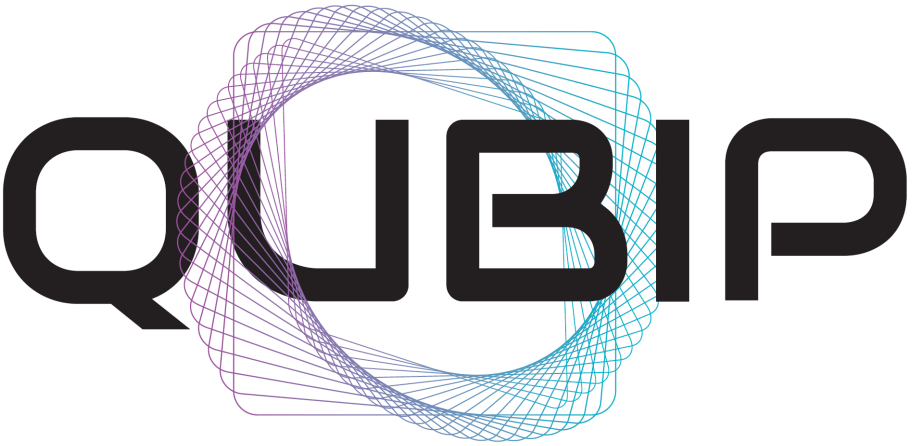
Horizon Europe



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

Data Management Plan (intermediate version)

Deliverable number: D5.3

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:	Javier Faba – UPM Juan Pedro Brito – UPM
Deliverable nature:	Report (R)
Dissemination level:	Public (PU)
Contractual Delivery Date:	28 February 2025
Actual Delivery Date:	11 February 2025
Number of pages:	24
Keywords:	Project Management, Data Management
Contributors:	ALL partners
Peer review:	Maria Chiara Molteni – SECPAT Dmitry Belyavskiy – REDHAT
Approved by:	ALL partners

Table 1: Document revision history

Issue Date	Version	Comments
07/01/2025	0.1	Initial table of contents.
31/01/2025	0.2	Complete draft version for internal review.
11/02/2025	1.0	Final version for submission.

Abstract

This document presents the intermediate version of the Data Management Plan (DMP) of the Quantum-oriented Update to Browsers and Infrastructures for the PQ Transition (QUBIP) project, updated at M18. It describes how reused and generated data will be managed during and after the project, according to the Findable, Accessible, Interoperable and Reusable (FAIR) principles, in alignment with the Horizon Europe guidelines [1, 2, 3]. This document contains a summary of relevant aspects of the data, which include details about the type, purpose, size, and origin. It also includes an explanation of various aspects related to compliance with the FAIR principles. Finally, an overview of resource allocation, data security, ethics and other issues are presented. The structure of this document follows the recommendations of OpenAIRE [2].

Contents

List of Figures

List of Tables

List of Acronyms

ACM	Association for Computing Machinery
CA	Consortium Agreement
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CRQC	Cryptographically Relevant Quantum Computer
DLT	Distributed Ledger Technology
DM	Data Manager
DMP	Data Management Plan
DOI	Digital Object Identifier
ETSI	European Telecommunications Standards Institute
EU	European Union
FAIR	Findable, Accessible, Interoperable and Reusable
GA	Grant Agreement
GDPR	General Data Protection Regulation
HW	Hardware
IACR	International Association for Cryptologic Research
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
INATBA	International Association for Trusted Blockchain Applications
IoT	Internet of Things
IP	Intellectual Property
ISO	International Organization for Standardization
KER	Key Exploitable Result
KoM	Kick-off-Meeting
KPI	Key Performance Indicator
L2S-M	Link-Layer Secure connectivity for Microservice platforms
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OS	Operating System
OSI	Open Source Initiative
OSM	Open Source MANO
PQ	Post-Quantum
PQ/T	Post-Quantum/Traditional
PQC	Post-Quantum Cryptography
QC	Quantum Computer
QKD	Quantum Key Distribution

QUBIP	Quantum-oriented Update to Browsers and Infrastructures for the PQ Transition
RSA	Rivest–Shamir–Adleman
SAB	Security Advisory Board
SE	Secure Element
SHA	Secure Hash Algorithm
SIG	ACM's Special Interest Groups
SO	Strategic Objective
SSI	Self-Sovereign Identity
SW	Software
TLS	Transport Layer Security
ToIP	Trust over IP
TRL	Technology Readiness Level
VC	Verifiable Credential
W3C	World Wide Web Consortium
ZK	Zero-Knowledge

1 Introduction

This document presents the intermediate version of the DMP of the QUBIP project, updated at M18. It describes different strategies, procedures, and aspects regarding the data management activities, including data generation and reuse, types and formats, purpose, expected size, origin, and utility. A clear and transparent data management plan is crucial for modern research collaborative projects since large amounts of data may be generated, processed and used among multiple partners from different disciplines and backgrounds. A well-structured and comprehensive DMP ensures that data is managed ethically, securely, and in compliance with relevant regulations and standards.

