Co-funded by the European Union

Strengthening Security Through EU-funded Research & Innovation: **Advancing Border and Forensic Capabilities**

Joint insights from the Horizon Europe security research projects:

FLEXI-cross, TENSOR, ODYSSEUS, and TENACITy

Joint Report, August 2025

FLEXIcross TENSOR ODYSSEUS TENACITy

Abstract

This document presents key insights from four EU-funded projects—**FLEXI-cross, TENSOR, ODYSSEUS, and TENACITy**—working on border management, travel security, and law enforcement intelligence support. It highlights common challenges, lessons learned, and gaps identified across technical and operational implementations.

This joint report serves as a roadmap for policymakers, security practitioners, industry stakeholders, and technology experts, fostering a more secure and intelligent approach to border management and law enforcement.

Authors

FLEXI-cross Authors

Giuseppe Vella – Engineering Ingegneria Informatica S.p.A. (ENG)

Marco Paleari – Engineering Ingegneria Informatica S.p.A. (ENG)

Maria Giuseppa Guella – Engineering Ingegneria Informatica S.p.A. (ENG)

Chrostos Bolakis – Kentro Meleton Asfaleias (KEMEA)

Thomas Azrak – Ebos Technologies Limited– (EBOS)

TENSOR Authors

Eleni Veroni – Netcompany S.A.

Spyridon Evangelatos – Netcompany S.A.

Apostolos Apostolaras – Centre for Research and Technology, Hellas (CERTH)

Katerina Kyriakou – Centre for Research and Technology, Hellas (CERTH)

Thanasis Korakis – Centre for Research and Technology, Hellas (CERTH)

Patrik Gonçalves – Central Office for Information Technology in the Security Sector (ZITiS)

Tabea Rosenkranz – Central Office for Information Technology in the Security Sector (ZITiS)

Claudia Mertinger – Fsas Technologies GmbH

ODYSSEUS Authors

Monica Florea – Software Imagination & Vision Romania (SIM)

Dana Oniga– Software Imagination & Vision Romania (SIM)

Diana Antonescu – Software Imagination & Vision Romania (SIM)

Dimitris Kassimis – TELESTO TECHNOLOGIES PLIROFORIKIS KAI EPIKOINONION EPE (TEL)

Martin David – THALES DIS CZECH REPUBLIC SRO (THALES)

Harry Kellett – RAPISCAN SYSTEMS LIMITED (RAPI)

TEANCITy Authors

Chrysostomos Antoniou – European Dynamics Luxembourg SA (ED)

Christiana Aposkiti – Kentro Meleton Asfaleias (KEMEA)

Mirela Rosgova – Kentro Meleton Asfaleias (KEMEA)

Deborah Manzi – Universita Cattolica Del Sacro Cuore (UCSC-TC)

Celia Calus – Nutcracker Research Malta Ltd (NMT)

Rodoula Makri – Institute Of Communication & Computer Systems (ICCS)

Credits

Design by Netcompany S.A.

Table of Contents

1. Brief introduction of the four projects

1.1. FLEXI-cross introduction

The FLEXI-cross project aims to increase security and reliability of EU border checks for people and goods through the development, deployment and validation of a toolkit of innovative border-checking solutions.

The resulting flexibility and dynamicity of border check planning will offer novel capabilities such as the dynamic deployment of checkpoints and support via mobile applications for border personnel while guaranteeing a high level of security, privacy of personal data and protection of people's fundamental rights.

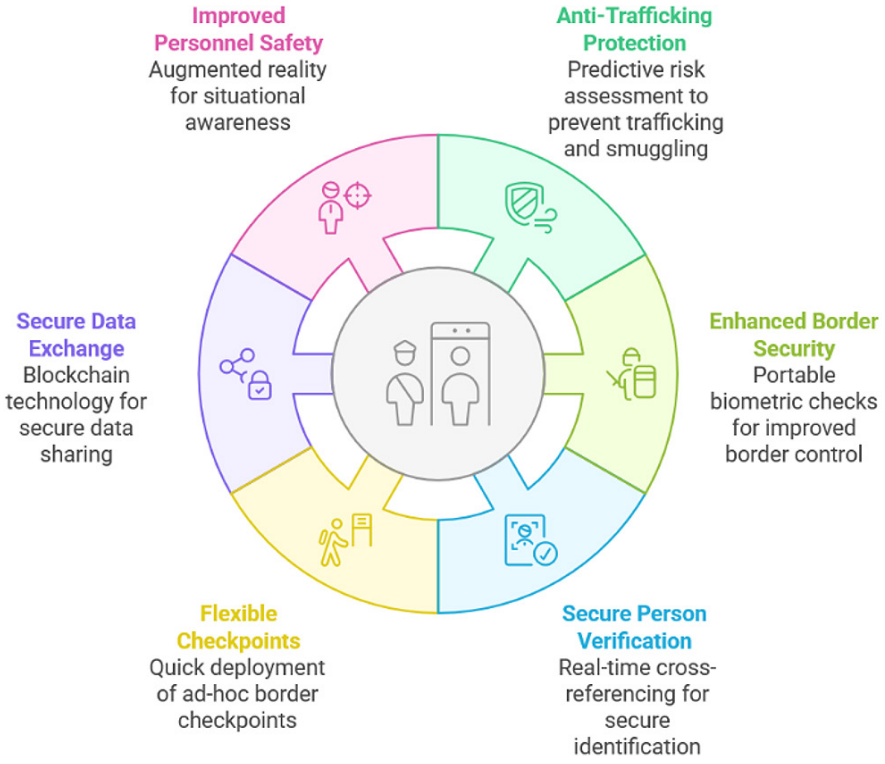

Figure 1: FLEXI-cross outcomes

Foreseeable Outcomes:

- anti-trafficking and anti-smuggling protection via predictive risk assessment of vehicle and people
- enhanced border security through portable biometric-based checks
- secure person verification through real-time multi-source cross-referencing
- flexible, fast and cost-effective deployment of ad-hoc Border Check Points
- secure, private and traceable sensitive / personal data exchange based on blockchain technology
- increased safety and improved experience for border personnel based on advanced Human Machine Interfaces and enhanced situational awareness via Augmented Reality

1.2. TENSOR introduction

The TENSOR project aims to revolutionize the way Law Enforcement Agencies (LEAs) across Europe identify suspects and combat serious crime and terrorism. In an era of increasingly sophisticated threats and fragmented investigative workflows, TENSOR provides innovative, AI-powered solutions for the extraction, analysis, storage, and secure cross-border sharing of biometric evidence.

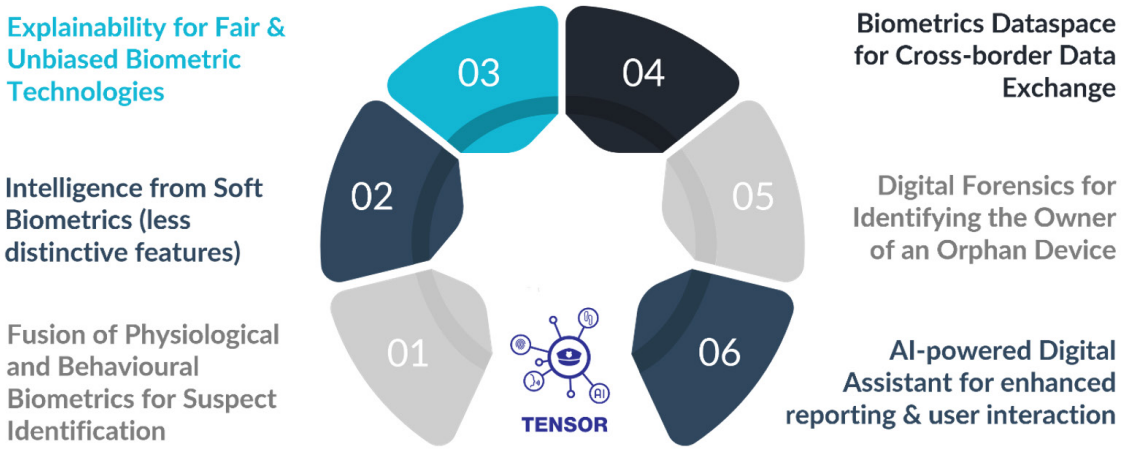

Figure 2: TENSOR outcomes

Foreseeable Outcomes:

- **Fusion of Physiological and Behavioural Biometrics:** Advanced multi-modal biometric identification system that supports law enforcement agencies in identifying suspects for combating crime and terrorism more effectively. The platform integrates a broad spectrum of biometric modalities, combining well-established methods, such as fingerprints and facial recognition, with emerging behavioural biometrics, including gait recognition (based on unique walking patterns) and keystroke dynamics (based on typing behaviour such as timing, rhythm, and pressure).
- **Intelligence from Soft Biometrics:** Derives a rich set of soft biometric traits, such as age, gender, body proportions, and language use, from multiple modalities to enrich suspect profiling and support cross-checking when hard biometric matches are unavailable.
- **Explainability for Fair and Unbiased Biometric Technologies:** Embedded explainability mechanisms and expert-in-the-loop workflows, enhancing the system's decision-making pipeline.
- **Biometrics Dataspace:** Enables suspect identification in transnational cases by performing secure biometric data matching (e.g., facial images, voiceprints, fingerprints) across jurisdictions without exposing sensitive information. Built on IDSA data space technology, TENSOR uses privacy-enhancing technologies like homomorphic encryption to preserve privacy during processing, and blockchain-based smart contracts for automated access control and lawful data use.
- **Digital Forensics:** Develops methodologies for extracting data of interest (e.g., app usage patterns, location traces, configuration data from health apps, media files, text messages, etc.) from seized mobile devices, bypassing the inherent encryption mechanisms.

- **AI-powered Digital Assistant:** Features an AI-powered Digital Assistant to support investigators, which consolidates biometric identification results into structured, natural language reports. Through a chat-based interface, the assistant explains how TENSOR's technologies work, helps users navigate the platform, and provides step-by-step guidance for key investigative tasks.

1.3. ODYSSEUS introduction

ODYSSEUS project represents a forward-looking response to the complex challenges European border management is facing. Funded under the Horizon Europe programme, ODYSSEUS is developing an integrated, and ethical border control platform that leverages cutting-edge technologies such as artificial intelligence (AI), machine learning (ML), and advanced biometric systems. Its mission is to enhance the security, efficiency, and scalability of border operations while respecting fundamental rights and ensuring compliance with EU regulations.

As migration pressures rise and security threats evolve, border authorities are confronted with the dual challenge of maintaining operational effectiveness and respecting privacy and individual rights. ODYSSEUS addresses this by designing solutions that are unobtrusive, user-friendly, and adaptable to diverse border contexts—land, sea, and train. Through the deployment of UAV-assisted vehicle scanning, AI-based risk assessment engines, multi-sensor data fusion, and digital travel credentials, ODYSSEUS platform provides a comprehensive framework for next-generation border control.

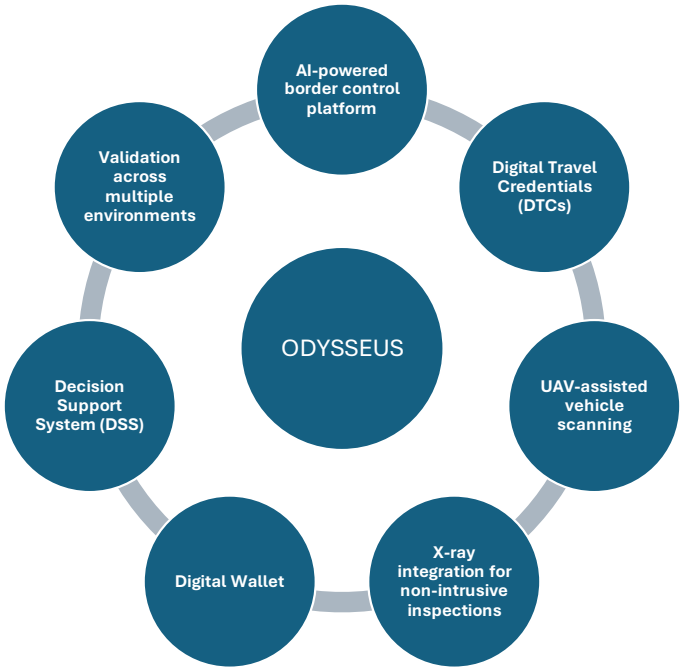

Figure 3: ODYSSEUS outcomes

Foreseeable Outcomes:

The ODYSSEUS project will deliver a series of innovative results that contribute to the future of secure, efficient, and ethical border management across the EU. Key outcomes include:

- **AI-powered border control platform:** A modular and scalable solution that integrates biometric verification, risk assessment, and surveillance into a unified system.
- **Digital Travel Credentials (DTCs):** Implementation of secure and privacy-respecting credentials that facilitate faster and more reliable traveller identification.
- **UAV-assisted vehicle scanning:** Deployment of unmanned aerial vehicles for license plate recognition, occupancy detection, and anomaly identification, enhancing situational awareness without disrupting traffic flow.
- **X-ray integration for non-intrusive inspections:** Use of AI to interpret high-resolution X-ray images for vehicle and train screening, detecting threats or contraband in real-time.
- **Digital Wallet:** A secure platform for travellers to manage and share personal and travel-related documentation, supporting GDPR compliance and minimizing manual checks.
- **Decision Support System (DSS):** A tool that synthesizes multi-source data to support real-time decision-making and risk profiling by border authorities.

Validation of these innovative solutions for border crossing systems at European level will improve the border crossing experience for travellers and for border guards. The evaluation and testing of the ODYSSEUS platform are performed in land, sea, and rail scenarios, demonstrating flexibility and real-world applicability for EU internal and external borders.

The security and reliability of border checks will be increased through new solutions of identification of people and goods crossing external borders, while protecting people's fundamental rights and personal data.

These outcomes will collectively support a more resilient, interoperable, and citizen-centric border management approach aligned with EU regulations and its strategic objectives.

