PiQASO

D6.1 - Communication, Dissemination, and General Awareness Plan

Grant Agreement	101190366
Project Title	DIGITAL-ECCC-2024-DEPLOY-CYBER-06
Project acronym	PiQASO
Project Start Date	01 January 2025
Number of Deliverable	D6.1
Report Title	Communication, Dissemination, and General Awareness Plan
Related Work Package	WP6
Related Task	T6.1, T6.2, T6.3
Lead Organisation	PLUR
Submission Date	30.06.2025
Last Change Date	30.06.2025
Dissemination Level	Public

EUROPEAN PARTNERSHIP

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Abstract

This document is the Communication, Dissemination and Exploitation Initial Plan for the PiQASO project. It contains detailed information about the Communication and Dissemination strategy, and the preliminary Exploitation strategy. It includes targets, key messages, information about branding, channels, social media, publications, events and overall KPIs both communication and dissemination actions.

Authoring & approval

Author(s) of the document

Name (Organisation name)	Date
Nicola Marcialis (PLUR)	22.05.2025
Savvoula Oikonomou (UBT)	27.05.2025
Maria Poulimenou (UBT)	27.05.2025
Angelina Broukou (UNILU)	05.06.2025
Romain Muguet (RAL)	13.06.2025
Isaac Dangana (RAL)	13.06.2025

Reviewed by

Name (Organisation name)	Date
Savvoula Oikonomou (UBT)	20.06.2025
Angelina Broukou (UNIL)	20.06.2025

Approved for submission to -

Name (Organisation name)	Date
Savvoula Oikonomou (UBT)- Project Coordinator	30.06.2025

Rejected by[1]

Name (Organisation name)	Date

[1] Representatives of the beneficiaries involved in the project

EUROPEAN PARTNERSHIP
Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Document history

Version	Date	Contributor/Organisation	Additional information
00.00	29.04.25	Nicola Marcialis (PLUR)	Table of Contents (First initial draft) First setup of the deliverable, identifying specific action items per partner
00.01	03.06.2025	Nicola Marcialis (PLUR) Savvoula Oikonomou (UBT) Maria Papadopolou (UBT) Romain Muguet (RAL) Isaac Dangana (RAL) Angelina Brokou (UNIL)	initial inputs collected on section 1, 2, 3, 4, 5, 6
00.02	13.06.2025	Nicola Marcialis (PLUR)	Processed all inputs into a coherent and readable deliverable. Transmitted to reviewers
00.03	20.06.2025	Savvoula Oikonomou (UBT) Angelina Brokou (UNIL)	Deliverable review
00.04	23.06.2025	Nicola Marcialis (PLUR)	Final draft version to be approved by PC
01.00	30.06.2025	Savvoula Oikonomou Project Coordinator	The document delivered to the EU Commission

PiQASO

Post-Quantum Cryptography As-a-Service for Common Transmission Systems and Infrastructures

The project funded under Grant Agreement No. 101190366 is supported by the European Cybersecurity Competence Centre

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them."

Table of contents

EUROPEAN PARTNERSHIP
Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

List of figures

List of tables

1 Introduction

1.1 Structure of the document

This section outlines the organizational framework of the deliverable, explaining how the document is structured to ensure clarity and coherence. It introduces the main chapters and sub-sections, each addressing a key component of the PiQASO project's communication, dissemination, and exploitation strategies. The structure is designed to guide the reader through an overview of the project, followed by detailed plans for communication and dissemination, performance measurement mechanisms, and collaborative synergies. Additionally, it highlights how the exploitation and sustainability of project results will be approached. This logical layout supports both comprehension and practical use by project partners, stakeholders, and evaluators.

This deliverable is organized into six main chapters, each addressing a crucial aspect of the PiQASO project's Communication, Dissemination, and Exploitation (C/D/E) framework. The structure has been designed to guide the reader through the background, strategy, actions, and expected impact of these activities.

- **Chapter 2:** PiQASO Project Overview. This chapter provides a comprehensive introduction to the PiQASO project, outlining its strategy, goals, key messages, and keywords relevant to communication and dissemination activities. It identifies the project's stakeholders and target groups across industries, research, and policy domains and presents mechanisms for measuring performance through KPIs and tracking tools.

- **Chapter 3:** Communication Strategy . This chapter details the communication objectives, tactics, and tools that will be employed to raise awareness and ensure engagement with PiQASO's stakeholders. It includes the editorial plan, branding elements (logo, templates, press kit), and the main communication channels such as the website, social media platforms, events, publications, and newsletters. The division of roles and responsibilities among project partners is also defined.

- **Chapter 4:** Dissemination Strategy. This section describes the dissemination approach and how project results will be shared with the scientific, industrial, and policy communities. The strategy includes participation in workshops, conferences, publications, and educational activities, ensuring that project outcomes reach relevant audiences and contribute to further research, standardization, and adoption.

- **Chapter 5:** Synergies and Clustering Activities. This chapter outlines how PiQASO will collaborate with related European projects and initiatives. It highlights potential synergies, clustering activities, and engagement with standardization bodies, with the aim of amplifying the impact of the project's results through cooperation and shared activities.

- **Chapter 6:** Exploitation and Sustainability Strategy. The final chapter focuses on the exploitation of PiQASO's results, describing the main tasks in the exploitation process, including IPR handling, identification of Key Exploitable Results (KERs), business model development, and market analysis. The strategy aims to ensure the long-term sustainability and market readiness of the project's technological outputs.

1.2 Definitions

Definitions	Explanations
GENERAL AWARENESS	Understanding and knowledge regarding a topic which is transmitted through a set of communication, dissemination (and eventually exploitation) actions of the topic itself.
LOGO	A symbol or other small graphic design adopted by an organization to identify its product and promote public identification and recognition
ICON	Picture or symbol that appears on a screen and is used to represent a file, an account or an application.
PROJECT FLYER	Small marketing material that is distributed to the public for widespread advertising purposes
PROJECT BANNER	Typically used at events, conferences, exhibitions, is a large-format visual communication tool designed to attract attention and promote the project, to provide immediate visibility, and to convey the project's identity, key messages, or branding elements in a bold and memorable way.
COMMUNICATION ACTIVITIES	All those activities informing and promoting the project, including its concept, ideas, findings, results and success.
EXPLOITATION ACTIVITIES	It is the use of results in further research activities other that those covered by the action concerned, or in developing, creating and marketing a product or process, or in creating and providing a service, or in standardisation activities.
DISSEMINATION ACTIVITIES	Any appropriate means of making the results public (other than those resulting from protecting or exploiting the results, including scientific publication.

Table 1 - Definitions

2 PiQASO Project overview

2.1 About

2.1.1 Project strategy

The primary goal of PiQASO is to bridge the gap between advanced theoretical developments in quantum-resistant cryptography and their real-world applications. This includes developing integration-ready, efficient, and secure PQC solutions that can be deployed across diverse industrial sectors—enabling organizations to proactively prepare for the quantum computing era. The project adopts a comprehensive strategy aimed at translating cutting-edge research in post-quantum cryptography (PQC) into practical, deployable solutions tailored for real-world industrial applications. The strategy emphasizes cross-sector collaboration, co-design with stakeholders, and continuous integration with evolving cybersecurity standards. PiQASO focuses on scalability, interoperability, and efficiency, ensuring that developed technologies can be seamlessly embedded into existing infrastructures. The consortium also emphasizes awareness-raising and skill development to ensure stakeholders are equipped to adopt PQC technologies ahead of the post-quantum transition.

2.1.2 Project goals relevant to Dissemination, Communication & Exploitation activities

The dissemination, communication, and exploitation efforts are designed to support the broader objectives of PiQASO:

- Raise awareness across industries and public administrations about the urgent need for quantum-resilient cryptographic solutions.
- Promote the outcomes of PiQASO through tailored content for diverse audiences including industry leaders, policymakers, and the research community.
- Engage stakeholders via strategic events, media presence, and educational content, facilitating adoption and feedback.
- Ensure project results are leveraged beyond the consortium through coordinated exploitation plans, including IP management and business model development.
- Establish synergies and visibility within the European cybersecurity ecosystem and standardization bodies.

