



PiQASO



D6.2 - PiQASO Interim Report on Communication, Dissemination, and Exploitation activities

Grant Agreement	101190366
Project Title	DIGITAL-ECCC-2024-DEPLOY-CYBER-06
Project acronym	PiQASO
Project Start Date	01 January 2025
Number of Deliverable	D6.2
Report Title	Interim Report on Communication, Dissemination, and Exploitation activities
Related Work Package	WP6
Related Task	T6.1, T6.2, T6.3
Lead Organisation	RAL
Submission Date	30.06.2026
Last Change Date	30.06.2026
Dissemination Level	Public

Abstract

This deliverable is the Interim Report on Communication, Dissemination, and Exploitation (C/D/E) activities of the PiQASO project, covering the first 18 months of implementation (M1–M18). Building on the strategy established in Deliverable D6.1, it reports on the activities carried out under Task 6.1 (Dissemination & Communication), Task 6.2 (Standardisation & Working Group Liaison), and Task 6.3 (Exploitation, IPR Handling, and Business and Sustainability Planning). The document presents the project's performance against the Key Performance Indicators (KPIs) defined in the Description of Action (DoA), including project synergies, scientific and non-scientific dissemination, communication channels, and standardisation engagement. It also details the project's exploitation methodology and the characterisation of its Key Exploitable Results (KERs), market analysis, and intellectual property (IP) tracking to date. The final assessment of Communication, Dissemination, and Exploitation activities, including the completed exploitation plan, will be presented in Deliverable D6.3 at the end of the project (M36).

Authoring & approval

Author(s) of the document

Name (Organisation name)	Date
Maria Poulimenou (UBITECH)	29.06.26
Isaac Dangana (RAL)	29.06.26
Nicola Marcialis (PLURIBUS)	29.06.26
Silvia Scano (PLURIBUS)	24.06.26
Angelina Broukou (UNIS)	29.06.26
Georgia Oikonomopoulou (UNIS GR)	24.06.26
Stefanos Chamalelis (DPG)	24.06.26
Symeon Tsintzos (QUBI)	24.06.26
Rafail Lingas (CERTH)	24.06.26
Dimosthenis Ioannidis (CERTH)	24.06.26
Dionysios Kehagias (CERTH)	24.06.26
Gizem Bozdemir (PAL)	24.06.26
Bárbara Guerra (PARTICLE)	24.06.26
Konstantin Klein (BIBA)	24.06.26

Reviewed by

Name (Organisation name)	Date
Symeon Tsintzos (QUBI)	26.06.26
Marios Siganos (K3Y)	29.06.26

Approved for submission by-

Name (Organisation name)	Date
Savvoula Oikonomou (UBITECH)	30.06.26

Document history

Version	Date	Contributor/Organisation	Additional information
00.00	29.04.26	Isaac Dangana (RAL)	Table of Contents (First initial draft) First setup of the deliverable, identifying specific action items per partner
0.1	05.06.26	All contributors	Initial input added by all partners
0.2	24.06.26	All contributors	Final input with plenary feedback incorporated
0.3	26.06.26	Savvoula Oikonomou (UBI)	Version ready for review
0.4	29.06.26	Isaac Dangana (RAL), Savvoula Oikonomou (UBI), Maria Poulimenou (UBI), Nicola Marcialis (PLUR)	Reviewers' comments addressed
1.0	30.06.26	Savvoula Oikonomou (UBI)	Submission ready version.

Copyright statement © 2025 – PiQASO Consortium
All rights reserved. Licensed to PiQASO under conditions.

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."



Co-funded by
the European Union



ECCC 
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Table of contents

Abstract	2
1 Introduction	8
1.1 Objectives	8
1.2 Connection to project objectives.....	8
1.3 Structure of the document	9
2 Key Performance Indicators Overview.....	11
2.1 About	11
2.2 Performance	12
2.3 Deviations from original plan & mitigation.....	15
3 Task 6.1: Dissemination & communication strategy.....	16
3.1 Dissemination activities	16
3.1.1 Scientific papers, articles and whitepapers.....	16
3.1.2 Organized & attended workshops & webinars	18
3.1.3 Digital liaisons with related project.....	20
3.1.4 Non-scientific publications & events	22
3.1.5 Conclusion	25
3.2 Communication activities.....	25
3.2.1 Website	25
3.2.2 Social Media	30
3.2.3 Audio & Video Material.....	38
3.2.4 Press releases	38
3.2.5 Articles	39
3.2.6 Conclusion	40
4 Task 6.2: Standardisation & WG Liaison	41
4.1 Formal Liaisons Established.....	42
4.1.1 Others to come.....	43
4.2 Specific Technical Contributions	43
4.3 Conclusion	43
5 Task 6.3: Exploitation, IPR Handling & Business and Sustainability Planning	44
5.1 Key Exploitable Results.....	47
5.1.1 KER 1: PQC Ensemble Secure Implementation with Optimisations and Accelerations.....	47
5.1.2 KER 2: PQ Data Security-by-Design Crypto Abstractions	51
5.1.3 KER 3: PQC-as-a-Service Modality.....	54
5.1.4 KER 4: PQ Crypto Assessment and Conformance Toolkit	57
5.2 Market Analysis & Competitive Landscape.....	60
5.2.1 Macro-Environmental Drivers & Market Dynamics (PESTEL Alignment).....	61
5.2.2 Socio-Technical Dynamics: Systemic Ecosystem Interdependency	63
5.2.3 Market Segmentation & Target End-User Profiles	63
5.2.4 Technical Barriers & Market Friction Points.....	65
5.2.5 Sector-Specific Market Profiles	67

5.3	IPR Tracking Table	72
5.3.1	What is agreed within the Consortium Agreement.....	73
5.3.2	IPR rules and procedures within PiQASO	75
6	Conclusion	77
	ANNEX I.....	80
	ANNEX II.....	86
	ANNEX III.....	87

List of figures

Figure 1	PiQASO Dissemination & Communication tracker.....	11
Figure 2	CRSN logo	21
Figure 3	Website structure	27
Figure 4	Website channels of traffic.....	28
Figure 5	Website top pages.....	29
Figure 6	Visitor highlights	30
Figure 7	Visitor metrics.....	31
Figure 8	Followers highlights.....	31
Figure 9	Followers metrics	32
Figure 10	Content highlights.....	32
Figure 11	Content metrics - Impressions	33
Figure 12	Content metrics - Clicks.....	33
Figure 13	Content metrics - Engagement.....	34
Figure 14	Content metrics - Reposts	34
Figure 15	Substack analytics overviewContent performance.....	35
Figure 16	Substack content performance	37
Figure 17	IPR & KERs registers	44
Figure 18	Exploitation workshops output	46
Figure 19	Macro-Environmental Drivers & Market Dynamics.....	61
Figure 20	Willingness to pay per market tier.....	62
Figure 21	Questionnaire results – Technical barriers.....	66
Figure 22	Questionnaire results – Unique Value Proposition.....	67

Figure 23 Primary Competitive Pillars.....	70
--	----

List of tables

Table 1 PiQASO overall dissemination, communication, exploitation & standardisation KPIs	12
Table 2 Traffic Analytics	27
Table 3 Visit Details.....	27
Table 4 Active users Details	28
Table 5 Views per Active users detail	28
Table 6 Average Visit Duration Details	28
Table 7 Bounce Rate Details.....	28
Table 8 List of website articles and blogs.....	39
Table 9 Standardisation KPIs.....	41
Table 10 KER 1 SWOT Analysis.....	47
Table 11 KER 1 DEDEP Characterization table	48
Table 12 KER 1 Preliminary Business Model Canvas	50
Table 13 KER 2 SWOT Analysis.....	51
Table 14 KER 2 DEDEP Characterization table	51
Table 15 KER 2 Preliminary Business Model Canvas	53
Table 16 KER 3 SWOT Analysis.....	54
Table 17 KER 3 DEDEP Characterization table	55
Table 18 KER 3 Preliminary Business Model Canvas	56
Table 19 KER 4 SWOT Analysis.....	57
Table 20 KER 4 DEDEP Characterization table	58
Table 21 KER 4 Preliminary Business Model Canvas	59
Table 22 PiQASO Key buyer personas	65
Table 23 Competitors & PiQASO UVP	71
Table 24 KERs IPR.....	76
Table 25 Action points for RP2	77

1 Introduction

This document constitutes the second deliverable of Work Package 6, reporting on the Communication, Dissemination, and Exploitation (C/D/E) activities implemented during the first 18 months of the PiQASO project (RP1). Building on the strategy established in D6.1, this report presents the activities carried out under Tasks 6.1, 6.2, and 6.3, assesses progress against the Key Performance Indicators (KPIs) defined in the Description of Action (DoA), and identifies the exploitation results achieved to date. The deliverable is intended to provide a transparent account of the project's outreach, standardisation, and exploitation performance, and to set the basis for the activities planned for the second reporting period (M19–M36).

1.1 Objectives

The objectives of Deliverable 6.2 are the following:

- ✓ Report on the dissemination and communication activities carried out under Task 6.1 during the first reporting period, including scientific and non-scientific publications, events, and digital channels.
- ✓ Present the standardisation and working group liaison activities conducted under Task 6.2, together with the technical contributions made by the consortium.
- ✓ Document the exploitation, Intellectual Property Rights (IPR) handling, and business and sustainability planning activities carried out under Task 6.3, including the Key Exploitable Results (KERs) identified to date.
- ✓ Assess project performance against the KPIs defined in the DoA and report on any deviations from the original plan, together with the corresponding mitigation measures
- ✓ Provide the consortium with a consolidated reference point for planning Communication, Dissemination, and Exploitation activities for the remainder of the project.

1.2 Connection to project objectives

PiQASO is driven by a set of interrelated objectives that collectively aim to enable the practical, secure, and scalable adoption of Post-Quantum Cryptography (PQC) in Common Transmission Systems (CTS) and digital infrastructures. These objectives, as already defined in the DoA, span technical, operational, and ecosystem dimensions and are monitored through a structured set of KPIs. Work Package 6 directly contributes to Objective 5.

OB5: Reinforced awareness towards the need for migration to PQC

DoA KPIs: 30% increase of the organizations actively involved in the technological and commercial network, indicating the level of engagement and collaboration during the lifetime of the project; Increase by 20% of the participation and engagement in knowledge sharing activities such as workshops, webinars, and knowledge-sharing platforms; Engage at least 30 stakeholders in active collaboration and knowledge sharing; Provision of 1 migration plan per industrial sector.

During the first half of the project, activities related to OB5 have focused on establishing a robust foundation and contacts laying the groundwork for the RP2, as the most intensive work for this objective is scheduled for the second reporting period (M19–M36).

PiQASO has continued to build its stakeholder engagement strategy in support of the project's collaborative technological and commercial network. Beyond the initial mapping of relevant organisations and projects, the consortium has translated several of these contacts into concrete activities: PiQASO presented alongside **CyberSuite**, **ORQUESTRA**, and **SEQURED** at the INCYBER Forum 2026, held in Lille, France, from 30 March to 2 April 2026, and QUBITECH has formally joined the **Q-PrEP community of experts**, supporting collaboration on Quantum-Proofing European Public Administrations, including PiQASO's participation in the Q-PrEP 2026 workshop in Athens. PiQASO has also become a member of the **Cyber-Resilience Synergy Network (CRSN)**, a cluster of 14 Digital Europe Programme-funded projects, including **VIGILANCE**, **VANTAGE**, **CIPHER**, **5G-TACTIC**, and **CyberAid**, among others, working together to advance cybersecurity across Europe's critical sectors. The projects identified for further exploration, namely cPAID and PQCSA, remain under consideration for future joint activities, as initial contacts have been established but no further activities have taken place. Detailed figures on stakeholder engagement and project synergies are reported in Section 3.1.3.

1.3 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 activities.

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) activities.

- **Chapter 2:** presents the KPIs used to monitor the project's Communication, Dissemination, and Exploitation activities. It describes the KPI monitoring framework, reports on performance against the targets defined in the DoA for the first reporting period and discusses any deviations from the original plan together with the mitigation measures adopted.
- **Chapter 3:** reports on the activities carried out under Task 6.1, covering both dissemination and communication. It details the scientific and non-scientific publications, events, workshops, and digital liaisons with related projects, as well as the channels used to reach PiQASO's audiences, including the website, social media, and audio-visual material.
- **Chapter 4:** addresses the standardisation and working group liaison activities carried out under Task 6.2. It presents the formal liaisons established with standardisation bodies and working groups, together with the specific technical contributions made by the consortium during the reporting period.
- **Chapter 5:** covers the exploitation, IPR handling, and business and sustainability planning activities carried out under Task 6.3. It introduces the project's KERs, presents the market analysis and competitive landscape, and reports on the management of IPR within the consortium.

- **Chapter 6:** concludes the deliverable with a summary of the progress achieved across all WP6 tasks during the reporting period and an outlook on the activities planned for the remainder of the project.

2.1 About

To support effective monitoring and reporting of KPIs related to dissemination and communication activities, we developed a dedicated tool: the Dissemination & Communication Tracker ([PiQASO - Dissemination & Communication Tracker.xlsx](#))

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.

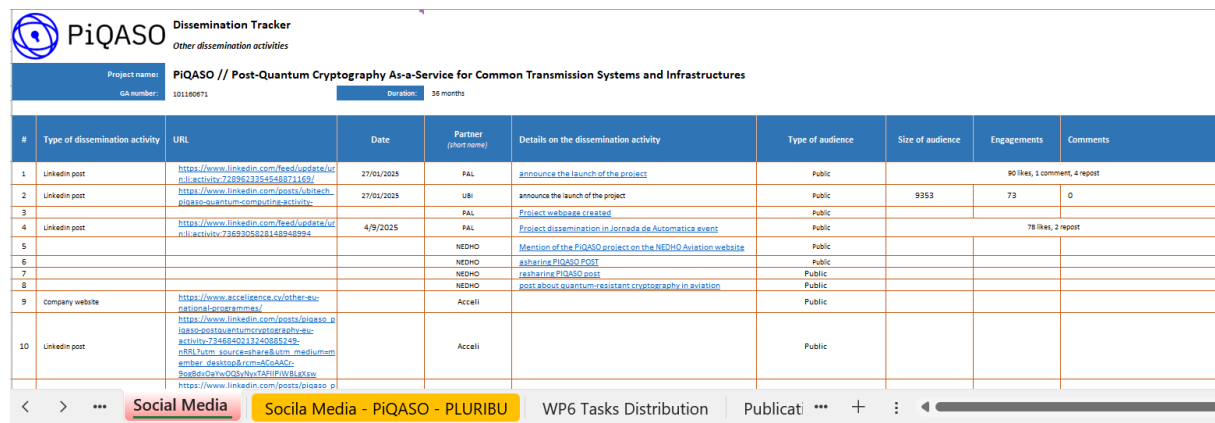


Figure 1 PiQASO Dissemination & Communication tracker

To ensure the effectiveness of these efforts, progress is monitored through a detailed set of dissemination KPIs, structured across three strategic phases: Awareness Creation, Continuity of Information Flow, and Result Orientation. During the first twelve months of the project, efforts were concentrated on Phase 1, with the primary goal of establishing a robust digital presence, defining the project's visual identity, and initiating broad-spectrum awareness through social media and public announcements.

2.2 Performance

During M1 – M18, PiQASO focused primarily on awareness creation and on establishing the project's public communication infrastructure. The Communication, Dissemination and General Awareness Plan was delivered on time, the visual identity was completed, and the official website and social media presence were launched, providing a stable foundation for long-term outreach. In terms of performance, the project showed good early traction through press releases, blog posts, the publication of the promo video, and the activation of LinkedIn and other outreach channels. The first half of the project also saw the first scientific publications and the initiation of links with related initiatives, supporting the project's visibility within both the research and policy ecosystems.

The following table details the specific KPIs associated with each phase, their target timelines, and a comprehensive summary of the status achieved during the first period of implementation.

Table 1 PiQASO overall dissemination, communication, exploitation & standardisation KPIs

KPI	Timeline	Status M18	Comments
Phase 1: Awareness Creation			
Announcement letter - Reach 3000 people via press releases in public & social media, on project website and on partners' websites	M1	Completed – https://www.piqasoproject.eu/press-release	KPI achieved.
Project website and branding: > 1000 unique visitors > 200 registrants > 350 blog interactions	M2 + throughout the project implementation	M1 – M18 results Visitors: 290 Registrants (Substack): 54 Blog interactions: 1300 views on Substack	No critical deviation at M18. During RP2 we will continue publishing on our website and social media, according to the editorial plan of the project.
Audio and Video Material: 1 Promo + 1/Pilot + 1 Impact + 2 to 4 interviews or podcast episodes	Throughout the project implementation	Promo video published on YouTube https://www.youtube.com/watch?v=hoh42NRomY8 1st interview published – George Pastras (Qubitech) – https://academy.piqasoproject.eu/course/view.php?id=18	No critical deviation at M18. Planned RP2: More interviews with experts (Ubitech, UniBwM, NCIS, Byte and more); the impact video; demo videos of the UCs.

		2nd interview published – Yassine El Hadi (RAL) – https://academy.piqasoproject.eu/enrol/index.php?id=19 1 interview under development with TAU	
Social media (FB, LinkedIn): > 500 followers > 400 posts/reposts > 5000 interactions	Throughout the project implementation	M1 – M18 results Followers (LinkedIn & Facebook): 318 Posts/reposts: 106 Interactions: 45.267 impressions, 3155 clicks, 1581 reactions	No critical deviation at M18. During RP2 we will continue posting on our social media to drive communication. Our aim is to improve the reposting rate of our posts and continue increasing the interactions.
Phase 2: Continuity of Information Flow			
Press releases (4 per year), blog posts (1000 people reached)	Throughout the project implementation	4 Press Releases published 18 blog posts published Available on our website https://www.piqasoproject.eu/blog People reached: 1130 blog views (Substack)	Outreach KPI achieved. RP2 will continue the efforts of RP1.
Scientific papers, articles, whitepapers: 4 Journal articles, 10 Conference papers	Throughout the project implementation	4 conference papers 2 journal articles	No critical deviation at M18. Planned for RP2: 6 conference papers; 2 journal articles.
Interaction with policy makers: > 6 synergies established with policy makers reached via e-mail or physically	Throughout the project implementation	2/6 ANSSI – Reached May 2026 Cyber Reunion – Reached April 2026	No critical deviation at M18. Planned for RP2:

Digital liaisons with related projects: Workshops organized (3) + attended (>5), > 500 visitors, 10 speakers;	Throughout the project implementation	Organized: 1/3 Attended: 3/5 Speakers: 4/10	No critical deviation at M18. During RP2 we will continue the work carried out so far. We are aiming to organise a workshop on November 2026 on Standardisation. We have contacted ANSSI to initiate this.
Digital liaisons with related projects: 5 posts in CORDIS/other EC systems;	Throughout the project implementation	This will be achieved after the finalization of the 1st review and the approval of the project public deliverables to be uploaded on EC systems.	This KPI is relevant only for RP2.
Digital liaisons with related projects: 10 project synergies	Throughout the project implementation	17/10	KPI achieved.
Non-scientific Publications: > 6 Industrial PQC Cyber Security Conferences, 1 exhibition, 1 demonstration days	Throughout the project implementation	Industrial conferences: 4/6 Expos: 2/1	No critical deviation at M18. During RP2 we will continue participating in relevant events. Demonstration days are expected near the project end in line with the technical work.
Standardization associations: (EU & International) PQC > 4, Standards Orgs > 3	Throughout the project implementation	Official membership secured in ETSI ISG QSC and the NIST PQC Migration Community of Interest (COI). Participation at TCG workshop 2026 https://trustedcomputinggroup.org/press-rooms/events/tcg-workshop-tokyo/	No critical deviation at M18. We expect our core technical contributions to happen during RP2.
Phase 3: Result orientation			

Pilot Demonstrations/ Workshops: > 1 demonstration per pilot > 20 attendees each	Througho ut the project implem entation	Towards project end	This KPI is relevant only for RP2.
PiQASO Day: > 80-100 participants	Towards project end	Towards project end	This KPI is relevant only for RP2.

The KPI results in the table above provide a comprehensive view of WP6 performance during the first reporting period (M1–M18). In terms of awareness creation, the project has established its public communication infrastructure, with the website, social media channels (LinkedIn and Facebook), and the PiQASO Academy now fully operational, supported by a promotional video and two published expert interviews.

Website traffic reached 390 visitors during M1-M18, while social media activity generated 45.267 impressions, 3155 clicks, 1581 reactions on LinkedIn, which confirms that the communication channels are functioning effectively and reaching the intended audiences. The project also recorded 318 LinkedIn followers and 106 posts/reposts, showing a solid base for continued growth in the second reporting period. In parallel, dissemination and awareness activities were strengthened through the PiQASO Academy and preparatory content for future workshops, webinars, and stakeholder engagement actions.

In terms of continuity of information flow, the project published 4 press releases, 18 blog posts, 4 conference papers, and 2 journal articles, and recorded 17 project synergies, exceeding the original target of 10. Engagement with policy makers and participation in digital liaison workshops have progressed more gradually, with 2 of 6 targeted policy-maker synergies and partial achievement of the workshop-related sub-targets reported to date. Standardisation engagement has also advanced through official membership in ETSI ISG QSC and the NIST PQC Migration Community of Interest, together with participation at the TCG Regional Workshop in Japan (February 2026).

2.3 Deviations from original plan & mitigation

No major deviations from the original WP6 plan were reported for the first year, and the work package was assessed as on track. The main difference between the original expectations and the actual RP1 status is rather the expected timing of impact-oriented outputs: activities related to standardization liaison, deeper policy engagement, workshops, and broader exploitation are scheduled more heavily for the second reporting period, when the technical results and demonstrators will be more mature. This means that some KPI values remain below their final targets, but this is consistent with the project lifecycle and not considered a delay. Risk management for WP6 was handled through regular monitoring and monthly work package coordination meetings, with no WP6-specific risks materializing during the reporting period. To mitigate the limited maturity of some dissemination and exploitation outputs in RP1, the consortium adopted a phased communication approach, prioritising foundational assets first, including branding, website setup, editorial planning, and the initial publication pipeline. In addition, early liaison activities with related projects and standardization bodies were initiated to reduce future integration risks and to ensure that WP6 can scale its impact once technical results become available.