The DMP is a “living document” that will describe the data management according to the evolution of the project. This means that changes in the data management procedures and activities will also be reflected in the last versions of the DMP, Deliverable D5.4 at M36.

This document has been developed taking into account feedback from all partners within the consortium. It is in line with the Guidelines for Open Access to Scientific Publications and Research Data in Horizon Europe [1], the General Data Protection Regulation (GDPR), and the Horizon Europe FAIR Data Management guiding principles [2, 3]. By establishing clear guidelines and procedures for data management, the DMP aims to maximize the value of the project’s data assets, promote open science and ensure compliance with regulatory requirements and ethical standards.

This document follows the recommendations of OpenAIRE A.M.K.E [6], which is a non-profit organization with a mission to promote open scholarship and improve discoverability, accessibility, shareability, reusability, reproducibility, and monitoring of data-driven research results, globally. Concretely, the DMP is based on the Research Data Management guide [2], which contains a template for the DMP. The structure of this document is here detailed:

- Chapter 2 briefly describes the QUBIP project in order to give the appropriate context to the DMP.
- Chapter 3 describes different aspects of the generated and reused data of the project.
- Chapter 4 outlines how the research data will follow the FAIR principles, in alignment with the Horizon Europe mandates.
- Chapter 5 describes other aspects of data management such as the allocation of resources, security and ethical aspects, and other research outputs.
- Chapter 6 draws the conclusions and provides the next steps for final iteration of the DMP.

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

2 QUBIP Overview

The development of Quantum Computers (QCs) pose a significant threat to traditional public-key cryptography, which is the cornerstone of today's security over the Internet. Traditional public-key cryptography relies on the complexity of mathematical problems such as large number factorisation and discrete logarithm computation [7, 8] which can be broken when powerful and stable Cryptographically Relevant Quantum Computers (CRQCs) become available [9, 10]. Consequently, the transition from traditional to Post-Quantum Cryptography (PQC) is mandatory, albeit complicated, given its extensive impact on numerous functions, algorithms, and protocols with unknown cascades of dependencies. The transition to PQC is expected to be more complicated than previous ones (e.g., from SHA1 to SHA256 or from RSA to Elliptic-curve cryptography), as rigorous analysis of its inherent complexity is required alongside ongoing standardisation efforts for PQC. It is therefore imperative to begin this transition now. This will help to identify and address the barriers and to experiment with effective strategies to overcome them.

QUBIP is designed to contribute to the EU transition to PQC with the aim of streamlining the process and creating a replicable transition model (and also to counter quantum threat as soon as possible). QUBIP focuses on digital systems addressing the 5 main building blocks that use public-key cryptography for security purposes: hardware, cryptographic libraries, operating system, communication protocols and applications. QUBIP addresses all 5 blocks coherently solving all dependency issues that may arise within each block and between blocks with the ultimate goal of validating at Technology Readiness Level (TRL) 6 three pilot systems: Internet of Things (IoT)-based Digital Manufacturing, Internet Browsing, and Software Networks Environments for Telco Operators.

The return on experience from the three practical exercises on the transition to PQC will then be maximised through the development of a migration playbook. This will include the lessons learned and an assessment of the technical, economic, and regulatory barriers encountered, together with the solutions to overcome them, to enable the definition of a replicable process and to provide structured support to industry stakeholders. The technical activities will be underpinned by three supporting activities: (*i*) evaluation of the capabilities of QC to assess their implication to algorithms and protocols adopted,(*ii*) contribution to standardization efforts addressing transition to PQC, and (*iii*) design of policy measures addressing technology changes coming from the advent of QC and PQC.

In achieving the Strategic Objectives recalled in Section 3.3, the QUBIP project may generate data that will need to be properly managed. This DMP provides a comprehensive plan and guidelines for the data management in the project.

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

3 Data Summary

This chapter serves as a comprehensive overview of the data generated, collected, and used throughout the duration of the QUBIP project.

3.1 Reused data

QUBIP is going to reuse data produced by other PQC-related initiatives.

Quantum-Secure IoT-based Digital Manufacturing pilot: it will reuse the PQC implementations provided by liboqs [11], PQClean [12], and pqm4 [13]. The specific Hardware (HW) and Software (SW) implementations can be verified using the test vectors published by the maintainers of these libraries or by National Institute of Standards and Technology (NIST) (e.g., SHA3/SHAKE and MACs algorithms). If the test vectors are not available, appropriate data from the literature will be used. In addition, existing performance data (e.g., key sizes, signature sizes, signature latency and verify latency) can be reused or generated by running the actual PQC implementations for comparison.

Quantum-secure Internet Browsing pilot: it will reuse the PQC implementations provided by liboqs [11], PQClean [12], libcrux [14], and noble-post-quantum [15]. Where relevant, data published by open source projects such as OpenSSL [16], NSS [17], Mozilla Firefox [18], oqs-provider [19] and standards/specifications can be used to extract guidelines for the correct use of PQC algorithms. In addition, existing performance data (e.g., key sizes, signature sizes, signature latency and verify latency) can be used or generated by running the actual PQC implementations for comparison.