And, in relation to the objectives defined in the Grant Agreement, to:

- Provide input and requirements related to market needs and trends.
- Maximize project's impact by aligning business opportunities with technical activities.
- Ensure proper communication and dissemination of PiQASO outputs.
- Provide recommendations to relevant standardization activities on PQC designs and secure implementations focusing on the interplay between performance and security level.

2.1.3 Project key messages

Quantum threat readiness is now: The transition to post-quantum cryptography is urgent and essential for digital sovereignty and data protection.

- From theory to practice: PiQASO is closing the gap between theoretical PQC advancements and operational deployment in real-world infrastructures.
- Integration-ready and future-proof: Solutions developed in PiQASO are designed to meet current needs while being adaptable for future threats.
- Collaboration strengthens security: In the context of PiQASO project, broad engagement across sectors ensures solutions are robust, interoperable, and adopted widely.
- Europe leads the way: PiQASO reinforces European leadership in cybersecurity by contributing to international standards and industry preparedness.

2.1.4 Project keywords

Post-Quantum Cryptography (PQC)

PQC is at the heart of PiQASO's mission. The project aims to develop and validate quantum-resistant cryptographic solutions to ensure long-term data security in the face of emerging quantum threats.

Cybersecurity

PiQASO contributes to strengthening Europe's cybersecurity posture by providing advanced, deployable cryptographic tools that secure communication systems against both current and future threats.

Quantum-Resistant Algorithms

A primary technical objective of PiQASO is to evaluate, select, and implement quantum-resistant algorithms suitable for integration into critical infrastructures, ensuring resilience in a post-quantum era.

Cryptographic Transition

PiQASO supports organizations in the transition from classical to post-quantum cryptography, offering strategies, tools, and best practices to manage this complex shift securely and efficiently.

Digital Sovereignty

By advancing European-developed PQC solutions, PiQASO helps reduce dependence on external technologies, reinforcing digital autonomy and aligning with EU strategic goals.

Secure Communication

One of PiQASO's practical outcomes is the delivery of secure communication frameworks that are robust against quantum attacks, tailored for industries such as defense, healthcare, and public administration.

Cryptographic Integration

PiQASO emphasizes ease of adoption by focusing on integration-ready cryptographic modules that can be embedded into existing systems with minimal disruption.

Standardization

PiQASO engages with ongoing standardization efforts, contributing practical insights and technical feedback that help shape international PQC standards aligned with European needs.

Awareness

Through its communication strategy, PiQASO aims to raise awareness about quantum threats and the importance of proactive PQC adoption among diverse stakeholders including SMEs, large enterprises, and governments.

Dissemination

PiQASO disseminates its findings, tools, and strategies to relevant audiences via conferences, publications, and digital platforms, ensuring broad visibility and knowledge transfer.

Exploitation

PiQASO includes a clear plan for the exploitation of results, aiming to maximize the long-term impact by supporting commercialization, further research, or policy influence.

Industrial Readiness

PiQASO's deliverables are engineered with real-world constraints in mind—prioritizing performance, scalability, and compliance to ensure they are viable for immediate industrial deployment.

European Cybersecurity

PiQASO contributes directly to the EU's cybersecurity framework by aligning with the objectives of the European Cybersecurity Competence Centre and reinforcing continental leadership in secure digital innovation.

Risk Mitigation

By addressing vulnerabilities posed by quantum computing early, PiQASO empowers organizations to mitigate long-term risks to data confidentiality and integrity.

Technology Adoption

A core objective of PiQASO is to facilitate the adoption of PQC technologies across sectors through demonstrations, training, and strategic stakeholder engagement.

2.2 Stakeholder identification

Stakeholders are individuals or groups that can be directly or indirectly affected by an organisation, project, or similar undertaking. They have a vested interest in the outcome of the project or organisation and may have a significant impact on its success or failure. Stakeholders include customers, employees, suppliers, investors, and communities where the

EUROPEAN PARTNERSHIP
Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

organisation operates. By considering stakeholders' needs and concerns, organisations can build better relationships and enhance their reputation while achieving their goals.

In PiQASO, Universities, companies, and associated partners from various countries will be involved. They represent a broad spectrum of stakeholders ranging from the academic to the industrial sector, including developers, researchers, and organisations focused on cybersecurity and Artificial Intelligence.

2.3 Project target groups

2.3.1 Targets groups identified in the Grant Agreement

A. User Organizations: These constitute the end users and consumers of the various services and applications.

B. Service Providers & Supply Chain Owners (e.g., Automotive, Automation, Energy, Finance, Healthcare, Aerospace, Transportation etc.)

C. Software & Hardware Security Solutions providers: They develop, extend, and provide security solutions.

D. Standardization & Certification Bodies: Impartial third-party operators that verify/certify the fulfilment of the required security and safety guarantees for the target devices stated in related standards and defined Protection Profiles.

E. National & EU Public Authorities & Policy Makers: They include the EC and its agencies, which are of interest in a secure IT landscape.

F. Academia & Research & other projects: They perform state-of the art research & innovation and disseminate their findings.

2.3.2 Use cases sectors of PiQASO project

- Automotive
- Automation
- Finance
- Energy
- Healthcare
- Aerospace
- Online Media
- UAVs
- Transportation

2.3.3 Industry, SMEs, University, Innovation Hubs, and EC Certification

These general categories of target groups critical to the resilience of the EU digital economy can also be identified in the context of the PiQASO project:

- SMEs/MEs, for which inexpensive, automated fixing is key.
- Industry at Large companies, which need large-scale processing for viable AI-enabled DevOps.
- Certification bodies such as the EU Digital SME Alliance, IDSA, and ECSO have dedicated technical WGs in charge of discussing the impact on their stakeholders of the EU legislation related to software development.
- Communities of science and practice need new input in research for scientific progress and widespread product development.
- European Digital Innovation Hubs (EDIH) and Enterprise Europe Network are contributing to boosting EU SMEs' and public sector's capacities in integrating new technologies in their products and services.
- Scientific and open-source communities require reproducibility and evidence-based scientific progress in AI for security and security for AI.
- Citizens are looking to increase their awareness of security and improve trust in digital technologies.
- Policymakers at the national and EU levels are looking for an improved understanding of Open Source and AI-augmented systems in relation to challenges such as EU sovereignty and the upcoming AI legislation.

2.4 Performance measurement

2.4.1 Dissemination & Communication Tracker

To support effective monitoring and reporting of key performance indicators (KPIs) related to dissemination and communication activities, we developed a dedicated tool: the Dissemination & Communication Tracker.

This tracker serves as a centralized management instrument for the Dissemination & Communication leader, enabling them to systematically oversee the implementation status of tasks distributed among consortium partners. As illustrated in Figure [1], the tracker provides a comprehensive overview of all planned dissemination and communication activities, clearly identifying the responsible partners, and internally agreed deadlines. These due dates were established through coordination and consensus between the Dissemination & Communication leader and each individual partner, ensuring alignment with the broader project timeline and goals.

By consolidating this information into a single, accessible document, the tracker enhances transparency, supports accountability, and facilitates timely follow-up on pending tasks, ultimately contributing to the overall efficiency and coherence of the project's communication strategy.

