

D6.3

Communication Strategic Plan (CSP), Dissemination Exploitation Plan (DEP) and synergies results.

Lead Author: Francesco Ghini
With contributions from: AVO, CEA, GRAD
Reviewer: CHU, TIME.LEX, CEA

Deliverable nature	Report
Dissemination level	Public
Delivery date	02-02-2026
Version	Final
Total number of pages	61
Keywords	Dissemination plan, communication plan, exploitation

EXECUTIVE SUMMARY

This deliverable presents a comprehensive overview of the Communication, Dissemination, and Exploitation (CDE) activities carried out within the TRUMPET project throughout its implementation. It consolidates the strategic approach, execution, and outcomes of the project's communication and dissemination efforts, highlighting how these activities supported scientific excellence, stakeholder engagement, and alignment with European policy priorities in the fields of trustworthy artificial intelligence, cybersecurity, and healthcare data governance.

TRUMPET implemented a **multi-layered communication and dissemination strategy** targeting a broad range of audiences, including the scientific community, healthcare professionals, industry stakeholders, policymakers, media, and the general public. Activities were designed to ensure both depth of technical dissemination and accessibility for non-specialist audiences. Particular emphasis was placed on **translating complex research results on federated learning and privacy-enhancing technologies into clear, policy- and practice-relevant messages**.

Scientific dissemination constituted a core pillar of the strategy, with peer-reviewed publications in high-quality international journals and conferences addressing key challenges in federated learning, homomorphic encryption, privacy preservation, and secure AI. These outputs contributed to advancing the state of the art while reinforcing TRUMPET's visibility within the European and international research landscape. In parallel, non-scientific publications, white papers, and policy-oriented reports further extended the reach of project results beyond academia.

The project placed strong emphasis on **high-level events and interactive formats** as vehicles for engagement and knowledge exchange. TRUMPET organised and co-led scientific conferences, thematic workshops, CrossTalk events within European clusters, and dedicated webinars (TRUMPET Exchange Talks), creating platforms for dialogue among researchers, clinicians, industry representatives, and institutional stakeholders. Flagship events such as Healthcare Claims Future, the European AI & Cybersecurity Network CrossTalks, and the Final Event at HealthTech Forward exemplified TRUMPET's role as a convenor within the European AI and digital health ecosystem.

Educational and societal outreach activities further strengthened the project's impact, notably through hackathons, summer schools, and gender-focused initiatives aimed at students and early-career professionals. These actions supported capacity building, STEM engagement, and inclusiveness, in line with Horizon Europe priorities.

Finally, TRUMPET actively **pursued synergies with other EU-funded initiatives** and policy frameworks, including the European Health Data Space, the European Beating Cancer Plan, and EU standardisation actions. Through cluster participation, joint publications, and policy dialogue, the project contributed to long-term sustainability and exploitation pathways for its results.

DOCUMENT INFORMATION

Grant agreement No.	101070038	Acronym	TRUMPET
Full title	TRUStworthy Multi-site Privacy Enhancing Technologies		
Call	HORIZON-CL3-2021-CS-01-04		
Project URL	https://cordis.europa.eu/project/id/101070038		
EU project officer	Ioannis ASKOXYLAKIS		

Deliverable	6.3	D6.3	Title	CSP, DEP and synergies results.
Work package	Number	WP6	Title	Collaboration, communication, dissemination and exploitation
Task	Number	T6.2	Title	Develop a communication strategy plan

Date of delivery	Contractual	M39	Actual	M39
Status	version 0. 3 <input checked="" type="checkbox"/> Final version			
Nature	<input checked="" type="checkbox"/> R <input type="checkbox"/> DEM <input type="checkbox"/> DMP <input type="checkbox"/> DEC <input type="checkbox"/> ETHICS <input type="checkbox"/> OTHER			
Dissemination level	<input checked="" type="checkbox"/> Public <input type="checkbox"/> Sensitive			

Authors (partners)	IRST, GRADIANT, CEA, AVO
Responsible author	FRANCESCO GHINI Francesco.ghini@irst.emr.it

Summary (for dissemination)	This plan provides a report about communication activities and updated version of Communication, dissemination and exploitation plan
Keywords	Dissemination plan, communication plan, exploitation

VERSION LONG			
Issue Date	Rev. No.	Author	Change
25/11/2025	0.0	Francesco Ghini	Table of Content
12/12/2025	0.1	Francesco Ghini, Zeev Pritzek, Nuria Barros Reguera, Augustin Lemesle, Zakaria Chihani	1st Draft
19/01/2026	0.2	Francesco Ghini, Zeev Pritzek, Nuria Barros Reguera	Draft revision
30/01/2026	0.3	Francesco Ghini, Nuria Barros Reguera	Final version

TABLE OF CONTENTS

1	Introduction.....	8
1.1	Purpose of the deliverable	8
1.2	Relation to previous CSP/DEP deliverables (D6.1 & D6.2).....	8
2	Summary of the Communication Strategic Plan (CSP)	10
2.1	CSP objectives and expected results	10
2.2	Implementation progress at project end.....	10
2.3	Deviations and changes from the initial plan.....	12
2.4	Lessons learned and best practices	12
3	Communication results	14
3.1	Digital communication outcomes	14
3.2	Offline communication achievements	18
3.3	Media relations and publications	21
4	Summary of the Dissemination & Exploitation Plan (DEP).....	23
4.1	Dissemination pathways.....	23
4.2	Exploitation pathways.....	24
5	Dissemination Results	25
5.1	Focus on scientific conferences, events and publications.....	25
5.2	Events organised by TRUMPET	27
5.3	Educational initiatives and GAP-related activities	30
6	Exploitation Results	33
6.1	KERs developed by the consortium.....	33
6.2	TRUMPET Platform Business Plan and PETRAI project	35
6.3	Standardisation Advice.....	39
6.4	Impact Assessment of TRUMPET solutions	41
7	Synergies with European Projects and Initiatives	45
8	Conclusion and recommendations.....	46
9	Annexes	47
	Annex 1. IPR Table.....	47
	Annex 2. List of KERs	53

LIST OF FIGURES

Figure 1 Example of Social media post.....	16
Figure 2 Youtube repository.....	17
Figure 3 Printed badge for event	18
Figure 4 Policy Brief	20
Figure 5 White paper covers.....	27
Figure 6 Social Media post on Trumpet Exchange talks.....	28
Figure 7 - Agenda of the HealthTech Forward meeting.....	30
Figure 8 Social media post on Summer School.....	31
Figure 9 Tech talks by Gradient	32
Figure 10 PETRAI Seal of Excellence	36
Figure 11 Federated Learning market stats	37
Figure 12 PETRAI business concept.....	38
Figure 13 Competitive advantage of TRUMPET technologies in PETRAI.....	39
Figure 14 Summary of the meetings with the HS Booster expert	40

LIST OF TABLES

Table 1 Communication concept.....	10
Table 2 Number of activities	11
Table 3 Target audience	12
Table 4 KPI on communications	14
Table 5 List of Press release.....	21
Table 6 KPIs on dissemination activities	24
Table 7 Event list.....	25
Table 8 List of publications.....	26
Table 9 List of Trumpet Exchange talks	28
Table 10 TRUMPET Key Exploitable Results.....	33
Table 11 Exploitation Pathways for identified KERs.....	35
Table 12 Trumpet KERs – Impact classification.....	41

ABBREVIATIONS AND ACRONYMS

- ICT:** Information and Communication Technologies
- PR:** Public relations
- SME:** Small medium enterprises
- GDPR:** General Data Protection Regulation
- EU:** European Union
- STEM:** Science, Technology, Engineering and Mathematics
- GAP:** Gender Action Plan
- ENISA:** European Union Agency for Cybersecurity
- ECCC:** European Cybersecurity Competence Centre
- ECSSO:** European Cyber Security Organisation
- HIMSS:** Healthcare Information, Management Systems Society
- ISACA:** Information Systems Audit and Control Association
- IAPP:** International Association Of Privacy Professionals
- ICT:** Information and Communication Technologies
- SoA:** Strategy of Action
- CSP:** Communication Strategic Plan
- DEP:** Dissemination and Exploitation Plan
- KER:** Key exploitable Results

1 Introduction

The TRUMPET project, funded under the Horizon Europe programme (Grant Agreement No. 101070038), has aimed to advance trustworthy and privacy-preserving federated learning solutions for healthcare applications. **Work Package 6 (WP6) — Collaboration, communication, dissemination and exploitation**, has played a central role in enhancing project visibility, fostering stakeholder engagement, and ensuring that TRUMPET outputs reach scientific, industrial, policy, and public audiences.

As the project reaches its final stage, this deliverable consolidates the final results of the Communication Strategic Plan (CSP), the Dissemination and Exploitation Plan (DEP), and the synergies established with other EU initiatives. It provides a comprehensive overview of the activities implemented, their impact, and the lessons learned during the project lifecycle.

1.1 Purpose of the deliverable

This deliverable provides the final and comprehensive overview of all communication, dissemination, and synergy-building activities undertaken throughout the TRUMPET project. Its purpose is to consolidate the work performed under the Communication Strategic Plan (CSP) and the Dissemination and Exploitation Plan (DEP), offering a complete account of their implementation and impact. The deliverable aims to ensure transparency regarding the methods, tools, and strategies adopted to maximise TRUMPET's visibility and outreach. It gathers evidence from the TRUMPET communication registry, the project website, digital channels, scientific publications, public-facing activities, media relations, and synergy actions with other Horizon Europe projects. In doing so, it highlights how TRUMPET's results have been disseminated to targeted audiences including the scientific community, policymakers, healthcare professionals, industry stakeholders, and the general public. Furthermore, the document serves as a reference for future initiatives wishing to replicate or build upon TRUMPET's approach to communication and dissemination, reflecting on lessons learned and best practices adopted by the consortium. Finally, this deliverable ensures that the project's work is properly documented, traceable, and communicated in a structured manner to the European Commission, project partners, and external stakeholders, marking the formal closure of CSP and DEP activities within TRUMPET.

1.2 Relation to previous CSP/DEP deliverables (D6.1 & D6.2)

This deliverable builds directly on two preceding documents:

- **D6.1 (Initial CSP, DEP and Synergies Establishment)** established the communication foundations of the project. It defined the communication baseline, the project's values and messaging, the identified target groups, and the tools to be employed. D6.1 set the strategic direction for the consortium, guiding how the project would inform and engage stakeholders, maintain a coherent identity, and ensure compliance with visual and communication guidelines.
- **D6.2 (Updated CSP, DEP and Synergies Establishment)** provided a mid-term assessment of progress, detailing the KPIs achieved during the first 18 months, including website metrics, social media engagement, event participation, publications, and the first synergy activities.

This final deliverable continues this trajectory by presenting the **completed implementation of the CSP and DEP**, offering a comprehensive overview of all activities carried out during the project and

assessing their impact. It transitions from planning and mid-term evaluation to full reporting, closing the sequence of WP6 deliverables.

2 Summary of the Communication Strategic Plan (CSP)

2.1 CSP objectives and expected results

The Communication Strategic Plan (CSP), initially defined in D6.1, set the foundation for how TRUMPET intended to communicate its mission, methodology, and results to a variety of audiences. The CSP identified the dual objective of informing and engaging (Table 1), recognising that federated learning and privacy technologies are complex topics that require clear, accessible communication to both specialised and non-specialised communities.

Informing	Making scientific and technical concepts accessible, especially regarding federated learning, privacy preservation, and cybersecurity in healthcare.
Engaging	Creating opportunities for interaction with diverse audiences, including researchers, healthcare professionals, policymakers, industry stakeholders, and the general public.

Table 1 Communication concept

One of the central objectives was to ensure that the consortium presented **a unified, recognisable, and trustworthy identity**. This included the development of the **TRUMPET logo, brand manual, colour palette, and communication guidelines**. These elements were crucial to establishing a visual coherence across **events, press releases, website materials, and social media interactions**. As described in D6.1, a considerable effort was dedicated to translating technical concepts, such as secure aggregation, multi-site privacy-enhancing technologies, and decentralized machine learning, into messages that different audiences could understand and relate to.

Another expected result of the CSP was to create a set of communication tools and channels that would accompany the entire project lifecycle. The website, social media channels (primarily LinkedIn), newsletters, offline materials, video interviews, and press releases formed a comprehensive ecosystem that supported continuous dissemination of updates.

2.2 Implementation progress at project end

The CSP was implemented extensively and consistently throughout the project. The consortium maintained an active digital presence through the website, LinkedIn channel, and newsletters while also producing a series of press releases and offline communication materials. Partners frequently participated in conferences, workshops, and public events, contributing to strong outreach performance across Europe.

Throughout the entire duration of the project, the implementation of the Communication and Dissemination Plans (CSP and DEP) has been carried out systematically and consistently across partners. The communication and dissemination activities accelerated over time, with a significant increase in outputs from M12 onward, reflecting both the project’s scientific maturity and its ability to generate concrete, shareable results.

Overall, by the end of the project, the consortium recorded **more than 240 documented communication and dissemination actions (Table 2)**, spanning scientific, technical, policy-oriented, and public-facing channels. Some activities targeted multiple audiences and formats; counting was performed per activity, not per audience occurrence. The activities covered a broad

range of formats, including peer-reviewed publications, conference presentations, workshops, educational events, press releases, website articles, and highly active social media communication, ensuring that TRUMPET reached diverse audiences such as researchers, clinicians, regulators, industry, citizens, and specialised communities in cybersecurity and federated learning.