Quantum-secure Software Network Environments of Telco Operators Pilot: it will reuse data from existing open source projects to optimise algorithms and their implementations, to set the configuration parameters, to select proper tests and compare performance. These open source projects include Open Source MANO (OSM) [20], TeraFlowSDN [21], Kubernetes [22] and L2S-M [23].

For the sake of clarity, QUBIP will make use of existing, largely revised implementations of PQC algorithms. Existing SW implementation of the building blocks that make up the three pilot demonstrators will also be used and leveraged to make the transition to PQC. When possible, QUBIP will not develop new software, but will focus on the transition of existing secure solutions.

3.2 Types and formats of data

The following types of data will be generated or reused during the QUBIP project:

1. Documentations, including technical reports, dissemination material, SW and HW documentation;
2. SW and HW implementations, consisting in source code, object files and executable files;
3. Key Performance Indicators (KPIs) and Targets, at building block level and at system level;
4. Benchmarks and test results, at building block level and at system level.

Table 3.1 reports an evolving set of formats and files extensions that are associated to the identified types of data.

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

Formats of data	File extensions
Source code	c, cpp, h, rs, bin, ini, py, m, Verilog-HDL
Structured or semi-structured data	csv, xls, ods, json
Text	txt, pdf, doc, pptx, html, md, log
Audio-visual	jpg, png, bmp, svg, mp4, mkv

Table 3.1: Formats of data generated or reused in QUBIP and corresponding file extensions.

3.3 Purpose of the data

The QUBIP project sets ten Strategic Objectives (SOs):

- **SO1**: Constantly evaluate the capabilities of quantum computers to assess their implication to Post-Quantum (PQ) primitives, algorithms, and protocols adopted by the QUBIP project.
- **SO2**: Address the transition of IoT devices focusing on HW implementation of quantum-resistant public-key cryptography in the form of both external and integrated Secure Elements (SEs). HW implementation considers (*i*) acceleration of most-time demanded operations, (*ii*) reduction of power consumption, (*iii*) minimization of resources (e.g., memory and chip size area), (*iv*) miniaturization of systems to ease the development and portability and (*v*) resilience against side channel and fault injection attacks with proper countermeasures.
- **SO3**: Explore the transition of OpenSSL and NSS cryptographic libraries to PQC through loadable modules with the main goal of plugging (*i*) PQ algorithms and schemes in the existing SW ecosystem and (*ii*) PQ HW implementations transparently.
- **SO4**: Start the transition of Fedora Operating System (OS) to PQC by addressing the integration of PQ libraries (i.e.OpenSSL and NSS) to provide the upper layers quantum-secure communication capabilities through Post-Quantum/Traditional (PQ/T) hybrid Transport Layer Security (TLS) v1.3. This objective subtends backwards compatibility with traditional cryptography-based operations.
- **SO5**: Experiment with the transition of Firefox browser toward a post-quantum security state through adoption of PQ/T hybrid TLS for key-exchange and authentication, and PQ Zero-Knowledge (ZK) Verifiable Credentials (VCs) for application level authentication and authorization.
- **SO6**: Hardening the security of IPsec by extending key exchange capabilities leveraging the convergence of Quantum Key Distribution (QKD) and PQC.
- **SO7**: Experiment with the transition of three systems to quantum-secure state leveraging a proper combination of cryptographic agile building blocks developed in accordance with previous five SOs (from SO2 to SO6). SO7 subtends to reach quantum-secure state while ensuring the minimum-security level provided by traditional cryptography and without introducing new attack vectors.
  - **SO7.1**: Enable quantum-secure IoT-based digital manufacturing.
  - **SO7.2**: Reach quantum-secure Internet browsing.
  - **SO7.3**: Deploy quantum-secure software network environments for telco operators.
- **SO8**: Validation of the three quantum-resistant systems.
- **SO9**: Build and maximize the return-of-experience from the transition exercises (addressed by SO7) evaluating all the technical, economic, and legal barriers encountered and proposing the solutions to overcome them.
- **SO10**: Maximize industrial impact by contributing to relevant standardization bodies and open-source projects directly involved or impacted by transition to PQC. Build awareness on the transition to PQC implications and solutions among other concerned standardization organisations and regulatory bodies.