1.4. TENACITy introduction

Law Enforcement Agencies (LEAs) across Europe rely on data from their information systems to make critical decisions that ensure the safety of European citizens. However, a recent report from the European Court of Auditors has revealed inconsistencies in how individual countries manage and utilize data. Differences in perception and methodology have led to incomplete, inaccurate, and outdated datasets being used by LEAs, with some countries not fully leveraging the central EU systems due to regulatory and "cultural" barriers. The TENACITy project aims to address these challenges through a comprehensive three-pillar approach. Firstly, it proposes modern and effective tools for travel intelligence data utilization, building an interoperable open architecture that integrates and analyses multiple transactional, historical, and behavioural data from diverse sources. By leveraging cutting-edge digital technologies, such as machine learning, AI, blockchain, and distributed ledger technologies, TENACITy ensures secure and trusted information sharing between authorities. Secondly, it emphasizes the training and sensitization of LEAs' personnel by establishing a living lab to organize hackathons, workshops, and interactive sessions for stakeholders, fostering knowledge exchange and practical application of the proposed digital tools. Finally, TENACITy envisions a holistic approach to crime prevention through the development of a Travel Intelligence Governance Framework that balances security with fundamental rights. By involving citizens, civil actors, and policymakers, the project addresses legal, ethical, and societal concerns while strengthening security measures against criminal and terrorist organizations.

Foreseeable Outcomes:

- **Advanced Travel Intelligence Utilization**: Game-changing technologies to exploit global travel intelligence data, using machine learning and AI to extract patterns and eliminate irrelevant data. These technologies provide updates about potential threats, the trends of enterprises of crime and will thus strengthen their intelligence, analytic capacity and decision-making.
- **Trusted and Secure Information Sharing**: Utilization of blockchain and distributed ledger technologies to securely share encrypted data among authorities, enabling transparent and traceable information exchange while protecting sensitive data.
- **Enhanced Decision-Making for Security Authorities**: Real-time analytics and risk management algorithms consolidate data from various sources, boosting intelligence capacity and providing updates on emerging threats and criminal trends.
- **Dynamic Training and Stakeholder Engagement**: Continuous training programs for law enforcement agencies (LEAs) through living labs, workshops, and hackathons to ensure thorough understanding and application of travel intelligence. Promotes collaboration and knowledge exchange among stakeholders. **Holistic Crime Prevention Approach**: Development of a Travel Intelligence Governance Framework to address legal, ethical, and societal concerns. Involves citizens, policymakers, and civil actors in shaping regulations to balance security with fundamental rights.

2. Challenges

2.1. Challenge 1: Biometric on the Move for seamless border crossing

The capabilities to capture and use the biometrics of travellers without them having to stop and in natural contexts for border checks, in full respect of fundamental rights and considerations to safeguard data and integrity, are crucial aspects linked to the border crossing system innovation.

New initiatives to accelerate the border crossing process are launched every year, introducing emerging technologies besides the established biometric methods, such as face recognition, since it is nonintrusive, fast, easy to use, and cost-effective. On the other hand, face recognition/identification, particularly in open environments and uncontrolled conditions, is a highly challenging task due to diverse variations of face appearance, face sizes, cluttered and complicated backgrounds, etc. and due to technical challenges, such as blurriness, low resolution, and acquisition conditions. An additional challenge is the efficient verification of travel documents in the case of minors, as their biometric features change rapidly until adulthood, thus making it impossible to verify the legal guardianship between them and the people accompanying them.

To address the above challenges, the FLEXI-cross project implements diverse biometrics-solutions in the respective trial sites. A two-step approach has been followed for the construction of a deep feature representation database. The first step applies Face Detection and Face alignment techniques based on deep Convolutional Neural Networks (CNNs), while the second utilises face embedding learning and deep face feature extraction.

Special emphasis has been given in increasing the accuracy and trustworthiness of the results, the usability and adaptation of the solution to real operational border environments. 5G connected portable devices will be used for multimodal biometrics to allow Law Enforcement Agencies (LEAs) to verify anyone in their territory with different databases in real time. Machine learning will be used to improve the system for the effective detection of people crossing borders.

2.2. Challenge 2: Unobtrusive technologies for border crossing facilitation of people and goods

One of the main challenges concerning EU external borders in 2024 was the irregular migration according to the latest "Annual Risk Analysis 2024/2025" published by Frontex in July 2024[1]. Even if the "Annual brief for 2024" issued by Frontex in February 2025 states that detections of illegal border-crossing on entry at the EU's external borders decreased by 38% compared in 2024 compared with 2023[2], the irregular migration remains a risk for the EU border management.

Another big challenge at EU external borders is detecting illegal activity without creating delays for other travellers, i.e. detecting false documents or smuggling illegal goods.

ODYSSEUS solutions are meant to support border guards' authorities to fight these challenges, while ensuring a smooth crossing for travellers across land borders- on the road and on railway and on sea borders of EU.

1 Annual Risk Analysis 2024/2025, Frontex, July 2024.

2 Annual brief for 2024,Frontex,February 2025.

2.3. Challenge 3: Modern biometric technologies in forensic science for enhanced suspect identification

The core challenge addressed by the TENSOR project lies in the effective integration of modern biometric technologies into forensic processes to enhance suspect identification in line with the evolving operational demands of law enforcement. Although biometric identification technologies have advanced significantly in recent years – largely through the application of AI – Law Enforcement Agencies (LEAs) continue to face practical barriers to their seamless adoption. TENSOR tackles this issue by delivering advanced suspect identification capabilities through an innovative multi-modal biometric fusion approach. This includes facial, voice, fingerprint, and gait recognition, along with behavioural patterns derived from mobile device usage. These diverse biometric modalities are intelligently combined and interpreted to reflect the real-world investigative contexts and time-sensitive scenarios in which LEAs operate.

More specifically, TENSOR aims to equip Police Authorities with advanced, explainable, and actionable insights, enabling them to make lawful and well-informed decisions. This responds to the growing demand for enhanced forensic capabilities and lawful evidence collection, supporting the apprehension of criminals and the presentation of robust biometric evidence in court. By emphasizing explainable AI and human-in-the-loop mechanisms, TENSOR promotes transparency and accountability in biometric analysis, avoiding the risks of black-box decision-making while remaining aligned with European legal and ethical standards.

Finally, TENSOR further contributes to the prevention, detection, and deterrence of various forms of crime by facilitating suspect identification through the analysis of behavioural data linked to the owners of mobile devices associated with criminal activity. The platform's ability to integrate fragmented and heterogeneous data sources enhances situational awareness for LEAs, enabling them to more effectively combat organized crime. By doing so, TENSOR contributes to the security of EU citizens through timely, reliable, and precise identification of suspects.

2.4. Challenge 4: Travel intelligence applied to FCT

The increasing pressure at the EU borders caused by recent security and migratory challenges has led to substantial investments in EU Information Systems. Additionally, Member States significantly contribute to the development and maintenance of their national systems. Despite these investments, the systems face several challenges that hinder their effectiveness in combating crime and terrorism.

One of the most critical challenges in utilizing travel intelligence effectively is ensuring the accuracy and quality of data within the information systems. Various national law enforcement agencies (LEAs), customs, visa, and judicial authorities are responsible for processing data, but data quality remains inconsistent. Incomplete or inaccurate data, as well as delays in data transfer from various sources, severely compromise the reliability of the systems. Furthermore, discrepancies in data collection practices among Member States aggravate the problem, as there is no unified standard for data accuracy and completeness. As a result, the proliferation of false positives not only wastes valuable resources but also risks overlooking crucial information that could help identify criminal networks and potential threats.

Another major obstacle is the decentralized nature of some travel intelligence systems, such as the Passenger Name Record (PNR) system. Unlike centrally regulated systems, PNR was established

through a directive rather than a regulation, giving Member States the flexibility to develop their own national implementations. This lack of a unified European platform has resulted in significant variability in the system's functionality and data availability. Consequently, the limited integration of PNR with other intelligence systems weakens the overall travel intelligence framework and diminishes the ability of authorities to identify high-risk individuals crossing EU borders.

Legal and regulatory inconsistencies across Member States present additional challenges. The PNR Directive (EU) 2016/681 requires each Member State to establish a Passenger Information Unit (PIU) to collect, process, and exchange PNR data. However, differences in data protection, storage, and disclosure regulations between Member States have led to fragmented implementation and limited data exchange capabilities. Cultural resistance to sharing sensitive data and the absence of standardized legal frameworks further exacerbate this issue. Such barriers not only hinder cross-border cooperation but also compromise the operational efficiency of the entire travel intelligence ecosystem.

The surge in data volume has also created significant processing and analytical challenges. This rapid growth has strained the processing capabilities of national and EU-level systems, leading to delays and suboptimal analyses. Border guards often find themselves in situations where they must make critical decisions without consulting the systems to avoid long waiting times and ensure smooth border control operations.

To address these challenges, the TENACITy vision was introduced as a Travel Intelligence Governance Framework that adopts a holistic approach to crime prevention. By leveraging advanced technologies via sophisticated tools and addressing societal, legal, and ethical concerns, TENACITy aims to enhance data quality, standardize system interoperability, and promote effective governance practices. Strengthening cooperation among Member States and harmonizing data management protocols are crucial steps to realizing the full potential of travel intelligence in crime and terrorism prevention.

3. Use cases on AI applied to Biometric Authentication, Travel intelligence, and goods and people crossing borders

3.1. FLEXI-cross use cases

The FLEXI-cross project aims to enhance border security and efficiency through the integration of advanced mobile and AI-driven technologies across three critical border-crossing scenarios: port-based, road-based, and rail-based trials.

The project is designed to modernise and optimise border control operations through the following overarching objectives:

- **Enhancing Security** by deploying AI, biometric authentication, and real-time monitoring technologies.
- **Increasing Efficiency** by integrating mobile and digital solutions to streamline inspection procedures.
- **Ensuring Data Interoperability** by consolidating information from multiple systems into a unified framework.
- **Ethical and Regulatory Compliance** by aligning AI-driven solutions with strict data protection and non-discrimination guidelines.

While each use case is tailored to its specific operational environment, they share these common goals.

1. Port-Based Border-Crossing Trial

The port-based trial at the Port of Galati focuses on strengthening security at one of Romania's most strategically significant triple-modal ports. This use case integrates high-performance mobile solutions with existing systems to improve the detection of high-risk individuals and dangerous goods. The deployment of AI-driven biometric recognition, drones, fixed cameras, radiation sensors, and acoustic analysis enhances monitoring capabilities while ensuring compliance with ethical standards in surveillance and data processing.

Key innovations include:

- Enhanced detection of illicit materials and unauthorised individuals through multimodal verification tools.
- Improved data integration from various sensors and control systems.
- Reduced inspection times while maintaining high-security standards.

2. Road-Based Border-Crossing Trial

The Ormenio border crossing between Greece and Bulgaria focuses on increasing the efficiency of vehicle and pedestrian processing. This use case integrates deployable mobile inspection technologies with legacy border control systems to streamline operations and mitigate detection delays.

Key innovations include:

- The introduction of biometric authentication and road-side cameras for identity verification.
- Digitisation of traveller validation processes to enhance security and reduce human workload.
- Improved data integrity and interoperability between multiple sources.
- Automated detection of irregular activities in real time, ensuring rapid response to potential threats.

3. Rail-Based Border-Crossing Trial

The rail-based use case at the Romanian-Moldova border is designed to modernise and digitise border control for both passengers and cargo, with a strong emphasis on combatting child trafficking. By leveraging blockchain technology and multimodal biometric identification, the trial enhances document authenticity and ensures real-time verification.

Key innovations include:

- Integration of portable 5G-connected devices for seamless checks against multiple databases.
- Deployment of acoustic detection and ionising radiation sensors to identify security threats.
- Streamlined processes to minimise delays in rail transport while maintaining strict security measures.

3.1.1. Preliminary results

The FLEXI-cross project has successfully developed and tested key technologies across all use cases, focusing on risk analysis, visual analytics, and data interoperability with EU and non-EU border control systems. A unified event generation system, using a CISE-like format, enables the assessment of detection, anomalies, and risk across different BCPs.

In **UC1 (port-based)**, we developed technologies such as mobile-based facial recognition (identification and verification), object detection for dangerous materials and vessel identification, acoustic sensing, positioning, and drone-based unusual pattern extraction. This use case also integrates two real-time monitoring tools: an augmented reality system and a geo-temporal, event-driven situational awareness platform, enhancing BCP awareness.

In **UC2 (road-based)**, facial and vehicle recognition were implemented alongside connectivity with legacy systems, road-side units, and on-board sensors. This use case offered the opportunity to fully develop an On-Board Unit (OBU) hardware that monitors vehicle parameters and may help detect illicit activities and unusual driving patterns.

In **UC3 (rail-based)**, advancements include mobile-based facial recognition (identification and verification), blockchain-based cargo tracking, acoustic and radiation sensors, position prediction, and phone-based passport reading.

Security constraints have limited full integration within existing BCP systems, but strong collaboration with border authorities has provided crucial insights and support. Within UC2, we have already tested systems in the real environment and interoperability with legacy BCP systems such as the Greek fingerprint and passport scanners; UC1/UC3 were mostly validated in controlled settings.

The final trials in Spring 2025 will be a key milestone in evaluating FLEXI-cross's impact.

3.1.2. Lessons learnt

As part of the FLEXI-cross project, a live and physical demonstration was conducted to test the developed tools, focusing on the mature modules that had already been implemented and integrated. This demonstration provided valuable hands-on experience for both technical and end-user partners, offering insights into the effectiveness, usability, and challenges of the developed solutions.

To systematically assess the experiences gained throughout the project, a survey/questionnaire was distributed to consortium partners. The assessment was divided into two key groups:

1. **Technology Partners** – Responsible for developing and integrating the necessary tools into a final toolkit.
2. **End Users (Border Control Personnel - BCPs)** – The actual personnel who will utilise the toolkit's functionalities to enhance border security while improving operational efficiency.

The survey findings provided important lessons regarding technical challenges, operational constraints, and user engagement, which are summarised below.

Q5. Challenges Faced by Technology Partners (actual responses reported in Figure 4)

a) Data Standardisation and Accessibility

- 50% of technical partners reported difficulties due to the lack of standardised data models across different BCP databases.
- The fragmented and decentralised nature of these databases created further challenges, as they were not interoperable or integrated.
- Limited access to BCP databases hindered technical teams from fully utilising real-world data, which affected system development and testing.

