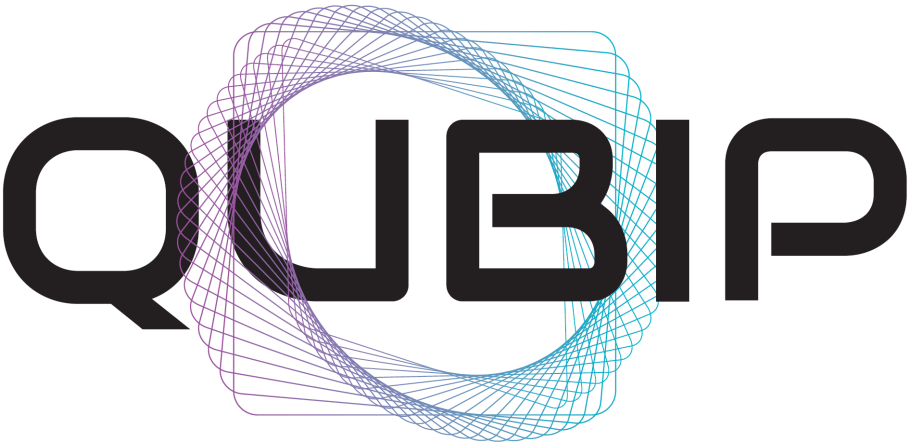
Horizon Europe



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

Standardization plan and activities (initial version)

Deliverable number: D4.4

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 Pastor	– TID
Deliverable nature:	Report (R)	
Dissemination level:	Public (PU)	
Contractual Delivery Date:	31 August 2024	
Actual Delivery Date	27 August 2024	
Number of pages:	31	
Keywords:	Standardization, Industry, Open-Source	
Contributors:	Andrea Vesco	– LINKS
	Grazia D'Onghia	– POLITO
	Davide Bellizia	– TELSY
	Maria Chiara Molteni	– SECPAT
	Eros Camacho	– CSIC
	David Arroyo	– CSIC
	Marc Almeida	– CSIC
	Izan Franco	– CSIC
	Diego Lopez	– TID
	Antonio Pastor	– TID
	Luis F. Gonzalez	– UC3M
	Ivan Vidal	– UC3M
	Francisco Valera	– UC3M
	Javier Faba	– UPM
	Juan Pedro Brito	– UPM
	Daniel Luoma	– TAU
	Akif Mehmood	– TAU
	Alex Shaindlin	– TAU
	Nicola Tuveri	– TAU
	Dmitry Belyavskiy	– REDHAT
	Sahana Prasad	– REDHAT
Peer review:	Antonio Lioy	– POLITO
	Davide Bellizia	– TELSY
Approved by:	ALL partners	

Table 1: Document revision history

Issue Date	Version	Comments
31/05/2024	0.1	Initial table of contents
12/07/2024	0.2	First draft version for internal review
07/08/2024	0.3	Second draft version for internal review
26/08/2024	0.4	Draft version for quality review
27/08/2024	1.0	Final version

Abstract

This document is the deliverable D4.4 of the Quantum-oriented Update to Browsers and Infrastructures for the Post-quantum transition (QUBIP) project. It reports on the first version of the QUBIP project plan for contributions to standardisation, industry associations, and open source communities. The document also reports on the results achieved during the first year of the project.

Contents

List of Tables

List of Acronyms

3GPP	3rd-Generation Partnership Programme
6G-IA	6G Smart Networks and Services Industry Association
API	Application Programming Interface
ASN.1	Abstract Syntax Notation One
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
CFRG	Crypto Forum Research Group
CMS	Cryptographic Message Syntax
CT	Core Network & Terminals
CVD	Coordinated Vulnerability Disclosure
DDoS	Distributed Denial of Service
DICE	Device Identifier Composition Engine
DID	Decentralised IDentifier
DIWG	Decentralised Identifier Working Group
DLT	Distributed Ledger Technology
DTLS	Datagram Transport Layer Security
ENISA	European Union Agency for Cybersecurity
EP	ETSI Project
ESO	European Standardisation Organisation
ETSI	European Telecommunications Standards Institute
eZTS	Enablers for Zero Touch Security
FGQT	Focus Group on Quantum Technologies
FIPS	Federal Information Processing Standards
GSMA	Global System Mobile Association
ICT	Information and Communication Technologies
I-D	Internet-Draft
IETF	Internet Engineering Task Force
IIAB	Industrial and Institutional Advisory Board
IoT	Internet of Things
IRTF	Internet Research Task Force
ISG	Industry Specification Group
ISO	International Standards Organisation
ITSC	IT and Security Committee
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
IWG	Identity Working Group
JHAS	JIL Hardware-related Attacks Subgroup
KEM	Key Encapsulation Mechanism
KPI	Key Performance Indicator
LAMPS	Limited Additional Mechanisms for PKIX and SMIME
ML-DSA	Module-Lattice-based Digital Signature Standard
ML-KEM	Module-Lattice-based Key-Encapsulation Mechanism Standard
MWC	Mobile World Congress
NFV	Network Functions Virtualization

NIST	National Institute of Standards and Technology
NSPR	Netscape Portable Runtime
NSS	Network Security Services
OQS	Open Quantum Safe
OSG	Open Source Group
OSM	Open Source MANO
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public-Key Infrastructure using X.509
PoC	Proof of Concept
PP	Partnership Project
PQ/T	Post-Quantum/Traditional
PQ	Post-Quantum
PQC	Post-Quantum Cryptography
PQTN	Post-Quantum Telco Network Taskforce
PQUIP	Post-Quantum Use In Protocols
PSA	Platform Security Architecture
QIRG	Quantum Internet Research Group
QKD	Quantum Key Distribution
QUBIP	Quantum-oriented Update to Browsers and Infrastructures for the Post-quantum transition
RAN	Radio Access Network
RFC	Request For Comments
S/MIME	Secure Multipurpose Internet Mail Extensions
SA	Services & Systems Aspects
SDG	Software Development Group
SDN	Software-Defined Networking
SDO	Standards Development Organisation
SKEX	Symmetric Key Exchange
SSI	Self-Sovereign Identity
SSL	Secure Sockets Layer
TC	Technical Committee
TCG	Trusted Computing Group
TFS	TeraFlow SDN
TLS	Transport Layer Security
TNC	Trusted Network Communications
TPM	Trusted Platform Module
TSG	Technical Specification Group
VC	Verifiable Credential
VCWG	Verifiable Credentials Working Group
W3C	World Wide Web Consortium
WG	Working Group
WIMSE	Workload Identity in Multi System Environments
ZK	Zero-Knowledge
ZSM	Zero-Touch Network and Service Management

1. Introduction

This document contains the first version of the QUBIP project plan for contributions to standardisation bodies, industry associations, and open source communities. Its purpose is to outline various strategies for influencing the communities involved in standardisation and open source software development. The deliverable D4.4 “Standardization plan and activities (initial version)” is issued at M12 (i.e., August 2024). It is a living document that will be updated periodically throughout the life of the project, not only to reflect new plans, but also to report on activities undertaken and results achieved.

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

2. General Strategy

This document outlines different strategies for influencing the communities involved in standardisation and open source software development.

Openly available standards are key to ensuring that different devices and systems can share information and work together, not only when connected to the Internet, but also in all kinds of network services. In addition, without open standards, the development, integration, and deployment of new security features becomes much more difficult.

This is certainly the case with the transition to Post-Quantum Cryptography (PQC), where the application of new algorithms, and the required evolution of protocols and services should be done carefully to maintain backward compatibility with legacy systems as new solutions consolidate.

Open source communities share a similar goal, but take an alternative approach by making software solutions and source code directly available. The goal of these communities is to make solution implementations openly available so that they can be used and adapted, fostering consensus among global players to use the applied technologies.

