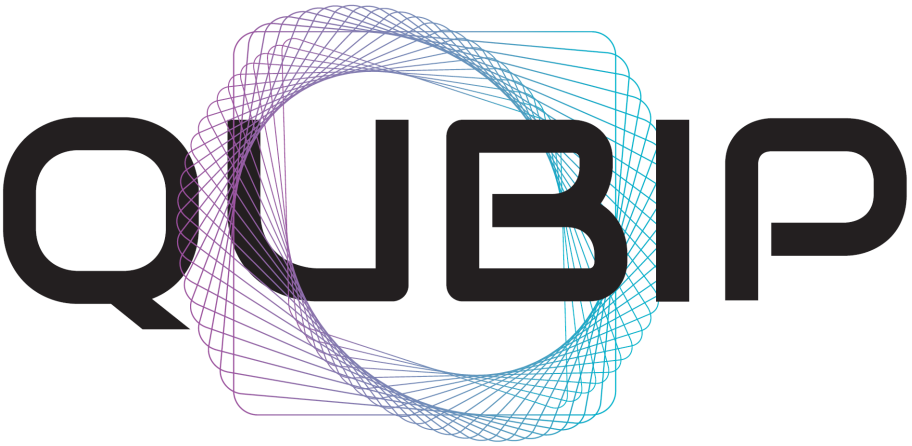
Horizon Europe



QUANTUM-ORIENTED UPDATE TO BROWSERS AND INFRASTRUCTURES FOR THE PQ TRANSITION (QUBIP)

Dissemination, exploitation and communication plan and activities (intermediate version)

Deliverable number: D4.2

Version 1.0

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

Project Acronym:	QUBIP
Project Full Title:	Quantum-oriented Update to Browsers and Infrastructures for the PQ transition
Call:	HORIZON-CL3-2022-CS-01
Topic:	HORIZON-CL3-2022-CS-01-03
Type of Action:	HORIZON-IA
Grant Number:	101119746
Project URL:	https://www.qubip.eu
Start date:	1 September 2023
Duration:	36 months

Editors:	Antonio Lioy – POLITO
Deliverable nature:	Report (R)
Dissemination level:	Public (PU)
Contractual Delivery Date:	28 February 2025
Actual Delivery Date	04 March 2025
Number of pages:	30
Keywords:	Communication, Dissemination, Exploitation, Key Exploitable Results (KERs), Intellectual Property Right (IPR)
Contributors:	Andrea Vesco – LINKS Grazia D'Onghia – POLITO Davide Bellizia – TELSY Agostino Sette – TELSY Maria Chiara Molteni – SECPAT Eros Camacho – CSIC Andrés Ruiz – CSIC Izan Franco – CSIC Marc Almeida – CSIC Antonio Pastor – TID Diego Lopez – TID Javier Faba – UPM Juan P. Brito – UPM Nicola Tuveri – TAU Akif Mehmood – TAU Dmitry Belyavskiy – REDHAT Enrico Bisio – SMART Andrés del Álamo – CIB
Peer review:	Davide Bellizia – TELSY Enrico Bisio – SMART
Approved by:	ALL partners

Table 1: Document revision history.

Issue Date	Version	Comments
27/01/2025	0.1	Initial table of contents
28/02/2025	0.2	First draft version for internal review
04/03/2025	1.0	Final version for submission

Abstract

This document represents the Deliverable D4.2 of the Quantum-oriented Update to Browsers and Infrastructures for the Post-quantum transition (QUBIP) project. It contains the intermediate version at month 18 of the dissemination, communication, and exploitation plans for QUBIP. This is a “live” document that will be periodically updated during the project, not only to reflect new plans but also to report the performed activities.

Contents

List of Figures

List of Tables

List of Acronyms

ACM	Association for Computing Machinery
API	Application Programming Interface
AXI	Advanced eXtensible Interface
B2B	Business-to-Business
B2B2C	Business-to-Business-to-Customer
B2C	Business-to-Customer
CA	Consortium Agreement
CCIPS	Centrally Controlled IPSec
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
DLT	Distributed Ledger Technology
EC	European Commission
ECDSA	Elliptic Curve Digital Signature Algorithm
ETSI	European Telecommunications Standards Institute
EU	European Union
FPGA	Field Programmable Gate Array
fTPM	firmware TPM
GA	Grant Agreement
HW	Hardware
IACR	International Association for Cryptologic Research
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIAB	Industrial and Institutional Advisory Board
IKE	Internet Key Exchange
INATBA	International Association for Trusted Blockchain Applications
IoT	Internet of Things
IP	Intellectual Property
IPR	Intellectual Property Right
IPsec	IP Security
ISO	International Organization for Standardization
JWP	JSON Web Proof
KEM	Key Encapsulation Method
KER	Key Exploitable Result
KoM	Kick-off-Meeting
KPI	Key Performance Indicator
MCU	Micro-Controller Unit
MPU	Micro-Processor Unit
NFV	Network Functions Virtualization
NIST	National Institute of Standards and Technology
NSS	Network Security Services
OP-TEE	Open Portable Trusted Execution Environment
OS	Operating System
OSH	Open-Source Hardware
OSM	Open Source MANO

OSS	Open-Source Software
PL	Programmable Logic
PQ/T	Post-Quantum/Traditional
PQ	Post-Quantum
PQC	Post-Quantum Cryptography
PQ-REACT	Post Quantum Cryptography Framework for Energy Aware Contexts
PS	Processing System
QKD	Quantum Key Distribution
QSNS	Workshop on Quantum Secure Networks and Services
QUBIP	Quantum-oriented Update to Browsers and Infrastructures for the Post-quantum transition
SAB	Security Advisory Board
SCP	Secure Channel Protocol
SDN	Software-Defined Networking
SE	Secure Element
SIG	Special Interest Group
SoC	System-on-Chip
SOTA	State of the Art
SPQR	Secure Post Quantum eRa
SSI	Self-Sovereign Identity
SW	Software
TA	Trusted Application
TFS	TeraFlow SDN
TLS	Transport Layer Security
ToIP	Trust over IP
TPM	Trusted Platform Module
UVP	Unique Value Proposition
VC	Verifiable Credential
VDR	Verifiable Data Registry
W3C	World Wide Web Consortium
WG	Working Group
WWW	World Wide Web
ZK	Zero-Knowledge

1. Introduction

This document contains the intermediate version of the dissemination, communication, and exploitation plan for the QUBIP project. It represents the deliverable D4.2 “Dissemination, exploitation and communication plan and activities (intermediate version)” issued at M18 (i.e., February 2025).

Its scope is to update the plan for these activities and to monitor the actions carried out in the initial period, in accordance with the Grant Agreement (GA) and the Consortium Agreement (CA). As such, it is a “living” document that will be further updated at M36 (i.e., August 2026), not only to reflect new plans, but also to report on the activities performed at the end of the QUBIP project.

The document has been prepared jointly by all partners.

1.1. Target groups and key message to deliver

The QUBIP project has its own target groups and intends to define the dissemination, exploitation and communication plan with their interests clearly in mind. Table 1.1 presents the target groups, their interest to the best of our knowledge, and the key message we want to deliver to attract their interest in the project activities and results, considering also the identified KERs.

Table 1.1: List of the target groups and key messages to deliver.