3 Task 6.1: Dissemination & communication strategy

The following chapter covers the work performed under Task 6.1 regarding the Dissemination & Communication activities of the project. 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.

At the same time, 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 main tools that have been used to communicate the project are website, social media and newsletters.

3.1 Dissemination activities

3.1.1 Scientific papers, articles and whitepapers

Seamless Post-Quantum Transition: Agile and Efficient Encryption for Data-at-Rest

Abstract: As quantum computing advances, its threat to traditional cryptographic protocols, especially for long-term encrypted data, becomes critical. This paper presents an agile cryptosystem designed to ease the transition from pre-quantum to post-quantum security by supporting efficient integration of post-quantum Key Encapsulation Mechanisms (KEMs). Our approach combines a CCA-secure KEM with robust Authenticated Encryption (AE), allowing only the encapsulated key to be updated during migration, without re-encrypting large data payloads—saving both computation and bandwidth. We formalize cryptographic agility via an agile-CCA security model, ensuring that neither the original nor updated ciphertexts leak information. A game-based proof shows that the construction remains agile-CCA secure if the underlying KEM and AE are individually CCA-secure in the random oracle model. The result is a future-proof scheme that enables enterprises and cloud providers to safeguard vast data volumes against emerging quantum threats with minimal disruption.

Status: Published – **Link to full article:** https://www.researchgate.net/profile/Thomas-Loruenser/publication/393266648_Seamless_Post-Quantum_Transition_Agile_and_Efficient_Encryption_for_Data-at-Rest/links/68a482891bee4d42a240dab8/Seamless-Post-Quantum-Transition-Agile-and-Efficient-Encryption-for-Data-at-Rest.pdf

Relaxing the Single Point of Failure in Quantum Key Distribution Networks: An Overview of Multi-path Approaches

Abstract: Quantum Key Distribution (QKD) networks are receiving growing attention by researchers and funding agencies, with the largest projects spanning hundreds of kilometers and large, multi-national initiatives well under way. The growing scale of QKD networks poses some extra challenges, due to the current impossibility of establishing end-to-end security between nodes: for large distances, reliance on intermediate trusted nodes is required, an aspect which increases the attack surface of QKD networks. A possible mitigation strategy for this problem lies in leveraging the complexity of the network: by making use of multiple paths and applying techniques issued from cryptography and/or error-correcting theory, it is possible to mitigate some attacks and force an adversary to compromise more nodes in the network.

This paper discusses relevant approaches to leverage multi-path aspects of QKD networks for increased security, analyzing the different security assumptions, guarantees, and performance of different techniques, and presenting their applicability to the different networks.

Status: Published – **Link to full article:** https://link.springer.com/chapter/10.1007/978-3-032-00642-4_11

FABS: Fast Attribute-Based Signatures

Abstract: Attribute-based signatures (ABS) provide fine-grained control over who can generate digital signatures and have many real-world applications. This paper presents a pair of fast ABS schemes: one for Key-Policy ABS (KP-ABS) and another for Signature-Policy ABS (SP-ABS). Both schemes support expressive policies using Monotone Span Programs (MSP), and offer practical features such as large universe, arbitrary attributes, and adaptive security. Most notably, we provide the first implementation of MSP-based ABS schemes and demonstrate that our schemes achieve the best-known asymptotic and concrete performance in this domain. Asymptotically, key generation, signing and verification time scale linearly with the number of attributes; verification requires only two pairing operations. In concrete terms, for 100 attributes, our KP-ABS scheme performs key generation, signing, and verification in 0.16s, 0.10s, and 0.13s, respectively; our SP-ABS scheme achieves times of 0.082s, 0.26s, and 0.21s for the same operations.

Status: Published – **Link to full article:** <https://eprint.iacr.org/2026/022>

SoK: Updatable Public-Key Encryption

Abstract: Updatable (public-key) encryption is a broad concept covering (public-key) encryption schemes whose keys can evolve over time to support secure key rotation and limit the impact of key compromise. The essential feature is that the encryption keys (and possibly also ciphertexts) can be updated from one epoch to the next via so called update tokens. This concept is useful in various applications, among them secure outsourced storage, secure messaging or low-latency forward-secret key-exchange protocols. The term, however, is used with varying meanings across the literature. Some works define key-updatable schemes, where only the public and secret keys evolve. Others extend this idea by also allowing ciphertexts to be updated during key evolution. Variants further differ in how evolution is triggered: in some schemes, the receiver performs key updates locally, while in others, the sender initiates the evolution by embedding update information in ciphertexts. Beyond achieving forward secrecy, many formulations also aim for post-compromise security, ensuring that once a compromised key is updated, future ciphertexts regain confidentiality under the new key. In this paper, we systematize this field with a focus on updatable public-key encryption schemes. Our aim is to first provide a taxonomy that sheds light into the currently fragmented terminology. It then compares their formal definition, syntaxes and formal security models found in the literature, clarifies their interrelations, and identifies common design patterns underlying current schemes. Beyond mapping the definitional landscape we provide a comparative analysis of existing instantiations, focusing on their properties and efficiency, and highlighting their main trade-offs. The paper concludes with open challenges outlining directions for advancing the field.

Status: Published – **Link to full article:** <https://eprint.iacr.org/2026/583.pdf>

HHE Kombat: Benchmarking Hybrid Homomorphic Encryption Schemes

Abstract: Not available yet.

Status: Accepted at 31st European Symposium on Research in Computer Security (ESORICS) 2026, September 14-18, 2026. – **Link to full article:** <https://sites.google.com/di.uniroma1.it/esorics2026/program/accepted-papers?authuser=0>

Efficient SIMD Implementation of the BLS Signature Scheme Using Intel AVX-512

Abstract: The BLS digital signature scheme, in particular its instantiation with the BLS12-381 curve, has become a cornerstone of modern blockchain protocols such as Ethereum Proof-of-Stake, due to its unique and attractive characteristics (e.g., support for non-interactive signature aggregation). Recently, Cheng et al. (CHES 2025) demonstrated that the enormous Single-Instruction-Multiple-Data (SIMD) computing power of the Intel AVX-512 extensions, when combined with carefully designed vectorization strategies, can be effectively leveraged to speed up the computation of the optimal ate pairing on BLS12-381, a major component of BLS. This naturally raises the question of whether such SIMD-parallel processing can be exploited more extensively to benefit the entire BLS signature scheme. The present paper answers this question positively by presenting a highly SIMD-optimized BLS implementation using Intel AVX-512, especially the AVX-512FMA instructions. In order to harness AVX-512 more efficiently for the performance-critical operations of BLS, we explored a wide range of optimization options, including various formulas and vectorization granularities for elliptic curve arithmetic operations, scalar multiplication, and hash-to-curve, as well as the fine-tuning and flexible use of different implementations of the finite-field arithmetic. Benchmarking results collected on an Intel Core i3-1005G1 ("Ice Lake") CPU show that our vectorized BLS software using AVX-512 is at least 1.57 times faster than an x64 assembly implementation of the widely-used blst library.

Status: Accepted not yet published – **Link to full article:** <https://ches.iacr.org/2026/>

3.1.2 Organized & attended workshops & webinars

3.1.2.1 Workshops

PrivCrypt 2026 - International Workshop on Foundations and Applications of Privacy-Enhancing Cryptography

PiQASO through UniBwM supported the organization of PrivCrypt 2026 on May 10th, 2026. The importance of the domain of privacy-enhancing cryptography can be witnessed by the numerous academic publications in the IACR community (CRYPTO, EUROCRYPT, ASIACRYPT, etc.), the Real-World Crypto community (presence in RWC Symposia) as well as the numerous recent deployments in industry. However, all existing publication and discussion venues are much broader and there does not exist a dedicated workshop on this subfield so far. The aim of this workshop is to bridge this gap with a clear focus on these topics and can bring together interested people from academia and industry.

Link for more information: <https://privcryptworkshop.github.io/index.html>

Related Target Groups: TG-F, TG-C, **Related Expected Outcome:** EO2.1

Q-PrEP 2026: Quantum Readiness in Practice

PiQASO participated in Q-PrEP 2026: Quantum Readiness in Practice held in Athens, on 05.02.2026. **Q-PrEP**, the project on Quantum-Proofing European Public Administrations is specifically suited and funded (by the European Commission) to support and promote this

transformation, paving the way to PQC in the public sector. The workshop organized brought together experts and project representatives from multiple projects.

Link for more information: <https://qprep.eu/the-athens-workshop-2026/>

Related Target Groups: TG-E, TG-F, **Related Expected Outcome:** EO3

INCYBER Forum 2026: ANSSI roadmap for the transition to post-quantum cryptography (PQC) in France

PiQASO participated in a short workshop organized by the French Cybersecurity Agency (ANSSI) in the context of INCYBER Forum, on April 2nd, 2026 in Lille France.

Link for more information: <https://cyber.gouv.fr/actualites/anssi-forum-incyber-2026/>

Related Target Groups: TG-E, TG-D, **Related Expected Outcome:** EO3.1

PQCrypto 2025

The **PQCrypto 2025** hosted the 16th International Conference on Post-Quantum Cryptography, which took place from April 8 to 10, 2025, at Academia Sinica in Taipei, Taiwan. This highly specialized academic and industrial forum brings together global researchers, cryptographers, and engineers to share advancements in security systems capable of resisting attacks from future, large-scale quantum computers. PiQASO participated in this event.

Link for more information: <https://pqcrypto2025.iis.sinica.edu.tw/>

Related Target Groups: TG-F, TG-C, **Related Expected Outcome:** EO1.1

3.1.2.2 Webinars

Post Quantum Cryptography Preparing for deployment, Webinar speaker, UniBwM

Webinar on the preparedness for deployment of post quantum cryptography (PQC) by examining the work which started in the mid-90s after it was demonstrated that quantum computers could break public key cryptography. 30 years later, a lot of theoretical work was done, numerous research initiatives conducted, new standards are in the process of being finalised, government regulations include PQC transition and industry is preparing for new frontiers in integration and deployment. The panellists discussed the current state of PQC, its aspects that need to be urgently addressed, integration and deployment challenges, economics and a lot more.

Link for more information: <https://trustindigitallife.eu/event/post-quantum-cryptography/>

Related Target Groups: TG-A, TG-B, **Related Expected Outcome:** EO1.2, EO1.3

Post Quantum Cryptography & Related Areas Challenges and the immediate future, Webinar speaker, UniBwM

Discussion on post quantum cryptography (PQC) focusing on the current state of the art and expectations for the next three to five years. The panellists addressed PQC applications, the state of standardisation, quantum key distribution (QKD), the most important research areas, practical approaches, challenges of hybrid environments and PQC transition and related topics.

Link for more information: <https://trustindigitallife.eu/event/pqc-and-related-areas/>

Related Target Groups: TG-A, TG-C, **Related Expected Outcome:** EO2.2

3.1.2.3 Keynotes & panel discussions

Australian Summer School on Privacy 2025

Prof. Daniel Slamanig was an invited speaker at the Australian Summer School on Privacy 2025, held at the University of New South Wales (UNSW) in Sydney and organized by Prof. Sushmita Ruj and Prof. Salil Kanhere. The summer school brought together students, researchers, and practitioners from academia and industry to explore current developments in privacy-enhancing technologies, including topics such as cryptography for privacy, differential privacy, usable privacy, and AI privacy.

Prof. Slamanig delivered two lectures titled “**Cryptography for Privacy**” and “**Anonymous Credentials: Past, Present and Future**”, and participated in a panel discussion on “**Bringing Privacy Research to Reality**”. His talks provided both a conceptual introduction and insights into ongoing research on cryptographic foundations for privacy-preserving systems.

Link for more information: <https://www.unibw.de/crypto-en/qusac-news/invited-speaker-at-the-australian-summer-school-on-privacy-2025>

Related Target Groups: TG-F, TG-C, **Related Expected Outcome:** EO2.2

3.1.3 Digital liaisons with related project

Q-PrEP: Quantum-Proofing European Public Administrations

QUBITECH, has become part of the [Q-PREP community](#) of experts, that aims to facilitate collaboration and joint activities among experts on the field of Post-Quantum Cryptography.

Link for more information: <https://qprep.eu>

CyberSuite: Uptake of Innovative Security-as-a-Service Solutions

Joint participation and technical presentation at the INCYBER Forum 2026, held on March 30th to April 2nd, 2026, in Lille, France.

Link for more information: <https://cybersuiteproject.eu/>

ORQUESTRA: Orchestrating the operational deployment of quantum resistant services for next-generation secure defence systems and communications (EDF)

Joint participation and technical presentation at the INCYBER Forum 2026, held on March 30th to April 2nd, 2026, in Lille, France.

Link for more information: [https://defence-industry-space.ec.europa.eu/document/download/5a308169-efa7-498f-a090-78fbb26e3adc_en?filename=FACTSHEET EDF 2024 LS RA DIS QUANT STEP 10122 4573 ORQUESTRA.pdf](https://defence-industry-space.ec.europa.eu/document/download/5a308169-efa7-498f-a090-78fbb26e3adc_en?filename=FACTSHEET_EDF_2024_LS_RA_DIS_QUANT_STEP_10122_4573_ORQUESTRA.pdf)

SEQURED: Strengthening defence networks for the quantum era (EDF)

Joint participation and technical presentation at the INCYBER Forum 2026, held on March 30th to April 2nd, 2026, in Lille, France.

Link for more information: https://defence-industry-space.ec.europa.eu/document/download/f7d2b036-4d0e-4eda-838a-109383f667d8_en?filename=EDF-2023-LS-RA-SMERO-NT%20SEQUURED.pdf

3.1.3.1 Cyber-Resilience Synergy Network

PiQASO is a proud member of the Cyber-Resilience Synergy Network (CRSN), a cluster of 14 EU-funded projects working together to advance cybersecurity across Europe's critical sectors.



Figure 2 CRSN logo

The CRSN unites complementary EU-funded initiatives under a shared mission: to strengthen Europe's cyber resilience and protect its critical infrastructures by delivering next-generation cybersecurity solutions. The network fosters trusted collaboration, promotes cross-

border information sharing, and works toward a secure and resilient digital Europe. Together, the CRSN member projects address the full spectrum of modern cybersecurity challenges from AI-driven autonomous defence and secure 5G networks to PQC and supply chain protection.

Link for more information: <https://www.piqasoproject.eu/cyber-resilience-synergy-network>

The members of the network are the following:

- **VIGILANCE** (Versatile Intelligent aGents for Interconnected Ledgers and Autonomous Next-generation Cybersecurity Ecosystems) is a European project funded under the Digital Europe Programme, specifically under the DIGITAL-ECCC-2024-DEPLOY-CYBER-07 call. **Link for more information:** <https://vigilance-project.eu/>
- **VANTAGE** (Vulnerability Assessment aNd Testing Automation for Global Enhancement) is a European project funded under the Digital Europe Programme, specifically through the DIGITAL-ECCC-2024-DEPLOY-CYBER-07 call. **Link for more information:** <https://vantageproject.eu/>
- **ACSOC** is a Digital Europe-funded initiative designed to strengthen cooperation between Security Operations Centres (SOCs), Computer Emergency Response Teams (CERTs), and Computer Security Incident Response Teams (CSIRTs). **Link for more information:** <https://acsoc-project.eu/>
- **CIPHER** (Cybersecurity Intelligence, Protection, and Holistic Enterprise Resilience) project contemplates creating an experimentation laboratory for essential service providers to evaluate their cybersecurity risk governance to bolster the preparedness against cyber-incidents and threats. **Link for more information:** <https://cipher-eu.com/>
- **5G-TACTIC** (5G Trusted And seCure network servICes) is a European project funded by the Digital Europe Programme, specifically under the DIGITAL-ECCC-2022-CYBER-03-SEC-5G-INFRASTRUCTURE call. **Link for more information:** <https://www.5g-tactic.eu/>
- **ACT4FOOD** (Advanced Cybersecurity Tools for Critical Food Supply Chains) is a European project funded under the Digital Europe Programme, specifically under the

DIGITAL-ECCC-2024-DEPLOY-CYBER-07 call: Deployment actions in the area of cybersecurity. **Link for more information:** <https://www.act4food.eu/>

- **CyberAid** will significantly enhance the cyber-resilience of European Critical Infrastructures (CIs) in the finance and other industrial sectors based on the development and deployment of a novel agentic AI infrastructure that will be used to autonomously and intelligently coordinate and orchestrate a pool of state-of-the-art cybersecurity tools and services for key digital technologies. **Link for more information:** <https://cyberaidproject.eu/>
- **ENFORCE** project addresses the growing trust, security, and orchestration challenges arising from the rapid evolution of IoT technologies combined with 5G connectivity and edge computing. **Link for more information:** <https://enforceproject.eu/>
- **SONIC** is a European cybersecurity project focused on enhancing the protection and resilience of digital infrastructures. The project brings together innovative technologies and services to support earlier threat detection, faster incident response, and more robust cyber resilience in increasingly complex and heterogeneous environments. **Link for more information:** <https://sonic-project.eu/>
- **CTIS4NIS** (CyberThreat Information Sharing enabling Network and Information systems Security in the EU) is a European project funded by the Digital Europe Programme, specifically under the DIGITAL-ECCC-2024-DEPLOY-CYBER-07 call. **Link for more information:** <https://ctis4nis.eu/>
- **AIAGENT4CYBER** is an EU-funded initiative developing a coordinated multi-agent AI framework for advanced, real-time cybersecurity defense. Its mission is to enhance Europe's cybersecurity resilience through trustworthy, AI-driven technologies that anticipate threats, accelerate response, and safeguard critical digital infrastructure. **Link for more information:** <https://www.aiagent4cyber.eu/>
- **CyberNEMO** aims to infuse end-to-end cybersecurity and trust on the IoT-Edge-Cloud-Data Computing Continuum. CyberNEMO delivers innovations that support resilience, risk preparedness, awareness, detection and mitigation within Critical Infrastructures deployments and across supply chains on top of NEMO (Next Generation Meta OS – HE 101070118), which manages the IoT-Edge-Cloud continuum, through an open-source, flexible, adaptable, and multi-technology meta-Operating System. **Link for more information:** <https://cybernemo.eu/>

3.1.4 Non-scientific publications & events

3.1.4.1 Industrial PQC Cyber Security Conferences

5th ENISA-ERA Conference on Cybersecurity in Railways, Streamowl

The European Union Agency for Cybersecurity (ENISA) and the European Union Agency for Railways (ERA), with the support of Estonian Railways, organized the 5th edition of the Cybersecurity in Railways conference, the annual event dedicated to exploring the latest advancements, best practices, and challenges in the field of cybersecurity in the railway sector.

Link for more information: <https://www.enisa.europa.eu/events/5th-enisa-era-conference-on-cybersecurity-in-railways>

Related Target Groups: TG-B, TG-E, **Related Expected Outcome:** EO1.3

XLVI Jornadas Automática, Pal Robotics

The Spanish Committee of Automation (CEA), a non-profit association and national representative of the International Federation of Automatic Control (IFAC), organizes the Jornadas de Automática (Automation Conference), a benchmark event held annually since 1977. This conference serves as a key meeting point for professionals whose work revolves around Automation, spanning fields such as research, teaching, and industry. The event offers a dynamic space for presenting results, debating ideas, and showcasing projects within this engineering discipline.

Link for more information: <https://eventos.upct.es/127169>

Related Target Groups: TG-B, TG-C, TG-F **Related Expected Outcome:** EO1.2, EO1.3

3.1.4.2 Exhibitions

2nd Automation and Robotics Expo, Acceligence

The 2nd Automation & Robotics Exhibition “A+R Expo 2026”, took place from April 25 to 27 at the Metropolitan Expo, Athens, Greece. More than 8,500 specialized professionals and 140+ companies from Greece and abroad shaped a panorama of innovation, presenting next-generation solutions and cutting-edge technologies in industrial automation, robotics, and artificial intelligence.

Link for more information: <https://ar-expo.gr/>

Related Target Groups: TG-A, TG-B, **Related Expected Outcome:** EO1.3

European Robotics Forum, Pal Robotics

The European Robotics Forum (ERF) is the leading event for the European robotics and AI community, bringing together over 1,000 participants from industry, academia, and the public sector. Held annually in a different European city, ERF is the go-to platform to explore cutting-edge technologies, foster collaboration, and address the latest challenges and trends shaping the future of robotics in Europe.

Link for more information: <https://erf2026.eu/>

Related Target Groups: TG-B, TG-C, **Related Expected Outcome:** EO1.2

INCYBER Forum, Ubitech, Qubitech Pluribus, Red Alert Labs

Founded in 2007, the INCYBER Forum is Europe’s leading event for digital security and trust and has also become a key event in Canada since 2022 and in Japan since 2025. Its unique feature is that it brings together the entire cybersecurity and “trusted digital” ecosystem: end-customers, service providers, solution vendors, consultants, law enforcement and government agencies, schools and universities. Its mission is to respond to a twofold urgency: Meet the operational challenges of cybersecurity and contribute to building a digital future in line with European interests and values.

Link for more information: <https://europe.forum-incyber.com/en/home-en/>

Related Target Groups: TG-A, TG-B, TG-C, TG-D, TG-E, TG-F **Related Expected Outcome:** EO2.2, EO3.2

Education Expo Japan, Nedho Aviation

EDIX is Japan's largest industry trade show gathering many kinds of education-related products and service providers. It serves as a best platform for professionals who aim to expand their business in Japanese educational field. Nedho Aviation presented the PiQASO Academy to interested participants.