Finally, the ability to reach consensus within the industry through targeted initiatives that act as precursors to standardisation helps to identify industry needs and to incorporate practical knowledge from practical experience with specifications and reference implementations.

Given industrial impact is a key objective of the QUBIP project, there is therefore a strong interest in integrating the solutions it develops into these open groups and in establishing consensus among stakeholders at a global level regarding the adoption of project outcomes.

The QUBIP partners will track their participation in the aforementioned activities that will contribute to the project objectives, ensuring proper acknowledgement according to each organisation's guidelines. This will allow the project to conduct ongoing impact assessments, addressing the Key Performance Indicators (KPIs) defined in the project and reflected in the Table 2.1.

Table 2.1: Key Performance Indicators

Key Performance Indicators	Description	Value
KPI33	Accepted contributions to standards bodies related to transition to PQC.	> 10
KPI34	Significant contributions to open-source projects related to transition to PQC.	> 3

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

3. Targeted Standardization Bodies

3.1. ETSI

The European Telecommunications Standards Institute (ETSI) is a standardisation organisation recognised by the European Union, and widely adopted as a global reference standardisation body. ETSI was created with the goal of producing standards for Information and Communication Technologies (ICT), including fixed, mobile, radio, converged, broadcast and Internet technologies. More than 800 organisations are members of ETSI, covering 64 countries all over the world. The standardisation activities are structured in committees, each addressing specific technology areas or standardisation goals. The main types of committees within ETSI include:

- Technical Committee (TC): Responsible for standardisation activities in specific technology areas.
- ETSI Project (EP): Similar to a Technical Committee but established for a fixed period.
- ETSI Partnership Project (PP): Formed to collaborate with other organisations to achieve standardisation goals, with 3rd-Generation Partnership Programme (3GPP) being the most notable example.
- Industry Specification Group (ISG): Focuses on specific activities, operating alongside traditional standards-making mechanisms.
- Software Development Group (SDG): Recently introduced to handle the production of open-source reference solutions.

The work program of each committee is established and maintained by ETSI members, comprising individual work items. While ongoing work items present opportunities for project influence and contribution, the project can also propose new items based on particularly relevant results.

In terms of the opportunity for impact they offer to the QUBIP project, the most relevant committees are:

- TC for Cybersecurity (TC CYBER) provides standards applicable across different domains, for the security of infrastructures, devices, services, protocols, and to create security tools and techniques. The Cyber Quantum-Safe Cryptography working group has been created as a specific Working Group (WG) inside TC CYBER to study the threat of quantum computers to current encryption methods by evaluating and recommending new algorithms primitives and implementation considerations. Their main focus is on practical implementations, performance aspects, or architectural considerations.
- ISG Network Functions Virtualization (NFV) is related to the virtualisation of network functions, that reflect the importance of this technology. The SEC WG is the security group that addresses aspects related to information, network and communications security, individual machines/processes, tools, controls, and techniques. Potential areas for contributing are the ones related to the adoption of quantum-safe technologies, including the execution of demonstrative deliverables, known as Proof of Concept (PoC), to provide evidence on how to apply QUBIP solutions in virtualised telco environments.
- ISG Quantum Key Distribution (QKD) was set in 2008 as a pioneer initiative for quantum-safe communications. Since then, many Standards Development Organisations (SDOs) have started to work on this and related quantum technologies. ISG QKD has produced more than twenty documents on detailed specifications, for example: key distribution interfaces (ETSI GS QKD 014 [1], ETSI GS QKD 004 [2]); the application of Software-Defined Networking (SDN) controllers to QKD systems (ETSI GS QKD 015 [3]) and orchestrators (ETSI GS QKD 018 [4]); a protection profile to prepare

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

and measure link (ETSI GS QKD 016 [5]). Other relevant documents in preparation are about a monitoring interface for QKD system, and cross-domain interactions for key distribution.

- ISG Zero-Touch Network and Service Management (ZSM) has been focusing for almost eight years on network service automation, emphasising closed-loops, intent-based network management and AI-driven automation. The group is concerned as well with security automation and the security requirements of the different automation technologies, making it a relevant target for QUBIP contributions and PoC proposals.

3.2. IETF/IRTF

The Internet Engineering Task Force (IETF) [6] acts as the main standards development organisation for the Internet. The primary function of IETF is to improve the Internet by producing technical documents that influence the way people continue to develop and manage the Internet.

A WG is the smallest unit inside the IETF where the technical work is done. The working groups are organised into several areas such as routing, security, and transport. The IETF operates by developing technical documents known as Request For Comments (RFC), which, after undergoing a formal approval process, are the primary publications that define protocols, policies, procedures, and concepts for the Internet. Internet-Drafts (I-Ds) are working documents submitted by individuals or groups to the IETF, which might be adopted by the relevant IETF WG, and through collective open discussions and revisions, may eventually be published as RFCs.

The Internet Research Task Force (IRTF) [7] is a parallel organisation to the IETF that focuses on the long-term research and development of the Internet. While the IETF is more focused on the promotion and development of standards, the IRTF takes on exploring new ideas. The work of the IRTF is organised into research groups that output informational or experimental RFCs as defined in the RFC 5743 [8].

The QUBIP project is mainly interested in the WGs and research groups that address the Post-Quantum (PQ) transition. Such groups inside IETF and IRTF are primarily Post-Quantum Use In Protocols (PQUIP), Crypto Forum Research Group (CFRG), Transport Layer Security (TLS), and Limited Additional Mechanisms for PKIX and SMIME (LAMPS), as detailed below.

- PQUIP [9] is an IETF WG that focuses on the integration of PQC into existing Internet protocols. Notably, PQUIP is maintaining a living document that tracks the state of PQC adoption and migration within and outside the IETF [10]. Recent and ongoing efforts within PQUIP include:
  - an I-D that explains the necessity of moving to PQC for engineers [11];
  - another I-D, which aims towards continuous tracking and categorizing emerging use cases [12] for PQC migration. Albeit not yet officially adopted, due to its relevance this draft is being actively discussed within the PQUIP WG.
  - A key aspect of the PQC Transition is the development of hybrid schemes. Therefore, to ensure consistency and clarity across different protocols, standards, and organisations, another adopted I-D [13] acts as glossary for the terminology concerning the hybridization of Traditional and PQ cryptography, i.e. Post-Quantum/Traditional (PQ/T) hybrids.
  - Yet another adopted I-D [14] explores design goals, security considerations, and their classification for hybrid digital signature schemes, examining concepts such as non-separability, interoperability, hybrid generality, and simultaneous verification.

    The discussion around this draft is of particular relevance for QUBIP, as it directly affects the designs for authentication in the PQ/T Hybrid setting, which fits the latest recommendations for the PQC transition.
- CFRG [15] is an IRTF research group characterised by their statement of serving as a bridge between theory and practice. Their goal is to introduce and promote new cryptographic techniques

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

for the use of the Internet community. As their name suggests, they are also providing a forum for discussion and questions concerning the subject.

Within the CFRG' activities related to PQC, a design team has been formed, to produce a document focusing on PQ/T Hybrid Key Encapsulation Mechanisms (KEMs). In QUBIP we are monitoring the initial output from this design team, and the follow-up discussions on the CFRG mailing list [16]. The design team will address the following:

- Identify KEM properties that are relevant for IETF.
- Provide a terse overview of well-reviewed techniques to safely produce the concrete combinations.
- Define an initial set of PQ/T Hybrid KEMs, covering different security levels, to match the current usage in widespread deployments of IETF protocols.

