Ref. Ares(2024)8996534 - 16/12/2024

Horizon Europe

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

Use Cases and Validation Plan

Deliverable number: D3.1

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:	31 December 2024
Actual Delivery Date:	16 December 2024
Number of pages:	103
Keywords:	use cases, key performance indicators, validation
Contributors:	Andrea Vesco – LINKS Davide Margaria – LINKS Grazia D'Onghia – POLITO Davide Bellizia – TELSY Agostino Sette – TELSY Maria Chiara Molteni – SECPAT Eros Camacho-Ruiz – CSIC Piedad Brox – CSIC Antonio Pastor – TID Luis F. Gonzales – UC3M Nicola Tuveri – TAU Akif Mehmood – TAU Daniel Luoma – TAU Nouman Khan – TAU Alex Shaindlin – TAU Dmitry Belyavskiy – REDHAT Enrico Bisio – SMART
Peer review:	Antonio Pastor – TID Antonio Lioy – POLITO
Security review:	Andrea D'Intino – FORKBOMB Estanislao Fernández – TID Juha Nurmi – TAU
Approved by:	ALL partners

Table 1: Document revision history

Issue Date	Version	Comments
01/09/2024	0.1	Initial table of contents.
21/11/2024	0.2	First version for security review.
16/12/2024	1.0	Final version for submission.

Abstract

This document provides a comprehensive overview of use cases specifically tailored to evaluate the adoption of Post-Quantum Cryptography (PQC) in three critical areas: IoT-based Digital Manufacturing, Internet Browsing, and Software Network Environments for Telco Operators. The use cases run on the three pilot demonstrators deployed in relevant environments; the pilot demonstrators are described in Deliverable D2.1. Each use case is described in detail along with the Key Performance Indicators (KPIs), the acceptance criteria and the test plan for validation at Technology Readiness Level (TRL) 6. Overall, the tests are intended to quantify and evaluate the trade-offs of the three Post-Quantum (PQ) pilot demonstrators.

Contents

List of Tables

List of Acronyms

CCIPS	Centrally Controlled IPSec
CNC	Computer Numerical Control
CNF	Container Network Function
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSR	Certificate Signing Request
CVE	Common Vulnerabilities and Exposures
DID	Decentralized IDentifier
DSP	Digital Signal Processor
FCP	First Contentful Paint
FPGA	Field Programmable Gate Array
HTTPS	Hypertext Transfer Protocol Secure
IKEv2	Internet Key Exchange version 2
IoT	Internet of Things
IPsec	IP Security
K8s	Kubernetes
KEM	Key Encapsulation Method
KPI	Key Performance Indicator
L2S-M	Link-Layer Secure connectivity for Microservice platforms
LUT	Look-Up Table
MCU	Micro-Controller Unit
MPU	Micro-Processor Unit
MQTT	Message Queuing Telemetry Transport
NFV	Network Functions Virtualization
NIST	National Institute of Standards and Technology
OCSP	On-line Certificate Status Protocol
OQS	Open Quantum Safe
OSM	Open Source MANO
PKI	Public-Key Infrastructure
PKIX	Public-Key Infrastructure using X.509
PLC	Programmable Logic Controller
PQ	Post-Quantum
PQ/T	Post-Quantum/Traditional
PQC	Post-Quantum Cryptography
QKD	Quantum Key Distribution
QUBIP	Quantum-oriented Update to Browsers and Infrastructures for the Post-quantum transition
RA	Remote Attestation
RAM	Random Access Memory
RoT	Root of Trust
SDN	Software-Defined Networking
SE	Secure Element
SSI	Self-Sovereign Identity
SW	Software
TLS	Transport Layer Security

TPM	Trusted Platform Module
TRL	Technology Readiness Level
TTFB	Time To First Byte
VC	Verifiable Credential
VP	Verifiable Presentation

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

1. Introduction

This document provides a detailed breakdown of the elements essential for the evaluation of the transition of the three systems described in Deliverable D2.1. The main objective of the QUBIP experimental evaluation campaign is twofold: to validate the systems at TRL 6, while continuously refining the implementation based on quantitative results, and to maximise the return on experience for the design of the reference transition process to PQC.

The document establishes a structured and coherent methodology for evaluating the transition to PQC at system level. The document describes the use cases and the real environments in which they will be run, enumerates the KPIs together with the corresponding acceptance criteria, and the validation plan consisting of a set of tests. Different use cases running on the same system are designed to solicit different components of the same system and collect comprehensive results. The document then defines, for each use case, the set of KPIs, with the metrics to be measured on the systems to calculate the KPIs, and the acceptance criteria. The acceptance criteria define the thresholds and conditions to be met. These criteria ensure that the proposed solutions not only meet the technical specifications, but also comply with industry standards and practical deployment requirements. Finally, the document reports the test procedures in the Appendix A.

The document structure is designed to provide a clear roadmap for the validation of the three quantum-secure systems, with a systematic and replicable evaluation process.

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

2. Testing and Disclosure of Vulnerabilities

The QUBIP project involves long-lasting testing of the three pilot systems and, in some cases, the participation of real people in testing the hardware and software. The security aspects related to the real-world environment in which the three systems will be deployed, the testing process, and the participants involved will be carefully considered. In particular, to protect participants, all hardware and software components will be pre-tested in controlled environments, and participants will be informed of potential risks and provided with clear guidelines for secure use during the testing phase.

In addition, any vulnerability identified during the project activities will be reported through established channels in accordance with responsible disclosure practices. The QUBIP consortium will work with relevant stakeholders to resolve issues and, where appropriate, Common Vulnerabilities and Exposures (CVE) will be requested to ensure transparency and rapid remediation.

3. Quantum-Secure IoT-based Digital Manufacturing

3.1. Use Case 1 – Production Monitoring System

Monitoring of the production ambient temperature and of the number of parts produced. The Micro-Controller Unit (MCU)-based Internet of Things (IoT) devices integrate a temperature transducer and the sensor to count rising edges to track the production. The use case runs in a real production environment at different customer sites, involving the following machines:

- **Automatic loading machine for mechanical parts on Computer Numerical Control (CNC)**: used for the automatic loading of parts for CNC machining.
- **Testing machine**: used for the final testing of assembled parts, ensuring product quality.

The production monitoring system collects the following data:

1. ambient temperature,
2. number of parts produced.

3.1.1. KPIs and Acceptance Criteria

Table 3.1: KPIs of Use Case 1 – IoT-based Digital Manufacturing

Name	Metric(s)	KPI	Acceptance criteria
LUT Count	Number of used Look-Up Tables (LUTs) in the Secure Element (SE) implementation	Combinational logic resources (LUTs) required in the SE implementation to evaluate penalty of the PQ inclusion in terms of area occupation	The number of used LUTs in the PQ SE implementation must not surpass more than 30% of the required LUTs in the classical SE implementation
Flip-Flops Count	Number of used Flip-Flops in the SE implementation	Binary shift registers (Flips-Flops) used to synchronize logic within the Field Programmable Gate Array (FPGA) circuitry in the SE implementation to evaluate penalty of the PQ inclusion in terms of area occupation	The number of used Flip-Flops in the PQ SE implementation must not surpass more than 30% of the required LUTs in the classical SE implementation

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

Name	Metric(s)	KPI	Acceptance criteria
DSP Count	Number of used Digital Signal Processor (DSP) in the SE implementation	DSP used to perform arithmetic operations within FPGA circuitry to evaluate penalty of the PQ inclusion in terms of area occupation	The number of used DSP in the PQ SE implementation must not surpass more than 30% of the required LUTs in the classical SE implementation
RAM Resources	Block-Random Access Memory (RAM) occupation in the SE implementation [%]	Occupation percentage of Block-RAM memories required in the SE implementation to evaluate penalty of the PQ inclusion in terms of area occupation	The occupation percentage of RAM memories in the PQ SE implementation must not surpass more than 30% of the required Block-RAM occupation in the classical SE implementation
Average Power Consumption	Power consumed by the whole IoT device (MCU/MPU plus the SE) while performing Transport Layer Security (TLS) 1.3 handshake [mW]	Average power consumption	The average power consumption in the PQ implementation at a fixed frequency must not surpass more than 50% of the required power consumption in the classical SE implementation working at the same operation frequency
TLS 1.3 Handshake	TLS 1.3 handshake latency [ms]	Ratio between TLS 1.3 handshake latency with full software and SE-based implementation of PQ algorithms	Ratio should be less than 1.5
OCSP Throughput	(same as KPI)	Number of On-line Certificate Status Protocol (OCSP) requests processed per second	OCSP responder should handle at least 200 requests per second
OCSP Response Verification	Time required for the client to verify OCSP responses signed by the OCSP responder [ms]	Verification time ratio between PQ signature vs. classical signature on the OCSP response	Ratio should be less than 1.5
Composite Certificate Verification	Time required to verify certificates [ms]	Verification time ratio between composite certificate and classical X.509 solution	Ratio should be less than 2

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

Name	Metric(s)	KPI	Acceptance criteria
Software Openness	Open source software license of each software component	Number of software components that adhere to an open source software license scheme	All system components must be open source and released with open licenses to foster future development and security assessment
Hardware Openness	Open source hardware license of each hardware component	Number of hardware components that adhere to an open source hardware license scheme	All hardware components must be open source and released with open licenses to foster future development and security assessment
License Risk	Licensing information of each dependency	Number of license violations arising from the licensing information assessment	No license violations were found

3.1.2. Validation Plan

- T-DM-UC1-01 : FPGA implementation of the SE
- T-DM-UC1-02 : Average power consumption
- T-DM-UC1-03 : TLS 1.3 handshake: SE vs SW implementation
- T-DM-UC1-04 : OCSP responder
- T-DM-UC1-05 : Composite certificate verification at client side
- T-DM-UC1-06 : Openness

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

3.2. Use Case 2 – Smart Production Tracker with Integrity Verification

Smart tracking of manufacturing machine data and production data. Micro-Processor Unit (MPU)-based IoT devices collect data from the manufacturing machine via Modbus. Secure and measured boot are enabled on the MPU-based devices along with periodical remote attestation for software integrity purpose. The use case runs in a real production environment at different customer sites, involving the following machines:

- **Automatic loading machine for mechanical parts on CNC**: used for the automatic loading of parts for CNC machining.
- **Testing machine**: used for the final testing of assembled parts, ensuring product quality.

The smart production tracker collects the following data:

1. number of parts produced,
2. number of parts discarded,
3. Programmable Logic Controller (PLC) Central Processing Unit (CPU) temperature,
4. PLC CPU load percentage,
5. error codes,
6. Cyclic Redundancy Check (CRC) field bus error count.

3.2.1. KPIs and Acceptance Criteria

This use case is evaluated using the same KPIs in Table 3.1 with the addition of the following:

Table 3.2: Additional KPIs of Use Case 2 – IoT-based Digital Manufacturing

Name	Metric(s)	KPI	Acceptance criteria
Boot Time	Time required to successfully perform boot sequence of the MPU-based IoT device with all security mechanisms provided by secure and measured boot [ms]	Boot time ratio between the PQ and the classical solution	Ratio should be less than 2
MPU Load during RA	(same as KPI)	MPU utilization during runtime [$\%$]	The total utilization must not exceed 60% during peak operations of remote attestation (PQ signature)
Bandwidth Utilization during RA	Bandwidth utilization during transmission of the enhanced PQ integrity report [bytes/s]	Percentage of total available bandwidth used during attestation report transfer	Percentage of used bandwidth capacity should be less than 1%
Remote Attestation Latency	Time required for an attestation cycle to complete [s]	Time interval between the attestation request and the attestation outcome	Time interval should be at most 20 s

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

Name	Metric(s)	KPI	Acceptance criteria
Time to Detect a Compromised Node	Time required for the Verifier to detect that a node has been compromised [s]	Time interval between the compromising of the node and the detection by the verifier	Time interval should be less than the sum of Remote Attestation latency and time elapsed before the next attestation cycle (configurable)
Firmware Image Size	(same as KPI)	Image size of the firmware deployed on the target MPU-based IoT device [bytes]	Post-migration image size should still fit the resources available on the device, without the needs of adding extra memory

3.2.2. Validation Plan

- T-DM-UC2-01 : FPGA implementation of the whole MPU-based IoT device
- T-DM-UC2-02 : Average power consumption
- T-DM-UC2-03 : TLS 1.3 handshake: SE vs SW implementation
- T-DM-UC2-04 : OCSP responder
- T-DM-UC2-05 : Composite certificate verification at client side
- T-DM-UC2-06 : MPU-based IoT device bootstrap
- T-DM-UC2-07 : MPU-based IoT device remote attestation
- T-DM-UC2-08 : Remote attestation latency and detection of a compromised node
- T-DM-UC2-09 : Firmware image size
- T-DM-UC2-10 : Openness

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

4. Quantum-Secure Internet Browsing

4.1. Use Case 1 – Web browsing (server-side TLS 1.3 authentication) with application-layer client authentication based on login form

Secure web browsing using TLS 1.3 with a two-tier authentication model. Browsing of the QUBIP web servers deployed on the real Internet. The server implements authentication at the transport layer through the TLS 1.3 protocol using Public-Key Infrastructure using X.509 (PKIX) certificates, while client authentication occurs at the application layer through a conventional web-based login form over Hypertext Transfer Protocol Secure (HTTPS). This authentication pattern represents the *de facto* standard for secure user authentication on the modern Internet for most end-users, being widely implemented across most public-facing web applications.

This use case involves the participation of real people acting as the Internet users, selected and invited by Cibervoluntarios.

