Post-Quantum Cryptography As-a-Service for Common Transmission Systems and Infrastructures

Announcement letter

EUROPEAN PARTNERSHIP

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

We are excited to introduce the PIQASO Digital Europe Action, a groundbreaking initiative aimed at implementing a robust framework for "Post-Quantum Cryptography As-a-Service for Common Transmission Systems (CTS) and Infrastructures." This initiative is designed to address the urgent need for quantum-safe cryptographic solutions in an increasingly connected and data-driven world.

The PIQASO project officially launched on January 1st, with a kick-off meeting held on January 22-23 in Athens. Funded by the European Commission, PIQASO will run from January 2025 to December 2027, providing an essential foundation for secure communication and data protection against quantum-enabled cyber threats.

The Challenge: As quantum computing advances, traditional cryptographic methods are becoming increasingly vulnerable. The National Institute of Standards and Technology (NIST) has taken significant strides in standardizing Post-Quantum Cryptography (PQC) algorithms to safeguard against these threats. However, migrating from existing cryptographic systems to quantum-safe alternatives presents a complex challenge that requires seamless integration with legacy infrastructures while maintaining high levels of security, agility, and scalability.

About PIQASO: PIQASO aims to provide a comprehensive suite of quantum-safe cryptographic services, ensuring secure and future-proof communication in the face of quantum computing threats. Our "as-a-service" solution will cover a range of cryptographic algorithms and protocols, including key encapsulation, digital signatures, key exchange, and authentication, safeguarding infrastructures without requiring additional specialist hardware.

How PIQASO Works: The PIQASO solution consists of three core components:

- **PQC Ensemble**: A cutting-edge cryptographic SDK leveraging lattice-based Key Encapsulation Mechanisms (KEMs) and digital signature algorithms to ensure secure storage, authentication, and data integrity.
- **PQ Data Encryption Server (PQ-DS)**: A cloud-based security hub that offers PQC encryption, signing, and authentication functionalities to end-users through an agile, software-based approach.
- **Crypto Agility Layer**: A programmable microservices architecture enabling flexible cryptographic operations through APIs, ensuring adaptability and future-proofing security measures.

Real-World Application and Industry Engagement: PIQASO's ambitious demonstration plan includes involvement from 14 end-users across diverse sectors, such as automotive, finance, healthcare, and aerospace. These demonstrations will showcase the practical integration and application of quantum-safe encryption services, reinforcing the project's impact across critical industries.

Why This Matters: Migrating to PQC is a complex but necessary process to future-proof our industries against quantum-based cyber threats. PIQASO offers a seamless, scalable, and cost-effective path for businesses and governments to adopt quantum-safe security without disrupting existing systems. By proactively embracing PQC solutions today, we can mitigate the risks of future quantum attacks and ensure long-term data integrity and confidentiality.

Join Us in Securing the Future We invite researchers, industry stakeholders, policymakers, and technology leaders to collaborate with us in this crucial endeavor. Together, we can pave the way for a quantum-secure digital future.

Stay updated with PIQASO's latest developments and impact by following us on our official channels and social media platforms.

For inquiries and collaboration opportunities, please contact us at [insert contact email].

Let's build a secure, quantum-resistant future—today!

Best Regards,
Savvoula Oikonomou
Project Coordinator

PIQASO Consortium
info@piqasoproject.eu

PiQASO

Post-Quantum Cryptography As-a-Service for Common Transmission Systems and Infrastructures

The project funded under Grant Agreement No. 101190366 is supported by the European Cybersecurity Competence Centre

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them."