Link for more information: <https://www.edix-expo.jp/hub/en-gb.html>

Related Target Groups: TG-F, TG-A, **Related Expected Outcome:** EO2.2

3.1.4.3 Other non-scientific events & publications

The small & the random, Qubitech

Full day event dedicated to promoting general awareness on quantum technologies and their applications across different domains. Invited talk by Qubitech on the Quantum Future. **Link for more information:** <https://www.quantumday.gr/>

Related Target Groups: TG-A **Related Expected Outcome:** EO2.2

Cyber Journey - Owasp Italy Day 2026, Nedho Aviation

Presentation of the PiQASO project at the EU Funded Projects corner by Nedho Aviation. **Link for more information:** <https://www.cyberjourney.it>

Related Target Groups: TG-C **Related Expected Outcome:** EO1.2

21st Conference of Greek Physics Association, Qubitech

Invited talk at the 21st Conference of Greek Physics Association. This year's theme was "Physics in the age of AI: Research Developments and Prospects for 21st-Century Physics". Qubitech gave a talk on The Emerging Quantum Era and Real-World Applications. **Link for more information:** <https://www.eef21.gr/home>

Related Target Groups: TG-F **Related Expected Outcome:** EO2.1

DEP CYBER (UPTAKE) program online projects gathering, Ubitech

Presentation of the PiQASO project during the online gathering of relevant EU funded projects, focusing on the impact of the project on SMEs and standards.

Related Target Groups: TG-F, TG-B, TG-D **Related Expected Outcome:** EO3.1, EO3.2

Project Presentation in Harokopio University of Athens, Motor Oil & Motor Oil Renewable Energy

Presentation of Piqaso Project in HUA university of Athens

Related Target Groups: TG-F, TG-B, **Related Expected Outcome:** EO1.3

Presentation at Sophia University, Nedho Aviation

Sharing about PiQASO project outputs with a special focus on the PiQASO Academy.

Related Target Groups: TG-F **Related Expected Outcome:** EO1.3, EO2.2

3.1.5 Conclusion

During the first reporting period, dissemination activities under Task 6.1 established a visible presence for PiQASO across scientific, technical, and non-scientific channels. On the scientific side, the consortium published several peer-reviewed papers and preprints addressing post-quantum migration, QKD network security, attribute-based signatures, and updatable encryption, complementing this with participation in dedicated workshops (PrivCrypt 2026, Q-PrEP 2026, PQCrypto 2025) and webinars on PQC deployment, as well as an invited keynote and panel contribution at the Australian Summer School on Privacy 2025.

Digital liaison activities expanded the project's network through direct engagement with SEQURED, ORQUESTRA, CyberSuite, and the Q-PrEP community, and through PiQASO's membership in the Cyber-Resilience Synergy Network, a cluster of 14 EU-funded cybersecurity projects. Non-scientific dissemination reached industrial, educational, and general-public audiences through conferences, expos, and presentations spanning the railway, robotics, education, and quantum-awareness sectors, both within Europe and internationally.

Taken together, these activities have positioned PiQASO within the broader post-quantum cryptography community and created a foundation for more result-oriented dissemination as the project's technical outputs mature.

The next reporting period should build on this foundation by increasing the volume and depth of scientific publications, translating dissemination outputs more directly into exploitation-relevant messaging, and continuing to strengthen the project's standing within existing and emerging synergy networks.

3.2 Communication activities

3.2.1 Website

The project website can be accessed at www.piqasoproject.eu.

3.2.1.1 Website navigation

Homepage

It introduces the PIQASO initiative and its core technical approach to securing digital infrastructures against quantum computing threats. The content is structured into two clear areas:

- The Technology Offer: Highlights the development of a Software Development Kit (SDK) and a "PQC-as-a-Service" model. It displays technical features like crypto agility, hardware/software acceleration, and automated conformance checking across edge and cloud layers.
- Project Statistics (Counters): Displays interactive, real-time counters showcasing the project's scale, specifically highlighting the involvement of 14 use cases deployed across critical sectors (healthcare, energy, finance, and transport), alongside the network of partners and tech providers.

Project

Introduces the PIQASO initiative, its timeline (January 2025 – December 2027), and its focus on implementing a "Post-Quantum Cryptography As-a-Service" framework to secure digital communication against quantum threats. The page content is organized into three main sections:

- **Key Benefits:** Details the technical advantages of the solution, highlighting post-quantum security without additional hardware, crypto agility, performance optimization/acceleration, wide applicability for legacy systems, and practical validation through 14 end-user demonstrations.
- **Key Objectives:** Outlines the core goals driven by the project, which include bridging the gap to real-world PQC applications, developing quantum-resistant migration strategies, ensuring continuous compliance, preparing for secure information exchange, and raising awareness.
- **Expected Outcomes (Impact):** Focuses on three specific Expected Outcomes (EO1, EO2, EO3) aimed at validating PQC technology for widespread deployment, ensuring long-term protection of critical assets, and providing tailored migration checklists and plans for unaddressed industrial sectors.

Consortium

- Displays the complete list of all the European institutions, companies, and research centers that make up the PiQASO team, presenting the full network of project members through dedicated partner cards.
- **Partner Detail (Consortium Subpage)** Displays a detailed description of the company or research institution and its exact operational role within the PiQASO project.

Use cases

Introduces how PiQASO applies Post-Quantum Cryptography (PQC) to protect critical infrastructures and services against future quantum computing threats. The page showcases the practical deployment of PiQASO's SDK and "As-a-Service" solutions across 9 distinct industrial sectors:

- **UC1: Enhanced Transportation:** Secures Vehicle-to-Infrastructure (V2I) communication channels to protect real-time data transmission (location, speed) for smart traffic management and incident response.
- **UC2: Autonomous Mobile Robots (AMRs):** Fortifies communication and trajectory data exchange between fleet managers and AMRs in manufacturing and logistics.
- **UC3: Mobile Financial Transactions:** Secures mobile payments (e-wallet, e-banking) by offloading heavy PQC cryptographic operations from resource-constrained mobile devices to the cloud backend.
- **UC4: Energy Supply Chain:** Implements end-to-end quantum-safe protection for electrical smart grids, securing communications from the edge grid nodes to the main datacenter and cloud.

- UC5: Healthcare and Digital Assistance: Protects sensitive patient data through two sub-scenarios: remote patient monitoring gateways and continuous authentication for smart mobile ambulances.
- UC6: Aviation Infrastructure: Secures simulation configurations during Hardware-in-the-Loop (HIL) testing and protects sensitive maintenance reports against eavesdropping.
- UC7: Online Media Services: Future-proofs media distribution networks to protect user billing information, secure account access, and encrypt content streaming/video-on-demand channels.
- UC8: Unmanned Aerial Vehicle (UAV) Communications: Tests and benchmarks lightweight PQC algorithms in resource-constrained drone fleets to secure ground-to-air mission data and trajectory controls.
- UC9: Railway Monitoring: Protects real-time track anomaly data transmitted by autonomous drones to the central infrastructure management system.

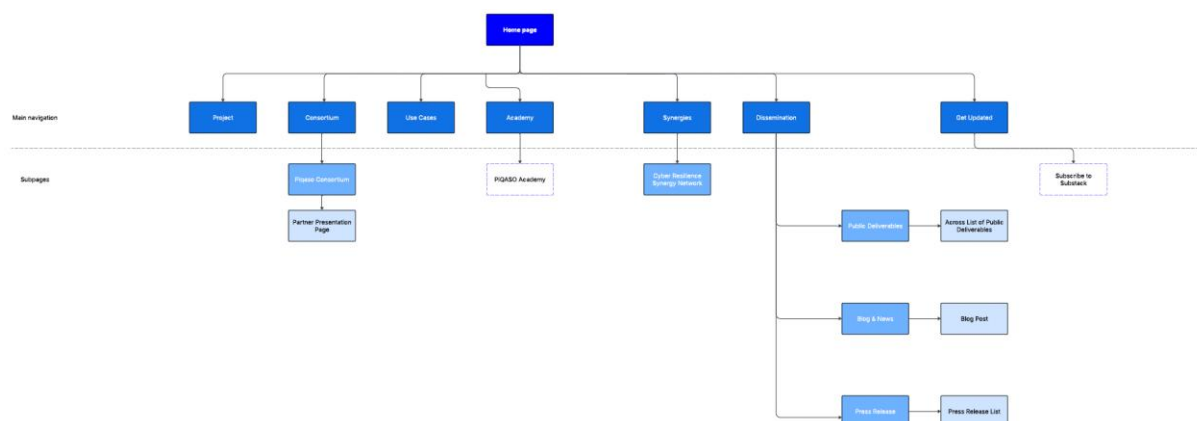


Figure 3 Website structure

3.2.1.2 Website analytics

Table 2 Traffic Analytics

Visits	Active users	Views per Active users	Visit duration	Bounce rate
643	390	3,06	08:10	43,00%

Table 3 Visit Details

Sep-Dec 2025	209	
Jan-Jun 2026	468	
Difference	259	+123,92%

Table 4 Active users Details

Sep-Dec 2025	177	
Jan-Jun 2026	213	
Difference	36	+20,34%

Table 5 Views per Active users detail

Sep-Dec 2025	2,5	
Jan-Jun 2026	4,12	
Difference	1,62	+64,8%

Table 6 Average Visit Duration Details

Sep-Dec 2025	00:03:41	
Jan-Jun 2026	00:12:39	
Difference	00:08:58	+243,44%

Table 7 Bounce Rate Details

Sep-Dec 2025	62,68%	
Jan-Jun 2026	23,32%	
Difference	39,36%	-62,8%

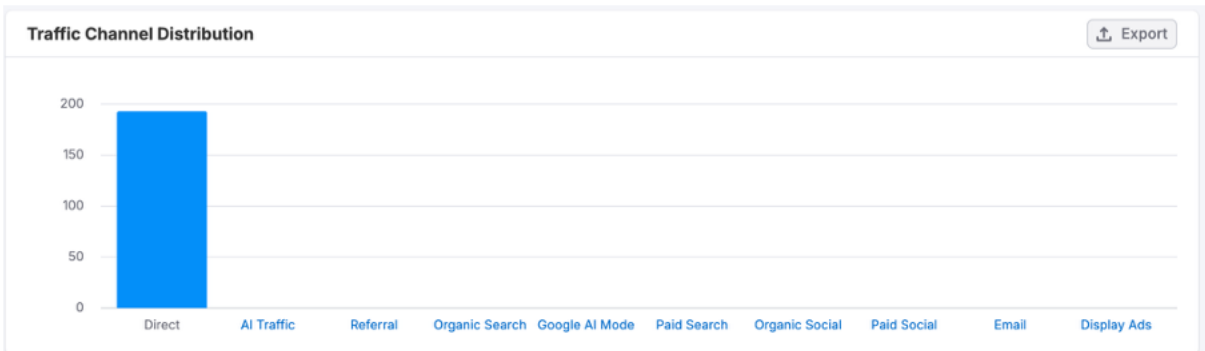


Figure 4 Website channels of traffic

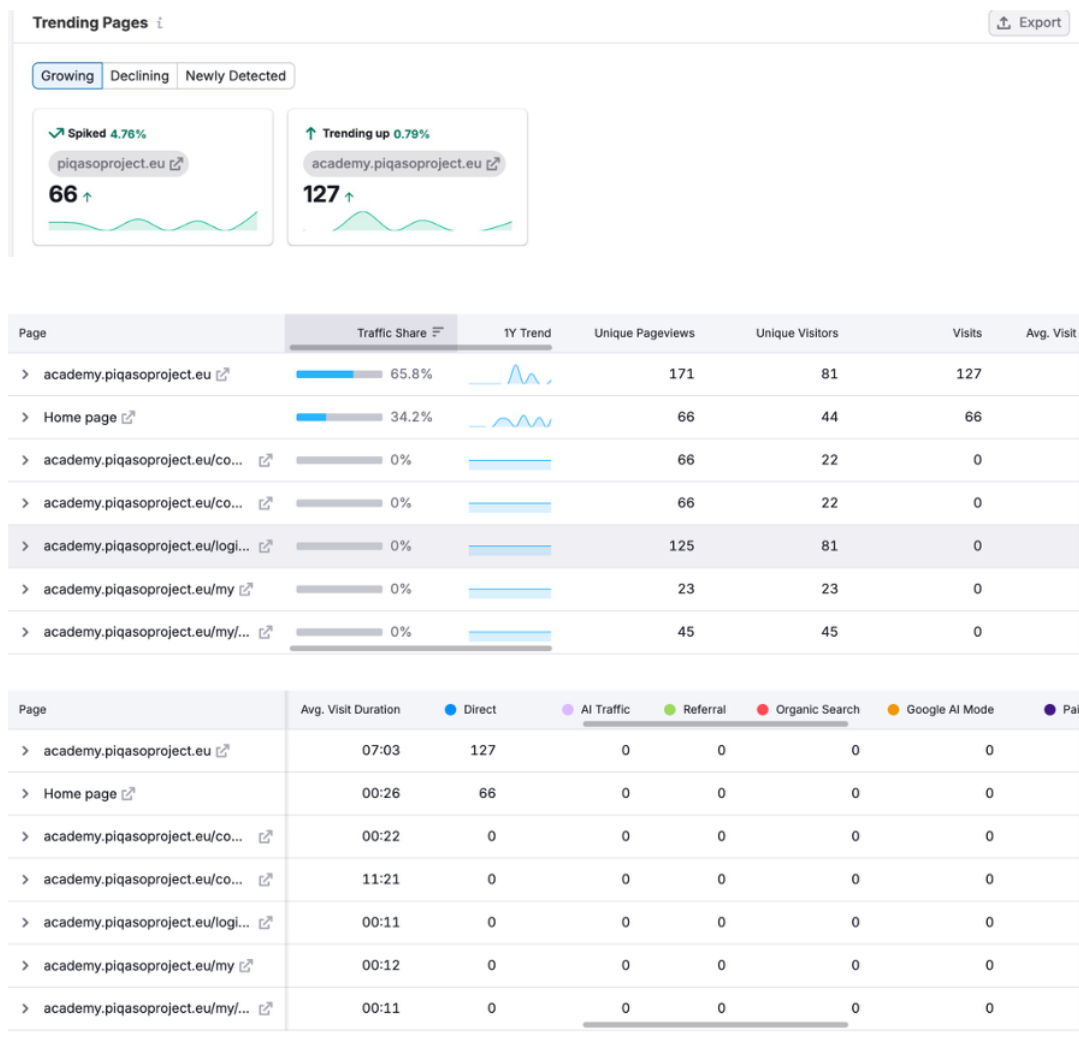


Figure 5 Website top pages

3.2.2 Social Media

PiQASO uses social media as a core communication channel to increase visibility, support community building, and direct stakeholders toward the project website, Academy, and public outputs. In the first reporting period, the project established an active presence on the main channels used by its target audiences, with a particular focus on LinkedIn and Facebook for professional outreach and broader ecosystem engagement.

The social media strategy is designed to support the project's communication objectives across the full lifecycle of the action. During Year 1, activity was concentrated on awareness creation, with regular posts and reposts, press-release amplification, and the promotion of project news, publications, and events through the consortium's digital channels.

3.2.2.1 Social media channels

PiQASO currently uses a combination of project-owned and partner-supported channels to disseminate information to different stakeholder groups. LinkedIn has been the most effective channel for professional and institutional outreach, while Facebook has supported broader visibility and community engagement; together, these platforms help the project reach researchers, industry actors, policymakers, and the wider cybersecurity ecosystem.

Analytics from M1 – M18 confirm that social media are functioning not only as an awareness tool, but also as a mechanism to drive traffic, stimulate engagement, and reinforce recognition of PiQASO's identity and results.

In addition to social networking platforms, the project also uses its website, blog content, and Substack updates as complementary channels to distribute more detailed information and to maintain continuity of communication. This multi-channel approach ensures that short-form social posts can be linked to more substantive material, improving reach and supporting sustained stakeholder interest over time. A good way to integrate social media with project newsletters is to make them part of one content pipeline: use social media to drive attention to the newsletter and use the newsletter to package and deepen the best social media content. In PiQASO's case, this fits well with the existing mix of LinkedIn, Facebook, website, blog, and Substack activity already used for dissemination.

PiQASO uses social channels to amplify project milestones such as publications, the Academy, dissemination activities, and standardization liaison, while the newsletter provides a more structured narrative for stakeholders who need detail. This is especially useful because RP1 showed strong early LinkedIn performance and active editorial work, but some impact-oriented actions are still maturing and benefit from clearer periodic packaging.