4.1.1. KPIs and Acceptance Criteria

Table 4.1: KPIs of Use Case 1 – Internet Browsing

Name	Metric(s)	KPI	Acceptance criteria
TLS 1.3 Handshake Latency	(same as KPI)	TLS 1.3 handshake latency of the overall system before and after the transition exercise [ms]	None[1]
TLS 1.3 Handshake Traffic Size	(same as KPI)	TLS 1.3 handshake traffic size of the overall system before and after the transition exercise [bytes]	None[1]
TLS 1.3 Handshake Establishment	(same as KPI)	TLS 1.3 connection establishment as part of the overall system before and after the transition exercise, or against alternative Post-Quantum/Traditional (PQ/T) Hybrid implementations for interoperability tests	99.9% of success

[1] Regarding TLS 1.3 related activities, QUBIP adopts state-of-the-art implementations and community choices, therefore we do not set an acceptance criteria for this KPI as it is the result of external choices. Nonetheless, documenting the impact of these external choices on this KPI is a valuable output of the QUBIP transition exercise.

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

Name	Metric(s)	KPI	Acceptance criteria
TLS 1.3 Handshake Latency Overhead	TLS 1.3 handshake latency of the overall system [ms]	Ratio of TLS 1.3 handshake latency of the overall system when using the QUBIP solution over `oqs-provider` (i.e., reference for the current community baseline)	The ratio should not exceed 1.10
TTFB	Time To First Byte (TTFB) measures the time between the request for a resource and when the first byte of a response begins to arrive [1]	TTFB measured via JavaScript on the browser	The median should be either "Good" (< 800 ms) or within "Needs Improvement" (between 800 and 1800 ms)
FCP	First Contentful Paint (FCP) measures the time from when the user first navigated to the page to when any part of the page's content is rendered on the screen [2]	FCP measured via JavaScript on the browser	The median should be either "Good" (< 1.8 s) or within "Needs Improvement" (between 1.8 and 3.0 s)
PKI Certificate Size	Total size of the composite X.509 certificates [byte]	Ratio between the size with a quantum-secure configuration and the corresponding size with a traditional configuration	TLS 1.3 handshake should complete successfully despite the size of the certificates
CSR Generation	Time required to generate a Certificate Signing Request (CSR) for composite certificates at end-entity [ms]	Ratio between the generation time with a specific quantum-secure (PQ or PQ/T hybrid) system configuration and the corresponding result with a traditional configuration	Ratio should be less than 2
PKI Verification	Time required to verify composite certificates [ms]	Ratio between the verification time with a specific quantum-secure (PQ or PQ/T hybrid) system configuration and the corresponding result with a traditional configuration	Ratio should be less than 2
PKI Algorithm Strength	(same as KPI)	Combined security strength of the composite algorithm (traditional plus PQ)	Combined key lengths or equivalent security provide at least 256-bit traditional and quantum resistance levels

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

Name	Metric(s)	KPI	Acceptance criteria
Ease of Use	Individual tasks within the user's playbook completed during the experiments with no assistance	Percentage of users reporting any problem while completing the tasks included within the experiments' playbook	95% of users should not require additional technical support to use the browser with the new components and complete the tasks included within the playbook
User Satisfaction	Percentage of positive answers from the user feedback questionnaire – crossed with the behavioral and demographic data gathered	User satisfaction scores collected via surveys or questionnaires, focusing on the ease of use and swiftness of use	At least 80% of users report more positive than negative feedback in the total of questions
Perceived TLS 1.3 Connection Latency	User perception of the time required to establish a TLS 1.3 connection, scored from 1 (slow) to 5 (fast)	Average user perception of the time require to establish a TLS 1.3 connection, before and after the transition exercise	90% of the end users taking part in the tests score $4/5$
Perceived Security, Privacy and Accessibility	Results from the user feedback questionnaire, to evaluate the psychological impact of migrating to PQC	Users' perception of their security, privacy and accessibility while browsing	Perceived accessibility to the PQ browser, as well as, security and privacy should be equal to or better than in the quantum-vulnerable scenario, indicating user confidence in PQC's ability to protect their data
Usability and Speed Perception	Scoring from the user feedback questionnaire	Percentage of users perceiving a significant difference in browsing usability and speed	At least 90% of users should not perceive a significant difference in browsing usability and speed
Adoption	YES/NO question from the feedback questionnaire	Percentage of users in the test group opting to keep the new features enabled after the test	At least 80% percent of users in the test group should opt to keep the new features enabled after the trial period

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

4.1.2. Validation Plan

- T-IB-UC1-01 : TLS 1.3 handshake
- T-IB-UC1-02 : TLS 1.3 handshake with different algorithm implementations
- T-IB-UC1-03 : TLS 1.3 latency variation with QUBIP solution for full configurability
- T-IB-UC1-04 : Overall system performance
- T-IB-UC1-05 : Public Key Infrastructure
- T-IB-UC1-06 : User experience

It is worth highlighting here the importance of the following set of interoperability tests with existing quantum-secure server infrastructure and web browsers of big Internet players.

- T-IB-UC1-INTEROPERABILITY-01 : Interoperability against Cloudflare
- T-IB-UC1-INTEROPERABILITY-02 : Interoperability against Open Quantum Safe (OQS)
- T-IB-UC1-INTEROPERABILITY-03 : Interoperability against QUBIP OpenSSL Server

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

4.2. Use Case 2 – Web browsing (mutual authentication via TLS 1.3)

Secure web browsing using TLS 1.3 with mutual authentication at the transport layer. Browsing of the QUBIP web servers deployed on the real Internet. Both the server and client implement authentication through the TLS 1.3 protocol using PKIX certificates, without the need for additional application-layer authentication mechanisms. This authentication pattern represents a more stringent security model commonly used in enterprise environments, specialized services, and scenarios requiring high security assurance. While less common for general Internet browsing, it provides stronger authentication guarantees through certificate-based client identification, particularly relevant in certain enterprise or governmental scenarios.

This use case involves the participation of real people acting as the Internet users, selected and invited by Cibervoluntarios.

4.2.1. KPIs and Acceptance Criteria

This use case is evaluated using the same KPIs in Table 4.1 with the addition of the following:

Table 4.2: Additional KPIs of Use Case 2 – Internet Browsing

Name	Metric(s)	KPI	Acceptance criteria
Cryptographic Agility	Ease of changing algorithms with different instances of the QUBIP Provider, scored from 1 (Strongly Disagree) to 5 (Strongly Agree) by expert users	Cryptographic Agility with the QUBIP Provider for OpenSSL	Switching algorithms and/or implementations with simple system configuration changes with score ≥ 4
Openness	Open source software license of each software component	Number of software components that adhere to an open source software license scheme	All system components must be open source and released with open licenses to foster future development and security assessment
License Risk	Licensing information of each software dependency	Number of license violations arising from the licensing information assessment	No license violations were found

4.2.2. Validation Plan

- T-IB-UC2-01 : TLS 1.3 handshake
- T-IB-UC2-02 : TLS 1.3 latency variation with QUBIP solution for full configurability
- T-IB-UC2-03 : Overall system performance
- T-IB-UC2-04 : Public Key Infrastructure
- T-IB-UC2-05 : User experience
- T-IB-UC2-06 : Cryptographic agility
- T-IB-UC2-07 : Openness

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

4.3. Use Case 3 – Web browsing (mutual authentication) with application-layer client authentication based on plaintext PQ and PQ/T Verifiable Credentials

Secure web browsing with client authentication at the application layer based on the Self-Sovereign Identity (SSI) model with plaintext PQ and PQ/T hybrid Verifiable Credentials (VCs). Browsing of QUBIP web servers, deployed on the real Internet, involves three agents (i.e., Issuer, Holder, and Verifier) that interact over a PQ TLS 1.3 channel. The Holder obtains a plaintext PQ VC from the Issuer and presents it to the Verifier, using a wallet extension inside the Firefox browser.

This use case involves the participation of real people acting as the Internet users, selected and invited by Cibervoluntarios.

4.3.1. KPIs and Acceptance Criteria

Table 4.3: KPIs of Use Case 3 (and Use Case 4) – Internet Browsing

Name	Metric(s)	KPI	Acceptance criteria
SSI Identity Generation Latency	Absolute time interval [ms] measured at the application level between the start and the end of a specific SSI Identity Generation operation (i.e., creation of the DID/DID document, issuance of a VC)	Ratio between the measured time with a specific quantum-secure (PQ or PQ/T hybrid) system configuration and the corresponding result with a traditional configuration	Among the different configurations under test, accept all options which result in an acceptable ratio
SSI Authentication Latency	Absolute time interval [ms] measured at the application level between the start and the end of a specific SSI Authentication operation (i.e., presentation of a VP, revocation of a VC)	Ratio between the measured time with a specific quantum-secure (PQ or PQ/T hybrid) system configuration and the corresponding result with a traditional configuration	Among the different configurations under test, accept all options which result in an acceptable ratio
SSI Identity Generation Traffic Size	Total size [bytes] of the data transmitted and received by client and server during a specific SSI Identity Generation operation	Ratio between the traffic size in a specific quantum-secure (PQ or PQ/T hybrid) system configuration and the corresponding result in a traditional configuration	Among the different configurations under test, accept all options which result in an acceptable ratio
SSI Authentication Traffic Size	Total size [bytes] of the data transmitted and received by client and server during a specific SSI Authentication operation	Ratio between the traffic size in a specific quantum-secure (PQ or PQ/T hybrid) system configuration and the corresponding result in a traditional configuration	Among the different configurations under test, accept all options which result in an acceptable ratio

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

Name	Metric(s)	KPI	Acceptance criteria
SSI Operation Client Memory Fingerprint	Total size [bytes] of the memory occupied by the test application during a specific SSI operation, at client-side (i.e., Holder)	Ratio between the memory fingerprint in a specific quantum-secure (PQ or PQ/T hybrid) system configuration and the corresponding result in a traditional configuration	Among the different configurations under test, accept all options which result in an acceptable ratio
SSI Operation Server Memory Fingerprint	Total size [bytes] of the memory occupied by the test application during a specific SSI operation, at server-side (i.e., Issuer and Verifier)	Ratio between the memory fingerprint in a specific quantum-secure (PQ or PQ/T hybrid) system configuration and the corresponding result in a traditional configuration	Among the different configurations under test, accept all options which result in an acceptable ratio
Overall SSI Process Error Rate	Ratio of the number of failures to the total number of executions per SSI operation performed during the test	Increase of the error rate in a specific quantum-secure (PQ or PQ/T hybrid) system configuration and the corresponding result in a traditional configuration	The increase of the error rate must be negligible, $\leq 10^{-3}$ (see [3, 4] for anonymous credentials)
SSI Algorithm Strength	(same as KPI)	Overall security strength of the cryptographic algorithms used in SSI operations with a specific system configuration (Traditional, PQ or PQ/T hybrid)	Key lengths or equivalent security provide at least 128-bit traditional and quantum resistance levels
Ease of Use	Individual tasks within the user's playbook completed during the experiments with no assistance	Percentage of users reporting any problem while completing the tasks included within the experiments' playbook	95% of users should not require additional technical support to use the browser with the new components and complete the tasks included within the playbook
User Satisfaction	Percentage of positive answers from the user feedback questionnaire – crossed with the behavioral and demographic data gathered	User satisfaction scores collected via surveys or questionnaires, focusing on the ease of use and swiftness of use	At least 80% of users report more positive than negative feedback in the total of questions
Perceived Security, Privacy and Accessibility	Results from the user feedback questionnaire, to evaluate the psychological impact of migrating to PQC	Users' perception of their security, privacy and accessibility while authenticating with a website	Perceived accessibility to the PQ browser, as well as, security and privacy should be better than with the current login form

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

Name	Metric(s)	KPI	Acceptance criteria
Usability and Speed Perception	Scoring from the user feedback questionnaire	Percentage of users perceiving a significant difference in browsing usability and speed	At least 90% of users should not perceive a significant difference in browsing usability and speed
Adoption	YES/NO question from the feedback questionnaire	Percentage of users in the test group opting to keep the new features enabled after the test	At least 80% percent of users in the test group should opt to keep the new features enabled after the trial period
Openness	Open source software license of each software component	Number of software components that adhere to an open source software license scheme	All system components must be open source and released with open licenses to foster future development and security assessment
License Risk	Licensing information of each software dependency	Number of license violations arising from the licensing information assessment	No license violations were found

4.3.2. Validation Plan

- T-IB-SSI-UC3-01 : SSI identity generation
- T-IB-SSI-UC3-02 : SSI identity authentication
- T-IB-SSI-UC3-03 : SSI identity revocation
- T-IB-SSI-UC3-04 : User experience with SSI authentication
- T-IB-SSI-UC3-05 : Openness

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

4.4. Use Case 4 – Web browsing (mutual authentication) with application-layer client authentication based on PQ anonymous credentials

Secure web browsing with client authentication at the application layer based on the SSI model with PQ anonymous credentials. PQ anonymous credentials represent a privacy-preserving alternative to the plaintext VCs, enabling the Holder to manage its VC by choosing the level of information disclosure. This approach protects the privacy of the Holder, since the VC, the contained claims, and the signature of the Issuer are not exchanged in plaintext. Browsing of QUBIP web servers, deployed on the real Internet, involves three agents (i.e., Issuer, Holder, and Verifier) that interact over a PQ TLS 1.3 channel. The Holder obtains a PQ credential from the Issuer and proves his identity with selective disclosure of attributes to the Verifier, using a wallet extension inside the Firefox browser.

This use case involves the participation of real people acting as the Internet users, selected and invited by Cibervoluntarios.

4.4.1. KPIs and Acceptance Criteria

This use case is evaluated using the same KPIs in Table 4.3, considering the use of PQ anonymous credentials with selective disclosure of identity attributes.

4.4.2. Validation Plan

- T-IB-SSI-UC4-01 : SSI identity generation
- T-IB-SSI-UC4-02 : SSI identity authentication
- T-IB-SSI-UC4-03 : SSI identity revocation
- T-IB-SSI-UC4-04 : User experience with anonymous authentication with selective disclosure
- T-IB-SSI-UC4-05 : Openness

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

5. Quantum-Secure Software Network Environments for Telco Operators

5.1. Use Case 1 – Deployment of secure connectivity services for CNF based on cloud-native NFV with hybrid IPsec

Deployment of Centrally Controlled IPSec (CCIPS) in a cloud-native environment similar to a telco cloud to provide secure connectivity services. The operator uses Kubernetes (K8s) to deploy two Container Network Function (CNF), representative of real telco services (e.g., DNS, radius, 5G Core, firewall, router, load balancer, etc.) as workloads in different K8s worker nodes and interconnect them through a transparent layer 2 overlay.