Communication actions represented a very large share of the project effort, supporting awareness, visibility, and engagement with non-scientific audiences. In particular, TRUMPET implemented:

- Social media posts
- Website articles and blogposts
- Press releases
- Event participation addressed to the general public
- Videos and communication clips
- Flyers and brochures
- Organisation of public-facing events

Dissemination actions targeted the scientific and expert communities. TRUMPET demonstrated exceptional research productivity and high-level dissemination, delivering:

- Peer-reviewed scientific publications
- Presentations at international conferences
- Workshops organised by TRUMPET
- Participation in scientific events and seminars
- Joint cluster sessions
- Policy-oriented presentations
- Educational webinars (TRUMPET Exchange Talks)

Total Activities delivered	240
Communication activities	110
Dissemination activities	130

Table 2 Number of activities

Target audiences reached

TRUMPET’s communication and dissemination activities addressed a wide range of target audiences, with a strong emphasis on public awareness and scientific dissemination (Table 3). The **General Public** represented the main audience, reflecting the project’s commitment to making complex AI and federated learning concepts accessible beyond specialist communities. The **Scientific Community** was also a key target, with different activities dedicated to conferences, workshops, publications, and technical exchanges. Targeted actions towards **Policy Makers** and **Media** supported policy alignment and broader visibility, while engagement with **Industry and Investors** focused on innovation and exploitation perspectives. More limited, use-case-specific outreach was directed at Customers. The ‘Other’ category includes internal coordination actions, cluster-level activities, and cross-cutting initiatives not attributable to a single audience. Overall, the distribution confirms a balanced strategy combining broad societal outreach with strong scientific and policy engagement.

Audience category	Number of activities
Scientific community	52
Industry	4
General Public	115
Policy Makers	9
Media	10
Investors	4
Customers	1
Other	45

Table 3 Target audience

2.3 Deviations and changes from the initial plan

During the implementation of the Communication Strategic Plan, a small number of adjustments were required to optimise resources and ensure that communication efforts remained aligned with the needs of the project and its audiences. Although these deviations did not alter the core objectives of the CSP, they improved the efficiency and quality of communication activities.

A first important change concerned the use of Facebook as a communication channel. As originally described in D6.1, the consortium intended to maintain a presence on Facebook to reach the general public. However, early monitoring of engagement levels demonstrated that Facebook was not an effective platform for TRUMPET’s type of content. Interactions were extremely limited and did not justify the effort needed to maintain the channel. More importantly, TRUMPET’s audience, primarily researchers, digital health professionals, and policymakers, proved far more active on LinkedIn. For this reason, and with full agreement of the partners, the consortium decided to discontinue Facebook and to concentrate social media communication exclusively on LinkedIn, where results showed a significantly higher engagement rate.

A second deviation concerned the newsletter implementation. Although the newsletter was successfully launched and maintained from 2023 onwards, its execution required more effort than anticipated. Shortly after activation, the project experienced a high influx of fake or automated email subscriptions, which forced the communication team to dedicate substantial time to manually identify and remove invalid accounts. This cleaning process was necessary to protect the integrity of the mailing list and avoid distorting analytics, but it delayed the setup of a stable subscriber base. Furthermore, the newsletter subscriber count remained below initial expectations, which is consistent with the nature of TRUMPET’s newsletter. Unlike marketing-oriented newsletters, TRUMPET’s newsletter served a strictly informational purpose, providing updates on scientific progress, events, publications, and project milestones. Such content, while highly relevant to specialists and project collaborators, is less attractive for broader audiences who may prefer more practical or end-user-oriented information. As a result, subscriptions tended to grow slowly despite good open and click rates among existing subscribers.

2.4 Lessons learned and best practices

Over the course of the project, TRUMPET generated an extensive body of experience on how to communicate highly technical content to a wide spectrum of audiences. One key lesson that emerged is that **clarity, contextualisation, and storytelling are essential when translating scientific complexity into accessible communication.** Below we detail key lessons learned.

Use concrete healthcare use case to communicate technical things

Federated learning and cryptographic methods are concepts that can be difficult for the general public, healthcare professionals, or policymakers to interpret. The project learned that communication becomes substantially more effective when **technical explanations are framed through concrete healthcare use cases**, real-world challenges, and practical benefits for society. This approach proved particularly successful in website articles, videos, and social media posts, where content oriented toward “why this matters for patients, hospitals and data governance” consistently achieved stronger engagement than content purely focused on methodology.

Multimodal formats are the best choice, ever

Another important lesson concerns the use of multimodal formats. TRUMPET demonstrated that **videos, visual narratives, and interactive sessions significantly outperform text-only materials when dealing with complex technical topics**. The steady production of short explanatory clips, interviews with researchers, and visual explainers was instrumental in maintaining high engagement levels across the project’s communication channels. These formats also served as a bridge between experts and non-expert audiences, reducing the perceived barrier to understanding AI and cybersecurity concepts.

Always involve young communities

A major milestone in the project's communication and educational strategy was the **AI-DEA Hackathon and its related activities**, documented extensively in previous dissemination deliverables. The Hackathon was one of the most successful outreach and educational initiatives of TRUMPET. It not only showcased the project’s technological foundations but transformed them into a concrete, creative challenge for high-school students. The enthusiastic participation of 100 young learners, organised in mixed-gender teams, demonstrated that even sophisticated AI and privacy concepts can be made accessible and engaging for younger audiences when framed through practical challenges and collaborative learning.

This specific experience provided two additional key lessons:

- Technical outreach to young people is most effective when hands-on. Young participants better assimilate complex concepts when they can experiment, ideate, and interact with real researchers rather than merely receiving theoretical instruction.
- STEM promotion must integrate inclusiveness at every step. Mixed-gender teams, dedicated mentoring, and equitable visibility were crucial in making the Hackathon not just a competitive event, but an educational platform that empowered students with different backgrounds and interests.

Promote a never ending relation between technical and communication teams

Finally, another best practice was the importance of continuous alignment between technical teams and communication teams. The project discovered that early involvement of technical experts in drafting communication materials and vice versa, communication officers attending scientific discussions, produced more accurate, coherent, and impactful content. This collaborative workflow ensured that messages were both scientifically rigorous and adapted to the communication strategy’s audience segmentation.

3 Communication results

The communication activities implemented throughout TRUMPET were designed to maximise visibility, promote public understanding of privacy-preserving AI, and support engagement with key stakeholders across digital health, cybersecurity, research, and public policy. This chapter summarises the results achieved across digital channels, offline communication, and media outreach, following the strategic framework defined in the Communication Strategic Plan (CSP) and updated in previous deliverables (Table 4).

KPI (Merged Area + Indicator)	M36 Target	M18 Achieved	M39
Website – Unique visitors / page views	2,500	3,854	6,570
Website – Average visit duration	≥2 min	2 min 32 sec	2 min
Website – Actions per visit	>2	2.5	2.0
Website – Downloads	≥200	189	505
Website – News published	18+	12	24
Newsletter – Number of newsletters issued	12	3	9
Newsletter – Subscribers	≥120	62	73
Newsletter – Open rate	≥50%	48–80%	≥50%
Newsletter – Click rate	≥10%	8–16%	17%
LinkedIn – Followers	250	203	376
LinkedIn – Posts	60+	54	108
LinkedIn – Impressions	15,000+	15,686	22,554 (Year 3)
YouTube – Videos published	≥5	5+	16
YouTube – Engagement (views & watch time)	Continuous increase	199 views / 5.1h	423
Press & Media – Press releases	9	5	10

Table 4 KPI on communications

3.1 Digital communication outcomes

Digital channels remained the core engine of TRUMPET’s communication strategy, ensuring continuous visibility and timely stakeholder engagement.

Website

The TRUMPET website functioned as the project's central public interface. Across the project lifecycle, partners published 24 articles covering scientific advances, policy developments, project milestones, technical explainers, and consortium updates.

The website played a key role in:

- Highlighting TRUMPET's progress and results
- Highlighting members contribution and EU support
- Providing accessible explanations of complex topics (PETs, federated learning, GDPR, AI Act)
- Communicating events, workshops, and review meetings
- Offering updates from cluster initiatives and synergies

As the project progressed toward its final phase, website content increasingly focused on demonstrators, results achieved, and the policy relevance of TRUMPET's work.

Social Media

LinkedIn was the primary social media channel and proved extremely effective in amplifying project visibility. TRUMPET partners posted more than 100 updates (almost 1 post/week), reflecting a highly active communication environment (Figure 1).

The content mix strategically covered:

- Project milestones and achievements
- Invitations and reports from conferences, workshops, and webinars
- Policy briefs
- Publications and white papers
- Insights on regulations and policy discussions (AI Act, GDPR, EHDS)
- Technical explainers authored by project researchers
- Announcements of cross-project synergies and cluster activities
- Visibility at major European events

The high posting frequency and collaborative engagement from multiple partners strengthened TRUMPET's reputation as a reference point in trustworthy AI and federated learning.



Figure 1 Example of Social media post

Newsletter

A periodic project newsletter was launched to provide curated updates for stakeholders. While the tool was functional, its implementation raised two important operational lessons:

1. Management of fake or automated subscriptions

The subscription system attracted a significant number of non-authentic or bot-generated email addresses. Safeguarding GDPR compliance required a manual verification and cleanup of these entries, which proved time-consuming.

2. Limited audience growth due to niche content

Newsletter subscriptions remained lower than originally forecast, mainly because the content focused on highly technical project updates. This confirmed that newsletters in research projects perform better when their scope extends beyond internal milestones to broader trends and cross-project synergies.

Despite these challenges, the newsletter remained a useful dissemination tool for engaged stakeholders in research, legal, and policy communities.

Video Communication

Video production significantly enhanced TRUMPET's communication impact. The consortium generated a wide range of videos, including:

- Researcher interviews
- Project explainers
- Event highlights
- Exchange Talk recordings
- Short social media videos promoting project activities

These formats were crucial for simplifying complex topics such as homomorphic encryption, SMPC, privacy risks in federated learning, and trustworthy AI methodologies (Figure 2). All videos have been uploaded on the [Youtube channel](#)

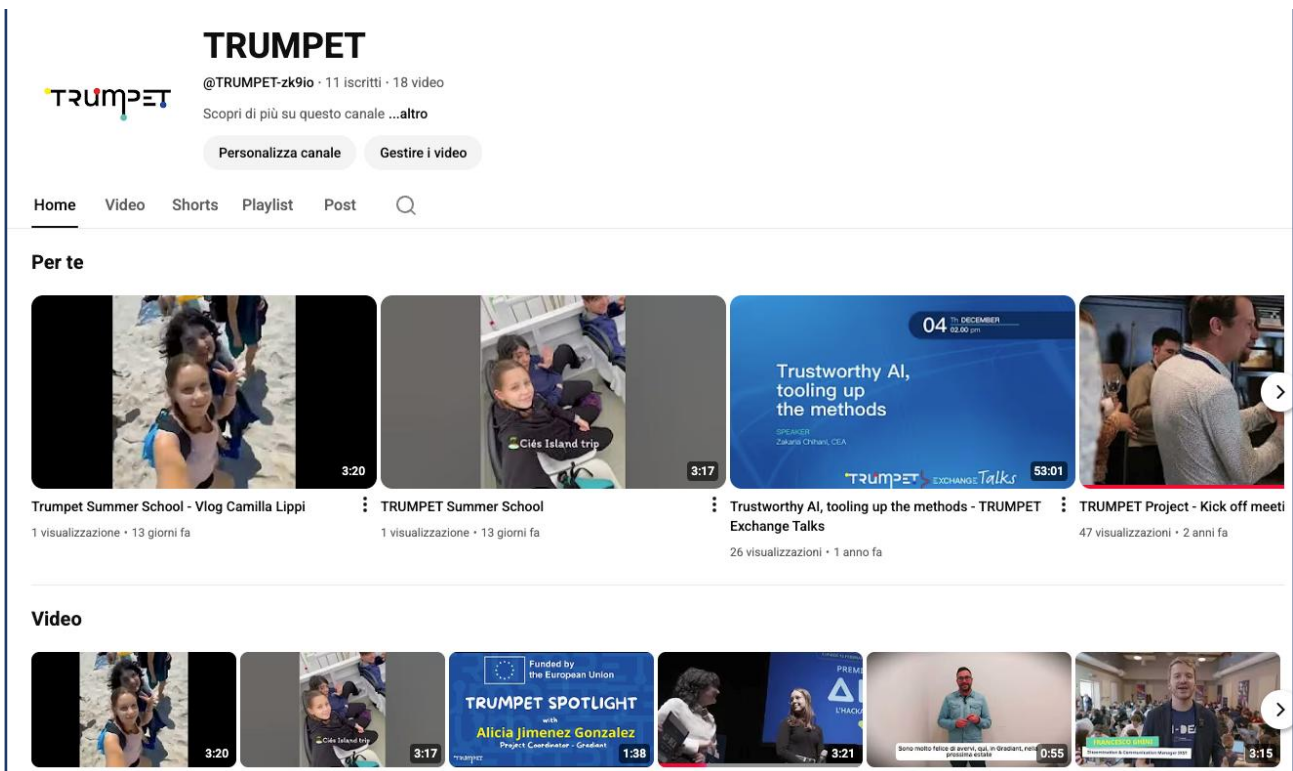


Figure 2 Youtube repository

3.2 Offline communication achievements

While TRUMPET achieved strong visibility through digital tools, offline communication activities were equally important in strengthening the project’s presence at physical events, conferences, and high-level policy discussions. These activities ensured that TRUMPET’s scientific, technical, and regulatory messages were conveyed through tangible materials designed for stakeholder engagement, particularly during strategic events such as HIMSS Europe.