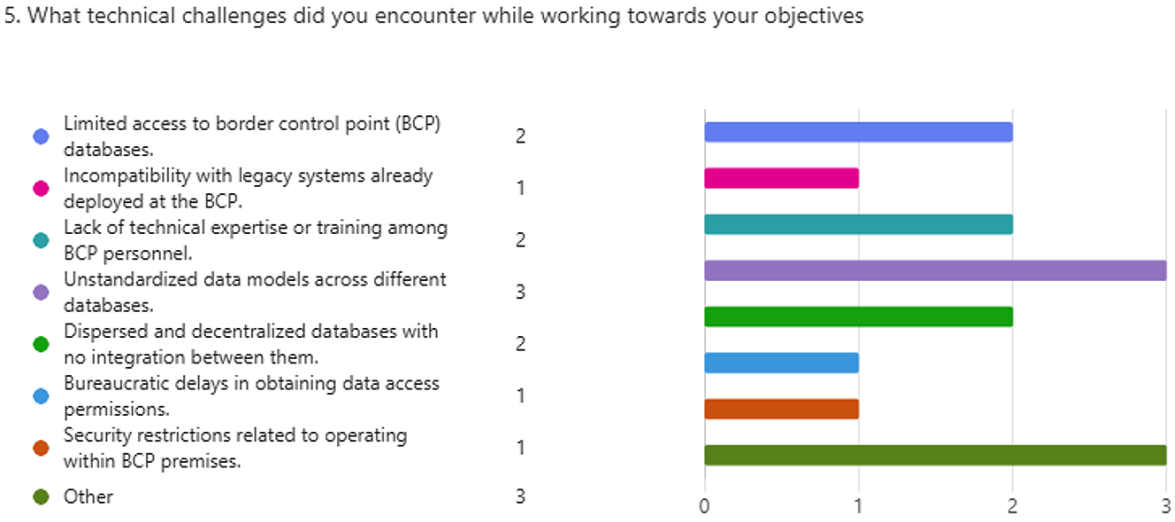

Figure 4: technical challenges reported

b) Limited End-User Technical Expertise

- A few partners highlighted the lack of technical expertise among BCP personnel.
- Many BCP staff had limited knowledge of their own pain points, making requirement gathering and technology adaptation more complex.

Q6. Mitigation Actions Taken (actual responses reported in Figure 5)

- Implementation of a Data Validation System: A structured approach was adopted to ensure technical partners could work with compliant and uniform data.
- Gradual Deployment Approach: A "start simple" methodology was followed—utilising existing technologies and data while refining the system over time as both users and developers adapted.
- Transparency Between Technical Teams and End Users: Regular communication was maintained to encourage active engagement and feedback loops.
- Early End-User Involvement: By integrating BCP personnel in all project phases, expectations were managed effectively, and user adoption improved.

ID ↑	Name	Responses
1	anonymous	We've created a common data model to be used by all partners for the generation of high level events allowing for more flexibility to the internal architectures. We've built a data validation tool and provided extensive feedback to all partners producing data. We've set several deadlines and provided additional help and guidance to partners.
2	anonymous	We defined a common data model for all partner to exchange events with the FLEXI-cross toolkit and a tool to allow technical partner to test event's production. We implemented ETL procedures to allow 'translation' of messages to different data-formats.
3	anonymous	Made focus meeting with some, available BCP personnel to align the dashboard with what they could be looking for within their daily operation
4	anonymous	Keeping track of open points; Short term and long term planning of achievements and challenges early on; Integration meetings between partners to overcome challenges/ blockers. Conducted Workshops/trainings and collaborated on overall solution.
5	anonymous	Continuous testing and refinements
6	anonymous	Worked with legacy systems to build the necessary modules. Installed additional equipment at borders to achieve the envisioned functionality

Figure 5: actions to overcome the challenges

Q7. Lessons Learnt from Technical Challenges (actual responses reported in Figure 6)

- Developing Compatibility Solutions: Innovative methods were required to bridge compatibility gaps between legacy systems and new technologies.
- Decentralised System Adaptation: New methodologies were designed to accommodate non-standardised and decentralised systems.
- Enhancing User Engagement: Special strategies were implemented to improve communication and training for non-technical end users.

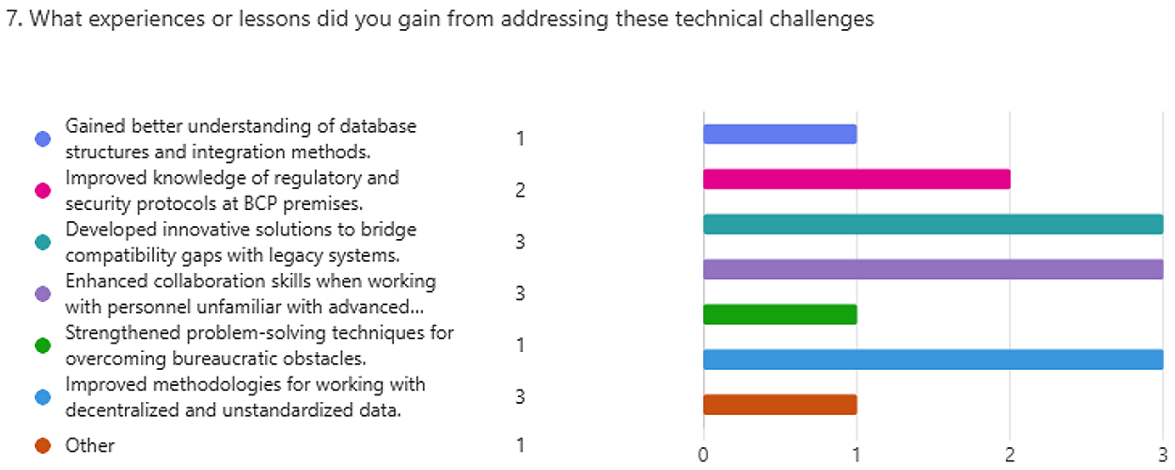

Figure 6: experience and lessons learned

Q15. Challenges Faced by End Users (BCPs) (actual responses reported in Figure 7)

a) Bureaucratic and Administrative Barriers

66% of end users cited difficulties related to bureaucratic hurdles, such as delays in approvals, restricted data access, and coordination challenges between multiple stakeholders.

b) Insufficient Training and Support

50% of participants mentioned that they lacked adequate training on new tools, leaving them unprepared for adoption.

Many BCPs struggled to integrate new technologies into their workflow due to the absence of structured training sessions.

c) High Workload Constraints

The demanding nature of BCP operations left personnel with little time to dedicate to project-related activities or research and development efforts.

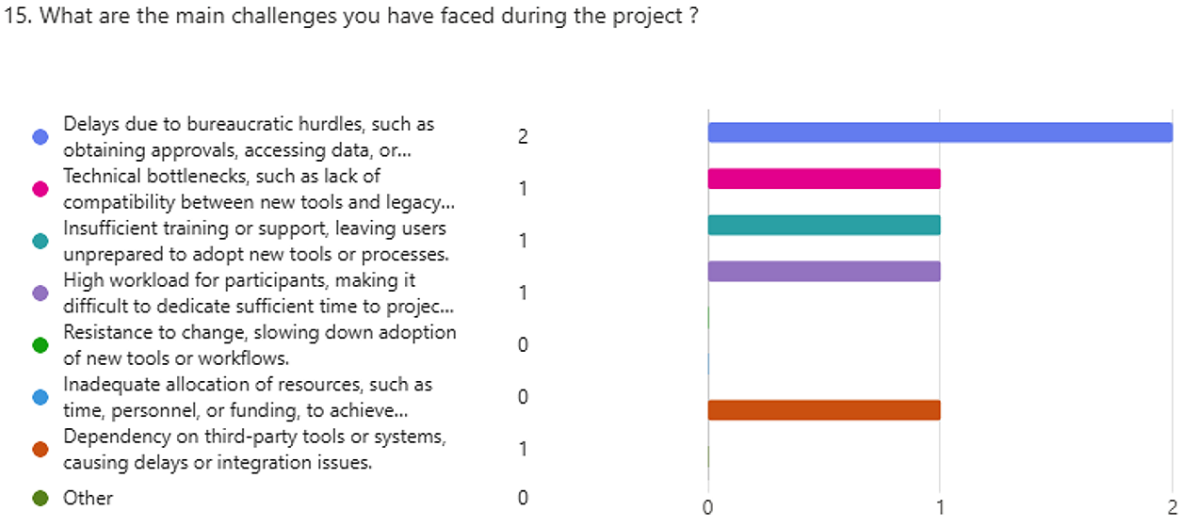

Figure 7: Challenges reported by end users

Q16. Experiences Gained and Positive Outcomes (actual responses reported in Figure 8)

Despite these challenges, the experience gained throughout the project was overwhelmingly positive. All participating end-user partners reported:

- Exposure to new technologies for the first time, expanding their awareness of digital solutions that could enhance border control operations.
- A better understanding of how technology can support security operations without compromising efficiency.
- Excitement about future collaboration between BCPs and the private sector, recognising the value of innovation in border security.

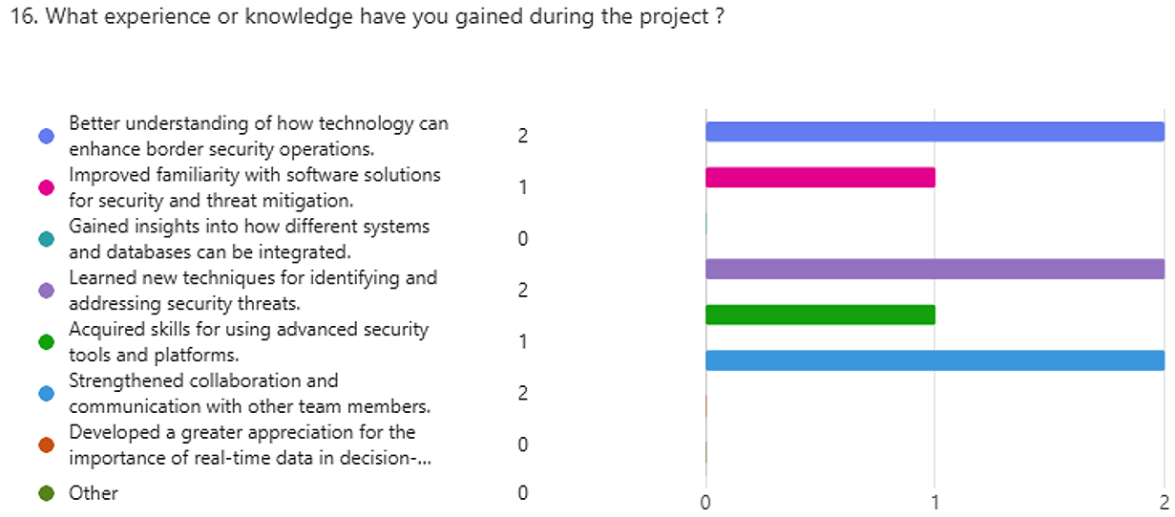

Figure 8: experience and lessons learned by end users

3.1.3. Gap Analysis

A thorough gap analysis was conducted, centred on identifying inefficiencies and areas for improvement in operational workflows, ensuring alignment with strategic objectives and technological advancements.

The work was conducted in two phases:

- **Phase 1:** Definition of the framework for redesigning operational processes.
- **Phase 2:** Definition of the anticipated complexity of executing these processes, based on the Key Performance Indicators explicitly identified and described in WP3, Trials and Validation.

During Phase 1, a three-step methodology was adopted, as shown below:

- **Step 1:** All of the end users' functional legacy systems were considered while thoroughly defining the current procedures being followed.
- **Step 2:** All suggestions for technological, operational, and other improvements were emphasised based on the identification of real-world gaps and direct extraction of end-users' experience.
- **Step 3:** The procedures were redesigned to enhance efficiency and effectiveness in terms of time, security, cost, and quality while checking passengers crossing the border points of interest.

An indicative result from Phase 1 related to UC3 is presented in the table below.

Existing Operational Process (Only for third-country nationals)	Technology used *[Only Legacy systems]*	Operational Gap or/and proposed optimised Processes	Redesign of the technological steps with time prioritisation, adding the tools of the FLEXI – cross solution
Identity check and verification Visa or residence permit check Duration of authorised stay check Departure, destination and purpose verification Means of subsistence verification Means of transport and carrying objects check	1. CREDENCE ONE-MRZ travel documents reader and verification, fingerprint scanner and verification 2. Visual and/or physical check by border guard	1. Biometric sensors, Document readers 2. 5G Communication infrastructure 3. Applications for authorities installed in relevant devices (smartphones) 4. Train wagons Thermal cameras Video cameras, acoustic sensors 5. Smartphones 5G	1. Installation of cameras and acoustic sensors 2. Implementing Biometric detection tool 3. Match with uploaded documents 4. Functionality checking. 5. Application of ML Algorithms on received data 6. Results Analysis and validation 7. Testing 5G network reliability 8. Integration in Control UI, where data monitoring takes place 9. Functionality validation on authorities' devices

During Phase 2, a methodological approach was applied to define complexity factors for KPIs in relation to process redesign. This allowed for the anticipation of an improved solution toolkit, with a focus on potential practical challenges during trial execution, particularly for **KPIs with high complexity factors**.

This method was applied to the three use cases of interest, independently assessing the complexity of each KPI.

Specifically, after determining that the Complexity Factor (CF) is defined by the number of redesigned steps included for each KPI, the trial and technical leaders of each use case assigned CF values to all KPIs across the three use cases. Finally, **by averaging the complexity factors per** use case, the results are presented in the figure below (Figure 9).

