



Open Call #1: DEVELOP

Annex 2: Technical Annex

Project website	www.pqreact.eu
Opening date:	1 st August 2024
Closing date:	30 th September 2024, 17:00 Brussels time
Open call platform:	Application link

* The deadline for submission is as stated in this Guidelines document. Please note that the platform for submission's time depends on the user's configured timezone and may or may not coincide with the correct time (this depends on the user, not the platform for submission). Any discrepancies in system time will not be grounds for deadline extension

All the Open Call documents and templates are available for download at
<https://tinyurl.com/2n56rnkv>

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101119547. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Union's Horizon Europe research and innovation programme. Neither the European Union nor the granting authority can be held responsible for them.



Table of Contents

1. Purpose of the Technical Annex	4
1.1 General objectives and key results of PQ-REACT	4
3. Use Case 1: Smart Grid Meters	6
4. Use Case 2: 5G and 6G architectures.....	8
5. Use Case 3: Context Agility Manager (PQC Benchmarking)	10
6. Use Case 4: Eclipse - Qrisp for PQC	13





Table 1: ACRONYMS

ACRONYMS	
CPU	Central Processing Unit
EEA	External Evaluator Average
ESR	Evaluation Summary Report
FIF	Financial Identification Form
FSTP	Financial Support to Third Parties
HPC	High Performance Computer
IoT	Internet of Things
KPI	Key Performance Indicators
NIS2	Network and Information Security Directive 2
NIST	National Institute of Standards and Technology
OAS	Overall Average Score
OC	Open Call
PKI	Public key infrastructure
PIC	Participant Identification Code
PQC	Post Quantum Cryptography
QAOA	Quantum Approximate Optimization Algorithm
QC	Quantum computer
QFT	Quantum Fourier transform
QKD	Quantum Key Distribution
SME	Small and medium-sized enterprise
VAT	Value Added Tax
VPN	Virtual private network





1. Purpose of the Technical Annex

The purpose of this annex is to provide applicants with an understanding of the main technical characteristics of the PQ-REACT framework, architecture and tools, and how the proposals can contribute and execute the validation and demonstration of those tools.

It is important to note that this document constitutes essential and complementary information to the Guidelines for Applicants.

1.1 General objectives and key results of PQ-REACT

The objectives described in this chapter serve as a base to understand what the PQ-REACT project will develop:

- **A Framework:** Project aims to design and build a framework for a faster and smoother transition from classical to post-quantum cryptography for a wide variety of contexts and usage domains. We will create an inventory of cryptographic assets and processes in the cryptographic system to be migrated; A recommendation engine to propose a migration plan, taking under consideration the assets and the various contexts that PQC will be employed.
- **Tools & Architecture:** Project will design architectures and develop innovative approaches and tools that enable cryptographic agility and migration to new cryptographic algorithms and standards in an ongoing way. We will create a tool for optimization of the performance of PQC algorithms on various implementation platforms (from large data centers to IoT devices), taking under consideration delay, memory, CPU and energy consumption restrictions; Strategies for the migration of existing network and telecommunication infrastructures and protocols (e.g. PKI, VPN tunnels, certificate chains, etc.) to post-quantum cryptography; QKD technology as a key exchange method for symmetric cryptography related to 5G networks.

2. General Technical Recommendations

As a fundamental part of the application process, we present this Technical Annex detailing the **essential requirements** and **recommendations** for the successful integration of your Use case projects. Keep in mind that the recommendations in this chapter are to be used with your own discernment as they might not be applicable for your selected Use Case.

This document provides a comprehensive guide on the technical criteria to be considered to ensure the efficient implementation and collaboration within the PQ-REACT platform. By adhering to these requirements, you will not only enhance the functionality of your proposals but also facilitate a seamless integration into this specialized environment.

We urge you to carefully review each section of this annex.



Self-Containment and Accessibility:

- Solutions must be self-contained, encompassing all necessary functionalities.
- Input for the service should be facilitated through an API or configuration file, promoting accessibility and ease of use.