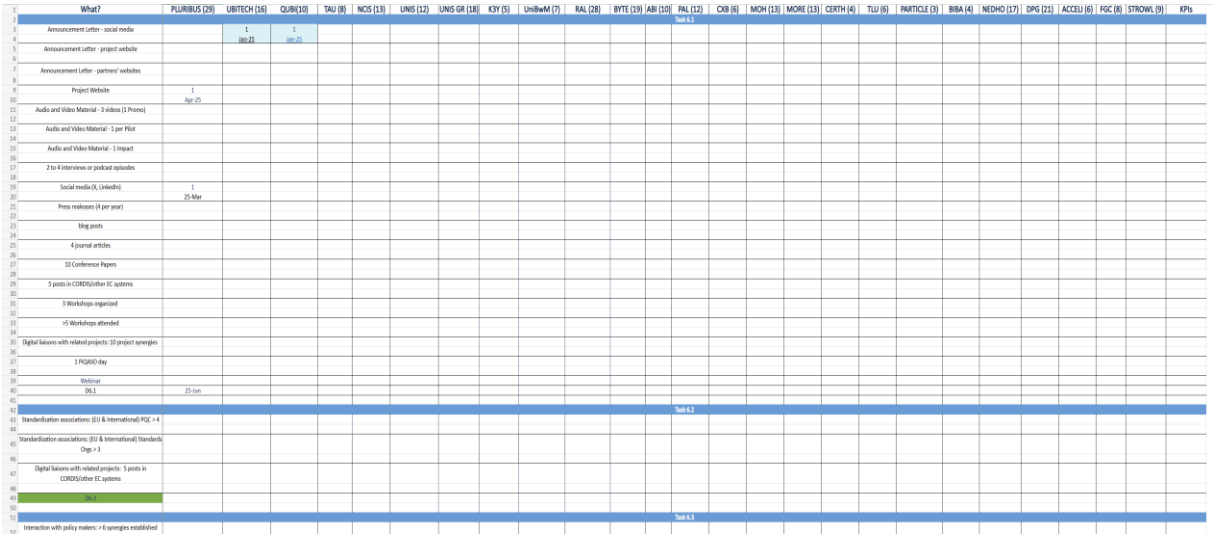

Figure 1 - Dissemination & Communication tracker

Within the same file, consortium partners are invited to record comprehensive information about their individual dissemination efforts. This includes detailed references to any scientific or technical publications they have produced, descriptions of conferences, workshops, or public events they have attended to promote project results, as well as information on datasets they have used or shared in the context of the project. Additionally, partners can report on other relevant dissemination activities they have undertaken, such as media outreach, social media engagement, or website updates. This structured input ensures that all dissemination efforts are properly documented, monitored, and aligned with the overall communication strategy and reporting obligations of the project.

PiQASO - Dissemination & Communication Tracker- Template.xlsx

2.4.2 Communication, Dissemination & Exploitation KPIs

To ensure the successful reach, uptake, and sustainability of PiQASO's outcomes, the project defines a clear set of Key Performance Indicators (KPIs) across the three pillars of outreach: Communication, Dissemination, and Exploitation (C/D/E). These KPIs provide both qualitative and quantitative benchmarks to monitor progress, ensure transparency and accountability, and allow for evidence-based assessment of the impact of our activities.

The KPIs are divided into three phases, following the lifecycle and objectives of the project:

- Awareness Creation – targeting visibility and initial engagement.
- Continuity of Information Flow – targeting knowledge exchange and stakeholder activation.
- Result Orientation – focusing on the uptake and exploitation of results.

The table below summarises the KPIs, timelines, and responsibilities.

KPI	Timeline	Responsible Partner	D/C/E	Notes
Phase 1: Awareness Creation				

EUROPEAN PARTNERSHIP
Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Announcement letter - Reach 3000 people via press releases in public & social media, on project website and on partners' websites	M1	PLUR, UBI	C	
Project website and branding: > 1000 unique visitors > 200 registrants > 350 blog interactions	M2 + throughout the project implementation	PLUR, All partners	D, C	
Audio and Video Material: 1 Promo + 1/Pilot + 1 Impact + 2 to 4 interviews or podcast episodes	Throughout the project implementation	PLUR, All partners	D, C	
Social media (X, LinkedIn): > 500 followers > 400 posts/reposts > 5000 interactions	Throughout the project implementation	PLUR, All partners	D, C	
Phase 2: Continuity of Information Flow				
Press releases (4 per year), blog posts (1000 people reached)	Throughout the project implementation	PLUR	C	
Scientific papers, articles, whitepapers: 4 Journal articles, 10 Conference papers	Throughout the project implementation	UBI, TAU	D	
Interaction with policy makers: > 6 synergies established with policy makers reached via e-mail or physically	Throughout the project implementation	PLUR, UNIS	D, E	
Digital liaisons with related projects: Workshops organized (3) + attended (>5), > 500 visitors, 10 speakers;	Throughout the project implementation	PLUR, UBI, TAU	D, E	
Digital liaisons with related projects: 5 posts in CORDIS/other EC systems;	Throughout the project implementation	PLUR, UBI	D	
Digital liaisons with related projects: 10 project synergies	Throughout the project implementation	PLUR, UNIS, UBI	D, E	
Non-scientific Publications: > 6 Industrial PQC Cyber Security Conferences, 1 exhibition, 1 demonstration days	Throughout the project implementation	PLUR, UNIS, UBI, TAU	D, E	
Standardization associations: (EU & International) PQC > 4, Standards Orgs > 3	Throughout the project implementation	RAL, UBI, TAU	E	
Phase 3: Result orientation				
Pilot Demonstrations/ Workshops: > 1 demonstration per pilot > 20 attendees each	Throughout the project implementation	PLUR, UNIS, NCIS & UC partners	D, E	
PiQASO Day: > 80-100 participants	Towards project end	PLUR, All partners	D	

Table 2 - C&D&E KPIs

1. Awareness Creation (Phase 1 – M1 to M6)

This initial phase focuses on building visibility for PiQASO across multiple channels and audiences, including general public, digital followers, and early adopters in the technical and policy fields. **PLUR** leads the branding, project identity, and launch campaign. Activities such as the project announcement, press releases, and the creation of the website are coordinated by PLUR with content inputs from all partners.

2. Continuity of Information Flow (Phase 2 – M6-M36)

This phase ensures sustained dissemination and stakeholder engagement. **PLUR** continues to coordinate public communication via social media, blogs, and general outreach. **Each partner is encouraged** to contribute to social media campaigns and repost project-related content on their institutional accounts.

UBI and TAU take the lead on scientific dissemination, responsible for the publication of four peer-reviewed journal articles and ten conference papers, in line with open access principles. Policy-oriented dissemination will be supported by **UNIS and PLUR**, aiming to establish at least six policy synergies, through targeted briefings of PiQASO results.

3. Result Orientation and Exploitation (Phase 3 – M25-M36)

The final phase focuses on demonstrating PiQASO's tangible value and facilitating uptake by industry, policymakers, and standardisation bodies.

Pilot demonstrations will be co-organised by **the use case partners (UC) with the support of NCIS** as Work Package 4 leader**, PLUR** as dissemination leader**, and UNIS** as exploitation leader**.** Each pilot is expected to host at least one demo session with a minimum of 20 attendees, ensuring real-world validation and stakeholder feedback loops. The PiQASO Day with the participation of 80-100 attendees, will be organized by PLUR with the support of project partners, towards the project end.

Engagement with **standardisation bodies and industry forums** is led by **RAL, TAU, and UBI**. The goal is to integrate PiQASO's technical outcomes into ongoing discussions around post-quantum cryptography (PQC) and cybersecurity standards at EU and international levels.

3 Communication strategy

The main goal of the project communication is to increase awareness of the project's purpose and progress among the target audience, facilitating the dissemination and the exploitation of the results. The communication strategy is in sync with the objectives and target audiences of PiQASO. The project's aims are transformed into communication objectives, which are then detailed into specific tactics, including establishing a website, leveraging social media, organising events, creating videos and producing papers. The project goals are being refined to formulate dissemination and exploitation objectives, which in turn shape the selection of communication channels.

Communication KPIs (Key Performance Indicators) have been set based on the objective of generating awareness about the PiQASO project. The main tools that have been used to communicate the project are website, social media and newsletters.

Sec. 2.4.2 shows the success metrics that represent measurements against the communications objectives, which have been identified. The KPIs will be reviewed periodically to highlight the strategy's strengths and weaknesses and identify suitable mitigation strategies when needed. These KPIs are connected to others, which are the objectives of dissemination and which we report in section 4.

3.1 Communication objectives

The communication objectives of the PiQASO project are centered on raising awareness, fostering engagement, and promoting understanding of the project's goals, activities, and outcomes among a diverse range of stakeholders. The overarching aim is to ensure that the value and urgency of post-quantum cryptography (PQC) are clearly conveyed to relevant audiences, including industry players, public institutions, researchers, policymakers, and the general public.

Key communication objectives include:

- Increase awareness about the quantum threat and the need for immediate action toward cryptographic transition.
- Promote the PiQASO project's vision, activities, and results through targeted messaging tailored to different audience segments.
- Engage stakeholders and end-users to foster dialogue, feedback, and collaboration throughout the project lifecycle.
- Support the uptake of project outputs by highlighting their practical relevance, integration readiness, and alignment with EU digital sovereignty goals.
- Position PiQASO as a key contributor to Europe's leadership in cybersecurity and standardization in the post-quantum era.
- Ensure consistency and clarity in external messaging, using a coherent brand identity and unified narrative across all channels.