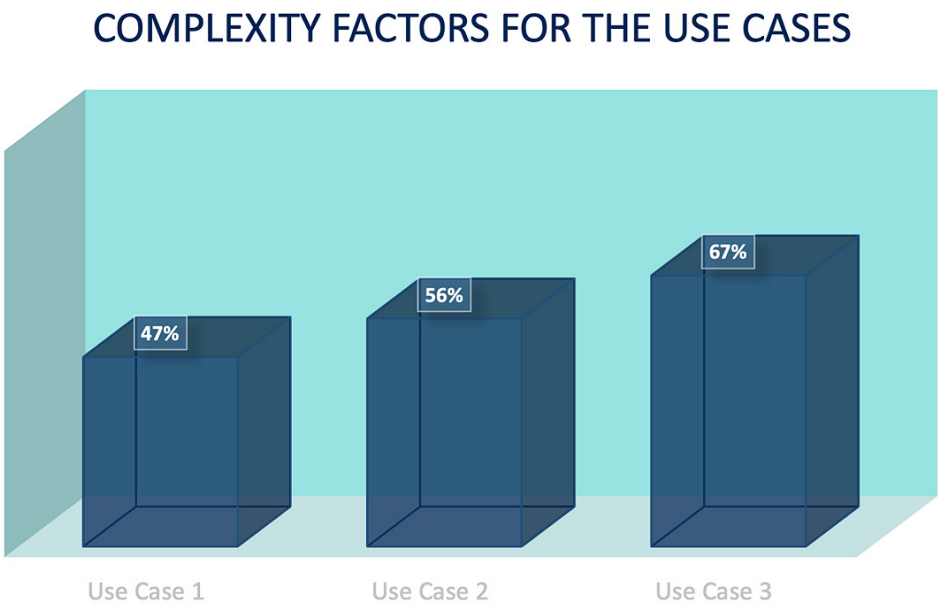

Figure 9: The averaged complexity factors (in percentages) for the three use cases of FLEXI-CROSS.

3.1.4. Recommendations on possible standardisation activities and strategies for policy experts

This section shows how recommendations or evidence have been collected in order to provide EC officers with some good practices that have been experienced during the FLEXI-cross project. Several methods have been followed since the beginning of the project to provide the aforementioned evidence. First, a multi-topic set of activities, like synergy webinars and workshops, was organized to gather ideas from different contexts. Secondly, the participation to topic-specific events, like the European Association for Biometrics events, has been very useful to discuss, in a European context, about the main challenges and experiences of the different European actors. The main outcomes of these events have been minutes and the collection of common results within the same topic or between European Research topics like Fight Crime and Terrorism and Border Management.

3.1.4.1. Recommendations

- Recommendation 1 – Projects Promotion
- Recommendation 2 – Joint Exploitation and Dissemination
- Recommendation 3 – Ethical and legal aspects curation
- Recommendation 4 – Standardization groups and working group promotion

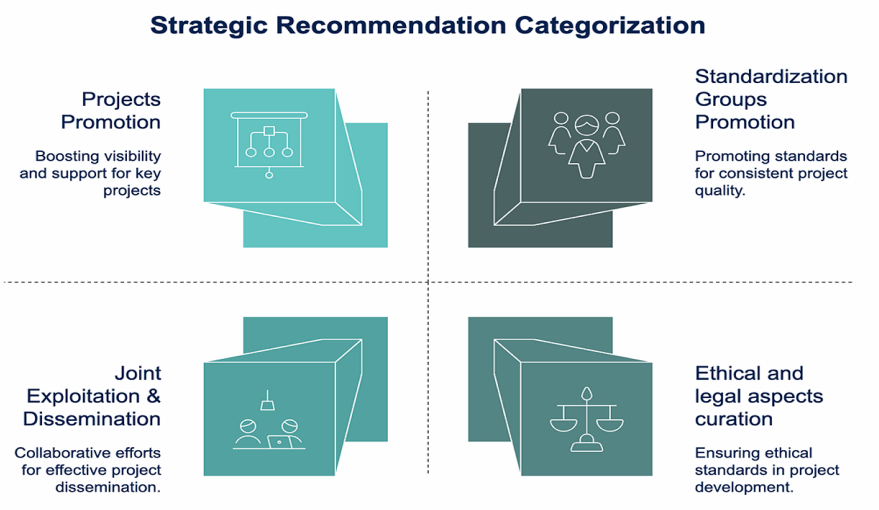

Figure 10: Recommendations overview.

Recommendation 1 – Projects Promotion

Aim 1: to intensively promote projects clustering activities and participation to synergy activities.

Aim 2: To actively promote the main results of the projects in order to identify scientific and innovation findings.

Where and Who was involved: EAB RPC conference, other Biometric conferences, Projects to Policy Seminar, CERIS, brokerage events.

Target audience: RTO, Academies, Large industries, EC officers and agencies.

Recommendation 2 – Joint Exploitation and Dissemination

Aim 1: to promote European services that support joint exploitation and dissemination. An additional advertisement is needed by increasing awareness of Horizon Results Booster and the related tools. Projects are stimulated to think more in the context of shared results, and possible impacts.

Where and Who was involved: PPS, Policy Officers and Project officers

Target audience: RTO, Academies, Large industries, EC officers and agencies, projects facilitating the task.

Recommendation 3 – Ethical and legal aspects curation

Aim 1: to create more confrontation moments on the AI Act and its application to the Innovation and Research projects.

Aim 2: to explore different nuances of research activities in order to cover with round tables and FAQ boards all the doubts related to the implementation of AI in the different contexts.

Where and Who was involved: EAB RPC conference, Ethical Experts, EC legal and ethical experts.

Target audience: RTO, Academies, Large industries, EC officers and agencies, projects facilitating the task.

Recommendation 4 – Standardization groups and working group promotion

Aim 1: to organize open consultation with representatives of thematic working groups and standardization bodies where projects can identify the challenges, needs, and findings on potential contribution to standards. More confrontation moments on AI Act and its application to the Innovation and Research projects are needed.

Where and Who was involved: EC officers.

Target audience: RTO, Academies, Large industries, EC officers and agencies, Standardization bodies, working groups.

3.2. TENSOR use cases

The TENSOR platform and its technology offerings were evaluated across three different use cases (UCs). The first pilot demonstration and validation phase took place in November 2024. The aim of the first pilot phase was not only to validate the platform, but also to gather valuable feedback from the end-users. This feedback will be the basis for enhancing the technologies and potentially improve TENSOR for the final pilot phase.

- The **UC1** "Evidence collection through intelligence derived from correlated physiological and behavioural biometrics based on CCTV footage" is a multi-modal and multi-contextual scenario to demonstrate the effectiveness in identifying and verifying the identity of a suspect. The Policejní Prezidium České Republiky (PCR) lead this pilot and validated different aspects of the platform throughout a demonstrator and an on-site workshop.
- The **UC2** "Digital Forensics Extensions allowing Orphan Device Owner Identification" demonstrates under the leadership of the Ministry of the Interior of Finland (MOI) TENSOR's digital forensics extension to extract information of interest from an orphan device, i.e., when the owner of a seized device is not known. The extracted information can be fed into an active investigation and might be used to identify the owner of said device. Furthermore, this UC focuses on the integration of novel behavioural biometric technologies of TENSOR into the device owner identification process.
- The **UC3** "Biometric data protection and secure exchange in a cross-border scenario" demonstrates a data exchange between Law Enforcement Agencies (LEAs) in a cross-border scenario through the European Biometrics Dataspace. This technology has the potential to streamline the data exchange process and by doing so accelerate international investigations. The partners involved in this UC are the Ministério da Justiça (PJ) of Portugal and the Inspectoratul General al Poliției (GPI) of Moldova.

To evaluate and validate the TENSOR platform and its components, 60 forensic experts from various LEAs were recruited, who have expert knowledge in the forensic work with biometric data, digital forensics or criminal investigations. Each participant had the possibility to conduct an online training to familiarise themselves with the TENSOR components by completing modules on a Moodle-based website. Any user feedback on the training itself was directly collected via a questionnaire on the Moodle platform.

Depending on the UC, the volunteers had then the possibility to gain insights in the TENSOR platform by participating in technology-specific on-site workshops or conducting extensive group testing sessions (in groups of 3) and the ability to interact with the TENSOR platform.

The workshop and testing sessions were concluded with each participant providing their opinions and insights participating in an online evaluation survey. This enabled us to collect the user feedback during the pilots and identify potential improvement for the second pilot iteration.

3.2.1. Lessons learnt

This section summarises the lessons learnt from the TENSOR project, collected throughout the whole piloting phase: from the planning and preparation of the pilot studies, over the training of the participants to familiarise with them with the TENSOR system and its components, and finally during the execution of the distinctive pilots.

3.2.1.1. General feedback

The measured operational KPIs focus on the LEAs' needs to operate the TENSOR platform for biometric data analysis and cross-border biometric data exchange. Some of the defined operational KPIs could already be achieved during the first pilot phase, and with the collected user feedback we aim to achieve the target values of the remaining KPIs in the second iteration of the pilots. In detail, the following KPIs (Figure 11) are assessed during the pilot phases.

- O1: Increased efficiency in criminal identification by 60% (achieved)
- O2: Improvements of search/classification speed by 25% (achieved)
- O3: Improvement of operational standards and processes for LEAs by 70% (in progress)
- O4: A percentage increase of automated processes across the investigative workflow by 70% (in progress)
- O8: User Acceptance Percentage at >96% (in progress)

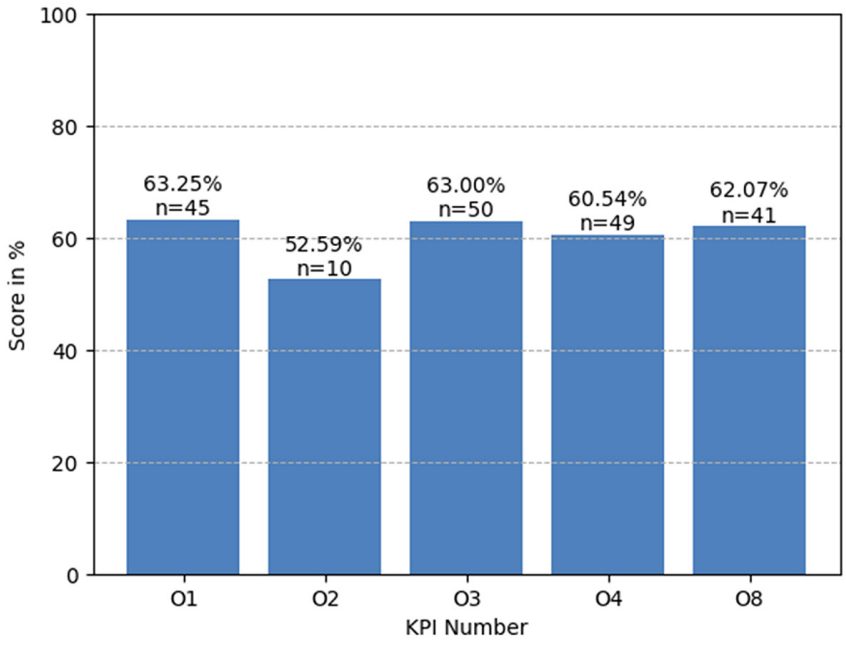

Figure 11: KPI evaluation results after the 1st pilot iteration

Feedback on the increased efficiency in criminal identification (O1) stated the need for providing a unified platform to gather and process biometric evidence in an investigation. A good performance of the overall system was stressed as essential in providing fast insights, increasing search and classification speeds (O2). The main reason behind this is the limited human and time resources during the forensic work and the analysis of large volumes of data. End users also highlighted the benefits of processing, fusing, and sharing multiple biometric modalities on one single platform, which will improve existing processes across the investigative workflow (O3), with some of the offered technologies complementing already existing commercial tools.

Also, some users remarked that the successful implementation of such a solution depends on the integration of already existing databases and registers within TENSOR, as well as the accompanying legislation. However, according to the end users the integration with legacy systems might not be feasible, as the specifications on the systems and database schemes are considered confidential information and not be shared outside the LEAs. As a direct consequence, this also impacts any interoperability requirements that may not be fully met. A successful integration of a system with existing legacy systems might significantly facilitate the end users' everyday work, instead of having "yet another platform" that cannot communicate with existing systems and imposing unnecessary user workload.

Overall, the end-users recognized the potential of the offered solutions and clearly showed an interest in them. In particular, the ability to fuse different biometric modalities was positively highlighted. Also, they appreciated the potential of the TENSOR solution in enhancing efficiency and increasing automation (O4) compared to methods, technologies and operational workflows within their agency.

3.2.1.2. User training

The user feedback regarding the online training encompassed the need to create an interactive and more engaging environment and the need to improve the overall quality of the provided training materials, rather than just providing "user manuals". End users stated the wish for more hands-on, practical training scenarios. The training should also be tailored to different levels of expertise, preliminary knowledge on the used technologies from potential users, and their specific roles. The different levels of expertise demand for customised training content that links the training material with the practical application of the presented technology.

3.2.1.3. Pilot validation and demonstration

Feedback regarding the pilot validation and demonstration itself addressed the need for realistic conditions of the demonstrated platform with the complete set of the presented functions. This encompasses not only the functionalities of the TENSOR components, but also the realism of the used dataset and files. The TENSOR platform should also be tested and deployed on premises during the pilots, which was not possible for the first pilot phase. The needed hardware and connection capabilities at the LEAs' premises can pose a critical factor for a successful pilot. On the one hand, the end users work in a security critical environment that limits the possibility to connect to any online services. On the other hand, the technical requirements of the technologies in question might surpass the hardware capabilities available at the testing location, creating the need for third parties to be involved in hosting the services.

3.2.1.4. Usability

Usability feedback addressed missing functionalities that may ease the forensic work while interacting with the system. This includes structuring visual components with meaningful information (e.g., chat views for extracted conversations from mobile devices, previewing file contents), the ability to view/interact with various file types (e.g., map for location data, video player), sophisticated search and filter mechanisms to efficiently reduce the number of data, and finally using and exporting standard file formats (e.g., NIST file format for storing biometric data). One suggestion to improve usability is to include the end users in the development process early on, which might aid finding and prioritising the needed functionalities for the platform.

At the same time, users praised the user-friendly environment and the ability to initiate the analysis with simple means and the easy creation of reports, though in-house standardised procedures must be considered to ensure that evidence can be used in court.

