven personalization. While commercially advanced, its niche market focus (eCommerce) limits overlap with ER15's target sectors.

The third competitor, **XMANAI**, aligns more closely with ER15's sectoral orientation. It is a Horizon 2020-funded project designed for the manufacturing sector, offering explainable AI for demand forecasting and production planning under an Industry 5.0 approach. XMANAI offers a user-centric platform with both technical and business-facing components and is expected to transition to a commercial license. While it targets similar clients, ER15 differentiates itself by combining explainability with **privacy-preserving capabilities**, and by being technically accessible through a **Streamlit front-end and FastAPI back-end**, which simplifies enterprise deployment.

Together, these competitors highlight the novelty of ER15's combination of **domain-specific deployment (banking and manufacturing), privacy protection, and flexible, real-time integration features**, positioning it uniquely in a maturing market.

Market Analysis

- **ER15 — X-AI for Privacy and Trust Enhancement within the Explainable AI (XAI) market**
  - **Segments**

ER15 addresses the **solution and services segments** of the Explainable AI market, with a clear focus on applications like fraud and anomaly detection, identity and access management, and healthcare diagnostics — all of which demand interpretable AI to ensure privacy, fairness, and compliance with EU data protection laws. By embedding explainability directly into AI models, ER15 supports sectors where transparency and trust are paramount, including finance, healthcare, and government services. These segments are already the most revenue-generating and fastest-growing within the XAI market

globally and in Europe, where GDPR-driven transparency requirements reinforce demand for privacy-preserving, explainable systems[269].

- **Size and Growth Rate**

The global explainable AI market is booming and projected to expand from USD 7.8 billion in 2024 to over USD 21 billion by 2030 at an impressive CAGR of 18% (Grand View Research). Some forecasts, shown in Figure 41, even estimate growth up to USD 34.6 billion by 2033, highlighting sustained investor confidence (MarketUs). For Europe specifically, robust growth is expected due to strict data protection laws like GDPR and the EU's push for trustworthy AI. This makes the region a fertile ground for ER15's XAI solutions that embed explainability into AI-driven privacy safeguards and transparent decision-making. Companies investing in XAI can thus address both regulatory requirements and societal trust concerns[270].

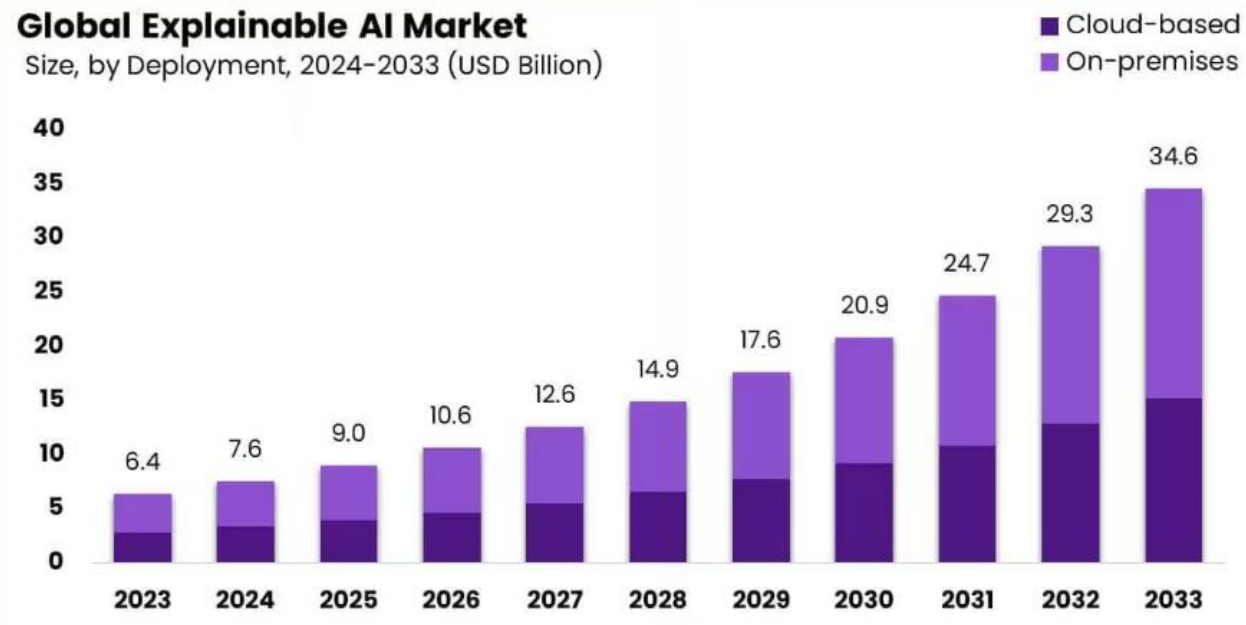


Figure 41: ER15 Explainable AI market size and growth rate (source: MarketUS)

- **Trends**

The momentum behind explainable AI in Europe is fuelled by the rising complexity of deep learning systems and the growing demand for transparency in high-stakes sectors. Industries such as healthcare and finance increasingly need AI that not only predicts outcomes but also justifies them in ways humans can understand — this is critical for compliance, auditability, and public trust. Multimodal explainability, which combines data types like text, images, and numerical data, is gaining traction, aligning with the EU's strategic vision for trustworthy, human-centric AI. Additionally, the push towards AI governance frameworks, such as the EU AI Act, will cement explainability as a must-have rather than a nice-to-have, providing ER15 with a tailwind[271].