Logging Mechanism for Debugging:

- A logging mechanism is crucial, enabling developers and maintainers to efficiently debug errors and ensure smooth operation.

Hardware Agnosticism:

- Solutions should be executable on off-the-shelf hardware.
- Special hardware components (e.g., GPU, TPM) are not required
- If special hardware is required beyond offered in the technical description of each Use Case, it should be provided by the granted company.

Linux OS Compatibility:

- Solutions must be executable on the Linux operating system, ensuring uniformity across the PQ-REACT platform.

Comprehensive Documentation:

- Use case projects are expected to provide thorough documentation, offering detailed deployment instructions and a user guide for efficient implementation.

Collaboration with Platform Developers:

- Any additional requirements or specific needs beyond this document should be communicated and discussed with PQ-REACT developers during the development phase.

Well-Defined API Specification:

- Solutions must feature a well-defined and documented API (*if applicable for selected Use case*), outlining the required input data and the corresponding results computed by the service.

Headless Execution and UI Integration:

- Solutions should be designed for headless execution on a server without a graphical interface.
- If a user interface is necessary, it must be provided through a web-based UI executable on the PQ-REACT platform or an external tool communicating through the specified API.



The following sections describe each Use Case. The general idea behind each Use Case is described: what challenges the proposal should address, what objectives should it aim towards and what the criteria of completion is. It also describes the desired or suggested implementation as well as methodologies and approach.

3. Use Case 1: Smart Grid Meters

[General description]

Smart Meters are usually provided with limited processing and/or storage capabilities, and also typically deployed in environments with low bandwidth. With this kind of constraints upgrading some of the functionalities protected by Asymmetric Crypto to rely Post-Quantum Crypto algorithms can lead to several problems.

Specifically, the test scenario is focused on the Firmware Update functionality. In some real deployments the FW is protected by means of Elliptic Curve Digital Signatures (e.g.: NIST P-256 Curve) just to address the limitations introduced above, and the Use Case target will be to measure/address the challenges raised by migrating to Post-Quantum Digital Signature Algorithms (or mixed classical/PQC deployments).

[Challenges addressing]

- Key Storage in the limited storage capacity of Smart Meters.
- Firmware Update operations on Smart Meters in low bandwidth environments.
- FW Key Update operations on Smart Meters in low bandwidth environments (i.e.: updating Utility Public Key required to verify the FW signature).
- Firmware Update functionality in the limited processing capacity of Smart Meters.
- Crypto Agility scenarios, where the Post-Quantum Digital Signature Algorithm needs to be updated with some frequency because of PQC Algorithm vulnerabilities.

[Objective of the Use Case/ the project should...]

- Measurement (or estimation) of the impact in specific functionalities due to the migration to Post-Quantum Digital Signature Algorithms protecting the Smart Meter FW. For instance:
 - Comparison of the times required to send the Key Update command in classical/PQC scenarios.
 - Comparison of the times required to send the FW Update command in classical/PQC scenarios.
 - Comparison of the times required by the Smart Meter to verify the received FW in classical/PQC scenarios.



Annex 2: Technical Annex

- Impact in the Smart Meter storage capacity because of higher PQC Keys sizes, also considering security implications (e.g.: inability to store the PQC Keys in secure storage)
- Possible operational impact because of frequent FW Update operations required by recurring Post-Quantum Digital Signature Algorithm vulnerabilities.
- Etc....
- Proposal of measures to address the found limitations. For instance: the proposal of specific PQC Algorithms depending on specific limitations scenarios:
 - Scenarios where the main limitation is the Smart Meter storage capacity.
 - Scenarios where the main limitation is the Smart Meter's network bandwidth.
 - Scenarios where the main limitation is the Smart Meter's processing capacity.