Leaflets and Printed Materials

Throughout the project, TRUMPET produced several printed communication items that supported in-person dissemination and stakeholder engagement (Figure 3). These included:

- Project leaflets summarising objectives, use cases, consortium composition, and expected outcomes
- Event-specific flyers, such as the one produced in 2024 to promote collaboration opportunities with TRUMPET
- Posters used during conferences, workshops, and consortium meetings to visually present the project’s architecture, federated learning workflow, and privacy-enhancing technologies

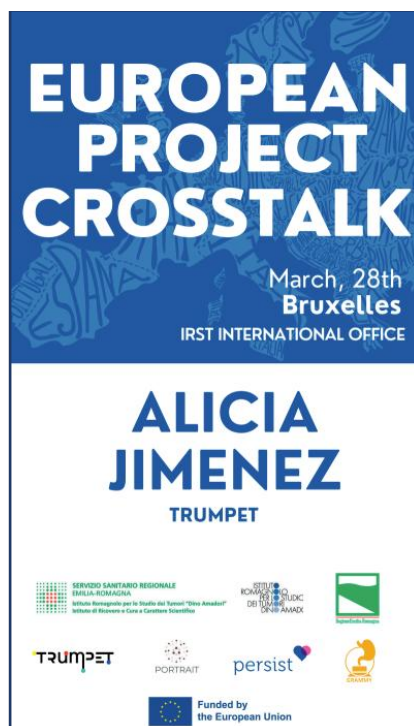


Figure 3 Printed badge for event

These materials served as essential tools for engaging stakeholders during physical events by providing an accessible and condensed overview of the project. Printed communication proved particularly valuable in settings where attendees had limited time to explore digital content or required takeaway materials to share with colleagues.

Policy Brief

One of TRUMPET's most significant offline communication assets was the **Policy Brief on Federated Learning, Privacy, and Regulatory Challenges**, developed to support engagement with policymakers, regulators, and digital health authorities. This document was disseminated during high-level events, including HIMSS Europe, where TRUMPET contributed to discussions on health data governance, EHDS implementation, cybersecurity, and trustworthy AI.

The Policy Brief (Figure 4) highlights four core regulatory challenges:

- Legal responsibility and accountability (e.g., identifying data controllers/processors in FL networks)
- Data protection and privacy metrics, stressing the need for standardised tools to quantify privacy leakage
- Alignment with GDPR principles, especially regarding data minimisation and privacy-by-design obligations
- Open questions related to secondary data use, regulatory sandboxes, certification, and transparency

It also summarises the project's contributions, including:

- Development of novel theoretical privacy metrics grounded in real-world inference attacks
- Evaluation of complementary PETs tailored for federated learning
- Creation of a regulatory roadmap for FL adoption in biomedical contexts

These elements were crucial in positioning TRUMPET as an authoritative voice in the EU discussion on privacy-preserving AI and health data governance. During the last year of the we either have presented or sent the policy brief to:

- policymakers from DG SANTE and DG CONNECT
- hospital CIOs and digital health leads
- cybersecurity specialists
- industry representatives
- cluster projects and EHDS stakeholders

This form of offline communication significantly amplified the project's influence and strengthened its visibility within strategic decision-making environments.

POLICY BRIEF



Funded by the European Union

Federated Learning, Privacy, and Regulatory Challenges

Federated Learning (FL) represents a promising approach for enabling large-scale biomedical research while preserving data privacy. By allowing models to be trained locally on decentralized data, FL aligns well with data minimisation and confidentiality principles outlined in the General Data Protection Regulation (GDPR). However, despite its advantages, FL introduces complex policy and regulatory challenges that must be addressed to ensure responsible, large-scale adoption—particularly in sensitive domains such as health and biomedical research.



Legal responsibility and accountability

- Who is considered the data controller or processor in a federated learning setup?
- How should liability be distributed when multiple institutions collaborate in an FL environment?
- What contractual or governance mechanisms are required to define roles and ensure compliance?



Data protection and privacy metrics

- Current PETs (Privacy-Enhancing Technologies) offer mitigation, but lack of reliable privacy metrics can lead to blind spots in risk evaluation.
- There is a need for standardized tools and methods to quantify privacy leakage and guide data-sharing decisions in real time.
- While FL helps minimize data sharing by design, incorporating PETs is essential to ensure stronger privacy guarantees during training.



Alignment with GDPR principles

- While FL supports data minimisation and local control, uncertainty remains about the sufficiency of existing PETs in meeting GDPR's expectations around data protection by design and by default.
- Policies must clarify how FL frameworks can demonstrate compliance in a legally defensible way.

OPEN QUESTIONS

1

How can **secondary use of health data** through FL infrastructures comply with GDPR?

2

Can **regulatory sandboxes** or pilot frameworks help test and validate FL technologies under real-world constraints?

3

What mechanisms can be used to **audit or certify FL implementations** for privacy compliance?

4

How can **transparency be ensured** without exposing sensitive architecture or training dynamics?

TRUMPET contribution

- Developed **new theoretical privacy metrics** to assess privacy leakage in FL.
- TRUMPET metrics are **grounded in real-world inference attacks** and aligned with IEEE standards and ENISA recommendations
- Created a **regulatory roadmap** to support broader adoption of FL in biomedical contexts.
- Provided policy-relevant evidence on how **PETs can mitigate risks and support GDPR compliance**.
- Evaluated the practical application of several complementary PETs tailored for Federated Learning.

www.trumpetproject.eu

Figure 4 Policy Brief

3.3 Media relations and publications

Media engagement supported broader public visibility and reinforced the credibility of TRUMPET’s mission.

Press Releases

Multiple partners published [official press releases](#) (Table 5) throughout the project, covering:

- Project launch
- Key achievements and milestones
- Participation in strategic events
- High-level partnerships (e.g., Hop-On expansion to the Turkish Ministry of Health)
- Announcement of final activities and project closure
- These press releases were disseminated across regional, national, and sector-specific media channels.

Date	Title of Press Release
December, 19 2025	TRUMPET project presents final results at Health Tech Forward 2025
July 17, 2025	Forlì–Vigo Round Trip: 4 students from Italy attend the TRUMPET project Summer School
February 11, 2025	Il progetto Therapy-Locker vince l’hackathon AI-DEA di IRST
October 22, 2024	European AI Security network CrossTalk event: leading the future of AI in Healthcare
October 8, 2024	L’intelligenza artificiale al servizio della salute: 100 liceali si sfidano a suon di idee
August 30, 2024	New partnership announcement: Ministry of Health, Republic of Türkiye, joins TRUMPET project through EU Hop On initiative
January 17, 2024	TRUMPET partners organize Special Session on security and privacy challenges in Federated Learning at IH&MMSec’24
April 21, 2023	Investigadores de atlantTic dirixen os avances científicos dun proxecto europeo de loita contra o cancro sen vulnerar a privacidade do paciente
April 7, 2023	Tumori: l’IRST di Meldola guarda all’Europa per portare in Italia modelli innovativi di ricerca e cura per i pazienti
March 25, 2023	La Commission Europeenee finance le project trumpet dans le cadre d’horizon Europe
March 7, 2023	The European Commission finances the TRUMPET project within Horizon Europe framework

Table 5 List of Press release

Popularised articles and public communication

The consortium produced [numerous non-scientific articles](#) aimed at translating complex privacy, cryptography, and AI concepts into accessible language. These articles proved effective in increasing public understanding of:

- How federated learning works
- Why privacy-preserving technologies are needed
- The challenges and opportunities of data governance in healthcare
- The meaning of “trustworthy AI”
- Implications of the European AI Act

Such communication helped demystify advanced technical concepts, which is essential in a field where the public may feel detached from scientific developments.

4 Summary of the Dissemination & Exploitation Plan (DEP)

4.1 Dissemination pathways

Dissemination activities played a central role in ensuring the project’s scientific visibility, fostering dialogue with specialised communities, and positioning the consortium as a key contributor to European research on **federated learning, cybersecurity, and privacy-enhancing technologies**. From the beginning, the consortium adopted a multi-layered dissemination strategy that evolved in line with the technological maturity of the project and the expectations defined in previous deliverables.

A significant outcome of the dissemination work is represented by the high quality of **peer-reviewed publications** produced by the consortium partners. These publications are all open access, published into [Zenodo repository](#), directly linked to Horizon Funding and part of the **EU Open Research Repository**. These articles cover critical topics such as:

- Homomorphic encryption
- Differential privacy
- Threat modelling
- Secure aggregation
- Federated Learning robustness
- Cryptographic methods for privacy-preserving AI

Dissemination through [conferences and workshops](#) represented another strong pillar of the project. TRUMPET partners actively participated in major international events dedicated to AI, machine learning, cybersecurity, cryptography, and health data governance. Over the three years of the project, **the consortium contributed presentations, invited talks, panel interventions, and organised sessions to more than one hundred scientific gatherings (Table 6)**. These included both domain-specific conferences, focused on cryptography, formal methods, or AI engineering, as well as interdisciplinary events examining the intersection of AI with healthcare and regulation.

One of the project’s most distinctive dissemination contributions was **the organisation of dedicated sessions on TRUMPET topics**, often in collaboration with other leading institutions or supported by larger conferences. These included **TRUMPET-organised workshops** such as the special sessions, the **TRUMPET Exchange Talks** series, and numerous cluster-level events within the **EASiNet community**.

Beyond scientific circles, TRUMPET also reached professional audiences through **invited talks at specialised seminars, technical industry-working groups, and hybrid events bridging academia, industry, and public administration**.

In the final year of the project, dissemination activities intensified, particularly as TRUMPET approached its final demonstration phase. Indeed, partners presented the project’s platform, KERs, and technical achievements at industry events.

KPI (Merged Area + Indicator)	M36 Target	M18 Achieved	M39
Scientific Output – Publications (Peer reviewed and conference papers)	≥5	3	6

Scientific Output – White papers / generalist articles	≥3	In progress	3
Events – Scientific participations	12	10	20
Events – Organised events	≥3	4	9
Events – Remote workshops	3	3	5 from consortium, 2 from EASiNet,
Events – Webinars delivered	3	3	5

Table 6 KPIs on dissemination activities

4.2 Exploitation pathways

TRUMPET exploitation pathways are structured into three complementary strands that aim to maximise the impact, sustainability and long-term uptake of the project results.

- 1) **Post-project approach**, ensuring project outcomes can continue to be used. Enable industry to build on the lessons learned and create new market opportunities.
- 2) **Standardisation actions** to stimulate the creation of guides for better cybersecurity capabilities, interoperability and cross-border collaboration between EU countries;

When it comes to particular exploitation actions, TRUMPET partners have deeply analysed the Key Exploitable Results (KERs) of the project, identifying **9 KERs**. While TRUMPET many technologies can be exploited on their own, the main KER is the TRUMPET platform itself. A detailed analysis about KERs is provided in Section 6 and the table with all KERs is included in Annex 2.

Based on the KERs, Trumpet partners, led by AVO, TVS and GRAD, have worked on developing a **Business Plan** (see Section 6.2 *TRUMPET Platform Business Plan and PETRAI project*) which has identified value propositions and competitors that have helped to visualise the potential future pathways for TRUMPET. Moreover, considering that TRUMPET platform is on a TRL4 level, and that the technology needs further efforts to be matured, AVO, TVS and GRAD applied to the call **EIC Transition**, reaching the interview phase and getting the EIC Seal of Excellence.

TRUMPET partners also submitted an application to the Horizon Standardisation Booster and obtained free support on **standardisation advice**. Through four dedicated sessions with a standardisation expert, the consortium obtained guidance on navigating the standardisation landscape, as well as recommendations on the most relevant standards and standardisation committees in which TRUMPET partners could actively participate. For more details, please refer to Section 6.3 Standardisation Advice.

5 Dissemination Results

5.1 Focus on scientific conferences, events and publications

TRUMPET partners actively disseminated scientific results by participating in a wide range of international conferences, workshops, and high-level events addressing federated learning, privacy-preserving technologies, cybersecurity, and health data governance. These activities ensured continuous engagement with the scientific community and contributed to positioning TRUMPET as a relevant actor in the European and international research landscape (Table 7).

TRUMPET results were presented in venues such as AICRYPT (affiliated with EUROCRYPT), DISC workshops, SAFECOMP, FHE.org conferences, and IEEE/ACM events allowed partners to share peer-reviewed research outcomes and methodological advances developed within the project. These events provided an effective forum for scientific validation, peer feedback, and visibility of TRUMPET’s technical contributions.

Overall, participation in scientific conferences and events enabled TRUMPET to:

- Disseminate peer-reviewed scientific results to international research audiences
- Foster collaboration with researchers working on complementary approaches and technologies
- Receive structured feedback supporting the refinement of TRUMPET’s technical solutions

Type of event	Number of activities achieved
Organisation of a conference	2
Organisation of a workshop	7
Participation to a Conference	22
Participation to a Workshop	17
Participation to an Event other than a Conference or a Workshop	9
Pitch Event	1
Trade Fair	2
Exhibition	3

Table 7 Event list

Scientific Publications

TRUMPET outputs include other scientific contributions addressing core technical challenges such as protocols for verifiable federated aggregation, privacy enhancements for collaborative machine learning, and methodological overviews of privacy-enhancing technologies. Several white papers and overview reports were also disseminated, consolidating research insights and providing practical guidance for future applications of federated learning in healthcare data environments. Together, this body of work contributed to both theoretical foundations and practical considerations for secure, scalable, and privacy-resilient AI systems, supporting TRUMPET’s visibility and credibility within the global research community (Table 8).