[269] Grand View Research, Explainable AI Market Report; MarketUs, Explainable AI Market
[270] Allied Market Research, Explainable AI Market
[271] Grand View Research; SNS Insider via GlobalNewsWire, Explainable AI Market

- **Barriers**

Despite this favourable climate, challenges could hinder ER15's deployment. The main barrier is the **complexity of designing explainable deep learning models** without sacrificing performance — balancing accuracy and interpretability remains technically challenging. Moreover, a shortage of skilled XAI professionals in Europe slows the ability to implement explainability at scale within existing AI pipelines. Smaller firms may also struggle with the upfront cost and integration effort required to embed advanced XAI techniques into legacy systems. These obstacles underline the importance of user-friendly, cost-efficient solutions, which ER15 must address to gain wide adoption (MarketUs; Allied Market Research).

- **Opportunities**

ER15 is ideally positioned to seize significant market opportunities. In Europe, sectors like healthcare, finance, and public administration face mounting regulatory and societal demands for fair, accountable AI. ER15's explainable AI can enhance data privacy compliance under GDPR, reassure regulators, and foster user trust — a competitive differentiator in Europe's ethically conscious digital economy. With the EU AI Act poised to enforce stringent transparency obligations for high-risk AI applications, solutions that embed explainability and privacy-by-design will be in high demand. This regulatory certainty creates an enabling environment for ER15 to become a key enabler of lawful, trusted, and auditable AI across Europe's high-value sectors (Grand View Research; MarketUs; Allied Market Research).

Value proposition analysis

The core value of ER15 lies in bridging the persistent gap between AI transparency and data privacy within enterprise systems. Specifically designed for banking and manufacturing organizations, ER15 delivers **interpretable AI insights** through proven explainability techniques such as SHAP, LIME, DeepLIFT, and Integrated Gradients. These insights are provided via an **intuitive Streamlit user interface** supported by a **scalable FastAPI backend**, allowing seamless enterprise deployment.

By integrating privacy-preserving mechanisms into the explainability pipeline, ER15 ensures that sensitive enterprise or customer data is never exposed during analysis. This capability enables companies to **satisfy regulatory requirements (e.g., GDPR, upcoming EU AI Act)**, gain stakeholder trust, and accelerate responsible AI adoption—all without compromising data confidentiality. In doing so, ER15 helps organizations **reduce risk, increase fairness, and ultimately improve user acceptance** of AI-driven decisions.

Barriers, obstacles and analysis of the standards and regulation

A key barrier to ER15's adoption is the **high complexity of integrating explainable AI tools into legacy enterprise systems**, especially in banking and manufacturing where systems are often deeply entrenched. Even when technical integration is feasible, **organizational inertia** and resistance to perceived non-essential changes (especially when current AI systems appear to perform adequately) can hinder adoption.

Additionally, there is a **lack of universally accepted standards** for measuring and validating explainability and privacy-preserving AI methods. This introduces uncertainty among enterprise adopters who may struggle to assess ER15's performance relative to undefined benchmarks. Regulatory uncertainty further compounds the challenge: although GDPR and the EU AI Act demand transparency, **the specific technical requirements remain under-defined**, particularly in industry-specific contexts such as finance and manufacturing.

Moreover, decision-makers often lack awareness of the **benefits and feasibility of privacy-preserving explainability**, leading to **budgetary hesitations and prolonged procurement cycles**—especially in highly regulated sectors. ER15 will need to overcome these hurdles through strategic education, accessible pricing models, and compliance-aligned messaging.

▸ Technology and market watch

The competitive and technological landscape for ER15 is rapidly evolving. SQD's input on this matter in depicted in Table 33. Notably, **2025 is being positioned as the "Year of Explainable AI"** due to regulatory momentum. Industry analysts predict a surge in demand for global and local explainability, especially in the **banking sector**, driven by accountability mandates. This trend opens a **massive first-mover opportunity** for ER15, particularly if it accelerates go-to-market strategies and aligns messaging with compliance needs.

Additionally, major players like **Siemens and Deloitte** are actively deploying XAI in manufacturing and banking, respectively. Siemens uses explainable AI for **predictive maintenance**, while Deloitte has developed **XAI frameworks for compliance in banking**. These developments validate the market direction and reinforce the need for ER15 to **differentiate through privacy integration and deployment flexibility**.

Emerging technical trends are also shaping the future of ER15. Patents and implementations are increasingly focused on **real-time explainability (e.g., SHAP/LIME live predictions)**, moving beyond batch processing. This creates both a **competitive threat and an opportunity**: ER15 can extend its FastAPI back-end to support real-time streaming explainability while protecting IP through defensive patents.

Table 33: ER15 Technology and Market watch

Item	Description	Possible Impact	Actions	Effective Date	Link
Emerging trend or development	2025 positioned as "Year of Explainable AI" with regulatory push. Industry experts predicted 2025 as breakthrough year for XAI adoption, driven by transparency and accountability requirements. Global vs. local explanations becoming standard requirement, with increased regulatory mandates for AI explainability in financial services.	Massive market opportunity expansion with regulatory tailwinds; increased demand across banking and manufacturing sectors creating first-mover advantage potential.	Accelerate go-to-market strategy leveraging regulatory momentum. Enhance global explanation capabilities in SHAP/LIME implementation. Develop compliance-focused marketing materials and case studies.	Ongoing	https://riveron.com/post/102jlmy/will-2025-be-the-year-of-explainable-ai-xai/
Active companies and their R&D	Siemens implements enterprise-scale XAI for AI-driven predictive maintenance in manufacturing, preventing	Validation of manufacturing and banking sector focus; potential major partnership	Analyse Siemens' and Deloitte's XAI approaches for competitive	Ongoing	https://blog.algoanalytics.co

strategies	equipment failures and reducing downtime. Deloitte provides comprehensive XAI banking framework guidance for risk, compliance, and business executives, positioning established players in target markets.	opportunities or competitive threats from established enterprise players with existing customer relationships.	differentiation. Develop manufacturing predictive maintenance and banking compliance case studies. Pursue strategic partnerships with industrial equipment and financial technology vendors.		m/2025/05/05/the-rise-of-explainable-ai-xai-a-critical-trend-for-2025-and-beyond/
Latest innovations and IP	New patents and innovations focus on integrating Explainable AI tools like SHAP and LIME for real-time model predictions in production banking and manufacturing systems, moving beyond batch processing to live environment implementations.	Direct competitive threat; significant opportunity to enhance real-time capabilities and establish IP protection for privacy-preserving real-time XAI.	Benchmark FastAPI implementation against real-time XAI solutions. File defensive patents for privacy-preserving real-time explainability. Develop streaming capabilities for live SHAP/LIME explanations.	Ongoing	https://www.javacodegeeks.com/2025/03/explainable-ai-in-production-shap-and-lime-for-real-time-predictions.html