Industries		
Hardware (HW) design and manufacture, Internet of Things (IoT) device manufacture, Network devices manufacture, Telco operators, Digital Identity.	**Interest**: New technology and knowledge transfer partners to build new products and services.	**Key message**: QUBIP is developing Post-Quantum (PQ) assets and new know-how on transition to Post-Quantum Cryptography (PQC) of HW, crypto libraries, Operating System (OS), communication protocols and applications. From their adoption, industry players in European Union (EU) can gain a competitive advantage on the market.
Solution Providers & Integrators		
PQ Solution Developers & Intellectual Property (IP) Providers, Integrators & Cybersecurity Companies.	**Interest**: Standalone, vertical solutions for specific security issues ready and easy to be integrated into digital infrastructures.	**Key message**: QUBIP is developing and validating new PQ building blocks that are reusable and solve specific security issues of the PQ era, giving pre-competitive advantages to the early adopters.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

Scientific Communities		
Institute of Electrical and Electronics Engineers (IEEE) Computer and Communication societies, Association for Computing Machinery (ACM) Special Interest Group (SIG) on Algorithms & Computation Theory, ACM SIG on Embedded Systems, Internet Society, International Association for Cryptologic Research (IACR).	**Interest**: Scientific PQC-related results and advances beyond state-of-the-art.	**Key message**: QUBIP is addressing the fundamental research questions and producing development efforts to make quantum-security a reality.
R&D Initiatives		
Open-HW communities, Crypto Libraries communities, Network protocol communities, OS Linux communities, Self-Sovereign Identity (SSI) & Distributed Ledger Technology (DLT) communities.	**Interest**: Developing Open-Source Software (OSS) and technical specifications with a shared purpose.	**Key message**: QUBIP is developing open-source assets for the purpose of counteracting future quantum threats and we are eager to share our experience.
Standardization Bodies & Working Groups		
Internet Engineering Task Force (IETF), International Organization for Standardization (ISO), European Telecommunications Standards Institute (ETSI), European Committee for Standardization (CEN)/European Committee for Electrotechnical Standardization (CENELEC), World Wide Web Consortium (W3C), Trust over IP (ToIP), International Association for Trusted Blockchain Applications (INATBA), StandICT.eu.	**Interest**: "Rough consensus and running code" and documented assets for steering the standardization of the foundations of PQ economy.	**Key message**: QUBIP is developing HW and Software (SW) PQ assets (KER1 to KER9), and replicable transition process to PQC for digital systems and infrastructures (KER10).
Policy Makers & Regulators		
Policy Makers, Regulatory Agencies & Certification Bodies (at local, regional, national, European level).	**Interest**: Defining the fundamentals and the parameters within which policy-making, delegated to regulators, can regulate data management and cybersecurity.	**Key message**: Addressing technology changes in a timely manner is hard; QUBIP is working to defragment the regulatory framework in the specific field of data and cybersecurity for the PQ era.
End Users		
EU Citizens.	**Interest**: Easy to use applications and tools for their digital life.	**Key message**: Quantum computing open the future to new exciting applications, but it may also threaten your security on-line, but "there is an app for that": QUBIP is making Firefox and other components secure also for PQ era.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

2. Communication

QUBIP proposes a variety of communication activities to ensure a wide spreading of the project's activities, ideas and results, with the aim of raising awareness among the scientific, technical and general interest communities.

All partners in the QUBIP consortium will regularly feed the different communication initiatives and channels with content and contribute to the preparation of communication materials to be used during the planned activities and events.

The QUBIP **website** – https://qubip.eu/ – is the central tool for communicating the project brand, concept, activities, and results. The home page (shown in Figure 2.1) contains not only the project logo (whose design is shown in Appendix A), but also the QUBIP emotional image (shown in Figure 2.2) to communicate the QUBIP concept more successfully than through words. This was done to leave a positive first impression on web visitors, and potentially having a strong impact on the engagement too.

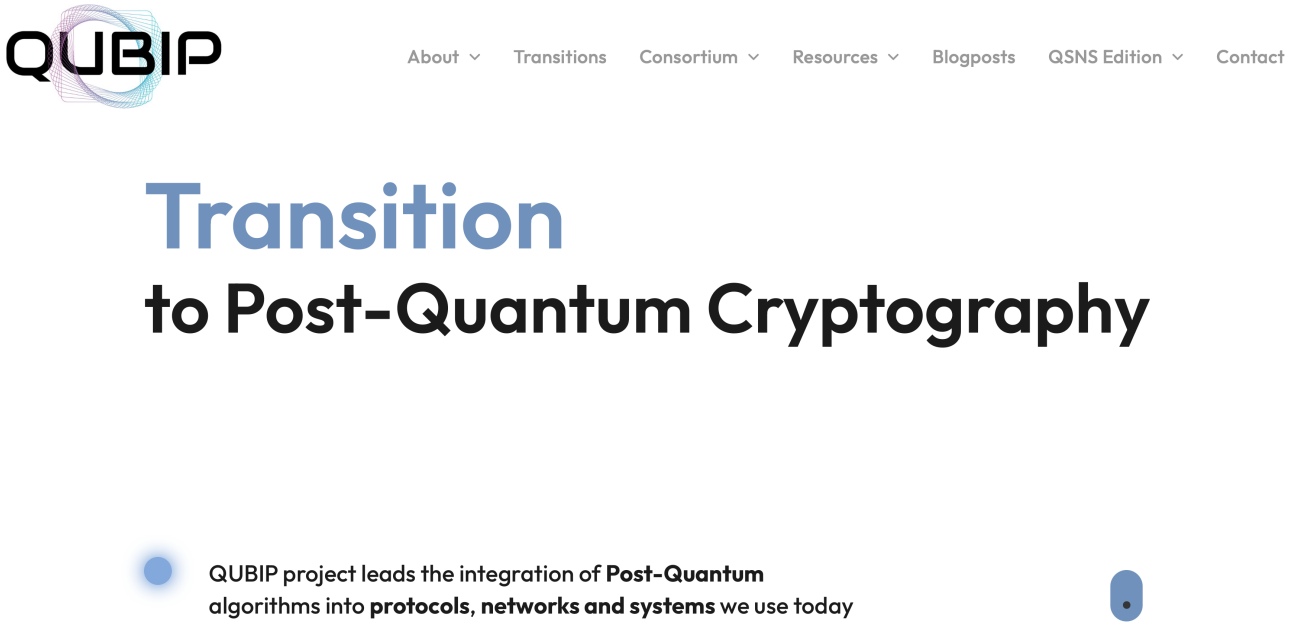


Figure 2.1: QUBIP website home page.

The QUBIP website contains the *About* section with the detailed description of the project concept, the 10 strategic objectives, and the scientific methodology underpinning the project activities to achieve these objectives.

The *Transition* section provides a clear graphical and textual description of the 3 core transitions to PQC exercises that QUBIP will perform (i.e., transition of an IoT-based Digital Manufacturing System, of Internet Browsing, and of Software Network Environment for Telco Operators). The word Transition has been carefully chosen to convey the right message: QUBIP is about the transition to PQC of systems we use today. The three images representing the use cases will be used throughout the communication activities for consistency.

The *Consortium* section provides information about the partners with their expertise, their role in the project and the contact details of each partner to make it easier for external contacts to get in touch with us.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