Title of publication	Date	Link
Private Sampling with Identifiable Cheaters	28/04/2023	https://trumpetproject.eu/wp-content/uploads/2023/04/hal-03904200.pdf
Introducing the TRUMPET project: TRUStworthy Multi-site Privacy Enhancing Technologies	11/05/2023	https://trumpetproject.eu/wp-content/uploads/2023/05/TRUMPET-paper.pdf
Practical Multi-Key Homomorphic Encryption for more Flexible and Efficient Secure Federated Average Aggregation	24/06/2023	https://trumpetproject.eu/wp-content/uploads/2023/06/PBCS_SZ23_IEEE_CSR_2P_DPA_2023.pdf
Building cross-border federated infrastructures for secure and private AI: an overview of privacy-enhancing technologies and their challenges	28/03/2024	https://trumpetproject.eu/wp-content/uploads/2024/06/Building-cross-border-federated-infrastructures-for-secure-and-private-AI_-an-overview-of-privacy-enhancing-technologies-and-their-challenges-1.pdf
Gain insights for latest cyber security trends from Horizon Europe funded projects – White Paper	12/11/2024	https://trumpetproject.eu/wp-content/uploads/2025/01/ENCYRPT_Joint_White_Paper1.pdf
Guidance for DPIA practices from EU-funded projects – White Paper	30/06/2025	https://trumpetproject.eu/wp-content/uploads/2025/07/Guidance-for-DPIA-practices-from-EU-funded-projects_Final.pdf
A Critical Look into Threshold Homomorphic Encryption for Private Average Aggregation	21/01/2025	https://ieeexplore.ieee.org/document/10840167
Fast polynomial arithmetic in homomorphic encryption with cyclo-multiquadratic fields	30/01/2025	https://link.springer.com/article/10.1007/s12095-024-00771-6
Security Guidelines for Implementing Homomorphic Encryption	13/01/2025	https://cic.iacr.org/p/1/4/26
European Projects Insight Report – White Paper	10/06/2025	https://zenodo.org/records/17878360
An Efficient Gradient-Based Inference Attack for Federated Learning	19/12/2025	https://arxiv.org/abs/2512.15143

Table 8 List of publications

White papers

In addition to scientific publications, TRUMPET contributed to the production of three strategic white papers aimed at strengthening policy dialogue, cross-project alignment, and practical guidance on privacy-preserving AI in healthcare (Figure 5).

The first white paper, developed jointly with other EU-funded initiatives, provides an [overview of privacy-enhancing technologies for federated and cross-border AI infrastructures](#), positioning TRUMPET results within a broader European research and innovation landscape

The second white paper focuses on [Data Protection Impact Assessment \(DPIA\) practices](#), translating lessons learned from multiple EU projects into practical guidance to support regulatory readiness and GDPR-compliant implementation of advanced data-driven technologies

Finally, TRUMPET contributed to the [European Projects Insight Report](#), a policy-oriented publication coordinated by HIMSS, which synthesises experiences and recommendations from leading EU digital health projects to inform decision-makers, foster value co-creation, and support the long-term sustainability and uptake of project results.



Figure 5 White paper covers

5.2 Events organised by TRUMPET

In addition to participating in external events, TRUMPET played a proactive role in organising high-impact dissemination and engagement activities. These events were strategically designed to reach different stakeholder groups, including researchers, policymakers, industry representatives, and the broader digital health community.

TRUMPET Exchange Webinars

TRUMPET organised a dedicated series of [Exchange Talks](#) (Table 9 and Figure 6), structured as online webinars focusing on specific technical and regulatory topics related to federated learning, privacy-enhancing technologies, and secure AI. These webinars provided an open forum for in-depth discussion and knowledge exchange, allowing consortium experts and invited speakers to present ongoing research, methodological challenges, and emerging solutions. The online format ensured accessibility and facilitated participation from a geographically diverse audience.

Title of the webinar	Partner presenting
GDPR for ensuring health data privacy in research	TIMELEX
Trustworthy AI, tooling up the methods	CEA
Encryption-based PETs for Federated Learning settings	GRADIANT
Privacy preserving machine learning: differentially private stochastic gradient descent with weight clipping	INRIA

The Case for Privacy: Why It Matters More Than You Think and How to Protect It	UVIGO
--	-------

Table 9 List of Trumpet Exchange talks



Figure 6 Social Media post on Trumpet Exchange talks

Scientific Live events

TRUMPET contributed to the organisation of thematic sessions and workshops within broader AI-focused events, including AI-related festivals and conferences addressing ethical, societal, and implementation aspects of artificial intelligence. These activities supported the dissemination of

project outcomes beyond strictly technical audiences, helping translate complex concepts such as federated learning into accessible narratives for wider communities.

TRUMPET also organised and co-organised two CrossTalk events within **European project clusters**, notably in collaboration with initiatives aligned with the **EU Beating Cancer Plan** and the **EASiNet network**. These CrossTalk events served as structured platforms for dialogue among EU-funded projects, fostering synergies, exchanging best practices, and aligning research efforts.

- **European Beating Cancer Plan CrossTalk Event 2023** : Within the framework of the European Beating Cancer Plan, TRUMPET co-organised a dedicated CrossTalk event held in Brussels, bringing together seven EU-funded projects active in cancer research and data-driven healthcare. The CrossTalk provided a structured opportunity for participating projects (TRUMPET, ONCOVALUE, PERSIST, IMPACT AML, FLUTE, REGION4PERMED, and GRAMMY) to exchange experiences, explore opportunities for collaboration, and discuss common challenges. The event also enabled direct interaction with the European Commission, including a talk by Dr Ioannis Vouldis from HaDeA.
- **Healthcare Claims Future Conference 2023**: Among the scientific events organised by TRUMPET, the conference “Healthcare Claims Future: navigating the landscape of Federated Learning in healthcare” represented a key dissemination milestone. Conceived as a free and open scientific conference, the event focused on exploring the role of Federated Learning (FL) in healthcare, with particular attention to its relevance within European research and policy initiatives.
- **European AI & Cybersecurity Network CrossTalk 2024**: the European AI & Cybersecurity Network CrossTalk on Project Solutions, held on 22 October 2024 in Brussels within the EASiNet cluster and hosted at the Delegation to the European Union of the Emilia-Romagna Region. The event had a strong institutional and policy-oriented dimension, bringing together EU-funded projects, European institutions, and key stakeholders. Designed to go beyond project-level dissemination, the event supported cross-project coordination, policy reflection, and exchange on concrete implementation pathways. The agenda addressed core topics including cloud security, privacy-enhancing technologies and certification, federated learning for medical data, and regulatory perspectives, with contributions from representatives of the European Commission and ENISA. TRUMPET played a central role in scientific coordination and in presenting project solutions, positioning its federated learning approach as a concrete response to the issues discussed.
- **Final Event at Health Tech Forward 2025** - The dissemination activities culminated in the final TRUMPET event, organised within HealthTech Forward 2025. The session, titled “*Sharing Without Sharing: the TRUMPET federated approach for privacy-preserving AI computation*” (Figure 7), showcased the project’s main results, including the federated learning platform and its relevance for secure, GDPR-compliant healthcare data analysis. **33 attendees have been registered to the event.** The workshop provided a high-visibility opportunity to present technical achievements, discuss implementation challenges, and explore future perspectives with a multidisciplinary audience of innovators, policymakers, and digital health stakeholders.

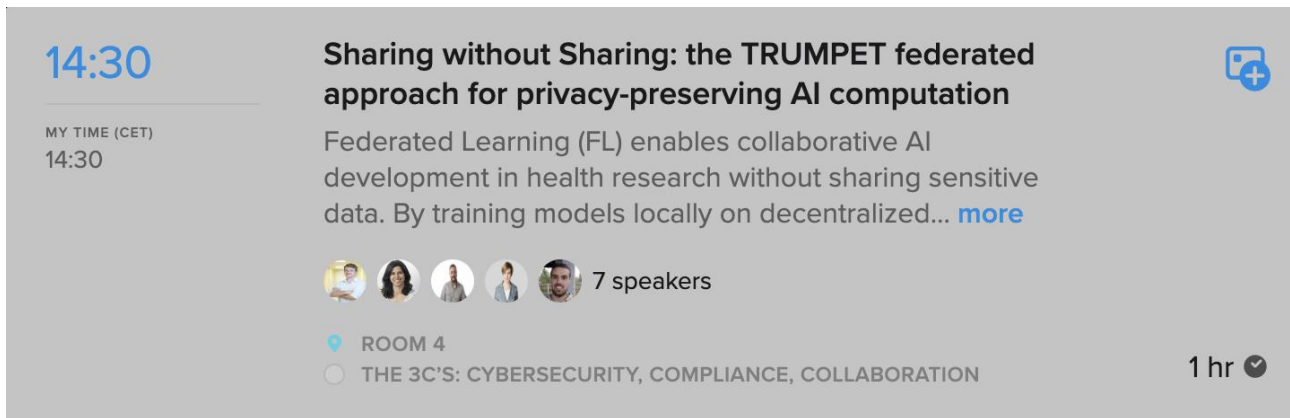


Figure 7 - Agenda of the HealthTech Forward meeting

Through these organised events, TRUMPET demonstrated strong leadership in dissemination and community building, ensuring that project results were communicated effectively, discussed critically, and positioned for long-term impact beyond the project’s lifetime.

5.3 Educational initiatives and GAP-related activities

Gender equality and the promotion of inclusive participation in STEM were central objectives of TRUMPET’s Gender Action Plan. Dissemination under the GAP focused on two complementary pillars:

- AI-DEA Hackathon: TRUMPET’s Flagship GAP Initiative
- Audiovisual Series: [“Women in Technology Conversations”](#)

AI-DEA Hackathon: TRUMPET’s Flagship GAP Initiative

The AI-DEA Hackathon (Figure 8) represented one of the most significant outreach and gender-balance achievements in the project. Organised by IRST in collaboration with local institutions and supported by TRUMPET partners, the event brought together 100 high-school students, **working in gender-balanced teams** (2 men and 2 women) to develop AI-driven solutions for healthcare challenges.

Key GAP outcomes:

- **Balanced participation:** Teams were intentionally composed to ensure equal involvement of female and male students.
- **STEM empowerment:** Female students were encouraged to take leadership roles, pitch ideas, and engage directly with mentors from scientific and technical fields.
- **Real-world problem-solving:** Students worked on concrete healthcare innovation challenges, improving understanding of AI and data privacy.
- **Visibility and impact:** The Hackathon received strong communication coverage across social media, the TRUMPET website, and regional media outlets, reinforcing the message that AI is a field accessible to all.

The winning team later participated in the **TRUMPET Summer School in Vigo**, giving continuity to the educational pathway and supporting young talents beyond the initial event.

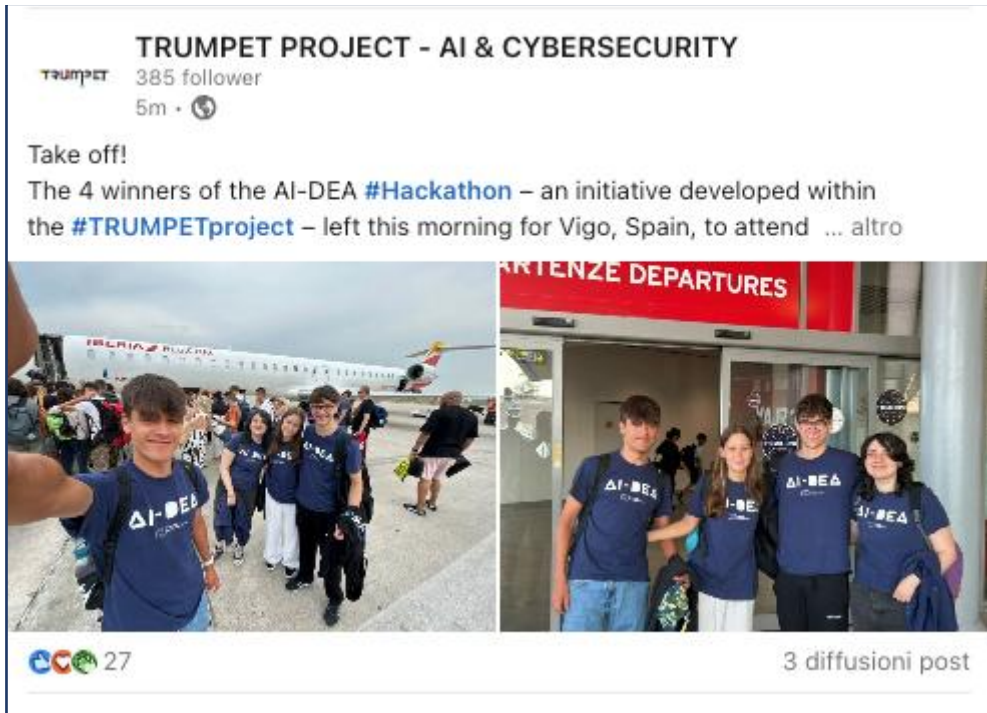


Figure 8 Social media post on Summer School

The Hackathon stands as a flagship example of how EU-funded projects can actively contribute to closing the gender gap while raising awareness about AI and digital health.