Additionally, since IETF 115, within the co-located IETF Hackathon, a group has been actively working on designs and experiments for the interoperable deployment of PQC within X.509 [17], to which we have been participating since before the start of the QUBIP project. To date, the major goals of these endeavours have been:

- Integrating PQ algorithms support into existing `X.509` structures and ensuring support across a diverse set of implementations, while following the updates around the various standardization efforts.
- Establishing a repository for automatic interoperability testing across different implementations.
- Creating a comprehensive compatibility matrix to document the collected results.
- Provide feedback about practical usage to the relevant IETF WGs.

- TLS [18] is an IETF WG that works on the homonymous protocol for ensuring secure communication over the Internet, providing confidentiality, integrity, and authentication. The evolution of the TLS protocol began after its predecessor Secure Sockets Layer (SSL) 3.0. The TLS 1.0 [19], TLS 1.1 [20], TLS 1.2 [21], and TLS 1.3 [22] versions have been developed and maintained by the TLS WG within IETF.
  - Recent PQC work addresses the use of PQ/T Hybrid Key Exchange in TLS 1.3 [23], to simultaneously use multiple key exchange algorithms and combine their results for achieving security.

    While this draft targets generic support for Hybrid Key Exchange in TLS 1.3, currently two more individual I-Ds instantiate it for specific combinations of Traditional Key Exchange algorithms with PQ KEMs:
    - `X25519Kyber768Draft00` [24] combines `X25519` [25] with `Kyber768` [26]. It has been deployed at scale at Google and Cloudflare, and is currently experimentally supported in official versions of Google Chrome and Mozilla Firefox.
    - `SecP256r1Kyber768Draft00` [27] combines National Institute of Standards and Technology (NIST) `P-256` [28] with `Kyber768` [26]. It derives TLS session keys with the same equivalent level of security of the I-D above, but adopting Federal Information Processing Standards (FIPS)-approved schemes.
  - Additionally, within the TLS WG, we are also monitoring the development of another I-D [29], which defines two Module-Lattice-based Key-Encapsulation Mechanism Standard (ML-KEM) (i.e., FIPS 203 [30]) parameter sets, `ML-KEM-768` and `ML-KEM-1024`, as standalone `NamedGroups` for use in TLS 1.3. This draft targets deployments using *exclusively* PQC for key exchange, rather than PQ/T hybridization, while in QUBIP we aim for PQ/T Hybrid solutions for the PQC transition.
- The LAMPS WG [31] is focused on developing extensions and improving Public Key Infrastructure (PKI); in particular Public-Key Infrastructure using X.509 (PKIX) [32], and Secure Multipurpose

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

Internet Mail Extensions (S/MIME) [33] and Cryptographic Message Syntax (CMS) [34] protocols. In the context of QUBIP, LAMPS' most relevant ongoing work related to PQC includes a few I-Ds:

- `draft-ietf-lamps-dilithium-certificates` [35] deals with the adoption of Module-Lattice-based Digital Signature Standard (ML-DSA) (i.e., FIPS 204 [36]) in PKIX [32].
- `draft-ietf-lamps-pq-composite-sigs` [37] addresses the use of ML-DSA composite signatures (i.e., PQ/T hybrid authentication) both in PKIX [32] and in the CMS [34] protocol.
- `draft-ietf-lamps-kyber-certificates` [38] defines algorithm identifiers and Abstract Syntax Notation One (ASN.1) encoding formats for ML-KEM in public key certificates.
- `draft-ietf-lamps-pq-composite-kem` [39] describes composite KEM solutions for use within PKIX [32] and the CMS [34] protocol.

3.3. 3GPP

The 3GPP covers cellular telecommunications technologies, including Radio Access Network (RAN), the core network, and service capabilities. These components collectively describe a comprehensive mobile telecommunications system. 3GPP specifications, also facilitate non-radio access to the core network and interoperability with non-3GPP networks.

Contributions from member companies drive 3GPP studies and specifications through WGs and Technical Specification Groups (TSGs). The three TSGs within 3GPP are RAN, Services & Systems Aspects (SA), and Core Network & Terminals (CT). The 3GPP release cycle spans approximately 15 months, with plenary sessions approving release content before each cycle begins.

The Security and Privacy Working Group 3 (SA WG 3), commonly referred to as SA3 [40], is responsible for security and privacy matters within 3GPP. SA3 defines security and privacy requirements, specifies security architectures and protocols, and evaluates cryptographic algorithms for inclusion in specifications. The reference document in this group is the TS33.501 [41], that defines the general security architecture. A dedicated subgroup, SA3-LI, focuses on lawful interception requirements and specifications. Furthermore, SA3 collaborates with the 3GPP Mobile Competence Centre to establish a Coordinated Vulnerability Disclosure (CVD) process, allowing the reporting and resolution of suspected or confirmed vulnerabilities in 3GPP specifications.

The nature of SA3 WG makes it a relevant target for the QUBIP project, and it has potential impacts on aspects related to the evolution of mobile communications to address the transition to PQC.

3.4. ITU-T

International Telecommunication Union (ITU) is the United Nations specialised agency for information and communication technologies, and International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) is the ITU telecommunication standardisation sector. Its mission is to develop international standards, known as ITU-T Recommendations. Those are created through Study Groups, made up from experts all around the world, and each Study Group is organised into a number of working parties. Each Study Group is focused on a specific theme, such as operational aspects, future networks, security, etc. The development workflow is the following. First, an organisation (member of ITU-T) identifies an issue of need of standardisation and submits the suggested research item to the relevant ITU-T Study Group. Then, if the idea is approved by the Study Group, the work is driven primarily in the form of study question and it is allocated to a Working Party. The development of a new draft for a ITU-T Recommendations starts, and when the draft is considered mature, it is moved forward into the alternative approval procedure to be approved.

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

The Study Group 17 (SG17) focuses on building confidence and security in the use of ICT. In particular, SG17 has a significant emphasis on quantum-based security, recognising its growing importance in the face of advancing quantum computing technologies. This involves developing standards and frameworks for QKD networks, considering aspects relevant for general key distribution mechanisms in qunatum-safe environments. In particular, recommendations like ITU-T X.1712 [42] address key management aspects, providing guidelines on the design, implementation, and operation of these systems. By creating robust security standards for quantum and quantum-safe technologies, SG17 aims to fortify ICT infrastructure, ensuring it remains resilient and secure against the potential risks introduced by quantum computing. The technical report XSTR-HYB-QKD [43] consists of an overview of hybrid approaches for key exchange with QKD. This report is relevant for the hybridisation of QKD/PQC work in QUBIP.

3.5. CEN/CENELEC

The European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC) are private, non-profit organizations that develop voluntary European standards. Their stakeholders include businesses, industry, public authorities, academia, and various interest groups. These standards ensure quality, safety, and interoperability, supporting European competitiveness and sustainable growth. CEN and CENELEC collaborate closely with international bodies like International Standards Organisation (ISO) to promote global standardisation. They work with the European Commission and EFTA to ensure standards support EU legislation, reinforcing the single market. Over 200,000 technical experts contribute to their extensive network.

The CEN and CENELEC Joint Technical Committee 22 (CEN/CLC/JTC 22 [44]) is developing standards for quantum technologies. Established in 2022, it builds on two deliverables by the CEN and CENELEC Focus Group on Quantum Technologies (FGQT): Standardization Roadmap on Quantum Technologies, and Quantum Technologies Use Cases. This group aims to produce standards covering quantum metrology, computing, communication, and other areas relevant to quantum technologies. The committee also collaborates with international standards bodies like ISO/IEC JTC 1 and coordinates closely with stakeholders including the European Quantum Flagship and Quantum Industry Consortium. The work of CEN/CLC/JTC 22 is organized in a plenary committee and four WGs.

CEN/CENELEC, specifically through their FGQT, have developed comprehensive documentation covering terminology, work plans, standardisation road-maps, and use cases for quantum technologies, including quantum communications. This makes them a pivotal entity for consideration within the QUBIP project.