3.2.2.2 Social media Analytics

3.2.2.2.1 LinkedIn

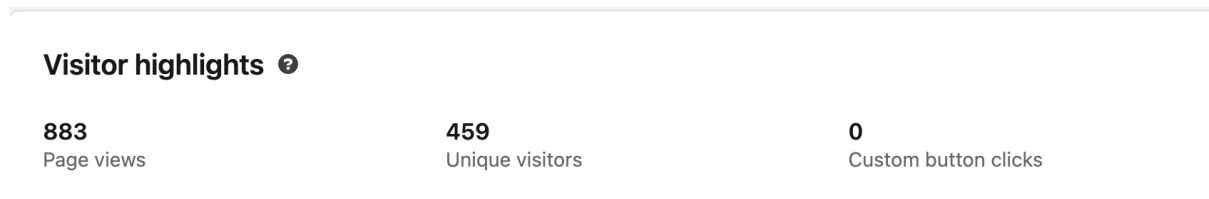


Figure 6 Visitor highlights

Visitor metrics

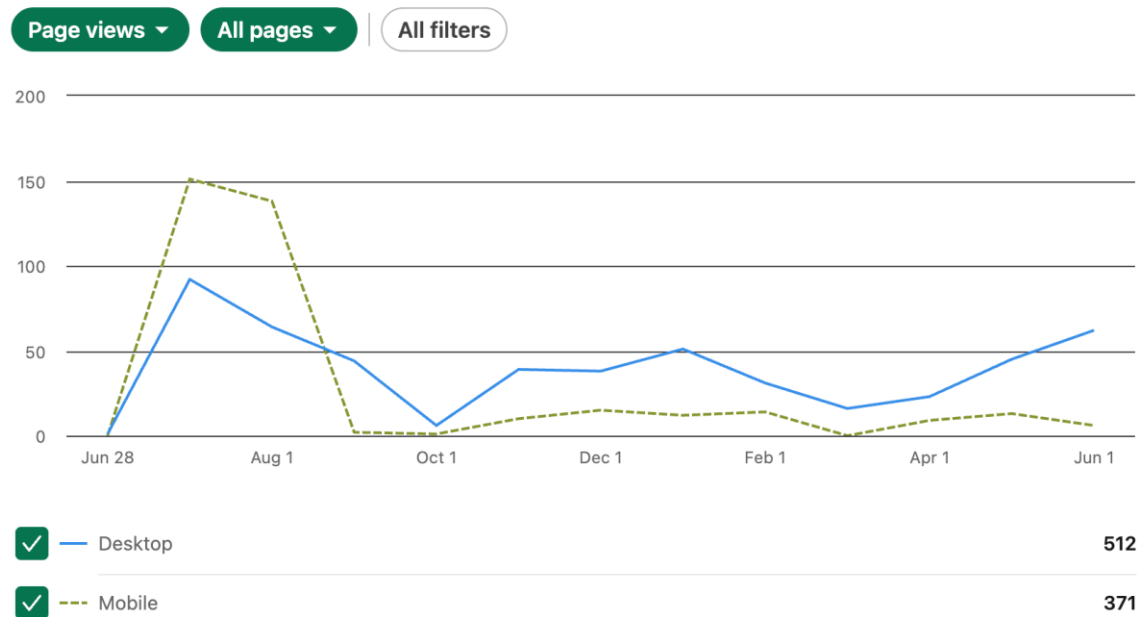


Figure 7 Visitor metrics

Followers

Follower highlights

318

Total followers

261

New followers in the last 365 days

Figure 8 Followers highlights

Follower metrics

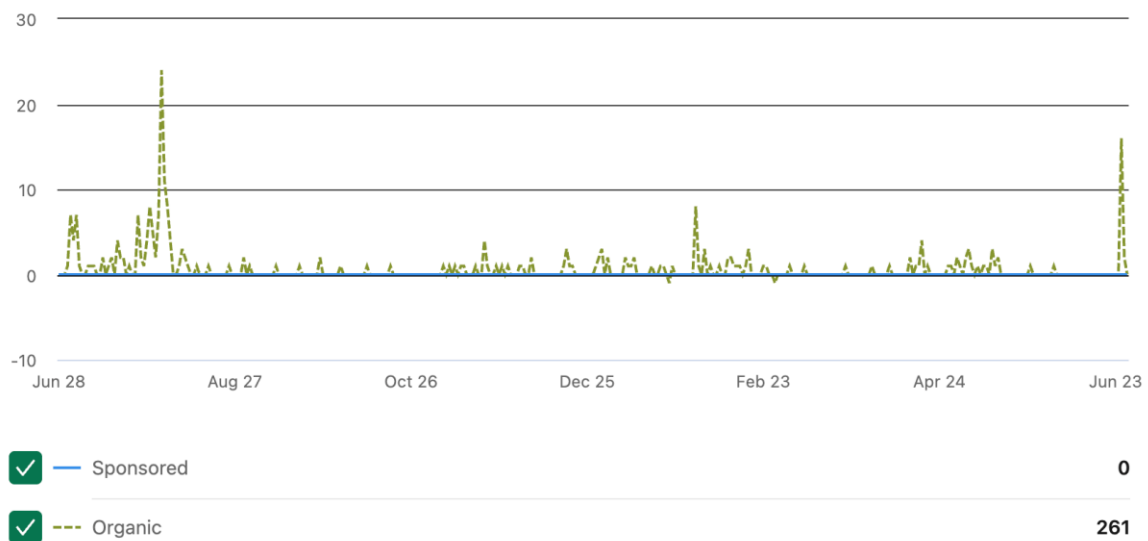


Figure 9 Followers metrics

Content

Highlights

Data for 6/24/2025 - 6/23/2026

45,267

Impressions

1,581

Reactions

7

Comments

17

Reposts

Figure 10 Content highlights

Metrics

Impressions ▾

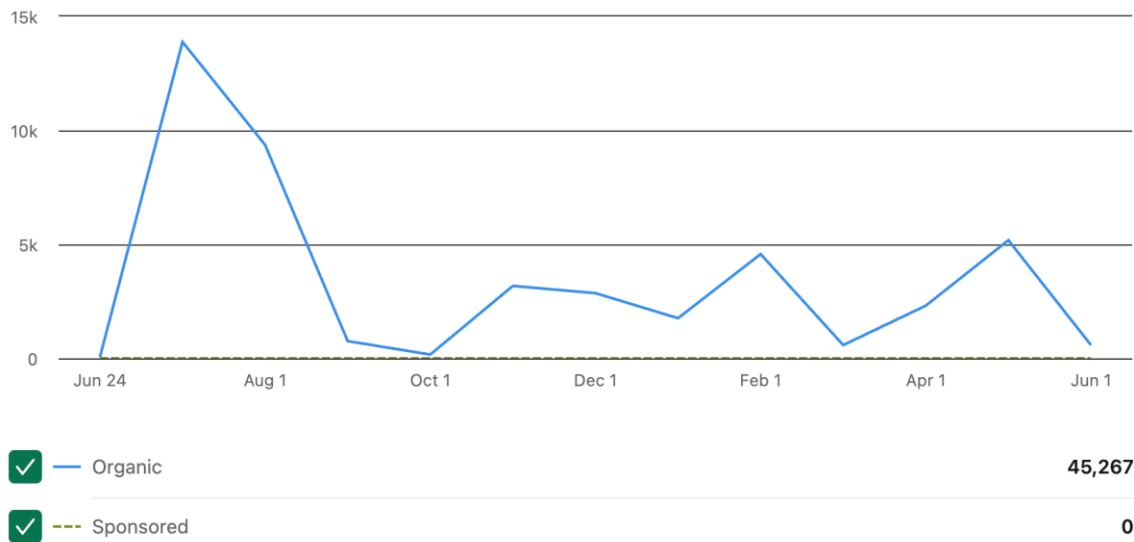


Figure 11 Content metrics - Impressions

Metrics

Clicks ▾

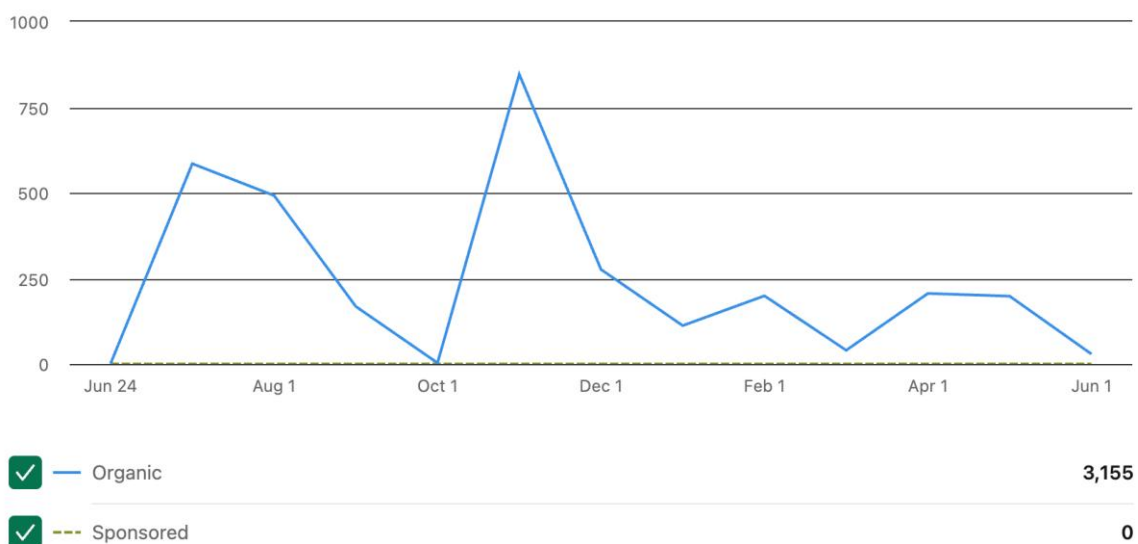


Figure 12 Content metrics - Clicks

Metrics

Engagement rate ▾

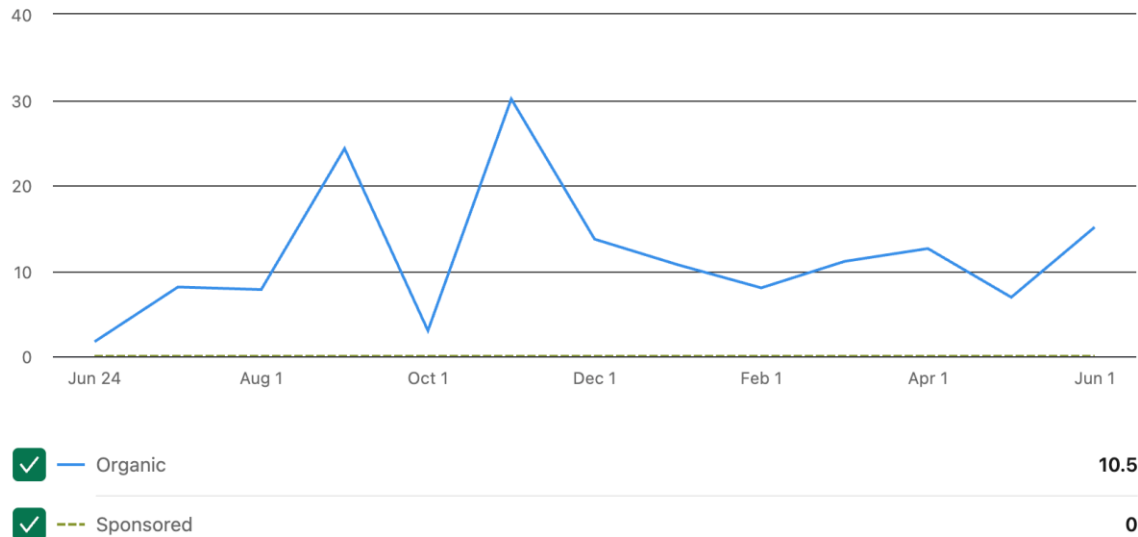


Figure 13 Content metrics - Engagement

Metrics

Reposts ▾

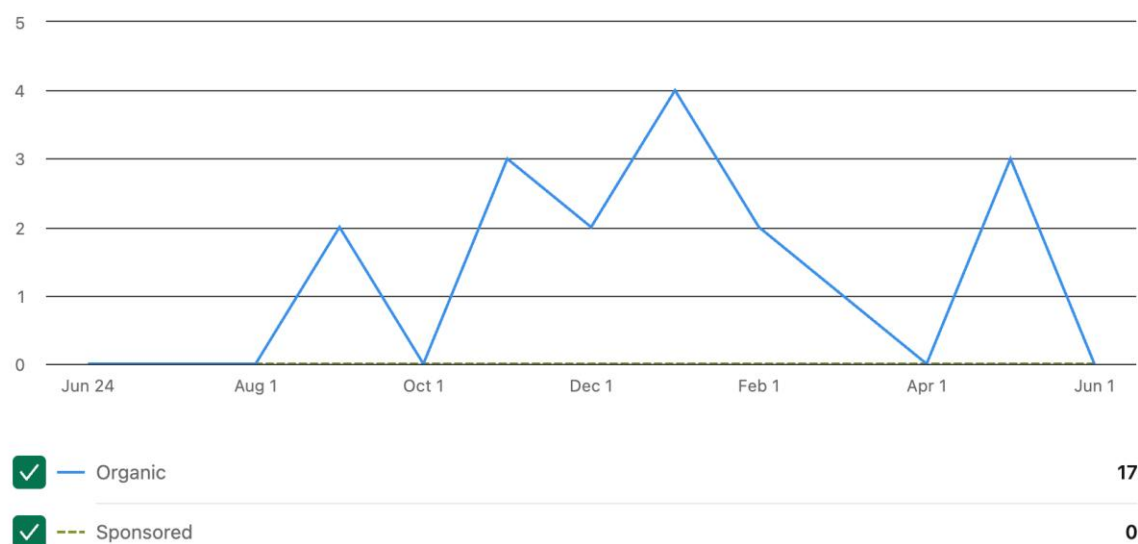


Figure 14 Content metrics - Reposts

3.2.2.2.2 Substack

Overview

All time ▾ ⋮



Figure 15 Substack analytics overview

Content performance

DECEMBER 2025						
	Post-Quantum Cryptography As-a-Service for Common Tra... 17 dicembre 2025 • Piqaso ♡ 4 💬 0	0 Subs	47 Views	100% Opened	↗	...
	PiQASO Consortium Advances European Post-Quantum Sec... 19 dicembre 2025 • Piqaso ♡ 3 💬 0	0 Subs	28 Views	100% Opened	↗	...
	Understanding the PiQASO language: The PiQASO glossary 19 dicembre 2025 • Piqaso ♡ 3 💬 0	0 Subs	19 Views	100% Opened	↗	...
JANUARY 2026						
	PiQASO at a glance: Building Europe's Quantum-Safe Future 7 gen • Piqaso ♡ 3 💬 0	2 Subs	53 Views	100% Opened	↗	...
FEBRUARY 2026						
	Cryptography Evolution: Lessons from the Past 3 feb • Piqaso ♡ 3 💬 1	0 Subs	63 Views	52% Opened	↗	...
	PiQASO Academy: Empowering the Community on Post-Qu... 3 feb • Piqaso ♡ 2 💬 0	1 Subs	83 Views	59% Opened	↗	...
	Two new papers published by UniBwM 6 feb • Piqaso ♡ 0 💬 0	0 Subs	90 Views	43% Opened	↗	...
	The Need to Transitioning to Post-Quantum Cryptography 9 feb • Piqaso ♡ 0 💬 0	0 Subs	55 Views	43% Opened	↗	...
	PiQASO Project Completes Successful First Year Advancing ... 11 feb • Piqaso ♡ 0 💬 0	0 Subs	68 Views	50% Opened	↗	...

	A new paper by UniBwM accepted by USENIX Security Sym... 16 feb • Piqaso 0 Sub 52 Views 43% Opened	 
MARCH 2026		
	PiQASO at the TCG Japan Regional Forum Workshop 25 mar • Piqaso 0 Sub 34 Views 52% Opened	 
APRIL 2026		
	The Quantum Countdown: Why EU Industries Must Migrate ... 7 apr • Piqaso 1 Sub 45 Views 43% Opened	 
MAY 2026		
	First Interview Now Available on the PiQASO Academy Platf... 4 mag • Piqaso 2 Sub 32 Views 38% Opened	 
	PiQASO at INCYBER Forum Europe 2026 5 mag • Piqaso 0 Sub 46 Views 50% Opened	 
	PiQASO: Securing the future of robotics in the quantum era 12 mag • Piqaso 2 Sub 22 Views 36% Opened	 
	PiQASO Project Showcased at Automation and Robotics Exp... 14 mag • Piqaso 1 Sub 17 Views 31% Opened	 
	PiQASO joins the Cyber-Resilience Synergy Network 19 mag • Piqaso 0 Sub 22 Views 45% Opened	 
	PiQASO Publishes First Core Technical Deliverable on Post- ... 25 mag • Piqaso 0 Sub 20 Views 37% Opened	 

Figure 16 Substack content performance

3.2.3 Audio & Video Material

Video 1 - Promo Video

The video outlines the major threat that the upcoming quantum computing era (predicted to arrive as early as 2030, known as "Q-day") poses to current global cryptographic standards. To tackle this challenge, it introduces PiQASO, an EU-funded project designed to smooth the transition toward PQC. The core of the video explains PiQASO's "as-a-service" architecture, which relies on three main technical components:

- PQC Ensemble: A cryptographic SDK designed to ensure data integrity and secure authentication.
- PQ Data Encryption Server: A cloud-based security hub that provides software-driven encryption and authentication capabilities.
- Crypto Agility Layer: A programmable microservices architecture that allows flexible cryptographic operations via Application Programming Interfaces (APIs). The presentation concludes by highlighting the project's real-world validation plan involving 14 end-users across various critical industrial sectors (including automotive, finance, energy, healthcare, and transportation), demonstrating how PiQASO offers a cost-effective, seamless transition to quantum security without disrupting legacy infrastructures.

Link: <https://youtu.be/hoh42NRomY8?si=hy-R5riS-07clfgE>

Video 2 - First Interview: George Pastras (QUBITECH)

The PiQASO Academy platform has officially launched its Guest Speaker Series with an exclusive first interview featuring Dr. George Pastras, leader of the PQC research team at Qubitech. This session focuses on the fundamentals of Public-Key Cryptography, exploring the profound impact that Quantum Computing will have on modern security protocols and diving into the emerging field of PQC. By balancing theoretical foundations with a highly practical perspective, Dr. Pastras addresses the current challenges and future developments necessary to maintain secure communications in a quantum era.

Link: <https://academy.piqasoproject.eu/course/view.php?id=18>

Video 3 – Second Interview: Yassine El Hadi (Red Alert Labs)

This session features Yassine El Hadi, IOT cybersecurity consultant, focuses on cybersecurity assurance, certification, and standards and regulatory frameworks. This is an introductory discussion on regulations and standards in the field of PQC.

Link: <https://academy.piqasoproject.eu/enroll/index.php?id=19>

3.2.4 Press releases

Press release announcing the start of the project and its selection for funding.

Read the full press release here:

[https://cdn.prod.website-files.com/67e56facf764a89af1e9fb52/697752c39286417743445e1d_PiQASO_Announcement_Letter_v00.01%20\(1\).pdf](https://cdn.prod.website-files.com/67e56facf764a89af1e9fb52/697752c39286417743445e1d_PiQASO_Announcement_Letter_v00.01%20(1).pdf)

PiQASO Consortium Advances European Post-Quantum Security at 2nd Plenary Meeting in Athens

Read the full press release here:

https://cdn.prod.website-files.com/67e56facf764a89af1e9fb52/6a0d6ba8a16745d7603283ca_Blogpost%20and%20Press%20Release%20-%202nd%20Plenary.pdf

PiQASO Project Completes Successful First Year Advancing PostQuantum Security for Critical Infrastructures

Read the full press release here:

https://cdn.prod.website-files.com/67e56facf764a89af1e9fb52/698c3c411cb0943c415ec535_PiQASO%201st%20year%20Press%20release.pdf

PiQASO Publishes First Core Technical Deliverable on PostQuantum Cryptographic Primitives

Read the full press release here:

https://cdn.prod.website-files.com/67e56facf764a89af1e9fb52/6a0d6e9ca7b814a51f3402e1_PiQASO%20D3.1%20Press%20release.pdf

3.2.5 Articles

Table 8 List of website articles and blogs

Date	Title	Link
07/01/2026	PiQASO at a Glance: Building Europe's Quantum-Safe Future	https://piqaso1.substack.com/p/piqaso-at-a-glance-building-europes?r=71ws4c
03/02/2026	Cryptography Evolution: Lessons from the Past	https://piqaso1.substack.com/p/cryptography-evolution-lessons-from?r=71ws4c
03/02/2026	PiQASO Academy: Empowering the Community on Post-Quantum Cryptography	https://piqaso1.substack.com/p/piqaso-academy-empowering-the-community?r=71ws4c
06/02/2026	Two New Papers Published by UniBwM	https://piqaso1.substack.com/p/two-new-papers-published-by-unibwm?r=71ws4c
09/02/2026	The Need to Transitioning to Post-Quantum Cryptography	https://piqaso1.substack.com/p/the-need-to-transitioning-to-post?r=71ws4c
09/02/2026	PiQASO Project Completes Successful First Year Advancing Post-Quantum Security for Critical Infrastructures	https://piqaso1.substack.com/p/piqaso-project-completes-successful?r=71ws4c

16/02/2026	A New Paper by UniBwm Accepted by USENIX Security Symposium 2026	https://piqaso1.substack.com/p/a-new-paper-by-unibwm-accepted-by?r=71ws4c
25/03/2026	PiQASO at TCG Japan Regional Forum Workshop	https://piqaso1.substack.com/p/piqaso-at-the-tcg-japan-regional?r=71ws4c
07/04/2026	The Quantum Countdown: Why EU Industries Must Migrate to Post-Quantum Cryptography Today	https://piqaso1.substack.com/p/the-quantum-countdown-why-eu-industries?r=71ws4c
04/05/2026	First Interview Now Available on the PiQASO Academy Platform	https://piqaso1.substack.com/p/first-interview-now-available-on?r=71ws4c
05/05/2026	PiQASO at INCYBER Forum Europe 2026	https://piqaso1.substack.com/p/piqaso-at-incyber-forum-europe-2026?r=71ws4c
12/05/2026	PiQASO: Securing the Future of Robotics in the Quantum Era	https://piqaso1.substack.com/p/piqaso-securing-the-future-of-robotics?r=71ws4c
14/05/2026	PiQASO Project Showcased at Automation and Robotics Expo 2026	https://piqaso1.substack.com/p/piqaso-project-showcased-at-automation?r=71ws4c
19/05/2026	PiQASO Joins the Cyber-Resilience Synergy Network	https://piqaso1.substack.com/p/piqaso-joins-the-cyber-resilience?r=71ws4c
25/05/2026	PiQASO Publishes First Core Technical Deliverable on Post-Quantum Cryptographic Primitives	https://piqaso1.substack.com/p/piqaso-publishes-first-core-technical?r=71ws4c

3.2.6 Conclusion

During the first 18 months of PiQASO, the communication activities have successfully established the project's public identity and ensured a steady flow of information to the relevant audiences. The website, social media channels, press releases, and audio-visual materials have created a solid communication baseline, allowing the project to increase visibility and make its objectives, activities, and early results accessible to stakeholders. In parallel, the consortium has developed a coherent communication style that supports recognition of the project across different channels and partner organisations.

The next phase should focus on maintaining regular communication activity while translating more project results into clear, engaging, and audience-specific messages. Social media should continue to support visibility and traffic generation, while the newsletter should be used to provide more detailed updates and strengthen audience engagement. As additional technical and dissemination outputs become available, communication efforts should increasingly move from general awareness creation to more targeted storytelling around project achievements, use cases, and impact.

4 Task 6.2: Standardisation & WG Liaison

To ensure the strategic goals of the PiQASO standardization roadmap are met, RAL tracks progress against the quantitative and qualitative KPIs established in the initial Dissemination and Communication Plan (D6.1).

As of Month 18, (June 2026), Task 6.2 has successfully achieved all milestone targets designated for the first half of the project lifecycle. The onboarding phase is complete, shifting the task's focus entirely toward active technical contributions and data injection in the upcoming reporting period.

Table 9 Standardisation Status

Standard Body	Engagement Type	Evidence	Technical Contribution	Planned RP2 Contribution	Responsible partner
ETSI QSC	Joined the WG, Active participation	ETSI QSC Sophia Antipolis (Remote) 7th July 2026	Planned contribution / Workshop participation	Technical findings related to Crypto agility & Advanced abstractions including challenges with implementing advanced cryptographic functionalities	RAL, UBITECH, QUBITECH
IETF PQC TLS	Active participation	IETF 126 Vienna (Remote) 18th July 2026	Planned contribution/ Workshop participation	Technical findings related to issues of fragmentation and certificate size requirements in TLS environments	RAL, UBITECH, QUBITECH, TAU
NIST NCCoE PQC migration	Active participation	Mailing list confirmation email	Planned contribution	Technical findings related to Crypto agility & Advanced abstractions including challenges with implementing advanced cryptographic functionalities	RAL, UBITECH, QUBITECH

NIST PQC Forum	Observer	Join Request Email	Technical monitoring activity	-	RAL
OWASP Quantum Security Project	Active participation	Joining Community: Kickoff Call slated for 30/06/2026	Planned contribution/ Workshop participation	PQC risks	RAL
PQCSA	Networks or Collaborative Forums or Platforms	We have been unable to meet PQCSA due scheduling issues on their side. Follow up will continue.	Workshop participation / Collaboration	TBD	RAL, UBITECH, QUBITECH, UniBwM
TCG Japan Regional Forum	Active participation	TCG Japan	Workshop participation	-	UBITECH

4.1 Formal Liaisons Established

During the initial 18 months of the PiQASO project, RAL successfully established direct, formal pipelines to the world's leading PQC standardization authorities and engineering communities. Rather than taking a singular approach, RAL has strategically embedded itself across all three vital layers of the standardization ecosystem: core cryptographic selection, network protocol definitions, and industrial enterprise implementation.

Leveraging RAL's existing ETSI membership and standing in the ecosystem, the PiQASO has transitioned from passive monitoring to an established stakeholder within the following groups:

- ETSI ISG QSC (Quantum Safe Cryptography):** RAL formally registered the PiQASO project mandate with the group leadership. This member-level conduit ensures a direct path to contribute empirical implementation and validation telemetry from PiQASO's 15 industrial use cases straight into upcoming ETSI Technical Reports and migration guidelines.
- NIST PQC Ecosystem Engagement:** RAL has established two distinct pipelines within the National Institute of Standards and Technology (NIST) frameworks to ensure broad coverage:
 - NIST NCCoE (Migration to PQC Project):** Official entry into this collaborative hub provides real-time insights into practical interoperability testing and infrastructure playbooks and allows PiQASO to make valued feedback from our use cases, on what works (or does not work) during migrations.

- **NIST PQC Forum:** Active subscription to this core cryptographic body ensures RAL can track ongoing security reviews, algorithm parameter changes, and formal public comment periods regarding upcoming FIPS standards.
- 3. **IETF PQC / TLS Integration:** RAL has integrated into the Internet Engineering Task Force (IETF) mailing list ecosystems (specifically PQ-TLS). This ensures the project can track and contribute to the evolution of post-quantum Internet Drafts, crypto-agile TLS 1.3 protocol profiles, and X.509 digital certificate formatting.

4.1.1 Others to come

OWASP Quantum Security Project: In further driving the project's standardization and industry alignment objectives, we will be expanding the PiQASO footprint into the soon-to-be-Kicked off OWASP Quantum Security Project.