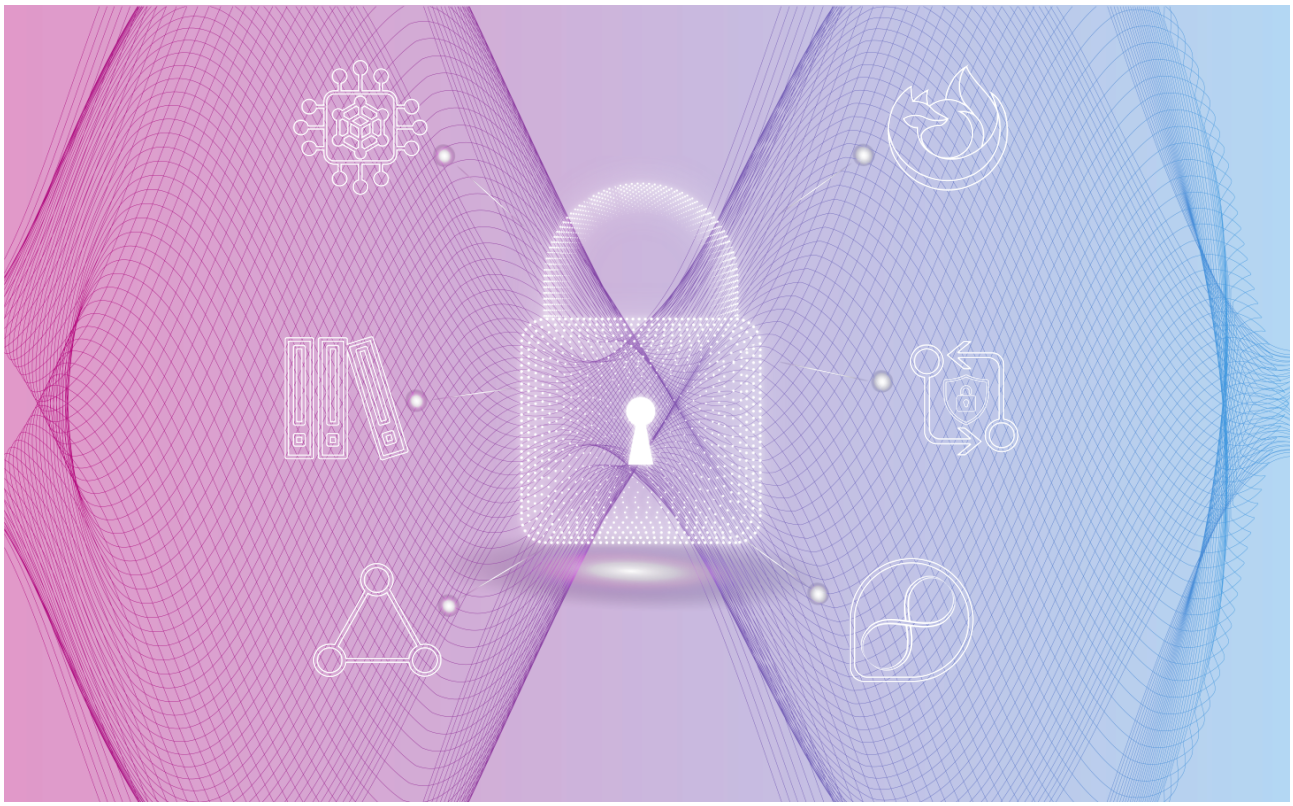


Figure 2.2: QUBIP emotional image.

The *Consortium* section also displays the logos of the distinguished Industrial and Institutional Advisory Board (IIAB) and Security Advisory Board (SAB) members to further enhance the attractiveness of the QUBIP project.

The *Resources* section is dedicated to the publication of all project results. It provides the link to the official QUBIP GitHub repository [1] that contains the developed open-source code, to deliverables, to scientific publications, and to communication materials.

The *QSNS Edition* section links to the websites of the **International Workshop on Quantum Secure Networks and Services (QSNS) editions**. It is the scientific flagship event organised by the QUBIP project in collaboration with the Post Quantum Cryptography Framework for Energy Aware Contexts (PQ-REACT) project within the framework of the Secure Post Quantum eRa (SPQR) cluster.

The *Contact* section provides an easy-to-use form for the external parties to contact the project coordinator.

Special attention should be paid to the *Blogposts* section. QUBIP has adopted the **post** and **vlog** formats as important tools to spread technical content on a monthly basis and to keep the interested stakeholders up to date with project insights, directions and results. The posts are technical in nature and provide useful content to the target audiences with the aim of widening the base of interested people and potential exploitation prospects. All partners agreed to provide contents for the posts. Insofar, the following ones have been published (and much more are planned, roughly with a 1-month periodicity):

- **QUBIP is all about Transition to PQC** – 21/09/2023, A. Vesco (LINKS).
- **Quantum Computers' Role in Shor's Algorithm** – 17/10/2023, A. J. Di Scala (POLITO).
- **New Problems Become Post-Quantum Solutions** – 06/11/2023, A. Pino (LINKS).
- **Current Realizability of Shor's Algorithm** – 04/12/2023, M. Russo (POLITO).

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

- **PQC Implementation on IoT: Challenges and Solutions** – 08/01/2024, E. Camacho Ruiz (CSIC).
- **Integration of PQC in TLS Protocol for IoT Devices** – 01/02/2024, M.C. Molteni, L. Nava, A. Gringiani, G. Greco (SECPAT).
- **Transition of MCU & MPU-based embedded devices to PQC** – 04/03/24, D. Bellizia (TELSY).
- **Transition of OpenSSL for implementing PQ/T TLS** – 02/05/24, A. Shaindlin, A. Mehmood, D. Luoma, N. Tuveri (TAU).
- **SPQR Cluster** – 30/05/24, A. Vesco (LINKS).
- **Fedora Linux Transition** – 14/06/24, D. Belyavskiy (REDHAT).
- **NSS and Firefox Transition to PQC** – 16/07/24, D. Luoma, N. Tuveri (TAU).
- **Post-Quantum Verifiable Credentials** – 12/09/24, C. Sanna (POLITO).
- **IPSec and the impact of the Quantum Era** – 04/11/24, A. Pastor (TID).
- **Hybridization for Quantum-Secure IPsec** – 03/12/24, J. Faba (UPM).
- **Integrity Verification** – 16/01/25, G. D'Onghia, A. Lioy (POLITO).

The vlog format has recently been added to generate value for the community from the internal presentations prepared by the QUBIP Innovation Manager, M.C. Molteni (SECPAT), to drive the research activities. The content of these internal presentations is recorded and published in regular episodes of "**The Innovation Management Corner: PQC news**" Youtube show [2]; **7 episodes have been published so far** and more are planned.

This is where the **social channels** come in. QUBIP has its own social media accounts to share the content of the blogposts and related videos:

- LinkedIn @qubip.eu [3];
- Twitter/X @qubip_eu [4];
- Youtube @qubip_eu [5].

The LinkedIn channel, where QUBIP has the largest number of interested followers, is also used to promote general PQC-related news and events organised by the project, using technical but accessible language to reach a wider audience. The LinkedIn account is also used to follow other relevant initiatives, with the aim of creating opportunities for QUBIP visibility and networking.

The **promotional material** will be designed and developed on demand before each relevant event organised by the project or attended by the project partners. In any case, all materials will also be available on the QUBIP website.

QUBIP has already issued and will continue to issue **press releases** when appropriate. A press release is an official statement issued to members of the main news media for the purpose of providing information, making an official statement or making an announcement intended for public release.

It is worth highlighting the success of the press release issued at the Kick-off-Meeting (KoM). The event was covered by:

- **RaiNews, the Radiotelevisione Italiana S.p.A. (RAI) news website**.
- **RAI Regional news 2 times on TV**.
- **Italian national newspapers: Corriere della Sera, La Repubblica, Il Messaggero**.

All partners of the project are committed to multiplying the impact of communication activities through their own channels, tools and networks. They will support the visibility of QUBIP through their social networks (i.e., LinkedIn and Twitter/X) by reposting the content produced (e.g., posts, announcements, news and events) and by posting their own QUBIP-related content. In addition, the individual researchers involved in QUBIP are encouraged to use their own social accounts to promote the communication content and to reach a wider audience.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

A group of partners will publish communication content on their institutional website, of the institution itself and/or of the specific research groups involved in the project, LINKS (https://www.linksfoundation.com), POLITO (https://www.polito.it), CSIC (https://www.csic.es/es), and UPM (http://www.ccs.upm.es). The three large industries involved in QUBIP will produce relevant posts on their own blogs, TELSY (https://www.telsy.com/blog/), TID (https://blogthinkbig.com/), and REDHAT (https://www.redhat.com/), reaching a large number of technical experts and relevant technical and scientific communities. Finally, it is worth mentioning the CIB's communication activities (https://www.cibervoluntarios.org/en/news) aimed at its network of 30,000 people (volunteers) who will also be involved in QUBIP as end-users of the Quantum-Secure Internet Browsing demonstrator.

Some **Posts** have been published on their websites:

- **QUBIP and the transition to post-quantum cryptography** [6] – 01/02/24, (REDHAT).
- **El proyecto europeo QUBIP está desarrollando una herramienta que emplea la computación cuántica para mejorar la seguridad digital** [7] – 15/04/24, (CIB).
- **IOTA Identity Integrates Zero Knowledge Credentials: In Partnership with the LINKS Foundation** [8] – 29/05/24, (LINKS & IOTA Foundation).
- **GiCP's posts on quantum communications and quantum preparedness** [9] – (GiCP-CSIC).