Audiovisual Series: “Women in Technology Conversations”

During TRUMPET, Gradient expanded its GAP initiatives by transitioning from written communication to audiovisual content, a strategic move to reach wider audiences (Figure 9).

As part of this evolution, four video episodes were produced, each focusing on a key theme relevant to women in technology:

- Innovation
- Challenges
- Future
- Leadership

These conversations—recorded in Spanish and subtitled in English—feature relaxed dialogues in which women technologists share their experiences, perceptions, and insights regarding participation and careers in the tech sector.

The videos were released every Tuesday in February, turning the initiative into a structured communication campaign with clear visibility and engagement objectives.

This audiovisual series strengthened TRUMPET’s GAP outreach by:

- Showcasing authentic voices and lived experiences of women in STEM
- Using an accessible and modern dissemination format
- Supporting gender equality through relatable role models
- Increasing the project's social impact beyond scientific communities



Figure 9 Tech talks by Gradiant

6 Exploitation Results

6.1 KERs developed by the consortium

The Consortium has analysed the project results and identified 9 KERs, classifying them according to their impact type: technical, societal, scientific, or policy/regulatory (Table 10 and Annex 2).

Impact	KER	Type	Description	Owner	TRL
Tech	PET:MKHE	Other	Solution for the execution of a private aggregation protocol based on the use of secret multi-key homomorphic encryption	UVIGO, GRAD	4
	PET: CDC+DP	Other	PET based on the Coded Distributed Computing with Differential Privacy that ensures privacy-preserving model aggregation through a structured workflow that maintains consistency across all DO.	GRAD	4
	FL Core	Other	Central component where model training occurs, communication between nodes is managed, and PETs are integrated to protect sensitive data.	GRAD	5
Societal	Inference attacks	Other	Membership inference attacks and attribute inference attacks.	GRAD	5
	TRUMPET platform and dashboard for users	Product	The TRUMPET platform is a privacy-preserving FL system designed to enable secure and GDPR compliant healthcare data analysis without sharing sensitive patient information	AVO, TVS, GRAD	4
Scientific	Multi-Secret-Key Homomorphic Encryption Protocol for Secure Aggregation	Method	Novel secure aggregation protocol for Federated Learning (FL) based on Multi-Secret-Key Homomorphic Encryption (MKHE)	UVIGO	4
	Privacy metrics and attacks based on Mutual Information	Method	Theoretical and practical framework for privacy evaluation FL, leveraging Mutual Information (MI) as a rigorous measure of privacy leakage.	UVIGO	4
Policy or regulatory	Tool for measurement and validation of privacy	Product	A dedicated framework designed to assess and ensure the privacy and security of Federated Learning systems, providing compliance with GDPR and robust protection against data leaks	UVIGO, GRAD, INRIA	4
	Legal know-how on the development and operation of a FL platform for medical purposes in a privacy preserving way	Method	Understanding of the legal roles and responsibilities, the relevant challenges and tools available to mitigate data protection issues	TLX	NA

Table 10 TRUMPET Key Exploitable Results

In summary, from the perspective of impact, four major categories emerge:

- **Technological**, with 3 KERs focused on core privacy-enhancing technologies (PETs) and the central FL system component.
- **Societal**, with 2 KERs related to the TRUMPET platform aimed at end users and to the evaluation of vulnerabilities through inference attacks.
- **Scientific**, with 2 methodological innovations linked to multi-key homomorphic encryption and privacy metrics based on mutual information.
- **Policy or regulatory**, with 2 results supporting GDPR-aligned validation, certification, and legal interpretation in the context of medical FL systems.

Regarding the distribution of **ownership**, the KERs are shared among 7 partners of the consortium (out of the total of 10 partners of TRUMPET). There is a particularly strong presence of GRAD, involved in 6 of them, reflecting its role as a core technological contributor. UVIGO participates in 4 KERs, especially those related to cryptography and privacy evaluation, demonstrating their impact in the scientific domain. AVO and TVS contribute primarily to the final user-oriented platform; INRIA supports the development of privacy validation tools; and TLX leads the single KER dedicated entirely to legal and regulatory expertise. This distribution shows a balanced alignment between technological, scientific, and regulatory capabilities across the consortium. **Annex 1** contains a complete table with all declared IPR status.

In terms of **TRLs**, the KERs mainly fall between TRL 4 and TRL 5, indicating that most developments have reached the stage of validation in a relevant environment. Specifically:

- 4 KERs are at TRL 4, corresponding to emerging PETs, the TRUMPET platform, foundational scientific methods.
- 2 KERs have reached TRL 5, including the **FL Core and the analysis of inference attacks—representing the components closest to pilot deployment.**

Owners of the results aim to exploit all the KERs identified. Below in Table 11 more information is provided on the **exploitation strategy** for each of the KERs

KERs	Access Rights	Target Groups	Exploitation
PET:MKHE	Restricted	Researchers, Sensitive Industry, Data Controllers	Demo or testing, PETRAI application
PET: CDC+DP	Restricted	Researchers, FL platforms, Data Controllers	Demo or testing, PETRAI application
FL Core	Restricted	Researchers, Industry, Business partners	Market study, PETRAI application
Inference attacks	Restricted	Researchers, Policy-makers and authorities	Demo or testing, market study
TRUMPET platform and dashboard for users	Restricted	Researchers, Industry, Business partners	Market study, PETRAI application
Multi-Secret-Key Homomorphic Encryption Protocol for Secure Aggregation	Open	Industry, Researchers	Demo or testing
Privacy metrics and attacks based on Mutual Information	Restricted	Researchers, Regulators and standardization bodies	Demo or testing

Tool for measurement and validation of privacy	Restricted	Researchers, Policy-makers and authorities	Other
Legal know-how on the development and operation of a FL platform for medical purposes in a privacy preserving way	Open	Policy-makers and authorities	Publications, workshops, engagement with EU research projects and representatives from regulatory authorities

Table 11 Exploitation Pathways for identified KERs

In terms of **access rights**, the majority of KERs (7 out of 9) are classified as Restricted/Private, due to the relevance for security-critical developments such as PETs, the FL Core, and evaluation tools. 2 KERs will follow an Open/Public approach: the Multi-Secret-Key Homomorphic Encryption method and the legal know-how. These are intended to foster collaboration with industry, researchers, and regulators by providing openly accessible technical and legal foundations for privacy-preserving FL.

The **target groups** addressed a broad spectrum of stakeholders. Researchers are the most targeted group (8 out of 9 KERs). Industry, business partners, and FL platform developers are reached through the major technological KERs, particularly the FL Core and the TRUMPET platform. Policy-makers, authorities, and regulators are engaged through KERs related to inference attacks, privacy validation tools, and the legal know-how, ensuring alignment with GDPR and facilitating future certification pathways.

Regarding the **steps towards exploitation**, additional demos and testing are central to the maturation of PETs, MKHE protocol and ML-based privacy metrics, scientific tools and the platform. Similarly, the TRUMPET platform require additional market studies to advance toward real-world uptake and commercial feasibility. Trumpet partners have worked in an initial business plan for the TRUMPET platform, as further explained in the next section *6.2 Trumpet Business Plan and PETRAI project*. Two KERs—the inference-attack analysis and the privacy-measurement tool—are classified under “Other exploitation steps”, indicating their role as enabling assets rather than stand-alone exploitable technologies. Their exploitation is expected mainly through integration into assessment workflows and contributions to policy guidance. The legal know-how follows a distinct trajectory based on dissemination and engagement activities, including publications, workshops, and collaborations with other EU-funded initiatives, aiming to facilitate compliance and knowledge transfer.

For further information on TRUMPET results, please refer to *Section 6.4 Impact Assessment of TRUMPET solutions*, and Annex 2, the complete KER analysis table, including Risks and Mitigation measures for each of the KERs.

6.2 TRUMPET Platform Business Plan and PETRAI project

While TRUMPET created a number of technologies that can be exploited on their own, as described above, its more remarkable KER is the TRUMPET platform itself. The most straightforward and impactful way to exploit it is to establish a commercial service based on it that will bridge between the AI developing organizations and the siloed data owners. Indeed, this was the original motivation behind the TRUMPET concept. To follow this exploitation pathway, three TRUMPET partners (SMEs AVO and TVS, and the TRUMPET coordinator, GRAD, a RTO) have teamed up to create the PETRAI proposal in response to the EIC Transition calls 2024 and 2025. Partners reached the interview phase in the 2025 call and got the **Seal of Excellence** (Figure 10). Next steps include analysing opportunities through the the Seal of Excellence at national and European level, as well

as revising the feedback from the evaluation to prepare a new version of the proposal for the next call of September 2026. The aim of the PETRAI proposal is to commercialize the TRUMPET platform by maturing it to TRL6, to be called the PETRAI platform, developing additional technological layers in it that will support commercialization, and creating an EU-headquartered startup that will operate the platform and deliver Federated Learning services in Europe and globally. PETRAI will be the industry’s first commercial platform that offers GDPR-safe Open Federated Learning Services, and the only FL platform that supports foundation models, deep explainability and strong AI model-agnostic cryptographic PETs in Federated Learning settings.



Figure 10 PETRAI Seal of Excellence

The market. The global 2024 AI market was US \$638.23 billion and is expected to reach \$3.68 trillion by 2034. While the FL market niche is currently at an early stage, it has been flagged by Gartner as approaching the peak of expectations in the 2024 technologies Hype Cycle. Three global market reports dedicated exclusively to Federated Learning, published in 2025, were used in our market research. The FL market stats are shown in Figure 11.

Federated Learning market report	2023	2032	CAGR	Forecast period
Value Market Research ²	137	~ 435	13.7%	2024-2032
Grand View Research ³	129	~ 378	12.7%	2023-2030
Expert Market Research ⁴	131	~ 328	10.7%	2024-2032

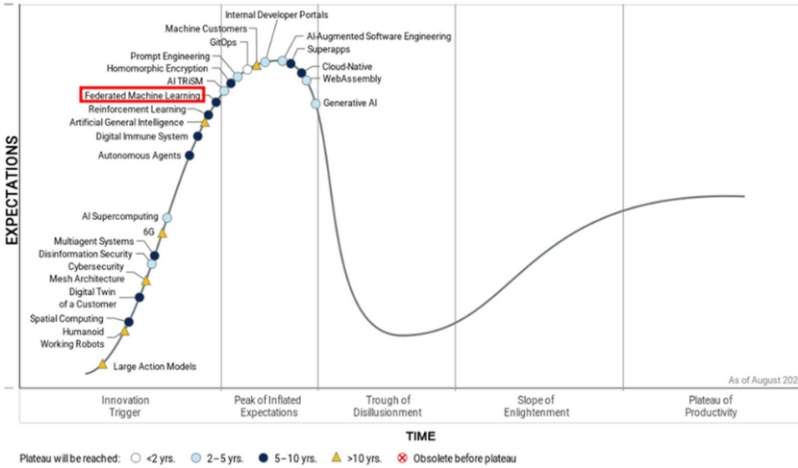


Figure 11 Federated Learning market stats

Business, revenue and pricing model will be based on the subscription of the AI developers for OFLS services. Premium and tiered pricing will be used to optimize the value of subscription to the AI developers' needs, and to maximize the revenues of PETRAIs – that will be shared with the data owners based on the use of their datasets.

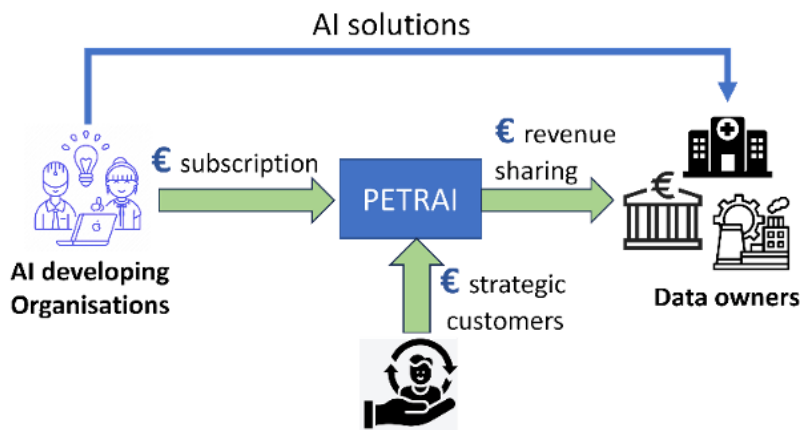
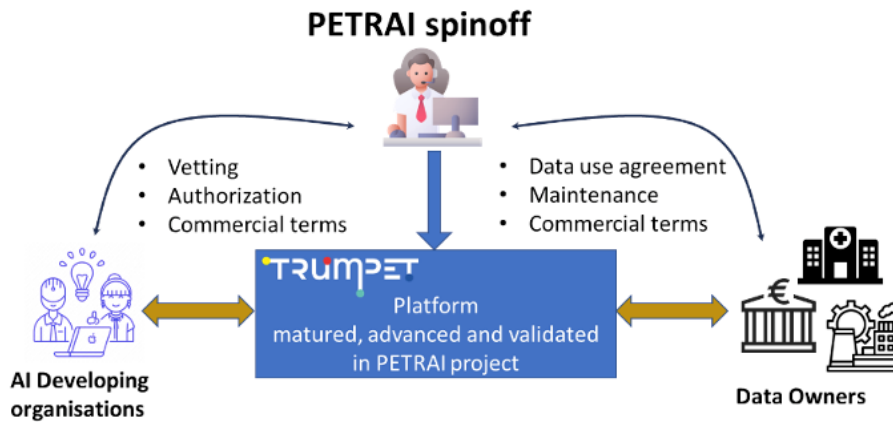


Figure 12 PETRAI business concept

Among the main innovations planned in PETRAI to enable and enhance the commercialization of the TRUMPET platform (Figure 12) there are planned the following activities:

- Creation of unlimited domain-agnostic Federated Learning networks
- Additional technological innovations in Privacy Enabling Technologies
- Incorporation of Domain-Specific Foundation Models and their training in FL settings
- Incorporation of AVO’s patent-pending Deeply Explainable Artificial Neural Network (DxANN) technology

Two TRUMPET partners, UVIGO and INRIA, have signed letters of commitment to license their technologies to PETRAI under reasonable business terms. The PETRAI team plans collaboration with the clinical partners of TRUMPET to seed the Life Sciences Federated learning network on the PETRAI platform, utilizing the Data Owner KERs and existing TRUMPET-generated installation of Data Owner nodes at their premises. Legal framework established during TRUMPET will serve as the basis of the compliant operation of the PETRAI platform by the PETRAI startup.