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

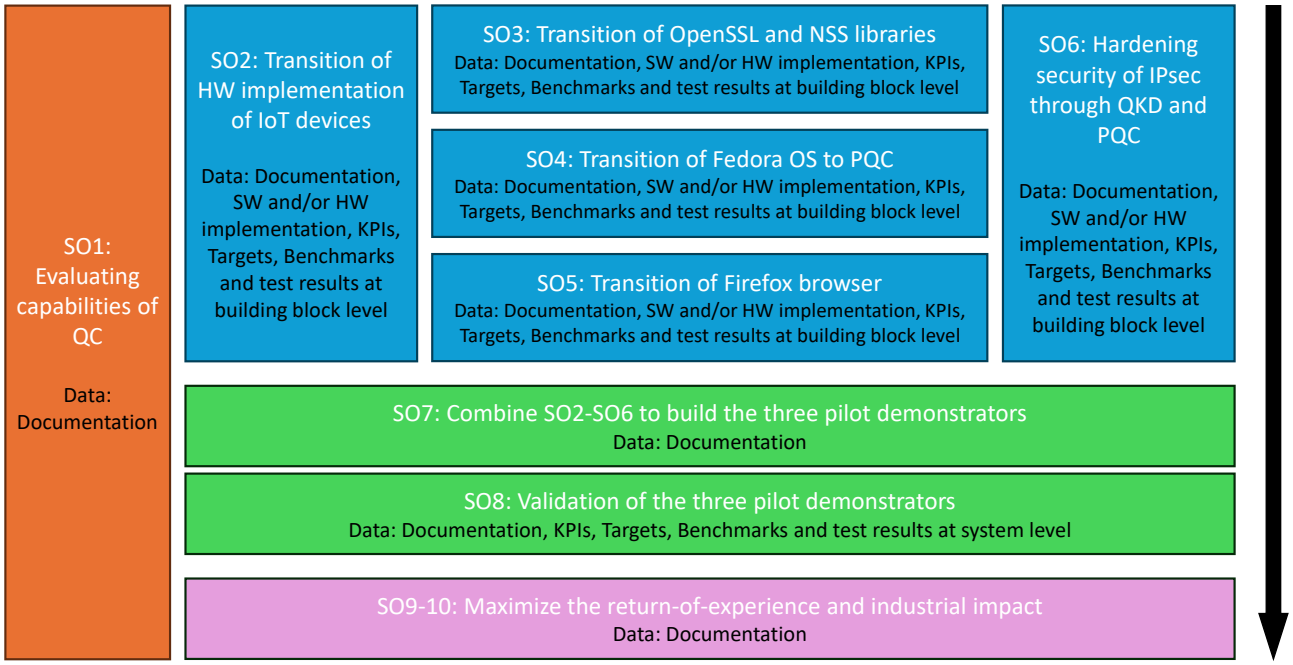


Figure 3.1: Structure of the Strategic Objectives of QUBIP project and its relation to data.

The purpose of data generation in QUBIP is related to one or more of the SOs, as shown in Figure 3.1. Table 3.2 presents the evolving list of data that will be generated during the activities foreseen to achieve the SOs, highlighting the relation between each SO, the types of data and the formats of data.

3.4 Expected size of the data

The expected size of generated data is very heterogeneous, depending on the nature of each activity. As a first estimation, data related to evaluation and validation of the demonstrators will be less than 100 GB per pilot.

3.5 Origin of the data

The origin of the generated data may be:

- Experimental: non-processed data generated from an experiment or test.
- Observational: data obtained during the execution of an experiment or test.
- Derived: processed data, generated from experimental data or directly by humans.
- Literature: source of information.

The origin of the reused data will be the source code and documentation of original software QUBIP relies on for the transition to PQC, specifications provided by entities such as Internet Engineering Task Force (IETF), NIST, World Wide Web Consortium (W3C), Organization for the Advancement of Structured Information Standards (OASIS) among others, and source code and documentation previously developed by the partners. Also, data from scientific literature from International Association for Cryptologic Research (IACR), Institute of Electrical and Electronics Engineers (IEEE), and Association for Computing Machinery (ACM) repositories on PQC implementations will be used as a reference.

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

Strategic Objectives	Types of data	Formats of data			
		Source code	Structured or semi-structured	Text	Audio-visual
SO1	Documentation			X	X
SO2, SO3, SO4, SO5, SO6	Documentation		X	X	X
	SW and/or HW implementation	X			
	KPIs and Targets at building block level		X		
	Benchmarks and test results at building block level		X		X
SO7	Documentation			X	X
SO8	Documentation			X	X
	KPIs and Targets at system level		X		
	Benchmarks and test results at system level		X		X
SO9, SO10	Documentation			X	X

Table 3.2: Relation between Strategic Objectives, types and formats of data.

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

3.6 Data utility

QUBIP project focuses on the transition from traditional cryptography to PQC of protocols, networks, and systems we use today. Therefore, data generated during the QUBIP project may be useful for a number of target groups, as shown in Figure 3.2.