These communication efforts are designed to not only inform, but also to inspire action, stimulate partnerships, and create a supportive environment for the adoption of quantum-resistant solutions developed within the project.

3.2 Communication tactics

In the following points, we will list and explain the communication tactics chosen to achieve the abovementioned objectives.

3.2.1 Editorial plan

The communication tactics will be guided by a structured and responsive editorial plan, which will ensure that PiQASO's messages are strategically delivered, audience-centered, and capable of driving awareness, understanding, and adoption of post-quantum cryptographic solutions. The Plan, as detailed in the following paragraph, will also define shared responsibilities between the involved partners.

PiQASO_Communication -Dissemination strategy_Editorial plan_v01.00.pdf

3.2.1.1 Sharing of responsibilities for communication activities

Following the Editorial plan, after the submission of the present Plan, PLUR, according with the Project Coordinator, will distribute the responsibilities for Communication activities among the partners involved in WP6.

3.2.2 Branding

A strong brand identity is fundamental to the success of communication initiatives. It enhances the brand's visibility, memorability, and credibility within its sector. Developing this identity requires a thoughtful selection of colours, typography, and stylistic choices that reflect the project's mission and values. Once established, these visual and tonal elements must be applied consistently across all communication outputs. Adhering to clear branding guidelines ensures coherence and reinforces the brand's message. Through a well-defined and consistent identity, PiQASO can position itself as a trusted and recognisable player in its field.

3.2.2.1 Logo

The logo balances a technical and trustworthy image with visual simplicity. The combination of the keyhole symbol and orbital-style lines evokes the idea of secured systems, network protection, or intelligent security frameworks.

Below the different design variants of project logo and brand

Figure 2 - Colour and BN project logo

Figure 3 - Colour and BN Brand

3.2.2.2 Brand Book

The Brand Book also known as Brand Guidelines or Brand Manual, is a comprehensive document that outlines the key elements of a brand's visual identity. It serves as a reference and set of instructions for maintaining consistency across all communication channels, ensuring that the project is presented in a cohesive and recognizable manner. The brand book includes specifications on the logo usage (variations, size, placement, and colour options), guidelines for the typography (font size and styles) and the colour palette.

3.2.2.3 Template

Has been developed a set of templates to enhance the efficiency and consistency of the documentations and presentations. The templates include a PowerPoint (.pptx) format for deliverable presentations, a Word template and a Latex format for general documents and a Word template for meeting minutes. These tools provide a unified and user-friendly framework, ensuring a cohesive and professional representation of research findings.

3.2.2.4 Press Kit

The PiQASO Press Kit is a curated set of promotional materials designed to provide essential information about the project. It is available on the PiQASO website and intended for use by media representatives, stakeholders, and communication partners to support accurate and consistent project promotion.

The press kit includes:

- Project Logo – Provided in high-quality formats for print and digital use.
- Project Abstract – A concise summary outlining PiQASO's objectives, scope, and impact.
- Social Media Guidelines – Instructions to ensure consistent and on-brand messaging across platforms.
- Project Images – A selection of visuals representing the project's activities, identity, and context.

These resources help maintain a unified visual and narrative identity, strengthening PiQASO's visibility and outreach across various communication channels.

3.3 Tools and channels

PiQASO leverages a multichannel communication approach that integrates different owned or earned media. This strategy ensures wide dissemination, active stakeholder engagement, and a strong, coherent project identity.

Owned Media	Earned Media
Project Website	Press articles
LinkedIn profile	Industry magazines
Facebook	Invitations to events
X (Twitter) account	Research blogs
ResearchGate presence	Community discussions
Organised events	Third-party social shares
YouTube channel	Academic citations

Table 3 - PiQASO Media Channels

3.3.1 Website

Accessible via https://www.piqasoproject.eu, the website serves as the central hub for all project-related information.

The website aims to:

- Disseminate results and project updates;
- Offer intuitive navigation;
- Encourage newsletter subscriptions;
- Promote accessibility and responsiveness across devices.

The site's visual identity — including the PiQASO logo, font, and colour palette — is harmonized with its presence on social media to ensure a cohesive and recognisable brand experience. Strategically placed call-to-action buttons invite users to subscribe or explore content.

3.3.2 Social media

Social media is a key channel in PiQASO's communication ecosystem. Dedicated accounts on LinkedIn (https://www.linkedin.com/company/piqaso), Facebook (https://www.facebook.com/profile.php?id=61574873307189), X (formerly Twitter, https://x.com/PiQASO_project), YouTube (https://www.youtube.com/@PiQASOproject), and ResearchGate (account to be created) allow us to engage directly with professionals, researchers, and stakeholders.

Official Handles and Hashtags:

- @piqasoproject

- #PiQASO #piqasoproject

PiQASO uses social media to:

- Disseminate news and results;
- Share updates from events;
- Highlight scientific publications;
- Drive traffic to the website and newsletter sign-ups.
- Profile and Cover Consistency

3.3.2.1 Social Media Profile & Cover images

Consistent profile and cover images across platforms ensure visual brand recognition. These assets convey PiQASO's identity at a glance and are updated periodically to reflect project milestones.

Social Media Templates: Pre-designed templates are used for posts, carousels, and event announcements. These ensure visual coherence and help maintain the project's tone and branding.

3.3.3 Events and conferences

Participation in relevant events ensures visibility and engagement with target audiences. PiQASO will be present at:

- Scientific conferences;
- Industrial showcases;
- Co-hosted academic workshops.

A dynamic events calendar will be maintained and updated regularly to reflect new opportunities and project developments.

3.3.4 Media Relations

Proactive engagement with media stakeholders supports broad dissemination:

- Press releases will announce milestones and findings;
- Distribution via partner networks and media lists;
- Encouragement for partners to localise content for regional outlets.

3.3.5 Newsletter

The newsletter reinforces PiQASO's identity and keeps stakeholders informed. At least bi-monthly starting on M7 will cover:

- Key outcomes;
- Project highlights;
- Upcoming events.

It will be distributed via email, promoted on social media, and archived on the website.

3.3.6 Communication material

3.3.6.1 Brochures & project leaflets

Tailored to different audiences, these materials are distributed at events and meetings.

- Brochures: In-depth information, ideal for expert audiences.
- Leaflets: Quick overviews for public engagement.

3.3.6.2 Roll-ups

Used at booths and presentations, roll-up banners enhance visibility and quickly communicate PiQASO's mission and achievements.

3.3.6.3 Videos

Based on project KPIs, throughout the project implementation, with regard to audio/video material, must be produced:

- 1 Promo
- 1/Pilot
- 1 Impact
- 2 to 4 interviews or podcast episodes

These videos will be hosted on the YouTube channel and embedded on the website and newsletters.

4 Dissemination strategy

The dissemination strategy of the PiQASO project aims to proactively share project results with relevant stakeholders from research, industry, standardisation bodies, policy makers, and the open-source community. Dissemination activities are designed to ensure that the project's outcomes are understandable, accessible, and usable by others who can further develop, apply, or build upon them. All dissemination actions are aligned with the PLUR principles: they are Planned, Legitimate, Understandable, and Reachable.

4.1 Dissemination objectives

The main dissemination objectives of PiQASO are:

- Raise awareness of PiQASO's goals, activities, and outcomes among stakeholders across research, industry, and policy.
- Promote the uptake of project results (including methods, tools, datasets, and frameworks) by scientific and technical communities.
- Foster collaboration and feedback loops with other research initiatives, EU projects, and open-source actors.
- Ensure sustainability and long-term visibility of results beyond the project's duration.
- These objectives will be monitored and refined during the project's lifecycle based on stakeholder feedback and project progress.

4.2 Dissemination channels

A diverse set of channels will be used to reach and engage with relevant target audiences, making PiQASO's outputs visible and accessible.

4.2.1 Workshops and webinars

PiQASO will organise dedicated workshops and online webinars to present intermediate and final results, demonstrate tools, and gather feedback from peers. These will be:

- Thematic (e.g., AI robustness, OSS security);
- Interactive (e.g., live demos, Q&A sessions);
- Open to the public or targeted to specific communities (e.g., SMEs, developers, academic groups).