3.6. W3C

The World Wide Web Consortium (W3C) [45] develops standards and guidelines to help everyone build a web based on the principles of accessibility, internationalisation, privacy, and security. The W3C is relevant to the QUBIP project because of its activities in the specification of Decentralised IDentifiers (DIDs) and Verifiable Credentials (VCs), two key technologies at the core of Self-Sovereign Identity (SSI) [46].

The Decentralised Identifier Working Group (DIWG) has a dual mission. The DIWG maintains the DID specification, and seeks consensus on the best way to achieve effective interoperability through common requirements, algorithms, architectural options, and various considerations for the DID resolution and DID URL dereferencing processes. The relevant documents so far are:

- Decentralised Identifiers v1.0 [47]: this W3C Recommendation specifies the DID syntax, a common data model, core properties, serialised representations, DID operations, and an explanation of the process of resolving DIDs to the resources that they represent.

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

- DID Specification Registries [48]: this note serves as an official registry of all known global parameters, properties, and values used by the DID ecosystem. In addition, this note summarises the DID method specifications currently under development, and essentially serves as a mechanism for developers to discover various DID methods that they may wish to implement.

The Verifiable Credentials Working Group (VCWG) is responsible for maintaining the Verifiable Credentials Data Model. The relevant documents so far are two candidate recommendation drafts:

- Verifiable Credentials Data Model v2.0 [49]: this specification provides a mechanism to express credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable.
- Bitstring Status List v1.0 [50]: this specification describes a privacy-preserving, space-efficient, and high-performance mechanism for publishing status information, such as suspension or revocation of VCs, using bitstrings.

While the specifications maintained by the DIWG and VCWG are important references for QUBIP activities on the transition to PQC of the SSI in the context of web browsing, the WGs represents an opportunity for QUBIP to disseminate, influence and contribute to future updates of the specifications to address quantum threats.

3.7. ENISA

The European Union Agency for Cybersecurity (ENISA) details the available standardisation outputs on the cybersecurity of products (including hardware and software components) carried out mainly by European Standardisation Organisations (ESOs) and international SDOs in the report “Cyber resilience act requirements standards mapping” [51]. It considers the following standards related to Internet of Things (IoT) devices, and the project could provide evidence of their applicability and any necessary adaptation:

- ETSI EN 303 645 V2.1.1 (2020-06) – Cyber Security for Consumer Internet of Things – Baseline Requirements: defines cybersecurity provisions for consumer IoT devices such as recommendations on the use of default passwords on the devices, secure storage of sensitive parameters and the management of the credentials (e.g., password generation, user authentication and change of default values). It contains provisions on systems’ resilience to outages, including mitigation against Distributed Denial of Service (DDoS) attacks.
- ITU-T Y.4810 (11/2021) – Requirements for Data Security of Heterogeneous Internet of Things Devices: defines some specific requirements for data transfer to and from heterogeneous IoT devices, in particular (*i*) it is required the function of data transfer to and from an IoT device – the process of a specific type of data transfer is required to be initiated only with explicit permission of end users, and (*ii*) it is required to have the anti-interference ability between the IoT device and network equipment.

In 2022, ENISA published an integration study of PQC and identifies the challenges to implementing PQC on digital systems [52], as well as standardisation efforts for protocols and standards adapted to PQC.

3.8. ISO

The ISO brings global experts together to agree on the best way of doing things, while standardising several different kinds of processes. An adequate implementation of eIDAS 2.0 should be conducted taking into account the security threats associated to quantum computing. In this regard, it is necessary to address the global challenge of implementing advance identity management framework allowing to differentiate between identity providers and relying parties.

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

From April 2024, ISO/IEC JTC 1/SC 27/WG 5 [53] has created an ad-hoc group to further discuss the main implications of digital wallets. There are also several projects and work items related to digital wallets in different ISO committees. The ISO/JTC 1/SC 27/WG 5 AHG/44-2 [53] is going to focus on establishing coordination among all these committees, having as one major reference the work already carried out in ISO/IEC JTC 1/SC 17/AG 3 – Digital Wallets [54]. A critical point on this matter is related to improving the current security model of digital wallets to foster quantum preparedness by means of adequate crypto-agility approaches.

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

4. Targeted Industrial Groups

4.1. GSMA

The Global System Mobile Association (GSMA) has been the leading organisation for the mobile industry, dating back to the very beginning of digital mobile technology. Initially focused on mobile network operators, the GSMA is now bringing together a wide variety of mobile ecosystem key players, including handset manufacturers, software equipment providers, Internet companies, and media.

The GSMA organises its works around common interests and goals within WGs in different matters, and uses Committees, like the Strategy Committee or Public Policy Committee, to set the overall direction for the WGs and ensure their projects align with the GSMA broader goals. Also, the GSMA utilises Task Forces alongside their working groups to address specific industry challenges or opportunities.

The bigger opportunity for QUBIP project today is the Post-Quantum Telco Network Taskforce (PQTN), which tries to address the challenges of securing mobile networks against future advancements in quantum computing, including impacts in the technology and infrastructure, use cases and guidelines to address the threat and transition [55, 56].

4.2. TCG

The Trusted Computing Group (TCG) [57] is an international industry standards group that develops and promotes open, vendor-neutral, global industry standards for trusted computing platforms. Established in 2003, TCG's primary mission is to enhance the security and trustworthiness of computing environments by creating specifications and tools that ensure the integrity and confidentiality of information and systems. TCG's members include a broad range of stakeholders such as hardware manufacturers, software developers, and system integrator, all working together to establish a baseline for trusted computing.

TCG's initiatives span several areas, including secure hardware, network security, and trusted infrastructure. Their work is widely adopted in industries ranging from finance and healthcare to government and telecommunications. By providing a foundation for building secure systems, TCG plays a crucial role in mitigating risks associated with digital threats and vulnerabilities.

The TCG includes different WGs that are related to key technologies developed in this context. The main products developed within the TCG are:

- Trusted Platform Module (TPM) [58], which is a secure crypto-processor that provides secure generation and storage of cryptographic keys, as well as secure boot and measured boot.
- Device Identifier Composition Engine (DICE) [59], an open architecture that enhances the security and privacy of IoT and embedded devices.
- Trusted Network Communications (TNC) [60], an open architecture for interoperable end-to-end trust in multivendor environments across a wide variety of endpoints, network technologies, and policies. TNC enables endpoint compliance evaluation, intelligent policy decisions, dynamic security enforcement, and security automation between disparate networking and security systems.

The technologies considered by the TCG are interesting opportunities for the QUBIP project. The challenge is to contribute in how to integrate PQC in the technologies mentioned above. This is currently being investigated, especially regarding the TPM [61] [62].

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

4.3. 6G-IA

The 6G Smart Networks and Services Industry Association (6G-IA) is the voice of European Industry and Research for next generation networks and services. Its primary objective is to contribute to Europe's leadership on 5G, 5G evolution and SNS/6G research. The 6G-IA brings together a global industry community of telecommunications and digital actors, such as operators, manufacturers, research institutes, universities, verticals, SMEs, and ICT associations.

The 6G-IA carries out a wide range of activities in strategic areas including standardisation, frequency spectrum, R&D projects, technology skills, collaboration with key vertical industry sectors, notably for the development of trials, and international cooperation. Activities within the 6G-IA are structured around WGs [63], formed to address certain issues and publish consolidated views established within the community. These WGs produce periodic white papers, specific reports and sponsor demonstration activities to which the project would be able to contribute, especially those that constitute a natural target for project results, namely:

- The Vision WG, developing a comprehensive scientific, technological and socio-economic vision for the upcoming next generation mobile system. The WG maintains a high-level technology roadmap, formulating a holistic view of the future networks, systems and their typical environments.
- The Open SNS WG, promoting and supporting the evaluation, adoption, deployment, and evolution of open solutions for 5G and beyond 5G/6G networks.
- The Pre-Standardisation WG, identifying standardisation and regulatory bodies to align with, and other relevant standards bodies. The group also keeps a roadmap of relevant standardisation and regulatory topics for 6G.