This approach simplifies the transition of existing CNFs and associated layer 3 to 7 vulnerable protocols to PQC by encapsulating the traffic in quantum-secure IP Security (IPsec) tunnels.

5.1.1. KPIs and Acceptance Criteria

The list of KPIs in Table 5.1 is organized around the main features of the underlying system: PQC/QKD hybridization, integrity verification via remote attestation, and end-to-end connectivity.

Table 5.1: KPIs of Use Case 1 – Software Network Environment for Telco Operators

Name	Metric(s)	KPI	Acceptance criteria
Hybrid Key Delivery Time	Time required for a key request to be served by the hybridization module [ms]	Ratio between the average key delivery time of the PQC/QKD hybridization module and the classical IKEv2	No significant overhead in the key response time
Min-entropy Quality	Min-entropy of the hybrid keys	Ratio between the average min-entropy of hybrid and classic IKEv2 keys	Min-entropy should be maintained at similar level
Key Generation Success Rate	Number of key requested and successfully generated in a unit of time	Ratio between the number of keys requested and successfully generated	100% of success
Hybrid Quote Generation Time	Total time to generate and wrap the attestation quote [ms]	Ratio between the average time for generating the wrapped quote and the Trusted Platform Module (TPM) classical quote	Ratio should be less than 2
Remote Attestation Latency	Time required for an attestation cycle to complete [s]	Time interval between the attestation request and the attestation outcome	Time interval should be at most 10 s

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

Name	Metric(s)	KPI	Acceptance criteria
Time to Detect a Compromised Node	Time required for the Verifier to detect that a node has been compromised [s]	Time interval between the compromising of the node and the detection by the verifier	Time interval should be less than the sum of Remote Attestation latency and time elapsed before the next attestation cycle (configurable)
Bandwidth Utilization during RA	Bandwidth utilization during transmission of the enhanced PQ integrity report [bytes/s]	Percentage of total available bandwidth used during attestation report transfer	Percentage of used bandwidth capacity should be less than 0.5%
Network Service Deployment	(same as KPI)	Successful deployments of interconnected CNFs within the K8s cluster	100% of success
Telco Management Software	Number of changes in operational steps on Software-Defined Networking (SDN)/Network Functions Virtualization (NFV) management tools; Time required for provisioning the service [s]	Changes in operational steps using SDN/NFV management tools	The expected changes or developments must be minimal, as well as, the time required to provide the service
Key Generation and Exchange	Network traffic captures outside of the security perimeter	Cryptographic keys visibility in transit for data plane traffic	The key management process must be robust and should not increase the Key Exposure Risk and compromise compared to the classic IKEv2 system
Encrypted Traffic Throughput	Throughput [bytes/s]	Average traffic throughput with classical and hybrid encryption keys	No significant deviation
IPsec Tunnel Provisioning	Time for establishing the IPsec tunnel [ms]	Ratio between the time for establishing the IPsec tunnel with the PQ and classic IKEv2 solution	Ratio should be less than 2.
IPsec Tunnel Re-keying	Time for re-keying the IPsec tunnel [ms]	Ratio between the time for re-keying the IPsec tunnel with the PQ and classic IKEv2 solution	Ratio should be less than 2

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

Name	Metric(s)	KPI	Acceptance criteria
Openness	Open source software license of each software component	Number of software components that adhere to an open source software license scheme	All system components must be open source and released with open licenses to foster future development and security assessment
License Risk	Licensing information of each software dependency	Number of license violations arising from the licensing information assessment	No license violations were found

5.1.2. Validation Plan

- T-SNE-UC1-01 : Quantum key delivery
- T-SNE-UC1-02 : PQ key delivery
- T-SNE-UC1-03 : Hybrid key delivery
- T-SNE-UC1-04 : Min-entropy
- T-SNE-UC1-05 : Hybrid quote generation
- T-SNE-UC1-06 : Detection of a compromised node during remote attestation
- T-SNE-UC1-07 : Bandwidth consumption during Remote Attestation
- T-SNE-UC1-08 : Telco management software integration for network service deployment
- T-SNE-UC1-09 : Encrypted traffic throughput
- T-SNE-UC1-10 : Key generation and management
- T-SNE-UC1-11 : IPsec tunnel provisioning
- T-SNE-UC1-12 : Openness

5.2. Use Case 2 – Deployment of secure connectivity services for CNF without support for integrity verification

Deployment of CCIPS in a cloud-native environment similar to a telco cloud to provide secure connectivity services. The operator uses K8s to deploy two CNFs, representative of real telco services (e.g., DNS, radius, 5G Core, firewall, router, load balancer, etc.) as workloads in different K8s worker nodes and interconnect them through a transparent layer 2 overlay. The underlying system does not support the integration of hardware and/or software Root of Trust (RoT) for implementing integrity verification. The mutual identification and authentication between CNFs is implicit in the key exchange through the Quantum Key Distribution (QKD) network.

This approach provides a transition strategy to PQC for telco environments that do not support the integration of TPM.

5.2.1. KPIs and Acceptance Criteria

This use case is evaluated using the same KPIs in Table 5.1 by excluding those KPIs related to remote attestation procedures.

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

5.2.2. Validation Plan

- T-SNE-UC2-01 : Quantum key delivery
- T-SNE-UC2-02 : PQ key delivery
- T-SNE-UC2-03 : Hybrid key delivery
- T-SNE-UC2-04 : Min-entropy
- T-SNE-UC2-05 : Telco management software integration for network service deployment
- T-SNE-UC2-06 : Encrypted traffic throughput
- T-SNE-UC2-07 : Key generation and management
- T-SNE-UC2-08 : IPsec tunnel provisioning

5.3. Use Case 3 – Deployment of secure connectivity services connectivity for CNF without QKD network

Deployment of CCIPS in a cloud-native environment similar to a telco cloud to provide secure connectivity services. The operator uses K8s to deploy two CNF, representative of real telco services (e.g., DNS, radius, 5G Core, firewall, router, load balancer, etc.) as workloads in different K8s worker nodes and interconnect them through a transparent layer 2 overlay. The underlying system does not support QKD, therefore the hybridization module combines classical with PQ keys.

This approach provides a transition strategy to PQC for telco environments not connected to a QKD network.

5.3.1. KPIs and Acceptance Criteria

This use case is evaluated using the same KPI in Table 5.1, with the addition of the following:

Table 5.2: Additional KPIs of Use Case 3 – Software Network Environment for Telco Operators

Name	Metric(s)	KPI	Acceptance criteria
Fallback	(same as KPI)	Time required to execute the fallback process due to the lack of QKD [ms]	No additional delay in establishing the IPsec tunnel

5.3.2. Validation Plan

- T-SNE-UC3-01 : PQ key delivery
- T-SNE-UC3-02 : Fallback procedure
- T-SNE-UC3-03 : Hybrid quote generation
- T-SNE-UC3-04 : Detection of a compromised node during remote attestation
- T-SNE-UC3-05 : Bandwidth consumption during Remote Attestation
- T-SNE-UC3-06 : Telco management software integration for network service deployment
- T-SNE-UC3-07 : Encrypted traffic throughput
- T-SNE-UC3-08 : Key generation and management
- T-SNE-UC3-09 : IPsec tunnel provisioning

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 in detail the use cases running on the three pilot demonstrators introduced in Deliverable D2.1. Each use case is accompanied by the list of KPIs with acceptance criteria and an appropriate validation plan.

Note that, the set of KPIs with acceptance criteria and the multi-test validation plans are defined here to the best of the consortium's knowledge at the time of writing. However, they may be further developed and/or adapted as a result of new knowledge gained during the next phases of the QUBIP project.

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

Bibliography

[1] J. Wagner and B. Pollard, “web.dev Time to First Byte (TTFB)”, June 2024, https://web.dev/articles/ttfb. Accessed: 2024-12-10

[2] P. Walton, “web.dev First Contentful Paint (FCP)”, December 2023, https://web.dev/articles/fcp. Accessed: 2024-12-10

[3] J. Camenisch, M. Drijvers, and A. Lehmann, “Anonymous Attestation Using the Strong Diffie-Hellman Assumption Revisited”, 9th International Conference on Trust and Trustworthy Computing, Vienna (AT), August 2016, pp. 1–20, DOI10.1007/978-3-319-45572-3_1

[4] J. Bootle, V. Lyubashevsky, N. K. Nguyen, and A. Sorniotti, “A Framework for Practical Anonymous Credentials from Lattices”, IACR Cryptology ePrint Archive, Paper 2023/560, 2023, https://eprint.iacr.org/2023/560

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

A. Experimental Test Sheets

A.1. Quantum-Secure IoT-based Digital Manufacturing

Table A.1: T-DM-UC1-01 Test Sheet

Test ID	Test Name	Responsible
T-DM-UC1-01	FPGA implementation of the SE	CSIC

Brief Description

This test evaluates the impact of PQC on the implementation of the SE in term of logical resource footprint on the target FPGA: XC7K325T-2FFG900C.

KPI Name(s)

- LUT Count
- Flip-Flops Count
- DSP Count
- RAM Resources

Test Procedure

1. Select the target FPGA under the *Setting* menu in the *Project Manager* section in Vivado.
2. Set the timing constraint for the main clock period to 10ns (corresponding to a 100MHz clock frequency).
3. Run the full design flow down to the bitstream.
4. Generate the utilization report, namely the *Report Utilization*, for the post place-and-route design related to the SE.
5. Collect all the required numbers for LUTs, Flip-Flops, DSPs and occupation of RAM blocks.
6. Evaluate the ratio for all the measured numbers and check if acceptance criteria are met.

Additional Notes

The version of the design environment AMD Xilinx Vivado, at the time of writing this document, is the 2024.1.

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

Table A.2: T-DM-UC1-02 Test Sheet

Test ID	Test Name	Responsible
T-DM-UC1-02	Average power consumption	SMART

Brief Description

This test evaluates the average power consumption of the MCU-based IoT device while performing TLS 1.3 handshakes.

KPI Name(s)

- Average Power Consumption

Test Procedure

1. Insert a shunt 0.1 Ohm resistor on the main power line that feeds both the STM32 board and the Genesys 2 board.
2. Power-up the system and wait for the system to boot.
3. Start measuring the power consumption.
4. Perform 1000 TLS 1.3 handshake between the IoT device and the MQTT Broker (server).
5. Stop measuring the power consumption.
6. Extract the average power consumption per TLS 1.3 handshake.
7. Evaluate the average power consumption against a solution with a SE with classical cryptography.
8. Evaluate the average power consumption against a software implementation of the algorithms in the SE.

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

Table A.3: T-DM-UC1-03 Test Sheet

Test ID	Test Name	Responsible
T-DM-UC1-03	TLS 1.3 handshake: SE vs SW implementation	SECPAT

Brief Description

This test evaluates the latency of establishing a TLS 1.3 channel using the Mbed-TLS library.

KPI Name(s)

- TLS 1.3 Handshake

Test Procedure

1. Power-up the board and wait for the system to boot.
2. Set up an on-chip timer of the STM32 with a resolution of 1us.
3. Repeat 1000 times the following operations:
   a) initialize the timer to 0,
   b) perform a TLS 1.3 handshake between the IoT device and the MQTT Broker (server),
   c) save the state of the timer at the end of the TLS 1.3 handshake.
4. Extract the average time in ms required to perform a TLS 1.3 handshakes and compare it against the time required with a TLS 1.3 implementation based on classical cryptography.
5. Evaluate also the average time against a software implementation of the TLS 1.3 handshake.

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

Table A.4: T-DM-UC1-04 Test Sheet

Test ID	Test Name	Responsible
T-DM-UC1-04	OCSP responder	POLITO
Brief Description		
This test evaluates the impact of adopting PQC in OCSP.		
KPI Name(s)		
• OCSP Throughput • OCSP Response Verification		
Test Procedure		
1. Set up the OCSP responder to handle requests for composite certificates. 2. Send 1000 requests to the OCSP responder over a specific amount of time (e.g., 1 minute). 3. Record the number of requests handled per second and verify that they confirm the acceptance criteria. 4. Measure the verification time on the client side for signed OCSP responses received from the OCSP responder and record the average time among 1000 responses.		

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

Table A.5: T-DM-UC1-05 Test Sheet.

Test ID	Test Name	Responsible
T-DM-UC1-05	Composite certificate verification at client side	POLITO
Brief Description		
This test evaluates the impact of using composite certificates on constraint MCU-based IoT devices.		
Name(s)		
• Composite Certificate Verification		
Test Procedure		
1. Power-up the board and wait for the system to boot. 2. Perform 1000 TLS 1.3 handshake between the IoT device and the MQTT broker (server). 3. Isolate and record the time required for an IoT device to verify the server's composite certificate. 4. Extract the average verification time and compute the ratio with the verification time required for classical X.509 certificates.		

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

Table A.6: T-DM-UC1-06 Test Sheet

Test ID	Test Name	Responsible
T-DM-UC1-06	Openness	SECPAT
Brief Description		
This test case evaluates the licensing terms of the involved software and hardware components to ensure compliance with recognized open-source licenses and compatibility across different licenses. The goal is to assess the software and hardware openness and identify potential licensing risks that could impact redistribution or usage.		
KPI Name(s)		
• Software Openness • Hardware Openness • License Risk		
Test Procedure		
1. Examine the software and hardware licensing terms for each component. 2. Verify the licensing terms match a recognized open-source license. 3. Verify the compatibility across different licensing terms. 4. Create a report with key findings.		

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

Table A.7: T-DM-UC2-01 Test Sheet.

Test ID	Test Name	Responsible
T-DM-UC2-01	FPGA implementation of the whole MPU-based IoT device	TELSY

Brief Description

This test evaluates the impact of PQC on the implementation of the whole MPU-based IoT device in term of logical resource footprint on the target FPGA: XCZU7EV-2FFVC1156.