The technologies developed in TRUMPET put the proposed PETRAI venture in a strong competitive position. The advantages are summarized in Figure 13. We have identified five market players that

use some level of privacy enabling technologies, that may compete with PETRAI; and one company (Zama) that sells technology that may potentially be purchased by competition and used to compete with PETRAI:

Feature	PETRAI	TuneInsight	Inpher	Owkin	Consilient	Rhino Health	PETRAI advantage
Homomorphic Encryption (HE)	Multi-party, Multi-Key ThHE	Multi-party FHE (BGV, CKKS)	No	No	No	No	Faster and more efficient and scalable homomorphic encryption
Threshold HE	Yes	Yes	No	No	No	No	More secure distributed computing
Multi-Key HE	Yes	No	No	No	No	No	Much increased efficiency of ThHE.
Differential Privacy (DP)	Sparse Vector DP with Selective Parameter Update	ϵ -DP (Laplace Mechanism)	Not mentioned	Rényi DP	None	Yes	Precise control of privacy budget by adding noise to only a few selected parameters, to maximize accuracy
Coded Distributed Computation (CDC)	Berrut Code Computing	No	No	None	No	No	Protection against privacy attacks by malicious servers
FL Aggregation in Trusted Execution Environment	Intel TDX and AMD SEV	No	Not used with FL	None	No	No	Strong protection against malicious FL aggregator
Protection against colluding semi-honest learning nodes (out of total of N nodes)	Yes, up to N-2 passive colluding nodes	Yes, up to N-1 passive colluding nodes	No	Yes	No	No	Efficient trade-off between accuracy and protection
Secure Multi-Party Computation (SMPC)	Yes, combined with MKHE and collective public key	Yes, combined with TrHE	Yes, without HE	Yes, without HE	No	No	Communication and computation tradeoff allows efficient implementation
Support for FL fine tuning of domain-specific foundation models	Yes	No	No	No	No	No	Possibility to apply FL to transfer learning using foundational models
Support for training Deeply Explainable Artificial Neural Networks (DxANN)	Yes	No	No	No	No	No	Make FL-trained deep learning models intrinsically explainable.
Multimodal FL training	Tool for extracting features from multimodal data	No	No	No	No	No	Breakthrough advancement in range of applicability of FL
GDPR compliance dashboard	Yes	No	No	No	No	No	Allows data owners to set and monitor GDPR compliance measures
Automated technical robustness testing	Suite of tests for AI Act-compliant robustness	No	No	No	No	No	Increased robustness of solutions and compliance with EU regulation
Standard Jupiter Notebook AI developer interface	Yes	Complex custom I/F	No	No	No	No	Very fast AI developer learning curve

Figure 13 Competitive advantage of TRUMPET technologies in PETRAI

PETRAI will create jobs and play a significant role in the helping Europe to achieve a stronger position vis-à-vis US and China in the global AI race.

6.3 Standardisation Advice

As also explained in D5.2 TRUMPET Regulatory Acceptance Plan, TRUMPET was selected for support by the European Commission’s initiative HS Booster (Figure 14). The aim of the initiative was to facilitate and streamline the dialogue between projects funded under Digital Europe, Horizon 2020 and Horizon Europe Research & Innovation programmes with Standards Developing Organisations (SDOs) to increase the European impact on (international) Standardisation and strengthen the European competitiveness. TRUMPET applied to an open call to obtain practical guidance by experts to assess the standardisation readiness of project results, particularly for privacy metrics and FL models, and obtain guidance on how to feed these results into standardisation working groups or technical committees. Participation in such an initiative aligned with the ‘Exploitation plan’ section of the GA, where it is mentioned that ‘TRUMPET solution informs and influences international standardization activities.

GRAD, UVIGO, and TLX attended four meetings with a standardisation expert to review core standardisation concepts and terminology, the relationship between standards and regulation, types of standardisation and criteria for engagement with SDOs. The sessions also covered the requirements and timelines involved for proposing new standardisation items, methods for identifying appropriate standards, an overview of the standardisation landscape related to the project, and guidance on how to engage in standardisation processes, including proposing new standardisation items and contributing to ongoing initiatives. The expert suggested joining specific national bodies to initiate standardisation efforts with ISO/IEC & CEN/CENELECs.

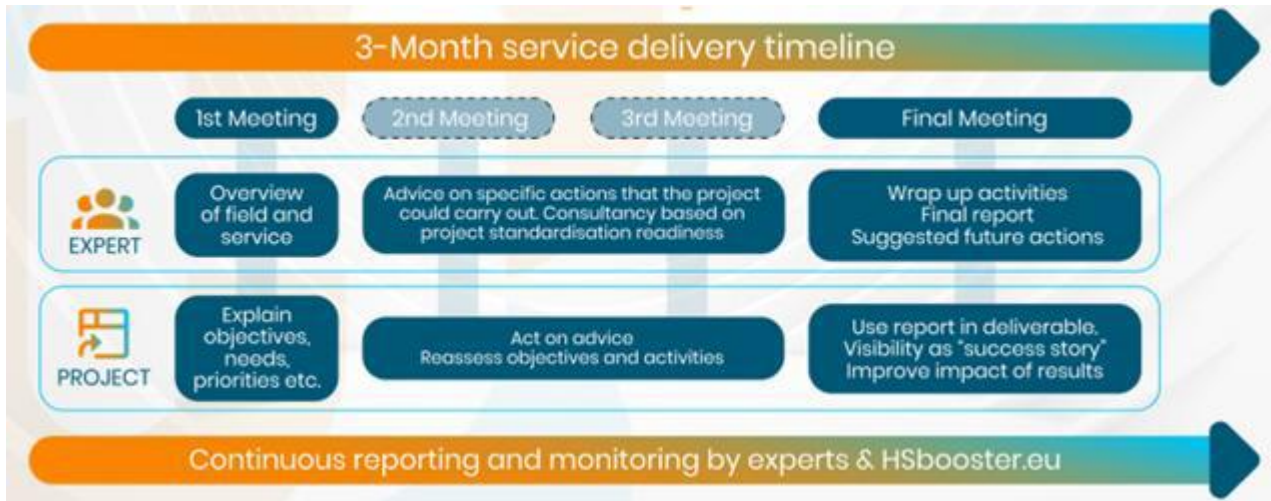


Figure 14 Summary of the meetings with the HS Booster expert

Based on this overview, the expert identified a set of relevant international and European technical committees and initiatives that the project may consider engaging with. These include:

- **International ISO/IEC Technical Committees:**
 - o ISO/IEC JTC 1/SC 42 – Artificial Intelligence
 - o ISO/IEC JTC 1/SC 27 – Information security, cybersecurity and privacy protection
 - o ISO/IEC JTC 1/SC 29 – Coding of audio, picture, multimedia and hypermedia information (including MPEG activities related to AI)
- **IEEE / MPAI Initiatives:**
 - o MPAI – Moving Picture, Audio and Data Coding by Artificial Intelligence (e.g., MPAI-AIH – Artificial Intelligence for Health)
 - o IEEE European Public Policy Committee (EPPC) – Call for New WG Members: ICT
- **European CEN/CENELEC Technical Committees:**
 - o CEN-CLC/JTC 21 – Artificial Intelligence
 - o CEN-CLC/JTC 13 – Cybersecurity and data protection
 - o CEN/TC 251 – Health informatics

Given that standardisation is a long-term investment and is a choice linked to the research interests and available resources, the consortium is currently investigating whether future exploitation of the project’s results by joining SDOs will benefit the project’s visibility, uptake and sustainability, particularly within ISO and CEN/CENELEC. Such participation could support the future exploitation of the project’s results through standardisation. It is noted that membership in ISO/IEC and CEN/CENELEC is obtained via the national bodies of the project partners. Additionally, TVS is already engaged at the national level through the British Standards Association (BSA), the national standards body responsible for developing and coordinating standardisation activities within the UK, participating in standardisation activities relevant to the project’s thematic areas, which can further support the alignment and future exploitation of the project’s results.

6.4 Impact Assessment of TRUMPET solutions

TRUMPET addresses the paradox of data-rich healthcare systems unable to fully exploit their own information due to strict privacy and data-protection constraints. By combining advanced AI with cutting-edge privacy-preserving technologies (PETs), TRUMPET unlocks the vast research potential hidden within hospital datasets while ensuring compliance with the GDPR. Although Federated Learning holds great promise for enabling secure cross-institutional data analysis, its adoption remains limited because existing implementations still face unresolved privacy challenges. TRUMPET provides concrete solutions that directly mitigate these barriers.

Throughout the project, TRUMPET has developed a suite of privacy preserving technologies, privacy metrics, measurement tools and a reference implementation of the TRUMPET platform, contributing to EU priorities in cybersecurity, privacy and responsible data reuse. The platform delivers:

- Scalable and reliable PETs for federated processing of personal data.
- Robust privacy guarantees for Data Owners through dedicated metrics and measurement tools.
- Ease of use across siloed, multi-site, cross-border datasets, offering researchers a unified view of distributed data.
- Promotion of privacy metrics and engagement with data-protection authorities to support future certification of privacy-preserving federated processing.
- An application-agnostic platform, reusable across multiple domains and use cases.

The TRUMPET Consortium has performed an impact-oriented assessment of the project’s 9 KERs. They have been classified according to their primary impact type—technical, societal, scientific, or policy/regulatory (Table 12).

IMPACT	Nº	NAME OF THE RESULTS	TYPE	TRL reached
Technical	1	PET: MKHE	Components	4
	2	PET: CDC+DP		4
	3	FL Core		5
Societal	4	Inference attacks	Component	5
	5	Trumpet platform and dashboard for users	Product	5
Scientific	6	Multi-Secret-Key Homomorphic Encryption Protocol for Secure Aggregation	Methods	4
	7	Privacy metrics and attacks based on Mutual Information		4
Policy or regulatory	8	Tool for measurement and validation of privacy	Product	?
	9	Legal know-how on the development and operation of a state-of-the-art FL platform for medical purposes in a privacy preserving way	Method	NA

Table 12 Trumpet KERs – Impact classification

Descriptions and high-potential impacts for the KERs identified are presented below:

TECHNICAL IMPACT:

1. PET: MKHE

Description: PET solution for the execution of a private aggregation protocol based on the use of secret multi-key homomorphic encryption.

High Potential: MKHE enables secure aggregation of encrypted data without the need for decryption at the aggregator, offering strong privacy guarantees especially for sectors requiring strict confidentiality (e.g., health, finance). It is adaptable to different FL topologies and supports future-proof data protection strategies.

2. PET: CDC+DP

Description: PET based on the Coded Distributed Computing with Differential Privacy, ensures privacy-preserving model aggregation through a structured workflow that maintains consistency across all Data Owners.

High Potential: CDC+DP combines privacy and fault tolerance in distributed model aggregation. Its structured nature makes it scalable and adaptable for federated deployments involving many nodes.

3. FL Core

Description: The FL Core is the central component where model training occurs, communication between nodes is managed, and PETs are integrated to protect sensitive data. It is responsible for coordinating training rounds, aggregating model updates, and ensuring efficient data exchange while maintaining security and scalability.

High Potential: The FL Core is domain-agnostic and can be applied in any sector requiring federated privacy-preserving machine learning, such as healthcare, finance, mobility, or manufacturing. Its modular and scalable architecture enables integration with various PETs, positioning it as a strong candidate for commercialization or integration into existing AI platforms across industries.

SOCIETAL IMPACT:

4. Inference attacks

Description: Membership inference attacks (attacks that aim to determine whether a specific data point was used to train a model) and attribute inference attacks (attacks that aim to reveal some sensitive attribute of data points used to train a model). Obtaining this knowledge about one of the private datasets of Data Owners violates the primary privacy goal of this paradigm, which is to protect training data by keeping it private

High Potential: Inference attacks highlight critical privacy vulnerabilities in federated learning. Understanding and demonstrating these attacks is essential for developers, policymakers, and regulators to design proper mitigations and ensure compliance with GDPR and other data protection regulations. These insights can inform guidelines, certifications, and auditing frameworks.

5. Trumpet platform and dashboard for users

Description: The TRUMPET platform is a privacy-preserving Federated Learning system designed to enable secure and GDPR-aligned healthcare data analysis without sharing sensitive patient information

High Potential: The platform is an integrated FL solutions that combines technical privacy guarantees with regulatory oversight. It can serve hospitals, research institutions, and med-tech

companies looking for compliant, secure Federated AI solutions. Its modular design makes it easy to adapt for other sectors (e.g., finance, industry etc...), providing high exploitation potential.