[Implementation]

The Project must be carried out preferably in real devices (e.g.: Smart Meters, Data Concentrators, ...) and in networks that can simulate real environments (e.g.: bandwidth and/or noise conditions). It will be admissible to include some results based in estimations when for technical limitations some scenario cannot be fully implemented in real devices (e.g.: based in real data from one classical algorithm in the test environment estimate the impact of PQC algorithm based in data from other environments).

[Open source]

It is admissible to rely on Open Source projects (e.g.: PQC Crypto implementation, Smart Grid network communication libraries, ...) to complete the Project.

[Completion criteria]

The Project results must include at least:

- Description and capabilities (e.g.: memory, processors, ...) of the devices where the Project is implemented.
- Description and capabilities (e.g.: bandwidth, noise simulation capabilities, ...) of network environment where the Project is carried out.
- Description of the different classical (reference) and PQC Scenarios executed. For instance:
 - Digital Signature Cryptographic algorithms, detailing Key & Signature sizes
 - FW size
 - Network conditions
 - Etc....
- Obtained performance classical/PQC results and comparison analysis.
- When possible, proposed measures to address the found problems.





[Suggested approaches and methodologies]

Whenever feasible, it is recommended:

- To start the Project from an already existing Smart Meter platform and testing environment, in order to focus on the PQC challenged not in the development of the platform and test environment.
- To consider more than one Post-Quantum Digital Signature Algorithm and mixed classical/PQC scenarios.

4. Use Case 2: 5G and 6G architectures

[General description]

Leveraging PQC and QKD hybridization approaches related to 5G and their evolution to 6G architectures. PQ-REACT will investigate their application to significant use-cases, especially related to authentication, and protection mechanism for the network infrastructure, addressing the security and performance requirements in highly-pervasive, critical networked environments.

Both infrastructures are part of the proposed EuroQCI-Spain network, and therefore suitable to extend experiments beyond, through the HellasQCI.

MadQCI environment: The QKD pilots will be demonstrated on the MadQCI environment, currently the largest QKD network deployed in Europe, connected to the 5TONIC testbed, an experimental infrastructure for next-generation network technologies and services, instrumental in the execution of many H2020, and now Horizon Europe projects regarding networking.

[Challenges addressing]

- Integration of standard QKD architectures (ETSI GS QKD 018 or ITU-T Y.3818) and PQC to address 5G network connectivity securely.
- Novel hybridization algorithms and techniques that combine QKD, PQC and classical algorithms to address main protocols related to 5G communications.
- Quantum Secure PKI solutions for 5G infrastructures
- Crypto agility for 5G and beyond scenarios
- Performance and impact evaluation on 5G network infrastructure for the PQC PKI use and QKD adoption.

[Objective of the Use Case / the project should...]

The goals of the Use Case involve addressing one or more of the following objectives:

- *Integration of QKD and PQC in 5G networks connectivity plane*
The objective is to propose solutions and evaluate the performance impact in 5G network connectivity with the integration of complementary technologies (QKD, classical and PQC), such as hybridization techniques (not limited), for the connectivity plane (data and control





Annex 2: Technical Annex

protocols). Results should be compared with classical existing approaches. The objective includes to measure the impact in:

- IT Resource consumption (CPU, Memory)
- Network resource consumption (bytes per second, packets per second)
- Network performance (delay in secure channel establishment, overhead in packets, fragmentation, etc.)

Expected outcomes include the identification of the recommended approach supported by measurements.

- *PKI impact in 5G networks management*

The objective is to evaluate the performance impact in the management process for identification and authentication of different 5G network components and services (backhaul, core, roaming) based on a quantum secure Public Key Infrastructure. Aspects to evaluate are:

- PQC algorithms selection to address 5G network management demands.
- Good practices and guidelines to deploy a Quantum Secure PKI in a 5G network (certificates lifetime, key size, etc.)
- Scalability analysis
- Applicability of PKI for QKD authentication

Expected outcomes include the identification of the recommended approach supported by results.