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

3. Scientific and industrial dissemination

The general Scientific and Industrial dissemination strategy of QUBIP is to present results at conferences, workshops, panels, Working Group (WG) meetings, industrial forums, and other events on a European and International scale, aiming both at public and private sectors. This will be supported by publications in international scientific journals (targeting an expert audience) and in scientific magazines (aimed to a broader audience). Additionally, QUBIP partners will present the project's concepts and results in webinars, tutorials, training events, and seminar with end users, possibly by establishing also liaison with other initiatives.

Thirteen scientific papers have been published, or accepted for publication, since the beginning of the projects: they are listed in the corresponding page of the QUBIP web site, https://qubip.eu/scientific-publications/. They include 3 journal papers, and 10 conference papers.

Two workshops have been organized by QUBIP partners during the first period of the project:

- **Side-Channel Analysis and Attacks** – 14/03/24, D. Bellizia (TELSY).
- **XVIII Jornadas STIC CCN-CERT: VI Jornadas de Ciberdefensa ESPDEF-CERT 2024** – 27-28/11/24, E. Camacho (CSIC).

Notably, QUBIP is the **initiator of a new workshop**, the Workshop on Quantum Secure Networks and Services (QSNS). Its first edition was co-located with the 29th IEEE Symposium on Computers and Communications, June 26-29, 2024, in Paris (France), while the second edition will be co-located with the 30th IEEE Symposium on Computers and Communications, July 2-5, 2025, in Bologna (Italy). The first edition had 12 papers submitted and 5 accepted. The program included also a very interesting keynote "State of the Post-Quantum Internet" by Bas Westerbaan of Cloudflare. Both editions have been co-organized with the PQ-REACT project, https://pqreact.eu/. This is the first tangible result of the cooperation established with this project, as part of **the SPQR cluster** (logo in Figure 3.1) initiated by QUBIP, but other joint initiatives are being planned.

Figure 3.1: Logo of the SPQR cluster.

Technical results of the project has been also presented in **Webinars**. Insofar, the following ones have been delivered:

- **Futuro della cybersecurity nell'era dei super computer** (Italian version for engineering students of Politecnico di Torino) – 31/01/23, A. Vesco (LINKS).
- **Quantum computing threat and Post Quantum Crypto**, four editions:
  1. 15/02/24 G. Bertoni (SECPAT),
  2. 12/03/24 M.C. Molteni (SECPAT),
  3. 25/03/24 M.C. Molteni (SECPAT),
  4. 12/03/24 M.C. Molteni (SECPAT).

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

- **EUROPOL event: Impact of Quantum on European Law Enforcement Authorities Industry and Policy Makers** – 27/11/24, A. Vesco (LINKS).
- **W3C Credential Community Group: Post-Quantum Cryptography in VC: PQ and PQ/T hybrid approaches** – 21/01/25, A. Vesco (LINKS).

It is worth noting that the QUBIP project has been invited by the European Commission (EC) to support the **PQC Workstream Group**, composed of national cybersecurity agencies and ENISA, to prepare the European roadmap for the transition to PQC. QUBIP will continue to support the group's activities upon request.

Finally, QUBIP believes in **liaising with other projects** in order to share information, practices and results. During its first 18 months, QUBIP has established links with the SPIRS (https://www.spirs-project.eu), ALLEGRO (https://www.allegro-he.eu), CHESS (https://chess-eu.cs.ut.ee), and TRUSTCHAIN (https://trustchain.ngi.eu) projects and, of course, with the PQ-REACT (https://pqreact.eu/) project and hopefully with the next projects funded by the EC on PQC topic.

The partners have planned the following scientific and industrial dissemination activities to support the QUBIP plan in the next half of the project.

LINKS will contribute to the scientific dissemination through peer-reviewed papers in relevant conferences. LINKS (if involved by academic partners) will contribute to training events on transition to PQC topics. In addition, LINKS will disseminate key results in workshops, seminars with end-users (e.g., those involved by CIB in the pilot demonstrator on Quantum-secure Internet Browsing) and at industrial events. LINKS will also participate in meetings with key industries (selected and involved by PONSIP in the context of T4.3) interested in the transition to PQC to create exploitation opportunities for the whole consortium. LINKS will also disseminate the results in PQC industry-led working groups (e.g., Identity WG led by the IOTA Foundation). Finally, LINKS will contribute to the liaison with other EU-funded projects.

POLITO will lead the scientific dissemination of the project. This will involve:

- suggest publication opportunities at conferences and journals,
- identify suitable venues for workshops,
- monitor scientific and industrial Key Performance Indicators (KPIs) and take corrective actions, if needed.

Additionally, the POLITO researchers will publish their results in the identified venues and will participate to common project activities (workshops, training, etc.).

TELSY plans to promote the findings of the QUBIP project by means of spreading the quantum-secure approach at industrial events as well as contributing to scientific dissemination by means of peer-reviewed publications in relevant conferences and journals.

SECPAT has been invited to participate to a webinar organized by Future Electronics (a distributor of electronic and electro-mechanical components), where it presented "Advantage of using FPGA in Cybersecurity equipment", focusing on quantum computing threats and post-quantum cryptographic algorithms; the audience was mainly composed of people from industries. It has also been invited for the future editions of the webinar. SECPAT will continue to record the *Innovation management corner* videos, to share the news collected during the project. SECPAT plans to continue its contribution participating to events and workshops.

CSIC will share QUBIP's results through peer-reviewed publications in relevant conferences and journals. It regularly participates in industrial exhibitions and conferences, presenting the latest project findings. To further enhance visibility, CSIC is developing a webpage highlighting advancements in Quantum Key Distribution (QKD) systems, promoting public understanding of quantum communication. Additionally, open source code publications will be made available in QUBIP's GitHub repository [1]. Dissemination efforts will also include outreach activities such as seminars and demonstrations.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

TID will focus on promoting project activities and achievements by actively participating in various telecommunications and networking industry events, as well as through demonstrations. Additionally, it will attend standardization-related events to raise industry awareness of the QUBIP solution. In the scientific domain, TID will foster collaborations with academic counterparts to support impactful publications in the telecommunications domain pertaining to quantum-safe approaches. Furthermore, TID will explore avenues to enhance QUBIP visibility through participation in open-source initiatives and events, such as Open Source MANO (OSM) [10] and TeraFlow SDN (TFS) [11]. Moreover, TID will contribute to improve the suitability and quality of the measures to maximize expected outcomes and impacts of the dissemination, including communication activities. In that sense, TID will perform an analysis throughout patent intelligence, to reach relevant industrial representatives.

UPM will contribute to the scientific dissemination with the publication of the results of the QUBIP project through peer-reviewed papers in relevant journals. Other scientific dissemination activities include organization of conference presentations and workshops as well as demonstrations.

TAU will contribute to the scientific dissemination through peer-reviewed papers in relevant conferences and journals.

REDHAT is going to contribute with conference presentations related to various technology aspects of PQ transition.

SMART will focus on the promotion of the project activities among the manufacturers of industrial automation hardware with whom it is currently collaborating.

CIB will incorporate QUBIP to their specific awareness cybersecurity campaigns. This campaign will also take form in face-to-face format within the context of the QUBIP pilots, when involving the end user in the testing of the QUBIP solution.

The list of venues identified for dissemination in the year 2025 is presented in Table 3.1.

Table 3.1: Some possible dissemination opportunities for the year 2025.

Event	Location and date	Opportunity
IEEE International Conference on Quantum Communications, Networking, and Computing	Nara (JP) 31/3-2/4/2025	papers, posters
IACR Post-Quantum Cryptography	Taiwan (TW) 8-10/4/2025	papers
International Symposium on Applied Reconfigurable Computing	Sevilla (ES) 9-11/4/2025	papers workshops
ETSI/IQC Quantum Safe Cryptography Conference	Madrid (ES) 3-5/6/2025	papers, posters
ACM Workshop on Secure and Trustworthy Cyber-Physical Systems	Pittsburg (PA, US) 6/6/2025	papers
IEEE Symposium on Computers and Communications	Bologna (IT) 2-6/7/2025	papers, tutorials, workshops
IEEE European Symposium on Security and Privacy	Venice (IT) 30/6-4/7/2025	papers
International Conference on Availability, Reliability and Security	Ghent (BE) 11-14/8/2025	papers, workshops
European Symposium on Research in Computer Security	Toulouse (FR) 22-26/9/2025	papers, workshops
Conference on Cryptographic Hardware and Embedded Systems	Kuala Lumpur (MY) 14-18/9/2025	papers
IEEE Mediterranean Electrotechnical Conference	Cairo (EG) 2-4/2/2026	papers, tutorials, workshops

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

4. Dissemination and Communication KPIs and Targets

Table 4.1 lists the KPIs for the project's dissemination and communication activities, as defined in the GA, along with the values achieved at M18 (February 2025).