▸ **Business Model Canvas**

Even though ER15 is not considered a key outcome of TANGO, SQD has provided a thorough BMC that elaboratively summarizes the organisation's plans for the result beyond the project's lifetime.

Business Model Canvas				
Key Partners	**Key Activities**	**Value Propositions**	**Customer Rela**	**Customer Segments**
AI Vendors: Integrate explainability tools	Develop and maintain XAI	Transparent, interpretable AI decisions	Self-service UI with documentation	Financial institutions using

to boost model transparency and compliance. **Cloud Platforms**: Enable scalable deployment of XAI via containerized services. **Regulatory Technology Firms**: Support regulatory compliance with explainability insights. **System Integrators**: Embed XAI modules into client AI pipelines for added trust. **AI Research Labs**: Use for testing, benchmarking, and developing new XAI methods. **Privacy Tech Firms**: Combine with secure AI tools to ensure private, interpretable models.	engine (SHAP, LIME, etc.) Design and test UI (Streamlit) for user interaction Operate and scale API/backend services (FastAPI) Containerize and deploy via Docker Collect feedback and iterate based on user input **Key Resources** Explainability libraries and in-house IP Streamlit UI and FastAPI backend components Docker containers for deployment Skilled AI/ML and DevOps team Secure data environments for privacy testing	Privacy-preserving explainability framework Ready-to-integrate, modular architecture Cross-domain application (finance + manufacturing) Scalable, demo-ready with feedback loop	Dedicated support for integration and compliance Feedback-driven updates and feature tuning API access and onboarding tutorials **Channels** Direct partnerships with AI vendors and system integrators Online deployment via cloud marketplaces Tech workshops and demos for enterprise clients GitHub and developer portals for adoption	AI for decision-making Manufacturing companies using vision-based AI AI product teams needing explainability Compliance and risk management teams AI research groups

Cost Structure	**Revenue Streams**
Development (engineering, testing) Infrastructure (cloud hosting, APIs, container orchestration)	Licensing (per deployment or usage tier) SaaS subscription for hosted version

Compliance and security assurance Customer support and training materials R&D for new XAI techniques	Custom integrations and enterprise support White-labeling or OEM licensing Training and consultation services

- **Exploitation Pathway**

The exploitation strategy for ER15 involves a **multi-pronged approach** focused on both service provision and product commercialization. First, **XAI-as-a-Service** will be delivered through the FastAPI backend, targeting banking and manufacturing clients seeking plug-and-play explainability features. Second, **software licensing** will be offered for on-premises deployment of the explainability engine, allowing enterprise clients to maintain full control over their infrastructure and data.

The business model for ER15 is structured as **B2B SaaS + Licensing**, featuring multiple revenue streams:

- **Subscription-based SaaS**: Monthly or annual tiers for API-based access, with pricing differentiated by usage level and enterprise features.
- **Software Licensing**: One-time or renewable licenses for organizations preferring on-premise deployment.
- **Professional Services**: Custom integration, deployment, and consultancy support.

The pricing strategy includes a **freemium model** to attract mid-market clients, **usage-based pricing** for scalable deployments, and **enterprise contracts** for high-value customers.

The broader exploitation plan includes three stages:

1. **Market Entry**: Launch a freemium SaaS offering, secure pilot users in banking and manufacturing, and initiate distribution through partnerships with AI consultancy firms.
2. **Scale & Validate**: Expand service tiers and secure endorsements from regulatory stakeholders in the financial sector. Build partnerships with AI platform vendors to boost accessibility.
3. **Growth & Diversification**: Develop vertical-specific modules for other sectors (e.g., healthcare, insurance), introduce white-label licensing options, and establish a regional presence in high-regulation markets to benefit from compliance-driven procurement.

This structured plan ensures ER15 becomes a sustainable, scalable, and compliance-aligned tool for trustworthy AI deployment in Europe and beyond.

SQD anticipates that given our privacy-preserving focus in banking and manufacturing sectors, a realistic market share target of 1-3% of the combined banking + manufacturing XAI market could generate $25-105 million potential annual revenue by 2030, leveraging the unique privacy differentiation in a high-growth environment.

Beyond direct industrial use (e.g., **loan decision support in banking**, **predictive maintenance in manufacturing**), SQD plans to offer **consultancy services** to support AI transparency compliance and implementation. Additionally, **training services** will be provided, including workshops and tailored courses on explainable AI for sector-specific use cases. A **joint venture strategy** is also being considered for building co-developed solutions with major sector stakeholders.