The initiation of this collaboration at the very end of June 2026 serves as the operational launchpad for the next phase of the project. The consortium will continue to actively identify, evaluate, and join relevant global working groups, forums, and consortia. A significant wave of additional high-impact participations of this nature is planned to systematically roll out across Reporting Period 2 (M19–M36), ensuring PiQASO's empirical validation data directly influences the full global software and hardware security pipeline.

4.2 Specific Technical Contributions

Having successfully established direct, formal liaison pipelines with ETSI ISG QSC, the NIST PQC Migration Community of Interest, the NIST PQC Forum, and relevant IETF working groups, the PiQASO project is uniquely positioned to act as an industrial feedback loop for global standards.

However, to respect and fully protect the commercial business imperatives and IPR of our consortium partners, PiQASO adopts an Output-Driven Contribution Model.

Instead of committing to the disclosure of proprietary architectural or implementation details upfront, the project will continuously monitor the active work items of target Standards Development Organizations (SDOs). As empirical data, performance telemetry, and architectural abstractions mature within our 15 use cases, the consortium will collectively review the outputs. We will selectively identify specific, non-proprietary high-value gaps where PiQASO can influence global standards, proceeding with formal technical contributions only after full consortium consensus is reached.

4.3 Conclusion

The primary focus of the first 18 months was access preparation ensuring RAL possessed the necessary legal, administrative, and portal access to act as a core conduit for the PiQASO consortium with ETSI, IETF and NIST.

As empirical data and testing telemetry comes out of the various pilots and use cases, technical contributions and networking will naturally ramp up to meet the defined KPIs.

Over the next reporting period (M19–M36), RAL will pivot to an active writing and submission stance, converting the raw performance results of the 15 industrial applications directly into the target standard documents presented to the SDOs.

The exploitation methodology of PiQASO builds on the framework established in Deliverable D6.1, which defined five core exploitation management tasks distributed across the project timeline. This section describes the activities carried out in execution of that plan from M7 to M18, reports on tasks currently underway, and outlines those planned for the remainder of the project. The methodology is structured around three implementation stages, each corresponding to a distinct phase of the project's lifecycle, and employs a combination of desk research, primary data collection, partner engagement, and structured exploitation planning tools to ensure that the four KERs are characterised, assessed, and prepared for post-project use.

The first stage addressed the three foundational tasks outlined in D6.1: the identification and initial classification of KERs, stakeholder analysis, and market and positioning analysis, which were carried out in parallel and collectively produced the evidence base from which the exploitation strategy in this deliverable is derived.

At the same time, the project developed a KER registry to identify the individual KERs per partner and start developing plans for their post project exploitation. Through this register partners identify results they may exploit independently of the four consortium KERs.

Figure 17 IPR & KERs registers

Stakeholder analysis was conducted through desk research supplemented by the primary data collection process described below. It identified three decision-maker archetypes relevant to PQC adoption across the nine sectors: Chief Information Security Officers and Chief Data Officers prioritising regulatory compliance under NIS2 and the Cyber Resilience Act; IT infrastructure managers focused on hardware lifecycle constraints and performance continuity; and Chief Technology Officers and Chief Executive Officers approaching quantum readiness as a long-term strategic investment.

Market and positioning analysis was carried out through a combination of secondary research and a primary questionnaire distributed to use case partners across all nine sectors. The secondary research tracked the post-quantum cryptography regulatory environment, including the NIST finalisation of FIPS 203, 204, and 205, the entry into force of EU Regulation 2024/482 establishing the European Cybersecurity Certification Scheme (EUCC), and the relevant obligations under NIS2 and the Cyber Resilience Act, as well as the competitive landscape, covering classical cryptography providers, hardware-based alternatives such as Quantum Key Distribution, and cloud-platform PQC offerings from major technology vendors.

The analysis of related EU-funded projects, synergy networks, and cluster engagements complemented this landscape review, with PiQASO establishing an active presence in the CRSN and initiating engagement with the QPrep project, which addresses quantum readiness at the institutional level.

The market analysis questionnaire was designed by UNIS and UNIS GR to collect sector-specific primary data from consortium use case partners on asset lifecycles, willingness to pay for quantum-safe security, preferred PQC deployment modalities, key market drivers, and barriers to adoption. Responses were obtained from partners representing all nine sectors. The analysis confirmed regulatory compliance as the primary driver of PQC adoption across all sectors, identified early-adopter organisations in the one-to-three-year adoption window, and produced the sector-level urgency, willingness-to-pay, and KER utility assessments presented in Section 5.1. The full questionnaire results were presented and discussed with the consortium at two dedicated partner workshops held in May 2026, co-organized by UNIS and UBITECH, with the participation of the whole consortium.

The first workshop, held on May 8th, 2026, focused specifically on the market analysis findings and sector segmentation, providing an opportunity for partners to validate and refine the questionnaire results in discussion. The second workshop, held on May 21st, 2026, brought together all consortium partners to review the questionnaire findings, examine the four KERs and their draft Business Model Canvases, and initiate the process of individual KER declaration. The session included a structured live activity on a collaborative digital whiteboard (Canva), in which partners mapped their organisations against an Exploitation Paths × KERs matrix covering nine exploitation paths and an Impact Grid covering five impact categories. This activity produced a consortium-wide visualisation of intended exploitation routes and anticipated impacts per KER. the following day.



Figure 18 Exploitation workshops output

During this period of implementation, we also concluded the formal registration of PiQASO as a pilot project within the DEDEP framework, the EU-supported exploitation and dissemination programme operating under the Digital Europe Programme. Following an introductory call with the DEDEP team and participation in the programme's onboarding workshop, PiQASO began integrating the DEDEP structured exploitation tools, specifically the KER characterisation table and the exploitation roadmap template, as the primary frameworks for the per-KER analysis presented in Section 5.1.

Initial Exploitation Analysis (M18–M30)

The second stage, now underway, addresses the initial exploitation analysis task defined in D6.1. It focuses on evaluating each KER in terms of its commercial readiness and exploitation potential, producing the per-KER outputs that constitute the core of Section 5.1.

The SWOT analysis for each KER, of which a preliminary version was included in D6.1, is developed in this stage into a full, evidence-grounded assessment drawing on the competitive landscape from Stage 1, the validated use case outputs from the project's technical work packages, and the partner engagement data collected at the May 2026 workshops. The characterisation tables and exploitation roadmaps are completed per KER using the DEDEP templates, and the Business Model Canvases drafted during Stage 1 are revised to reflect updated market evidence, partner input, and any revisions to pricing assumptions and customer segment definitions.

Two dedicated individual coaching sessions between PiQASO and the DEDEP team, each of two hours, held on June 2026, provided structured external review and guidance on the KER characterisation and roadmap outputs. A partner workshop at the project's plenary meeting, held on June 11th, 2026, provided the primary mechanism for collecting KER lead and consortium partner input on the exploitation outputs before they are finalised.

Business Model Development and Exploitation Routes (M24–M36)

The third stage, planned for the second half of the project, addresses the business model development task defined in D6.1. It will produce partner-specific business models with financial projections, revenue stream definitions, and go-to-market strategies; define the exploitation routes for each KER across pathways including licensing, spin-off, direct productization, and open-source contribution; and conduct a risk analysis per proposed route.

The outputs of this activity will be incorporated into the final exploitation plan reported in Deliverable D6.3 at M36.

5.1 Key Exploitable Results

This section provides detailed characterization, strategic positioning, and exploitation analysis for the core technical and socio-technical outputs generated throughout the PiQASO project lifecycle. Building upon the foundational framework established in Deliverable D6.1, the consortium has advanced its exploitation planning from the initial four candidate technical results to a comprehensive, finalized set.

This total encompasses a holistic post-quantum cryptography ecosystem designed to address the challenges of quantum migration across 9 diverse industrial sectors. Specifically, the following subsections detail the strategic profiles for the PQC Ensemble Secure Implementation (KER 1), the PQ Data Crypto Abstractions (KER 2), the PQC-as-a-Service Modality (KER 3) and the PQ Crypto Assessment and Conformance Toolkit (KER 4).

To ensure a commercially sound and standardized evaluation of each result's readiness and viability, the subsequent subsections analyze each individual KER through three complementary strategic frameworks. First, a comprehensive SWOT analysis; second, a standardized DEDEP Characterization Table that defines the underlying industry problem, existing alternative market solutions, target early adopters, and the specific Unique Selling Point that differentiates the PiQASO innovation; finally, an initial Business Model Canvas outlines the operational and commercial dimensions necessary for sustainable post-project deployment, explicitly detailing ecosystems, customer segments, delivery channels, cost structures, and preferred revenue models.

The following Tables of PiQASO KERs are live documents that will be updated through the duration of the project and are stored in PiQASO SharePoint Repository. Below is presented the current version of these tables, including input of the early discussions that have been conducted, among the consortium, during the first 18 Months of PiQASO project. The final version of these Tables will be presented and analyzed in Deliverable D6.3 – PiQASO Final Report on Communication, Dissemination, and Exploitation activities.

Together, these structured profiles establish the commercial and operational baseline necessary to execute the concrete exploitation pathways detailed in the final stages of the project.

5.1.1 KER 1: PQC Ensemble Secure Implementation with Optimisations and Accelerations

Table 10 KER 1 SWOT Analysis

Strengths	Weaknesses
Features an optimized, high-performance cryptographic design well-suited for real-world deployments. Capable of being effectively deployed across diverse platforms, including embedded systems, IoT devices, and content delivery networks (CDNs).	Potential difficulties in integrating the solution across highly diverse and heterogeneous hardware environments. Performance claims still require rigorous validation across multiple sectors to cement stakeholder confidence and ensure reliable operation.

Broad Sector Relevance for various high-demand sectors requiring robust security.	
Opportunities	Threats
Positioned to capitalize on the increasing demand for secure messaging and mobile applications in the emerging post-quantum era. Strong potential to secure Software Development Kit (SDK) licensing agreements within security-sensitive sectors like telecommunications and defense.	Risk of competing solutions developed by global technology vendors, which could aggressively diminish market share. Heavy reliance on hardware-specific optimizations may limit portability and scalability across heterogeneous system environments.

Table 11 KER 1 DEDEP Characterization table

KER 1	Description
Problem	Organizations across industrial sectors currently rely on older encryption methods that quantum computers will soon be able to crack, resulting in massive security breaches where hackers can steal sensitive corporate data, intercept communications, or physically hack into devices to steal security keys. The major hurdle in upgrading to new quantum-safe security is that it requires immense computing power, which creates a severe slowdown. This causes a critical issue with real-time latency, meaning the system suffers from operational lag or delayed response times. For time-sensitive systems like automated braking in cars, flight controls in planes, or instant banking transactions, even a millisecond of delay can cause the entire system to fail. As a result, businesses face severe regulatory non-compliance , risking heavy legal penalties and exclusion from global markets as governments begin legally mandating these new security standards.
Alternative solution	Organizations either remain on classical cryptography, accepting future quantum risk, or attempt integration using unoptimized open-source reference implementations.
Unique Selling Point USP - Unique Value Proposition UVP	Unlike standard software alternatives or unoptimized open-source references, this solution solves the post-quantum transition crisis by delivering quantum-grade security without compromising on-the-ground operational performance. By pairing a lightweight software SDK with dedicated FPGA hardware acceleration, it eliminates the system lag (latency) that typically causes real-time embedded systems in automotive, aerospace, and banking to fail. Furthermore, its unique configurable security postures allow organizations to seamlessly tune their hardware balance between maximum speed and maximum data protection, rather than being forced into a rigid, one-size-fits-all setup. Because the system's core mathematical correctness is fully validated against NIST-certified golden references and hardened against physical hacking, it provides an immediate, foolproof pathway to global regulatory compliance. This ensures critical infrastructure can safely adopt quantum-resistant encryption without risking operational delays, catastrophic security breaches, or legal supply-chain exclusions.

Description	This product is a complete software and hardware security package that protects electronic systems from future quantum computing threats. It combines a lightweight software library (SDK) containing advanced quantum-safe encryption algorithms with a specialized microchip module (QR-TCB) that acts as a hardware accelerator. While the software handles the underlying security and includes built-in shields to block hackers from physically scanning the device for security keys, the hardware module offloads the heavy mathematical processing to eliminate data delays. Together, they deliver a unified, high-speed security solution that allows industries like automotive, aerospace, and finance to easily upgrade their electronic platforms to quantum-grade protection without sacrificing operational performance.
"Market" – Target market	The primary target market for this specific hardware-accelerated pathway consists of automotive Tier-1 suppliers and aerospace OEMs who develop safety-critical embedded systems with strict, millisecond-level response times and high exposure to physical tampering. These high-reliability sectors represent the immediate priority because their operational needs directly align with the product's core value proposition of high-speed, hardware-insulated quantum protection. While financial institutions requiring high throughput, on-premises transaction processing and semiconductor manufacturers looking to license hardware, IP cores represent massive commercial opportunities, they are treated as secondary and tertiary waves. They will be approached via tailored, separate pathways later to ensure the current deployment remains strictly focused on solving the immediate real-time latency and safety-certification constraints of the automotive and aerospace markets.
"Market" – Early Adopters	Finance industry: FPGA-accelerated modality Automotive industry Aerospace industry: HIL testbench operators
"Market" – Competitors	Thales, Infineon, NXP: PQC-capable HSMs in development, strong brand trust, not yet production-ready at scale. Open-source libraries (liboqs, PQCclean): free and widely used as testing references, but no hardware acceleration layer. Global technology vendors.
Go to Market – Use model	The commercial exploitation strategy relies strictly on a B2B technology licensing model targeted at technology providers and system integrators (such as semiconductor manufacturers, hardware vendors, and Tier-1 automotive/aerospace suppliers) who will embed this quantum-safe technology directly into their own product lines. Revenue will be generated through commercial IP core licensing for FPGA designs, source code/SDK licensing per deployment, and specialized certification consultancy services.
Go to Market – Timing	Approximately 2 years after the end of the project
Go to Market – IPR Background	UBITECH: prior expertise in embedded security and FPGA design AMD Zynq UltraScale+ MPSoC ZCU104 platform; OP-TEE as the trusted execution environment base NIST FIPS 203, 204, 205 as publicly available underlying standards

Go to Market – IPR Foreground	UBITECH: QR-TCB FPGA implementation, hash and polynomial-multiplication acceleration cores, SDK architecture TAU/UniBwM: algorithm optimisation and implementation contributions IP strategy: publication preferred by all partners; patent filing to be explored for the FPGA acceleration architecture and side-channel countermeasure design where demonstrably novel
--------------------------------------	---

Table 12 KER 1 Preliminary Business Model Canvas

Key Partners	Value Proposition	Customer Segments
Semiconductor and chip manufacturers FPGA/ASIC vendors (Defense and aerospace prime contractors IoT device OEMs integrating PQC at chip level NIST/ ETSI standardisation bodies for algorithm certification	Side-channel and fault-injection attack resistance built in by design Supports full crypto-agility across algorithm families Validated in safety-critical real-time environments: V2X under 100ms, UAV flight control, aerospace HIL Drop-in compatible with NIST-standardised algorithms Validated at TRL 7–8	Primary Semiconductor and chip manufacturers embedding PQC at silicon level Automotive Tier-1 suppliers upgrading OBU/RSU security stacks Defense integrators requiring certified, attack-resistant cryptography Secondary IoT platform vendors requiring lightweight PQC for constrained devices Aerospace OEMs needing certified real-time PQC for avionics
Key Activities	Customer Relationships	Cost Structure
Optimisation and maintenance of PQC algorithm implementations FPGA/ASIC hardware core development and testing Side-channel attack resistance validation Benchmarking against performance standards Licensing negotiation and IP management	Technology licensing with technical integration support Long-term R&D partnership agreements with hardware vendors Reference implementation access for evaluation and prototyping Certification support for Common Criteria / EUCC compliance	– FPGA and ASIC hardware development and testing infrastructure Side-channel attack laboratory validation and red-teaming Certification and compliance processes (Common Criteria, EUCC) Ongoing algorithm maintenance as NIST standards evolve Technical support for licensees during integration
Key Resources	Channels	Revenue Streams
Optimised software implementations of ML-DSA, ML-KEM, FALCON, SLH-DSA	Direct licensing to chip and hardware manufacturers NIST / ETSI standardisation contributions as credibility signal	<i>Preferred</i> Technology licensing Source code licensing <i>Secondary</i>

FPGA hardware cores developed on ZCU104 and equivalent platforms Side-channel countermeasure library and test vectors Performance benchmark dataset across 9 industrial sectors	Academic publication and conference presence (CCS, CHES, Eurocrypt) Pilot demonstrations in automotive and aerospace sectors	R&D partnership agreements with hardware vendors Certification consultancy
---	---	---

5.1.2 KER 2: PQ Data Security-by-Design Crypto Abstractions

Table 13 KER 2 SWOT Analysis

Strengths	Weaknesses
Offers a solid, foundational cryptographic architecture specifically tailored for secure system design. Perfectly aligned with critical, high-security use cases such as blockchain, electronic voting (eVoting), and sensitive data management systems.	Estimated commercial realization is two years post-project, delaying immediate industry impact. The abstract nature of the solution may necessitate developing or integrating complementary tools to facilitate practical adoption.
Opportunities	Threats
Well-positioned for adoption in high-growth sectors driven by secure design, such as digital identity, eGovernment, and fintech. Strongly aligns with the rising global prioritization of privacy-first architectures and urgent quantum-resilient mandates.	Full value realization depends heavily on widespread, ecosystem-wide adoption, which requires complex industry coordination. Conceptual nature may deter early adopters unless supported by strong, practical demonstration cases illustrating real-world benefits.

Table 14 KER 2 DEDEP Characterization table

KER 2	Description
Problem	Adopters seeking secure outsourced storage or granular, policy-driven access control are trapped between unusable, academic prototypes and outdated classical encryption systems. Facing this gap carries a devastating 100% risk of data theft from "Harvest Now, Decrypt Later" quantum attacks, especially since 91% of global businesses currently lack a roadmap to defend against quantum threats. Relying on current, non-quantum-safe tools or coarse, all-or-nothing encryption setups forces organizations into a 30% to 40% increase in data management costs due to massive technical debt and the overhead of managing complex, manual user access lists. Ultimately, this lack of production-ready, quantum-safe abstractions leads to immediate regulatory non-compliance with emerging international data protection mandates; this exposes critical industries like healthcare and energy to severe legal penalties, compromised patient or operational telemetry, and catastrophic breaches that directly impact corporate survival.

Alternative solution	Organizations either settle for basic symmetric encryption without granular access control, or commission expensive bespoke cryptographic engineering.
Unique Selling Point USP - Unique Value Proposition UVP	Instead of offering unoptimized academic prototypes or rigid, expensive encryption alternatives, this solution delivers immediate commercial value by eliminating the risk of quantum data theft through a production-ready, quantum-safe abstraction layer. It directly solves the problem of high data management costs and complex access lists by providing automated key rotation (UPKE) and fine-grained, policy-driven access control (ABE) tailored for heavy-use sectors like automation, energy, and aerospace. Furthermore, it translates compliance risks into a seamless operational advantage; for example, in the highly regulated healthcare sector, its functional encryption (FE) allows organizations to perform secure calculations over sensitive telemetry without ever exposing personally identifiable information. By unifying this advanced data-at-rest protection with secure data-in-transit (PQ-TLS), adopters can effortlessly eliminate technical debt, satisfy strict global data protection mandates, and protect their data from future exploitation.
Description	This product is a production-ready cryptographic software toolkit (SDK) that acts as an easy-to-use security shield, allowing software developers to protect sensitive digital data from current and future quantum computing threats without writing complex mathematics. The toolkit provides a simplified security layer featuring three core tools: a policy-based lock (ABE) that automatically limits data access based on specific corporate roles, an automatic key rotation system (UPKE) that constantly updates keys to keep past data safe, and a blind data processing tool (Functional Encryption) that allows systems to analyze sensitive data without ever decrypting it. Combined with an integrated secure communication channel (PQ-TLS) to protect data while it travels across networks, this toolkit enables organizations to easily build quantum-safe protection directly into their applications.
"Market" – Target market	The primary target market for this specific pathway is focused on healthcare data platform operators and medical software integrators who manage highly confidential patient records and continuous telemetry data. This sector represents our immediate priority because their operational needs perfectly match the product's unique capability to perform blind data calculations (Functional Encryption) without exposing sensitive, personally identifiable information. While EU Digital Identity Wallet providers, smart grid operators, and online media platforms are highly viable potential adopters, they represent distinct compliance and operational use cases that will be addressed through separate, dedicated characterisation pathways to ensure this specific commercial rollout remains completely aligned with healthcare data privacy demands.
"Market" – Early Adopters	Healthcare Industry Aerospace Industry Online Media Industry Energy Industry
"Market" Competitors	Bouncy Castle, OpenSSL+liboqs: no ABE/FE support Zama.ai/IBM HElib: FHE, different paradigm OpenABE, CHARM: ABE but not quantum-safe

Go to Market – Use model	This pathway follows a vendor-focused commercialization strategy utilizing a B2B SDK licensing model, where the primary customers are healthcare software vendors and cloud data platform providers who will integrate these quantum-safe abstractions directly into their products. Revenue is generated through a freemium model offering an open-source core to drive industry adoption, alongside paid enterprise licenses for advanced features like automated key rotation and optimized functional encryption. To support these vendors and their corporate end-users, we will offer specialized professional services for advanced cryptographic policy design as a secondary, high-value add-on rather than a separate business model, ensuring a unified market pathway focused entirely on technology integration.
Go to Market – Timing	Approximately 3 years after the project ends.
Go to Market – IPR Background	TAU: prior research in ABE and lattice-based cryptography UniBwM: prior protocol engineering expertise
Go to Market – IPR Foreground	TAU/UniBwM: novel PQ-ABE, PQ-FE, PQ-UPKE constructions UBITECH: SDK integration layer IP strategy: publication preferred by TAU and UniBwM; patent filing considered for specific novel constructions, including the UPKE construction

Table 15 KER 2 Preliminary Business Model Canvas

Key Partners	Value Proposition	Customer Segments
EU Digital Identity Wallet programme and eIDAS stakeholders Identity and access management (IAM) platform vendors Healthcare data exchange networks Smart grid and energy management platform providers Zero-trust architecture solution providers ETSI and IETF working groups on PQ-TLS and protocol standardisation	Hardware-agnostic abstraction layer Attribute-Based Encryption (ABE) enables fine-grained, policy-driven access control on encrypted data PQ-Direct Anonymous Attestation allows identity verification without revealing device or user identity First-mover advantage: protocols like PQ-TLS remain immature, creating a standardisation leadership opportunity Validated across healthcare, finance, aerospace, online media, and automation sectors Validated at TRL 7–8	Primary Software developers and system architects building quantum-safe applications Healthcare data platform operators managing sensitive patient records EU Digital Identity Wallet providers requiring privacy-preserving identity Secondary Smart grid and energy operators managing access to operational data Military and intelligence agencies requiring zero-trust data sharing Online media and content platforms

		managing editorial access control
Key Activities	Customer Relationships	Cost Structure
SDK development and maintenance across platforms and languages ABE and IBE policy engine design and updates Developer documentation and integration tooling Interoperability testing with existing TLS/IPSec stacks Regulatory alignment monitoring (eIDAS, GDPR, NIS2)	SDK licensing with developer support portal Professional services for policy design and ABE deployment Open-source community version to drive adoption and awareness Training and certification through PiQASO Academy	SDK development, versioning, and cross-platform maintenance ABE policy engine design and security auditing Interoperability testing with major TLS/IPSec implementations Developer support and documentation infrastructure Standardisation body participation and contribution costs Regulatory compliance monitoring across multiple jurisdictions
Key Resources	Channels	Revenue Streams
PiQASO SDK codebase with HAL and PQ-TLS implementation ABE, IBE, and PQ-DAA algorithm libraries Validated integration with healthcare (Tellu), finance (CXB), and media (DPG) systems Developer documentation and reference architectures per sector Contributions to IETF/ETSI PQ-TLS working groups	Developer portal and open-source repository (GitHub/GitLab) Direct B2B sales to platform vendors and system integrators EU regulatory and procurement frameworks (eIDAS, NIS2) Standardisation contributions as credibility and visibility channel	<i>Preferred</i> SDK licensing Freemium: open-source core with paid enterprise features <i>Secondary</i> Professional services and integration consulting Training and certification

5.1.3 KER 3: PQC-as-a-Service Modality

Table 16 KER 3 SWOT Analysis

Strengths	Weaknesses
Boasts a fast time to market (under one year) enabled by a cloud-native delivery model. Directly addresses high-demand verticals where secure communication is critical, including healthcare, energy, finance, and industrial automation. Designed as a scalable, modular architecture that supports seamless legacy	Relying entirely on cloud infrastructure may spark trust and regulatory compliance concerns in strictly governed industries. Technical complexities tied to legacy system integration could slow down user onboarding and increase upfront implementation challenges.

migration, making it highly attractive to small and medium enterprises.	
Opportunities	Threats
Strong avenues for growth via commercial partnerships with established cloud service providers and system integrators. Directly aligns with ongoing corporate digital transformations and increasingly stringent international cybersecurity mandates.	Data sovereignty issues and cloud security anxieties in highly regulated markets could stall adoption. High risk of market crowding as major technology giants enter the PQCaaS space, intensifying pressure on smaller providers to differentiate.