Table 4.1: Dissemination and communication planned activities with KPIs and targets.

Activity	KPIs and Targets	Values at M18
Web and Social Networks		
Website	total = 1, total visitors $\geq$ 1000	1 website, avg no. of unique visitors = 501 per month, total visitors = 9813, + GitHub and Zenodo official repos
LinkedIn, Twitter, YouTube	total followers $\geq$ 500	total followers = 319
Media		
Blogposts and news	total = 20, total views $\geq$ 1000	18 blogposts, total impressions = 7343, avg engagement rate = 6.4%, avg no. of views = 34 per blogpost, total views = 496
Video	total = 10, total views $\geq$ 1000	total = 12, total views = 277
Press releases	total $\geq$ 6	total = 1
Press coverage	total covered = 1	total covered = 1
Events		
Webinars	total = 10, participants per webinar $\geq$ 100	7 webinars, avg participants per webinar = 41, total views = 285, recording available on-line
Workshops	total = 3, participants per workshop $\geq$ 20	3 workshops, avg participants per workshop = 28, one workshop with 8400 participants
Workshops with IIAB	total = 3	total = 1
WGs	total participation = 3	total participation = 1
In-person (congresses, conferences, tutorials, panels, keynotes)	total = 30	total = 8
Industrial fairs and forums	total = 3	total = 1
Training	total = 8	0
Seminars with end users	total = 6	total = 1
Liaisons		
Liaison with other initiatives	total = 6	total = 6
Cluster	total = 1	total = 1 (SPQR cluster)
Scientific Publications		
Journals, proceedings, magazines, books (chapters)	total = 30	total = 13 (journals = 3, proceedings = 10)

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

5. Exploitation

This chapter presents an early analysis of potential exploitation strategies, taking into account the KERs defined in the project. We will analyse each KER through the lens of individual project partners' exploitation capabilities. Additionally, lead partners involved in each pilot and demonstrator, in collaboration with the rest of the partners, have identified opportunities offered by the pilots for an initial common exploitation roadmap. The chapter also outlines the role of the IIAB in guiding project activities with constructive feedback to ensure that project outcomes are as close as possible to market needs. Finally, the chapter presents the strategy that QUBIP will follow to identify and foster possible commercial exploitation opportunities with proper IPR management.

5.1. Key Exploitable Results

The QUBIP project is committed to produce KERs. The following Table 5.1 presents the updated list of KERs committed, as a reference for next subsections.

Table 5.1: List of key exploitable results.

Key Exploitable Result	IP	Open-Source
KER1 – PQ Secure Element with Crypto API. The Secure Element (SE) is an tamper resistant element containing the modules to perform cryptographic operations (e.g., key generation, key storage, signature, and other PQ algorithms) at hardware level with classical and PQC. The SE is complemented by the Crypto API working as a software reference for hardware developing.	CSIC	OSH, OSS
KER2 – PQ Micro-Controller Unit (MCU)-based IoT. A PQ IoT device with external SE. The MCU is connected to the SE through the i2c protocol, protected by SCP-03. The communication with the remote endpoints makes use of Post-Quantum/Traditional (PQ/T) hybrid Transport Layer Security (TLS) implemented over MbedTLS.	CSIC, SECPAT	OSH, OSS
KER3 – PQ Micro-Processor Unit (MPU)-based IoT. A PQ IoT device implemented in a System-on-Chip (SoC), where the SE is hosted on the Programmable Logic (PL), and the embbeded Operating System uses the Processing System (PS). The SE is connected to the PS using AXI interfaces and can be used by the operating system by means of a dedicated custom kernel module. The communication with the remote endpoints makes use of PQ/T hybrid TLS implemented over OpenSSL.	CSIC, TELSY	OSH, OSS
KER4 – PQ-mbedtls. An improved version of the MbedTLS library offering PQ and PQ/T hybrid TLS implementation for IoT devices.	SECPAT	OSS

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

Key Exploitable Result	IP	Open-Source
KER5 – Aurora & Openssl_provider_forge. The first Rust crate implements a shallow Provider for OpenSSL 3.2+, focused on easily integrating external Key Encapsulation Method (KEM) and Signature implementations conforming to the NIST PQC API. The focus is primarily on PQ/T Hybrid (or Composite) schemes. The second Rust crate is a support crate to aid developers in creating OpenSSL Providers in Rust. It is leveraged by aurora as its foundation, but it is versatile enough to be used for other Providers.	TAU	OSS
KER6 – Qryptotoken. This Rust crate implements a PKCS#11-compatible *shallow* loadable module, specifically tailored to be interoperable with Mozilla Firefox's vendored fork of Network Security Services (NSS), with the goal of easily supporting external PQC implementations for KEM and Signatures, as long as they conform to the NIST PQC API. The goal is initially to allow for alternative implementations for the algorithms selected by the Firefox maintainers, and eventually to provide enough flexibility to allow injecting also alternative selections of algorithms. The focus is primarily on PQ/T Hybrid (or Composite) schemes.	TAU	OSS
KER7 – CCIPS (KER7a) & PQ Remote Attestation of IPsec endpoints (KER7b). First (KER7a), CCIPS product implements a solution for establishing IPsec tunnels without relying on the traditional or PQC (IKEv2). Instead, it leverages a centralized key management system to distribute encryption keys, eliminating the need for asymmetric algorithms in the data plane. This approach can also support external cryptographic PQC methods or QKD to generate equivalent keys as IKE. Second (KER7b), PQ Remote attestation provides a solution for PQC based integrity verification over existing classical HW modules such as Trusted Platform Module (TPM) based on wrapping classical attestation quotes over PQC algorithms and its application into IPsec.	TID, POLITO	OSS
KER8 – PQC/QKD Hybridization module. An interface between the QKD module and the agent that hybridizes quantum-distributed key, PQ key and classical key, such that the resulting hybrid key remains secure provided that at least one of the component keys remains secure. The hybridization module obtains the component key through PQ/classical algorithms and standardized interfaces such as ETSI GS QKD 004, it performs the hybridization, and it delivers the hybrid cryptographic material to the agent through ETSI GS QKD 004.	UPM, TID	OSS
KER9 – PQ Container. A Fedora OS-based container that provides a setup suitable for PQ experiments.	REDHAT	OSS
KER10 – PQ Firefox/NSS. Upstream Firefox and NSS have some design limits that hinder broader cryptographic agility when compared to the QUBIP solution for OpenSSL-based stacks. This KER explores least-invasive code changes in Firefox and its vendored fork of NSS, to increase the overall cryptographic agility, specifically in the context of PQ/T Hybrid (or Composite) mechanisms.	TAU	OSS

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

Key Exploitable Result	IP	Open-Source
KER11 – PQ and PQ/T hybrid Verifiable Credentials (VCs). An SSI framework for issuing, holding/presenting and verifying PQ and PQ/T hybrid VCs) with W3C standard data model. The framework supports `did:web`, `did:jwk`, and the new `did:compositejwk` methods until the release of a first PQ Verifiable Data Registry (VDR).	LINKS	OSS
KER12 – PQ Anonymous Credentials. PQ Zero-Knowledge (ZK) algorithm implementation for issuing, holding/presenting and verifying PQ ZK VCs with selective disclosure of identity attributes. The proofs are encoded in JSON Web Proof (JWP) format.	LINKS	OSS
KER13 – Identity Wallet. Identity Wallet, developed as an extension of Mozilla Firefox browser, to handle Traditional, PQ, PQ/T hybrid, and ZK VCs.	LINKS	OSS
KER14 – PQ firmware TPM (fTPM). PQ fTPM running as a Trusted Application (TA) in OP-TEE.	POLITO	OSS
KER15 – PQ Remote Attestation framework. Keylime Verifier enhanced with PQ algorithms to support the verification of the signature on the PQ quote provided by the Attester (i.e., the Keylime agent). In MPU-based IoT device the quote is provided by the PQ fTPM, while in CCIPS the quote is generated and signed (with ECDSA) by the physical TPM and then wrapped with a PQ signature before being sent to the Verifier.	POLITO	OSS
KER16 – PQC Transition Process. A set of practical guidelines for EU agencies and industries to manage the transition to PQC. A summary of a reference and replicable transition process to PQC.	All partners	Open Doc

5.2. Individual exploitation plan

This section presents the partner's individual plans, outlining the chosen strategy, targets, and anticipated outcomes associated with KERs within the respective partner's ecosystem. These varied approaches offer insights for a multifaceted value proposition of the project and its potential for broader societal and economic impact.