Based on Project KPIs:

- 3 Workshops organized
- 5 Workshop attended (> 500 visitors, 10 speakers).

Workshops will also serve as bridges to standardisation efforts and integration with other EU-funded projects.

EUROPEAN PARTNERSHIP
Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

4.2.2 Participation to third-party events

Partners will actively participate in high-profile third-party conferences and events, including:

- Scientific conferences (e.g., ICSE, NeurIPS, ARES);
- Industry-focused forums (e.g., KubeCon, OWASP);
- EU and national cluster meetings.

This participation will ensure wide dissemination of technical contributions and create networking opportunities with relevant stakeholders. Contributions may include:

- Presentations and posters;
- Demos and pitches;
- Panel discussions and co-organised sessions.

Based on Project KPIs:

- 5 Workshop attended (> 500 visitors, 10 speakers).

4.2.3 Educational resources and training

PiQASO will contribute to the education and training of future professionals by:

- Developing training modules, tutorials, and demonstrators based on project outcomes;
- Integrating content into academic curricula or MOOCs via participating universities;
- Providing open-access learning materials on AI quality, security, and risk management for open-source software.

These materials will be promoted through the project website, educational portals, and partners' institutional channels.

4.2.4 Publications and articles

Scientific and technical dissemination will be carried out through peer-reviewed publications in top-tier journals and conferences in the fields of software engineering, cybersecurity, AI, and open-source development.

Additional efforts will include:

- White papers and policy briefs addressing research directions, challenges, and recommendations;
- Blog articles and technical write-ups targeting a broader audience;
- Cross-publication with other EU projects and contribution to standardisation-related documentation.

Based on Project KPIs, PiQASO aims to produce at least 4 Journal articles and 10 Conference papers in top-tier venues.

5 Synergies and clustering activities

5.1 Standardization & WG Liaison

Within the broader scope of the PiQASO project, this specific task centers on ensuring the project's adherence to and alignment with pertinent global standards and evolving legislative frameworks. This necessitates an inflow of information, meaning PiQASO must be informed by external inputs that could potentially influence its trajectory, design, or implementation. Such inputs are not limited to legal mandates but also encompass emerging best practices, technical specifications, and industry guidelines from various international bodies such as National Cybersecurity Agencies for example (see ANSSI's Follow up position paper on Post-Quantum Cryptography or BSI's joint statement from partners from 18 EU member states).

Conversely, the outward communication from the project is equally vital. It is imperative for PiQASO to actively engage with the external world, disseminating its progress, methodologies, and outcomes. This is where the proactive promotion of PiQASO within relevant working groups and liaison groups becomes important. By engaging with these diverse stakeholders – which may include standards organizations, regulatory bodies, research consortia, and professional associations – PiQASO can effectively share its groundbreaking findings and the innovative solutions it develops. This two-way exchange not only validates PiQASO's work against established norms but also allows the project to contribute meaningfully to the broader discourse, potentially influencing the development of future standards and legislative initiatives in its domain. We are planning to initiate contact with multiple organizations who we estimate might find the outcome of our project interesting.

The process of selecting these organizations to be contacted will include evaluation of their reach and influence in a given technical domain, and their influence in the use of PQC in a geographical area, notably Europe and North America. Examples of such entities include the Internet Engineering Task Force (IETF), for their influence in the standardization and use of cryptography in secure communication that rely on TLS; European Telecommunications Standards Institute (ETSI) for their strong implication in information and communication technologies (ICT) ; ANSSI, the French National Cybersecurity Agency will also be contacted due to their influence in the adoption and use of cryptography particularly in France but also in Europe at large.

When we reach out to these stakeholders, our initial goal will be to create awareness on the work we are doing in PIQASO through presentations, and panel discussions in technical groups and forums. As a second step, we will seek collaborations with interested parties in the standardization of PQC based on our output in this project.

5.2 Identified Synergies

At this stage of the project, we carried out targeted research to identify opportunities for potential synergies with other ongoing or recently completed projects that share similar objectives, themes, or target audiences. The aim of this effort is to foster collaboration, exchange best practices, and amplify the impact of our dissemination and communication activities by leveraging shared knowledge, networks, and resources. As a result of this initial mapping exercise, we have shortlisted a number of relevant projects that align with our goals and areas of interest. We are planning to initiate contact with the coordinators or communication leads of the following projects to explore opportunities for joint activities, mutual promotion, or knowledge-sharing initiatives:

Q-PREP - Quantum-Proofing European Public Administrations: The Q-PREP project aims at fostering a European PQC community by establishing synergies between academic and industrial stakeholders as well as facilitating structured dialogue between these stakeholders. The proposed expertise network shall comprise national and European cybersecurity agencies, public administration networks and organizations, technical experts, and other relevant entities. In accordance to Capgemini own company strategies, Q-PREP envisages the creation of sustainable channels, which shall pave the way towards a robust community and warranty a resilient and reliable cybersecurity environment within the European Union The project will focus not only on the creation and growing of an expertise network, but also will ensure a systematic way of working by identifying of requirements and by creating of a standardized and coordinated roadmap, which shall cover the topic of transition to the PQC era. These developments can be used by public administration entities to accomplish this transition.

PQCSA- Post--Quantum Cryptography Support Action: The PQCSA project will organize the European ecosystem in the area of PQC standardization, to achieve consensus on what cryptographic functionalities and protocols to target and which choices to propose for standardization. A unified European view is necessary to counterbalance the influence of large countries which dominate the tech sector. Consensus will be reached through iterative engagement of researchers, industry as well as the security agencies of the member states and ENISA. Once it is reached, PQCSA will start processes in the respective standardization bodies. Furthermore, PQCSA will deliver a clear and broadly supported PQC migration roadmap to clarify the next steps, when they should be taken, and also what products will be needed to get there. Both serve to give certainty to European industry that their investments will be long lived and supported by EU regulations, whether they are on the side of delivering solutions or requiring solutions. As a third objective, PQCSA will contribute to putting PQC migration on the agendas for companies and decision makers through outreach, dissemination, and training events.

SEQURED - Strengthening Defense Networks for the Quantum Era : SEQURED aims to fortify, future-proof, and enhance the resilience of defence systems and communication infrastructures against potential threats from quantum computing attacks. The project designs a quantum-resistant cryptographic suite for data-sharing, processing, and secure storage. This suite will be resilient to quantum computing advancements and practical for integration into existing defence sector legacy systems, facilitating the transition to the post-quantum era. This will be achieved by developing specifications and implementing prominent quantum-resistant cryptographic algorithms and protocols, optimized for the defence sector's strict timing and security requirements. The project will focus on implementing the four quantum-resistant algorithms.

PQC4eMRTD - Post-Quantum Cryptography for electronic Machine-Readable Travel Documents: The vision of the PQC4eMRTD project is to join forces with world leading European players in the field of security, as well as PQC experts from academia to push previous PQC research results towards the international standardization working groups in order to unlock the implementation of QR protocols, mainly in the fields of digital identities and eMRTDs.

This section will be updated in Deliverable D6.2 – PiQASO Interim Report on Communication, Dissemination, and Exploitation activities (M18) with the established synergies for the project.

5.3 Clustering activities

As part of our broader collaboration strategy, we aim to establish a series of clustering activities with other projects that share similar objectives, target groups, or thematic areas. These activities are designed to promote dialogue, foster mutual learning, and enhance the visibility and impact of project results through collective outreach. By engaging with other initiatives, we seek to identify common goals and explore opportunities for coordinated action.

The planned clustering activities include thematic webinars where project teams can present outcomes and exchange knowledge, interactive workshops focused on addressing shared challenges or developing joint approaches, and participation in dedicated clustering events involving multiple projects. These initiatives will not only strengthen cross-project cooperation but also contribute to building a more cohesive and aligned research and innovation ecosystem.

5.4 Outcomes and impact

Establishing synergies and clustering activities with other relevant projects can lead to a range of meaningful outcomes and long-term impacts. One of the primary benefits is the facilitation of knowledge exchange and mutual learning. Through collaboration, projects can share best practices, methodologies, tools, and lessons learned, which can enhance the quality and effectiveness of their individual efforts and results. This also improves the collective understanding of common challenges and solutions, fostering a more informed and strategic approach to implementation.