Annex D – List of TANGO Exploitable Results

#	Exploitable Result (ER)	Ownership	Owner(s)	Contrib.	Related Task(s)	Result type	Current TRL
1	Blockchain-based data storage and sharing	Single	NOR	NOR	T3.1	Integrated platform	TRL 6
2a	Trustworthiness Scoring Module (TSM)	Single	FUJ	FUJ	T3.2	System/ Model	TRL 4
2b	Ubiquitous Personal Context Vectors (UPCVs)	Single	VTT	VTT	T3.2	SW (standalone)	TRL 6
2c	Privacy Risk Score (PRS)	Single	FHG	FHG	T3.2	System/ Model	TRL 4
3a	Confidentiality and Privacy by Design: PEP and Sticky Policies	Single	UMU	DUT	T3.3, T4.1	SW (standalone)	TRL 4
3b	Confidentiality and Privacy by Design: ABE-toolset	Single	ATOS		T3.3, T4.1	SW (standalone)	TRL 4
4	Self-encryption and Decryption Techniques with Multi-Factor Information Recovery Mechanisms	Single	DUT	NOR, FHG, DUT, UMU	T3.4	Algorithm	TRL 3
5	ePrivacy Mechanisms, Protocols and Processes	Single	KUL	NOR, SQUAD, DBC, DUT, UTH, LIC	T3.5	Guideline	N/A
6a	SSI Wallet	Single	VTT		T4.1	SW (standalone)	TRL 4
6b	SSI Zero Knowledge Proof	Single	UMU		T4.1	SW (standalone)	TRL 4
6c	SSI Agent	Single	ATOS		T4.1	SW (standalone)	TRL 4

#	Exploitable Result (ER)	Ownership	Owner(s)	Contrib.	Related Task(s)	Result type	Current TRL
6d	IoT Machine-to-Machine Device Authentication	Single	UMU		T4.1	SW (standalone)	TRL 4
7	Seamless onboarding for users	Single	QBE	QBE	T4.2	SW (standalone)	TRL 5
8	User continuous behavioural authentication	Single	QBE	QBE	T4.3	SW (standalone)	TRL 5
9	Device continuous behavioural authentication	Single	UTH	UTH	T4.4	SW (standalone)	TRL 4
10	Hardening against Sidechannel Attacks	Single	CEA	CEA, VTT, DUT	T4.5	SW (standalone)	TRL 4
11	Exploratory Data Analysis engine (EDAE)	Single	EXUS	EXUS, UOM, UOG	T5.1	SW (standalone)	TRL 6
12a	Energy efficient AI model training Support for MLOps	Single	ATOS	ATOS, EXUS, XLAB, UOM, ANYS	T5.2	SW (standalone)	TRL 6
12b	Energy efficient AI model training Support for Federated Learning	Single	ATOS	ATOS, EXUS, XLAB, UOM, ANYS	T5.2	SW (standalone)	TRL 6
12c	Energy efficient AI model training Support for AutoML	Single	ATOS	ATOS, EXUS, XLAB, UOM, ANYS	T5.2	SW (standalone)	TRL 4
13	Dynamic Intelligent Execution	Single	UOM	UOM, ATOS, UTH, EXUS, TUB, ETH, FORTH, LUX	T5.3	SW (standalone)	TRL 6 – TRL7

#	Exploitable Result (ER)	Ownership	Owner(s)	Contrib.	Related Task(s)	Result type	Current TRL
14a	Privacy Threat Modelling and Identification for Trustworthy AI Privacy Enhancing Component (PEC)	Single	UOG	UOG	T5.4	SW (standalone)	TRL 6
14b	Privacy Threat Modelling and Identification for Trustworthy AI Privacy Assurance Tool (PAT)	Single	FUJ_LU	FUJ_LU	T5.4	SW (standalone)	TRL 4
15	X-AI for Privacy and Trust Enhancement	Single	SQD	SQD, ATOS, EXUS, SVI, QBE, XLAB, KUL	T5.5	AI & ML Model/ Method	TRL 6
16	Infrastructure Management based on AI	Single	XLAB	XLAB	T5.6	AI & ML Model/ Method	TRL 4
17	TANGO Modular Platform	Joint	All partners	ATOS, ATOS SP, FSDE, FUJ_LU, SQUAD, NOR, LSTECH, QBE, SQD, XLAB, CEA, VTT, DUT, UMU, UTH, UOM, UOG, ANYS	T6.1, T6.2, T6.3, T6.4	Integrated platform	TRL 4
18	TANGO Connectors	Joint	UTH, INTRA, ATOS, UMU, VTT		T2.5, T6.1	SW (standalone)	TRL 6

Annex E – Joint Exploitation Agreement (JEA) Template

Joint Exploitation Agreement – JEA (Template)

In (city, country) on the (date) and between:

(Name of the partner 1), (Address, city-country-pc), (Tax identification number or any other identification information used in the country of interest), hereinafter referred to as **"LICENSOR"**

And

(Name of partner 2 or any third party), (Address, city-country-pc), (Tax identification number or any other identification information used in the country of interest), hereinafter referred to as **"LICENSEE"**

also both, hereinafter, jointly or individually, referred to as "Parties"

now, therefore, it is hereby agreed as follows:

Article 1 – Description of works

The LICENSOR states / warrants:

i. that they hold or represent formally all rights including but not limited to patents of the TANGO's results,
ii. that no intellectual property rights of third party/parties are infringed,
iii. that they exclusively own or otherwise control (and shall continue to own or control) all rights of the of the TANGO's results,
iv. that they will at all times defend, indemnify and hold harmless the LICENSEE and each and every user of the TANGO's results, as referred to in article 2, from and against any claims, damages, liabilities, costs and expenses, including legal expenses and reasonable counsel fees, arising out of any alleged breach or breach by LICENSOR by any warranty, representation or agreement, express or implied made by LICENSOR herein,
v. they are solely responsible should any third party's intellectual right be infringed by the TANGO's results, as referred to in article 2,
vi. To the extent possible, the Licensor waives and/or agrees not to assert any moral rights held by the Licensor

Article 2 - TANGO's Results

i. For the purposes of this contract, with the term "TANGO's results" we shall refer to details and a description of the exploitable result(s) for which the agreement will be conducted related to each status, operation and utilization in general.
ii. The aforementioned results have been developed by the LICENSOR as a result of their participation in the TANGO project, funded by the European Union's Horizon Europe research and innovation programme under grant agreement No 101070052.
iii. The LICENSOR shall remain the owner of the patent related to the TANGO 's results and the licensee shall seek protection and maintain the patent aforesaid, in accordance with the applicable regulations.