LINKS is committed to working towards the exploitation of KER11 and KER12, an SSI framework with PQ, PQ/T hybrid and PQ ZK VCs. LINKS intends to release the resulting SSI framework as OSS and contribute upstream to the IOTA Identity project [12]. LINKS will also work for the exploitation of KER13. LINKS will use OSS to gain credibility within the reference community and then attract and acquire potential customers interested in technology and knowledge transfer, technical consultancy, and custom developments (properly licensed) to create new revenue streams to invest in research and development.

In addition, LINKS is committed to working towards the exploitation of KER16, the replicable transition to PQC process. LINKS will disseminate this key result to gain visibility within the growing PQ technical and scientific community and then attract industrial clients interested in technical guidance and advice on their transition to PQC.

Finally, the knowledge and competence about PQC and the transition of current networked systems to PQC acquired during the project will feed new research ideas that will be instrumental in competing in the funded research market.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

POLITO is committed to exploit KER14 and KER15 as part of its long-term research plan about trust monitoring in distributed infrastructures. Additionally, most of the other KERs will be used internally, in the teaching and research activities of POLITO (as part of MSc and PhD programs), and externally, as part of consultancy towards public and private bodies and proposal of new research projects.

TELSY is committed to work on the exploitation of different KERs. KER3 will provide the baseline to enable the development of new PQC-based technologies and products. The exploitation of KER16 is twofold. On one hand, it will help the internal IT policies of TELSY to ease the transition process, increasing the company awareness and updating its infrastructure. From a technological point of view, KER16 will also increase the technological background to develop and enhance the security of existing and future products of TELSY.

SECPAT will work on the implementation of a version of MbedTLS library enhanced with a PQ and PQ/T hybrid TLS implementation for IoT devices (KER4). SECPAT will work also on KER2, in collaboration with industry and university partners; the goal is to migrate to PQ protocols for the communications between an MCU and a SE both integrated in an FPGA-based implementation. SECPAT is committed to use Open-Source Hardware (OSH) and OSS for the achievement of the result.

CSIC will primarily focus on the development and exploitation of KER1. This PQ secure element, implemented in HW, will be released in an open form, meaning that any industrial company or academic institution can utilize these results. Moreover, CSIC will collaborate with other partners in KER2 and KER3, that could form the basis for future products.

TID will work with different industry partners to achieve the KER7a exploitation in the IPsec migration strategies, achieving a quantum secure alternative for the mid-term adoption in the Telecom sector. This includes any scenarios impacted by IPsec, such as network orchestration and datacenter interconnection. In high-security demand cases, KER7b associated with Quantum-safe remote attestation, and KER8 for hybridization, will be positioned as a complementary service. The open-source-oriented activity for the projects associated with these KERs searches to foster industry adoption and commercialization. Finally, TID will increase its internal company awareness to the quantum transition, by promoting the project results in its business units and clients to offer quantum secure solutions.

UPM will work towards the exploitation of the PQC/QKD Hybridization Module (KER8) to increase the security of next-generation networks based on cloud-native software network functions.

TAU will work with the other partners to exploit KER5, KER6, and KER10, through its research and teaching activities. To this end, TAU is committed, whenever possible, to release its research results in the form of open-science, open-data, open-source artifacts, and especially as contributions to upstream OSS projects.

REDHAT is committed to working towards the exploitation of KER9 and is going to maintain Fedora as a relevant platform for PQ Research and Development platform. REDHAT relies on OSS implementing algorithms and protocols and provides this software as a part of OS altogether with necessary OS-level infrastructure to attract the potential parties interesting in technology and knowledge transfer. Working on KER9, REDHAT heavily relies on KER5, KER6, and KER10, the building components for PQ transition and quantum-secure Internet browsing. REDHAT will include and maintain the algorithms/protocols implementation in Fedora.

SMART is interested KER2 and KER3 for real industrial application environment. The idea is to use the results to implement next generation IoT solutions for machine and plants telemetry and control.

CIB will incorporate the Internet browsing solution into its toolkit of recommended tools for safe and trustworthy Internet and disseminate about the need of safer browsing, offering the QUBIP solution as an accessible one.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

5.3. Initial common exploitation plan

This section outlines the preliminary analysis of possible collaborative exploitation paths based on the pilot cases in development in the project.

5.3.1. Quantum-secure IoT-based digital manufacturing

The IoT-based Digital Manufacturing pilot is strongly representative of many IoT systems tailoring the Industry 4.0, where an IoT-based system and low-end devices will be enabled to securely communicate by means of PQC-protected technologies, by leveraging on quantum-aware building blocks that are both hardware and software.

All the building blocks of the demonstrator can be exploited as a baseline to strengthen and enhance the security of quantum-aware IoT-based products. The straightforward option for the exploitation is the development of proprietary solutions by partners based on this demonstrator, in order to ease the transition for their IoT-based products. Clearly, hardware/software building blocks and the overall demonstrator can be exploited in many directions, not only limiting to the Industry 4.0. Following the open-science approach of the project, the exploitation plan involves also making the contributions publicly available, allowing other researchers and developers to re-use our PQC-enabled building blocks, easing their transition process and enabling them to further validate the solution. In detail, hardware accelerators for PQC algorithms can be adapted to particular scenarios to guarantee the transition process in other contexts. In certain cases where a customer requires ad-hoc solutions based on the hardware derived from the project, the involved partners will consider the exploration of different ways of collaboration (industrial contracts, consulting, bilateral partnerships and public-private partnerships). A similar consideration applies for the Remote Attestation and software integrity verification that includes PQ/T versions of Mbed TLS [13] and OpenSSL [14].

5.3.2. Quantum-secure Internet browsing

The Quantum-secure Internet Browsing pilot demonstrator will combine PQ/T hybrid building blocks to enable quantum-secure mutual authentication of servers and clients (at the application level). The necessary transition of the underlying libraries and applications to PQC will maintain interoperability with the existing World Wide Web (WWW) infrastructure. The building blocks of the pilot demonstrator are the Firefox browser [15], the OpenSSL [14] and NSS [16] libraries, and the IOTA identity framework [12]. All these blocks will be properly integrated and shipped with a PQ build of the Fedora OS [17].

Therefore, the initial exploitation plan considers the possibility of contributing these building blocks upstream to make them widely available, ready for further security analysis, and developed for the overall benefit of the Internet user community. Specifically, following an open science approach, QUBIP envisages the possibility of shipping a PQ build of the Fedora OS, contributing the PQ/T version of OpenSSL and OSSLProvider to the OpenSSL project, the PQ/T version of NSS and Firefox to the Mozilla projects and the PQ ZK VC framework to the IOTA Identity open project. Any other possible commercial exploitation strategy will be considered in the next phases of the project with a clearer view of the market landscape as described in Section 5.5.