4.4. Eurosmart

Eurosmart [64], established in 1995, is a non-profit organization that gathers companies, institutions, and evaluation laboratories involved in the digital security market. Eurosmart's main mission is to advocate for a high level of security in digital interactions by promoting a strong and comprehensive approach to cyber resilience. Eurosmart has been involved in several activities towards the European institutions and stakeholders, bringing together the expertise of its members to promote and enable security for all digital markets and applications in a scalable way. Committee, task forces and working groups coordinated and/or operated by Eurosmart work on many security-related fields. The most relevant for the QUBIP project are:

- IoT Committee, bridging the Eurosmart community to the ETSI TC CYBER.
- JIL Hardware-related Attacks Subgroup (JHAS), that is an industry-led expert group operated by Eurosmart.
- IT and Security Committee (ITSC), which is in charge of addressing security evaluation and certification aspects occurring in the smartcard and secure element technical domains.

Recently, Eurosmart has been thoroughly involved in the definition of the PP-0117 V2 Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile [65] updates for the Common Criteria certification scheme in collaboration with the GSMA (not yet available at the time of writing). The PP-0017 V2 is particularly relevant for the QUBIP project, as it is representative of SoCs that can be found in IoT devices where security services are provided by an on-chip Root-of-Trust or Secure Element. The migration to PQC is still an open point from a functional and certification perspective, and it represents an opportunity for the QUBIP project to contribute to the future updates.

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

4.5. PSA Certified

Platform Security Architecture (PSA) Certified, originated from the Platform Security Architecture specifications created by ARM Limited, provides a security framework and independent third-party evaluation focusing on IoT security [66]. One important principle of PSA Certified is the Root of Trust built into the silicon. It is defined as a combination of the Immutable Platform RooT of Trust and the Updateable Platform Root of Trust, and PSA Certified considers this to be the most trusted security component on the device. The system software and the device leverage this Root of Trust, bringing confidentiality and integrity to the whole value chain. To achieve that, 10 main security principles have been outlined, based on best-practices in IoT security, that should be met by all connected products [67]. Multiple levels of silicon security have been designed that scale with silicon security robustness: from PSA level one to PSA level four. It is of value for the QUBIP project to be constantly informed about the decisions and solutions provided by PSA Certified, to participate in the discussion and finally to contribute to the specifications. The main idea is to focus on the context of the Root of Trust, as it is one of the key components that QUBIP is considering for the transition to PQC of the IoT.

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

5. Targeted Open Source Initiatives

5.1. Open Quantum Safe

The Open Quantum Safe (OQS) project [68] is dedicated to developing and prototyping PQC algorithms. It provides the liboqs library [69] that includes implementations of various PQC algorithms, which can be integrated into PKI systems to enhance their security against quantum threats. OQS also implements OQS provider [70] bringing PQ algorithms to OpenSSL [71] using its provider architecture. QUBIP activities include collaboration with the upstream project, which was selected as the functional compatibility target for our own QUBIP OpenSSL provider, as it explores the boundaries of the OpenSSL Provider Application Programming Interface (API) and challenges in the integration of PQC algorithms within the TLS and PKI stacks.

5.2. OpenSSL

OpenSSL [71] is a very popular open source cryptography toolkit, containing a fully featured TLS implementation as well as more granular features for working with keys, certificates, and digital signatures. OpenSSL offers support for dynamically extending its collection of cryptographic schemes and primitives via loadable modules known as “providers”. Starting with version 3.2, providers can offer full support of PQ and PQ/T hybrid cryptography in the TLS stack. Although the open source project OQS [68] maintains an OpenSSL provider that offers PQ and PQ/T hybrid cryptography through the algorithm implementations included in their `liboqs` library, their provider does not offer the ability to use other algorithm implementations. The QUBIP OpenSSL provider will serve as an interface layer enabling other researchers and developers to test and use their PQC algorithms in real-world scenarios. This interface layer will facilitate the integration and experimentation with new PQC schemes, thereby allowing OpenSSL to better adapt to the rapid changes in the developing PQC environment.

5.3. Network Security Services

The Network Security Services (NSS) [72] is another open-source cryptography toolkit, developed primarily by the Mozilla Foundation and tightly integrated with their popular browser, Mozilla Firefox [73]. NSS provides essential cryptographic functionality and enables secure browsing through TLS. The key components of NSS are `libnss` and `libnspr`, i.e. Netscape Portable Runtime (NSPR). To introduce PQC capabilities to NSS, we are developing a loadable module that utilises the NSS support for Public Key Cryptography Standards (PKCS) #11 [74]. In our approach, QUBIP NSS-Modules do not contain PQC algorithms directly, but link to external PQC software implementations. The goal for the QUBIP NSS approach is to establish a framework that allows for flexibility and rapid updates, as new PQC implementations can be integrated without altering the core NSS.

5.4. Mbed-TLS

The Mbed-TLS library [75], currently maintained and developed by the Trusted Firmware Project [76], is written in C language and implements essential cryptographic primitives at the core of the algorithms and protocols for securing data. In addition, Mbed-TLS includes the implementations of the TLS and

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

Datagram Transport Layer Security (DTLS) protocols, and offers extensive support for X.509 certificate manipulation. Mbed-TLS has been specifically designed for providing cryptographic functionalities with a small code footprint. This feature makes the library particularly well-suited for use in embedded systems, where memory and storage resources are limited. QUBIP is going to contribute to this initiatives the PQ solutions developed during the project.

5.5. Fedora Linux

Fedora [77] is a Linux distribution developed by the Fedora Project. The Fedora Project creates an innovative, free, and open source platform for hardware, clouds, and containers that enables software developers and community members to build tailored solutions for their users. Rapid release cycle is a major enabling factor in Fedora's ability to innovate. Being a center of innovation, Fedora Linux may include versions of software based on non-finalized specifications of PQ algorithms and protocols. Fedora Linux includes OpenSSL [71], NSS [72] and other cryptography libraries. As a part of QUBIP, `liboqs` library and `oqs-provider` implemented by OQS [68] were added to Fedora and are maintained as a regular part of the distribution. A Fedora based container for PQ experiments [78] implemented for QUBIP purposes is publicly available.

5.6. Mozilla Firefox

Firefox is an open-source Internet browser developed by the Mozilla Foundation [73]. Firefox has gained popularity due to its privacy and security features that provide the user a secure browsing experience. Within QUBIP, we are introducing PQC capabilities to Firefox by updating the set of security libraries it is built on, NSS. Our approach involves implementing loadable modules for NSS that will act as a framework, allowing other developers and researchers to test their PQC implementations in a real browsing environment.

5.7. IOTA Identity

The IOTA Identity [79] is a major open source initiative dealing with decentralised identity for people and things. The IOTA Identity is a widely used SSI library [80] written in the RUST language and is the result of a large open source, community-led SSI project maintained by the IOTA Foundation. The library implements the most common W3C and IETF standards and patterns for decentralised identity in both a Distributed Ledger Technology (DLT) agnostic and `iota` method specific manner. In essence, it is a general purpose SSI library and therefore the perfect target for QUBIP to contribute to the practical transition of the SSI ecosystem to PQC. It is worth noting that the IOTA Foundation funded the Identity Working Group (IWG) in 2023, to bring together industry and research to collaborate on the development of the IOTA Identity library and deliver significant improvements. The LINKS Foundation, partner of QUBIP, is an active member of the IWG and the IOTA Foundation is a member of the QUBIP Industrial and Institutional Advisory Board (IIAB). This collaborative structure is intended to facilitate the contribution of QUBIP results upstream for the benefit of the entire SSI community.