Article 3 - Non-exclusive license, including sub-license and power of attorney

i. License of rights:
   a. The LICENSOR, owns 100% of all rights of the above mentioned results and grants the LICENSEE the non-exclusive, (royalty free), worldwide (or limited to specific regions) exploitation and sub licensing right of the TANGO's results.
   b. The LICENSOR is still competent to exploit the TANGO's results or to license the above mentioned results to third parties (this applies only in case of a non-exclusive agreement).
   c. The LICENSOR authorizes the LICENSEE and their sub licensees at their expense to make control, settle and release, on Licensor's behalf, any claims related to intellectual property infringement with respect to the above mentioned TANGO's results.

ii. Exploitation by the LICENSEE:

This license includes global exploitation by all means (or limited in specific regions). The LICENSEE is granted to exploit the above mentioned TANGO's results via: (add the way the exploitation will be done)

Article 4 – Payment terms

The LICENSEE agrees to pay the amount of (agreed payment) to the LICENSOR (the agreement could foresee a one-time payment or any other ways such as for instance milestone payments, royalties on net sales, etc, which shall be described in detail here)

(the way the LICENSOR could be able to claim the payment shall also be described, such as the prior issue of a payment document for instance)

The amount of money payable here is non-creditable and non-refundable and does not include taxes.

Article 5 – Exploitation period

(please define the exploitation period in months, years, or any other applicable way. It may refer to a period of time following the signing of this agreement, indefinitely or for a specific period of time.)

Article 6 – Termination

i. The LICENSOR and LICENSEE have the right to terminate the present contract at any time, after a written claim (you can always agree otherwise). Following this, the LISENSEE will refrain from any exploitable activities on the TANGO's results effective immediately.
ii. In case the contract is terminated for any reason, this termination will also affect the effective contracts which have been concluded by the LICENSEE with any third party up to the moment of termination.

Article 7 – Applicable law

i. This contract is governed by (country of origin) Law
ii. Any dispute regarding the construction or performance of this contract shall be submitted to the competent courts of (country of origin).

Article 8 – General rules

i. Should one term/clause under the present agreement is judged illegal or void, the validity and effect of the remaining contract are not affected.

ii. The LICENSEE is encouraged to seek legal advice if any of the above mentioned terms are unclear or when the LICENSEE is unsure if he/she is entitled to sign this contract. the LICENSEE hereby declares that he or she understands the clauses and scope of this agreement.

The undersigned legal representatives of both parties acknowledge to have thoroughly read this non-exclusive exploitation contract in its totality and agree to its provisions without reservation.

On behalf of the LICENSOR, as represented by their legal representative:

Full name: _____

Job title: _____

Date: _____

Signature: _____

On behalf of the LICENSEE, as represented by their legal representative:

Full name: _____

Job title: _____

Date: _____

Signature: _____

Annex - F Exploitation plan - Table for all partners

ATOS	Eviden is leader in cybersecurity with large portfolio of cryptographic and IAM solutions (https://eviden.com/solutions/cybersecurity/digital-identity/) with established customer channels and sales activities. In 2024, Eviden announced the launch of Evidian Orbion, next-generation Identity-as-a-Service (IDaaS) solution that integrates Identity Governance and Administration (IGA), Access Management (AM), and Privileged Access Management (PAM) into a single as-a-Service solution designed for hybrid environments. The solution also provides advanced capabilities like identity proofing and decentralized identities (SSI). We also plan to integrate TANGO results into existing value propositions and position it within our IAM solution.
ATOS SP	Same like above
FTSDE	Fujitsu will leverage especially the practical the insights of the TANGO project for further research on IoT Trustworthiness. Moreover, these insights support the consulting branch with respect t the role of Trustworthiness as a contribution of access management considering space, devices and data.
FUJ_LU	FUJ_LU will exploit the knowledge and technological advancements gained in TANGO through further development, integration, and consultancy around its Privacy Assurance Tool (PAT) developed in ER14b. The partner plans to incorporate PAT into GDPR-compliant data-sharing platforms, particularly in sectors like hospitality and health. The exploitation strategy includes offering consultancy services, software integration, and participation in Horizon Europe projects focused on privacy-preserving technologies. FUJ_LU also plans to use PAT as a tool in training, system architecture design, and policy promotion around digital privacy.
INTRA	As the integrator of the TANGO project, Netcompany-Intrasoft has implemented CI/CD pipelines and contributed to the development of TANGO connectors across its use cases. Our primary exploitation pathway is via IT consulting services in both public and private sector projects that require secure, decentralized data management, basically in line with TANGO's vision of privacy-enhanced, trusted data sharing. The expertise and technical know-how we gained during the deployment of the TANGO technologies, including federated identity and data sovereignty mechanisms, positions us to support future digital transformation initiatives requiring similar architectural and/or interoperability frameworks. We also aim to capitalize new research opportunities and to actively contribute to a potential Innovation Action (IA) that extends TANGO's technological foundations, as a continuation of the concept of TANGO from a research project (RIA), to a more mature and market oriented and mature project (IA). Moreover, the project helped us to build strong networks with industry partners and end users, particularly via active involvement in use case implementation. Particularly in domains such as smart manufacturing, digital public services, and cross-border data ecosystems.