Table 17 KER 3 DEDEP Characterization table

KER 3	Description
Problem	Adopters managing large networks of legacy hardware, resource-constrained IoT devices, or long-lifecycle embedded systems face an immediate crisis: their existing devices lack the computational power to execute quantum-safe algorithms natively. From the adopter's perspective, a complete hardware overhaul is financially and operationally impossible in the short term, leaving them stuck with vulnerable systems. Furthermore, operators managing device fleets or unmanned aerial vehicle (UAV) swarms have a critical need for centralized key management and uniform trust architectures; attempting to implement individual, device-level quantum security creates an unmanageable operational burden and introduces massive system inefficiencies. Adopters urgently need a way to patch their severe security gaps and achieve quantum compliance without being forced into expensive, premature infrastructure replacements.
Alternative solution	Status Quo Inertia: Delaying PQC adoption entirely and accepting the escalating long-term quantum risk to legacy infrastructure. Unoptimized Software Workarounds: Relying on software-only PQC implementations, which results in unacceptable operational latency and performance degradation on resource-constrained hardware. Capital-Intensive Infrastructure Upgrades: Deploying highly expensive on-premises Hardware Security Module (HSM) upgrades, which are financially prohibitive and currently not yet fully PQC-capable or production-ready at scale.
Unique Selling Point USP - Unique Value Proposition UVP	This solution delivers immediate financial and operational value by completely decoupling post-quantum security adoption from individual hardware capabilities, allowing adopters to protect their existing infrastructure without costly equipment replacements. For operators of UAV fleets and robotic swarms, the value is an affordable, centralized governance architecture that offloads heavy cryptographic math to a cloud server; this eliminates individual device lag, ensures uniform security across the entire fleet, and allows lightweight drones to remain agile and synchronized. For critical energy infrastructure operators, the value is seamless, automated business continuity; the centralized system generates and distributes quantum-safe keys automatically during algorithm transitions, eliminating manual network

	downtime, reducing maintenance overhead, and ensuring continuous regulatory compliance across sprawling utility grids.
Description	This product is a cloud-deployable Software-as-a-Service (SaaS) platform and API network (driven by the PQ Data Encryption Server) that provides quantum-safe security operations over the internet. It operates as a centralized software hub, allowing resource-constrained or legacy devices to act as "thin clients" that offload their heavy cryptographic workloads to the cloud via secure APIs instead of running the complex algorithms locally. This complete software service integrates seamlessly with hardware and abstraction layers to deliver a unified, plug-and-play network security solution across entire device fleets. <i>Confirmed unified go-to-market narrative across KER 1 and KER 3</i>
"Market" – Target market	The primary target market for this pathway consists of government agencies and critical infrastructure operators (such as energy utilities, defense contractors, and transportation networks) with long-lifecycle assets that are under immediate, legally mandated pressure from frameworks like the NIS2 Directive and the European Common Criteria (EUCC). This compliance-driven sector represents the absolute priority because these organizations are legally obligated to achieve quantum-safe security but are trapped by legacy infrastructure that cannot natively run PQC algorithms. By focusing strictly on this regulatory pathway, the service directly solves their most urgent business problem: avoiding severe legal penalties, compliance failures, and operational shutdowns without forcing them to undergo a financially prohibitive hardware overhaul.
"Market" – Early Adopters	Energy industry UAV industry Finance industry Transportation industry
"Market" Competitors	<i>AWS KMS, Azure Key Vault, Thales Luna Cloud HSM, Entrust nShield, IBM Quantum Safe</i>
Go to Market – Use model	<i>Tiered SaaS subscription; fixed government contracts; hybrid deployment</i>
Go to Market – Timing	Approximately 2 years after the project ends.
Go to Market – IPR Background	QUBI: cloud service architecture and key management expertise INTRA: PQ-DS server architecture
Go to Market – IPR Foreground	QUBI: PQaaS service architecture, PQ-DS implementation, swarm/fleet governance protocols UPKE delivery integration (KER 2) algorithm transition signal protocol jointly exercised with the TAF (KER 4)

Table 18 KER 3 Preliminary Business Model Canvas

Key Partners		Value Proposition	Customer Segments
Cloud providers	infrastructure	Enables legacy systems to become quantum-resistant via API	Primary
National agencies	cybersecurity		Critical infrastructure operators with legacy

Sector regulators (EBA for finance, EASA for aerospace) System integrators deploying critical infrastructure ETSI / NIST standardisation bodies Hardware vendors for legacy device compatibility System integrators deploying critical infrastructure	Protects against Harvest Now, Decrypt Later attacks immediately Crypto-agile: algorithms updated centrally as standards evolve Validated in 6+ operational sectors Reduces time-to-compliance with NIS2 and Cyber Resilience Act Validated at TRL 7–8	systems (energy, transport, finance) SMEs unable to invest in on-premises PQC hardware Government agencies under NIS2 / EUCC compliance pressure Secondary Cloud service providers offering quantum-safe tiers Defence and aerospace organisations with long-lifecycle assets
Key Activities	Customer Relationships	Cost Structure
Operation and maintenance of secure PQC cloud service API development and integration support Customer onboarding and cryptographic migration support Compliance monitoring and certification alignment Continuous algorithm updates as NIST standards evolve	Managed onboarding with migration roadmap per sector SLA-backed service with defined uptime and response time Self-service API portal for technical users Dedicated account support for enterprise/government clients	Cloud infrastructure operation and scaling Security auditing and certification maintenance R&D for algorithm updates and new NIST candidates Customer onboarding and integration engineering Compliance monitoring across regulatory frameworks Key infrastructure management and HSM costs
Key Resources	Channels	Revenue Streams
PQC algorithm implementations (Kyber, Dilithium, FALCON) Secure cloud infrastructure and key management system PQ-DS server developed in PiQASO WP3 API and SDK for client integration Validated use case deployments as reference implementations	Direct B2G sales to government and defence procurement B2B via system integrators and managed security service providers PiQASO Academy and training programmes Standardisation body contributions Industry events and sector-specific pilot demonstrations	<i>Preferred</i> Tiered subscription Fixed contract for government/defense <i>Secondary</i> Per-transaction One-off onboarding and migration support

5.1.4 KER 4: PQ Crypto Assessment and Conformance Toolkit

Table 19 KER 4 SWOT Analysis

Strengths	Weaknesses
Directly addresses the urgent global demand for post-quantum cryptography (PQC)	Requires ongoing sector-specific customization to meet distinct conformance

readiness assessments and standards compliance. Driven by strong enterprises and government interest, with a projected return on investment exceeding €1 million. Widely applicable across public safety, healthcare, industrial IoT, and quantum software sectors.	requirements, potentially escalating complexity and cost. Long-term success is tightly coupled with the widespread adoption of PQC frameworks, which are still evolving unevenly across regions.
Opportunities	Threats
Positions PiQASO as an early market leader in specialized PQC migration and compliance tooling. High potential to influence or seamlessly align with landmark post-quantum certification frameworks being developed by the EU and NIST.	Rapidly evolving PQC standards could demand frequent, costly software updates, straining development resources. Threat of rapid market entry by large, established cybersecurity firms launching competing assessment tools.

Table 20 KER 4 DEDEP Characterization table

KER 4	Description
Problem	From the perspective of regulated enterprises, cybersecurity agencies, and testing laboratories, organizations have an urgent operational need to rapidly identify hidden cryptographic vulnerabilities across their codebases and networks without relying on slow, costly, and error-prone manual audits. Adopters face immense pressure to prove compliance with strict new mandates, such as EU Regulation 2024/482 (EUCC), yet they lack verified tools to confirm that their post-quantum implementations actually meet conformance standards. Furthermore, because threat levels and cryptographic standards evolve constantly, security leaders suffer from a dangerous lack of real-time visibility; they concretely need an automated way to continuously monitor their systems and dynamically update weak encryption before it leads to regulatory penalties or catastrophic security breaches.
Alternative solution	Manual cryptographic audits; Generic security scanners with no PQC-readiness capability
Unique Selling Point USP - Unique Value Proposition UVP	The toolkit is two distinct, complementary components (CAI & TAF), that combine static analysis with crypto agility. Directly addresses EU Regulation 2024/482 (EUCC)
Description	CAI (Crypto Asset Inventorying): a static discovery and evidence-collection layer, already released open-source on GitLab. Four operational analysis modes: Network Analysis, Package Manager Analysis, SSH Key Analysis, and Software Analysis. Rates flows on a four-tier post-quantum readiness scale: post-quantum ready, acceptable/transitional, partial, or vulnerable TAF (Trust Assessment Framework): a live, dynamic monitoring and decision layer, distinct from CAI, that continuously evaluates cryptographic posture at runtime and triggers automated algorithm transitions when a deployed suite falls below an acceptable threshold

"Market" – Target market	EUCC-accredited testing laboratories, national cybersecurity agencies, regulated enterprises, audit/consulting firms, infrastructure operators specifically seeking automated crypto-agility orchestration
"Market" – Early Adopters	Finance, critical infrastructure, energy, healthcare, EUCC labs
"Market" – Competitors	Cryptosense/PwC, IBM Quantum Safe Explorer
Go to Market – Use model	The commercial exploitation strategy is built on a "land-and-expand" B2B commercial licensing model, utilizing the free, open-source Crypto Asset Inventorying (CAI) tool as a credible entry-level driver to capture market adoption and establish industry trust. This entry tier serves as a direct funnel shifting corporate adopters into a highly profitable, long-term paid scheme centered on enterprise software licensing for the Trust Assessment Framework (TAF). Long-term recurring revenue will be secured through annual commercial licenses for runtime monitoring dashboards, automated policy orchestration, and premium compliance reporting features. This primary licensing framework is further supported by white-label software licensing tailored directly for EUCC testing laboratories and audit firms, alongside fixed-term government framework contracts for continuous public-sector infrastructure monitoring.
Go to Market – Timing	Approximately 2 years after the end of the project
Go to Market – IPR Background	UBITECH: CAI architecture and the four analysis modes
Go to Market – IPR Foreground	TAU & UniBwM: TAF decision logic, mutation-based fuzzing framework (strongest patent candidate)

Table 21 KER 4 Preliminary Business Model Canvas

Key Partners	Value Proposition	Customer Segments
ENISA and national cybersecurity agencies (ANSSI, BSI, CCN) EUCC accredited testing laboratories National accreditation bodies for ICT product certification ETSI and NIST for standards alignment and reference test vectors Enterprise IT security auditing firms (Big 4, specialist cybersecurity consultancies) Sector regulators mandating cryptographic compliance (EBA, EASA, NIS authorities)	Automated discovery of all cryptographic assets across systems, producing a structured Cryptography Bill of Materials (CBOM) Real-time monitoring of cryptographic posture against NIST and EUCC compliance requirements Mutation-based fuzzing identifies implementation vulnerabilities beyond standard test vectors Structured migration roadmap output Directly addresses EU Regulation 2024/482 (EUCC), which came into force in 2025 Urgent regulatory demand	EUCC accredited testing laboratories requiring PQC validation tools National cybersecurity agencies (ENISA, ANSSI, BSI) mandating compliance Large enterprises in regulated sectors needing cryptographic inventory and audit trails Secondary Enterprise IT security and compliance departments System integrators conducting security assessments for clients Critical infrastructure operators in energy, transport, and finance

Key Activities	Customer Relationships	Cost Structure
Development and maintenance of the CBOM generation engine Mutation-based fuzzing and vulnerability scanning against PQC implementations Continuous alignment with evolving NIST and ETSI standards Sector-specific migration checklist and assessment report generation Integration with existing enterprise security and audit toolchains	Subscription-based access with automated report generation Managed assessment service for organisations without internal security expertise Audit firm partnerships Government procurement via framework agreements with national agencies	Toolkit development, testing infrastructure, and vulnerability research Continuous standards monitoring and update cycles (NIST, ETSI, EUC)C Sector-specific migration checklist development and validation Regulatory engagement and accreditation body liaison Enterprise integration and API development for audit toolchain compatibility Customer support for managed assessment service delivery
Key Resources	Channels	Revenue Streams
CBOM generation engine and cryptographic discovery tooling Fuzzing and vulnerability testing framework for PQC implementations Sector-specific migration checklists Test vector library aligned with NIST FIPS 203/204/205 Assessment reports from 9 industrial sectors	Direct B2G Partnership with EUC) testing laboratories as resale or integration channel Enterprise sales via cybersecurity consultancies and audit firms ENISA and EC policy forums Publication of sector-specific migration guides as market-building content	<i>Preferred</i> Annual SaaS subscription Government framework contracts <i>Secondary</i> Managed assessment service White-label licensing to audit firms and EUC) testing laboratories

5.2 Market Analysis & Competitive Landscape

The transition to PQC represents a fundamental paradigm shift in cyber-resilience, moving from reactive threat mitigation to proactive, long-term cryptographic lifecycle management. Based on the provided PiQASO Market Analysis and Questionnaire (ANNEX I) results, European critical infrastructure and high-stakes commercial sectors are facing structural vulnerabilities driven by the "Harvest Now, Decrypt Later" (HNDL) paradigm. Adversaries are actively intercepting and archiving encrypted data today with the intent of decrypting it once cryptanalytically relevant quantum computers (CRQCs) become operational. This threat compresses the available timeline for migration, transforming PQC implementation from a forward-looking roadmap item into an immediate regulatory and operational necessity.

At this stage of the PiQASO project, we have identified the UC partners and their respective industries as early adopters. The PiQASO use cases are composed of nine (9) different industries: Automotive, Automation, Finance, Energy, Healthcare, Aerospace, Online Media,

UAVs, and Transportation. One or two representatives from these industries participated in a survey for the PiQASO Market Analysis, which was conducted via a questionnaire. The results of this survey assisted in the overall PiQASO Market Analysis.

The overall results of the questionnaire are available here:
https://docs.google.com/spreadsheets/d/1Fy-mJaxlGeyJ6dJNejwTLSPZTSLCKKvTMvry0XzJ4_E/edit?usp=sharing.

5.2.1 Macro-Environmental Drivers & Market Dynamics (PESTEL Alignment)

To understand the market potential for the PiQASO platform, we must analyze the macroeconomic forces driving or inhibiting adoption. Aligning the primary market feedback from the file "PiQASO Market Analysis Questionnaire" with a structured PESTEL framework reveals that the transition to PQC is not merely a technical upgrade, but a highly complex shift influenced by regulatory, economic, and systemic market constraints.

Political & Legal Drivers: Regulatory Mandates as the Primary Catalyst

The primary catalyst forcing organizations to evaluate and adopt PQC across all critical European sectors is regulatory compliance. Voluntary risk management has historically been insufficient to drive cryptographic migration due to immediate cost concerns; however, evolving European legislative frameworks are fundamentally changing this dynamic.

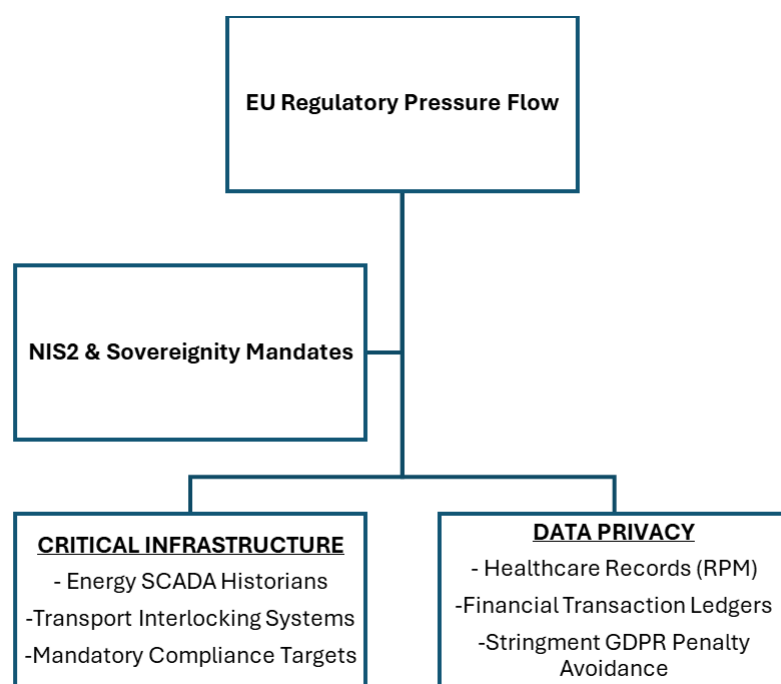


Figure 19 Macro-Environmental Drivers & Market Dynamics

The NIS2 Directive & Critical Infrastructure: Cyber-resilience mandates, such as the NIS2 Directive, place strict legal and financial liabilities on executives to secure essential supply chains. This pressure is concentrated in **Segment 1 (Energy, Transportation, and Finance)**, where infrastructure operators manage assets with national security implications.

European Digital Sovereignty: As highlighted in the Transportation sector analysis (UC9), the protection of cross-border transmission networks and shared European infrastructure is

increasingly viewed through the lens of digital sovereignty. Migrating to quantum-safe frameworks ensures that European logistical and operational links remain secure against foreign intelligence interception.

GDPR and Everlasting Data Privacy: In the Healthcare sector (UC5), the legal imperative is driven by the threat of severe GDPR penalties. Because Remote Patient Monitoring (RPM) and Electronic Health Records (EHR) hold data that must remain confidential for the lifetime of the patient, the legal framework essentially requires "everlasting privacy", meaning data must be protected today against future decryption.

Economic Realities: The Asymmetric Security Premium

The financial willingness to absorb the costs of PQC implementation, as indicated from the questionnaire responders, varies significantly across sectors, revealing a highly fragmented economic landscape. Initial evidence suggests that the market is divided into categories based on asset importance and the ability to tolerate additional costs:

Market Tier	Target Sectors	Willingness to Pay (Security Premium)	Economic Rationale & Investment Profile
High-Premium / Critical	Energy, Transportation, Finance, UAVs	15% – 25%	High Liability: High cost of a hardware "rip-and-replace" or catastrophic loss of trust. High initial Capex for gateway upgrades is offset by long-term grid and transaction stability.
Moderate-Premium / Value	Automation, Healthcare, Aerospace, Automotive	5% – 15%	ROI and Compliance Driven: Investment is bounded by supply chain requirements, high R&D certification overheads, or fixed firmware upgrade cycles.
Low-Premium / Commodity	Online Media	0% – 5%	Platform Dependent: Security is treated as a transparent backend feature. Organizations heavily resist early adoption costs, viewing migration as a commodity update handled via cloud SaaS fees.

Figure 20 Willingness to pay per market tier

Cost Internalization and Commercial Constraints

A critical economic insight from market participants (specifically noted by CAIXA in Finance and FGC in Transportation) indicates that large enterprise operators plan to internalize the costs of migrating to PQC. These organizations intend to adopt the functionality "for free" as part of routine system maintenance or vendor updates, rather than transferring additional premium costs to their end-line customers. Consequently, commercial PQC vendors cannot rely on a simple pass-through pricing model; they must instead market PQC as a risk-mitigation tool that prevents downstream liabilities and operational downtime.