3.2.1.5. Technological aspects

AI poses a potential technology for aiding forensic experts in their everyday work for finding biometric matches and the identification of persons. Nevertheless, many AI-based models have their own definitions for similarity scores and thus making the interpretation of the results, e.g., likelihood or the level of confidence, very difficult, which might be needed as a reasoning to defend the results in court. Thus, information on the model's internal mechanisms might be a crucial addition.

Independent from the type of technology, the end users demanded for each technology to include an explanation on the following points:

- its capabilities (what it can and cannot do)
- its functionalities (how to use the technology)
- understanding the technology (how does it create results)
- interpreting the results (what does this result mean)

This information might not just be part of the training but also be integrated in the final platform to provide context-based on-demand help for users.

3.2.1.6. Legal aspects

Although inside the EU, the member states are bound to the GDPR, we found that the individual partners from different countries embrace different levels of national laws, that expand on the GDPR. Apart from national laws, the LEAs might impose additional in-house policies that makes the processing and sharing biometric data between countries particularly challenging.

Also, using real datasets from criminal records was not possible to validate the components as they are not available or restricted by law and thus posing a special challenge for creating a realistic testing environment. Therefore, we needed to consider alternatives to obtain realistic data (e.g., from volunteers) and enrich the datasets to a realistic volume (e.g., using synthetic data).

Any legal discussions towards implementing data processing agreements or consent forms should therefore be initiated as early as possible in the project. Based on our past experiences these processes tend to be tedious and lengthy, as various (legal) departments of the affected partners need to be included in the discussions.

3.2.2. Gap Analysis

3.2.2.1. Identified Technical Gaps

Integration Challenges - One of the most critical barriers to the advancement and deployment of next-generation biometric technologies lies in their integration with existing operational infrastructures. TENSOR has faced pronounced challenges in this domain – challenges that reflect systemic issues across many law enforcement and security-related digital ecosystems while also highlighting the broader issue of accessing closed, proprietary, siloed infrastructures and databases, which are often highly restricted and not designed to accommodate the testing or validation of cutting-edge technologies. In particular, TENSOR has been unable to gain access to critical systems such as AFIS (Automated Fingerprint Identification System) and ABIS (Automated Biometric Identification System), which are extremely important for the real-world evaluation and functional validation of novel biometric technologies. This absence of access to operational data and systems presents a substantial bottleneck for evaluating interoperability, latency and detection efficacy in a controlled yet representative environment. Without such access, the project's ability to carry out empirical testing, integration trials and performance benchmarking in situ is severely compromised. Furthermore, this situation reflects a broader, structural challenge in the EU, namely *the lack of policy frameworks and technical standards that facilitate secure, conditional integration of research-stage solutions into mission-critical public sector systems for testing purposes*. Given these constraints, and in order to maintain the continuity of development and demonstration activities, TENSOR opted to develop simulated versions of these systems. These sandboxed environments replicate key functionalities and workflows of ABIS, enabling the project to showcase integration concepts, demonstrate the potential of each biometric technology and validate the overall system behaviour.

The aforementioned integration challenges experienced by TENSOR emphasize the urgent need for policy innovation. More specifically, there is a pressing requirement to *establish controlled testing sandboxes that will allow research consortia to access anonymized or synthetic datasets within operational system architectures under strict legal and ethical oversight*. Creating such frameworks would not only accelerate the development cycle for security technologies but also ensure that these tools are aligned with the actual operational realities of law enforcement stakeholders. Moreover, public-private collaboration models should be fostered to *facilitate modular interface standards between legacy systems and emerging digital components*, reducing friction in future integration efforts.

Interoperability Issues – In the pursuit of developing an advanced and secure biometric analysis system, TENSOR has encountered significant challenges related to interoperability – a key aspect for any robust and scalable law enforcement technological framework. The integration of multiple biometric modalities (e.g., facial recognition, fingerprint analysis, gait patterns, behavioural trends and voice authentication) within a single system architecture poses both technical and procedural obstacles, particularly when these modules originate from diverse providers or legacy systems. One of the core impediments lies in the incompatibility among the system's technical modules, which often operate using heterogeneous standards, proprietary data formats and different communication protocols. This diversity results in fragmented data flows and increased complexity in cross-module coordination, which in turn, hinder the seamless exchange of critical information across subsystems causing a significant delay to the operational decision-making.

To mitigate these issues, TENSOR adopted a modular, service-oriented architecture grounded in OpenAPIs and harmonized with internationally recognized interoperability standards. This architectural paradigm ensured that different modules can evolve independently while still maintaining their ability to interoperate, thus enhancing the overall cohesion and functionality of the system. In addition, a critical enabler for the integration task has been the deployment of a Continuous Integration/Continuous Delivery (CI/CD) environment, which functions as a middleware orchestration layer. This environment automates the deployment, testing and integration of new components into the ecosystem. It allows for the early detection of compatibility issues and fosters agile updates and reconfigurations without compromising the integrity or security of the system. The CI/CD framework also supported version control, dependency tracking and backward compatibility, facilitating the incremental evolution of the system in response to emerging operational needs and stakeholder feedback.

To ensure long-term interoperability and integration efficiency in biometric systems, it is important to *adopt standardized, open approaches the early stages of development*. All technical components should *adhere to internationally recognized standards for data formats, APIs and communication protocols*, with well-documented, reusable APIs to enable seamless system extension and interoperability across diverse platforms and use cases. Establishing standardized testing and validation frameworks will further ensure compatibility across diverse modules and vendors. Moreover, projects should *adopt Continuous Integration/Continuous Delivery (CI/CD) environments as operational norms to streamline updates, automate testing and proactively address integration issues*. The creation of a common middleware infrastructure can support modular integration and align projects with broader digital policy objectives. These policy measures together would strongly promote a more scalable and secure biometric technology ecosystem for European law enforcement agencies.

Scalability Concerns – TENSOR, a forward-leaning initiative designed to equip LEAs and security stakeholders with advanced tools to detect and counter terrorism and organised crime, has reached a critical stage concerning the scalability of biometric technologies. As the project transitioned from prototype testing to broader implementation, a series of structural and operational challenges emerged that posed significant challenges in the system's ability to scale effectively across jurisdictions, use cases and infrastructure environments.

The first major challenge lies in the technological fragmentation across EU Member States, particularly in their biometric data infrastructure. Each country or law enforcement agency may use a different combination of hardware (e.g., sensors, cameras, databases, etc.) and software (e.g., biometric matching algorithms, data storage systems, etc.), most of which are not designed to interoperate. TENSOR's biometric tools, when developed and tested in controlled or modernized environments, may not function efficiently when deployed into these fragmented ecosystems. This leads to high integration costs and significant delays during deployment phases, as systems must often be adapted on a case-by-case basis.

A second challenge arises from the inconsistencies in biometric data types and quality, which directly impact system reliability at scale. TENSOR is designed to process various biometric modalities, such as facial recognition and fingerprints. However, in operational environments, these data inputs are frequently imperfect, low-resolution images from surveillance footage, partial or smudged fingerprints, or images taken under poor lighting conditions. Such conditions degrade the performance of even the most sophisticated algorithms, especially when scaled across multiple sites or jurisdictions with differing data collection capabilities.

The third scalability issue is rooted in computational demands and performance constraints. Biometric systems, especially those required to operate in real time, place heavy loads on computing infrastructure. For instance, analysing multiple video feeds to identify faces against large databases involves intensive processing. This becomes problematic when the TENSOR platform is deployed in locations lacking high-performance servers or where cloud solutions are restricted due to data protection laws. Without scalable, decentralized (e.g., edge-based) processing options, system responsiveness deteriorates, compromising usability in time-sensitive operations.

To address these challenges, a coordinated EU-wide approach is needed. First, the *development of harmonized standards for biometric integration would ensure interoperability across national systems.* These standards should cover both technical specifications and procedural guidelines for data handling, making it easier for biometric components to integrate seamlessly with local infrastructures. Second, *investment in federated and edge computing infrastructures* is critical. Such resources would allow decentralized processing of biometric data, reducing dependence on centralized systems and aligning with privacy regulations. EU funding mechanisms should prioritize projects that support scalable and privacy-preserving computing environments tailored to LEA use cases. Third, *a regulatory sandbox should be introduced to enable controlled experimentation with biometric technologies in law enforcement settings*. This approach would help reconcile legal ambiguities and foster clearer, consensus-based interpretations of GDPR as applied to biometric surveillance, facilitating legally secure scalability. Finally, the human dimension must not be overlooked. A *comprehensive EU training and certification framework for biometric system operators* would help harmonize user capabilities across LEAs. Coupled with mandatory biometric-specific Data Protection Impact Assessments (DPIAs), these measures would ensure that scaling efforts uphold legal and ethical standards while maximizing operational effectiveness.

Documentation Shortfalls - One of the most pressing challenges encountered during the implementation of the TENSOR project, was the pervasive lack of thorough documentation and detailed operational guidance for the underlying systems and tools. The consortium members built upon a variety of pre-existing biometric analysis frameworks, many of which were proprietary but some of them were sourced from the open-source ecosystem. However, the technical teams frequently encountered severe gaps in documentation, ranging from missing architectural overviews and absent API specifications to ambiguous configuration instructions and incomplete deployment guidelines. These gaps increased significantly the cognitive load for software developers towards the integration of the components in a single system. This issue was particularly pronounced with open-source software, which often lacked lifecycle maintenance. In many cases, the available documentation was outdated, community-maintained, or fragmented across various discussion threads, developer wikis and archived web pages. Consequently, critical aspects of system behaviour were either misunderstood or misapplied, a fact that resulted in deployment failures and performance bottlenecks.

To mitigate these challenges, TENSOR's technical teams relied on informal knowledge sources such as online forums (e.g., GitHub Issues, Stack Overflow), direct communication with tool maintainers and peer community engagements. In more complex scenarios, the teams resorted to extensive trial-and-error practices, involving reverse engineering of codebases and exhaustive debugging to decipher the functional logic of modules whose inner workings were poorly or inconsistently described. While this approach yielded results over time, it incurred significant delays and diverted valuable resources away from innovation and toward basic technical enablement.

To address the systemic challenges faced by security projects that emphasize software development, it is important to improve the quality, accessibility and sustainability of technical documentation. Policymakers should mandate *robust documentation practices for any publicly funded software development*, ensuring that APIs, system architectures and configuration details are clearly and consistently described. Establishing a *centralized European platform to host and maintain documentation for open-source security tools* would also promote long-term usability and community engagement. Additionally, *support mechanisms should be created to incentivize the ongoing maintenance of critical biometric and AI tools beyond initial project lifecycles*. Finally, projects should be required to *assess the technical maturity of third-party tools before integration*, considering documentation quality and support availability.

3.2.2.2. Identified Operational Gaps

Process Inconsistencies – A critical operational gap identified during the implementation of TENSOR pertains to the significant inconsistency in procedures and workflows across the various participating LEAs, namely police authorities and forensic institutes. These discrepancies stem from diverse institutional practices, different degrees of technological maturity and varying levels of user readiness. The lack of harmonized protocols made it difficult to establish a cohesive operational baseline, often leading to misalignments in system deployment, interoperability challenges and confusion over technology integration responsibilities. As each partner approached the use of TENSOR's tools from different starting points and with different assumptions, the project faced barriers in creating a shared operational understanding, necessary for the exploitation of the platform's full capabilities.

To overcome these inconsistencies, policy efforts should focus on *promoting procedural harmonization* through *common operational frameworks and capacity-building programs tailored to the needs of LEAs* with lower technological readiness. EU-level coordination bodies, such as Europol or CEPOL, could lead the *development of standardized best practices and interoperability guidelines*, ensuring they are flexible enough to accommodate national specificities while promoting convergence. Additionally, EU funded projects should include dedicated funding for *cross-partner training and simulation exercises* that foster a mutual understanding of procedures, user roles and system expectations. It is worth highlighting that investing in the alignment of operational cultures is not only critical for rapid technology adoption but also for maximizing the return on investment in EU security research and innovation programs.

Lack and Limitations of Real Available Biometric Data - A critical operational gap encountered in TENSOR was the limited access to real-world biometric data, which significantly hampered the ability to develop, test and validate robust, mature biometric analysis systems. Due to stringent legislative and ethical constraints, including privacy protections and data minimization principles, access to authentic biometric datasets – especially those held by Law Enforcement Agencies (LEAs) – was either highly restricted or entirely unavailable. Additionally, legal uncertainties surrounding the reuse of historical data from closed investigations further complicated data acquisition efforts. As a result, the project was forced to rely on synthetic or open-access biometric datasets, which, despite being useful for preliminary development, often failed to capture the complexity and diversity of real operational environments.

To bridge this data gap, policymakers should *prioritize the creation of a secure, standardized and ethically governed framework that enables the controlled use of existing biometric datasets for research and innovation purposes*. This framework should incorporate privacy-preserving technologies, such as data anonymization, federated analysis environments or secure multiparty computation, to ensure legal compliance while allowing meaningful access. At the same time, *clear legal pathways should be established to permit the reuse of historical biometric data*, always under strict oversight and with transparency, particularly in cases where the data can meaningfully contribute to the development of public safety tools. Funding should also *support the creation of realistic benchmark datasets – especially with the use of Generative AI methods – in collaboration with LEAs, academic institutions and ethics experts*, ensuring that future projects can perform operationally relevant validation while maintaining public trust and adherence to fundamental rights.

Lack of Accessing a Knowledge Base of Best Practices – Another significant operational gap identified during TENSOR is the lack of a centralized knowledge base that aggregates best practices for the deployment, management and ethical oversight of biometric systems. Currently, LEAs partners work in silos, relying on organization-specific procedures and ad hoc operational standards. This fragmentation results in inconsistent implementation and missed opportunities for cross-agency learning. A unified repository of validated best practices, covering topics such as system calibration, data protection protocols, algorithm performance evaluation and user training, among others, would allow all stakeholders to align their operations with field-tested methodologies, thus increase system interoperability, accountability and efficiency.