5.8. Kubernetes

Kubernetes, commonly referred to as K8s, is one of the most utilised open source systems for the management and orchestration of microservice-based applications (in this case, container-based environments) [81]. Part of the Linux Foundation, K8s enables the simple, agile and flexible deployment of complex

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

container-based applications by providing a wide set of tools that facilitates the instantiation of these elements into distributed architectures, whose nodes can be located in various geographical zones. Some of these tools include automatic application discovery, automated rollouts and rollbacks, self-healing environments, and other features. K8s has been chosen to host the telco services for the "Quantum-secure Software Network Environments for Telco Operators" pilot, and QUBIP will provide post-quantum capabilities to enable the secure communications between each of their components through the open-source tool L2S-M [82], which enables the creation of virtual networks in K8s clusters.

5.9. Open Source MANO

Open Source MANO (OSM) [83] is one of the main ETSI initiatives in open source (known as Software Development Groups), in an effort to provide an open source platform that enables effective management and orchestration of NFV functionalities. Naturally, OSM follows the ETSI standards for the composition, connectivity, and deployment of NFV functionalities in virtualisation environments. In this regard, OSM has supported the deployment of K8s-based network functions since its SEVEN Release [84], although it currently does not have native support to enable virtual networking in K8s clusters (necessary for the effective deployment of Network Services). Thanks to the efforts of L2S-M and its feature proposal "Connectivity among CNFs using SDN" (currently in the implementation phase) [85], OSM will be utilised by the "Quantum-secure Software Network Environments for Telco Operators" pilot to properly deploy its functionalities by providing its virtualised components secured communication to enable their function chaining in K8s environments. And this will provide the opportunity to contribute a quantum-safe environment for NFV orchestration and infrastructural networking.

5.10. TeraFlowSDN

TeraFlow SDN (TFS) [86] is an ETSI Software Development Group developing an open source cloud native SDN controller enabling smart connectivity services for future networks beyond 5G. Given it is tightly connected with OSM, the developments based on L2S-M will be suitable to be contributed here, enabling quantum-safe SDN stacks, and simplifying the use of PQC solutions in SDN environments.

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

6. First-year Activities

Several activities have been done in various SDOs and open source initiatives, spanning from September 2023 to August 2024. Key highlights include:

ETSI

- New work items (Wis) on testing and protection profiles for access and transport networks, associated with project goals and use cases in ETSI TC CYBER.
- Main proponent to define a monitoring interface development for QKD systems in ETSI ISG QKD.
- Long-term proposals for OSM and research projects in the context of Technical steering committee as part of ETSI Open Source Group (OSG) OSM.
- Participation to the ETSI Quantum-Safe Cryptography Conference (May 14-16, 2024) to establish links and introduce QUBIP.

GSMA

- Contributions to published guidelines for Quantum Risk Management [55] and Post Quantum Cryptography guidelines for Telecom Use [56] as part of the PQTN activities.
- Presentations at the Mobile World Congress (MWC) focusing on post-quantum seminars.

IETF related security and routing areas

- Contributions to Symmetric Key Exchange (SKEX) framework proposal for alternative mechanism to asymmetric encryption for key distribution.
- Incorporating hybridization QKD/PQC experiences in Quantum Internet Research Group (QIRG) at IRTF.
- Participating and supporting the creation of different WG impacted by quantum transition. These activities include discussion, presentations, and side meetings in IETF physical events. Some of the topics includes attestation, secure network paths, operational issues identification or cloud workloads identities.
- Participation through discussions and experiments on hackathon related to challenges/solutions of PQ migration of X.509.

3GPP

- Contributions to the Enablers for Zero Touch Security (eZTS) SID for the upcoming 3GPP Release 19 with considerations for evolved crypto and PKI.

ISO/IEC JTC SC 27

- Periodically participation and discussion on the ISO/JTC 1/SC 27/WG 5 AHG/44-2 (Digital Wallets), a group with interest on PQC and crypto-agility.

IOTA

- The IOTA Foundation integrated the `zkryptium` and `json-proof-token` libraries developed by the LINKS Foundation to add full support for Zero-Knowledge (ZK) VCs to the IOTA Identity library. These contributions not only provide a relevant enhancement for the SSI community, but also form the basis for the future transition of the IOTA Identity library to PQC.

The details about the specific groups and contributions are available in the Table A.1 of Appendix A.

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

7. Conclusions

This deliverable presents the plan for standardisation and participation in industry associations and open source initiatives. It also includes several results achieved during the first year of activity. The plans will be monitored and updated throughout the project lifetime to ensure that objectives are met and that corrective action can be taken quickly, if necessary. The updates are foreseen in D4.5 (M24) and D4.6 (M36). They will contain the list of activities carried out and results achieved, the critical evaluation of the 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] ETSI, “GS QKD 014 V1.1.1 – Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API”, 2019, https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf

[2] ETSI, “GS QKD 004 V2.1.1 – Quantum Key Distribution (QKD); Application Interface”, 2020, https://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/02.01.01_60/gs_QKD004v020101p.pdf

[3] ETSI, “GS QKD 015 V2.1.1 – Quantum Key Distribution (QKD); Control Interface for Software Defined Networks”, 2022, https://www.etsi.org/deliver/etsi_gs/QKD/001_099/015/02.01.01_60/gs_QKD015v020101p.pdf

[4] ETSI, “GS QKD 018 V1.1.1 – Quantum Key Distribution (QKD); Orchestration Interface for Software Defined Networks”, 2022, https://www.etsi.org/deliver/etsi_gs/QKD/001_099/018/01.01.01_60/gs_qkd018v010101p.pdf

[5] ETSI, “GS QKD 016 V1.1.1 – Quantum Key Distribution (QKD); Common Criteria Protection Profile – Pair of Prepare and Measure Quantum Key Distribution Modules”, 2023, https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/01.01.01_60/gs_QKD016v010101p.pdf

[6] IETF, “The Internet Engineering Task Force”, https://www.ietf.org/

[7] IRTF, “The Internet Research Task Force”, https://www.irtf.org/

[8] A. Falk, “Definition of an Internet Research Task Force (IRTF) Document Stream”, RFC-5743, December 2009, DOI 10.17487/rfc5743

[9] IETF, “Post-Quantum Use In Protocols (PQUIP) WG”, https://datatracker.ietf.org/wg/pquip/about/

[10] IETF PQUIP, “State of protocols and PQC”, https://github.com/ietf-wg-pquip/state-of-protocols-and-pqc, 2024

[11] A. Banerjee, T. Reddy.K, D. Schoinianakis, and T. Hollebeek, “Post-Quantum Cryptography for Engineers”, Internet Draft, May 2024, https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-engineers/04/

[12] A. Vaira, H. Brockhaus, A. Railean, J. Gray, and M. Ounsworth, “Post-quantum cryptography migration use cases”, Internet Draft, July 2024, https://datatracker.ietf.org/doc/draft-vaira-pquip-pqc-use-cases/02/

[13] F. Driscoll and M. Parsons, “Terminology for Post-Quantum Traditional Hybrid Schemes”, Internet Draft, May 2024, https://datatracker.ietf.org/doc/draft-ietf-pquip-pqt-hybrid-terminology/03/

[14] N. Bindel, B. Hale, D. Connolly, and F. Driscoll, “Hybrid signature spectrums”, Internet Draft, May 2024, https://datatracker.ietf.org/doc/draft-ietf-pquip-hybrid-signature-spectrums/00/

[15] IRTF, “Crypto Forum Research Group (CFRG)”, 2024, https://www.irtf.org/cfrg.html

[16] IRTF CFRG, “KEM Combiners Design Team Output”, 2024, https://mailarchive.ietf.org/arch/msg/cfrg/CwrVvm-J7o85TEWkG9RJxZwfXDY/