5.2.2 Socio-Technical Dynamics: Systemic Ecosystem Interdependency

The findings from the PiQASO market questionnaire confirm a critical systemic challenge: PQC solutions cannot be effectively deployed in isolation.

The 85% Interdependency Rule: Aggregated sector feedback reveals that 85% of surveyed respondents consider their market viability entirely dependent on their upstream suppliers (e.g., semiconductor chipmakers, software vendors) and downstream customers (e.g., infrastructure operators) migrating at the exact same time.

This high level of interdependency creates localized market deadlocks across key use cases:

Automotive (SDVs): Original Equipment Manufacturers (OEMs) cannot successfully deploy secure Over-the-Air (OTA) updates unless Tier-1 and Tier-2 component suppliers design and deliver PQC-compliant microcontrollers and hardware security modules.

Aerospace: Migration is effectively stalled by hardware lock-in. Aerospace operators are unable to upgrade satellite telemetry links until semiconductor manufacturers develop and certify space-grade, radiation-hardened PQC chipsets.

Online Media: The commercial viability of PQC-protected Digital Rights Management (DRM) and billing platforms is completely dependent on web browser engines (Google, Apple) and operating systems supporting post-quantum cryptographic primitives natively.

Industrial Automation: Heterogeneous factory floors feature equipment from multiple competing vendors (e.g., Siemens, ABB). Securing multi-robot coordination or Programmable Logic Controller (PLC) loops requires broad industry consensus and protocol alignment; otherwise, a single classical link breaks the security of the entire operational chain.

This environmental reality informs PiQASO's market positioning. By identifying these bottlenecks, the project can position its open-source core, software-defined SDKs, and PQCaaS cloud offloading capabilities as tools to bypass the hardware scarcity delay, allowing early adopters to achieve quantum resistance without waiting for complete hardware supply chain replacement.

5.2.3 Market Segmentation & Target End-User Profiles

The target market for early adoption can be categorized into three distinct segments. These segments are defined by their specific asset types, the longevity of their infrastructure, and the operational risks they face.

Segment 1: Quantum-Urgent Infrastructure (Energy, Transportation, Finance)

This segment represents the most immediate market opportunity due to the extreme operational lifecycles of its assets and the potential impact on national security. Organizations in this group are driven by the need to secure critical services against HNDL tactics.

Energy Operations: This sub-segment involves securing legacy Operational Technology (OT), Supervisory Control and Data Acquisition (SCADA) historians, and Renewable Energy Source (RES) parks. These systems have an average asset lifecycle of 15 to 25 years, meaning hardware deployed today must withstand the transition to quantum computing.

Transportation Networks: Focuses on securing critical cross-border transmission systems, airport infrastructure, and railway interlocking systems. The primary objective is to protect public safety and maintain European digital sovereignty.

Financial Institutions: High-volume transaction processing and Know Your Customer (KYC) ledgers require early transition to maintain transactional integrity. For example, the top 5 banks manage approximately 70% of the market in Spain, serving as a concentrated point of origin for early market adoption.

Segment 2: Real-Time Safety & Hardware-Constrained Environments (Automotive, UAVs, Aerospace, Automation)

This segment includes high-stakes industrial and commercial environments where Post-Quantum Cryptography (PQC) must integrate directly into complex, real-time safety systems and embedded hardware.

Software-Defined Vehicles (SDVs): The automotive sector is transitioning toward connected, software-driven architectures with 10 to 20-year vehicle hardware cycles. The critical challenge is deploying low-latency embedded PQC algorithms to secure safety-critical Over-the-Air (OTA) updates and Vehicle-to-Everything (V2X) communications.

Unmanned Aerial Vehicles (UAVs): Commercial drone fleets require real-time payload encryption to protect active aerial data streams during surveillance and logistics missions. Because weight and power are constrained on-board, this sub-segment relies heavily on cloud-offloaded architectures like PQCaaS to avoid heavy hardware overhead.

Aerospace Applications: Requires securing satellite telemetry links and flight data protection in radiation-hardened environments. This domain faces long development cycles (15–20 years) and high certification barriers.

Industrial Automation: Focuses on securing Autonomous Mobile Robots (AMRs), Programmable Logic Controller (PLC) control loops, and factory-floor IoT sensors. It features heterogeneous device environments requiring lightweight, optimized software development kits (SDKs) to protect corporate IP and operational connectivity.

Segment 3: Privacy & Long-Term Data Protection (Healthcare, Online Media)

This segment focuses on data confidentiality, regulatory compliance, and managing user access across cloud architectures.

Healthcare Providers: Remote Patient Monitoring (RPM) and Electronic Health Records (EHR) require long-term data security by design. The primary driver is preventing data leaks that could violate GDPR mandates, requiring "everlasting privacy" for patient records over 10 to 15-year lifecycles.

Online Media Platforms: This sub-segment focuses on protecting subscriber databases, user billing information, and secure Digital Rights Management (DRM) content distribution. With short asset lifecycles (3–5 years), this sector treats security as a transparent, cloud-native feature and has a low tolerance for cost premiums.

Target End-User Profiles: B2B Decision Makers

To effectively position the PiQASO solution, commercialization strategies must address the distinct technical and economic priorities of three key buyer personas identified in the survey:

Table 22 PiQASO Key buyer personas

Chief Information Security Officer (CISO) / Chief Data Officer (CDO)	
Core Focus:	Risk management, liability reduction, and corporate governance.
Key Drivers:	Compliance with European mandates like the NIS2 Directive and avoiding regulatory fines.
Primary Sectors:	Highly active within the Healthcare, Finance, and Transportation sectors.
Value Alignment:	They prioritize cryptographic solutions that integrate smoothly into existing risk reporting frameworks without disrupting standard compliance workflows.
IT Infrastructure Manager	
Core Focus:	Operational continuity, system latency, and hardware deployment constraints.
Key Drivers:	Managing network bandwidth limitations and hardware lifecycles. They are cautious about large PQC key sizes impacting storage or causing processing bottlenecks.
Primary Sectors:	Dominant in the Aerospace, UAV, and Energy sectors.
Value Alignment:	They prefer highly optimized SDKs and hybrid cloud-edge deployments (PQCaaS) that limit the need for immediate, expensive hardware replacement.
Chief Technology Officer (CTO) / Chief Executive Officer (CEO)	
Core Focus:	Long-term technology strategy, product differentiation, and market positioning
Key Drivers:	Building "everlasting" security into their core product lines to establish a Unique Value Proposition (UVP) against competitors
Primary Sectors:	Most influential in the Industrial Automation, Robotics, and Automotive sectors
Value Alignment:	They look for scalable, crypto-agile solutions that protect corporate intellectual property and future-proof products against evolving technological threats

5.2.4 Technical Barriers & Market Friction Points

A successful market entry strategy for the PiQASO platform depends on its ability to directly mitigate the technical friction points identified by industry practitioners.

Data from the file "PiQASO Market Analysis Questionnaire" reveals that deployment challenges are divided between immediate runtime operational constraints and broader systemic uncertainties regarding hardware availability and protocol agility.

The Performance vs. Security Trade-Off

Integrating PQC introduces severe processing and operational trade-offs that directly collide with the requirements of real-time industrial and automotive application.

Technical Barriers: Which technical challenge is most likely to slow market uptake in your sector?

14 responses

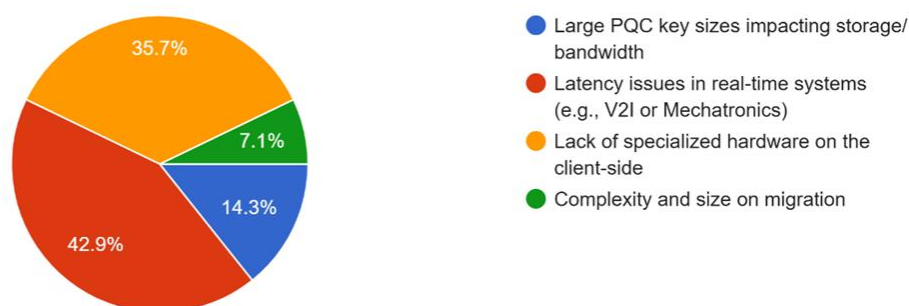


Figure 21 Questionnaire results – Technical barriers

Real-Time Latency Constraints (42.9% of Responses): The largest share of market participants identifies runtime latency as the primary technical barrier slowing down PQC market uptake. In fast-moving operational loops (such as Automotive Vehicle-to-Infrastructure (V2I) safety systems (UC1) or Mechatronic multi-robot coordination paths (UC2)) the additional microsecond overhead generated by mathematically intense asymmetric PQC operations can compromise safety-critical functions.

Key Size, Storage, and Bandwidth Strains (14.3% of Responses): Standard asymmetric cryptography relies on relatively small keys; conversely, quantum-resistant algorithms often demand significantly larger keys and signature sizes. This structural change places severe strain on legacy communication channels, multiplying bandwidth consumption and exhausting the constrained memory storage capacity of edge sensors, UAV controllers, and embedded vehicle modules.

The Client-Side Hardware Deficit

A primary obstacle preventing local execution of quantum-safe algorithms is the widespread deficiency of optimized infrastructure at the edge.

Embedded Hardware Scarcity (35.7% of Responses): More than a third of surveyed professionals note that a lack of specialized client-side or embedded hardware severely limits their deployment roadmaps. Current microcontrollers, field-programmable gate arrays (FPGAs), and programmable logic controllers (PLCs) lack the dedicated hardware acceleration blocks needed to compute complex PQC primitives efficiently.

The PiQASO Mitigation Pathway (PQCaaS): This widespread hardware gap provides a strong market entry point for PiQASO's architectural design. By offloading heavy cryptographic computations to a cloud-based or edge-gateway-hosted Post-Quantum Cryptography as a Service (PQCaaS) framework, the project allows hardware-constrained systems (like UAVs or remote medical monitors) to achieve quantum resistance without undergoing expensive, premature physical hardware overhauls.

The Crypto-Agility Paradox

A major point of strategic uncertainty within the market relates to the concept of Crypto-Agility, the architectural capability of a system to seamlessly swap cryptographic algorithms without modifying the underlying application software infrastructure.

Unique Value Proposition (UVP): For your specific market, does the benefit of Crypto Agility outweigh the benefit of Performance/Latency?

14 responses

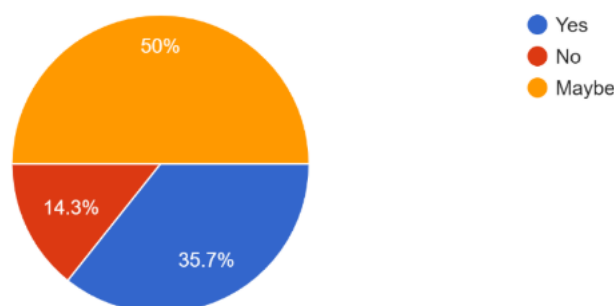


Figure 22 Questionnaire results – Unique Value Proposition

The Consensus Divide: While 35.7% of respondents recognize that the long-term protection of crypto-agility outweighs operational degradation, a small but significant 14.3% outright reject this trade-off due to rigid, real-time performance requirements.

The 50% "Maybe" Ambiguity: Exactly half of the market participants surveyed (50.0%) remain undecided. This large, uncommitted segment indicates that the market lacks clear performance benchmarks. These organizations understand the theoretical value of long-term cryptographic agility to protect against changing quantum threats, but they are hesitant to commit due to fears of systemic performance penalties, bandwidth inflation, and integration complexity.

5.2.5 Sector-Specific Market Profiles

To align PiQASO's technical assets with commercial realities, we must evaluate the unique operational profiles, cost behaviors, and deployment requirements of each sector, as the responders has indicated them in the survey.

Use Case 1: Automotive

- **Operational Horizon & Primary Asset:** 10–20-year vehicle hardware cycles protecting CAN Bus systems and safety-critical operations.
- **Urgency & Driver: High;** driven by the transformation toward Software-Defined Vehicles (SDVs) and the critical need to secure remote Over-the-Air (OTA) updates and Vehicle-to-Everything (V2X) links against safety liabilities.
- **Financial & Premium Profile:** Willingness to pay a **5%–10% premium**. High volume constraints make this sector highly price-sensitive, requiring low-cost software integrations rather than expensive hardware modifications.

- **Deployment Modality:** Embedded SDKs designed to handle strict real-time execution.

Use Case 2: Industrial Automation

- **Operational Horizon & Primary Asset:** 10–15 year factory-floor lifecycles protecting Programmable Logic Controller (PLC) control loops and Autonomous Mobile Robots (AMRs).
- **Urgency & Driver: Medium;** driven by the need to protect corporate IP and trade secrets from HNDL industrial espionage.
- **Financial & Premium Profile:** Willingness to pay a **10%–20% premium**. Investment is typically triggered by upstream supply chain prerequisites rather than immediate customer demand.
- **Deployment Modality:** Optimized, lightweight SDKs capable of operating across diverse, multi-vendor device environments without requiring a full hardware refresh.

Use Case 3: Finance

- **Operational Horizon & Primary Asset:** 5–10-year system lifecycles securing high-volume transactional data, financial ledgers, and Know Your Customer (KYC) databases.
- **Urgency & Driver: High;** driven by severe regulatory pressure, compliance mandates, and the threat of catastrophic loss of customer trust.
- **Financial & Premium Profile:** Willingness to pay a **15%–20% premium**. Major costs are centered around upgrading physical Hardware Security Modules (HSMs). Notably, institutions plan to *internalize* these costs rather than passing a premium down to consumers.
- **Deployment Modality:** Cloud-based Post-Quantum Cryptography as a Service (PQaaS) for high-frequency transactional validation.

Use Case 4: Energy

- **Operational Horizon & Primary Asset:** Critical 15–25-year operational horizons protecting Supervisory Control and Data Acquisition (SCADA) historians and Renewable Energy Source (RES) parks.
- **Urgency & Driver: Critical;** driven by strict national security concerns and mandatory compliance targets defined under the European NIS2 Directive.
- **Financial & Premium Profile:** Willingness to pay a **25% premium** (the highest among surveyed sectors). The catastrophic cost of physical hardware replacement makes operators comfortable with a security premium to avoid grid disruption.
- **Deployment Modality:** Hybrid implementations and dedicated PQC Gateways to shield legacy infrastructure.

Use Case 5: Healthcare

- **Operational Horizon & Primary Asset:** 10–15-year lifecycles protecting sensitive Remote Patient Monitoring (RPM) streams and lifetime Electronic Health Records (EHR).
- **Urgency & Driver: Medium;** driven by the absolute legal necessity of maintaining "everlasting privacy" for medical records and mitigating severe GDPR non-compliance penalties.
- **Financial & Premium Profile:** Willingness to pay a **10%–15% premium**. Providers expect PQC capabilities to be seamlessly bundled directly into existing hospital management systems and device firmware updates.
- **Deployment Modality:** Hybrid PQaaS configurations to balance cloud accessibility with local data control.

Use Case 6: Aerospace

- **Operational Horizon & Primary Asset:** 15–20-year lifecycles securing satellite telemetry links and flight data protection.
- **Urgency & Driver: Medium;** bounded by long research and development cycles and highly specialized governmental/defense contract specifications.
- **Financial & Premium Profile:** Willingness to pay a **15% premium**. Commercial feasibility is highly constrained by intense R&D and certification overheads, making the sector dependent on public/governmental funding.
- **Deployment Modality:** Local SDKs optimized radiation-hardened hardware environments where external cloud connectivity is impossible.

Use Case 7: Online Media

- **Operational Horizon & Primary Asset:** Short 3–5-year technology refresh cycles protecting subscriber databases and Digital Rights Management (DRM) distribution networks.
- **Urgency & Driver: Medium;** driven by routine data-security updates and customer billing privacy.
- **Financial & Premium Profile:** Low willingness to pay, capped at a **0%–5% premium**. Security is viewed as a commodity feature rather than a commercial differentiator.
- **Deployment Modality:** Native Cloud PQC integrations, heavily dependent on upstream platform updates (e.g., operating systems and web browsers).

Use Case 8: Unmanned Aerial Vehicles - UAVs

- **Operational Horizon & Primary Asset:** Short 3–5-year fleet lifecycles protecting real-time aerial data streams, active payload encryption, and logistics links.
- **Urgency & Driver: High;** driven by the active threat of exploitation and interception of sensitive surveillance data during operations.

- **Financial & Premium Profile:** Willingness to pay a **20% premium**. Commercial operators view early quantum resistance as a high-value differentiator for enterprise clients requiring verified data integrity.
- **Deployment Modality:** Cloud-offloaded PQaaS to protect real-time performance while bypassing the weight and power limitations of on-board hardware.

Use Case 9: Transportation

- **Operational Horizon & Primary Asset:** Extended 15–25-year infrastructure horizons protecting cross-border transmission networks and centralized railway traffic control systems.
- **Urgency & Driver: High;** focused heavily on preserving EU Digital Sovereignty and safeguarding public safety against cross-border data manipulation.
- **Financial & Premium Profile:** Willingness to pay a **10%–20% premium**. Similar to the finance vertical, major transportation operators (such as FGC) intend to internalize migration costs entirely to insulate end consumers from increased pricing.
- **Deployment Modality:** Hybrid PQC Gateways designed for centralized lifecycle management across sprawling transit networks.

5.2.6 Competitive Landscape & Positioning Analysis

Developing a sustainable go-to-market model for the PiQASO platform requires evaluating the market forces currently dictating the cryptographic landscape. Initial evidence suggests three primary competitive pillars have identified that each posing distinct challenges to adoption.

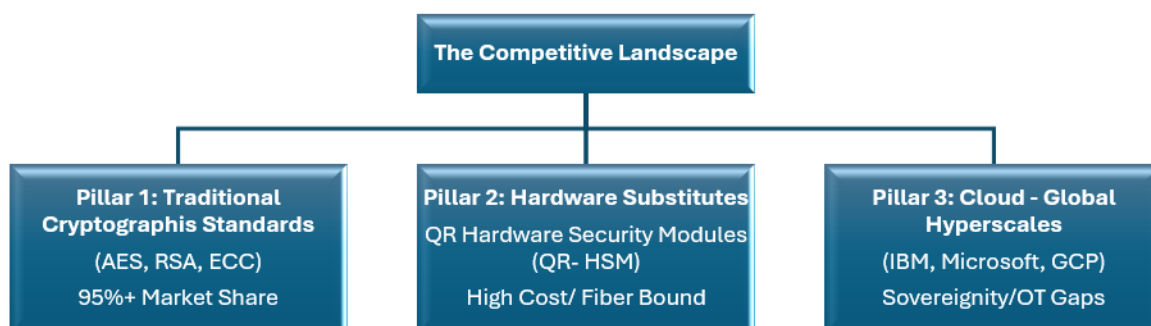


Figure 23 Primary Competitive Pillars

Pillar 1: Traditional Cryptographic Standards (The Status Quo)

Market Dominance: Incumbent classical protocols (including AES-256, RSA-4096, and Elliptic Curve Cryptography (ECC)) currently command over 95% of the global market.

Competitive Inertia: These frameworks are deeply embedded into legacy software stacks, hardware microcontrollers, and communication protocols. While they are completely vulnerable to future quantum decryption via the HNDL paradigm, their established presence creates a strong status-quo bias. Organizations heavily resist replacing them due to the costs and operational risks associated with a cryptographic overhaul.

Pillar 2: Hardware Substitutes (QR Hardware Security Modules (QR- HSM))

The Competitors: Marketed heavily by tier-one security and hardware providers, including Toshiba, IDEMIA, and Thales.

Market Constraints: QR-HSMs provide robust cryptographic agility and vital mathematical protection against future quantum threats, but their commercial adoption is heavily constrained by operational overhead and legacy ecosystem friction. Unlike software-defined cryptography, upgrading to a QR-HSM requires organizations to replace or significantly overhaul expensive, rigid physical server architecture.

Pillar 3: Non-European Cloud Monopolies (The Hyperscalers)

The Competitors: Strategic global technology giants, including IBM, Microsoft, and Google Cloud Platform (GCP).

Market Constraints: These providers are quickly integrating PQC-enabled software stacks into their cloud infrastructure. While they are highly competitive in cloud-native business environments (such as commercial banking), they fail to meet the market needs of sovereign European Operational Technology (OT) environments, localized manufacturing systems, or highly specialized aerospace hardware.

Competitor Matrix and PiQASO Differentiation

The table below outlines how PiQASO differentiates its value proposition across its primary use case categories compared to current standard options and emerging quantum-safe alternatives:

Table 23 Competitors & PiQASO UVP

Sector	Current Primary Competitor	Quantum Safe Alternative	PiQASO UVP
Automotive	Vector Informatik, ETAS, Bosch	N/A (Early Research)	Real-time V2I Latency Control
Automation	Toshiba, IDEMIA	QKD (Limited Scalability)	Multi-robot secure coordination
Finance	IBM, PA, GCP (Cloud)	PQ KEMs & PQ Signatures	Sovereign European Control

Energy	Schneider Electric, Siemens Energy, Phoenix Contact	OpenQKD (Pilots), Hash-sigs	Agility across legacy lifecycles
Healthcare	Cisco, Microsoft Azure, Philips Healthcare	Toshiba / IDEMIA (QKD)	Cloud-based offloading (PQaaS)
Aerospace	Thales Alenia Space	N/A (Primarily Research)	Radiation-hardened PQC SDK
Online Media	Cloudflare	N/A	OptiSecure Personal User Data DRM
UAVs	DJI Enterprise, PX4/Auterion Ecosystem	Vendor-specific secure stacks	Optimized hardware acceleration
Transportation	IDEMIA, Thales	Quantum Key Distribution	Centralized Lifecycle Management

Strategic Positioning Synthesis

PiQASO project by centering its architecture on crypto-agility and flexible software modalities (such as specialized edge SDKs and cloud-offloaded PQCaaS), PiQASO positions itself as a practical alternative for the European market.