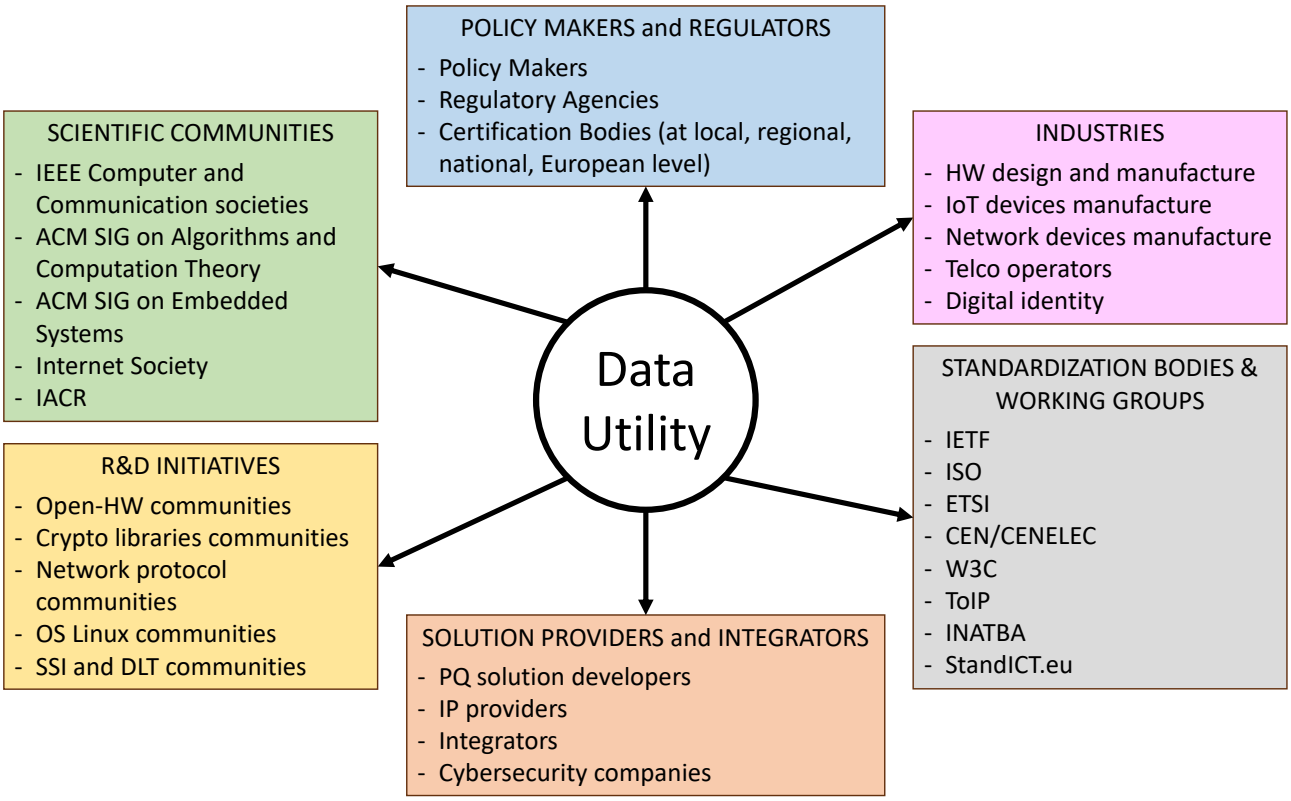


Figure 3.2: Data utility for the QUBIP project.

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

4 FAIR Data

The FAIR principles [3, 24] serve as a foundational framework for ensuring that research data and outputs are Findable, Accessible, Interoperable, and Reusable. These principles are crucial for fostering transparency, collaboration, and efficiency in research endeavours, and they are particularly relevant in the context of Horizon Europe projects, which aim to advance scientific knowledge and address societal challenges through interdisciplinary collaboration and innovation.

Findability of data makes research outputs easy to find for both humans and machines. This involves assigning unique identifiers such as Digital Object Identifier (DOI) to datasets and other research outputs. Additionally, metadata should be richly described using standardized vocabularies and made available through searchable repositories or databases. Adhering to this principle ensures that the outcomes of funded research are discoverable, maximizing the impact of the research.

Accessibility is essential for other researchers to retrieve and use research outputs easily. This involves ensuring that data and resources are stored in accessible repositories and that appropriate access controls are in place to protect sensitive data. By adhering to the accessibility principle, Horizon Europe projects promote collaboration among researchers from different institutions and fields.

Interoperability refers to the ability of different systems, tools, and datasets to work together without difficulties. In the context of research data, this means adopting common data formats, standards, and protocols to facilitate data integration, analysis, and reuse across different disciplines and platforms. By ensuring interoperability, Horizon Europe projects enhance the reproducibility of research, enabling the possibility to combine and compare data from multiple sources.

Reusability emphasizes the importance of designing research data and outputs in a way that enables their reuse for future research purposes. This involves providing clear and comprehensive documentation, including metadata, and open licences, to facilitate understanding and reuse. Data should also be stored and preserved in a sustainable manner to ensure its long-term usability and reproducibility.

By adhering to these principles, researchers can enhance the visibility, accessibility, and impact of their work, promote collaboration and knowledge exchange across disciplines, and accelerate scientific progress.

4.1 Making data findable, including provisions for metadata

With the goal of making data findable, data will be automatically identified by a corresponding persistent identifier when deposited in a trusted repository. The type of persistent identifier will depend on the specifications of the repository. Documents such as technical reports, user/developer manuals for SW, contributions to standards and similar documentation will be identified through a DOI.

Metadata will be added to ease data discovery. It will contain information such as title, authors, description, origin, etc. The exact structure or content of the metadata will depend on the nature of the data. Standards for metadata creation and management will be used in compliance with the selected data repository. Data deposited in Zenodo[1] will be provided with public machine-readable metadata. The metadata will be compliant with DataCite's Metadata Schema [25] minimum and recommended terms, with a few additional enrichment. Metadata of each record is indexed and searchable directly in Zenodo's search engine immediately after publishing, and it is sent to DataCite servers during DOI registration and indexed there.