Policymakers should consider supporting *the development of such a repository under the framework of existing EU security and innovation programs*. This knowledge base could be hosted by an EU agency such as Europol, FRONTEX or eu-LISA, and co-developed with ongoing research projects and practitioner communities. It should be dynamic, allowing for *continuous updates as technologies evolve and new operational insights emerge*. Additionally, participation in this platform should be incentivized, encouraging LEAs and developers to *contribute case studies, deployment lessons, appropriate datasets (compliant with national and EU regulations) and policy compliance workflows*. Such a shared infrastructure would streamline future biometric system rollouts and enhance the EU's collective preparedness and resilience in the face of emerging security threats.

Misaligned Expectations - Misaligned expectations between end users and the technology offerings further complicate the project's operational landscape. Security practitioners and law enforcement agencies often anticipate mature, ready-to-deploy solutions that can seamlessly integrate into their workflows. However, many of the tools being piloted remain in mid-stage development (Technology Readiness Levels (TRL) 6-7), where performance inconsistencies and integration challenges are to be expected. This disparity creates frustration, undermines trust in innovation-driven initiatives and risks reducing user engagement at the pivotal stages of deployment and validation.

To bridge this gap, policy should require *early and continuous user involvement in the design and validation process of security technologies*, supported by structured co-creation methodologies. Funding programs should mandate that project consortia should *include clear roadmaps for expectation management*, with phased communication strategies that align technological maturity with user preparedness and operational constraints. Furthermore, *periodic reassessments of technical readiness and user requirements should be institutionalized within project workflows*, enabling adaptive planning and mutual understanding. These measures will improve the usability and adoption of emerging biometric tools while also foster long-term collaboration between technical experts and practitioners, ensuring that innovation remains anchored in operational reality.

3.2.3. Recommendations on possible standardization activities and strategies for policy experts

The implementation of reliable biometric technologies for law enforcement requires robust standardisation to ensure interoperability, data security, and ethical AI deployment. However, achieving certification within the scope of a three-year EU project presents common challenges, particularly when relevant standards are still in development. The evolving nature of regulatory and technical frameworks means that projects must often navigate shifting requirements while contributing to the maturation of emerging standards. This chapter outlines key recommendations for standardisation activities and strategies that can enhance the effectiveness of biometric systems and facilitate cross-border collaboration among Law Enforcement Agencies (LEAs).

3.2.3.1. Interoperability

Interoperability with biometric legacy systems is crucial for effective investigations, resource optimisation, and cross-border collaboration. Standardisation in this area will reduce integration costs and ensure that biometric systems can function seamlessly across different institutions and technological environments.

Recommendation 1: Prioritise the adoption of existing international standards for biometric data interchange, such as the ISO/IEC 19794 series, which defines specifications for various biometric modalities (fingerprint, face, voice). Ensuring compatibility with existing frameworks for cross-border law enforcement cooperation and data exchange will further support interoperability.

Strategy: Actively participate in standardisation bodies where possible and contribute to refining and extending standards to address forensic application needs. Focus on developing standardised APIs and data formats for biometric modalities, enabling seamless integration with legacy systems and avoiding vendor lock-in. Harmonising data formats and protocols will facilitate efficient data exchange between biometric platforms and existing law enforcement infrastructures.

3.2.3.2. Data Sharing and Governance

A harmonised approach to biometric data sharing will enable LEAs to collaborate securely while ensuring adherence to legal and ethical standards. Establishing a trusted data exchange ecosystem will enhance operational efficiency and promote responsible handling of sensitive biometric information.

Recommendation 2: Establish a standardised framework for data sharing agreements between LEAs, incorporating clear guidelines on data usage, access control, and liability. The framework should align with international best practices and relevant legal frameworks to ensure lawful and ethical data exchange.

Strategy: Develop reusable templates for data sharing agreements, covering key aspects such as data ownership, purpose limitation, and security requirements. Introduce a certification process for data providers to ensure compliance with these agreements. The framework should also adhere to fundamental privacy principles, such as transparency, accuracy, and storage limitation, to maintain trust and legal compliance.

3.2.3.3. Privacy and Security

Privacy and security concerns surrounding biometric data are critical, and standardised privacy-enhancing technologies will provide LEAs with secure data processing methods that do not compromise individual privacy. Strengthening security measures, such as robust encryption, access controls, and authentication mechanisms, will help build public trust in biometric technologies.

Recommendation 3: Advocate for the adoption of standardised privacy-enhancing technologies for biometric data processing, such as homomorphic encryption and secure multi-party computation. Implementing these technologies will help minimise data breach risks and enhance compliance with privacy regulations.

Strategy: Conduct research on the performance and scalability of privacy-enhancing technologies in biometric applications. Develop reference implementations and encourage adoption through open-source initiatives and industry collaborations. Ensure data minimisation techniques are in place, aligning processing activities with their intended purpose to maintain privacy safeguards.

3.2.3.4. Ethical AI

Ethical AI practices are fundamental to mitigating bias and ensuring fair outcomes in biometric applications. Standardisation in this area will help define clear accountability measures and ensure that biometric technologies are deployed responsibly, reducing the risk of discriminatory outcomes.

Recommendation 4: Promote the development and adoption of ethical guidelines, benchmarks and standards for AI in biometric applications, ensuring transparency, fairness, and accountability. Addressing bias and discrimination risks is essential for responsible AI use in law enforcement, and standards around metrics and bias auditing could contribute to the development of responsible AI practices.

Strategy: Develop best practices for responsible AI development, incorporating principles of explainable AI (XAI) and fairness-aware machine learning. Promote an AI auditing methodology to help developers understand and incorporate regulatory expectations related to human oversight bias, explainability and risk mitigation generally. Establish a certification process for AI systems to ensure compliance with ethical standards. AI systems should be designed to be unbiased and non-discriminatory, fostering trust, transparency and fairness in their application.

3.2.3.5. Digital Forensics and Device Security

Standardisation in digital forensics is essential to ensure the integrity and admissibility of biometric evidence in investigations. Creating awareness throughout all participants and establishing clear guidelines and methodologies will enhance the effectiveness of digital forensic practices and support lawful access to critical biometric data.

Recommendation 5: Develop standardised guidelines for digital forensics investigations involving biometric data, focusing on secure device unlocking, data extraction, and chain of custody procedures. These guidelines should align with international best practices for handling digital evidence.

Strategy: Collaborate with LEAs and forensic experts to establish practical methodologies for digital forensics investigations. Promote the use of secure, standardised tools and techniques for data extraction and analysis to maintain forensic integrity.

By actively engaging in standardisation efforts and promoting the adoption of these recommendations, biometric technology initiatives can contribute to a more secure, interoperable, and ethically responsible ecosystem for law enforcement applications. This will not only enhance operational efficiency but also strengthen public confidence in the use of biometric technologies.

3.3. ODYSSEUS use cases

3.3.1. Lessons learnt

The ODYSSEUS project aims at validating and demonstrating eight key technical solutions through five distinct pilots (2 Train Pilots, 2 Land Pilots and the Water Pilot), implementing a diversity of Use Case Scenarios. The main objectives of this phase were to develop a comprehensive evaluation and validation plan, engage end-users for pilot demonstrations, assess ODYSSEUS platform performance, validate ODYSSEUS solutions across different environments, and analyse the pilots' results for further improvements, ensuring the integral execution of them, and aligning with ODYSSEUS key performance indicators (KPIs). To this end, a structured methodology, as depicted in the following figure (Figure 12), was designed and established in order to bridge the gap between the initial project objectives and the real-world constraints encountered during the pilot phase, linking each objective with an 'action' phase adhering to a timeline.

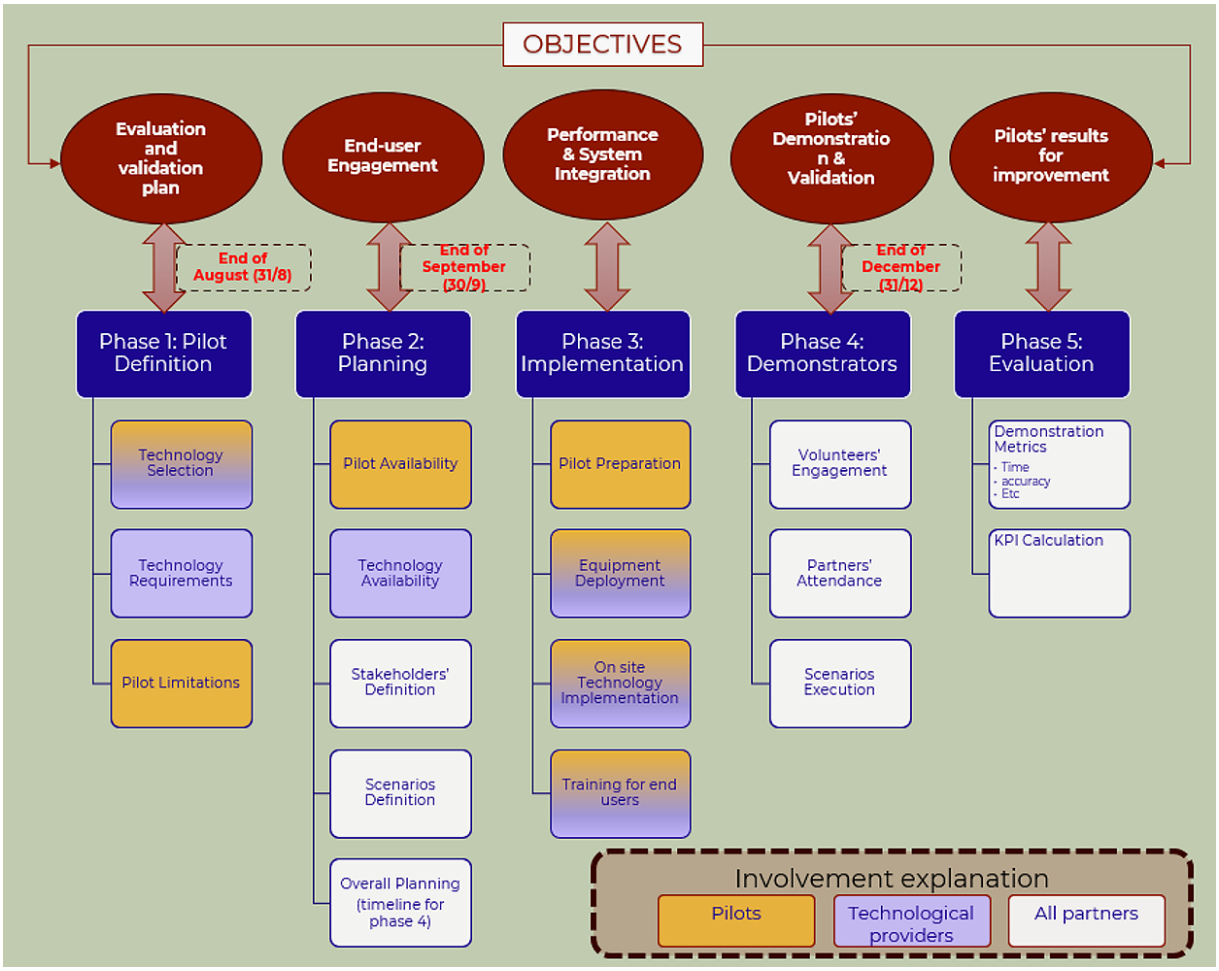

Figure 12: Pilot preparation and demonstration methodology

Our concept consisted of five consecutive phases, starting from the most critical, the **Pilot Definition**, where our major efforts were devoted to identify the pilots' limitations, the technology providers' pilot specific requirements, and the technology selection to be implemented in each pilot. The two lessons learnt from this phase are presented below.

Lesson 1: **Technologies' Comprehension from Stakeholders' View is Critical for Technology Selection and Implementation**:

Stakeholders' understanding of the technological solution that are going to be deployed is crucial for decision-making in the context of technology selection and effective implementation. In particular, in the case that the stakeholders, especially end-users, do not fully grasp how a solution works or what it entails, this can result in misalignments, mismanagement, and underperformance during the pilot execution.

Lesson 2: **Pilots' Limitations/Regulations and Technology Deployment Requirements Definition are Crucial for Smooth Pilot Execution**

It is of high importance to clearly understand the constraints and the regulations that a pilot has to compliant, and also, to define the requirements for technology deployment. In some cases, photos or indicative videos of the pilot facilities should be provided for a better view and comprehension, or even more an onsite visit could be a good idea.

Mitigation measures:

Technology providers must clearly communicate the functionalities, limitations, and potential benefits of their solutions. This communication should not only emphasize on technical specifications, but also, should make sure that the end-users can perceive how the technology will be utilised and what might be impact on their processes.

The second phase, **Planning**, incorporated the pilots' availability and, respectively, the logistical barriers per technological solution. During this phase, we allocated the Use Case Scenarios per pilot along with the stakeholders' definition, and we interpreted the former to demonstration/execution Scenarios. The lessons learnt consist of:

Lesson 3: Considering availability and logistical barriers prevents delays

Failure to take into consideration the logistical challenges, such as equipment transport and infrastructure readiness, can lead to significant project delays.

Lesson 4: Translating scenarios into operational demonstration plans enhances end-users' and tech providers' understanding

Simply defining use case scenarios is not enough; translating them into actionable, step-by-step demonstration plans ensures that all stakeholders, and especially end-users, grasp the technical aspects and expected outcomes. This enhances collaboration and reduces misalignment between expectations and implementation.

Lesson 5: Defining and engaging stakeholders improves acceptance and increases the likelihood of smooth pilot execution

Engaging key stakeholders from the outset ensures their needs and constraints are addressed, fostering greater acceptance of the technology. Lack of early involvement can result in resistance, operational conflicts, or unanticipated integration challenges.

Mitigation measures:

Close cooperation between end-users and tech providers ensures that operational requirements and constraints are continuously addressed, preventing misalignment and ensuring smoother execution.

Afterwards, the **Implementation phase** followed, when some of the selected solutions were deployed to the pilot sites beforehand, because of logistical and commissioning constraints, Additionally, we introduced the technological solutions outlining the Use Cases Scenarios to the end-users, and simultaneously, we were presenting the functionalities of the ODYSSEUS platform as a training workshop. Lessons learnt 6 and 7 are representative of this phase.