KPI Name(s)

- LUT Count
- Flip-Flops Count
- DSP Count
- RAM Resources

Test Procedure

1. Select the target FPGA under the *Setting* menu in the *Project Manager* section in Vivado.
2. Set the timing constraint for the main clock period to 10ns (corresponding to a 100MHz clock frequency).
3. Run the full design flow down to the bitstream.
4. Generate the utilization report, namely the *Report Utilization*, for the post place-and-route design related to the device.
5. Collect all the needed numbers for LUTs, Flip-Flops, DSPs and RAM blocks.
6. Evaluate the ratio for all the measured numbers to check if acceptance criteria are met.

Additional Notes

The version of the design environment AMD Xilinx Vivado, at the time of writing this document, is the 2024.1.

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

Table A.8: T-DM-UC2-02 Test Sheet

Test ID	Test Name	Responsible
T-DM-UC2-02	Average power consumption	SMART
Brief Description		
This test evaluates the average power consumption of the MPU-based IoT device while performing TLS 1.3 handshakes.		
KPI Name(s)		
• Average Power Consumption		
Test Procedure		
1. Insert a shunt 0.1 Ohm resistor on the main power line of the ZCU-104 board. 2. Power-up the board and wait for the system to boot. 3. Start measuring the power consumption. 4. Perform 1000 TLS 1.3 handshake between the IoT device and the MQTT Broker. 5. Stop measuring the power consumption. 6. Extract the average power consumption per TLS 1.3 handshake.		

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

Table A.9: T-DM-UC2-03 Test Sheet

Test ID	Test Name	Responsible
T-DM-UC2-03	TLS 1.3 handshake: SE vs SW implementation	TAU
Brief Description		
This test evaluates the TLS 1.3 handshake latency, leveraging the full configurability of the *QUBIP Provider* for OpenSSL to assess the impact of the SE implementation over a purely software alternative.		
KPI Name(s)		
• TLS 1.3 Handshake		
Test Procedure		
1. Repeat the following procedure twice, first with a setup leveraging the SE, then again using exclusively a software implementation: a) power-up the board and wait for the system to boot, b) start the timing measurement with *time.h* Linux library (or similar), c) perform 1000 TLS 1.3 handshake between the IoT device and the MQTT Broker (server), d) stop the timing measurement, e) extract the average time in ms required to perform a successful TLS 1.3 handshake. 2. Compare the averages to assess the impact of each different implementation. 3. Compare the averages to assess the impact against the implementation with classical cryptography.		

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

Table A.10: T-DM-UC2-04 Test Sheet

Test ID	Test Name	Responsible
T-DM-UC2-04	OCSP responder	POLITO
Brief Description		
This test evaluates the impact of PQC in OCSP.		
Name(s)		
• OCSP Throughput • OCSP Response Verification		
Test Procedure		
1. Set up the OCSP responder to handle requests for composite certificates. 2. Send 1000 requests to the OCSP responder over a specific amount of time (e.g., 1 minute). 3. Record the number of requests handled per second and verify that they confirm the acceptance criteria. 4. Measure the verification time on the client side for signed OCSP responses received from the OCSP responder and record the average time among 1000 responses.		

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

Table A.11: T-DM-UC2-05 Test Sheet

Test ID	Test Name	Responsible
T-DM-UC2-05	Composite certificate verification at client side	POLITO
Brief Description		
This test evaluates the impact of using composite certificates on MPU-based IoT devices.		
Name(s)		
• Composite Certificate Verification		
Test Procedure		
1. Power-up the board and wait for the system to boot. 2. Perform 1000 TLS 1.3 handshake between the IoT device and the MQTT broker (server). 3. Isolate and record the time required for the IoT device to verify the server's composite certificate. 4. Extract the average verification time and compute the ratio with the verification time required for classical X.509 certificates.		

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

Table A.12: T-DM-UC2-06 Test Sheet

Test ID	Test Name	Responsible
T-DM-UC2-06	MPU-based IoT device bootstrap	POLITO
Brief Description		
This test assesses the boot time of the MPU with PQC-enabled secure and measured boot to evaluate performance overhead due to added security layers. The aim is to ensure the boot time does not exceed twice that of the classical implementation.		
KPI Name(s)		
• Boot Time		
Test Procedure		
1. Initiate boot sequence with PQC-enabled secure and measured boot mechanism activated. 2. Record the total time from power-on to successful completion of the boot sequence. 3. Repeat the process with classical algorithms and record the boot time for a comparison baseline. 4. Verify that the PQC boot time does not exceed twice the classical boot time by computing the ratio between PQ and classical boot time.		

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

Table A.13: T-DM-UC2-07 Test Sheet

Test ID	Test Name	Responsible
T-DM-UC2-07	MPU-based IoT device remote attestation	POLITO
Brief Description		
This test evaluates the impact of PQ remote attestation on MPU-based IoT device performance during runtime.		
KPI Name(s)		
• MPU Load during RA • Bandwidth Utilization during RA		
Test Procedure		
1. Enable PQ remote attestation on the MPU-based IoT device. 2. Execute typical runtime operations. 3. Monitor and log: a) MPU usage – measure peak and average MPU utilization over the attestation cycle, b) Bandwidth consumption – record data sent/received in kbps during attestation, c) Repeat the measurement for 1000 attestation cycles, d) Compute the average MPU usage and bandwidth consumption. 4. Confirm that resource consumption remains below target values, indicating that PQ attestation does not compromise performance.		
Additional Notes		
Test results will be used to confirm that PQ remote attestation meets usability standards during runtime, ensuring minimal disruption.		

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

Table A.14: T-DM-UC2-08 Test Sheet

Test ID	Test Name	Responsible
T-DM-UC2-08	Remote attestation latency and detection of a compromised node	POLITO

Brief Description

This test evaluates the time required for a complete remote attestation cycle and the time needed for the Verifier to detect a compromised node. The remote attestation latency measures the interval between the attestation request and the attestation outcome. The detection time of a compromised node is the interval from when a node is compromised to when it is detected by the Verifier. The latency should not exceed 20 seconds, and the detection time should remain less than the sum of the remote attestation latency and the configured attestation cycle interval.

KPI Name(s)

- Remote Attestation Latency
- Time to Detect a Compromised Node

Test Procedure

1. Setup.
   a) Ensure the attestation framework is configured and operational.
   b) Configure the attestation cycle interval to a known value, such as 40 s.
2. Remote Attestation latency test.
   a) Send an attestation request from the Verifier to a selected Attester node.
   b) Record the time at which the attestation request is sent.
   c) Record the time at which the Verifier receives and processes the attestation outcome.
   d) Calculate the latency as the difference between these two timestamps.
   e) Repeat the process 1000 times and compute the average value.
   f) Verify that the latency does not exceed 20 seconds.
3. Detection of a compromised node.
   a) Simulate a compromise on the Attester node by introducing an invalid measurement or altering the attestation report.
   b) Start the attestation cycle.
   c) Record the time at which the node is compromised.
   d) Record the time at which the Verifier detects the compromise.
   e) Calculate the detection time as the difference between these two timestamps.
   f) Repeat the process 50 times and compute the average value.
   g) Verify that the detection time is less than the sum of the attestation latency and the configured attestation cycle interval.
   h) Ensure both KPIs meet their respective thresholds.

Additional Notes

Ensure that the time measurement tools have sufficient resolution to accurately capture the timestamps in both cases.

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

Table A.15: T-DM-UC2-09 Test Sheet

Test ID	Test Name	Responsible
T-DM-UC2-09	Firmware image size	POLITO

Brief Description

This test evaluates the size of the firmware image after integrating PQC. The firmware image size must fit within the device's available memory resources without requiring additional memory.

KPI Name(s)

- Firmware Image Size

Test Procedure

1. Image Size Measurement.
   a) Compile the firmware with all features integrated.
   b) Measure the resulting firmware image size in bytes.
   c) Record the image size.
2. Validation.
   a) Verify that the firmware image size is less than or equal to the available memory size on the MPU.
   b) Confirm that no additional memory resources are required for the firmware deployment.

Additional Notes

If the image exceeds the available memory size, optimization techniques (e.g., code compression or removal of unused features) should be employed.

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

Table A.16: T-DM-UC2-10 Test Sheet

Test ID	Test Name	Responsible
T-DM-UC2-10	Openness	TELSY
Brief Description		
This test case evaluates the licensing terms of all software and hardware components to ensure compliance with recognized open-source licenses and compatibility across different licenses. The goal is to assess the software and hardware openness and identify potential licensing risks that could impact redistribution or usage.		
KPI Name(s)		
• Software Openness • Hardware Openness • License Risk		
Test Procedure		
1. Examine the software and hardware licensing terms for each component. 2. Verify the licensing terms match a recognized open-source license. 3. Verify the compatibility across different licensing terms. 4. Create a report with key findings.		

A.2. Quantum-Secure Internet Browsing

Table A.17: T-IB-UC1-01 Test Sheet

Test ID	Test Name	Responsible
T-IB-UC1-01	TLS 1.3 handshake	TAU

Brief Description
This test evaluates the establishment of a TLS 1.3 handshake, measuring latency and traffic size using a suite of scripts that initiate a connection to a specified server. After successfully connecting to the server and completing the test script suite, the results can be retrieved for analysis. The goal is to assess the impact of the PQ transition on the performance of TLS 1.3 handshakes.
KPI Name(s)
• TLS 1.3 Handshake Latency • TLS 1.3 Handshake Traffic Size • TLS 1.3 Handshake Establishment
Test Procedure
1. Open Terminal. 2. Execute the `T-IB-UC1-01` test suite script. 3. Collect the results from the the output of the `T-IB-UC1-01` test suite script. 4. Close Terminal.

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

Table A.18: T-IB-UC1-02 Test Sheet

Test ID	Test Name	Responsible
T-IB-UC1-02	TLS 1.3 handshake with different algorithm implementations	TAU

Brief Description

This test leverages the full configurability of the *QUBIP Provider* solution to assess the impact on performance of selecting different implementations for the same algorithm. In particular, we measure the impact on TLS 1.3 handshake latency when using two instances of the *QUBIP Provider*, configured to utilize two different backend external implementations for the same algorithm (and same parameter set).
The goal is to showcase how the extreme agility of the QUBIP solution allows stakeholders to make different choices and tradeoffs to better suite their operational conditions.

KPI Name(s)

- TLS 1.3 Handshake Latency

Test Procedure

1. Open Terminal.
2. For each selected *ciphersuite* configuration:
   a) For each selected alternative implementation:
      i. Run `export OPENSSL_CONF=~/implementation_X.cnf` to select a QUBIP Provider instance for the selected backend implementation.
      ii. Execute the `T-IB-UC1-01` test suite script.
      iii. Collect the results from the the output of the `T-IB-UC1-01` test suite script.
   b) Compare the measures to assess the impact of each different implementation.
3. Close Terminal.

Additional Notes

For this test, a *ciphersuite* configuration consists of the tuple

$$((\text{algorithm}, \text{parameter set})_{\text{KEx}}, (\text{algorithm}, \text{parameter set})_{\text{Auth}})$$

of settings for the TLS 1.3 key exchange and authentication mechanisms. A number of relevant *ciphersuites* must be selected to showcase relevant scenarios. For each selected *ciphersuite* a number of alternative implementations (compatible with the requirements of the QUBIP Provider) is selected to showcase the different impact on TLS 1.3 Handshake Latency. The results obtained are also compared with those obtained using classical algorithms.

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

Table A.19: T-IB-UC1-03 Test Sheet

Test ID	Test Name	Responsible
T-IB-UC1-03	TLS 1.3 latency variation with QUBIP solution for full configurability	TAU

Brief Description

The design of the QUBIP solution is characterized by a high degree of configurability and cryptographic agility. This test aims to assess the impact of these properties on the TLS 1.3 latency, compared to current community trends for PQC transition experiments.
We selected the `oqs-provider` alternative as our baseline, as it reflects current community trends and is also functionally similar to the QUBIP solution: the QUBIP Provider aims for an even higher degree of flexibility.
As the extra flexibility can have an impact on memory and computation costs, we assess the overhead of the QUBIP solution through its impact on TLS 1.3 latency against the selected baseline.

KPI Name(s)

- TLS 1.3 Handshake Latency Overhead

Test Procedure

1. Open Terminal.
2. For each selected *ciphersuite* configuration:
   a) Run `export OPENSSL_CONF=~/QUBIP_conf_X.cnf` to select a QUBIP Provider instance for the selected *ciphersuite* configuration.
   b) Execute the `T-IB-UC1-01` test suite script.
   c) Collect the TLS 1.3 Handshake Latency results from the the output of the test suite script.
   d) Run `export OPENSSL_CONF=~/oqs-provider_conf_X.cnf` to select an alternative baseline for the selected *ciphersuite* configuration based on `oqs-provider`.
   e) Execute the `T-IB-UC1-01` test suite script.
   f) Collect the TLS 1.3 Handshake Latency results from the the output of the test suite script.
   g) Compute the overhead as the ratio between the metric for the QUBIP solution and the baseline.
3. Close Terminal.

Additional Notes

For this test, a *ciphersuite* configuration consists of the tuple

$$((\mathrm{algorithm}, \mathrm{parameter\ set})_{\mathrm{KEx}}, (\mathrm{algorithm}, \mathrm{parameter\ set})_{\mathrm{Auth}})$$

of settings for the TLS 1.3 key exchange and authentication mechanisms. The same *ciphersuites* selection of T-IB-UC1-02 can be used to showcase relevant scenarios.

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

Table A.20: T-IB-UC1-04 Test Sheet

Test ID	Test Name	Responsible
T-IB-UC1-04	Overall system performance	TAU

Brief Description

This test evaluates the overall system performance as experienced by the user, based on the metrics TTFB and FCP. The goal is to measure how quickly a user notices a response when a resource is requested from the server, providing insight on the impact of the network changes on the user experience.