[Implementation]

The Project will be executed in a virtualized and programable infrastructure environment that will allow to deploy basic 5G functionalities, specifically those related to backhaul, core and roaming connectivity. Radio functionalities are not the focus for this Use Case.

[Open source]

Not mandatory but recommended. Any extension over existing open-source frameworks is welcome to enhance the community and provide guidelines, experiences, and repeatability. Some examples of open-source initiatives aligned with the Use Case are:

- Performance evaluation framework: QUJATA
- 5G networks: Open5Gs, Free5G, UERANSIM
- PKI: OpenSSL
- Crypto libraries: liboqs

[Completion criteria]

The completion criteria will require:

- Delivery of developed tools and applications to address the objectives.





- In case of proprietary solutions, licenses, manual and support during the PQ-REACT project lifetime are required.
- In case of open-source tools, the public access to the same.
- Complete documentation detailing architectural design of the Project software involved, KPI defined, test executed, results and recommendations.
- Solution demonstration and presentation on public event or in a dedicated PQ-REACT consortium event.

[Suggested approaches and methodologies]

Follow-up existing standards and recommendation (GSMA, 3GPP, ETSI, IETF) for PQ transition in the design decision, such as QKD, PQC and hybridization algorithms or performance KPIs to measure.

Adopt open-source solutions, including testing frameworks, crypto libraries and applications, extending public repositories of code.

5. Use Case 3: Context Agility Manager (PQC Benchmarking)

[General description]

Test and validation of innovative services/apps that use PQC algorithms, in terms of various parameters like CPU, memory, power consumption, bandwidth, etc., over a virtualized infrastructure via a monitoring tool provided by the project. The algorithms may be NIST approved or submitted in the [NIST Post-Quantum Cryptography Standardization Call for proposals](#).

NCSRD's (Network Operations Center (NOC)): Designed to be the nerve center for the pilot project on Context Agility Manager (PQC Benchmarking) pilot. This specialized NOC serves as the hub for monitoring, management, and maintenance of the network infrastructure that supports the pilot, as well as remote connectivity for the OC application winners.

Equipped with state-of-the-art technology and staffed by experts in the field, the NOC aims to ensure the seamless execution of Post-Quantum Cryptography (PQC) algorithms in the Context Agility Manager Framework.

[Challenges addressing]

The test and validation of innovative services and applications utilizing Post-Quantum Cryptography (PQC) algorithms present several challenges, particularly when evaluated across multiple parameters such as CPU usage, memory consumption, power consumption, and bandwidth. These evaluations are conducted over a virtualized infrastructure using a monitoring tool provided by the project. Key challenges include:





- **Algorithm Diversity and Complexity:** The PQC algorithms under evaluation may be either NIST-approved or submitted in the NIST Post-Quantum Cryptography Standardization Call for proposals. This diversity introduces complexity in testing, as each algorithm has distinct characteristics and requirements, necessitating tailored testing protocols and methodologies.
- **Resource Consumption:** Accurately measuring the impact of PQC algorithms on CPU, memory, and power consumption is challenging due to the algorithms' computational intensity. Ensuring that these measurements reflect real-world usage scenarios within a virtualized infrastructure adds an additional layer of complexity.
- **Performance Metrics:** Balancing performance metrics such as bandwidth utilization while maintaining robust security features is critical. Determining optimal performance without compromising security is a nuanced challenge, requiring extensive testing and analysis.
- **Virtualization Overhead:** Testing within a virtualized infrastructure introduces potential overhead that can affect performance metrics. Differentiating between the inherent resource demands of PQC algorithms and the overhead introduced by virtualization is essential for accurate assessment.
- **Tool Accuracy and Reliability:** The reliability and accuracy of the monitoring tool are paramount. Any discrepancies in data collection or analysis can lead to incorrect conclusions, impacting the overall evaluation process. Ensuring the tool's precision and consistency across diverse testing scenarios is crucial.
- **Scalability and Real-World Simulation:** Simulating real-world conditions and ensuring the scalability of services and applications under the stress of PQC algorithms pose significant challenges. The ability to replicate large-scale deployment conditions within a controlled virtualized environment is essential for comprehensive validation.