Lesson 6: Comprehensive testing of systems across diverse environments requires adjustments to scenarios and components, preventing integration failures

A technological component working in one specific environment may not function or have to be adjusted in another, due to variations in infrastructure, connectivity, or environmental conditions. Iterative testing across different pilot sites allows for scenario refinement and transformation to operational ones, and for system optimization.

Lesson 7: Organizing training sessions and hands-on workshops prior to execution is crucial
End-users must be adequately trained before deployment to ensure they can operate the system

effectively. Hands-on workshops help ensure that end-users are fully equipped to interact with the new system, facilitating smoother adoption.

Mitigation measures:

1. Tech partners adjust their solutions according to specific scenarios, incorporating buffer time for testing and troubleshooting.
2. Briefing and debriefing sessions facilitate knowledge transfer and end-user adoption.

The fourth phase of our plan, titled **Demonstration**, is strongly related to the previous ones, though we have to distinguish them, due to the latter acts as the actual demonstration process with the physical presence of all relevant partners and pilot execution in real world conditions. The lessons learnt identified during this phase are introduced as follows.

Lesson 8: Real-world testing and active stakeholder engagement provide critical insights into system performance and offer feedback for continuous improvement
Pilots' execution in real-world environment help reveal unpredictable issues. Feedback loops from stakeholders can provide fine-tuned aspects for the ODYSSEUS integrated solution.

Lesson 9: External factors, such as weather conditions, transport delays (train/ferry cancellations), or long vehicle queues, should be taken into serious consideration
Unforeseen external conditions can derail pilots' execution plans. By incorporating flexibility into scheduling may mitigate such disruptions.

Mitigation measures:

1. Extensive discussions with stakeholders gather insights into potential disruptions and necessary adaptations.
2. Flexible scheduling and back-up plans help adjust to real-time challenges, ensuring smooth operations.

Last but not least was the **Evaluation phase** which is highly pertained to the Pilot Validation, Pilot Assessment and User Acceptance Evaluation, and its title reveals that it assesses the effectiveness of the demonstration through performance metrics and KPIs. The lessons learnt are following.

Lesson 10: User experience and ethics questionnaires/surveys preparation raises awareness and transparency

Diving into user experience and ethical considerations is critical for technology adoption and helps raise awareness among stakeholders and ensures transparency in the pilot processes. These surveys also provide valuable data on user perceptions and system performance, improving acceptance, identify concerns, and ensure compliance with ethical regulations.

Lesson 11: Assigning KPIs per partner and clearly defining measurement methods enhances accountability and performance tracking

Assigning KPIs to partner ensures accountability and transparency, resulting in aligning expectations on the project's outcomes.

Mitigation measures:

1. Expert-prepared, GDPR-compliant questionnaires ensure transparency and regulatory compliance.
2. Early KPI allocation, along with a well-structured responsibility matrix, ensures effective monitoring and reporting.

As a key takeaway of the ODYSSEUS project, the critical role of the end-users' thorough understanding in the technological solutions to be developed. This might help in a wider adoption, which hinges on clear communication, comprehensive training, and iterative feedback from them. It is notable that the project demonstrates that a collaborative, user-centred approach enhances the viability of ODYSSEUS innovations and maximizes the long-term ODYSSEUS real-world impact.

3.3.2. Gap Analysis

In ODYSSEUS the gap analysis was conducted at two axes:

- Analysis of state-of-the-art technologies and processes was conducted by workshops with border control partners and technological experts.
- Surveys were conducted for travellers, border control officers and technological border control experts to collect perception of current processes and define requirements of the ODYSSEUS platform as perceived by the stakeholders.

The results of the border control state of the art provided following improvement points:

- **Cost of the border crossing**: cost of deployment of new equipment and training of new staff is a significant problem for the BCA and reduction in either would improve both the efficiency of the process and traveller experience.
- **Expertise of BCA staff and process guidance**: the efficiency of the process and ability to detect fraud strongly depends on experience of the BCA teams. The experience impacts the ability to detect document forgery, identification of suspicious behaviour, ability to find illicit goods and human trafficking. Deployment of guidance systems that would increase detection rates for less experienced staff would be an improvement to security of the border crossing.
- **Deployment of advanced tools**: even though there are advanced tools and technologies available on the market they are rarely deployed due to cost reasons.

In review of technologies selected for border crossing in ODYSSEUS we identified following gaps:

- **Paperless border crossing**: usage of digital credentials for travel are at early stage of deployment. Even though the specification has been ready for several years there is no large-scale deployment, only pilots are ongoing and all activities are related to border crossing for airports.

The deployment models have several gaps: there are legal and organizational gaps in who will be responsible for identification of the travellers, who will be responsible for issuance of the DTC and who will be responsible for the data processing of the travellers.

At technical levels we identified a few gaps that prevent deployment of the DTC on smartphones when it is currently impossible for iOS and deployment on Android is possible only with a workaround.

- **Touchless border control** based on face match technologies is currently in pilot mode for airport border crossing but was not yet tested or piloted in other types of crossing.
- **UAV deployment** for border crossing is hindered by technological gaps in the UAVs themselves. The UAVs for deployment in such conditions need high battery time, high load due to additional sensors needed to collect required information, they also need to be able to transmit high amount of data collected from the sensors.

  Process wise the UAVs need to be autonomous during the scanning to reduce staff needed for their deployment.

- **X-ray scanning technology** currently has low dosage, but still too high enough to be regulated for large-scale deployment. Current solutions are focused on container scanning for illicit goods, but in BC environment the detection of unauthorized persons is as important. There is a lack of solutions capable of detection of chemical, biological and explosive threats.

Current solutions may be improved by AI usage to increase detection for less experienced staff.

- **Crowd monitoring and counting** was never deployed in BC environment before and parameters of such solution such as crow density detection, occlusion need to be adjusted and the solution deployment customized for BC lighting conditions and camera placement. We also expect the crowd dynamics will be different than in standard conditions the solution was deployed in.
- **AI and XAI deployment** for decision support in BC conditions is an ODYSSEUS innovation and we expect several gaps to be addressed:
  - Accuracy: such solution needs to provide accurate decision support which will rely on correctness and representativeness of training data.
  - Security and privacy: the solution will be operated in highly sensitive environment and handle personal information.

Explainability: the decision support system needs to provide optimal guidance and transparency regarding the risk assessment. The system may have impact on fundamental human rights, so it needs to provide maximum information why the traveller risk was assessed.

3.3.3. Recommendations on possible standardization activities and strategies for policy experts

3.3.3.1. Overview

The ODYSSEUS project aims to enhance border security and operational processes through a well-structured standardisation strategy. The project is divided into three phases. In **Phase 1,** the Standardisation Task Force is established, and preliminary mapping is conducted through an online survey to gather initial data and insights. **Phase 2** involves engaging project partners and end-users in workshops to ensure collaborative development. During this phase, a detailed analysis of innovations is performed, and the Action Plan is defined. **Phase 3** focuses on implementing the Action Plan, with continuous monitoring, evaluation, and reporting in last deliverables of the project.

3.3.3.2. Applicable Standards Identified

Several applicable standards have been identified for the ODYSSEUS project. For digital and virtual passports, the ICAO Digital Travel Credentials (DTC) and ICAO Doc 9303 are relevant. UAV-assisted X-Ray technologies should comply with ISO/IEC 27001, ISO 9001:2015, and ISO 14001:2015. Seamless identity verification in border crossing scenarios must adhere to ICAO standards and ISO/IEC 19794-5 compliance. Multi-modal fusion and AI-based decision support systems should follow ISO/IEC 23894:2023, ISO/IEC TR 24028:2020, and ISO/IEC TR 24027:2021. Behavioural authentication models need to comply with ISO/IEC 27001, ISO/IEC 23894:2023, and ISO/IEC TR 24028:2020.

3.3.3.3. Feedback and Contributions

Feedback and contributions are essential for refining these innovations:

- **Digital and Virtual Passports**: Usability on mobile devices, Integration with legacy systems.
- **UAV-assisted X-Ray Technologies**: Safety standards, Ethical considerations, Data protection standards, Interoperability, Regulatory compliance, Quality assurance, Environmental impact.
- **Seamless Identity Verification**: Efficiency standards, Cost reduction standards, Quality standards.
- **Multi-modal Fusion and AI-based Decision Support Systems**: Quality decision-making standards, Trustworthy AI principles.
- **Behavioural Authentication Models**:
- Anonymization, Encryption, Ethical AI principles.

3.3.3.4. Engagement with Standardisation Bodies

Engagement with relevant standardisation bodies is a key part of the strategy. The ODYSSEUS project will be presented to the ICAO NTWG on the topic of future forms of eMRTD and associated systems. Additionally, the project will be showcased at the CEN TC 224 Plenary meeting in June 2024. These presentations will help position the ODYSSEUS project as a leader in border security innovations and standardisation.

3.3.3.5. European Commission's Standardisation Strategy

Launched on February 2, 2022, it aims to:

- **Bolster EU Leadership**: Enhance the EU's leadership in global standards.
- **High-Level Forum**: Establish a High-Level Forum on European Standardisation to set priorities.
- **Improve Governance**: Enhance governance within the European standardisation system.
- **Strengthen International Standardisation**: Strengthen the European approach to international standardisation.
- **Support Innovation**: Connect research and innovation with standards.
- **Promote Academic Awareness**: Increase academic awareness and prepare future standardisation experts.

3.3.3.6. Conclusion

- In conclusion, the ODYSSEUS project's standardisation strategy is designed to ensure that innovations are efficiently delivered. By engaging with key standardisation bodies and adhering to identified standards, the project aims to enhance border security and operational efficiency.

3.4. TENACITy use cases

The TENACITy project aims to enhance travel intelligence and security through the implementation of advanced data analysis, risk management, and interoperability frameworks. The project's overarching objective is to modernize travel intelligence governance through the following key objectives:

- Increasing Data Reliability by enhancing the accuracy and consistency of PNR data through advanced analysis and pattern identification tools.
- Strengthening Risk Management through cutting-edge AI and agent-based modelling approaches to predict and mitigate security threats.
- Enabling Secure Data Exchange through blockchain technology to safeguard data integrity and privacy.
- Promoting Interoperability by ensuring seamless integration of new tools into existing operational environments.
- Enhancing Stakeholder Trust by applying societal frameworks to improve transparency and citizen engagement.

While each case study is tailored to its specific operational environment, they share these common goals.

Use Case "Known Suspect Traveling Between Member States"

This piloting case study addresses the challenge of tracking a known criminal moving between European countries. Due to the absence of API data for intra-Schengen movements, the use case emphasizes the improvement of PNR data reliability by collecting and analysing data from multiple points along the suspect's journey. By leveraging risk management and pattern identification, law enforcement agencies from Greece and Spain will collaborate to increase situational awareness and exchange reliable travel intelligence.

Key innovations include:

- Advanced PNR data verification and enhancement through cross-border collaboration.
- Real-time behavioral pattern analysis to track suspect movements.
- Secure data exchange through blockchain for reliable and tamper-proof information sharing.

Use Case "Firearms Trafficking"

This piloting case study targets the detection and prevention of illegal firearms trafficking into the EU via third countries. Utilizing open-source intelligence from darknet data sources, the project aims to track operational patterns of firearm trafficking networks. The solution will integrate resilience-oriented risk management, addressing systemic risks associated with violence enablers. By combining OSINT with travel intelligence governance, law enforcement and customs authorities will collaborate to mitigate firearm smuggling threats.

Key innovations include:

- Advanced threat pattern detection using OSINT and AI-driven risk assessment.
- Secure cross-border data exchange for coordinated response.
- Real-time tracking of criminal networks via advanced pattern identification techniques.

Use Case "Lone Terrorist or Small Group Entering Europe"

This case study focuses on the challenge of identifying unpredictable movement patterns of lone terrorists or small groups entering Europe from third countries. By employing advanced pattern identification combining AI with agent-based modelling, the system aims to detect emerging risks from individual or small group behaviors, predicting their next movements and possible threats. Collaboration between UK and European LEAs will ensure comprehensive data integration and rapid response to emerging threats.

Key innovations include:

- Combining AI-driven pattern recognition with agent-based modelling for enhanced threat prediction.
- Real-time data analysis from diverse data sources to identify and mitigate risks.
- Secure and transparent data sharing through blockchain technologies.

Use Case "Virtual Setting"

In this unique piloting case study, a virtual simulation environment will be created to test interoperability and integration of TENACITy's solutions with existing law enforcement frameworks. The primary goal is to demonstrate the project's capability to enhance collaboration among diverse stakeholders while preserving data security and privacy through blockchain technologies.

Key innovations include:

- Virtual integration of multiple data sources and operational frameworks.
- Comprehensive testing of interoperability between new and legacy systems.
- Privacy-preserving data exchange with blockchain.

3.4.1. Lessons learnt

Through practical pilots, technical innovation, and stakeholder engagement, the project generated critical insights into how data-driven approaches can enhance law enforcement capabilities while respecting legal and ethical boundaries. This section synthesizes part of the key lessons learned from the project.

3.4.1.1. Strategic Use of PNR Data & Travel Intelligence

The strategic application of Passenger Name Record (PNR) data and travel intelligence has proven to be a valuable asset in enhancing preventive measures against a spectrum of transnational crimes. One of the key lessons from the project was that the analysis of travel patterns, can significantly bolster efforts to detect and mitigate threats such as terrorism, human trafficking, and organized crime. By identifying behaviour that aligns with known criminal methodologies, authorities are able to intervene before illegal activities occur, thus contributing to more effective and proactive security operations.

However, the relevance of PNR data is not uniform across all crime types. It demonstrates the greatest utility in addressing offenses closely linked to travel logistics, including drug trafficking and migrant smuggling. In contrast, its value diminishes for crimes with less direct travel components, such as environmental offenses or the trafficking of cultural goods. This distinction underscores the need for strategic deployment of PNR data in areas where it has the highest preventive and investigative return.

Certain data fields within the PNR system have proven to be particularly impactful. These fields allow for a nuanced understanding of passenger behaviour and facilitate the identification of anomalous or suspicious patterns that may warrant further investigation.