KPI Name(s)

- TTFB
- FCP

Test Procedure

1. For each selected *ciphersuite* configuration:
   a) Run a webserver instance using *OpenSSL with QUBIP Provider* as the `target` for testing. The instance must be configured according to the specific *ciphersuite* configuration, and serve content embedding the JavaScript code required to measure the metrics.
   b) Run a browser automation script to repeat 1000 times a connection between *(QUBIP) Mozilla Firefox* and `target`. recording the metrics measured through the JavaScript content.
   c) Statistically analyze the collected results, to generate a report for the selected *ciphersuite*.
2. Report the impact of each selected *ciphersuite* on the metrics, providing objective insight on the effects on user experience.

Additional Notes

For this test, a *ciphersuite* configuration consists of the tuple

$$((\text{algorithm}, \text{parameter set})_{\text{KEx}}, (\text{algorithm}, \text{parameter set})_{\text{Auth}})$$

of settings for the TLS 1.3 key exchange and authentication mechanisms.

Table A.21: T-IB-UC1-05 Test Sheet

Test ID	Test Name	Responsible
T-IB-UC1-05	Public Key Infrastructure	POLITO

Brief Description

This test evaluates the performance and security metrics of PKI certificates across different *profiles*, consisting of different configurations for Root, Intermediate and Leaf certificates.

KPI Name(s)

- PKI Certificate Size
- CSR Generation
- PKI Verification
- PKI Algorithm Strength

Test Procedure

For each *PKI profile*:

1. generate certificate chain,
2. measure root, intermediate, and leaf certificate sizes,
3. measure overall verification speed,
4. take note of algorithm strength (i.e., NIST security level) for Root, Intermediate, and Leaf certificates.

Additional Notes

A *PKI profile* consists of the selected algorithms and parameter sets for Root, Intermediate, and Leaf certificates. A selection of *PKI profile* to be tested must be performed before the tests. Repeat for all *PKI profile* and summarize the results.

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

Table A.22: T-IB-UC1-06 Test Sheet

Test ID	Test Name	Responsible
T-IB-UC1-06	User experience	CIB

Brief Description

This test will be focused on users' human-machine interaction mechanisms needed for measuring the impact of quantum-secure elements integrated within the tools enabling their everyday life experience in the Internet as digital citizens. Apart from Demographic Data, and Level of Understanding, the users will be asked to score the perceived usefulness of the quantum-secure system implemented, their overall satisfaction from a UX perspective, the ease of use of the functionalities implemented, or its perceived level of performance, security and privacy.

KPI Name(s)

- Ease of Use
- User Satisfaction
- Perceived TLS 1.3 Connection Latency
- Perceived Security, Privacy and Accessibility
- Usability and Speed Perception
- Adoption

Test Procedure

1. Open the feedback form link from the playbook.
2. Answer all the mandatory questions included.
3. Review the answers.
4. Submit the fulfilled feedback form.
5. Close the tab.

Additional Notes

A virtual a preparatory session to the users intended to be joining this test will be delivered prior to be running this test itself.

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

Table A.23: T-IB-UC1-INTEROPERABILITY-01 Test Sheet

Test ID	Test Name	Responsible
T-IB-UC1-INTEROPERABILITY-01	Interoperability against Cloudflare	TAU

Brief Description

This test verifies the establishment of a TLS 1.3 handshake using PQC. Both *(QUBIP) Mozilla Firefox* and *OpenSSL with QUBIP Provider* are tested against Cloudflare's PQC testing website to confirm successful handshake establishment and interoperability.

KPI Name(s)

- TLS 1.3 Handshake Establishment
  - *(QUBIP) Mozilla Firefox* against Cloudflare
  - *OpenSSL with QUBIP Provider* against Cloudflare

Test Procedure

For each selected *ciphersuite* configuration:

1. select corresponding Cloudflare PQC testing webserver as the `target` for interoperability testing,
2. run an `s_client` instance of *OpenSSL with QUBIP Provider* to connect against `target`,
3. record TLS 1.3 Handshake Establishment result,
4. run a browser automation script to have *(QUBIP) Mozilla Firefox* connect against `target`,
5. record TLS 1.3 Handshake Establishment result.

Additional Notes

For this test, a *ciphersuite* configuration consists of the tuple

$$((\text{algorithm}, \text{parameter set})_{\text{KEx}}, (\text{algorithm}, \text{parameter set})_{\text{Auth}})$$

of settings for the TLS 1.3 key exchange and authentication mechanisms.

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

Table A.24: T-IB-UC1-INTEROPERABILITY-02 Test Sheet

Test ID	Test Name	Responsible
T-IB-UC1-INTEROPERABILITY-02	Interoperability against OQS	TAU

Brief Description

This test verifies the establishment of a TLS 1.3 channel using PQC. Both *(QUBIP) Mozilla Firefox* and *OpenSSL with QUBIP Provider* are tested against OQS test servers to confirm successful handshake establishment and interoperability.

KPI Name(s)

- TLS 1.3 Handshake Establishment
  - *(QUBIP) Mozilla Firefox* against OQS
  - *OpenSSL with QUBIP Provider* against OQS

Test Procedure

For each selected *ciphersuite* configuration:

1. select corresponding OQS testing webserver as the `target` for interoperability testing,
2. run an `s_client` instance of *OpenSSL with QUBIP Provider* to connect against `target`,
3. record TLS 1.3 Handshake Establishment result,
4. run a browser automation script to have *(QUBIP) Mozilla Firefox* connect against `target`,
5. record TLS 1.3 Handshake Establishment result.

Additional Notes

For this test, a *ciphersuite* configuration consists of the tuple

$$((\text{algorithm}, \text{parameter set})_{\text{KEx}}, (\text{algorithm}, \text{parameter set})_{\text{Auth}})$$

of settings for the TLS 1.3 key exchange and authentication mechanisms.

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

Table A.25: T-IB-UC1-INTEROPERABILITY-03 Test Sheet

Test ID	Test Name	Responsible
T-IB-UC1-INTEROPERABILITY-03	Interoperability against QUBIP OpenSSL Server	TAU

Brief Description

This test verifies the establishment of a TLS 1.3 handshake using PQC. Both *upstream Mozilla Firefox* and *Google Chrome* are tested against a *QUBIP OpenSSL Server* to confirm successful handshake establishment and interoperability.

KPI Name(s)

- TLS 1.3 Handshake Establishment
  - *Upstream Mozilla Firefox* against *QUBIP OpenSSL Server*
  - *Google Chrome* against *QUBIP OpenSSL Server*

Test Procedure

For each selected *ciphersuite* configuration:

1. run a webserver instance using *OpenSSL with QUBIP Provider* as the `target` for interoperability testing; the instance must be configured according to the specific *ciphersuite* configuration,
2. run a browser automation script to have *(upstream) Mozilla Firefox* connect against `target`,
3. record TLS 1.3 Handshake Establishment result,
4. run a browser automation script to have *Google Chrome* connect against `target`,
5. record TLS 1.3 Handshake Establishment result.

Additional Notes

For this test, a *ciphersuite* configuration consists of the tuple

$$((\text{algorithm}, \text{parameter set})_{\text{KEx}}, (\text{algorithm}, \text{parameter set})_{\text{Auth}})$$

of settings for the TLS 1.3 key exchange and authentication mechanisms.

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

Table A.26: T-IB-UC2-01 Test Sheet

Test ID	Test Name	Responsible
T-IB-UC2-01	TLS 1.3 handshake	TAU
Brief Description		
This test evaluates the establishment of a TLS 1.3 handshake, measuring latency and traffic size using a suite of scripts that initiate a connection to a specified server. After successfully connecting to the server and completing the test script suite, the results can be retrieved for analysis.		
KPI Name(s)		
• TLS 1.3 Handshake Latency • TLS 1.3 Handshake Traffic Size • TLS 1.3 Handshake Establishment		
Test Procedure		
1. Open Terminal. 2. Execute the `T-IB-UC2-01` test suite script. 3. Collect the results from the the output of the `T-IB-UC2-01` test suite script. 4. Close Terminal.		

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

Table A.27: T-IB-UC2-02 Test Sheet

Test ID	Test Name	Responsible
T-IB-UC2-02	TLS 1.3 latency variation with QUBIP solution for full configurability	TAU

Brief Description

The design of the QUBIP solution is characterized by a high degree of configurability and cryptographic agility. This test aims to assess the impact of these properties on the TLS 1.3 latency, compared to current community trends for PQC transition experiments.
We selected the `oqs-provider` alternative as our baseline, as it reflects current community trends and is also functionally similar to the QUBIP solution: the *QUBIP Provider* aims for an even higher degree of flexibility.
As the extra flexibility can have an impact on memory and computation costs, we assess the overhead of the QUBIP solution through its impact on TLS 1.3 latency against the selected baseline.

KPI Name(s)

- TLS 1.3 Handshake Latency Overhead

Test Procedure

1. Open Terminal.
2. For each selected *ciphersuite* configuration:
   a) run `export OPENSSL_CONF=~/QUBIP_conf_X.cnf` to select a QUBIP Provider instance for the selected *ciphersuite* configuration,
   b) execute the `T-IB-UC2-01` test suite script,
   c) collect the TLS 1.3 Handshake Latency results from the the output of the test suite script,
   d) run `export OPENSSL_CONF=~/oqs-provider_conf_X.cnf` to select an alternative baseline for the selected *ciphersuite* configuration based on `oqs-provider`,
   e) execute the `T-IB-UC2-01` test suite script,
   f) collect the TLS 1.3 Handshake Latency results from the the output of the test suite script,
   g) compute the overhead as the ratio between the metric for the QUBIP solution and the baseline.
3. Close Terminal.

Additional Notes

For this test, a *ciphersuite* configuration consists of the tuple

$$((\text{algorithm}, \text{parameter set})_{\text{KEx}}, (\text{algorithm}, \text{parameter set})_{\text{Auth}})$$

of settings for the TLS 1.3 key exchange and authentication mechanisms. The same *ciphersuites* selection of T-IB-UC2-01 can be used to showcase relevant scenarios.

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

Table A.28: T-IB-UC2-03 Test Sheet

Test ID	Test Name	Responsible
T-IB-UC2-03	Overall system performance	TAU

Brief Description

This test evaluates the overall system performance as experienced by the user, based on the metrics TTFB and FCP. The goal is to measure how quickly a user notices a response when a resource is requested from the server, providing insight on the impact of the network changes on the user experience.

KPI Name(s)

- TTFB
- FCP

Test Procedure

1. For each selected *ciphersuite* configuration:
   a) run a webserver instance using *OpenSSL with QUBIP Provider* as the `target` for testing. The instance must be configured according to the specific *ciphersuite* configuration, and serve content embedding the JavaScript code required to measure the metrics,
   b) run a browser automation script to repeat 1000 times a connection between *(QUBIP) Mozilla Firefox* and `target`, recording the metrics measured through the JavaScript content,
   c) statistically analyze the collected results, to generate a report for the selected *ciphersuite*.
2. Report the impact of each selected *ciphersuite* on the metrics, providing objective insight on the effects on user experience.

Additional Notes

For this test, a *ciphersuite* configuration consists of the tuple

$$((\text{algorithm}, \text{parameter set})_{\text{KEx}}, (\text{algorithm}, \text{parameter set})_{\text{Auth}})$$

of settings for the TLS 1.3 key exchange and authentication mechanisms.

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

Table A.29: T-IB-UC2-04 Test Sheet

Test ID	Test Name	Responsible
T-IB-UC2-04	Public Key Infrastructure	POLITO
Brief Description		
This test evaluates the performance and security metrics of PKI certificates across different *PKI profile*, consisting of different configurations for Root, Intermediate and Leaf certificates.		
KPI Name(s)		
• PKI Certificate Size • CSR Generation • PKI Verification • PKI Algorithm Strength		
Test Procedure		
For each *PKI profile*: 1. generate certificate chain, 2. measure root, intermediate, and leaf certificate sizes, 3. measure overall verification speed, 4. take note of algorithm strength (i.e., NIST security level) for Root, Intermediate, and Leaf certificates.		
Additional Notes		
A *PKI profile* consists of the selected algorithms and parameter sets for Root, Intermediate, and Leaf certificates. A selection of *PKI profile* to be tested must be performed before the tests. Repeat for all *PKI profile* and summarize the results.		

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

Table A.30: T-IB-UC2-05 Test Sheet

Test ID	Test Name	Responsible
T-IB-UC2-05	User experience	CIB

Brief Description
This test will be focused on end-users' human-machine interaction mechanisms needed for measuring the impact of quantum-secure elements integrated within the tools enabling their everyday life experience in the Internet as digital citizens. Apart from Demographic Data, and Level of Understanding, the end users will be asked to score the perceived usefulness of the quantum-secure system implemented, their overall satisfaction from a UX perspective, the ease of use of the functionalities implemented, or its perceived level of performance and security.
KPI Name(s)
• Ease of Use • User Satisfaction • Perceived TLS 1.3 Connection Latency • Perceived Security, Privacy and Accesibility • Usability and Speed Perception • Adoption
Test Procedure
1. Open the feedback form link from the playbook. 2. Answer all the mandatory questions included. 3. Review the answers. 4. Submit the fulfilled feedback form. 5. Close the tab.
Additional Notes
A virtual a preparatory session to the end users intended to be joining this test will be delivered prior to be running this test itself.