[Objective of the Use Case / the project should...]

- **Scalability and Robustness Testing:**
 - Objective: To assess the scalability and robustness of PQC protocols under high-traffic conditions and large-scale deployments.
 - Expected Outcome: Validation of PQC protocols' ability to maintain performance and security standards in large, dynamic environments.
- **Energy Efficiency Analysis:**
 - Objective: To evaluate the energy consumption of PQC algorithms and identify methods to optimize power usage in client-server interactions.





Annex 2: Technical Annex

- Expected Outcome: Recommendations for energy-efficient implementations of PQC protocols, contributing to greener technology solutions.
- **Interoperability with Existing Systems:**
 - Objective: To ensure that PQC algorithms can seamlessly integrate with current communications protocols and networks, including widely used protocols such as curl, HTTP, and nginx.
 - Expected Outcome: Demonstration of PQC algorithms' compatibility with existing infrastructure, facilitated by implementations based on liboqs where possible.
- **Protocol-Specific Performance Testing:**
 - Objective: To test PQC algorithms across different widely used protocols such as curl, HTTP, and nginx, leveraging the liboqs library.
 - Expected Outcome: Detailed performance metrics and insights into how various PQC algorithms perform within these widely adopted protocols, providing practical guidelines for developers and engineers.

[Implementation]

The implementation shall be carried out across different hosts connected with each other to assess connectivity and performance across their inter-communication. NCSRD will provide a subset of private virtualized infrastructure where the experimenters can finally assess their proposed applications, in terms of energy efficiency, performance, resource consumption, etc.

[Open source]

The underlying testbed will be based on the Open Source framework Qujata. The Qujata project aims to evaluate the performance of supported Post-Quantum Cryptography (PQC) protocols through a testbed that assesses client and server vital signs, including memory and CPU usage, connection time, and download speed. Various Projects applying for the open call can have diverse objectives, reflecting the specific needs and goals of their respective domains.

[Completion criteria]

To ensure the successful completion of the test and validation of innovative services and applications utilizing Post-Quantum Cryptography (PQC) algorithms, the following criteria must be met:

- **Comprehensive Performance Evaluation:**
 - Successful measurement and documentation of CPU usage, memory consumption, power consumption, and bandwidth utilization for each PQC algorithm under evaluation.
 - Clear differentiation between the inherent resource demands of PQC algorithms and the overhead introduced by the virtualized infrastructure.
- **Algorithm Compatibility:**





- Demonstrated interoperability of PQC algorithms with existing communication protocols and networks, including widely used protocols such as curl, HTTP, and nginx.
- Verification of PQC algorithms' compatibility with the liboqs library.
- Scalability and Robustness:
 - Validation of the PQC protocols' ability to maintain performance and security standards under high-traffic conditions and large-scale deployments.
 - Documentation of PQC algorithms' behavior and performance in simulated real-world conditions.
- Energy Efficiency:
 - Comprehensive analysis of the energy consumption of PQC algorithms.
 - Recommendations for optimizing power usage in client-server interactions.
- Accuracy and Reliability of Monitoring Tools:
 - Ensuring the precision and consistency of the monitoring tool provided by the project across diverse testing scenarios.
 - Addressing any discrepancies in data collection or analysis.

[Suggested approaches and methodologies]

Diverse Algorithm Testing:

Evaluate a wide range of PQC algorithms, including those approved by NIST and those submitted to the NIST Post-Quantum Cryptography Standardization Call for proposals. Tailor testing protocols to address the unique characteristics and requirements of each algorithm.

6. Use Case 4: Eclipse - Qrisp for PQC

[General description]

Practical validation and assessment of the resilience of new applications/solutions (including IoTs) using PQC techniques, exploiting the capabilities of an HPC (High Performance Computer) or QC (Quantum Computer) via a suite of tools (C++/Python/Qrisp). Additional tools like, Quantum Approximate Optimization Algorithm (QAOA), Shor's algorithm, algorithmic primitives (e.g., quantum Fourier transform (QFT), quantum phase estimation (QPE)) and solving QUBO problem instances with QAOA are available in Qrisp.