Joint activities such as webinars, workshops, and clustering events allow for greater visibility and dissemination of project results. By reaching broader audiences and engaging with diverse stakeholders, these collaborative efforts help amplify the impact of each project's communication strategy. Additionally, working together enables the development of shared outputs—such as co-authored publications, joint tools, or policy briefs—which can hold greater influence than isolated contributions. Engaging in clustering activities also strengthens stakeholder engagement. Events that feature multiple perspectives are often more dynamic and appealing to external audiences, including policymakers, and industry actors.

Ultimately, clustering activities and synergies contribute to systemic change and accelerate innovation by aligning efforts across projects that share common goals. This alignment supports broader strategic objectives. In this way, collaboration not only strengthens individual project outcomes but also enhances their collective contribution to societal and environmental progress.

6 Exploitation and sustainability strategy

6.1 Main tasks involved in the exploitation management process

The exploitation management process encompasses a series of coordinated tasks aimed at maximizing the impact and value of project results. This section outlines the main activities involved in ensuring effective use, dissemination, and potential commercialization of outcomes.

- **Identification and Classification of Key Exploitable Results (M7 – M36)**

The initial phase entails the identification and classification of Key Exploitable Results (KERs), commencing with the development of a comprehensive inventory of technological artefacts and project deliverables. These assets will subsequently be categorized according to their types—such as software, algorithms, protocols, or know-how. Thereafter, each asset will be systematically mapped to the corresponding project partners to facilitate the clarification of potential ownership and intellectual property rights (IPR) considerations.

- **Stakeholder Analysis (M7 – M18)**

The stakeholder analysis involves mapping out all relevant stakeholders, including those from industry, academia, and policymaking sectors. This process aims to gain a clear understanding of each stakeholder's needs, roles, and their influence on the adoption of developed technologies. Additionally, the analysis identifies potential early adopters and strategic partners who could play a critical role in the successful deployment and scaling of the solution.

- **Market and Positioning Analysis (M7 – M18)**

The market and positioning analysis entails a quantitative study of the post-quantum cybersecurity landscape to gain a detailed understanding of the current and future market environment. This includes identifying the overall market size, projected growth, key market segments, and specific application domains. It also involves analysing competitors, alternative solutions, and potential substitutes, as well as tracking relevant technological and economic trends. Based on these insights, the unique value proposition of PiQASO will be defined, clarifying its competitive advantage and strategic position within the market and broader supply chain.

- **Initial Exploitation Analysis (M18 – M30)**

The initial exploitation analysis involves evaluating each identified KER in terms of its readiness level and commercial potential. This includes a thorough assessment using a SWOT analysis to understand the strengths, weaknesses, opportunities, and threats associated with each KER. Based on this evaluation, assets that demonstrate the highest potential for exploitation are identified and prioritized for further development and strategic planning.

- **Business Model Development (M24 – M36)**

Business model development involves creating partner-specific business models using structured frameworks. This includes detailing financial projections, identifying potential revenue streams, and outlining go-to-market strategies tailored to each partner's strengths and objectives. The process also takes into account regulatory requirements and intellectual property protection to ensure that the models are both viable and compliant with legal and industry standards.
The definition of exploitation routes involves exploring viable paths for commercialization, such as licensing agreements, spin-offs, or direct productization of the developed assets. Each asset is carefully matched with the most suitable exploitation route, considering both the nature

of the asset and the interests of the partners involved. Additionally, a risk analysis is conducted for each proposed route to evaluate potential challenges and ensure informed decision-making in the exploitation strategy.

6.2 IPR Handling

Intellectual property (IP) refers to any original creation that holds commercial value and can be traded (European IPR Helpdesk, 2022). It is safeguarded through legal mechanisms such as patents, trademarks, industrial designs, and copyrights. IP encompasses the outcomes of innovation, research, and creative processes. In the context of Digital Europe projects, typical examples of IP include:
- Invention (e.g., device, process, method)
- Software
- Scientific article
- Design Name of a technology/product
- Know-how
- Website
More information on IP can be found in the European IPR Helpdesk (EU-IPR Helpdesk 2022).

Intellectual property rights (IPR) are the legal protections granted to individuals for the creation of their minds, typically providing them with exclusive rights to use their creations for a set period.

The successful commercialization of research results relies heavily on the effective management of IP. Research and demonstration outcomes often require significant additional investment to reach the market, and these investments are only worthwhile if the results are adequately protected. IPR can offer a competitive edge by safeguarding innovations from being copied by competitors, providing a temporary technological advantage, protecting strong brands, helping establish market standards, or securing critical components of an innovation.

Various forms of IPR, such as patents and industrial designs, require novelty to be granted protection. An early public disclosure of the creation may jeopardize its novelty, potentially risking the ability to secure a patent or industrial design. This would prevent the innovator from exercising exclusive rights to the creation, hindering the ability to fully capitalize on it. Through IP protection, innovators can disclose their ideas more securely (European IPR Helpdesk, 2015b).

6.2.1 What is agreed within the Consortium Agreement

6.2.1.1 Results

- **Ownership of result**

Results are owned by the Party that generates them.

- **Joint Ownership**

Joint ownership is governed by Grant Agreement Article 16.4 and its Annex 5, Section Ownership of results, with the following additions:
Unless otherwise agreed, each joint owner has the right to use jointly owned results for non-commercial research and teaching activities on a royalty-free basis, without needing prior consent from the other owners. Each owner is also entitled to exploit the jointly owned results

commercially and grant non-exclusive licenses to third parties, provided that the other owners receive at least 45 calendar days' advance notice and fair, reasonable and mutually agreed compensation. Furthermore, the joint owners must mutually agree on the protection measures for the results and the allocation of any related costs in advance.

- **Transfer of results**

Each party may transfer ownership of its results, including its share of jointly owned results, following the procedures outlined in the Grant Agreement and its Annex 5. Parties may list specific third parties to whom they intend to transfer ownership in Attachment (3) of the Consortium Agreement, with the other parties waving their right to object to these transfers. The transferring party must inform the other parties and ensure officially and in writing that their rights under the agreement are unaffected. Changes to Attachment (3) require a decision from the General Assembly. In the event of mergers or acquisitions, it may not be possible to provide the required 45-day notice for transfers. These obligations remain in effect as long as the other parties retain access rights to the results.

6.2.1.2 Dissemination

For the avoidance of doubt, the confidentiality obligations set out in Section 10 apply to all dissemination activities described in Section 8.4 as far as Confidential Information is concerned.

- **Dissemination of own (including jointly owned) Results**

During the project and for one year after its completion, the dissemination of results by any party, being a member of the project's consortium, including publications and presentations, will follow the procedure outlined in Article 17.4 of the Grant Agreement and its Annex 5, Section "Dissemination." Parties must provide prior notice of any planned publication at least 45 days in advance. Objections, if any, must be submitted in writing to the Coordinator and the proposing party, within 30 days of receiving the notice. If no objection is raised within this period, the publication is approved.

- **Dissemination of another Party's unpublished Results or Background**

A Party shall not include in any dissemination activity another Party's Results or Background without obtaining the owning Party's prior written approval, unless they are already published.

6.2.1.3 Cooperation obligations

The Parties undertake to cooperate to allow the timely submission, examination, publication and defense of any dissertation or thesis for a degree that includes their Results or Background subject to the confidentiality and publication provisions agreed in this Consortium Agreement.

6.2.1.4 Use of names, logos or trademarks

Nothing in this Consortium Agreement shall be construed as conferring rights to use in advertising, publicity or otherwise, the name of the Parties or any of their logos or trademarks without their prior written approval.

6.2.1.5 Access Rights

In Attachment 1, the Parties have identified and agreed on the Background for the Project, and where applicable, have noted any legal restrictions on access. Anything not listed in Attachment 1 is not subject to access rights for Background. Parties can add additional Background by providing written notice, but any modifications or withdrawals from Attachment 1 require General Assembly approval.
Access rights to Results and Background necessary for performing tasks under the project are granted on a royalty-free basis unless otherwise stated. For exploitation purposes, access

rights to Results are granted under fair and reasonable conditions, while access to Background needed for exploitation is also granted on such conditions. Access rights can be requested up to twelve months after the project's end or the termination of a party's participation.
Entities under the same control can request access rights under the conditions of the Grant Agreement, and such rights are granted based on fair and reasonable terms. Access rights may also be granted or refused at the discretion of the owning party and are subject to confidentiality obligations.
For new or leaving parties, access rights are granted based on the terms for Background, with specific provisions for defaulting and non-defaulting parties. Additionally, access rights for software follow the same general provisions, excluding rights to source code or detailed documentation unless explicitly provided.