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

Table A.31: T-IB-UC2-06 Test Sheet

Test ID	Test Name	Responsible
T-IB-UC2-06	Cryptographic agility	REDHAT
Brief Description		
This test case evaluates the agility provided by QUBIP solution, ensuring the system can seamlessly switch between algorithms, such as PQ/T hybrid, as needed for security or compliance. Therefore, the results for each implementation are collected and compared.		
KPI Name(s)		
• Cryptographic Agility		
Test Procedure		
1. Open terminal. 2. Run `export OPENSSL_CONF=~/config_1.cnf`. 3. Run test scripts for `T-IB-UC1-01` (for TLS 1.3 Handshake Establishment). 4. Run `export OPENSSL_CONF=~/config_2.cnf`. 5. Run test scripts for `T-IB-UC1-01` (for TLS 1.3 Handshake Establishment). 6. Collect and compare the results. 7. Close terminal.		
Additional Notes		
`config_1.cnf` and `config_2.cnf` should be modeled after selected *ciphersuites* used in T-IB-UC1-INTEROPERABILITY-01. The two *ciphersuites* should be selected to be different enough to effectively demonstrate the cryptographic agility of the QUBIP solution. `T-IB-UC1-01` scripts refer to Table A.17		

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

Table A.32: T-IB-UC2-07 Test Sheet

Test ID	Test Name	Responsible
T-IB-UC2-07	Openness	TAU
Brief Description		
This test evaluates the licensing terms for *NSS Module*, the *QUBIP Provider*, and the PKI to ensure compliance with recognized open-source licenses and compatibility across different licenses. The goal is to assess the openness of the software and identify potential licensing risks that could impact redistribution or usage.		
KPI Name(s)		
• Openness • License Risk		
Test Procedure		
1. Examine the software licensing terms for each component. 2. Verify the licensing terms match a recognized open-source license. 3. Verify the compatibility across different licensing terms. 4. Create a report with key findings.		

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

Table A.33: T-IB-SSI-UC3-01 Test Sheet

Test ID	Test Name	Responsible
T-IB-SSI-UC3-01	SSI identity generation	LINKS

Brief Description

This test aims to measure and assess the relevant metrics and KPIs for specific operations during the SSI Identity Generation, that are the creation of the DID and the issuance of a VC. This test involves only the Holder (i.e., client) and the Issuer (i.e., server) agents in the SSI generation process. This test assumes that the Holder has already installed and properly configured the wallet extension inside the Firefox browser, and the Issuer is up and running.

KPI Name(s)

- SSI Identity Generation Latency
- SSI Identity Generation Traffic Size
- SSI Operation Client Memory Fingerprint
- SSI Operation Server Memory Fingerprint
- Overall SSI Process Error Rate
- SSI Algorithm Strength

Test Procedure

1. Open the wallet extension.
2. Choose the desired system configuration (Traditional, PQ, or PQ/T hybrid) and generate the DID.
3. Connect to the Issuer web page and enter the required information for the credential subject of the VC.
4. Select the DID to bind to the VC, and execute a challenge-response protocol to authenticate the DID.
5. Request the VC to the Issuer.
6. Validate and save the issued VC into the wallet extension.
7. Take note of algorithm strength (i.e., NIST security level or equivalent) for cryptographic algorithms used in SSI operations.
8. Repeat the previous steps for the selected system configurations with Traditional, PQ, and PQ/T hybrid algorithms (at security level 1, 3, and 5).

Additional Notes

The aim of this test is to collect data that will improve the overall statistics, helping to assess the selected KPIs at the end of the measurement campaign. Among the different configurations under test, the QUBIP consortium will apply the acceptance criteria to identify the options with an acceptable performance.

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

Table A.34: T-IB-SSI-UC3-02 Test Sheet

Test ID	Test Name	Responsible
T-IB-SSI-UC3-02	SSI identity authentication	LINKS

Brief Description

This test aims to measure and assess the relevant metrics and KPIs for specific operations during the SSI Identity Authentication, related to the presentation of a VP. This test involves only the Holder (i.e., client) and the Verifier (i.e., server) agents in the SSI authentication process. This test assumes that the Holder has successfully completed the SSI Identity Generation procedure described in Table A.33 and the Verifier is up and running.

KPI Name(s)

- SSI Authentication Latency
- SSI Authentication Traffic Size
- SSI Operation Client Memory Fingerprint
- SSI Operation Server Memory Fingerprint
- Overall SSI Process Error Rate
- SSI Algorithm Strength

Test Procedure

1. Connect to the Verifier web page and start the authentication process.
2. Select the appropriate VC for the desired system configuration (Traditional, PQ, or PQ/T hybrid) from the wallet extension to begin the VP generation and presentation procedures.
3. Wait for the end of the authentication process (successful in case of a valid VC, or failure in case of a revoked VC).
4. Take note of algorithm strength (i.e., NIST security level or equivalent) for cryptographic algorithms used in SSI operations.
5. Repeat the previous steps for the selected system configurations with Traditional, PQ, and PQ/T hybrid algorithms (at security level 1, 3, and 5).

Additional Notes

The aim of this test is to collect data that will improve the overall statistics, helping to assess the selected KPIs at the end of the measurement campaign. Among the different configurations under test, the QUBIP consortium will apply the acceptance criteria to identify the options with an acceptable performance.

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

Table A.35: T-IB-SSI-UC3-03 Test Sheet

Test ID	Test Name	Responsible
T-IB-SSI-UC3-03	SSI identity revocation	LINKS

Brief Description

This test aims to measure and assess the relevant metrics and KPIs for specific operations during the revocation of a VC. This test involves the three agents (Holder, Issuer, and Verifier) in the SSI revocation process. This test assumes that the Holder has successfully completed the SSI Identity Generation procedure described in Table A.33 and both Issuer and Verifier are up and running.

KPI Name(s)

- SSI Authentication Latency
- SSI Authentication Traffic Size
- SSI Operation Client Memory Fingerprint
- SSI Operation Server Memory Fingerprint
- Overall SSI Process Error Rate
- SSI Algorithm Strength

Test Procedure

1. Connect to the Issuer web page and start the revocation process.
2. Select the appropriate VC for the desired system configuration (Traditional, PQ, or PQ/T hybrid) from the wallet extension to begin the VC revocation procedure.
3. Wait for the end of the revocation procedure.
4. Execute the SSI Identity Authentication process described in Table A.34, selecting the revoked VC, expecting its failure.
5. Take note of algorithm strength (i.e., NIST security level or equivalent) for cryptographic algorithms used in SSI operations.
6. Repeat the previous steps for the selected system configurations with Traditional, PQ, and PQ/T hybrid algorithms (at security level 1, 3, and 5).

Additional Notes

The aim of this test is to collect data that will improve the overall statistics, helping to assess the selected KPIs at the end of the measurement campaign. Among the different configurations under test, the QUBIP consortium will apply the acceptance criteria to identify the options with an acceptable performance.

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

Table A.36: T-IB-SSI-UC3-04 Test Sheet

Test ID	Test Name	Responsible
T-IB-SSI-UC3-04	User experience with SSI authentication	CIB

Brief Description

This test will be focused on users' human-machine interaction mechanisms needed for measuring the impact of quantum-secure elements integrated within the tools enabling their everyday life experience on the Internet as digital citizens. Apart from Demographic Data, and Level of Understanding, the users will be asked to score the perceived usefulness of the quantum-secure system implemented, their overall satisfaction from a UX perspective, the ease of use of the functionalities implemented, or its perceived level of performance, security and privacy.

KPI Name(s)

- Ease of Use
- User Satisfaction
- Perceived Security, Privacy and Accessibility
- Usability and Speed Perception
- Adoption

Test Procedure

1. Open the feedback form link from the playbook.
2. Answer all the mandatory questions included.
3. Review the answers.
4. Submit the fulfilled feedback form.
5. Close the tab.

Additional Notes

A virtual a preparatory session to the end users intended to be joining this test will be delivered prior to be running this test itself.

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

Table A.37: T-IB-SSI-UC3-05 Test Sheet

Test ID	Test Name	Responsible
T-IB-SSI-UC3-05	Openness	LINKS

Brief Description

This test evaluates the licensing terms of the SSI building block for PQ and PQ/T hybrid plaintext VCs to ensure compliance with recognized open-source licenses and compatibility across different licenses. The goal is to assess the openness of the software and identify potential licensing risks that could impact redistribution or usage.

KPI Name(s)

- Openness
- License Risk

Test Procedure

1. Examine the software licensing terms for each component.
2. Verify the licensing terms match a recognized open-source license.
3. Verify the compatibility across different licensing terms.
4. Create a report with key findings.

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

Table A.38: T-IB-SSI-UC4-01 Test Sheet

Test ID	Test Name	Responsible
T-IB-SSI-UC4-01	SSI identity generation	LINKS

Brief Description

This test aims to measure and assess the relevant metrics and KPIs for specific operations during the SSI Identity Generation, that are the creation of the DID and the issuance of an anonymous credential. This test involves only the Holder (i.e., client) and the Issuer (i.e., server) agents in the SSI generation process. This test assumes that the Holder has already installed and properly configured the wallet extension inside the Firefox browser, and the Issuer is up and running.

KPI Name(s)

- SSI Identity Generation Latency
- SSI Identity Generation Traffic Size
- SSI Operation Client Memory Fingerprint
- SSI Operation Server Memory Fingerprint
- Overall SSI Process Error Rate
- SSI Algorithm Strength

Test Procedure

1. Open the wallet extension.
2. Choose the desired system configuration (Traditional or PQ) and generate the DID.
3. Connect to the Issuer web page and enter the required information for the credential subject of the VC.
4. Select the DID to bind to the VC, and execute a challenge-response protocol to authenticate the DID.
5. Request the VC to the Issuer.
6. Validate and save the issued VC into the wallet extension.
7. Take note of algorithm strength (i.e., NIST security level or equivalent) for cryptographic algorithms used in SSI operations.
8. Repeat the previous steps for the selected system configurations with Traditional and PQ algorithms.

Additional Notes

The aim of this test is to collect data that will improve the overall statistics, helping to assess the selected KPIs at the end of the measurement campaign. Among the different configurations under test, the QUBIP consortium will apply the acceptance criteria to identify the options with an acceptable performance.

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

Table A.39: T-IB-SSI-UC4-02 Test Sheet

Test ID	Test Name	Responsible
T-IB-SSI-UC4-02	SSI identity authentication	LINKS

Brief Description

This test aims to measure and assess the relevant metrics and KPIs for specific operations during the SSI Identity Authentication, related to the presentation of anonymous credentials. This test involves the three agents (Holder, Issuer, and Verifier) in the SSI authentication process. Note that Issuer will only be involved in the process if the VC validity timeframe is expired and needs to be updated. This test assumes that the Holder has successfully completed the SSI Identity Generation procedure described in Table A.38 and both Issuer and Verifier are up and running.

KPI Name(s)

- SSI Authentication Latency
- SSI Authentication Traffic Size
- SSI Operation Client Memory Fingerprint
- SSI Operation Server Memory Fingerprint
- Overall SSI Process Error Rate
- SSI Algorithm Strength

Test Procedure

1. Connect to the Verifier web page and start the authentication process.
2. Select the appropriate VC for the desired system configuration (Traditional or PQ) from the wallet extension.
3. Select the attributes in the VC to be disclosed to the Verifier (if any) to begin the presentation procedures.
4. Wait for the end of the authentication process (successful in case of a valid VC, or failure in case of a revoked VC).
5. (Optional) Wait for the natural expiration of the VC validity timeframe and repeat the previous steps.
6. Take note of algorithm strength (i.e., NIST security level or equivalent) for cryptographic algorithms used in SSI operations.
7. Repeat the previous steps for the selected system configurations with Traditional and PQ algorithms.

Additional Notes

The aim of this test is to collect data that will improve the overall statistics, helping to assess the selected KPIs at the end of the measurement campaign. Among the different configurations under test, the QUBIP consortium will apply the acceptance criteria to identify the options with an acceptable performance.

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

Table A.40: T-IB-SSI-UC4-03 Test Sheet

Test ID	Test Name	Responsible
T-IB-SSI-UC4-03	SSI identity revocation	LINKS

Brief Description

This test aims to measure and assess the relevant metrics and KPIs for specific operations during the revocation of a VC. This test involves the three agents (Holder, Issuer, and Verifier) in the SSI revocation process. This test assumes that the Holder has successfully completed the SSI Identity Generation procedure described in Table A.38 and both Issuer and Verifier are up and running.

KPI Name(s)

- SSI Authentication Latency
- SSI Authentication Traffic Size
- SSI Operation Client Memory Fingerprint
- SSI Operation Server Memory Fingerprint
- Overall SSI Process Error Rate
- SSI Algorithm Strength

Test Procedure

1. Connect to the Issuer web page and start the revocation process.
2. Select the appropriate VC for the desired system configuration (Traditional or PQ) from the wallet extension to begin the VC revocation procedure.
3. Wait for the end of the revocation procedure.
4. Execute the SSI Identity Authentication process described in Table A.39, selecting the revoked VC, expecting its failure.
5. Take note of algorithm strength (i.e., NIST security level or equivalent) for cryptographic algorithms used in SSI operations.
6. Repeat the previous steps for the selected system configurations with Traditional and PQ algorithms.

Additional Notes

The aim of this test is to collect data that will improve the overall statistics, helping to assess the selected KPIs at the end of the measurement campaign. Among the different configurations under test, the QUBIP consortium will apply the acceptance criteria to identify the options with an acceptable performance.

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

Table A.41: T-IB-SSI-UC4-04 Test Sheet

Test ID	Test Name	Responsible
T-IB-SSI-UC4-04	User experience with anonymous authentication with selective disclosure	CIB

Brief Description
This test will be focused on end-users' human-machine interaction mechanisms needed for measuring the impact of quantum-secure elements integrated within the tools enabling their everyday life experience in the Internet as digital citizens. Apart from Demographic Data, and Level of Understanding, the end users will be asked to score the perceived usefulness of the quantum-secure system implemented, their overall satisfaction from a UX perspective, the ease of use of the functionalities implemented, or its perceived level of performance and security.
KPI Name(s)
• Ease of Use • User Satisfaction • Perceived Security, Privacy and Accessibility • Usability and Speed Perception • Adoption
Test Procedure
1. Open the feedback form link from the playbook. 2. Answer all the mandatory questions included. 3. Review the answers. 4. Submit the fulfilled feedback form. 5. Close the tab.
Additional Notes
A virtual a preparatory session to the end users intended to be joining this test will be delivered prior to be running this test itself.