The project aims to build a portfolio of open tools for evaluation of the resilience of PQC algorithms and cryptanalytical methods. These tools will enable benchmarking new PQC algorithms and new cryptanalytical methods with quantum computing and high-performance computing resources. The high-level programming framework Eclipse Qrisp, developed by scientists at Fraunhofer FOKUS, enables developers to write quantum code with ease.

[Challenges addressing]





Shor's algorithm, probably the most famous quantum algorithm in cryptanalysis, can efficiently factorize large numbers and thereby break the widely used RSA public key cryptosystem. Therefore, such quantum-insecure algorithms must be replaced by post-quantum cryptography algorithms which are conjectured to be secure against quantum attacks. Typically, the security of such PQC algorithms is based on the hardness of solving a mathematical problem, e.g., learning with errors or multivariate polynomial equations, hash functions. In this Use Case the resilience of relevant PQC algorithms with respect to quantum or hybrid quantum-classical attacks should be validated. That is, it should be tested if PQC algorithms are indeed robust against quantum attacks, and under which conditions (e.g. side channel information) they are not secure anymore.

[Objective of the Use Case / the project should...]

A quantum or hybrid quantum-classical attack against a relevant PQC algorithm (i.e., NIST candidates) shall be implemented using open-source tools such as Python and the python-based high-level programming framework Eclipse Qrisp.

- Testing:
 - The attack should be tested against small sized instances of the underlying mathematical problem for the PQC algorithm. Quantum algorithms may be tested on classical devices using the Qrisp simulator.
- Complexity analysis:
 - An analysis of the quantum algorithm in terms of suitable metrics, e.g., qubit count, gate count or circuit depth.
- Scalability analysis:
 - Based on the results of the testing and the complexity analysis, the scalability of the proposed quantum attack should be discussed.

[Implementation]

The implementation shall be carried out using open-source software and libraries such as Python (NumPy, SciPy, etc.), and the python-based framework Eclipse Qrisp for quantum algorithms.

[Open source]

The implementation shall be carried out using open-source software.

[Completion criteria]

To demonstrate the efficiency of the implemented attacker the following items should be considered:

- Generate secret keys of different lengths and try to reconstruct them by means of the implemented quantum or hybrid-quantum attacker. If the PQC-algorithm is based on a learning with error problem (LWE problem), the length of secret key can be increased by





Annex 2: Technical Annex

increasing the dimension of the underlying LWE problem. A LWE problem consists of a linear system of equations whose matrix and right-hand side are sampled from a probability distribution over a modular ring. The solution of this linear system of equations represents the secret key. Perform the test described in the last item many times. Thereby, the number of successful attacks should be counted for each key length. By this, a success probability of the implemented attacker for a given key can be computed. Represent your results by means of an appropriate data structure or table such that a potential user of the attacked cryptosystem can look up its security level.

[Suggested approaches and methodologies]

The performance of the attackers that have been implemented should be tested by means of a Lattice based cryptosystem that is described in the following NIST report:

National Institute of Standards and Technology, “FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard,” <https://csrc.nist.gov/pubs/fips/203/ipd>, 202

To test the resilience of secret keys with a certain length, the key generator described in the report from above could be reimplemented such that smaller keys can be produced. This is necessary, since many quantum-based attackers can reconstruct only small keys. Furthermore, nowadays quantum hardware also only the handling of small test problems. This is due to the fact that only a few qubits are available and that there is no effective error correction.

Inform yourself about algorithms or means reducing the computational effort that is required to reconstruct the secret key or the solution of a given LWE problem. Well-known algorithms in this context are the LLL algorithm or the BKZ algorithm. Apart from that information from side-channel attacks could be used.