SQUAD	Although SQUAD, as a technology provider with expertise in cybersecurity and data privacy, SQUAD is expected to capitalize on the project's outcomes by integrating TANGO technologies into its existing security services. In line with the proposal's strategy for technology providers, SQUAD will likely enhance its product offering with secure data-sharing features and may consider participating in spin-offs or start-ups, leveraging TANGO's research to strengthen its commercial positioning in trusted computing and data protection.
NORB	Norbloc will build on the results of the TANGO project to strengthen and expand the use of its Fides platform, which is already commercially deployed for secure, consent-based data sharing. The pilot validated Fides in cross-border and public sector use cases, particularly for visa processing and identity verification. These results will support ongoing improvements to the platform and open new opportunities in regulated sectors such as digital identity and government onboarding. Throughout the project, Norbloc also established a strong network of collaborators across both technical and institutional domains, which will support future deployments and partnerships. Additionally, Norbloc plans to contribute insights from the pilot to EU-level digital identity standardization initiatives.
DBC	DBC, a consulting company, sees TANGO as an opportunity to expand its innovation management and research commercialization services. The exploitation strategy includes: i) Expansion into new markets: DBC plans to offer consulting services to a broader range of clients, leveraging expertise gained from the project. ii) Participation in future R&D projects: By actively participating in TANGO, DBC strengthens its profile as a key partner in Horizon Europe and digital industries initiatives. iii) Intellectual Property utilization: DBC expects that TANGO will generate valuable IP that can be leveraged to facilitate the development of new businesses and services. With its established presence in consulting and exploitation planning, DBC aims to solidify its position as a leader in research commercialization and digital industries innovation.
EXUS	EXUS participation in TANGO aligns with its business strategy in exploiting innovation results from EU projects as a trade secret. Its leading activities in AI & Data analytics activities are part of the implementation roadmap of the EXUS AI Technologies (EXAITE) Suite, which is a major mid-term commercial milestone that will ensure its greater scaling-up and financial viability. EXUS foresees to enhance its portfolio offering of managed services through TANGO developments by advancing them beyond project closure to enable commercialisation pathways via its sales network in 35 countries worldwide, following the TANGO participatory approach with end-user co-designing and acceptance. The results of TANGO will be combined with other EXUS solutions in the retail sector enabling the company to

	establish a strong presence in the niche field of retail data analysis and possibly sustainable hospitality that is on the rise.
LSTECH	As a technology provider involved in ICT and AI, LSTECH is expected to incorporate the insights and components developed in TANGO into its commercial and pre-commercial offerings. Although it did not lead an ER/KER, it will likely use the project outcomes to improve the robustness, scalability, and security of its systems. This could involve enhancing current services, transferring technologies to partners, or participating in future R&I activities focused on AI governance and trust.
SVI	SVI is expected to pursue exploitation through the integration of TANGO results into its cybersecurity solutions. Even though it did not develop a specific ER/KER, it may adopt relevant AI-based threat identification or trust-enhancing mechanisms in its commercial roadmap. Additionally, SVI may explore training services, licensing opportunities, and contributions to regulatory policy via participation in industry dialogues shaped by TANGO outcomes.
QBE	QBE will capitalize on the project's results to deliver secure, user-friendly digital identity solutions. By offering cloud-based services and SDKs for seamless onboarding and continuous behavioural authentication, QBE targets sectors such as banking, fintech, gaming, and law enforcement agencies. These solutions will help clients meet privacy and regulatory standards, while reducing onboarding costs and enhancing fraud prevention. To support adoption, QBE will integrate these technologies into its cybersecurity portfolio and provide consulting services aligned with digital transformation needs. Additionally, it will pursue licensing agreements and research opportunities through Horizon Europe to advance AI-driven identity technologies.
SQD	SQD will exploit ER15 ("X-AI for Privacy and Trust Enhancement") through a multifaceted plan including the provision of XAI-as-a-Service for banking and manufacturing clients, software licensing of its explainability engine, and direct industrial use within financial and manufacturing AI systems. It will offer consultancy and training services and pursue joint ventures to co-develop vertical-specific solutions. The business model follows a B2B SaaS approach with freemium and usage-based pricing tiers. SQD will also participate in further R&D and regional deployments to expand market presence and regulatory alignment.
XLAB	XLAB will exploit the results following two paths, namely the commercial and scientific. In the scientific context, XLAB will utilize the project outcomes to strengthen its position in AI domains and will further pursue the research activities. In the commercial sense, XLAB intends to further develop RENOPS into a market-ready service or solution. XLAB will continue to disseminate the TANGO results it contributes to through its communication channels and use the research activities from the project for academic publication, as well as participate in joint actions in conferences or organizing its own activities that are directly connected to XLAB's commercial interests. XLAB will also pitch the result to existing partners. XLAB has positioned itself also as a proven solution integrator, thus being in a good position to propose and integrate the

	development and run-time management aspects into a commercial third-party system.
FN	Although not directly involved in the development of specific Key Exploitable Results (KERs) or Exploitable Results (ERs), FN will strategically exploit the knowledge, networks, and experience gained through its active participation in Work Packages 6 and 8 of the TANGO project. Through its contributions to WP6, FN deepened its expertise in user interface and user experience (UI/UX) design within complex, secure data-sharing environments—an area that now enriches FN's service portfolio and positions the company to support future projects requiring human-centric digital platforms. Simultaneously, FN's involvement in WP8 (Exploitation) allowed it to gain first-hand experience in innovation management, market analysis, and exploitation planning in the context of EU-funded research. These activities have expanded FN's operational capabilities in the EU innovation landscape and enhanced its understanding of how to collaboratively build and structure exploitation strategies. Most importantly, FN will leverage the strong relationships built within the TANGO consortium to pursue follow-up Horizon Europe project opportunities, identifying synergies for new joint proposals and reinforcing its position as a valuable partner for future cross-sector collaborations.
ANYS	Although ANYS was not directly associated with an ER/KER, it is expected to contribute to exploitation through its role in ICT system integration. ANYS may apply the trust and security mechanisms developed in TANGO to upgrade its data-sharing infrastructure, especially in IoT and smart city domains. As with other technology providers, ANYS may also explore commercial licensing, integration services, or collaborations in future EU projects.
CEA	CEA's goal is to transfer its technology to the industry. CEA will exploit TANGO results by applying them to various ciphers, including post-quantum cryptography, and will continue to disseminate the results, in order to support the necessary transition to post-quantum algorithms. CEA will propose expertise to adapt and customize the countermeasures to the industrial's need and constraints, using countermeasure combination if necessary, and code polymorphism where deemed useful. The expertise of CEA, on both masking and hiding, that TANGO results strengthen, will help innovate to solve industrial's issues with minimal impact on performance.
FHG	FHG, which leads ER2c, plans to exploit its results through further research initiatives and potential spin-off development. FHG will continue to use the research for internal knowledge growth and publication while transferring applicable technologies to industry through licensing or R&D partnerships. FHG may also incorporate the solutions into teaching and student-led prototyping, reinforcing its role as a bridge between research and industry.
VTT	VTT, as the lead for ER6a, will exploit the result by furthering its research into secure digital identities and data sovereignty. VTT's exploitation pathway includes incorporating project outcomes into its institutional R&D agenda, engaging with stakeholders across Finnish and European ecosystems, and pursuing additional