[1] Zenodo is a general purpose repository described in Section 4.2.1

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

Standard keywords from QC, PQC, cybersecurity, and networking science will be used.

4.2 Making data accessible

4.2.1 Repositories

Data generated by the QUBIP project will be deposited in the QUBIP official Zenodo repository [4] to facilitate findability and accessibility, and linked on the QUBIP project website. Zenodo is a general purpose repository developed under the European OpenAIRE program and operated by CERN, with clear and open policies for data, in line with the FAIR principles and the European Union (EU) standards. As a common principle, data sharing will follow recommendations from the Security Advisory Board (SAB) to comply with security requirements.

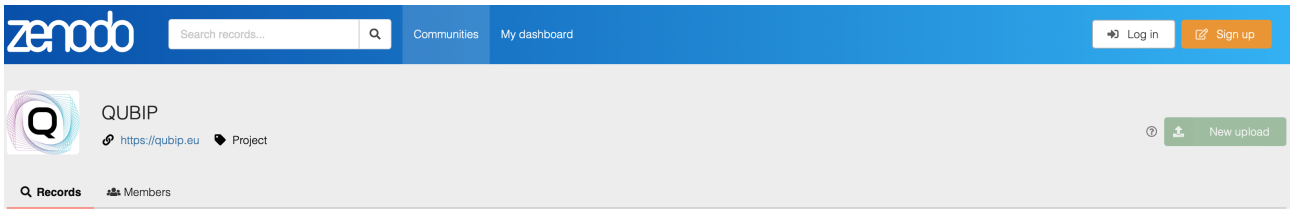


Figure 4.1: QUBIP official Zenodo repository [4].

It is worth to highlight that open access research data do not jeopardize future intellectual property and exploitation rights that may arise in during the project, in accordance with the Consortium Agreement (CA).

When relevant, data will also be available through the institutional repositories of the partners (e.g., Digital.CSIC repository, Fedora repository, Tampere University Research Portal). Different trusted repositories may enforce specific security policies depending on the characteristics of the data. These security policies include data classification by sensitivity level, backup mechanisms, or protocols for controlled data access and authentication. QUBIP will adhere to these security policies.

4.2.2 Data

Following FAIR and *'as open as possible, as closed as needed'* principles, all non-sensitive data will be made openly available. This data will be deposited on Zenodo under the Creative Commons licence CC BY 4.0. The related metadata will be deposited under Creative Commons Public Domain Dedication (CC0) licence to ensure reusability. The corresponding service will provide persistent identifiers to promote data identification and citation.

Some datasets generated during the project may be so focused on the development of a specific activity that there is no apparent utility outside this context. In this case, this should be clearly explained, and the dataset should not be published.

Sensitive data will be managed following the Grant Agreement (GA) and the CA. This data includes software under exportation law, personal data, and data derived from experimental realizations, including specific segments of algorithms protected by intellectual property rights. GDPR will be followed for personal data. Not publishing, or under embargo, or other restrictions is allowed, but only if there are sufficient grounds to do so (e.g., to seek protection of the intellectual property). In general, research data will be made available as soon as possible. However, in case an embargo is applied, the specific duration of the embargo will depend on the nature and characteristics of the data, and this will be made available after the embargo period. The Industrial Property Units or Technology Transfer Offices for each partner will help in

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

designing and implementing, in close collaboration with the researchers involved, a protection strategy for the results of research of commercial and industrial relevance.

Concerning the data access, data will be openly accessible though free and standardized protocols. These protocols will depend on the repository where the data is stored.

Sensitive data will be kept private. If a third party is requiring access to data, the representative of the corresponding institution will discuss this request with the consortium, and a contact information will be provided. The identity of the person accessing the data will be ascertained through standard protocols and methods whenever applicable.

Finally, no data access committee is needed for the QUBIP project, since there is no need to evaluate/approve access requests to published data.

4.2.3 Metadata

Following the FAIR principles, metadata will be made openly available and licensed under a Creative Commons Public Domain Dedication (CC0). If required, metadata will contain information to enable the user to access the data. Both metadata and data will be available as long as they remain deposited in the corresponding repository, as a general principle, no less than five years after the conclusion of the QUBIP project. In general, all information will be accessible through standard, commonly used formats and open source applications. If scripts are required to process data or metadata, they will be included under Open Source Initiative (OSI) approved licences.

4.3 Making data interoperable

Standard vocabularies and formats will be used to make the data interoperable. If non-standard or unfamiliar vocabularies (e.g., specific context-dependent abbreviations or similar) are used, they will be explained through metadata or README files in a text-based format. Community-endorsed interoperability best practices will be followed, whenever possible. This includes the use of common (open) formats and standards for data, controlled vocabularies, or avoiding the creation of data which needs a proprietary software to be used. In case it is unavoidable the use of uncommon or project specific ontologies or vocabularies, mappings or explanations in terms of standard ontologies or vocabularies will be provided. If needed or required, qualified references [26] will be included.

4.4 Making data reusable

In order to facilitate data reusability, README files will be provided; they will provide clear and comprehensive explanation of the metadata and data contents. All published data will be usable by third parties under the corresponding licences, and provenance of the data will be documented through metadata, README files and citations.