SCIENTIFIC IMPACT:

6. Multi-Secret-Key Homomorphic Encryption Protocol for Secure Aggregation

Description: Novel secure aggregation protocol for Federated Learning based on Multi-Secret-Key Homomorphic Encryption (MKHE). Unlike threshold or multiparty HE schemes, each data owner encrypts with its own secret key, and yet the encrypted updates can be aggregated directly. Decryption requires collaboration (version-1) or can be performed more efficiently through masked aggregation (version-2), significantly reducing communication costs. The implementation is openly available under an Apache license at [Github](#) and has been validated through extensive performance benchmarks.

High Potential: The MKHE-based aggregation protocol supports practical deployment of secure FL in sensitive domains such as healthcare, finance, or cross-institutional collaborations. By combining strong security guarantees (based on RLWE) with reduced communication overhead, it lowers the barrier for industrial adoption. Its open-source implementation further enhances reusability and accelerates technology transfer.

7. Privacy metrics and attacks based on Mutual Information

Description: Theoretical and practical framework for privacy evaluation in Federated Learning, leveraging Mutual Information (MI) as a rigorous measure of privacy leakage. This approach quantifies the dependency between shared gradients and underlying sensitive data. Additionally, it has been designed and implemented membership inference attacks to empirically validate the strength and applicability of the proposed metrics.

High Potential: The framework allows both researchers and technology integrators to objectively evaluate privacy leakage risks in FL. Its adoption supports the certification of compliance with privacy standards and enables the benchmarking of different defense mechanisms (e.g., Differential Privacy, Homomorphic Encryption, etc.). The framework not only defines rigorous information-theoretic privacy metrics but also establishes a direct connection with the ENISA methodology for assessing data breaches. This integration bridges theory and practice by linking Mutual Information-based metrics with the severity estimation of privacy leakage in real FL deployments. This unique contribution from UVIGO enhances the regulatory impact of the tool, positioning it as a reference framework for GDPR compliance and European data protection standards.

POLICY IMPACT

8. Tool for measurement and validation of privacy

Description: A dedicated framework designed to assess and ensure the privacy and security of Federated Learning systems, providing compliance with GDPR and robust protection against data leaks

High Potential: The framework allows both researchers and technology integrators to objectively evaluate privacy leakage risks in FL. Its adoption supports the certification of compliance with privacy standards and enables the benchmarking of different defense mechanisms (e.g., Differential Privacy, Homomorphic Encryption, etc.). The framework not only defines rigorous information-theoretic privacy metrics but also establishes a direct connection with the ENISA methodology for assessing data breaches. This integration bridges theory and practice by linking Mutual Information-based metrics with the severity estimation of privacy leakage in real FL deployments. This unique

contribution from UVIGO enhances the regulatory impact of the tool, positioning it as a reference framework for GDPR compliance and European data protection standards.

9. Legal know-how on the development and operation of a state-of-the-art FL platform for medical purposes in a privacy preserving way

Description: Legal know-how on the development and operation of a state-of-the-art federated learning platform for medical purposes in a privacy preserving way. In particular, the understanding of the legal roles and responsibilities, the relevant challenges and tools available to mitigate data protection issues – including techniques for data pseudonymization and anonymization and other privacy enhancing technologies (PETs), such as federated learning – are invaluable in any medical data sharing contexts. The lessons learned in TRUMPET will be readily reusable in other initiatives through the development of a regulatory acceptance plan that takes into account all relevant guidance from data protection and cybersecurity authorities and adjusts it to the requirements of an environment that involves the processing of sensitive data. More specifically, this know-how can be re-used in other contexts and sectors, notably towards data providers (hospitals, biobanks, research organizations and companies), data intermediaries and data users, that deploy or rely on data.

High Potential: This know-how can be re-used in other contexts and sectors, notably towards data providers (hospitals, biobanks, research organizations and companies), data intermediaries and data users, that deploy or rely on data. As Timelex provides legal services to all of these categories of stakeholders, it can further use, exploit and disseminate this know-how. Further to the regulatory acceptance plan, this can be done through, e.g. data use policies, platform use terms, data protection impact assessments, privacy policies, layered information notices and so forth, all of which have direct exploitable value.

7 Synergies with European Projects and Initiatives

During the length of the project, the partners of TRUMPET have worked with various European actors to foster collaboration at a European scale for safe and secure AI applications. For that goal multiple initiatives have been deployed. Though their impact is difficult to quantify, the different actions led by TRUMPET and its partners brought together a variety of actors, certainly creating new synergies at European level.

The first initiative led by TRUMPET was the creation of the **European AI Security Network (EASiNet)**, already introduced in the previous deliverable, this is a network of 10 different European projects brought together on the subjects of AI for healthcare, federated learning, private and safe AI. Following its launch on January 2024, a series of meetings and webinars have been organised, presenting the various projects and leading to a successful crosstalk event on October 22, 2024 in Brussels. This event was the opportunity for the members of EASiNet to discuss across projects on the core topics behind them (cloud security, privacy-enhancing technologies and certification, federated learning for medical data, and regulatory perspectives). Representatives from the **European Commission** and **AI Office** as well as **ENISA** were present sharing key insights on the perspectives on these topics. Following the crosstalk event, where further synergies were identified between the project, a white-paper “Guidance for DPIA practices from EU-funded projects” was written in collaboration with eight members of the network. Published freely on Zenodo at the end of May 2025, this white paper concretises the efforts around the EASiNet.

On another note, members of the TRUMPET consortium have been involved in various European initiatives to help shape the future of AI safety & security in Europe. Through their implication in the **European Cybersecurity Community support project (ECCO)**, CEA participated in the elaboration of the roadmap and future calls of the **European Cybersecurity Competence Centre (ECCC)**, allowing to position insights from the TRUMPET project on the future of research and innovation at the intersection of cybersecurity and AI. The participation of GRAD and CEA in working groups and board of directors of the **European Cyber Security Organisation (ECSO)** further allowed the TRUMPET project results and insights to be taken into account at European level.

Within the European trustworthy AI community, links have been established with **the European Trustworthy AI Association (ETAIA)**, of which CEA is a member, and its various events. This is an important venture where CEA’s trustworthy AI tools and the results from TRUMPET can be made accessible to a wide array of partners at the European level.

Additionally, in the eHealth community, TRUMPET has been able to foster relationship with the **European Health Telematics Association (ETHL)** with the help of CHU. The participation and organisation of the final event of TRUMPET in **Health Tech Forward in Barcelona**, also allowed for further interaction in this community.

Overall, this involvement from the TRUMPET project in various European initiatives allowed for TRUMPET to incorporate its key insights in the European landscape.

While the TRUMPET project concludes, the synergies established with various European initiatives remain and will allow to disseminate the final results of the project widely. On EASiNet’s side, while most European project involved in the initiative will soon be concluded (or already are), the discussion avenues created between partners of the projects will still exist and will allow further collaboration between them.

8 Conclusion and recommendations

This deliverable has provided a consolidated overview of the Communication Strategic Plan (CSP), Dissemination and Exploitation Plan (DEP), and the synergies achieved throughout the TRUMPET project. Building on the foundations set by previous deliverables, it demonstrates how communication and dissemination activities were implemented coherently and adapted over time to maximise impact across scientific, professional, policy, and societal audiences.

Through a balanced mix of scientific publications, high-level events, educational initiatives, cross-project collaborations, and policy-oriented outputs, TRUMPET successfully enhanced the visibility, understanding, and uptake potential of its results. The project's active engagement within European clusters and initiatives further strengthened alignment with EU priorities, including trustworthy AI, cybersecurity, and the European Health Data Space.

Overall, the communication and dissemination strategy supported both short-term visibility and long-term sustainability of TRUMPET outcomes, positioning the project as a relevant contributor to European research, innovation, and policy dialogue on privacy-preserving federated learning in healthcare.



9 Annexes

Annex 1. IPR Table

IP ANALYSIS								
	Type	Partners claiming IPR	WPs	Tasks	Intent to file a patent	Patent Authority	Status of patent application	Notes
Brief description of the innovaton/IP								
CAISAR Platform for Characterizing AI Safety And Robustness	Background	CEA	2	2.4, 2.5	No			CAISAR was released as open-source before the start of TRUMPET
FL Platform Core: A SW platform serving as the foundational core for implementing Federated Learning (FL) processes. This core platform facilitates the coordination, management, and execution of FL workflows, allowing multiple decentralized data owners to collaboratively train machine learning models without sharing sensitive data. It ensures data privacy, scalability, and efficient communication across different nodes involved in the FL process, making it a comprehensive solution for implementing secure and effective federated learning applications.	Foreground	GRAD	4	All	No	N/A	N/A	
PET1: A FL-tailored MKHE (Multi-Key Homomorphic Encryption) SW scheme designed for secure and private data aggregations within Federated Learning (FL) processes. This scheme ensures that data from multiple participants can be aggregated without exposing individual data points, maintaining both security and privacy. By leveraging homomorphic encryption techniques, PET1 allows encrypted data to be processed without decryption, providing a robust solution for preserving confidentiality in collaborative learning environments. This innovation significantly enhances the privacy and security of FL applications, making it ideal for scenarios involving sensitive data	Foreground	GRAD	2	T2.1, T2.2, T2.3 and T2.5	No	N/A	N/A	

PET2: An advanced FL-tailored Secure Multi-Party Computation (SMPC) SW protocol that integrates Coded Distributed Computation (CDC) with Differential Privacy (DP) to enable secure and private aggregations within Federated Learning (FL) processes. This protocol is specifically designed to enhance the security and privacy of data aggregation by allowing multiple parties to collaboratively compute without revealing their individual data. The combination of CDC ensures efficient and fault-tolerant distributed computation, while DP adds an additional layer of output privacy by preventing the exposure of sensitive information on outputs.	Foreground	GRAD	2	T2.1, T2.2, T2.3, T2.4 and T2.5	No	N/A	N/A	
A SaaS Solution for Homomorphic SVM Inferences: A Software-as-a-Service (SaaS) solution that provides secure and efficient Homomorphic Support Vector Machine (SVM) inference capabilities. This solution enables the use of SVM classifiers while ensuring data privacy through homomorphic encryption.	Background	GRAD	4	T4.2 and T4.4	No	N/A	N/A	
Researcher dashboard	Foreground	TVS	4	all	N/A	N/A	N/A	
Researcher Server	Foreground	TVS	4	all	N/A	N/A	N/A	
Data owner dashboard	Foreground	TVS	4	all	N/A	N/A	N/A	
Data owner server	Foreground	TVS	4	all	N/A	N/A	N/A	
Advertised dataset browser	Foreground	TVS	4	all	N/A	N/A	N/A	
Operator node	Foreground	TVS	4	all	N/A	N/A	N/A	
Clinical datasets	Background	CHUL	4	T4.1	No	N/A	N/A	A set of clinical data for the treatment and follow-up of cancer patients in the following indications: head and neck cancer, metastatic cancer treated by stereotactic radiotherapy collected according the applicable clinical guidelines.

Study datasets	Foreground	CHUL	4	T4.1	No	N/A	N/A	Curated, cleansed and consolidated datasets for the treatment and follow-up of cancer patients in the following indications: head and neck cancer, metastatic cancer treated by stereotactic radiotherapy.
Legal agreements, policies, templates, assessment and other legal documents	Foreground	TLX	5	All	No	N/A	N/A	Any legal documents or written advice produced in relation to the project work
A secure federated framework for camera attribution and processing encrypted multimedia content	Background	UVIGO	2	T2.1, T2.2, T2.3 and T2.5	No	N/A	N/A	<ul style="list-style-type: none"> - Specific restrictions and/or conditions for implementation: UVIGO will grant a royalty-free user license on a strict “need-to-know” basis to those TRUMPET partners that demonstrate the need for the purpose of the implementation of their tasks. This non exclusive license will be limited to the strict time necessary. No sub-licensing will be allowed. - Specific restrictions and/or conditions for Exploitation: Necessary access will be granted under fair and reasonable conditions

<p>A simulation tool for neural network training and encrypted average aggregation based on multi-key homomorphic encryption</p>	Background	UVIGO	2	T2.1, T2.2, T2.3 and T2.5	No	N/A	N/A	<p>- Specific restrictions and/or conditions for implementation: UVIGO will grant a royalty-free user license on a strict "need-to-know" basis to those TRUMPET partners that demonstrate the need for the purpose of the implementation of their tasks. This non exclusive license will be limited to the strict time necessary. No sub-licensing will be allowed.</p> <p>- Specific restrictions and/or conditions for Exploitation: Necessary access will be granted under fair and reasonable conditions</p>
---	------------	-------	---	---------------------------	----	-----	-----	--