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

Table A.42: T-IB-SSI-UC4-05 Test Sheet

Test ID	Test Name	Responsible
T-IB-SSI-UC4-05	Openness	LINKS
Brief Description		
This test evaluates the licensing terms of the SSI building block for PQ anonymous credentials to ensure compliance with recognized open-source licenses and compatibility across different licenses. The goal is to assess the openness of the software and identify potential licensing risks that could impact redistribution or usage.		
KPI Name(s)		
• Openness • License Risk		
Test Procedure		
1. Examine the software licensing terms for each component. 2. Verify the licensing terms match a recognized open-source license. 3. Verify the compatibility across different licensing terms. 4. Create a report with key findings.		

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

A.3. Quantum-Secure Software Network Environments for Telco Operators

Table A.43: T-SNE-UC1-01 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC1-01	Quantum key delivery	UPM
Brief Description		
To measure the delay for a key request to the hybridization module to be served when only the QKD module is available.		
KPI Name(s)		
• Hybrid Key Delivery Time • Key Generation Success Rate		
Test Procedure		
1. Start two K8s worker nodes and the K8s controller node. 2. Configure the hybridization module such that the network link corresponding to the PQ KEM is not available. 3. Establish an IPsec tunnel between the two K8s worker nodes, measuring and saving the time between the key request of the agent to the hybridization module, and the successful key delivery from the hybridization module to the agent. If no key is delivered, mark this attempt as failed. 4. Delete the IPsec tunnel. 5. Repeat 1000 times steps 3 and 4. 6. Establish a classical IPsec tunnel between the two K8s worker nodes, measuring and saving the time between the key request of the agent and the successful key delivery from the classic IKEv2. 7. Delete the classical IPsec tunnel. 8. Repeat 1000 times steps 6 and 7 9. Compute the average delivery time for the quantum-secure IPsec tunnel and the classical one, together with the ratio of successful key requests for the quantum-secure IPsec tunnel.		
Additional Notes		
Both wire and free-space QKD links will be tested.		

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

Table A.44: T-SNE-UC1-02 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC1-02	PQ key delivery	UPM

Brief Description
To measure the delay for a key request to the hybridization module to be served when only the PQ KEM link is available.
KPI Name(s)
• Hybrid Key Delivery Time • Key Generation Success Rate
Test Procedure
1. Start two K8s worker nodes and the K8s controller node. 2. Configure the hybridization module such that the QKD module is not available. 3. Establish an IPsec tunnel between the two K8s worker nodes, measuring and saving the time between the key request of the agent to the hybridization module, and the successful key delivery from the hybridization module to the agent. If no key is delivered, mark this attempt as failed. 4. Delete the IPsec tunnel. 5. Repeat 1000 times steps 3 and 4. 6. Establish a classical IPsec tunnel between the two K8s worker nodes, measuring and saving the time between the key request of the agent and the successful key delivery from the classic IKEv2. 7. Delete the classical IPsec tunnel. 8. Repeat 1000 times steps 6 and 7. 9. Compute the average delivery time for the quantum-secure IPsec tunnel and the classical one, together with the ratio of successful key requests for the quantum-secure IPsec tunnel.

Table A.45: T-SNE-UC1-03 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC1-03	Hybrid key delivery	UPM

Brief Description

To measure the delay for a key request to the hybridization module to be served when the PQ KEM and the QKD links are both available.

KPI Name(s)

- Hybrid Key Delivery Time
- Key Generation Success Rate

Test Procedure

1. Start two K8s worker nodes and the K8s controller node.
2. Establish an IPsec tunnel between the two K8s worker nodes, measuring and saving the time between the key request of the agent to the hybridization module, and the successful key delivery from the hybridization module to the agent. If no key is delivered, mark this attempt as failed.
3. Delete the IPsec tunnel.
4. Repeat 1000 times steps 3 and 4.
5. Establish a classical IPsec tunnel between the two K8s worker nodes, measuring and saving the time between the key request of the agent and the successful key delivery from the key exchange in IKEv2.
6. Delete the classical IPsec tunnel.
7. Repeat 1000 times steps 6 and 7.
8. Compute the average delivery time for the quantum-secure IPsec tunnel and the classical one, together with the ratio of successful key requests for the quantum-secure IPsec tunnel.

Additional Notes

Both wire and free-space QKD links will be tested.

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

Table A.46: T-SNE-UC1-04 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC1-04	Min-entropy	UPM
Brief Description		
To measure the min-entropy of the hybrid key delivered by the hybridization module.		
KPI Name(s)		
• Min-entropy Quality		
Test Procedure		
1. Start two K8s worker nodes and the K8s controller node. 2. Establish a quantum-secure IPsec tunnel between the two K8s nodes, saving the hybrid key used to generate the IPsec tunnel and computing the min-entropy of such key. 3. Delete the IPsec tunnel. 4. Repeat 1000 times the steps 2 and 3. 5. Establish a classical IPsec tunnel between the two K8s nodes, saving the classical key used to generate the IPsec tunnel and computing the min-entropy of such key. 6. Delete the IPsec tunnel. 7. Repeat 1000 times the steps 5 and 6.		
Additional Notes		
Both wire and free-space QKD links will be tested.		

Table A.47: T-SNE-UC1-05 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC1-05	Hybrid quote generation	POLITO
Brief Description		
This test assesses the time required to generate a hybrid quote and compares it to classical quote. It evaluates whether PQ wrapping introduces manageable overhead in both generation time and network usage.		
KPI Name(s)		
• Hybrid Quote Generation Time		
Test Procedure		
1. Initialize remote attestation and verify both agent and trust manager are operational. 2. Execute 1000 cycles of remote attestation with classical quotes to assess stability. All cycles should return a success if no integrity violation occurs. 3. repeat with hybrid quote, recording the time taken. 4. Calculate the ratio of hybrid quote generation time to classical quote generation time and confirm it meets the target.		
Additional Notes		
Collected data will support the validation of acceptance criteria and enhance statistical accuracy for KPI assessment. The QUBIP consortium will analyze results to confirm configurations that meet stability, detection, and timing performance thresholds.		

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

Table A.48: T-SNE-UC1-06 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC1-06	Detection of a compromised node during remote attestation	POLITO

Brief Description
This test run during the process of the L2S-M setting up the tunnel and evaluates the remote attestation latency, namely the time to detect a compromised node.
KPI Name(s)
• Remote Attestation Latency • Time to Detect a Compromised Node
Test Procedure
1. Setup: a) Ensure the attestation framework is configured and operational. 2. Detection of compromised node: a) Simulate a compromise on the Attester node by introducing an invalid measurement or altering the attestation report. b) Start the attestation process. c) Record the time at which the node is compromised. d) Record the time at which the Verifier detects the compromise. e) Calculate the detection time as the difference between these two timestamps. f) Repeat the process 1000 times and compute the average value. g) Ensure that the KPI meets its respective threshold.
Additional Notes
Ensure that the time measurement tools have sufficient resolution to accurately capture the timestamps.

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

Table A.49: T-SNE-UC1-07 Test Sheet

Test ID	Test Name	Responsible
T-SNE–UC1-07	Bandwidth consumption during remote attestation	POLITO
Brief Description		
This test measures the bandwidth consumption during the transmission of the hybrid integrity report, and compares it with the case of a classical report.		
KPI Name(s)		
• Bandwidth Utilization during RA		
Test Procedure		
1. Initialize remote attestation and verify both agent and trust manager are operational. 2. Execute 1000 cycles of remote attestation with classical quotes. All cycles should return a success if no integrity violation occurs. 3. Repeat with hybrid quote, recording the time taken. 4. Calculate the ratio of hybrid quote generation time to classical quote generation time and confirm it meets the target.		
Additional Notes		
Collected data will support the validation of acceptance criteria and enhance statistical accuracy for KPI assessment. The QUBIP consortium will analyze results to confirm configurations that meet stability, detection, and timing performance thresholds.		

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

Table A.50: T-SNE-UC1-08 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC1-08	Telco management software integration for network service deployment	TID
Brief Description		
The addition of CCIPS and its integration into the management tools will require changes in management and operational activities. This test will measure, over open-source solutions such as K8s or OSM, how many changes are needed in the operational procedures to set up a secure network service with IPsec in NFV/SDN architecture and the deployment success rate.		
KPI Name(s)		
• Network Service Deployment • Telco Management Software		
Test Procedure		
1. Deploy a defined network service with 2 CNFs and activate IPsec connectivity over classical algorithms. 2. Measure the time required and the number of commands used. 3. Repeat the process with the CCIPS hybrid approach. 4. Measure the time required and the number of commands used. 5. Repeat last two steps 1000 times and measure whether errors have occurred.		
Additional Notes		
The analysis focuses on evaluate the end to end functionality and the impact of additional complexity and the time required to add transition methods into existing management tools (not on the code or the integration to implement the functionality). Open-source tools will be used.		

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

Table A.51: T-SNE-UC1-09 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC1-09	Encrypted traffic throughput	TID

Brief Description
This test will measure the average traffic throughput between 2 CNFs with classical and hybrid encryption keys.
KPI Name(s)
• Encrypted Traffic Throughput
Test Procedure
1. Deploy a network service in K8s with L2S-M to provide connectivity with 2 different CNFs (pods). 2. Enable IPsec with the classical IKEv2. 3. Execute a set of 5 iterations with a duration of 1 min with *iperf* (or a similar tool) to measure the bandwidth between two CNFs protected by IPsec. 4. Enable IPsec with CCIPS implementation and hybrid keys. 5. Repeat step 3.
Additional Notes
This test aims to evaluate the impact of the proposed transition approach to bandwidth consumption.

Table A.52: T-SNE-UC1-10 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC1-10	Key generation and management	TID
Brief Description		
This test analyses the network traffic in the data plane between different workloads, searching keys related information exposed during the key generation and exchange phase.		
KPI Name(s)		
• Key Generation and Exchange.		
Test Procedure		
1. Deploy a network service in K8s with L2S-M to provide connectivity with 2 different CNFs (pods). 2. Configure a probe or tap in the overlay network defined by L2S-M towards another pod and activate the traffic capture and record. 3. Enable the CCIPS with different hybrid key combinations (classical, PQC and quantum) and interchange a few packets in each mode. 4. Stop the capture and analyse the traffic with *tcpdump* or *wireshark* searching plain text. 5. Identify if keys or related materials has been exposed.		
Additional Notes		
The test assess the processes involved in key lifecycle management, where a security perimeter offered by the facility is assumed, including the generation of secure keys and safe storage.		

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

Table A.53: T-SNE-UC1-11 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC1-11	IPsec tunnel provisioning	TID

Brief Description

This test measure the overhead in setting-up the IPsec-based connectivity service. The impact on the re-keying process is based on pre-defined security policies.

KPI Name(s)

- IPsec Tunnel Provisioning
- IPsec Tunnel Re-keying

Test Procedure

1. Deploy a network service with 2 CNFs.
2. Activate IPsec connectivity over classical IKEv2 and measure the time.
3. Trigger a re-keying process using IKEv2 and measure time.
4. Verify that the hybrid module has enough key to deliver to CCIPS.
5. Repeat the step 2 and 3 process with the CCIPS and hybrid key.

Additional Notes

Adding a CCIPS hybrid solution will require additional processes, such as key generation and collection from QKD network, PQ KEM, and key hybridization, jointly with remote attestation processes. Most of these processes can be executed beforehand (e.g., collecting keys and generating hybrid ones) and are not considered because they are done the first time and do not affect the service's performance later on.
Both wire and free-space QKD links will be tested.

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

Table A.54: T-SNE-UC1-12 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC1-12	Openness	TID
Brief Description		
This test case evaluates the licensing terms of all software components to ensure compliance with recognized open-source licenses and compatibility across different licenses. The goal is to assess the openness of the software and identify potential licensing risks that could impact redistribution or usage.		
KPI Name(s)		
• Openness • License Risk		
Test Procedure		
1. Examine the software licensing terms for each component. 2. Verify the licensing terms match a recognized open-source license. 3. Verify the compatibility across different licensing terms. 4. Create a report with key findings.		

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

Table A.55: T-SNE-UC2-01 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC2-01	Quantum key delivery	UPM
Brief Description		
To measure the delay for a key request to the hybridization module to be served when only the QKD module is available.		
KPI Name(s)		
• Hybrid Key Delivery Time • Key Generation Success Rate		
Test Procedure		
1. Start two K8s worker nodes and the K8s controller node. 2. Configure the hybridization module such that the network link corresponding to the PQ KEM is not available. 3. Establish an IPsec tunnel between the two K8s worker nodes, measuring and saving the time between the key request of the agent to the hybridization module, and the successful key delivery from the hybridization module to the agent. If no key is delivered, mark this attempt as failed. 4. Delete the IPsec tunnel. 5. Repeat 1000 times steps 3 and 4. 6. Establish a classical IPsec tunnel between the two K8s worker nodes, measuring and saving the time between the key request of the agent and the successful key delivery from the classic IKEv2. 7. Delete the classical IPsec tunnel. 8. Repeat 1000 times steps 6 and 7 9. Compute the average delivery time for the quantum-secure IPsec tunnel and the classical one, together with the ratio of successful key requests for the quantum-secure IPsec tunnel.		
Additional Notes		
Both wire and free-space QKD links will be tested.		

Table A.56: T-SNE-UC2-02 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC2-02	PQ key delivery	UPM
Brief Description		
To measure the time delay for key request to the hybridization module when only the PQ KEM link is available.		
KPI Name(s)		
• Hybrid Key Delivery Time • Key Generation Success Rate		
Test Procedure		
1. Start two K8s worker nodes and the K8s controller node. 2. Configure the hybridization module such that the QKD module is not available. 3. Establish an IPsec tunnel between the two K8s worker nodes, measuring and saving the time between the key request of the agent to the hybridization module, and the successful key delivery from the hybridization module to the agent. If no key is delivered, mark this attempt as failed. 4. Delete the IPsec tunnel. 5. Repeat 1000 times steps 3 and 4. 6. Establish a classical IPsec tunnel between the two K8s worker nodes, measuring and saving the time between the key request of the agent and the successful key delivery from the classic IKEv2. 7. Delete the classical IPsec tunnel. 8. Repeat 1000 times steps 6 and 7. 9. Compute the average delivery time for the quantum-secure IPsec tunnel and the classical one, together with the ratio of successful key requests for the quantum-secure IPsec tunnel.		