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

5 Resources, security, ethical aspects and other issues

5.1 Allocation of resources

There are no additional costs for making QUBIP data FAIR and publishing it on the selected repositories.

The General Assembly appointed Javier Faba, representative of UPM, as the Data Manager (DM) for the QUBIP project during the QUBIP Kick-off-Meeting (KoM). The DM oversees the data collection, preparation and publication, performs data quality management and is responsible for the application of the DMP.

5.2 Data security

Data will be deposited in trusted repositories to promote long-term preservation and curation. For data deposited in public trusted repositories, security will be provided by the entity responsible for the management of the repository. For data deposited in the institutional repositories of each partner, security provisions will be determined and provided by the corresponding institution. They usually include frequent backups, storage of copies on local drives, etc. As stated in Section 4.2.1, data sharing will follow recommendations from the SAB to comply with security requirements.

5.3 Ethics

Because of the nature of the QUBIP project, no data will cause ethical or legal issues with respect to data management or sharing, but personal data could be collected under the context of some activities (e.g., running of the Quantum-secure Internet Browsing pilot demonstrator, conferences, workshops, and webinars organized by QUBIP project, etc). In these contexts, QUBIP adheres to the principles of informed consent, ensuring that participants are adequately informed about the purpose of data collection, storage, and sharing. QUBIP data sharing practices are aligned with the GDPR. We ensure that all data processing activities, including sharing, adhere to these legal frameworks. Informed consent for data sharing and long-term preservation will be included in all questionnaires that involve the collection of personal data.

5.4 Other research outputs

In addition to the data management procedures, this DMP considers and plans for the management of other research outputs that will be generated during the project. These outputs include all open source software and hardware, see the list of Key Exploitable Results (KERs) in Deliverable D4.2, that will be made available via the QUBIP official GitHub repository [5].

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

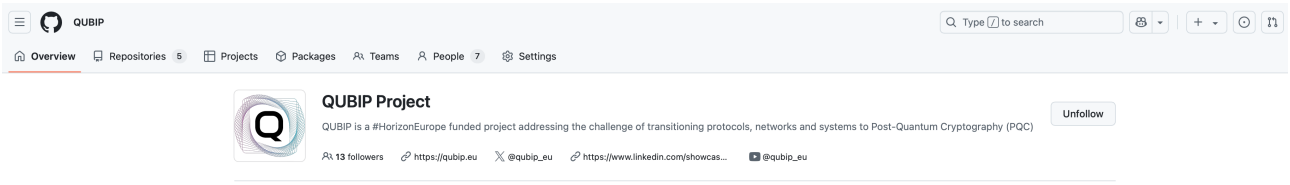


Figure 5.1: QUBIP official GitHub repository [5].

5.5 Other issues

If necessary, internal further procedures will be adopted for data management (e.g., standard Fedora SW development procedures). These internal procedures will not violate the GA and the CA.

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

6 Conclusions

This document has presented the intermediate version of the DMP of the QUBIP project, updated at M18. The DMP describes the data that will be reused and generated during the QUBIP project, and it outlines how this data will follow the FAIR principles.

The data reused and generated, and more generally the outputs of the project, will be very heterogeneous due to the multidisciplinary nature of QUBIP. This is reflected in the different types and formats of data that the project may generate in the course of its activities to achieve its ten SOs. QUBIP will adopt all necessary procedures to manage data in accordance with FAIR principles.

Finally, it is important to note that the DMP is a living document. This means that it should evolve and that it will be updated according to the lessons learned and future needs. The final version of the DMP, Deliverable D5.4 at M36, will include possible changes and updates to this intermediate version, together with the final list of open datasets and other research outputs generated.

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

Bibliography

[1] European Commission, “Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020”, [Online]. Available: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf

[2] OpenAIRE, “How to comply with Horizon Europe mandate for Research Data Management, Guides for Researchers”, [Online]. Available: https://www.openaire.eu/how-to-comply-with-horizon-europe-mandate-for-rdm

[3] M. D. Wilkinson *et al.*, “The FAIR Guiding Principles for scientific data management and stewardship”, Scientific Data, vol. 3, Mar 2016, p. 160018, DOI 10.1038/sdata.2016.18

[4] QUBIP project, “QUBIP Zenodo repository”, [Online]. Available: https://zenodo.org/communities/qubip/

[5] QUBIP project, “QUBIP GitHub repository”, [Online]. Available: https://github.com/QUBIP

[6] OpenAIRE, “OpenAIRE becomes a fully fledged organisation ”, [Online]. Available: https://www.openaire.eu/openaire-organisation-in-the-making

[7] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems”, Commun. ACM, vol. 21, feb 1978, p. 120–126, DOI 10.1145/359340.359342

[8] W. Diffie and M. Hellman, “New directions in cryptography”, IEEE Transactions on Information Theory, vol. 22, no. 6, 1976, pp. 644–654, DOI 10.1109/TIT.1976.1055638

[9] P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring”, Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124–134, DOI 10.1109/SFCS.1994.365700