6.2.2 IPR rules and procedures within PiQASO

6.2.2.1 Development and Project phase

Both the Grant Agreement and the Consortium Agreement outline several rules concerning Intellectual Property Rights (IPR).
The Grant Agreement serves as the legal foundation for carrying out the project and is the official EU contract that defines the main terms for project execution and funding. While the agreement is formally signed between the EU and the project coordinator, all participating partners become individual parties to the contract with the European Commission by signing their respective Accession Forms.
Article 16 of the Grant Agreement defines the rights and obligations of beneficiaries regarding background and project results. Beneficiaries must grant each other access to relevant pre-existing knowledge (background) necessary to carry out or use the project's outcomes, as outlined in Annex 5. If the background is owned by a third party, the beneficiary must ensure compliance with the agreement.
Project results remain the property of the beneficiaries. These results include any outputs, such as data or intellectual property, whether or not they are legally protected. The EU does not claim ownership of these results.
The granting authority, however, has the right to use non-sensitive materials from the beneficiaries—like reports, summaries, and media—for communication and publicity purposes. These rights are royalty-free, non-exclusive, and apply both during and after the project.
Beneficiaries are responsible for securing necessary rights if third-party or moral rights are involved. Specific rules on intellectual property, background, and results are detailed in Annex 5 of the Grant Agreement. Non-compliance with these obligations may lead to financial penalties or other measures (Article 16.5 of the Grant Agreement).
The Consortium Agreement establishes the legal foundation for cooperation among all participating beneficiaries and outlines their binding obligations. It references key elements of the Grant Agreement while adding further project-specific details. In its annexes, beneficiaries have listed the background information required for the project and, where applicable, notified others of any legal restrictions on its access. Beneficiaries may also add additional background during the project, provided they notify the others in writing and obtain approval from the General Assembly.

6.2.2.2 Post project phase

According to the Grant Agreement, beneficiaries are generally required to provide each other with access to background and results—on fair and reasonable terms—when needed to exploit their own results after the project ends. Each beneficiary must evaluate whether its results should be protected and, if they have potential for commercial or industrial use, take

appropriate steps to secure that protection. Ownership of results may be transferred or licensed, as long as this does not conflict with the Grant Agreement's requirements.
Further details on PiQASO's exploitation strategy and planned actions are outlined in Deliverable D6.2 – (PiQASO's Interim Report on Communication, Dissemination, and Exploitation activities; Public; M18, updated in M36 with Deliverable D6.3).
To complement this deliverable, an IPR repository will be created in M7 to capture the IP generated by the project and the planned protections considered by the innovators. The IPR repository is a living document, available on the project repository (SharePoint). It will be updated by the Innovation Manager and the beneficiaries in parallel to project progress.
At this stage of the project, IPR agreements are still under discussion.

6.3 Key Exploitable Results

The consortium partners are committed to open-source principles and have adopted a multi-tiered strategy for managing project-generated knowledge. Under this approach, the creator of the knowledge retains ownership but shares software implementations with other consortium members.
Some of the project's Key Exploitable Results (KERs) will be released as open-source versions—under specific conditions to prevent misuse—to support academic and research advancements. Other KERs hold significant commercial potential for consortium members.
Initial plans for exploiting the PiQASO KERs are outlined in Table 4 and will be further developed during the project's course. For KERs intended for joint commercial use, intellectual property arrangements will be agreed upon in advance.

PiQASO KER	Owner(s)	Time to market (Post project)	Targeted market	Expected Return on Investment (ROI)	TRL
PQC Ensemble Secure implementation with optimizations and accelerations	UBITECH, QUBI, TAU, UniBwM, BYTE	1y	Embedded & Commodity Systems (i.e., PCs, laptops, ECUs, PLCs, etc.), IoT, Content Delivery Networks	~50% increase in digital services and mobile technologies (e.g. messaging apps) purchase	4 → ≥7
PQ Data "Security-by-Design" Crypto Abstractions	TAU, UniBwM, UBITECH, QUBI	2y	Electronic Transactions, Blockchain, eVoting, Healthcare, Content Delivery Networks	~20% increase in telecom operations	4 → ≥7
PQC-as-a-Service Modality	QUBI, UBITECH, TAU, UniBwM	<1y	Cloud Service Providers, Automotive, Energy, Finance, Automation, Healthcare	~40% increase cloud-based storage & services usage	4 → ≥7
PQ Crypto Assessment & Conformance Toolkit	RAL, UBITECH, QUBI, UniBwM, TAU	1y	Public Safety Applications, Healthcare, Industrial & IoT, Content Delivery Networks, Quantum Software Development	> 1M Euros from enterprises & Govs to ease their migration to quantum-safe standards	4 → ≥7

Table 4 - PIQASO's KERs

6.4 Preliminary exploitation strategy

This section presents the preliminary exploitation strategy for the PiQASO project. The purpose is to outline early plans and envisioned pathways for ensuring that PiQASO project results are utilized effectively by a broad spectrum of stakeholders, including industry, academia, policymakers, and the general public. As the project progresses, these strategies will be refined and validated based on technical progress, stakeholder engagement, and evolving market conditions. Updated versions of the Exploitation Strategy will be presented in Deliverable D6.2 – (PiQASO Interim Report on Communication, Dissemination, and Exploitation activities; Public; M18, updated in M36 with Deliverable D6.3).

6.4.1 SWOT Analysis: PiQASO Key Exploitable Results (KERs)

In the context of the PiQASO exploitation strategy, a SWOT analysis is essential for identifying and evaluating the project's Key Exploitable Results (KERs) in a structured and strategic manner. It enables the consortium to assess internal capabilities and constraints while recognizing external opportunities and risks within the evolving landscape of post-quantum cybersecurity. This analysis supports evidence-based prioritization of assets, ensuring that the most commercially viable, technically mature, and impactful outcomes are targeted for further development. Ultimately, the SWOT analysis strengthens PiQASO's ability to align its exploitation efforts with market needs, stakeholder expectations, and long-term sustainability goals.

6.4.2 PQC Ensemble Secure Implementation with Optimizations and Accelerations

Strengths: One of the key strengths of the PQC Ensemble Secure Implementation lies in its high-performance, optimized cryptographic design, which is well-suited for deployment in real-world environments. Its versatility further enhances its value, as it can be effectively applied across a wide range of platforms, including embedded systems, Internet of Things (IoT) devices, and content delivery networks, making it a robust solution for various high-demand sectors.

Weaknesses: Despite its strengths, the PQC Ensemble Secure Implementation faces certain weaknesses, notably the potential complexity involved in integrating the solution across diverse hardware environments. Additionally, its performance claims must be rigorously validated across multiple sectors to ensure reliability and maintain stakeholder confidence in its effectiveness.

Opportunities: The PQC Ensemble Secure Implementation benefits from significant market opportunities, particularly due to the rising demand for secure messaging and mobile applications in the emerging post-quantum era. Additionally, there is strong potential for establishing SDK licensing agreements in security-sensitive sectors such as telecommunications and defense, further expanding its commercial reach.

Threats: The PQC Ensemble Secure Implementation also faces notable threats, including the risk of competing solutions developed by global technology vendors, which could diminish its market share. Moreover, its reliance on hardware-specific optimizations may limit portability and scalability, potentially restricting its adoption across heterogeneous system environments.

6.4.3 PQ Data "Security-by-Design" Crypto Abstractions

Strengths: PQ Data's "Security-by-Design" crypto abstractions offer a robust foundational cryptographic architecture tailored for secure system design. These abstractions demonstrate strong alignment with critical use cases such as blockchain, electronic voting (eVoting), and systems managing sensitive data.

Weaknesses: Despite its strengths, PQ Data's "Security-by-Design" crypto abstractions face certain limitations. The expected longer time to market—estimated at two years post-project—delays its commercial realization and potential industry impact. Additionally, the abstract nature of the solution may necessitate the development or integration of complementary tools to facilitate practical adoption and implementation.