	Horizon Europe funding. Use cases from TANGO will be used to attract industry collaborations and inform national digital transformation strategies.
DUT	Delft University of Technology (DUT), as a leading public university in the Netherlands, will continue to play a pioneering role in advanced research on encryption techniques. While the outcomes of TANGO project from DUT are not intended for direct commercial use - given TU Delft's non-commercial nature - the software toolkit developed within the TANGO project lays a strong foundation for future research, particularly in areas such as efficiency optimization and security enhancement of distributed multi-party encryption technique. Furthermore, TU Delft's vital role in education ensures that the TANGO project outcomes will serve as a valuable prototype for coursework at both the bachelor's and master's levels.
UMU	The University of Murcia, as a public institution without a primary focus on direct commercial gain, will leverage the TANGO project's technological components by embedding them into existing research lines, ongoing funded projects, and promoting open-access dissemination of designs and source code via institutional repositories. Additionally, UMU is exploring technology transfer of dataspace–related results by focusing on the use of the connector and identity wallet for developments in sectors such as oceanography and food, providing specialized training in these areas, and integrating these technologies into bachelor's and master's curricula to foster broader adoption and capacity building.
KU Leuven	Teaching New HE projects
UTH	UTH delivers an open-source, research-grade continuous behavioural authentication framework that (a) roots Android devices to collect system logs and RSSI data, (b) processes logs through a BERT-based ML Risk Assessment Engine for real-time anomaly detection, and (c) integrates localization to support secure smart-manufacturing access control. UTH will exploit the produced results by focusing on knowledge sharing—through publications, GitHub, and workshops—we empower academic and non-commercial stakeholders to adopt, adapt, and extend state-of-the-art continuous device authentication without commercial barriers.
UPRC	While UPRC did not lead a specific ER/KER, as a university and RTO it will exploit the results of TANGO primarily through academic dissemination, integration into teaching materials, and follow-up research proposals. UPRC may use TANGO's insights to launch new MSc and PhD topics, publish technical papers, and support spin-off initiatives from its AI and data privacy labs.
IDSA	As a data-sharing association, IDSA will exploit TANGO by promoting its outputs through its network of members and integrating best practices into future data space architecture guidelines. IDSA may also use TANGO outcomes to influence standardization activities and European policy, ensuring that trustworthy and explainable AI systems become part of data-sharing frameworks across the EU.

EGI	EGI did not lead a specific ER/KER, but will disseminate the results of TANGO to its Federation members and the broader EGI community. Additionally, EGI could consider referencing TANGO outcomes in future project proposals where relevant. EGI might aim to bring insights from TANGO into ongoing or future technical discussions related to data governance models and policy frameworks, where appropriate. Ultimately, EGI could integrate TANGO's results (Policy Enforcement Points and Sticky Policies from the Confidentiality and Privacy by Design KER) into test environments to validate best practice solutions within the EGI Community to improve service security.
ECO	ECO, as a think tank and policy intermediary, will exploit TANGO's results by disseminating them to national and EU-level regulators and industry groups. It will aim to inform upcoming digital policy, especially in relation to AI regulation, ethical data use, and consent management. ECO may also promote the results through white papers and stakeholder engagement activities.
LIC	LIC is expected to use TANGO's findings to support consumer protection and data rights advocacy. While not directly involved in ER/KER development, LIC can disseminate project outcomes to citizens and policymakers, highlight best practices in privacy assurance, and contribute to consultations and roundtables on ethical data sharing and trustworthy AI systems.
IDIADA	IDIADA will likely exploit the TANGO outcomes in the context of mobility and connected vehicles. Although not linked to a specific result, it can leverage the privacy and trust-enhancing technologies for automotive cybersecurity solutions, particularly in ensuring GDPR and AI Act compliance in vehicular data systems. Potential exploitation includes licensing, pilot deployment, and co-development with automotive OEMs.
ABI	As an industrial association, ABI will focus on disseminating the results of TANGO to its members and using them to inform policy and innovation agendas. While it has no direct ER/KER, ABI is well-positioned to drive technology transfer and help shape sectoral strategies for adopting trustworthy AI and secure data sharing.
RIAS	RIAS, despite not being directly linked to a result, can incorporate TANGO's findings into its ICT infrastructure operations, particularly in high-performance computing or digital twin environments. It may explore integrating TANGO mechanisms into research infrastructures or offering training and adoption support to regional innovation ecosystems.
FMAKE	FMAKE, a policy and industry forum, is likely to exploit TANGO's outcomes through the promotion of ethical AI practices and secure data-sharing frameworks. It will support member organizations in aligning with European digital policies and participate in working groups for AI governance and data ethics.
CESGA	As an HPC and data analytics provider, CESGA will likely apply TANGO's technical outputs to enhance the security, transparency, and regulatory compliance of its cloud and computing offerings. It may also contribute to exploitation through training services and support to regional SMEs.
AHOP	AHOP will use TANGO outputs to promote cross-border collaboration in AI policy and privacy standardization. While not linked to a specific ER, it may focus on