5.3.3. Quantum-secure software network environments for telco operators

The network management and operation landscape is shifting towards cloud native solutions and methods, in line with the principles of Network Functions Virtualization (NFV) and Software-Defined Networking (SDN). Additionally, confidential computing principles (remote attestation and trusted execution envi-

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

ronments) are part of the same equation. However, these technologies do not adequately address the quantum security risks posed by vulnerable algorithms.

To mitigate these risks, QUBIP quantum-secure software network environments for telco operator pilot will build solution against quantum threat based on evolution of open-source projects that support cloud native and NFV/SDN environments, such as Kubernetes, OSM [10] or TeraFlow SDN [11]. These projects were born directly from the related standards in ETSI, and offer an attractive technology to be integrated into commercial support by vendors or integrators, such as TID.

Another interesting option is to develop proprietary solutions by partners derived from those open-source frameworks that can offer agile hybridization solutions as an addition so it can leverage based on different commercialization strategies, such as Business-to-Customer (B2C), Business-to-Business (B2B), or Business-to-Business-to-Customer (B2B2C).

5.4. Industrial and Institutional Advisory Board

The QUBIP consortium has set up an IIAB to help steer the project towards solutions that meet real needs. The IIAB is currently composed of 10 relevant members (i.e., institutions and industries interested in QUBIP technologies and results).

Figure 5.1: Institutional and Industrial Advisory Board.

New members could be added in the future based on the evolution of the project. The QUBIP partners have proposed and will propose new members; the composition of the IIAB is always the result of a full agreement between all the QUBIP partners. The main role of the IIAB members is to provide constructive feedback during the three years of the project, so that the results are as close as possible to the market needs, thus facilitating the adoption of the results with a minimum of further development and in a cost-effective manner. From an operational perspective, prior to each meeting with the IIAB, the consortium prepares and shares with the IIAB members updated documentation on QUBIP requirements, critical decisions and the research and development roadmap. This process allows the IIAB to provide constructive feedback to keep the project activities in line with industrial interests.

The QUBIP consortium held the **first IIAB workshop** at M16 during the third General Assembly. Other workshops are expected to be organized in the second period of the project.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

5.5. Strategy for the identification of opportunities to commercial exploitation of results

Besides the open source publication of the KERs and the possible upstream contribution to the related open source projects (e.g., OpenSSL, OSM and IOTA Identity), QUBIP is also envisioned to have at the end a close gap with the commercialisation phase of some of the KERs. In the scenario that all project results will potentially be commercialised and introduced to the market, it will be necessary to identify the organisations, the key market players and the potential users of the QUBIP technologies. This is the plan:

1. Market study considering preliminary KERs: this involves identifying the potential buyers or licensees, the regions where these technologies would have the greatest impact, and the most relevant players in those markets. It is important to understand how the technology fits current and future market needs, as well as to identify trends and opportunities.
2. Complement the market research with a State of the Art (SOTA) analysis: this will help the consortium members to better understand the competitive landscape and recent innovations. This information will be used to create a list of potential buyers or licensees who might be interested in the project exploitable results.
3. Create a commercial technology roadmap for each KER: this document should clearly present the technology, its advantages, potential applications and how it can benefit potential customers. The document will be useful for both internal presentations – with the different consortium members concerned – and external public presentations.
4. Systematic contact with potential organisations: this stage will consist in contacting all members of the list of potential buyers, and includes talking to the relevant departments and stakeholders.
5. Negotiations with potential buyers.
6. Formalising the agreement with the legal/commercial department.

5.5.1. Horizon Results Booster

The above strategy is complemented by the activities within the **Horizon Booster**. The QUBIP application has been approved and the Booster service focuses on providing tailored support to advance the project's readiness for further commercial exploitation.

Two key consultations, or *ELC calls*, were held to align expectations, assess progress, and strategize on future steps. The first call (30/10/2024) focused on introducing the Digital & Ecosystem (D&E) framework, aligning expectations on the services offered by the Booster, and discussing the KERs. During the call, the "Readiness Assessment" tool was shared to assess the project's readiness for exploitation. After the call, the QUBIP consortium submitted relevant documents (e.g., exploitation plans) to help tailor the services to their needs.

The second call (15/11/2024) focused on the responses to the "Readiness Assessment" tool to ensure that the information accurately reflected the current readiness of QUBIP. Based on this, a **Service Roadmap** was developed to outline the most appropriate Booster services for further development.

Table 5.2: Booster services.

Service	Timing
2.3_Go to Market Module A – Kick-off	February 2025
2.3_Go to Market Module B – Unique Value Proposition (UVP) & KERs	May 2025
2.3_Go to Market Module C – Exploitation Strategy	July 2025
2.3_Go to Market Module D – Business Plan	September 2025
2.3_Go to Market Module F – Reporting	November 2025

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

The activities in Table 5.2 aims at the identification of key project components and potential areas for exploitation, including open-source technologies and contributions to industry standards. The roadmap and readiness assessments have set the stage for further engagement with industrial stakeholders, particularly in quantum-secure infrastructure field.

In addition to the calls, the QUBIP project engaged with the broader D&E ecosystem to identify external opportunities for funding, networking, and collaboration.

5.6. Strategy for the management of intellectual property

Management of ownership and access to knowledge is of utmost importance to ensure the proper exploitation of the work and its outcomes for both the individual project partners and the consortium. QUBIP results will be released in open source to the respective community of interest, as detailed in Section 5.1. In principle, software and hardware design will be released, with proper copyright and licence enabling reuse for both research and commercial purposes. In some cases, QUBIP will contribute directly to upstream repository and projects; in those cases, the licence will comply with the one already adopted. It is worth noting the upstream of interest for QUBIP are favourable to (not precluding) commercial exploitation. However, when commercial exploitation opportunities arise, during the project lifetime, QUBIP will leverage three main elements for an effective IP management and exploitation. Firstly, a system that enables the protection of IP (e.g., patents, copyrights, brand, industrial design, trade secrets) that includes clarity about the ownership and use of IPR, the rights and freedom of parties to transfer (assign) IP, and the freedom to publish. Secondly, a technology transfer framework, preferably with the support of specialised knowledge transfer offices with professional staff, such as the European IPR Helpdesk. Thirdly, a fair law enforcement system in each partner's country that caters for dispute settlement. IPR issues will be identified and addressed according to the Consortium Agreement, that regulates the relation between partners. The basic principle is that foreground knowledge, i.e., created within (or resulting from) the project, belongs to the project partner who generated it. If knowledge is generated jointly and separate parts cannot be distinguished, it will be jointly owned under Joint Ownership Agreements, unless the contractor concerned agrees on a different solution. The granting of Access Rights to jointly owned foreground will be royalty-free and based on fair and reasonable conditions. Regarding background IP, the granting of Access Rights will be royalty-free for the execution of work during the project, unless otherwise agreed before the signature of the Grant Agreement. For the purposes of promoting innovation, the European Community will be given a non-exclusive royalty-free license to use the public knowledge generated in the project. Confidential information relating to individuals, data or inventions will be collected and protected in strict accordance with EU and national regulations and best practice regarding data confidentiality.

In some cases, QUBIP will contribute directly to upstream repositories and projects; in those cases, the license will comply with the one already adopted. It is worth noting that the upstream of interest for QUBIP is favourable to (not precluding) commercial exploitation. However, when commercial exploitation opportunities arise, during the project lifetime, QUBIP will leverage three main elements for effective IP management and exploitation.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

6. Conclusions

The QUBIP partners have described in this deliverable their plans for dissemination, communication, and exploitation activities, and reported the corresponding results achieved in the first 18 months of the project. The QUBIP communication and dissemination strategy is designed to reach all the target audiences specified in the Section 1.1 and to provide useful results to the scientific and industrial communities as well as to the general public. Regarding the exploitation of results, QUBIP is designed to balance the need for protecting valuable results with the goal of maximizing their exploitation for both research and commercial purposes. By establishing clear ownership structures, a robust technology transfer framework, and legal mechanisms for IP protection and dispute resolution, QUBIP aims to ensure that its innovations contribute to the success of the project and beyond. Furthermore, the open-science approach will encourage the broader community to benefit from and build upon the results, fostering innovation across various sectors and ensuring the long-term sustainability of quantum-secure technologies.