<p>An FL-tailored Multi-Key Homomorphic Encryption (MKHE) scheme and a baseline implementation for private average aggregation. The solution consists of a lattice-based MKHE scheme specifically designed for the average aggregation primitive widely used in federated learning. It includes a full description of the required security assumptions, building blocks, and protocol algorithms. The solution also provides several protocol versions offering different computation/communication trade-offs, along with algorithms for selecting suitable scheme parameters to optimize efficiency and security.</p> <p>An academic implementation of the protocol steps is available. It utilizes the Lattigo library (specifically, the low-level 'ring' and 'utils' packages from Lattigo v5.0.2) for cryptographic primitives, incorporating several optimizations for parallelization in Golang. The tailored MKHE scheme guarantees privacy under a semi-honest aggregator and does not require a public-key infrastructure. Moreover, it is naturally secure against all recent attacks proposed under the new IND-CPA-D security definition for modern HE schemes. To fully ensure privacy against any dishonest data owner, it must be combined with Differential Privacy (DP) or other techniques that measure leakage in the aggregated updates. Finally, the scheme can be upgraded to handle malicious aggregators with negligible overhead compared to the semi-honest version.</p>	<p>Foreground</p>	<p>UVIGO</p>	<p>2</p>	<p>T2.1, T2.2, T2.3, T2.4 and T2.5</p>	<p>No</p>	<p>N/A</p>	<p>N/A</p>	<p>- Specific restrictions and/or conditions for implementation: UVIGO will grant a royalty-free user license on a strict "need-to-know" basis to those TRUMPET partners that demonstrate the need for the purpose of the implementation of their tasks. This non exclusive license will be limited to the strict time necessary. No sub-licensing will be allowed.</p> <p>- Specific restrictions and/or conditions for Exploitation: Necessary access will be granted under fair and reasonable conditions</p>
<p>Clinical datasets</p>	<p>Background</p>	<p>IRST</p>	<p>4</p>	<p>T4.1</p>	<p>No</p>	<p>N/A</p>	<p>N/A</p>	<p>A set of clinical data for the treatment and follow-up of cancer patients in the following indications: head and neck cancer, advanced NSCLC patients treated with immunotherapy alone or in combination with chemotherapy during their first-line of therapy collected according the applicable clinical guidelines.</p>

Study datasets	Foreground	IRST	4	T4.1	No	N/A	N/A	Curated, cleansed and consolidated datasets for the treatment and follow-up of cancer patients in the following indications: head and neck cancer, advanced NSCLC patients treated with immunotherapy alone or in combination with chemotherapy during their first-line of therapy
----------------	------------	------	---	------	----	-----	-----	--

Annex 2. List of KERs

Trumpet Project Results

TRUMPET Project Results											
No	WP	Name of Results	Description	Type	KER? (does result have a high potential?)	If yes, Description of the High Potential	Market Maturity	Individual / Joint Result	Owner	Will owner exploit the result?	Access for partners and/or 3rd parties
1	2	PET:MKHE	Solution for the execution of a private aggregation protocol based on the use of secret multi-key homomorphic encryption	Other	High tech, business or economic potential	MKHE enables secure aggregation of encrypted data without the need for decryption at the aggregator, offering strong privacy guarantees especially for sectors requiring strict confidentiality (e.g., health, finance). It is adaptable to different FL topologies and supports future-proof data protection strategies.	Emerging: growing demand, scarce supply	Individual	UVIGO, GRAD	Yes	Licensing
2	2	PET: CDC+DP	PET based on the Coded Distributed Computing with Differential Privacy, ensures privacy-preserving model aggregation through a structured workflow that maintains consistency across all DO.	Other	High tech, business or economic potential	CDC+DP combines privacy and fault tolerance in distributed model aggregation. Its structured nature makes it scalable and adaptable for federated deployments involving many nodes.	Emerging: growing demand, scarce supply	Individual	GRAD	Yes	Licensing

3	4	FL Core	The FL Core is the central component where model training occurs, communication between nodes is managed, and PETs are integrated to protect sensitive data. It is responsible for coordinating training rounds, aggregating model updates, and ensuring efficient data exchange while maintaining security and scalability.	Other	High tech, business or economic potential	The FL Core is domain-agnostic and can be applied in any sector requiring federated privacy-preserving machine learning, such as healthcare, finance, mobility, or manufacturing. Its modular and scalable architecture enables integration with various PETs, positioning it as a strong candidate for commercialization or integration into existing AI platforms across industries.	Emerging: growing demand, scarce supply	Individual	GRAD	Yes	Licensing
4	3	Inference attacks	Membership inference attacks (attacks that aim to determine whether a specific data point was used to train a model) and attribute inference attacks (attacks that aim to reveal some sensitive attribute of data points used to train a model). Obtaining this knowledge about one of the private datasets of DO violates the primary privacy goal of this paradigm, which is to protect training data by keeping it private	Other	High societal potential (non climate and enviro)	Inference attacks highlight critical privacy vulnerabilities in federated learning. Understanding and demonstrating these attacks is essential for developers, policymakers, and regulators to design proper mitigations and ensure compliance with GDPR and other data protection regulations. These insights can inform guidelines, certifications, and auditing frameworks.	Emerging: growing demand, scarce supply	Individual	GRAD	Yes	
5	4	TRUMPET PLATFORM AND DASHBOARD FOR USERS	The TRUMPET platform is a privacy-preserving Federated Learning system designed to enable secure and GDPR compliant healthcare data analysis without sharing sensitive patient information	Product	High societal potential (non climate and enviro)	The platform is an integrated FL solutions that combines technical privacy guarantees with regulatory oversight. It can serve hospitals, research institutions, and med-tech companies looking for compliant, secure Federated AI solutions. Its modular design makes it easy to adapt for other sectors (e.g., finance, industry etc...), providing high exploitation potential.	Emerging: growing demand, scarce supply	Joint	AVO, TVS, GRAD	Yes	Open access

6	2	Multi-Secret-Key Homomorphic Encryption Protocol for Secure Aggregation	UVIGO has designed and implemented a novel secure aggregation protocol for Federated Learning (FL) based on Multi-Secret-Key Homomorphic Encryption (MKHE). Unlike threshold or multiparty HE schemes, each data owner encrypts with its own secret key, and yet the encrypted updates can be aggregated directly. Decryption requires collaboration (version-1) or can be performed more efficiently through masked aggregation (version-2), significantly reducing communication costs. The implementation is openly available under an Apache license at https://github.com/apedrouzouloa/mkagg and has been validated through extensive performance benchmarks.	Method	High scientific potential	The MKHE-based aggregation protocol supports practical deployment of secure FL in sensitive domains such as healthcare, finance, or cross-institutional collaborations. By combining strong security guarantees (based on RLWE) with reduced communication overhead, it lowers the barrier for industrial adoption. Its open-source implementation further enhances reusability and accelerates technology transfer.	Emerging: growing demand	Individual	UVIGO	Yes	Open source
7	3	Privacy metrics and attacks based on Mutual Information	UVIGO has developed a theoretical and practical framework for privacy evaluation in Federated Learning (FL), leveraging Mutual Information (MI) as a rigorous measure of privacy leakage. This approach quantifies the dependency between shared gradients and underlying sensitive data. Additionally, UVIGO has designed and implemented membership inference attacks to empirically validate the strength and applicability of the proposed metrics.	Method	High scientific potential	The framework allows both researchers and technology integrators to objectively evaluate privacy leakage risks in FL. Its adoption supports the certification of compliance with privacy standards and enables the benchmarking of different defense mechanisms (e.g., Differential Privacy, Homomorphic Encryption, etc.). The framework not only defines rigorous information-theoretic privacy metrics but also establishes a direct connection with the ENISA methodology for assessing data breaches. This integration bridges theory and practice by linking	Emerging: growing demand	Individual	UVIGO	Yes	Secret/Non-disclosure agreement

						Mutual Information–based metrics with the severity estimation of privacy leakage in real FL deployments. This unique contribution from UVIGO enhances the regulatory impact of the tool, positioning it as a reference framework for GDPR compliance and European data protection standards.					
8	3	Tool for measurement and validation of privacy	A dedicated framework designed to assess and ensure the privacy and security of Federated Learning systems, providing compliance with GDPR and robust protection against data leaks	Product	High policy or regulatory potential	This tool addresses a critical gap in federated learning deployments by enabling quantifiable, repeatable, and regulatory-aligned privacy assessments. It can be used by any FL solution provider to demonstrate compliance and trust, making it a highly valuable asset in sectors like health, finance, and public data services.	Emerging: growing demand, scarce supply	Joint	UVIGO, GRAD, INRIA	Yes	Licensing

9	5	<p>Legal know-how on the development and operation of a state-of-the-art FL platform for medical purposes in a privacy preserving way</p>	<p>With respect to the legal and ethical findings, the crucial exploitable output is the legal know-how on the development and operation of a state-of-the-art federated learning (FL) platform for medical purposes in a privacy preserving way. In particular, the understanding of the legal roles and responsibilities, the relevant challenges and tools available to mitigate data protection issues – including techniques for data pseudonymization and anonymization and other privacy enhancing technologies (PETs), such as federated learning – are invaluable in any medical data sharing contexts. The lessons learned in TRUMPET will be readily reusable in other initiatives through the development of a regulatory acceptance plan that takes into account all relevant guidance from data protection and cybersecurity authorities and adjusts it to the requirements of an environment that involves the processing of sensitive data. More specifically, this know-how can be re-used in other contexts and sectors, notably towards data providers (hospitals, biobanks, research organizations and companies), data intermediaries and data users, that deploy or rely on data. As Timelex provides legal services to all of these categories of</p>	Method	High policy or regulatory potential	<p>This know-how can be re-used in other contexts and sectors, notably towards data providers (hospitals, biobanks, research organizations and companies), data intermediaries and data users, that deploy or rely on data. As Timelex provides legal services to all of these categories of stakeholders, it can further use, exploit and disseminate this know-how. Further to the regulatory acceptance plan, this can be done through e.g. data use policies, platform use terms, data protection impact assessments, privacy policies, layered information notices and so forth, all of which have direct exploitable value.</p>		Individual	Timelex	Yes	Open access
---	---	--	--	--------	-------------------------------------	---	--	------------	---------	-----	-------------

stakeholders, it can further use, exploit and disseminate this know-how. Further to the regulatory acceptance plan, this can be done through e.g. data use policies, platform use terms, data protection impact assessments, privacy policies, layered information notices and so forth, all of which have direct exploitable value.

Exploitation Strategy

KER No	Use	Target group 1	Target group 2	Steps for exploitation	Other exploitation steps	Access Rights	Background IP	Require access to Background of partners?	If YES, which Background?	Require access to another KER of one or several partners?	If YES, which KER?	Partners interested in Exploitation	Does the exploitation of the KER require THIRD PARTY IPR?	If YES, describe the measures taken/envisaged to get access to required IP	Expected IPR Measures
1	Other	Researchers	sensitive industry, data controllers	Pilot, demo or testing	PETRAI application	Restricted/Private	N/A	No	N/A	Yes	FL core	No	No	N/A	
2	Other	Researchers	federated learning platforms, data controllers	Pilot, demo or testing	PETRAI application	Restricted/Private	N/A	No	N/A	Yes	FL core	No	No	N/A	
3	Other	Researchers	Industry, business partners	Market study	PETRAI application	Restricted/Private	N/A	No	N/A	No	N/A	No	No	N/A	
4	Other	Researchers	Policy-makers and authorities	demo or testing	Market study	Restricted/Private	N/A	No	N/A	No	N/A	No	No	N/A	

5	Other	Researchers	Industry, business partners	Market study	PETRAI application	Restricted/Private	N/A	No	N/A	Yes	PETs, privacy measurement	AVO, TVS	No	N/A	
6	Licensing (indirect use)	Industry	Researchers	demo or testing		Open/Public	Apache-licensed open-source software (UVIGO). Published scientific paper (CSR 2023).	No	N/A	No	N/A	UVIGO (lead), with potential exploitation by technology providers and federated learning platform developers.	No	N/A	Copyright
7	Other	Researchers	Regulators and standardization bodies	demo or testing		Restricted/Private	N/A	No	N/A	No	N/A	UVIGO	No	N/A	Copyright
8	Other	Researchers	Policy-makers and authorities	Other		Restricted/Private	N/A	No	N/A	No	N/A	No	No	N/A	
9	Other	Policy-makers and authorities		Other	Publications, workshops, engagement with other EU-funded research projects and representatives from regulatory authorities	Open/Public	N/A	No	N/A	No	N/A	TIMELEX	No		Copyright

Risk Management

No	Barriers & Risks (market-related)	Proposed Mitigation Measures
1	High computational overhead	Optimize encryption and aggregation routines
2	trade-offs between accuracy and privacy	Performance benchmarking with adjustable privacy budgets
3	High technical entry barrier; Limited awareness of FL in target sectors	Targeted dissemination to strategic partners in key sectors
4	Lack of clear regulatory guidance on how to assess and address inference attacks in federated and decentralized contexts.	Engage with data protection authorities and standardization bodies to translate attack scenarios into compliance frameworks or checklists.
5	Interoperability challenges with existing hospital IT infrastructure	Develop FHIR-compatible modules; provide integration toolkits and technical support during deployment;
6	Need for careful parameter tuning to ensure both security and efficiency. Limited awareness and expertise among end-users in deploying HE-based solutions.	Optimize protocol design and provide benchmarks for practical scenarios. Offer clear guidelines for parameter selection and secure deployment. Dissemination through publications, open-source code, and training workshops.
7	Lack of international standardization of privacy metrics in FL. Potential reluctance from providers to integrate metrics that expose vulnerabilities in their models.	Active contribution to standardization bodies (IEEE, ENISA). Release of reference software under open academic license to foster adoption and transparency. Training and dissemination among clinical and industrial partners.
8	Privacy validation in FL is not yet standardized	contribute to standardization bodies and ensure ongoing updates to the tool based on evolving legal frameworks
9	Changing legal frameworks affecting project results	Dedicated WP monitoring the evolving legal frameworks during the entire duration of the project. This ensures that at the end of the project the produced results are up to date and clearly outline the relationship among the applicable legislative frameworks and the requirements to comply with in each of those.