[10] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”, SIAM Journal on Computing, vol. 26, no. 5, 1997, pp. 1484–1509, DOI 10.1137/S0097539795293172

[11] D. Stebila and M. Mosca, “Post-quantum key exchange for the Internet and the Open Quantum Safe project”, Proc. 23rd Conference on Selected Areas in Cryptography (SAC) 2016 (R. Avanzi and H. Heys, eds.), October 2017, pp. 1–24, DOI 10.1007/978-3-319-69453-5_2

[12] M. J. Kannwischer, P. Schwabe, D. Stebila, and T. Wiggers, “Improving software quality in cryptography standardization projects”, IEEE European Symposium on Security and Privacy, EuroS&P 2022 - Workshops, Genoa, Italy, June 6-10, 2022, Los Alamitos, CA, USA, 2022, pp. 19–30, DOI 10.1109/EuroSPW55150.2022.00010

[13] M. J. Kannwischer, R. Petri, J. Rijneveld, P. Schwabe, and K. Stoffelen, “PQM4: Post-quantum crypto library for the ARM Cortex-M4”, [Online]. Available: https://github.com/mupq/pqm4

[14] Cryspen, “libcrux - the formally verified crypto library ”, [Online]. Available: https://github.com/cryspen/libcrux

[15] Paul Miller, “noble-post-quantum - auditable & minimal JS implementation of post-quantum public-key cryptography”, [Online]. Available: https://github.com/paulmillr/noble-post-quantum

[16] OpenSSL project, “OpenSSL Cryptography and SSL/TLS Toolkit”, [Online]. Available: https://www.openssl.org

[17] Mozilla, “Network Security Services (NSS)”, [Online]. Available: https://firefox-source-docs.mozilla.org/security/nss/index.html

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

[18] Mozilla, “Firefox Source Tree Documentation”, [Online]. Available: https://firefox-source-docs.mozilla.org/index.html

[19] Open Quantum Safe project, “oqs-provider – OpenSSL 3 provider containing post-quantum algorithms”, [Online]. Available: https://github.com/open-quantum-safe/oqs-provider

[20] Open Source MANO project, “Documentation”, [Online]. Available: https://osm.etsi.org/docs/user-guide/latest/#

[21] ETSI Software Development Group, “ETSI Open Source Group for TeraFlowSDN (OSG TFS)”, [Online]. Available: https://tfs.etsi.org

[22] Kubernetes project, “Kubernetes - Production-Grade Container Scheduling and Management”, [Online]. Available: https://kubernetes.io

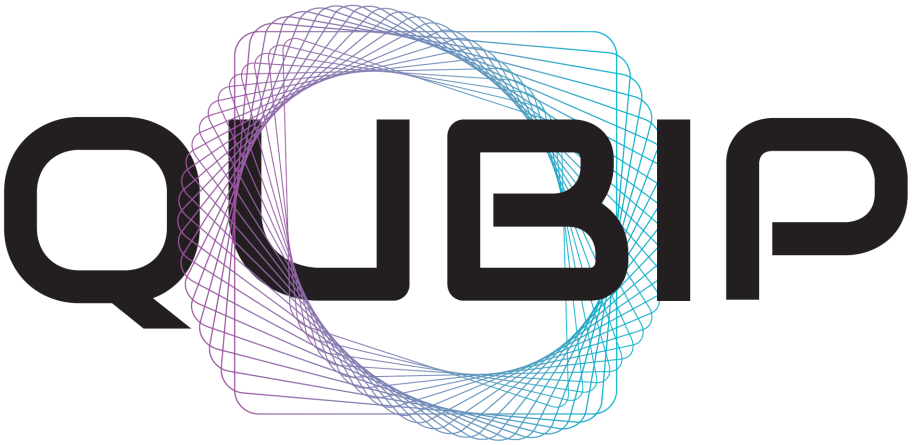
[23] L. F. Gonzalez, I. Vidal, F. Valera, and D. R. Lopez, “Link layer connectivity as a service for ad-hoc microservice platforms”, IEEE Network, vol. 36, no. 1, 2022, pp. 10–17, DOI 10.1109/MNET.001.2100363

[24] S. Bezjak, A. Clyburne-Sherin, P. Conzett, P. Fernandes, E. Görögh, K. Helbig, B. Kramer, I. Labastida, K. Niemeyer, F. Psomopoulos, T. Ross-Hellauer, R. Schneider, J. Tennant, E. Verbakel, H. Brinken, and L. Heller, “The Open Science Training Handbook”, [Online]. Available: https://book.fosteropenscience.eu/

[25] DataCite Metadata Working Group, “DataCite Metadata Schema for the Publication and Citation of Research Data and Other Research Outputs. Version 4.5.”, DataCite e.V. [Online]. Available: https://doi.org/10.14454/g8e5-6293

[26] GO FAIR, “I3: (Meta)data include qualified references to other (meta)data”, [Online]. Available: https://www.go-fair.org/fair-principles/i3-metadata-include-qualified-references-metadata/

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

D5.3 – Data Management Plan
(intermediate version)

Version 1.0

Horizon Europe