[17] IETF Hackathon, “PQC Certificates”, 2024, https://github.com/IETF-Hackathon/pqc-certificates?tab=readme-ov-file

[18] IETF TLS, “Transport Layer Security (TLS) WG”, https://datatracker.ietf.org/wg/tls/about/

[19] C. Allen and T. Dierks, “The TLS Protocol Version 1.0”, RFC-2246, January 1999, DOI 10.17487/RFC2246

[20] T. Dierks and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.1”, RFC-4346, April 2006, DOI 10.17487/RFC4346

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

[21] E. Rescorla and T. Dierks, “The Transport Layer Security (TLS) Protocol Version 1.2”, RFC-5246, August 2008, DOI 10.17487/RFC5246

[22] E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.3”, RFC-8446, August 2018, DOI 10.17487/RFC8446

[23] D. Stebila, S. Fluhrer, and S. Gueron, “Hybrid key exchange in TLS 1.3”, Internet Draft, April 2024, https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/10/

[24] B. Westerbaan and D. Stebila, “X25519Kyber768Draft00 hybrid post-quantum key agreement”, Internet Draft, September 2023, https://datatracker.ietf.org/doc/draft-tls-westerbaan-xyber768d00/03/

[25] S. Turner, A. Langley, and M. Hamburg, “Elliptic Curves for Security”, RFC-7748, January 2016, DOI 10.17487/rfc7748

[26] P. Schwabe and B. Westerbaan, “Kyber Post-Quantum KEM”, Internet Draft, January 2024, https://datatracker.ietf.org/doc/draft-cfrg-schwabe-kyber/04/

[27] K. Kwiatkowski and P. Kampanakis, “Post-quantum hybrid ECDHE-Kyber Key Agreement for TLSv1.3”, Internet Draft, May 2023, https://datatracker.ietf.org/doc/draft-kwiatkowski-tls-ecdhe-kyber/01/

[28] E. Barker, L. Chen, A. Roginsky, A. Vassilev, and R. Davis, “Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography”, April 2018, https://doi.org/10.6028/nist.sp.800-56ar3

[29] D. Connolly, “ML-KEM Post-Quantum Key Agreement for TLS 1.3”, Internet Draft, March 2024, https://datatracker.ietf.org/doc/draft-connolly-tls-mlkem-key-agreement/01/

[30] NIST, “FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard”, August 2024, DOI 10.6028/NIST.FIPS.203

[31] IETF LAMPS, “Limited Additional Mechanisms for PKIX and SMIME (LAMPS) WG”, https://datatracker.ietf.org/wg/lamps/about/

[32] S. Boeyen, S. Santesson, T. Polk, R. Housley, S. Farrell, and D. Cooper, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, RFC-5280, May 2008, DOI 10.17487/RFC5280

[33] J. Schaad, B. C. Ramsdell, and S. Turner, “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification”, RFC 8551, April 2019, DOI 10.17487/RFC8551

[34] R. Housley, “Cryptographic Message Syntax (CMS)”, RFC 5652, September 2009, DOI 10.17487/RFC5652

[35] J. Massimo, P. Kampanakis, S. Turner, and B. Westerbaan, “Internet X.509 Public Key Infrastructure: Algorithm Identifiers for ML-DSA”, Internet Draft, July 2024, https://datatracker.ietf.org/doc/draft-ietf-lamps-dilithium-certificates/04/

[36] NIST, “FIPS 204: Module-Lattice-Based Digital Signature Standard”, August 2024, DOI 10.6028/NIST.FIPS.204

[37] M. Ounsworth, J. Gray, M. Pala, J. Klaußner, and S. Fluhrer, “Composite ML-DSA for use in Internet PKI”, Internet Draft, July 2024, https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs/02/

[38] S. Turner, P. Kampanakis, J. Massimo, and B. Westerbaan, “Internet X.509 Public Key Infrastructure – Algorithm Identifiers for Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)”, Internet Draft, March 2024, https://datatracker.ietf.org/doc/draft-ietf-lamps-kyber-certificates/03/

[39] M. Ounsworth, J. Gray, M. Pala, J. Klaußner, and S. Fluhrer, “Composite ML-KEM for Use in the Internet X.509 Public Key Infrastructure and CMS”, Internet Draft, July 2024, https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-kem/04/

[40] 3GPP SA, “SA WG3 – Security and Privacy”, 2024, https://www.3gpp.org/3gpp-groups/service-system-aspects-sa/sa-wg3

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

[41] 3GPP, “TS 133 501 – 5G; Security architecture and procedures for 5G System”, 2024, https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/18.05.00_60/ts_133501v180500p.pdf

[42] ITUT SG17, “X.1712 : Security requirements and measures for quantum key distribution networks – key management”, 2021, https://www.itu.int/rec/T-REC-X.1712-202110-I

[43] ITUT SG17, “XSTR-HYB-QKD – Overview of hybrid approaches for key exchange with quantum key distribution”, 2022, https://www.itu.int/pub/T-TUT-ICTS-2022-1

[44] CEN/CENELEC, “CEN/CENELEC Quantum Technologies”, https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/quantum-technologies/

[45] W3C, “The World Wide Web Consortium”, https://www.w3.org/

[46] A. Preukschat and D. Reed, “Self-Sovereign Identity – Decentralized digital identity and verifiable credentials”, Manning, 2021, ISBN: 9781617296598. https://www.manning.com/books/self-sovereign-identity

[47] W3C, “Decentralized Identifiers (DIDs) v1.0. Core architecture, data model, and representations. W3C Recommendation”, 2022, https://www.w3.org/TR/did-core/

[48] W3C, “DID Specification Registries. The interoperability registry for Decentralized Identifiers. W3C Group Note”, 2024, https://www.w3.org/TR/did-spec-registries/

[49] W3C, “Verifiable Credentials Data Model v2.0. W3C Candidate Recommendation Draft”, 2024, https://www.w3.org/TR/vc-data-model-2.0/

[50] W3C, “Bitstring Status List v1.0: Privacy-preserving status information for Verifiable Credentials. W3C Working Draft”, 2024, https://www.w3.org/TR/vc-bitstring-status-list/

[51] J. L. H. Ramos, G. Karopoulos, I. N. Fovino, R. Spigolon, L. Sportiello, G. Steri, S. Gorniak, P. Magnabosco, R. Atoui, and C. C. Martinez, “Cyber Resilience Act Requirements Standards Mapping, Publications Office of the European Union”, 2024, https://publications.jrc.ec.europa.eu/repository/handle/JRC137340

[52] D. J. Bernstein, A. Hülsing, and T. Lange, “Post-Quantum Cryptography – Integration study”, 2022, https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study

[53] ISO/IEC JTC 1/SC 27, “WG 5 – Identity Management and Privacy Technologies”, https://committee.iso.org/sites/jtc1sc27/home/projects.html

[54] ISO/IEC JTC 1/SC 17, “AG 3 – Digital Wallets”, https://www.iso.org/committee/45144.html

[55] GSMA, “Guidelines for Quantum Risk Management for Telco”, https://www.gsma.com/aboutus/workinggroups/resources/guidelines-for-quantum-risk-management-for-telco

[56] GSMA, “Post Quantum Cryptography Guidelines for Telecom Use Cases”, https://www.gsma.com/newsroom/gsma_resources/pq-03-post-quantum-cryptography-guidelines-for-telecom-use-cases/

[57] TCG, “Trusted Computing Group”, https://trustedcomputinggroup.org

[58] TCG, “TPM 2.0 Library”, https://trustedcomputinggroup.org/resource/tpm-library-specification/

[59] TCG, “DICE WG”, https://trustedcomputinggroup.org/work-groups/dice-architectures/