A key outcome emerging from the project is to broaden the scope of PNR data collection. Currently, systems largely focus on commercial aviation; however, expanding to include private aviation and additional transport modes would significantly improve detection capabilities and enable a more comprehensive response to illicit activities. Additionally, the systematic and timely sharing of intelligence among EU Member States is essential.

3.4.1.2. Risk Assessment Methodology

The project also shed light on the importance of refining risk assessment methodologies. Tailored risk indicators, developed from patterns substantially improve the precision of identifying high-risk individuals. These indicators are not designed to establish guilt but rather to highlight behavioural similarities with previously known offenders, acting as a trigger for deeper investigative scrutiny.

Nevertheless, there is an inherent need for caution when interpreting risk scores. A high score indicates potential alignment with known risk profiles but does not equate to criminal intent. Thus, expert interpretation and the incorporation of complementary intelligence are essential to avoid false positives and to maintain the credibility of the assessment process.

The integration of artificial intelligence and machine learning technologies further enhanced the detection process. The TENACITy project demonstrated how AI-based tools can identify anomalies, establish links between passengers, and map broader criminal networks. While these tools offer substantial potential, their operational use must be carefully aligned with existing and

forthcoming regulatory frameworks, particularly those outlined in the EU AI Act. Clear legal guidance and standards are necessary to support the responsible and lawful application of these technologies.

An ongoing barrier to methodological innovation is the restricted access to real PNR data due to legal constraints. These limitations hinder the ability to validate tools at scale and slow the development of more effective detection systems. A more flexible and harmonized EU-wide data policy would be instrumental in supporting cross-border innovation, enabling Member States to collaborate more effectively and bring novel solutions into operational use.

3.4.1.3. Operational & Technological Implementation

From an operational standpoint, the project highlighted several implementation challenges and opportunities. The use of the SIENA network remains mandatory for secure communication among Member States, yet the project explored alternative solutions such as Distributed Ledger Technologies (DLTs) including Blockchain. These alternatives offer more flexible and secure options that could potentially complement or enhance current systems.

Since access to real data was not feasible, the development and deployment of synthetic datasets became a necessity. High-quality synthetic data proved essential in training and validating AI tools, allowing for experimentation and refinement without compromising privacy or breaching data protection regulations. This approach supports continued innovation in the absence of live operational data.

Another operational strength was the integration of Open-Source Intelligence into Passenger Information Unit (PIU) workflows. End-users responded positively to this addition, noting that it enhanced situational awareness and added context to PNR data. The inclusion of OSINT sources allowed for more comprehensive risk assessments and facilitated cross-validation of data points.

Although there was broad support for the adoption of AI tools in the PIU environment—particularly for tasks such as similarity searches, anomaly detection, and network mapping—there remains a degree of caution. Legislative clarity and governance structures must evolve to keep pace with technological advancements, ensuring that these tools are deployed ethically, lawfully, and effectively.

3.4.1.4. Pilots & Training: Methodological Lessons

The pilot initiatives and associated training programs provided valuable methodological insights. Chief among these was the importance of early stakeholder engagement. When local partners and end-users were involved from the outset, there was higher alignment, smoother adoption, and more relevant outcomes. Conversely, delayed engagement often led to inefficiencies, miscommunication, and reduced impact.

Flexibility emerged as another critical factor for success. Real-world pilot scenarios demanded adaptability, and rigid implementation frameworks were often impractical. Teams that employed a more dynamic, responsive approach were better able to manage unforeseen challenges and capitalize on emerging opportunities.

In terms of capacity building, blended training formats proved most effective. Combining online modules, in-person sessions, and on-the-job training allowed for wider participation and deeper learning. This approach accommodated varying learning preferences and operational realities, leading to more meaningful skill development.

Lastly, the emphasis on continuous learning was a key takeaway. The most successful pilot programs included not just initial training but also follow-up modules, peer exchange sessions, and refresher courses. These components helped sustain knowledge over time and fostered a culture of ongoing professional development within PIUs.

Taken together, these lessons highlight the multifaceted nature of PNR data utilization and underscore the need for strategic, adaptable, and collaborative approaches to maximize its value in safeguarding EU citizens and upholding justice across Member States.

3.4.2. Gap Analysis

A comprehensive gap analysis was carried out to identify inefficiencies and improvement opportunities within operational workflows, ensuring alignment with strategic goals and technological progress. The analysis followed a three-step methodology:

- Step 1: Assessed the current state, including a detailed review of the technologies in use.
- Step 2: Highlighted recommendations for technological, operational, and other enhancements based on real-world gaps and direct input from end-users.
- Step 3: Proposed solutions aimed at improving the efficiency and effectiveness of the Passenger Information Units in combating crime and terrorism.

Some preliminary results are presented in the table below.

Current Status	Technology used	Operational / Technology Gap	Proposed Solution
Data silos, limited interoperability and integration capabilities for travel data	Legacy data processing systems, non-interoperable databases	Challenges in integrating diverse data sources and analysing complex data effectively	Deployment of TENACITy Open Architecture allowing comprehensive data integration and advanced analytics capabilities
Limited pattern recognition capabilities; inadequate tools for detailed travel behaviour analytics	Conventional data analysis techniques, limited machine learning integration	Insufficient granularity and accuracy in identifying travel patterns and criminal behaviours	Application of advanced Pattern Identification Tool utilizing ML and Deep Learning for enhanced behaviour clustering and anomaly detection
Manual, cumbersome risk assessment processes; slow threat identification and response	Traditional manual risk evaluation processes	Lack of automated and efficient risk assessment mechanisms; limited real-time responsiveness	Implementation of the Risk Management Tool featuring automated, GUI-driven risk rule formulation and real-time risk scoring capabilities
Inefficient OSINT processes; limited Darknet data integration capabilities	Basic OSINT practices without advanced analytics or automated risk assessment	Challenges in retrieving high-quality, targeted data from complex sources (Clearnet and Darknet)	Advanced OSINT/Web Crawling Tool with targeted data retrieval, ML-based context awareness, and integrated risk assessment features
Security concerns and limited transparency in PNR/API records exchange	Centralised databases vulnerable to single points of failure and unauthorized access	Lack of secure, transparent, and auditable exchange mechanisms for sensitive data	Blockchain-based Tool employing Hyperledger and IPFS, including smart contracts to ensure decentralized, secure, and auditable data exchange
Complex and manual analysis of criminal organisations; limited predictive and visual analytical support	Basic manual analytical methods, insufficient predictive capabilities	Difficulties in visualizing, summarizing, and predicting criminal organisation activities	AI-based Criminal Organisation Persona Tool utilizing predictive analytics, persona generation, and advanced visualization for enhanced investigative efficiency
Fragmented travel intelligence governance; limited oversight in human rights integration	Legacy compliance frameworks; traditional monitoring approaches	Lack of integrative governance approach combining legal, ethical, societal, and technological dimensions	Implementation of TENACITy Governance Framework combining dialogue, negotiation, and consensus-based oversight mechanisms

3.4.3. Recommendations on possible standardization activities and strategies for policy experts

Recommendation 1: Broaden PIUs' Scope to Include All Transport Modes

Description: The European Union and its Member States are encouraged to adopt a consistent and coordinated framework to expand the operational mandate of Passenger Information Units beyond aviation, encompassing maritime, rail, and bus travel. This expansion should be guided by the principles of necessity and proportionality to ensure a fair and balanced approach to data collection and passenger privacy. In today's interconnected transport landscape, individuals involved in terrorism or serious criminal activity may deliberately avoid air travel, which is currently the most regulated mode, by using alternative means of transport. By extending PIU capabilities to cover these additional travel modes, authorities can close critical gaps in information sharing that may be exploited by offenders using complex or indirect routes, commonly referred to as "broken travels." A comprehensive approach to collecting and analysing travel data across all transport sectors would provide a unified view of passenger movements across the EU, significantly improving the accuracy and effectiveness of threat detection and response. It would also strengthen cross-border cooperation, enabling Member States to exchange data more efficiently and respond faster to emerging threats. Moreover, this integrated system would avoid duplication of efforts across different agencies, lead to better use of existing resources, and enhance operational synergy. Importantly, a transparent and proportionate implementation of such a framework would contribute to increased public trust, as citizens would see the EU taking proactive and equitable steps to safeguard transportation systems.

Recommendation 2: Advance Automated Tools for Generating Data-Driven Risk Indicators

Description 2: It is recommended that the European Union and its Member States prioritise the development and refinement of automated tools designed to generate risk indicators based on previous detection cases and operational feedback. These tools, driven by machine learning and data analytics, can analyse historical records of confirmed cases alongside evaluations from Passenger Information Unit (PIU) operators to identify patterns and propose new, evidence-based risk indicators over time. To maximise the relevance and reliability of these suggestions, the integration of real-time feedback mechanisms is essential. PIU personnel should be able to confirm or dismiss alerts, with these decisions feeding directly into the system to fine-tune how specific factors are weighted or combined in future proposals. Suggested indicators should include clear explanations of how and why they were generated, including the criteria used and their relative importance. This level of transparency is critical for maintaining oversight and ensuring that the system's outputs remain understandable, justifiable and in line with the AI Act. All proposed risk indicators should be subject to manual review by trained analysts, who can assess their operational value, adjust them if needed, and determine whether they warrant temporary implementation for evaluation in real-world conditions. This collaborative process, blending automated efficiency with human judgment, enables PIUs to stay agile in the face of shifting threats while maintaining strong control over the decision-making process. Ultimately, the use of adaptive, data-driven risk indicators will strengthen the EU's capacity to detect and respond to serious crime and terrorism in a timely, targeted, and proportionate manner.

Recommendation 3: Establish Secure AI Sandboxes with Legal Access to Operational Data

Description 3: To unlock the full potential of artificial intelligence in the field of security and risk detection, it is recommended that the European Union and its Member States facilitate the creation of secure AI sandbox environments where researchers can access and test models using realistic datasets. At present, a significant barrier to progress lies in the limited availability of operational data from Law Enforcement Authorities (LEAs), owing to the highly sensitive nature of such data and strict data protection obligations. While these concerns are valid and necessary, they must be balanced with the need to foster innovation and evidence-based policy-making. To address this challenge, controlled and legally compliant environments such as Sandshould be established to allow authorised researchers to experiment with anonymised or synthetic data that reflect real-world complexities. These data could be sourced from transport carriers, mandated data providers, or LEAs, provided that clear legal grounds and safeguards for data processing are in place. Such sandboxes would serve as testing grounds where machine learning models can be trained, evaluated, and fine-tuned in conditions that simulate real operational environments without compromising individuals' privacy. This approach would enable the development of more accurate and responsible AI tools for use in areas such as risk assessment, anomaly detection, and pattern recognition. It would also encourage stronger collaboration between the research community, public authorities, and industry stakeholders. Ultimately, the creation of secure, transparent, and well-regulated AI sandboxes would accelerate technological advancement in a way that aligns with both EU data protection standards and operational needs, ensuring that security innovations are not hindered by a lack of accessible, actionable data.

4. Conclusions

In this section the four projects have summarized the common needs and the commonalities that emerged during the different iterations and the two synergy workshops that have been organized.

4.1. Commonalities

The projects highlighted the importance of **systems interoperability** even if each project is using a different approach to exchange data because of the context.

Biometric **data exchange** among LEAs, people travel experience (notwithstanding the fragmented travel intelligence governance) and data interoperability among BCP are of primarily importance. But the interoperability suffers of two constraints: legal and regulatory constraints, the confidentiality and the lack of real data.

Moreover, two other commonalities have been identified:

- the usage of the blockchain for accessing people/travellers and goods information
- the extraction of patterns from raw unstructured data

4.2. Needs

1. **Common Methodology for Risk Assessment**: to establish a standardized risk assessment methodology that can be applied across all operations, processes, or security projects. This will ensure consistency and allows for the integration of diverse risk factors (e.g., financial, technical, operational) defining a unified data model whose output should be pursued by the projects.
2. **Training:** to recommend the dissemination leaders to implement training programs during the projects focused the usage with proficiency of the developed tools. Training should be planned with a market-oriented profile, in order to have the end users of the projects as the primary customers of the tools.
3. **Uniform Method for Data Generation**: to develop a consistent method for generating synthetic data to be used as a knowledge base for the different topics of HORIZON clusters. This could involve defining clear data standards (formats, structures, sources) to ensure that all data is comparable, accurate, and easy to analyse. Data management platforms or frameworks, such as ETL (Extract, Transform, Load) processes, can help standardize data workflows, ensuring uniformity and quality. All projects could start from this knowledge base enriching it at the end of the development and testing cycle.
4. **Best Practice for Extracting Operational Scenarios and requirements:** Extracting operational scenarios requires a structured approach to ensure that all relevant information is captured and the scenarios are useful for decision-making, forecasting, and tactical planning. The need here is to build a knowledge base that should contain all the historical data from which to extract recurring operational patterns. The knowledge base could be built by leveraging automation for data collection and scenario generation. This could include data analytics platforms, AI models, or specialized software to collect, analyse, and

generate operational scenarios in real-time, reducing manual errors and saving time and above not disclosing to requestors of new scenarios all the confidential information to similar scenarios stored by different project on behalf of different end users participating to the projects. The knowledge base could be useful also to store requirements and to extract patterns from the knowledge base through the usage of AI tools in order to suggest very well consolidated and standardized requirements

The implementation of these needs will would streamline processes, reduce inconsistencies, and ensure that all stakeholders of research projects are aligned in terms of risk management, data generation, and scenario extraction and training.

5. Acknowledgements

FLEXI-cross – Funded by the European Union under Grant Agreement no. 101073879. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

TENSOR – Co-funded by the European Union under Grant Agreement no. 101073920. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

ODYSSEUS – Unobtrusive Technologies for Secure and Seamless Border Crossing for Travel Facilitation. ODYSSEUS has received funding from European Union's Horizon Europe Innovation Programme under Grant Agreement N°101073910. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

TENACITy – Funded by the European Union under Grant Agreement no. 101074048. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or REA. Neither the European Union nor the granting authority can be held responsible for them.