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

Table A.57: T-SNE-UC2-03 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC2-03	Hybrid key delivery	UPM

Brief Description

To measure the delay for a key request to the hybridization module to be served when the PQ KEM and the QKD links are both available.

KPI Name(s)

- Hybrid Key Delivery Time
- Key Generation Success Rate

Test Procedure

1. Start two K8s worker nodes and the K8s controller node.
2. Establish an IPsec tunnel between the two K8s worker nodes, measuring and saving the time between the key request of the agent to the hybridization module, and the successful key delivery from the hybridization module to the agent. If no key is delivered, mark this attempt as failed.
3. Delete the IPsec tunnel.
4. Repeat 1000 times steps 3 and 4.
5. Establish a classical IPsec tunnel between the two K8s worker nodes, measuring and saving the time between the key request of the agent and the successful key delivery from the classical KEM in IKEv2.
6. Delete the classical IPsec tunnel.
7. Repeat 1000 times steps 6 and 7.
8. Compute the average delivery time for the quantum-secure IPsec tunnel and the classical one, together with the ratio of successful key requests for the quantum-secure IPsec tunnel.

Additional Notes

Both wire and free-space QKD links will be tested.

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

Table A.58: T-SNE-UC2-04 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC2-04	Min-entropy	UPM
Brief Description		
To measure the min-entropy of the hybrid key delivered by the hybridization module.		
KPI Name(s)		
• Min-entropy Quality		
Test Procedure		
1. Start two K8s worker nodes and the K8s controller node. 2. Establish a quantum-secure IPsec tunnel between the two K8s nodes, saving the hybrid key used to generate the IPsec tunnel and computing the min-entropy of such key. 3. Delete the IPsec tunnel. 4. Repeat 1000 times the steps 2 and 3. 5. Establish a classical IPsec tunnel between the two K8s nodes, saving the classical key used to generate the IPsec tunnel and computing the min-entropy of such key. 6. Delete the IPsec tunnel. 7. Repeat 1000 times the steps 5 and 6.		
Additional Notes		
Both wire and free-space QKD links will be tested.		

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

Table A.59: T-SNE-UC2-05 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC2-05	Telco management software integration for network service deployment	TID
Brief Description		
The addition of CCIPS and its integration into the management tools will require changes in management and operational activities. This test will measure, over open-source solutions such as K8s or OSM, how many changes are needed in the operational procedures to set up a secure network service with IPSec in NFV/SDN architecture and the deployment success rate.		
KPI Name(s)		
• Network Service Deployment • Telco Management Software		
Test Procedure		
1. Deploy a defined network service with 2 CNFs and activate IPsec connectivity over classical algorithms. 2. Measure the time required and the number of commands used. 3. Repeat the process with the CCIPS hybrid approach. 4. Measure the time required and the number of commands used. 5. Repeat last two steps 5 times and measure whether errors have occurred.		
Additional Notes		
The analysis focuses on evaluate the end to end functionality and the impact of additional complexity and the time required to add transition methods into existing management tools (not on the code or the integration to implement the functionality). Open-source tools will be used.		

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

Table A.60: T-SNE-UC2-06 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC2-06	Encrypted traffic throughput	TID
Brief Description		
This test will measure the average traffic throughput between 2 CNFs with classical and hybrid encryption keys.		
KPI Name(s)		
• Encrypted Traffic Throughput		
Test Procedure		
1. Deploy a network service in K8s with L2S-M to provide connectivity with 2 different CNFs (pods). 2. Enable IPsec with the classical IKEv2. 3. Execute a set of 5 iterations with a duration of 1 min with *iperf* (or a similar tool) to measure the bandwidth between two CNFs protected by IPsec. 4. Enable IPsec with CCIPS implementation and hybrid keys. 5. Repeat step 3.		
Additional Notes		
This test aims to evaluate the impact of the proposed transition approach to bandwidth consumption.		

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

Table A.61: T-SNE-UC2-07 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC2-07	Key generation and management	TID
Brief Description		
This test analyses the network traffic in the data plane between different workloads, searching keys related information exposed during the key generation and exchange phase.		
KPI Name(s)		
• Key Generation and Exchange		
Test Procedure		
1. Deploy a network service in K8s with L2S-M to provide connectivity with 2 different CNFs (pods). 2. Configure a probe or tap in the overlay network defined by L2S-M towards another pod and activate the traffic capture and record. 3. Enable the CCIPS with different hybrid key combinations (classical, PQC and quantum) and interchange a few packets in each mode. 4. Stop the capture and analyse the traffic with *tcpdump* or *wireshark* searching plain text. 5. Identify if keys or related materials has been exposed.		
Additional Notes		
The test assess the processes involved in key lifecycle management, where a security perimeter offered by the facility is assumed, including the generation of secure keys and safe storage.		

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

Table A.62: T-SNE-UC2-08 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC2-08	IPsec tunnel provisioning	TID

Brief Description
This test measure the overhead in setting-up the IPsec-based connectivity service. The impact on the re-keying process is based on pre-defined security policies.
KPI Name(s)
• IPsec Tunnel Provisioning • IPsec Tunnel Re-keying
Test Procedure
1. Deploy a network service with 2 CNFs. 2. Activate IPsec connectivity over classical IKEv2 and measure the time. 3. Trigger a re-keying process using IKEv2 and measure time. 4. Verify that the hybrid module has enough key to deliver to CCIPS. 5. Repeat the step 2 and 3 process with the CCIPS and hybrid key.
Additional Notes
Adding a CCIPS hybrid solution will require additional processes, such as key generation and collection from QKD network, PQ KEM, and key hybridization. Most of these processes can be executed beforehand (e.g., collecting keys and generating hybrid ones) and are not considered because they are done the first time and do not affect the service's performance later on. Both wire and free-space QKD links will be tested.

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

Table A.63: T-SNE-UC3-01 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC3-01	PQ key delivery	UPM
Brief Description		
To measure the time delay for key request to the hybridization module when only the PQ KEM link is available.		
KPI Name(s)		
• Hybrid Key Delivery Time • Key Generation Success Rate		
Test Procedure		
1. Start two K8s worker nodes and the K8s controller node. 2. Configure the hybridization module such that the QKD module is not available. 3. Establish an IPsec tunnel between the two K8s worker nodes, measuring and saving the time between the key request of the agent to the hybridization module, and the successful key delivery from the hybridization module to the agent. If no key is delivered, mark this attempt as failed. 4. Delete the IPsec tunnel. 5. Repeat 1000 times steps 3 and 4. 6. Establish a classical IPsec tunnel between the two K8s worker nodes, measuring and saving the time between the key request of the agent and the successful key delivery from the classic IKEv2. 7. Delete the classical IPsec tunnel. 8. Repeat 1000 times steps 6 and 7. 9. Compute the average delivery time for the quantum-secure IPsec tunnel and the classical one, together with the ratio of successful key requests for the quantum-secure IPsec tunnel.		

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

Table A.64: T-SNE-UC3-02 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC3-02	Fallback procedure	UPM
Brief Description		
To evaluate the effectiveness of the fallback procedure due to the lack of QKD availability. The procedure involves the reconfiguration of the IPsec tunnel such that the hybrid key used to secure the communication doesn't have a quantum key as a component key.		
KPI Name(s)		
• Fallback		
Test Procedure		
1. Start two K8s worker nodes and the K8s controller node. 2. Establish a quantum-secure IPsec tunnel between the two K8s nodes. 3. Start a fallback procedure for QKD and measure the time employed.		

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

Table A.65: T-SNE-UC3-03 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC3-03	Hybrid quote generation	POLITO
Brief Description		
This test assesses the time required to generate a hybrid attestation quote and compares it with a classical quote.		
KPI Name(s)		
• Hybrid Quote Generation Time		
Test Procedure		
1. Initialize remote attestation and verify both agent and trust manager are operational. 2. Execute 1000 cycles of remote attestation with classical quotes and record the quote generation time. All cycles should return a success if no integrity violation occurs. 3. Repeat with hybrid quote, recording the time taken. 4. Calculate the ratio of hybrid quote generation time to classical quote generation time and confirm it meets the target.		
Additional Notes		
Collected data will support the validation of acceptance criteria and enhance statistical accuracy for KPI assessment. The QUBIP consortium will analyze results to confirm configurations that meet stability, detection, and timing performance thresholds.		

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

Table A.66: T-SNE-UC3-04 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC3-04	Detection of a compromised node during remote attestation	POLITO
Brief Description		
This test runs during the process of the L2S-M setting up the IPsec tunnel and evaluates the remote attestation latency, namely the time to detect a compromised node.		
KPI Name(s)		
• Remote Attestation Latency • Time to Detect a Compromised Node		
Test Procedure		
1. Setup: a) Ensure the attestation framework is configured and operational. 2. Detection of compromised node: a) Simulate a compromise on the Attester node by introducing an invalid measurement or altering the attestation report. b) Start the attestation process. c) Record the time at which the node is compromised. d) Record the time at which the Verifier detects the compromise. e) Calculate the detection time as the difference between these two timestamps. f) Repeat the process 1000 times and compute the average value. g) Ensure that the KPI meets its respective threshold.		
Additional Notes		
Ensure that the time measurement tools have sufficient resolution to accurately capture the timestamps.		

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

Table A.67: T-SNE-UC3-05 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC3-05	Bandwidth consumption during remote attestation	POLITO
Brief Description		
This test measures the bandwidth consumption during the transmission of the hybrid integrity report, and compares it with the case of a classical report.		
KPI Name(s)		
• Bandwidth Utilization during RA		
Test Procedure		
1. Initialize remote attestation and verify both agent and trust manager are operational. 2. Execute 1000 cycles of remote attestation with PQ-wrapped quotes. All cycles should return a success if no integrity violation occurs. Record data sent/received in [kbps]. 3. Calculate the average of bandwidth consumption and confirm it meets the target.		
Additional Notes		
Collected data will support the validation of acceptance criteria and enhance statistical accuracy for KPI assessment. The QUBIP consortium will analyze results to confirm configurations that meet stability, detection, and timing performance thresholds.		

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

Table A.68: T-SNE-UC3-06 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC3-06	Telco management software integration for network service deployment	TID
Brief Description		
The addition of CCIPS and its integration into the management tools will require changes in management and operational activities. This test will measure, over open-source solutions such as K8s or OSM, how many changes are needed in the operational procedures to set up a secure network service with IPsec in NFV/SDN architecture and the deployment success rate.		
KPI Name(s)		
• Network Service Deployment • Telco Management Software		
Test Procedure		
1. Deploy a defined network service with 2 CNFs and activate IPsec connectivity over classical algorithms. 2. Measure the time required and the number of commands used. 3. Repeat the process with the CCIPS hybrid approach. 4. Measure the time required and the number of commands used. 5. Repeat last two steps 1000 times and measure whether errors have occurred.		
Additional Notes		
The analysis focuses on evaluate the end to end functionality and the impact of additional complexity and the time required to add transition methods into existing management tools (not on the code or the integration to implement the functionality). Open-source tools will be used.		

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

Table A.69: T-SNE-UC3-07 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC3-07	Encrypted traffic throughput	TID
Brief Description		
This test measure the average traffic throughput between 2 CNFs with classical and hybrid encryption keys.		
KPI Name(s)		
• Encrypted Traffic Throughput		
Test Procedure		
1. Deploy a network service in K8s with L2S-M to provide connectivity with 2 different CNFs (pods). 2. Enable IPsec with the classical IKEv2. 3. Execute a set of 5 iterations with a duration of 1 min with *iperf* (or a similar tool) to measure the bandwidth between two CNFs protected by IPsec. 4. Enable IPsec with CCIPS implementation and hybrid keys. 5. Repeat step 3.		
Additional Notes		
This test aims to evaluate the impact of the proposed transition approach to bandwidth consumption.		

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

Table A.70: T-SNE-UC3-08 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC3-08	Key generation and management	TID
Brief Description		
This test analyses the network traffic in the data plane between different workloads, searching keys related information exposed during the key generation and exchange phase.		
KPI Name(s)		
• Key Generation and Exchange		
Test Procedure		
1. Deploy a network service in K8s with L2S-M to provide connectivity with 2 different CNFs (pods). 2. Configure a probe or tap in the overlay network defined by L2S-M towards another pod and activate the traffic capture and record. 3. Enable the CCIPS with different hybrid key combinations (classical, PQC and quantum) and interchange a few packets in each mode. 4. Stop the capture and analyze the traffic with *tcpdump* or *wireshark* searching plain text. 5. Identify if keys or related materials has been exposed.		
Additional Notes		
The test assess the processes involved in key lifecycle management, where a security perimeter offered by the facility is assumed, including the generation of secure keys and safe storage.		

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

Table A.71: T-SNE-UC3-09 Test Sheet

Test ID	Test Name	Responsible
T-SNE-UC3-09	IPsec tunnel provisioning	TID
Brief Description		
This test measure the overhead in setting-up the IPsec-based connectivity service. The impact on the re-keying process is based on pre-defined security policies.		
KPI Name(s)		
• IPsec Tunnel Provisioning • IPsec Tunnel Re-keying		
Test Procedure		
1. Deploy a network service with two CNFs. 2. Activate IPsec connectivity over classical IKEv2 and measure the time. 3. Trigger a re-keying process using IKEv2 and measure time. 4. Verify that the hybrid module has enough key to deliver to CCIPS. 5. Repeat the step 2 and 3 process with the CCIPS and hybrid key.		
Additional Notes		
Adding a CCIPS hybrid solution will require additional processes, such as key generation and collection from QKD network, PQ KEM, and key hybridization, jointly with the remote attestation processes. Most of these processes can be executed beforehand (e.g., collecting keys and generating hybrid ones) and are not considered because they are done the first time and do not affect the service's performance later on.		

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

D3.1 – Use Cases and Validation Plan

Version 1.0

Horizon Europe