	awareness campaigns, multi-stakeholder engagement, and advisory roles for public sector organizations interested in deploying privacy-preserving technologies.
VISA	VISA, though not a technology developer in the project, may support the replication and standardization of trustworthy AI solutions in European public administration. It can help ensure that TANGO results influence regional governance structures for digital services, particularly in areas of procurement, interoperability, and privacy.
MET	MET may explore integrating trustworthy AI features from TANGO into their operational systems for smart metering, logistics, or energy management. While not a result leader, MET could leverage TANGO to enhance compliance and citizen trust in AI-driven services and pursue public-private partnerships around these areas.
UOM	The University of Manchester (UOM), through its work on ER13, will exploit its result by embedding TornadoVM into research, education, and commercial offerings. UOM aims to launch a spin-off, apply for additional Horizon Europe funding, and leverage ER13 in AI curriculum development. It also plans to develop enterprise-ready editions of the tool under an open-core model.
UOG	The University of Greenwich (UOG), responsible for KER14a, plans to exploit the result through a dual path of academic research and industrial collaboration. UOG will refine its privacy threat modelling tool for broader adoption and seek further research funding. It may also participate in consortia focused on trustworthy AI frameworks and ethical design.
NTT	NTT, while not leading an ER/KER, is expected to integrate trusted AI elements developed in TANGO into its international R&D pipeline. As a global ICT company, NTT may use TANGO technologies to reinforce its offerings in data compliance and security, especially for clients in finance and smart cities.
ACV	ACV's exploitation is likely to focus on leveraging TANGO results to support regulatory compliance and data protection in their operational or policy activities. While not leading a result, ACV can act as a conduit between project innovations and policy/industry stakeholders, facilitating adoption through national strategies or guidance documents.

Annex G - TANGO Stakeholder Mapping per Target Market

Introduction

As part of Task 8.3 (Business and Sustainability Planning) of the TANGO project, this document provides a structured stakeholder mapping across TANGO's six targeted markets. The mapping utilises the Business Model Canvases prepared for the project's Key Exploitable Results, and incorporates stakeholder insights gathered through co-creation and innovation workshops, including the Final General Assembly workshop held in Mallorca (May 2025).

TANGO's platform, consisting of modular privacy-preserving data sharing, identity verification, and analytics tools, supports a wide range of stakeholders with sector-specific needs. These stakeholders were identified through engagement with pilot partners, exploitation template responses, desk research, and validation workshops.

Stakeholders per Target Market

1. Smart Hospitality

Stakeholders encompass organisations responsible for guest-facing services, environmental monitoring, and privacy compliance.

- Hospitality Managers & IT Directors (e.g., hotels, resorts, boutique chains)
- Guests/Travelers (users of onboarding and identity tools)
- Hospitality Technology Vendors (offering PMS, check-in systems)
- Tourism Boards & Destination Management Organisations
- IoT device integrators for environmental sensing and occupancy control
- Energy optimisation service providers leveraging analytics on room usage
- Local authorities are monitoring environmental impact and customer satisfaction

2. Smart Manufacturing

Focuses on secure factory data exchange, digital twins, and energy-efficient AI:

- Factory/Plant Managers (OEMs, Tier-1 suppliers in automotive, aerospace)
- Industrial Automation Vendors (providing MES, access control, robotics)
- Cybersecurity Teams in manufacturing plants
- IT/OT System Integrators
- Regulatory Compliance Auditors
- Energy Management Consultants supporting green AI
- AI/ML Engineers deploying federated learning at the edge

3. Retail Sector

Data-driven retail operations, behavioural authentication, and privacy-aware marketing:

- Retail Chain Managers & Store Operations Executives
- Retail Analytics Providers
- Customer Experience Designers
- IT Teams implementing privacy-preserving analytics

- Digital Loyalty Platform Operators
- Regulators on consumer data use and consent
- In-store IoT Solution Providers

4. Banking Sector

Secure and compliant customer onboarding, AI-based transaction monitoring:

- Bank Compliance Officers (focused on PSD2, GDPR, KYC)
- Digital Identity Managers
- Fraud Prevention Experts
- RegTech Vendors implementing eIDAS-compliant onboarding
- FinTech companies adopting SSI and decentralised data flows
- Open Banking Platform Providers

5. Public Authorities

Enabling secure cross-border services and citizen-centric data governance:

- National and Local Government Agencies (municipal platforms, registries)
- Public IT Providers managing digital ID, citizen onboarding, and service portals
- Regulators and Data Protection Authorities
- Smart City Platform Managers
- Cloud and Edge Infrastructure Operators
- EU Digital Identity Wallet stakeholders (aligned with eIDAS 2.0)

6. IoT & Autonomous Systems

Critical for mobility and sensor-rich environments:

- Autonomous Vehicle Manufacturers and Fleet Managers
- Mobility Service Providers
- Edge AI Engineers working on real-time analytics
- Trust Framework Developers
- IoT Platform Operators
- Security Auditors for Cyber-Physical Systems
- Insurance Providers using trust scores in vehicle-sharing contexts

The stakeholder identification aligns directly with the TANGO platform's modular, cross-sector deployment strategy. These categories will be used in follow-up stakeholder engagement activities, targeted communication, and exploitation paths. Importantly, this mapping supports the platform's post-project go-to-market strategy, anchoring it in high-growth, compliance-driven domains with strong demand for privacy-preserving digital transformation.