[60] TCG, “Trusted Network Communications (TNC) WG”, https://trustedcomputinggroup.org/work-groups/trusted-network-communications/

[61] S. Paul, F. Schick, and J. Seedorf, “TPM-Based Post-Quantum Cryptography: A Case Study on Quantum-Resistant and Mutually Authenticated TLS for IoT Environments”, 16th International Conference on Availability, Reliability and Security, Vienna (Austria), 2021, DOI 10.1145/3465481.3465747

[62] Infineon, “Future-proof security solution: Infineon launches world’s first TPM with a PQC-protected firmware update mechanism”, https://www.infineon.com/cms/en/about-infineon/press/market-news/2022/INFCSS202202-051.html

[63] 6G-IA, “6G IA Working Groups”, https://6g-ia.eu/6g-ia-working-groups/

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

[64] Eurosmart, “Eurosmart – The Voice of the Digital Security Industry”, https://www.eurosmart.com/

[65] Eurosmart, “Eurosmart Unveils Ground-breaking PP-0117 V2 Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile”, https://www.eurosmart.com/tag/pp-0117-v2/

[66] ARM Limited, “Using the PSA Certified IoT Security Framework”, https://www.psacertified.org/what-is-psa-certified/using-psa-certified/

[67] ARM Limited, “The PSA Certified 10 Security Goals Explained”, https://www.psacertified.org/blog/psa-certified-10-security-goals-explained/

[68] Open Quantum Safe, “Open Quantum Safe project”, https://openquantumsafe.org/

[69] Open Quantum Safe project, “liboqs”, https://openquantumsafe.org/liboqs/

[70] Open Quantum Safe project, “OQS OpenSSL provider”, https://openquantumsafe.org/applications/tls.html#oqs-openssl-provider

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

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

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

[74] OASIS, “PKCS#11 Technical Committee”, https://groups.oasis-open.org/communities/tc-community-home2?CommunityKey=922ef643-1e10-4d65-a5ea-018dc7d3f0a4

[75] Trusted Firmware project, “MbedTLS library”, https://github.com/Mbed-TLS/mbedtls

[76] Trusted Firmware project, “Trusted firmware, Open Source Secure Software”, https://www.trustedfirmware.org/

[77] Fedora project, “Fedora Linux”, https://fedoraproject.org/

[78] S. Prasad, “Fedora PQ container”, https://gitlab.com/sahprasa/pq-container

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

[80] IOTA Foundation, “IOTA Identity library”, https://github.com/iotaledger/identity.rs

[81] Linux Foundation, “Kubernetes: Production-Grade Container Orchestration”, https://kubernetes.io

[82] L. F. Gonzalez, I. Vidal, F. Valera and D. R. Lopez, “Link-Layer Secure connectivity for Microservice platforms (L2S-M)”, http://l2sm.io

[83] ETSI, “Open Source MANO (OSM)”, https://osm.etsi.org

[84] ETSI, “OSM Realese SEVEN: Container Network Functions and More”, https://osm.etsi.org/news-events/blog/64-osm-release-seven-container-network-functions-and-more

[85] L. F. Gonzalez, I. Vidal, F. Valera, B. Nogales, Diego R. Lopez, “Feature 10921: Connectivity among CNFs using SDN”, https://osm.etsi.org/gitlab/osm/features/-/issues/10921

[86] ETSI SDG, “ETSI Software Development Group TeraFlowSDN”, https://tfs.etsi.org

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

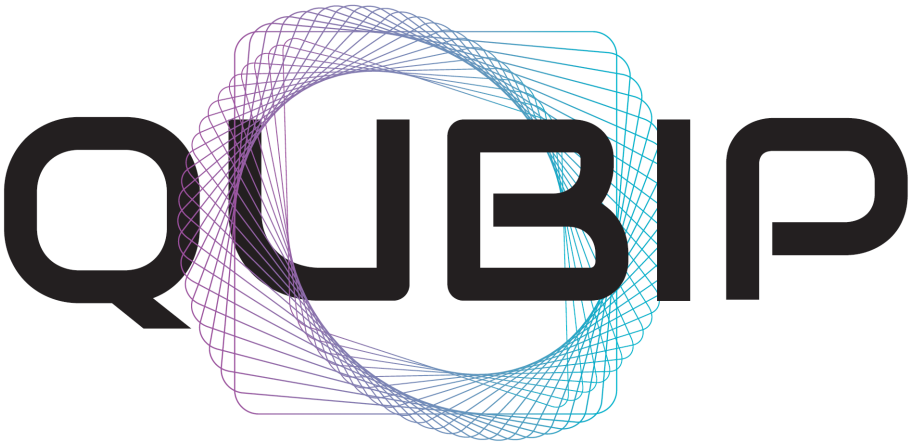
A. List of Contributions

The Table A.1 shows the list of tracked contributions to standardisation, industry associations and open source initiatives.

Date	SDO/Project/Organization	Activity	Description
23/09/23	ETSI TC CYBER	Charter	New Wis on testing and protection profiles for access and transport networks
29/09/23	GSMA PQTN	Publication	Guidelines for Quantum Risk Management for Telco
21/10/23	IETF JOSE	Contribution	Revision and Contribution to draft-ietf-jose-json-proof-algorithms-02
04/11/23	IETF 118 HACKATON	Meeting	Attendance and participation in discussions and experiments around challenges/solutions of PQ migration of X.509
10/11/23	IETF Sec. & Rtg. Areas	Meeting	Side meeting on Parh Validation mechanisms
21/11/23	3GPP SA3	Contribution	eZTS SID for 3GPP Release 19
07/12/23	ETSI QKD	Charter	WI on monitoring interface for QKD system
29/01/24	GSMA PQTN	Contribution	Post Quantum Cryptography Guidelines for Telecom Use
16/02/24	GSMA PQTN	Contribution	Post Quantum Cryptography Guidelines for Telecom Use
16/02/24	ETSI OSM	Contribution	Proposal for OSM long-term view in connection with research projects
17/02/24	IETF	Contribution	Proposal for activities on attestation and secure routing
26/02/24	GSMA	Presentation	Third Post Quantum Seminar at MWC
29/02/24	GSMA	Presentation	GSMA SEC CON 2024 at MWC
07/03/24	IETF ART Area	Charter	New WG on Workload Identity in Multi System Environments (WIMSE)
19/03/24	IETF Sec. & Rtg. Areas	Charter	Side meeting on attestation for secure network paths
19/03/24	IETF Sec. & Rtg. Areas	Charter	New WG charter proposal, on secure network paths (NASR)
19/03/24	IETF Sec. & Rtg. Areas	Presentation	NASR architecture proposal
19/03/24	IETF NETMOD WG	Presentation	Update on “Applying COSE Signatures for YANG Data Provenance”
20/03/24	IETF OPS Area	Charter	New WG NMOP created
21/03/24	IETF Security Area	Contribution	Symmetric Key Exchange (SKEX) framework
21/03/24	IETF RATS WG	Presentation	Introduction to the NASR concepts
21/03/24	IRTF QIRG	Meeting	Update on the QIA architecture framework proposal
22/03/24	GSMA	Publication	Post Quantum Cryptography – Guidelines for Telco Use case and Executive Summary
22/03/24	IETF ART Area	Charter	WG on Workload Identity in Multi System Environments (WIMSE)
25/04/24	ISO/IEC JTC SC 27	Meeting	Contribution to ISO/JTC 1/SC 27/WG 5 AHG/44-2 (Digital Wallets). PQC and crypto-agility are two major topics in the work of this group.
29/05/24	IOTA Identity	Contribution	IOTA Identity Integrates Zero Knowledge Credentials: In Partnership with the LINKS Foundation.

Table A.1: Table of contributions and activities

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

D4.4 – Standardization plan and activities (initial version)

Version 1.0

Horizon Europe