Opportunities: PQ Data's solution is well-positioned to capitalize on emerging opportunities driven by the growing demand for secure design in sectors such as digital identity, eGovernment, and fintech. Its relevance is further amplified by the increasing importance of privacy-first architectures and the urgent need for quantum-resilient infrastructures, making it a timely and strategic asset in the evolving cybersecurity landscape.

Threats: The effectiveness of PQ Data's solution faces potential threats that could hinder its widespread impact. Achieving its full value depends on ecosystem-wide adoption, which can be challenging without broad industry coordination. Moreover, its conceptual nature may present adoption barriers, particularly in the absence of strong demonstration cases that clearly illustrate its practical benefits and real-world applicability.

6.4.4 PQC-as-a-Service (PQCaaS) Modality

Strengths: The PQC-as-a-Service (PQCaaS) modality boasts significant strengths, notably its rapid time to market—under one year—enabled by a cloud-native delivery model. It strategically targets high-demand verticals such as healthcare, energy, finance, and industrial automation, where secure communication is critical. Designed to be scalable and modular, PQCaaS is particularly well-suited for small and medium-sized enterprises (SMEs) and supports seamless migration from legacy systems, enhancing its appeal across a broad range of organizational contexts.

Weaknesses: Despite its advantages, the PQC-as-a-Service (PQCaaS) model presents certain weaknesses. Its dependence on cloud infrastructure may raise trust and regulatory compliance concerns, particularly in industries with strict data governance requirements. Additionally, the technical complexity involved in integrating the service with existing legacy systems could slow down onboarding processes and increase implementation challenges for some organizations.
Opportunities: PQC-as-a-Service (PQCaaS) presents strong opportunities for growth through potential commercial partnerships with cloud service providers and system integrators. Its offering aligns directly with ongoing digital transformation initiatives and increasingly stringent cybersecurity mandates, positioning it as a timely solution for organizations seeking to enhance security while modernizing their IT infrastructure.
Threats:PQC-as-a-Service (PQCaaS) faces notable threats that could impact its market success. Cloud security concerns and data sovereignty issues, particularly in highly regulated industries, may hinder adoption. Additionally, the market is at risk of becoming saturated as major tech giants enter the PQCaaS space, intensifying competition and potentially challenging smaller or emerging providers to differentiate their offerings.

6.4.5 PQ Crypto Assessment & Conformance Toolkit

Strengths: Offers key strengths by addressing the critical need for post-quantum cryptography (PQC) readiness assessments and compliance with emerging standards. It responds to strong enterprise and government demand, with a projected return on investment exceeding €1 million. Broadly applicable across various sectors, including public safety, healthcare, industrial IoT, and quantum software, the toolkit is positioned as a versatile solution for organizations seeking to evaluate and strengthen their cryptographic resilience.
Weaknesses: It may require customization to meet the specific conformance requirements of different sectors, potentially increasing implementation complexity and cost. Furthermore, its overall success is closely tied to the widespread adoption and standardization of PQC frameworks, which are still evolving and may vary across industries and regions.
Opportunities: The PQ Crypto Assessment & Conformance Toolkit presents significant opportunities, positioning PiQASO as a leader in PQC migration and compliance tooling. Additionally, it has the potential to influence or align with key post-quantum certification frameworks, such as those being developed by the EU and NIST, further enhancing its strategic value in shaping industry standards and driving adoption.
Threats: The PQ Crypto Assessment & Conformance Toolkit faces potential threats, including the risk of frequent updates if PQC standards evolve rapidly, which could strain resources and impact its long-term viability. Additionally, the emergence of competing assessment tools from large cybersecurity firms could intensify competition, potentially challenging PiQASO's position in the market.

6.4.6 Buyers, early adopters and End users

6.4.6.1 Buyers

Buyers of the PiQASO technologies, services, and frameworks are organizations or stakeholders with the budget authority to make procurement or investment decisions.
They include Chief Information Security Officers (CISOs), Chief Information Officers (CIOs), and IT procurement officers within financial institutions, healthcare providers, critical infrastructure operators (such as those in energy and transport), and large enterprises managing sensitive digital assets. Public sector entities—such as government IT procurement agencies, ministries of interior, defence, and digital affairs, as well as EU and national cybersecurity agencies like ENISA—also represent key buyer groups. Additionally, cybersecurity service providers, including managed security service providers (MSSPs), cloud service providers, and infrastructure vendors, form an essential part of the buyer landscape.

Finally, investors and corporate venture capital arms interested in commercializing PiQASO's intellectual property or funding related spin-offs are strategic buyers driving adoption and scale
Motivation to Buy:

- Regulatory compliance (e.g., NIS2, GDPR, upcoming PQC mandates)
- Business continuity and risk mitigation
- Competitive advantage in offering quantum-safe services
- Reduction in cyber insurance premiums and legal liability

6.4.6.2 Early Adopters

Early adopters of PiQASO solutions are innovation-driven stakeholders who are open to testing and implementing new technologies at an early stage, even before full market maturity. Their involvement is essential for validating the solutions, providing feedback, and refining functionalities.
This group includes pilot partners and participants engaged in PiQASO's nine use cases, as well as cybersecurity innovation teams embedded within large enterprises and public authorities. It also encompasses advanced R&D units in the financial sector (such as banks and fintechs), healthcare IT providers, and organizations managing critical infrastructure or smart city projects. National Research and Education Networks (NRENs), along with technology incubators and accelerators supporting cybersecurity innovation, are also key early adopters expected to play a pivotal role in the project's testing and development phases.
Motivation to Adopt Early:

- Desire to stay ahead of quantum threats
- Internal R&D or strategic innovation goals
- Opportunity to co-develop or co-own innovation (e.g., through joint ventures)
- Influence future standards and gain early market leadership

6.4.6.3 End Users

End users of PiQASO are the individuals and institutions who directly apply the project's technologies, tools, or services within their operational environments.
This group includes security operations teams within enterprises and government bodies, as well as IT administrators and software developers responsible for integrating PiQASO modules or post-quantum cryptography (PQC) APIs into existing systems. Small and medium-sized enterprises (SMEs) also form a key segment, particularly those leveraging PiQASO's freemium or open-source tools to enhance their cybersecurity posture. Additionally, healthcare and public sector IT personnel who manage sensitive data are expected to benefit from the project's outcomes. Academic researchers and students will use PiQASO's datasets and tools for scientific and educational purposes, while consumers and citizens, though not direct users, will gain from the increased protection and trustworthiness of digital services secured through PiQASO technologies.

Usage Examples:

- Deploying post-quantum VPNs, email encryption, or key exchange systems
- Conducting crypto-readiness audits with PiQASO tools
- Using the PQC-as-a-Service (PQCaaS) platform to secure legacy systems
- Incorporating PiQASO innovations into cybersecurity curricula or thesis research

Role	Who They Are	Motivation
Buyers	CIOs, CISOs, public sector IT heads, MSSPs, investors	Compliance, resilience, ROI, reputation
Early Adopters	Pilot users, advanced IT teams, NRENs, tech incubators	Innovation leadership, co-creation opportunities
End Users	Security teams, IT staff, SMEs, students, researchers	Operational use, skill-building, data protection

Table 5- PIQASO's Exploitation target groups

6.4.7 Apply to DEDEP.eu Framework

To maximise the exploitation of PiQASO's project results, we intend to engage with the DEDEP.eu Framework. The DEDEP.eu framework (available at https://dedep.eu/) has been established to provide structured support to DIGITAL officers, project beneficiaries, and other key stakeholders in their dissemination and exploitation (D&E) efforts. It is grounded in recognised best practices identified across a broad range of DIGITAL projects and presents a coherent structure designed to enhance both the visibility and the effective utilisation of project outcomes. One of the principal functions of **DEDEP.eu** is the development of a comprehensive and robust dissemination and exploitation (D&E) framework, intended to serve as a strategic reference for all projects funded under the DIGITAL programme. This framework is designed to support projects in effectively communicating their results to relevant stakeholders, thereby maximising the potential of project outcomes to inform policy, foster market uptake, and stimulate further innovation.

Keep in touch

PiQASO

PiQASO Linkedin

PiQASO Youtube

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

ECCC Newsletter

ECCC LinkedIn

ECCC Twitter/X

ECCC Website