This software-defined approach allows early adopting European organizations to successfully deploy quantum resistance across legacy physical hardware and real-time networks without waiting for complete supply chain hardware overhauls

5.3 IPR Tracking Table

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). 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).

5.3.1 What is agreed within the Consortium Agreement

5.3.1.1 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.

5.3.1.2 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.

5.3.1.3 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.

5.3.1.4 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.

5.3.1.5 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.

5.3.2 IPR rules and procedures within PiQASO

5.3.2.1 Development and Project phase

Both the Grant Agreement and the Consortium Agreement outline several rules concerning 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 preexisting 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 IP, whether 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 IP, 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.

5.3.2.2 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.

The initial IPR Management Table has been created for PiQASO Foreground IP has been created and it is presented below:

Table 24 KERs IPR

No	Owners	Result Name
1	UBITECH, QUBI, TAU, UniBwM, BYTE	PQC Ensemble Secure implementation with optimizations and accelerations
2	TAU, UniBwM, UBITECH, QUBI	PQ Data “Security-by-Design” Crypto Abstractions
3	QUBI, UBITECH, TAU, UniBwM,	PQC-as-a-Service Modality
4	RAL, UBITECH, QUBI, UniBwM, TAU	PQ Crypto Assessment & Conformance Toolkit

Also, a separate IPR Management table has been created and stored in PiQASO SharePoint Repository for the Background IP, and it will be completed throughout the project duration (see also *Annex II*)

6 Conclusion

This deliverable has reported on the Communication, Dissemination, and Exploitation activities carried out by the PiQASO consortium during the first 18 months of the project (M1–M18). Under Task 6.1, the project established a visible and increasingly diverse public presence, combining scientific dissemination, participation in workshops, webinars, and conferences, digital liaisons with related projects and synergy networks, and a multi-channel communication strategy built around the project website, social media, press releases, and the PiQASO Academy.

Under Task 6.2, the consortium, led by RAL, completed the onboarding phase into the relevant PQC standardisation bodies and working groups, securing formal entry points into ETSI ISG QSC, the NIST PQC ecosystem, and IETF PQC/TLS activities, and laying the groundwork for active technical contributions in the second half of the project.

Under Task 6.3, the consortium advanced its exploitation methodology through KER identification, stakeholder and market analysis, and the integration of the DEDEP structured exploitation tools, producing the KER characterisation tables, market analysis, and IPR tracking presented in this report.

As detailed in Chapter 2, the KPI monitoring framework shows that the dissemination and communication baseline planned for the first reporting period has been established, with some targets already exceeded, most notably project synergies and events. A number of other metrics, covering website traffic, scientific publication volume, and certain digital liaison and standardisation indicators, remain below their targets; this is consistent with a project at the mid-point of its lifecycle, where the most resource-intensive dissemination, technical contribution, and demonstration activities are concentrated in the second reporting period (M19–M36), once the use case pilots and technical results from WP3–WP5 reach sufficient maturity to support them.

Looking ahead to the second reporting period (M19–M36), WP6 will shift towards more result-oriented activities: increasing the volume and depth of scientific and non-scientific dissemination, translating communication efforts into more targeted messaging around project results and use cases, converting the standardisation groundwork into active technical contributions and submissions, and advancing the exploitation methodology ahead of the final exploitation report due in Deliverable D6.3.

Table 25 Action points for RP2

KPI	Task	Planned activity	Owner	Timing
Phase 1: Awareness Creation				
Project website and branding: > 1000 unique visitors > 200 registrants > 350 blog interactions	T6.1	Continue publishing on the website and social media according to the project's editorial plan	PLURIBUS	Throughout RP2

Audio and Video Material: 1 Promo + 1/Pilot + 1 Impact + 2 to 4 interviews or podcast episodes	T6.1	Produce additional expert interviews (Ubitech, UniBwM, NCIS, Byte, and others), the impact video, and demo videos of the use cases	K3Y	Throughout RP2, impact and demo videos to be delivered by M36.
Social media (FB, LinkedIn): > 500 followers > 400 posts/reposts > 5000 interactions	T6.1	Continue posting on social media; improve the reposting rate and continue increasing interactions	PLURIBUS	Throughout RP2
Phase 2: Continuity of Information Flow				
Press releases (4 per year), blog posts (1000 people reached)	T6.1	Continue press release and blog publication at the same pace as RP1	PLURIBUS / UBITECH	Throughout RP2
Scientific papers, articles, whitepapers: 4 Journal articles, 10 Conference papers	T6.1 - T6.2	Publish 6 additional conference papers and 2 additional journal articles	TAU, UBITECH, UniBwM, QUBITECH	2 new articles by M24.
Interaction with policy makers: > 6 synergies established with policy makers reached via e-mail or physically	T6.1 - T6.3	Participation in events and forums, email communication with policy makers.	UBITECH, RAL	M24 – M36
Digital liaisons with related projects: Workshops organized (3) + attended (>5), > 500 visitors, 10 speakers;	T6.1 - T6.3	Continue organising and attending workshops; organise a workshop on Standardisation in collaboration with ANSSI (already contacted)	UBITECH, RAL	Next planned workshop: November 2026 (M23)
Digital liaisons with related projects: 5 posts in CORDIS/other EC systems;	T6.1	Publish the required posts following finalisation of the 1st review and approval of public deliverables	UBITECH	M26
Non-scientific Publications: > 6 Industrial PQC Cyber Security	T6.2 - T6.3	Continue participating in relevant industrial conferences and exhibitions; hold demonstration	All partners	Throughout RP2

Conferences, 1 exhibition, 1 demonstration days		day(s) aligned with technical progress		
Standardization associations: (EU & International) PQC > 4, Standards Orgs > 3	T6.2	Deliver core technical contributions to the standardisation bodies and working groups already joined	RAL, UBITECH, QUBITEC H	Throughout RP2, focus on M24– M36
Phase 3: Result orientation				
Pilot Demonstrations/ Workshops: > 1 demonstration per pilot > 20 attendees each	T6.3	Conduct pilot demonstrations/workshops in line with technical progress in WP3–WP5	UC partners	M33 – M36
PiQASO Day: > 80-100 participants	T6.1	Organise PiQASO Day	PLURIBUS	M33 – M36

ANNEX I

PiQASO Market Analysis Questionnaire
<https://docs.google.com/forms/d/e/1FAIpQLSdXFSW6rLP1MTRcXj2uVCuFgtadQFt5wU9SdEdTdOuMdCAog/viewform?usp=header>

Questionnaire results: https://docs.google.com/spreadsheets/d/1Fy-mJaxlGeyJ6dJNejwTLSPZTSLCKKvTMvry0XzJ4_E/edit?usp=sharing

PiQASO - Market Analysis Questionnaire for UCs owners

* Indicates required question

Indicate your Organization: *

Your answer

Choose in which Use Case you are End User: *

- ☐ UC1 – Sector: Automotive
- ☐ UC2 – Sector: Automation
- ☐ UC3 – Sector: Finance
- ☐ UC4 – Sector: Energy
- ☐ UC5 – Sector: Healthcare
- ☐ UC6 – Sector: Aerospace
- ☐ UC7 – Sector: Online Media
- ☐ UC8 – Sector: UAVs
- ☐ UC9 - Sector: Transportation

I. Market Characterization & Segmentation

Target Market Size: Within your specific industry, how many potential "Early Adopters" (organization likely to adopt PQC within 1-3 years) do you estimate exist in your national market? *

Your answer

End-User Profiles: Who are the primary decision-makers for cryptographic upgrades in your organization? (e.g., CISO, IT Infrastructure Manager, Compliance Officer). *

Your answer

Application Scope: Beyond the primary project scenario, list at least two other application domains in your sector where PiQASO's Results could be applied. *

Your answer

II. Market Drivers & Specific Needs

Driver Identification: Rate the following drivers by their importance in motivating ^{*}
your sector to transition to PQC:

	Trivial	Minor	Moderate	Major	Extreme
Compliance with EU regulations (e.g., NIS Directive, Cyber Resilience Act)	☐	☐	☐	☐	☐
Protection against "Harvest Now, Decrypt Later" threats	☐	☐	☐	☐	☐
Requirement for secure cross-border communication	☐	☐	☐	☐	☐
Customer/User demand for "Everlasting Data Security"	☐	☐	☐	☐	☐

Unique Value Proposition (UVP): For your specific market, does the benefit of ^{*}
Crypto Agility outweigh the benefit of Performance/Latency?

- ☐ Yes
- ☐ No

III. Barrier & Constraint Analysis

Technical Barriers: Which technical challenge is most likely to slow market uptake in your sector? *

- ☐ Large PQC key sizes impacting storage/bandwidth
- ☐ Latency issues in real-time systems (e.g., V2I or Mechatronics)
- ☐ Lack of specialized hardware on the client-side
- ☐ Other: _____

Economic Barriers: Estimate the maximum "Security Premium" (percentage over current crypto costs) your sector's customers would be willing to pay for certifiable quantum-level security. *

Your answer _____

IV. Competitor & Alternative Assessment

Current Solutions: What traditional (classical) cryptographic solutions are the primary competitors currently using to address long term data security? *

Your answer _____

Market Substitutes: Are you aware of other quantum-safe technologies being considered in your market (e.g., Quantum Key Distribution - QKD) that might compete with or complement PiQASO results? *

Your answer _____

V. Business Models & Commercialization Strategy

Revenue Streams: Based on your sector's procurement behavior, which commercial model is most viable? *

- ☐ Per-Transaction: Paying for each authenticated/encrypted Data Payload
- ☐ Tiered Subscription: Annual fees based on the number of devices/users
- ☐ Freemium: Open-source core with paid custom optimization and support

Supply Chain Integration: To what extent do your suppliers and customers need to participate in the PQC migration for the market to be viable? *

Your answer

VI. ROI & Sustainability

Economic Impact: Beyond preventing breaches, can you identify any operational cost savings (eg., centralized key management via PQaaS) that would improve the Return on Investment (ROI)? *

Your answer

Life Cycle: What is the average hardware lifecycle for devices in your sector? *

Your answer

VII. KER Utility & Value Proposition

PiQASO has identified several Key Exploitable Results (KERs). Please rate the *
potential impact of each on your organization's operation (Low, Medium, High):

	Low	Medium	High
PQC Ensemble Secure implementation with optimizations and accelerations	☐	☐	☐
PQC-as-a-Service Modality (PQaaS): Cloud-based offloading of resource-intensive crypto operations	☐	☐	☐
PQ Crypto Assessment & Conformance Toolkit: Tool for monitoring system posture and vulnerabilities	☐	☐	☐
PQ Data "Security-by- Design" Crypto Abstractions: Policy- based sharing , ABE, and Homomorphic Encryption	☐	☐	☐
PiQASO Academy	☐	☐	☐

ANNEX II

IPR Management Table [\[Link\]](#)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Component	Description	Interacting Component	Interactive Component Description	Expected TRL	Reached TRL	Ownership	Background underlying assets	Other underlying assets	IP condition	License	GitLab Repository	Public availability	Reference task	NOTES / COMMENTS
4															
5															
6															
7															
8															
9															
10															
11															
12															
13															
14															
15															
16															
17															
18															
19															
20															
21															
22															
23															
24															
25															
26															
27															
28															
29															
30															
31															
32															
33															
34															
35															
36															

ANNEX III

Proof 1

29/05/2025, 13:40

Red Alert Labs Mail - Confirmation: You joined the Migration to Post-Quantum Cryptography Community of Interest



Isaac Dangana <isaac.dangana@redalertlabs.com>

Confirmation: You joined the Migration to Post-Quantum Cryptography Community of Interest

NCCoE <nccoe-webmaster@nist.gov>

Tue, May 19, 2026 at 12:24 PM

Reply-To: NCCoE <nccoe-webmaster@nist.gov>
To: isaac.dangana@redalertlabs.com

Thanks for joining our Migration to Post-Quantum Cryptography community of interest.

We look forward to engaging with you. As a member of this community, you will receive news about upcoming events, publications, and opportunities to contribute.

You may also reach out to us with questions or comments at
applied-crypto-pqc@nist.gov



<https://mail.google.com/mail/u/0/?ik=518a290335&view=pt&search=all&permmsgid=msg-f:1865612048720234520&siml=msg-f:1865612048720...> 1/1

Proof 2



Isaac Dangana <isaac.dangana@redalertlabs.com>

Your REGISTRATION to CYBERQSC#44 (Sophia-Antipolis - FRANCE)

meetings@etsi.org <meetings@etsi.org>
To: isaac.dangana@redalertlabs.com

Fri, May 8, 2026 at 12:29 PM

Dear Mr. Isaac Dangana,

Thank you for your registration.

You have registered for the following meeting: [CYBERQSC#44](#)

Registration summary:

Meeting contacts:

[Kim Nordström](#)

[Cassandra Ranchin](#)

Presence type allowed: Face to face and Online

Your registered presence type: Online

Location and time: Sophia-Antipolis - FRANCE, from: **2026-07-07 09:00 to 2026-07-07 17:30**, time zone:
(GMT+02.00) Brussels, Copenhagen, Madrid, Paris.

If you wish to update or cancel your registration for this meeting, click on the following link: [Update my Registration](#).

[Add this meeting/event to your calendar.](#)

Please note that this physical meeting in ETSI may be subject to cancellation or change into a virtual meeting should the covid-19 situation require so.

You would be informed by us nearer the time and with sufficient notice.

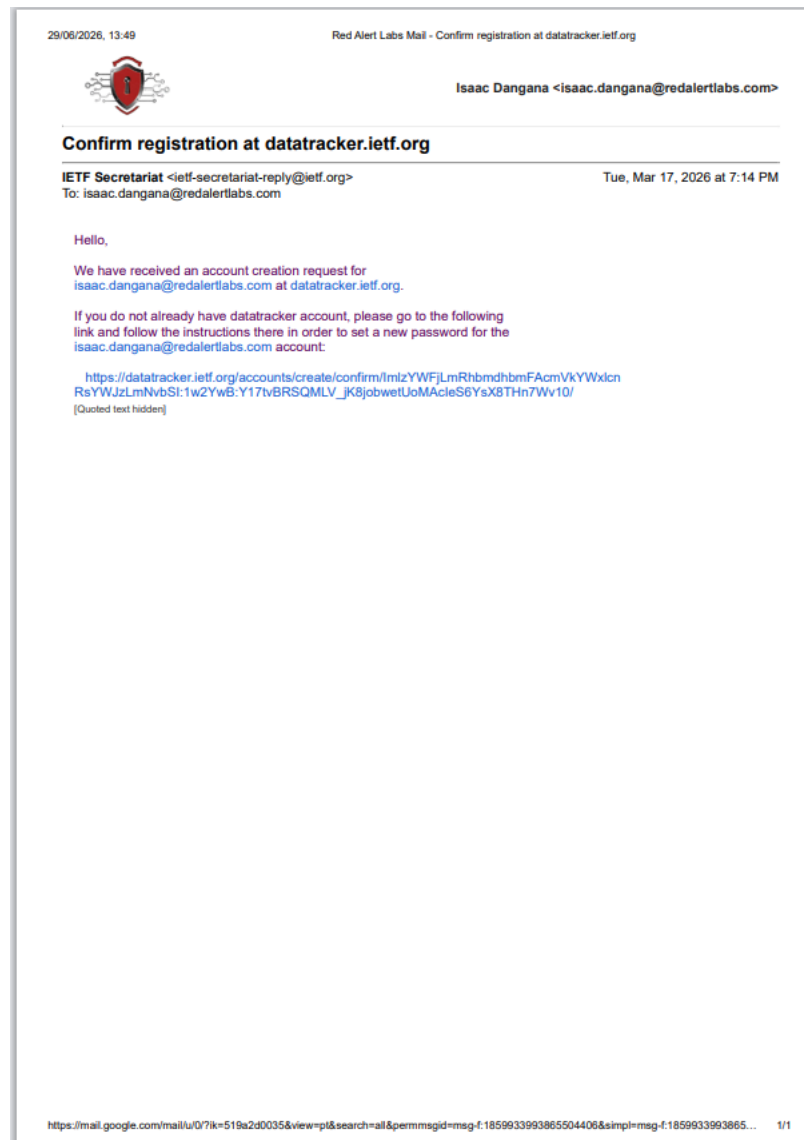
Please note that, in accordance with GDPR Regulation n°2016/679 and in compliance with the [ETSI Privacy policy](#), your personal data are collected and stored in order to register for and participate in this meeting/event and for the minutes, if applicable. This personal data processing is based on ETSI's legitimate interest. If you have any question about your personal data or should you want to exercise your rights of access, rectification and/or erasure, please send an e-mail to privacy@etsi.org

If you receive this confirmation of registration after the meeting has taken place, it is simply a confirmation that you attended. Should this not be the case, kindly inform [ETSI Meeting Support](#) so that we can correct our data.

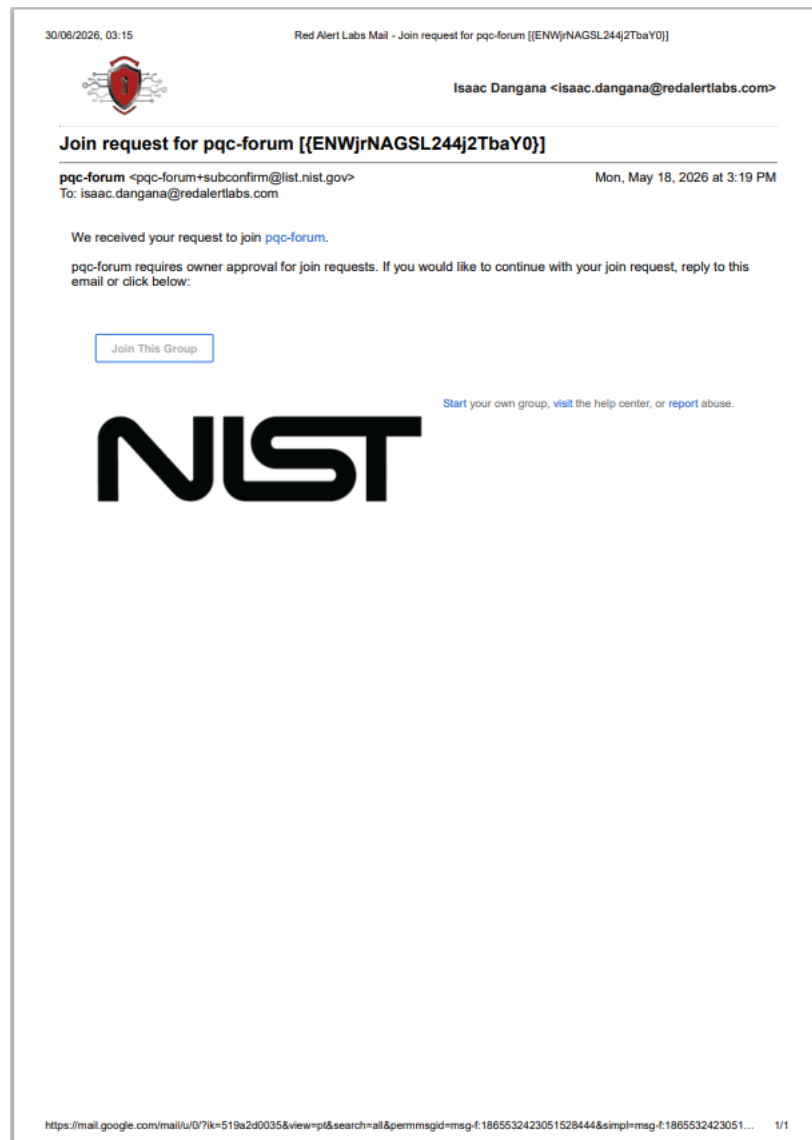
We wish you a fruitful meeting!

Your ETSI Meeting Support Team

Proof 3



Proof 4



Proof 5

30/06/2026, 04:51

Red Alert Labs Mail - IETF 126 Registration Confirmation: 44ELLPFR



Isaac Dangana <isaac.dangana@redalertlabs.com>

IETF 126 Registration Confirmation: 44ELLPFR

no-reply@ietf.org <no-reply@ietf.org>
To: isaac.dangana@redalertlabs.com

Tue, Jun 30, 2026 at 4:43 AM



Thank you for registering for **IETF 126 Vienna**! Below is a summary of your registration details and helpful next steps.

Registration Details

Participant: Mr. Isaac DANGANA
Registration Type: Remote - One Day Pass
Confirmation Number: 44ELLPFR

Your Self-Service Dashboard

Your self-service dashboard allows you to:

- Request and view a Letter of Invitation
- Sign up for additional events
- Edit your registration details

Access your dashboard here:

<https://registration.ietf.org/participant-dashboard/>

Benefits of the One Day Pass

1. Attend all sessions during any day of the Meeting.
2. Pass can be upgraded to a full Meeting Registration, however, late fee may apply if initial Pass payment is not made before the Early Bird deadline.
3. Attend Sunday Tutorials at no additional charge.
4. Attend Sunday Welcome Reception at no additional charge.
5. Attend Technical and Administrative Plenary at no additional charge.

IMPORTANT NOTE: Your badge will be available for pick up at the On-site Registration Desk. Your badge will not be available in the Pre-paid registration lines because it must be stamped with the day you will be attending.

Meeting Information

For information on meeting agenda, hackathon, mobile apps, newcomer-specific programs and other useful links, please see our [IETF 126 Online meeting page](#).

Your Selected Options

- **How many IETF meetings have you attended?:** This is my first
- **Please add me to the new participant mail list:** Yes
- **I would like to subscribe to the attendees mailing list:** Yes

If you need to make updates or have questions about your registration, please contact support@ietf.org.

For more information about the meeting, see:
<https://www.ietf.org/meeting/126/>

We look forward to seeing you at IETF 126!

<https://mail.google.com/mail/u/0/?ik=519a2d0035&view=pt&search=all&permmsgid=msg-f:1869388104315792283&simpl=msg-f:1869388104315...> 1/2

Keep in touch



PiQASO [LinkedIn](#)



PiQASO [Youtube](#)



[ECCC Newsletter](#)



[ECCC LinkedIn](#)



[ECCC Twitter/X](#)



[ECCC Website](#)