The planning here discussed will be monitored and updated during the lifetime of the project, to ensure reaching the objectives and quickly taking corrective actions, if needed. One more update is planned in the form of D4.3 at M36 (i.e., August 2026). It will contain the final list of performed activities, the final evaluation of KPIs, and updates to the various plans.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

Bibliography

[1] QUBIP, “GitHub Repository”, https://github.com/QUBIP

[2] QUBIP, “The innovation Manager Corner: PQC news”, https://www.youtube.com/@qubip_eu/playlists

[3] QUBIP, “LinkedIn page”, https://www.linkedin.com/showcase/qubip-eu

[4] QUBIP, “Twitter/X page”, https://twitter.com/qubip_eu

[5] QUBIP, “Youtube page”, https://www.youtube.com/@qubip_eu

[6] Red Hat, “QUBIP and the transition to post-quantum cryptography”, https://research.redhat.com/blog/article/qubip-and-the-transition-to-post-quantum-cryptography/

[7] Cibervoluntarios.org, “El proyecto europeo QUBIP está desarrollando una herramienta que emplea la computación cuántica para mejorar la seguridad digital”, https://www.cibervoluntarios.org/es/actualidad/

[8] IOTA & LINKS Foundations, “IOTA Identity Integrates Zero Knowledge Credentials: In Partnership with the LINKS Foundation”, https://blog.iota.org/iota-identity-zero-knowledge/

[9] Grupo de investigación en Ciberseguridad y Protección de la Privacidad, CSIC, “GiCP’s post on quantum communications and quantum preparedness”, https://gicp.es/tag/qubip/

[10] ETSI, “Open Source MANO”, https://osm.etsi.org/

[11] ETSI, “Open Source Group for TeraFlowSDN (OSG TFS)”, https://tfs.etsi.org

[12] IOTA Foundation, “IOTA Identity”, https://wiki.iota.org/identity.rs/welcome/

[13] Linaro Limited, “Mbed TLS”, https://www.trustedfirmware.org/projects/mbed-tls/

[14] OpenSSL, “Cryptography and SSL/TLS Toolkit”, https://www.openssl.org

[15] Mozilla, “Firefox browser”, https://www.mozilla.org/en-GB/firefox/browsers/

[16] Mozilla, “Network Security Services”, https://firefox-source-docs.mozilla.org/security/nss/index.html

[17] Red Hat, “Fedora Project”, https://fedoraproject.org

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

A. QUBIP Logo

Figure A.1 shows the complete design of the QUBIP logo, the identity of the QUBIP project. The design document guides the partners in the correct use of the logo by presenting simple and self-explanatory guidelines (e.g., fonts, colour, size, and version).

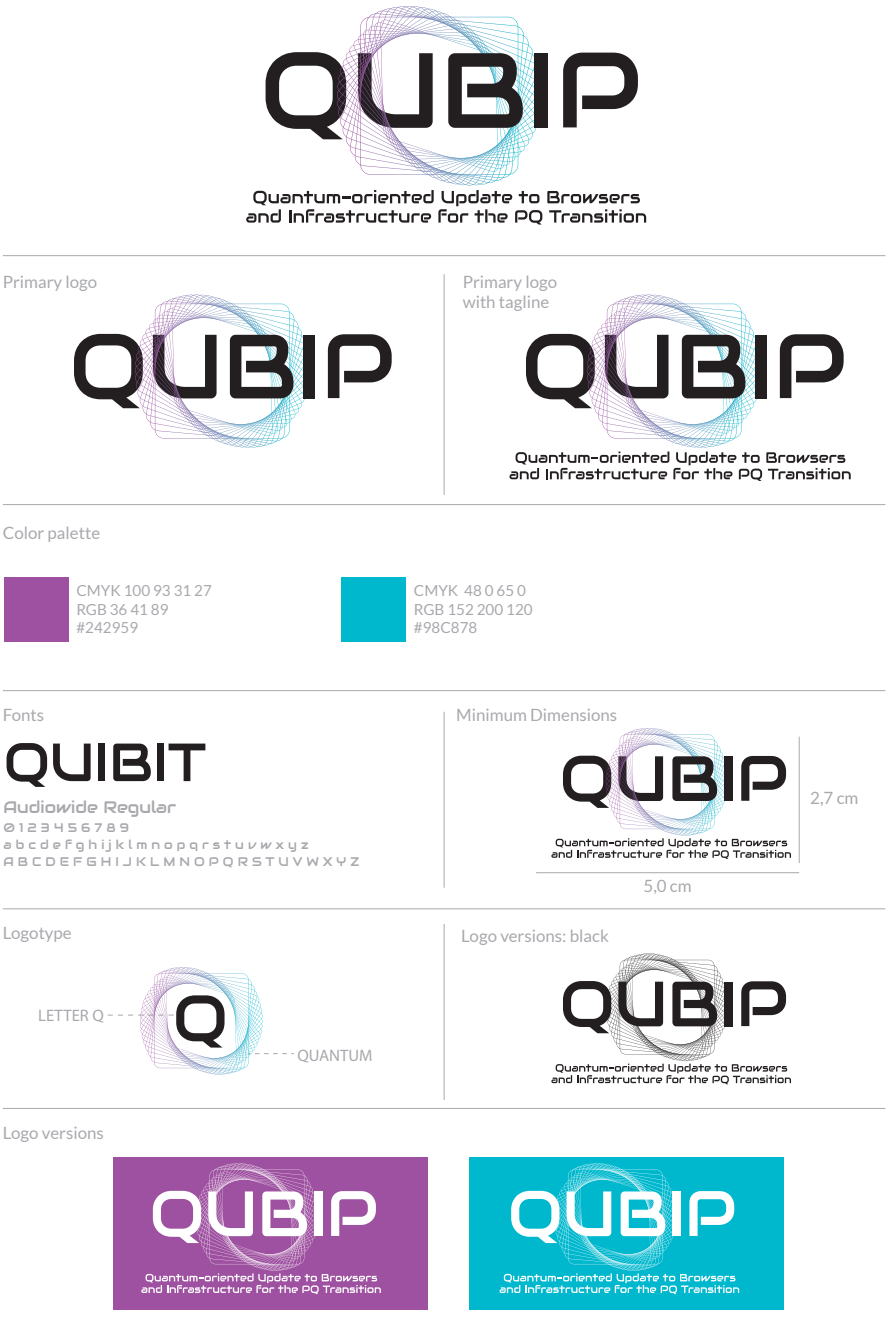
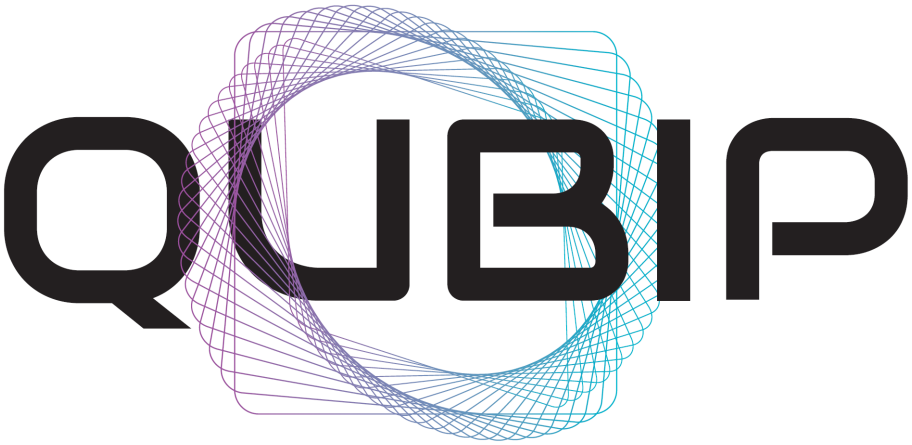


Figure A.1: QUBIP logo design.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].



Quantum-oriented Update to Browsers and Infrastructures for the PQ transition (QUBIP)

https://www.qubip.eu

D4.2 – Dissemination, exploitation and communication plan and activities (intermediate version)

Version 1.0

Horizon Europe